Microsoft

Informe de defensa digital de Microsoft 2022

Iluminar el panorama de las amenazas y potenciar una defensa digital.

Índice

Los datos, la información y los eventos de este informe corresponden al periodo comprendido entre julio de 2021 y junio de 2022 (año fiscal 2022 de Microsoft), a menos que se indique lo contrario.

Para una mejor experiencia en la visualización y navegación de este informe, recomendamos el uso de Adobe Reader, disponible como descarga gratuita en el sitio web de Adobe.

Introducción de Tom Burt

Vicepresidente corporativo, Seguridad y confianza del cliente

"Los billones de señales que analizamos de nuestro ecosistema mundial de productos y servicios revelan la ferocidad, el alcance y la escala de las amenazas digitales en todo el mundo"

Una instantánea de nuestro panorama...

Alcance y escala del panorama de amenazas

El volumen de ataques a las contraseñas ha aumentado hasta un estimado de 921 ataques cada segundo, un aumento del 74 % en solo un año.

Desmantelamiento de la ciberdelincuencia

Hasta la fecha, Microsoft ha eliminado más de 10 000 dominios utilizados por los ciberdelincuentes y 600 utilizados por actores de estado nación.

Cómo hacer frente a las vulnerabilidades

El 93 % de nuestros compromisos de respuesta ante incidentes de ransomware revelaron controles insuficientes sobre el acceso a privilegios y el movimiento lateral.

El 23 de febrero de 2022, el mundo de la ciberseguridad entró en una nueva era, la era de la guerra híbrida. Ese día, horas antes de que se lanzaran los misiles y los tanques atravesaran las fronteras, los actores rusos lanzaron un ataque cibernético masivo y destructivo contra objetivos del gobierno, la tecnología y el sector financiero ucranianos. Puede leer más sobre estos ataques y las lecciones que hay que aprender de ellos en el capítulo de Amenazas para los estados nación de esta tercera edición anual del Informe de defensa digital de Microsoft (MDDR). La clave de estas lecciones es que la nube proporciona la mejor seguridad física y lógica contra los ataques cibernéticos y permite avances en la inteligencia de amenazas y la protección de puntos de conexión que han demostrado su valor en Ucrania.

Aunque cualquier estudio sobre los avances del año en materia de ciberseguridad debe comenzar por ahí, el informe de este año ofrece una inmersión profunda mucho más detallada. En el primer capítulo del informe, nos enfocamos en las actividades de los ciberdelincuentes, seguidas de las amenazas para los estados nación en el segundo capítulo. Ambos grupos han aumentado enormemente la sofisticación de sus ataques, lo que ha incrementado de manera drástica el impacto de sus acciones. Mientras Rusia acaparaba los titulares, los actores iraníes intensificaron sus ataques tras la transición del poder presidencial, lanzando ataques destructivos dirigidos a Israel, y operaciones de ransomware y pirateo y filtración dirigidas a infraestructuras críticas en Estados Unidos. China también ha incrementado sus actividades de espionaje en el sudeste asiático y en otros lugares del sur del mundo, tratando de contrarrestar la influencia de Estados Unidos y de robar datos e información críticos.

Los actores extranjeros también están usando técnicas muy eficaces para permitir las operaciones de influencia propagandística en regiones de todo el mundo, como se trata en el tercer capítulo. Por ejemplo, Rusia se ha esforzado por convencer a sus ciudadanos, y a los ciudadanos de muchos otros países, de que su invasión de Ucrania estaba justificada, a la vez que ha sembrado la propaganda de descrédito de las vacunas COVID en occidente y ha promovido simultáneamente su eficacia en el país. Además, los actores están apuntando cada vez más a los dispositivos de la Internet de las Cosas (IoT) o a los dispositivos de control de la tecnología de operaciones (OT) como puntos de entrada a las redes y a la infraestructura crítica, lo que se analiza en el capítulo cuatro. Finalmente, en el último capítulo, entregamos las ideas y lecciones que hemos aprendido durante el pasado año en la defensa contra los ataques dirigidos a Microsoft y a nuestros clientes, al tiempo que repasamos los avances del año en materia de resiliencia cibernética.

En cada capítulo se proporcionan las principales lecciones aprendidas y la información basada en el punto de vista único de Microsoft. Los billones de señales que analizamos de nuestro ecosistema mundial de productos y servicios revelan la ferocidad, el alcance y la escala de las amenazas digitales en todo el mundo. Microsoft está tomando medidas para defender a nuestros clientes y al ecosistema digital contra estas amenazas, y puede leer sobre nuestra tecnología que identifica y bloquea miles de millones de intentos de phishing, robos de identidad y otras amenazas para nuestros clientes.

Introducción de Tom Burt

Continuación

También utilizamos medios legales y técnicos para incautar y cerrar la infraestructura utilizada por los ciberdelincuentes y los actores de estado nación, y notificar a los clientes cuando están siendo amenazados o atacados por un actor de estado nación. Trabajamos para desarrollar funciones y servicios cada vez más eficaces que utilizan la tecnología de IA/ML para identificar y bloquear las ciberamenazas, y los profesionales de la seguridad se defienden e identifican las intrusiones cibernéticas con mayor rapidez y eficacia.

Y lo que es más importante, a lo largo del MDDR ofrecemos nuestros mejores consejos sobre las medidas que pueden tomar los individuos, las organizaciones y las empresas para defenderse de estas crecientes amenazas digitales. Adoptar buenas prácticas de ciberhigiene es la mejor defensa y puede reducir considerablemente el riesgo de ciberataques.

El estado de la ciberdelincuencia

Los ciberdelincuentes siguen actuando como sofisticadas empresas con ánimo de lucro. Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad de cómo y dónde alojan la infraestructura de operación de las campañas. Al mismo tiempo, los ciberdelincuentes son cada vez más frugales. Para reducir sus gastos generales y aumentar la apariencia de legitimidad, los atacantes están comprometiendo las redes y los dispositivos de las empresas para hospedar campañas de suplantación de identidad (phishing), malware o incluso utilizar su potencia de cálculo para minar criptomonedas.

> Más información en la página 6

"La llegada de la implementación de armas cibernéticas en la guerra híbrida de Ucrania es el inicio de una nueva era de conflictos".

Amenazas para los estados nación

Los actores de estado nación lanzan ciberataques cada vez más sofisticados, diseñados para evadir la detección y promover sus prioridades estratégicas. La llegada de la implementación de armas cibernéticas en la guerra híbrida de Ucrania es el inicio de una nueva era de conflictos. Rusia también ha apoyado su guerra con operaciones de influencia informativa, utilizando la propaganda para influir en las opiniones de Rusia, Ucrania y el resto del mundo. Fuera de Ucrania, los actores de estado nación han aumentado su actividad y han comenzado a utilizar los avances en la automatización, la infraestructura en la nube y las tecnologías de acceso remoto para atacar un conjunto más amplio de objetivos. Las cadenas de suministro de TI corporativas que permiten el acceso a los objetivos finales fueron atacadas con frecuencia. La higiene de la ciberseguridad se volvió aún más crítica cuando los actores explotaron rápidamente las vulnerabilidades sin revisiones, utilizaron técnicas sofisticadas y de fuerza bruta para robar credenciales y ofuscaron sus operaciones utilizando software open source o legítimo. Además, Irán se une a Rusia en el uso de ciberarmas destructivas, incluido el ransomware, como elemento básico de sus ataques.

Estos acontecimientos exigen la adopción urgente de un marco global coherente que dé prioridad a los derechos humanos y proteja a las personas del comportamiento imprudente del estado en línea. Todas las naciones deben trabajar juntas para aplicar las normas y reglas para una conducta de estado responsable.

> Más información en la página 30

Dispositivos e infraestructura

La pandemia, unida a la rápida adopción de dispositivos de todo tipo conectados a Internet como componente de la aceleración de la transformación digital, ha aumentado de manera considerable la superficie de ataque de nuestro mundo digital. Como resultado, los ciberdelincuentes y los estados nación se están aprovechando rápidamente. Mientras que la seguridad del hardware y el software de TI se ha reforzado en los últimos años, la seguridad de los dispositivos de IoT y OT no ha seguido el ritmo. Los actores de amenaza están explotando estos dispositivos para establecer el acceso en las redes y permitir el movimiento lateral, para establecer un punto de apoyo en una cadena de suministro, o para interrumpir las operaciones de OT de la organización objetivo.

> Más información en la página 56

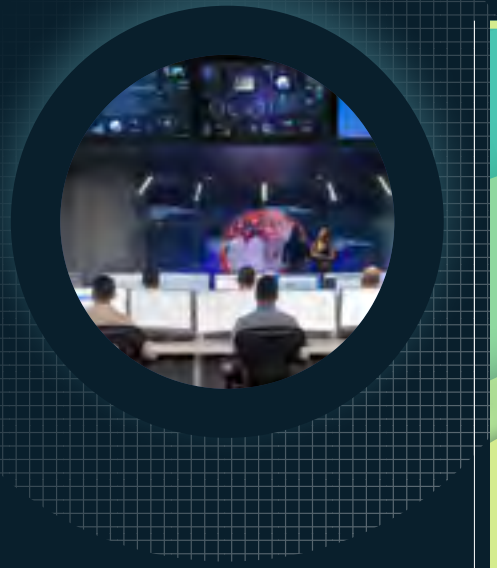
Introducción de Tom Burt

Continuación

Operaciones de influencia cibernética

Los estados nación recurren cada vez más a sofisticadas operaciones de influencia para distribuir propaganda e influir en la opinión pública, tanto en el nivel nacional como en el internacional. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos. Los actores expertos en manipulación persistente avanzada están utilizando los medios de comunicación tradicionales junto con Internet y las redes sociales para aumentar enormemente el alcance, la escala y la eficacia de sus campañas, así como el impacto desmesurado que están teniendo en el ecosistema informativo mundial. En el último año, hemos visto cómo estas operaciones se han utilizado como parte de la guerra híbrida de Rusia en Ucrania, pero también hemos visto cómo Rusia y otras naciones, incluidas China e Irán, implementan cada vez más operaciones de propaganda impulsadas por las redes sociales para ampliar su influencia global en una serie de temas.

Más información en la página 71



Resiliencia cibernética

La seguridad es un factor clave del éxito tecnológico. La innovación y la mejora de la productividad solo pueden conseguirse al introducir medidas de seguridad que hagan a las organizaciones lo más resilientes posible contra los ataques modernos. La pandemia nos ha desafiado en Microsoft a dar un giro a nuestras prácticas y tecnologías de seguridad para proteger a nuestros empleados dondequiera que trabajen. El año pasado, los actores de amenaza continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido administrar la prevalencia y la complejidad de diversos métodos de ataque y el aumento de la actividad de los estados nación. En este capítulo, detallamos los desafíos a los que nos hemos enfrentado y las defensas que hemos movilizado en respuesta con nuestros más de 15 000 socios.

Más información en la página 86

Nuestro punto de vista único

37 mil millones
de amenazas de correo electrónico bloqueadas

34,7 mil millones
amenazas de identidad bloqueadas

43 billones
de señales sintetizadas a diario, utilizando sofisticados análisis de datos y algoritmos de IA para comprender y proteger contra las amenazas digitales y la ciberactividad delictiva.

2,5 mil millones
de señales de puntos de conexión analizados a diario

Más de 8500
ingenieros, investigadores, científicos de datos, expertos en ciberseguridad, cazadores de amenazas, analistas geopolíticos, investigadores y personal de primera línea de 77 países.

Más de 15 000
socios de nuestro ecosistema de seguridad que aumentan la resiliencia cibernética de nuestros clientes.

Del 1 de julio de 2021 al 30 de junio de 2022

Introducción de Tom Burt

Continuación

Creemos que Microsoft,-de forma independiente y a través de estrechas colaboraciones con otros miembros de la industria privada, el gobierno y la sociedad civil, tiene la responsabilidad de proteger los sistemas digitales que sustentan el tejido social de nuestra sociedad y promover entornos informáticos seguros para todas las personas, estén donde estén. Esta responsabilidad es la razón por la que hemos publicado el MDDR cada año desde 2020. El informe es la culminación de los amplios datos y la exhaustiva investigación de Microsoft. Comparte nuestra visión única sobre cómo está evolucionando el panorama de las amenazas digitales y las acciones cruciales que se pueden tomar hoy para mejorar la seguridad del ecosistema.

Esperamos infundir un sentido de urgencia, para que los lectores tomen medidas inmediatas basadas en los datos y las ideas que presentamos tanto aquí como en nuestras numerosas publicaciones sobre ciberseguridad a lo largo del año. Al considerar la gravedad de la amenaza en el panorama digital, y su traslación al mundo físico, es importante recordar que todos estamos facultados para tomar medidas para protegernos a nosotros mismos, a nuestras organizaciones y a las empresas contra las amenazas digitales.

Gracias por tomarse el tiempo de revisar el Informe de defensa digital de Microsoft de este año. Esperamos que le proporcione una visión y unas recomendaciones valiosas para ayudarnos a defender colectivamente el ecosistema digital.

Tom Burt
Vicepresidente corporativo,
Seguridad y confianza del cliente

Nuestro objetivo con este informe es doble:

1. Iluminar el panorama de las amenazas digitales en evolución para nuestros clientes, socios y partes interesadas que abarcan el ecosistema más amplio, iluminando tanto los nuevos ciberataques como las tendencias en evolución de las amenazas históricamente persistentes.
2. Empoderar a nuestros clientes y socios para mejorar su resiliencia cibernética y responder a estas amenazas.

El estado de la ciberdelincuencia

A medida que las ciberdefensas mejoran y más organizaciones adoptan un enfoque proactivo de prevención, los atacantes adaptan sus técnicas.

Información general del estado de la ciberdelincuencia

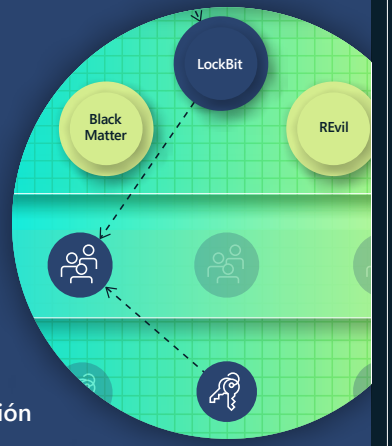
A medida que las ciberdefensas mejoran y más organizaciones adoptan un enfoque proactivo de prevención, los atacantes adaptan sus técnicas.

Los ciberdelincuentes siguen actuando como sofisticadas empresas con ánimo de lucro. Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad de cómo y dónde alojan la infraestructura de operación de las campañas. Al mismo tiempo, los ciberdelincuentes son cada vez más frugales. Para reducir sus gastos generales y aumentar la apariencia de legitimidad, los atacantes están comprometiendo las redes y los dispositivos de las empresas para hospedar campañas de suplantación de identidad (phishing), malware o incluso utilizar su potencia de cálculo para minar criptomonedas.

La ciberdelincuencia sigue aumentando a medida que la industrialización de la economía de la ciberdelincuencia reduce la barrera de entrada de las habilidades al proporcionar un mayor acceso a las herramientas y la infraestructura.

Más información en la página 18

La amenaza del ransomware y la extorsión es cada vez más audaz, con ataques dirigidos a gobiernos, empresas e infraestructuras críticas.

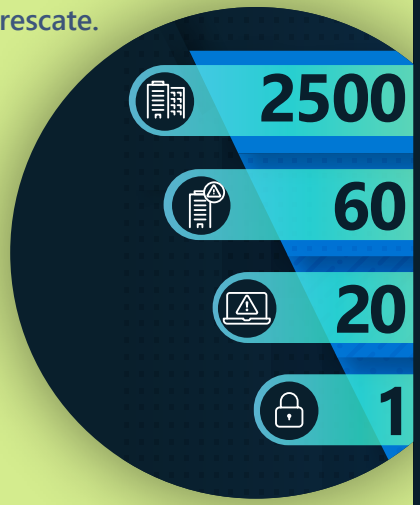


Más información en la página 9

Los atacantes amenazan cada vez más con revelar datos sensibles para fomentar el pago de rescates.

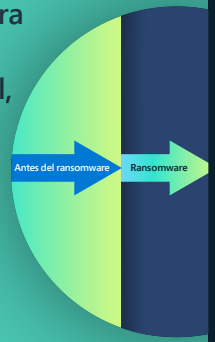
Más información en la página 10

El ransomware operado por humanos es el más frecuente, ya que un tercio de los objetivos se ven comprometidos con éxito por los delincuentes que utilizan estos ataques y el 5 % de ellos reciben un rescate.



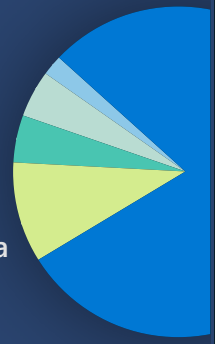
Más información en la página 9

La defensa más eficaz contra el ransomware incluye la autenticación multifactorial, los revisiones de seguridad frecuentes y los principios de Confianza cero en toda la arquitectura de la red.



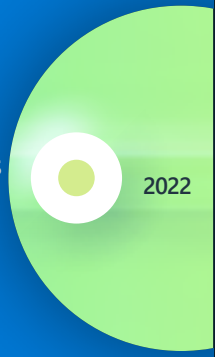
Más información en la página 13

Los esquemas de phishing de credenciales que se dirigen indiscriminadamente a todas las bandejas de entrada van en aumento y el compromiso del correo electrónico comercial, incluido el fraude de facturas, supone un importante riesgo de ciberdelincuencia para las empresas.



Más información en la página 21

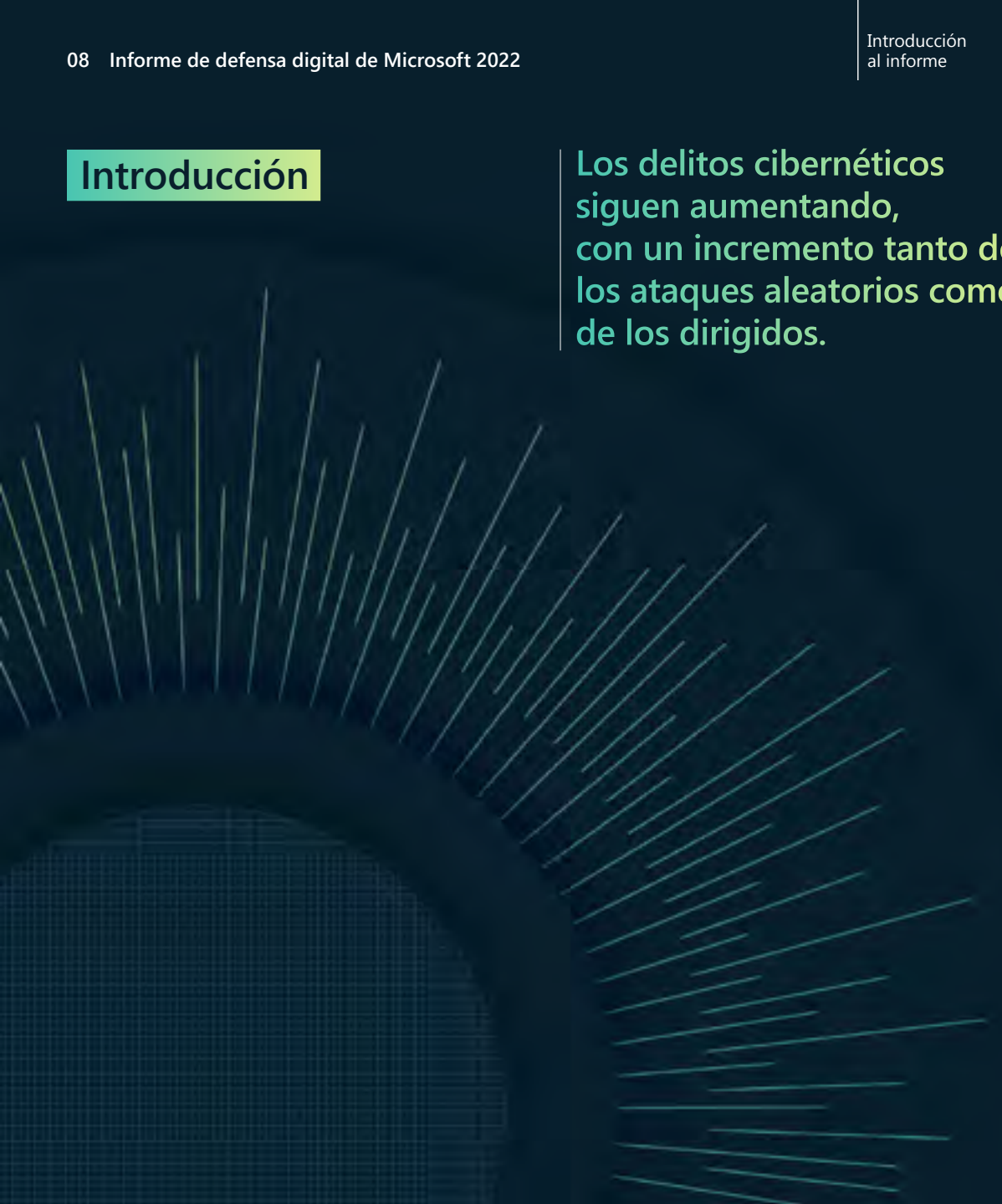
Para desbaratar las infraestructuras malintencionadas de los ciberdelincuentes y de los actores de estado nación, Microsoft se basa en enfoques legales innovadores y en nuestras asociaciones públicas y privadas.



Más información en la página 25

Introducción

Los delitos cibernéticos siguen aumentando, con un incremento tanto de los ataques aleatorios como de los dirigidos.



A medida que las ciberdefensas mejoran y más gobiernos y empresas adoptan un enfoque proactivo para la prevención, vemos que los atacantes utilizan dos estrategias para obtener el acceso necesario para facilitar la ciberdelincuencia. Un enfoque es una campaña con objetivos amplios que se basa en el volumen. El otro utiliza la vigilancia y una orientación más selectiva para aumentar la tasa de rendimiento. Incluso cuando la generación de ingresos no es el objetivo, como en el caso de la actividad de los estados nación con fines geopolíticos, se utilizan tanto los ataques aleatorios como los dirigidos. El año pasado, los ciberdelincuentes siguieron apostando por la ingeniería social y la explotación de temas de actualidad para maximizar el éxito de lasz campañas. Por ejemplo, mientras que los señuelos de phishing con temática COVID se utilizaban con menos frecuencia, observamos que aumentaban los señuelos que solicitaban donaciones para apoyar a los ciudadanos de Ucrania.

Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad de cómo y dónde alojan la infraestructura de operación de las campañas. Hemos observado que los ciberdelincuentes se han vuelto más austeros y los atacantes ya no pagan por la tecnología. Para reducir sus gastos generales y aumentar la apariencia de legitimidad, algunos atacantes buscan cada vez más comprometer a las empresas para hospedar campañas phishing, malware o incluso utilizar su potencia de cálculo para minar criptomonedas.

En este capítulo, también examinamos el aumento del hacktivismo, una perturbación provocada por ciudadanos privados que realizan ciberataques para promover objetivos sociales o políticos. Miles de personas en todo el mundo, tanto expertos como novatos, se han movilizado desde febrero de 2022 para lanzar ataques como la inutilización de sitios web y la filtración de datos robados en el marco de la guerra entre Rusia y Ucrania. Es demasiado pronto para predecir si esta tendencia continuará tras el fin de las hostilidades activas.

Las organizaciones deben revisar y reforzar periódicamente los controles de acceso y aplicar estrategias de seguridad para defenderse de los ciberataques. Sin embargo, eso no es todo lo que pueden hacer. Explicamos cómo nuestra Unidad de delitos digitales (DCU) ha utilizado los casos civiles para incautar la infraestructura malintencionada que usan los ciberdelincuentes y los actores de estado nación. Debemos luchar juntos contra esta amenaza mediante asociaciones públicas y privadas. Esperamos que al compartir lo que hemos aprendido en los últimos 10 años, ayudemos a otros a entender y considerar las medidas proactivas que pueden tomar para protegerse a sí mismos y al ecosistema en general contra la amenaza continuamente creciente de la ciberdelincuencia.

Amy Hogan-Burney
Gerente general, Unidad de delitos digitales

Ransomware y extorsión: una amenaza de nivel nacional

Los ataques de ransomware suponen un peligro cada vez mayor para todas las personas, ya que las infraestructuras críticas, las empresas de todos los tamaños y los gobiernos estatales y locales son el objetivo de los delincuentes que aprovechan un ecosistema de delincuencia cibernética en crecimiento.

En los últimos dos años, los incidentes de ransomware de alto perfil (como los que afectan a las infraestructuras críticas, la salud y los proveedores de servicios de TI) han atraído una considerable atención pública. A medida que los ataques de ransomware se han vuelto más audaces en su alcance, sus efectos se han vuelto más amplios. Los siguientes son ejemplos de ataques que ya hemos visto en 2022:

- En febrero, un ataque a dos empresas afectó a los sistemas de procesamiento de pagos de cientos de gasolineras del norte de Alemania.[1]
- En marzo, un ataque contra el servicio postal griego interrumpió temporalmente la entrega del correo y afectó al procesamiento de las transacciones financieras.[2]
- A fines de mayo, un ataque de ransomware contra organismos gubernamentales de Costa Rica obligó a declarar una emergencia nacional tras el cierre de hospitales y la interrupción de la recaudación de aduanas e impuestos.[3]
- También en mayo, un atentado provocó retrasos y cancelaciones en los vuelos de una de las mayores aerolíneas de la India, dejando a cientos de pasajeros varados.[4]

El éxito de estos ataques y el alcance de sus repercusiones en el mundo real son el resultado de la industrialización de la economía de la ciberdelincuencia, que permite el acceso a herramientas e infraestructuras y amplía las capacidades de los ciberdelincuentes al reducir la barrera de entrada de sus habilidades.

En los últimos años, el ransomware ha pasado de un modelo en el que una única "banda" desarrollaba y distribuía una carga útil de ransomware al modelo de ransomware como servicio (RaaS). RaaS permite a un grupo administrar el desarrollo de la carga útil del ransomware y proporcionar servicios de pago y extorsión a través de la filtración de datos a otros ciberdelincuentes, los que realmente lanzan los ataques de ransomware, denominados "afiliados" para obtener una parte de los beneficios. Esta franquicia de la economía de la ciberdelincuencia ha expandido el grupo de atacantes. La industrialización de las herramientas de los ciberdelincuentes ha facilitado a los atacantes la realización de intrusiones, la filtración de datos y la implementación de ransomware.

ransomware operado por humanos[5] (término acuñado por los investigadores de Microsoft para describir las amenazas impulsadas por personas que toman decisiones en cada etapa de los ataques en función de lo que descubren en la red de su objetivo y delimitan la amenaza de los ataques de ransomware básicos) sigue siendo una amenaza importante para las organizaciones.

Modelo basado en datos de Microsoft Defender para puntos de conexión (EDR) (enero-junio de 2022).

Ransomware y extorsión: una amenaza de nivel nacional

Continuación

Los ataques de ransomware se han vuelto aún más impactantes a medida que la adopción de una estrategia de monetización de doble extorsión se ha convertido en una práctica habitual. Se trata de filtrar los datos de los dispositivos comprometidos, cifrar los datos de los dispositivos y luego publicar o amenazar con publicar los datos robados para presionar a las víctimas para que paguen un rescate.

Aunque la mayoría de los atacantes de ransomware implementan el ransomware de forma oportunista en cualquier red a la que consiguen acceder, algunos compran el acceso a otros ciberdelincuentes, aprovechando las conexiones entre los agentes de acceso y los operadores de ransomware.

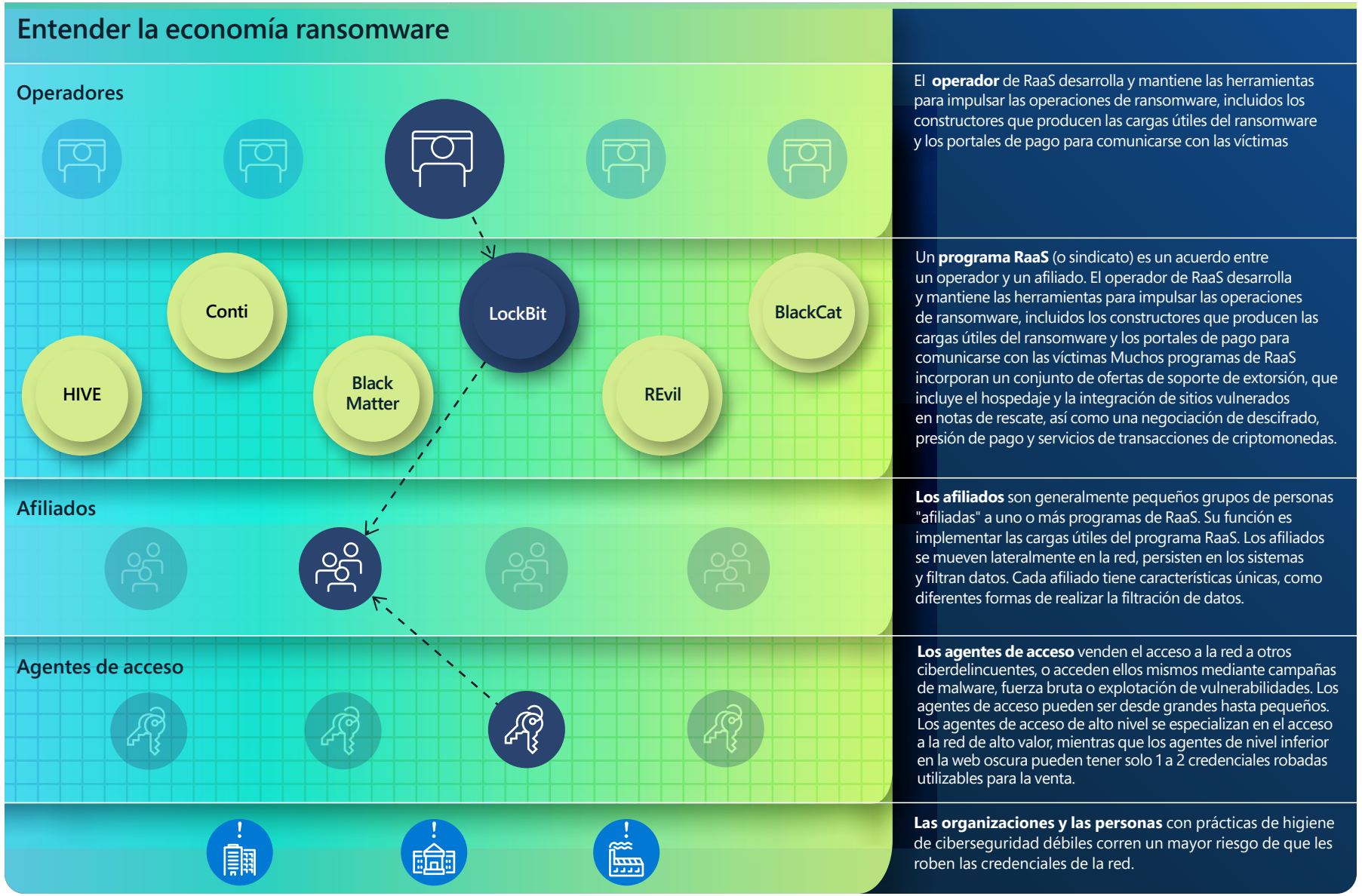
Nuestra amplitud única de inteligencia de señales se recopila a partir de varias fuentes (identidad, correo electrónico, puntos de conexión y nube) y entrega una visión de la creciente economía del ransomware, que se completa con un sistema de afiliación que incluye herramientas diseñadas para atacantes con menos conocimientos técnicos.

La ampliación de las relaciones entre los ciberdelincuentes especializados ha aumentado el ritmo, la sofisticación y el éxito de los ataques de ransomware. Esto ha impulsado la evolución del ecosistema de ciberdelincuencia en actores conectados con diferentes técnicas, objetivos y conjuntos de habilidades que se apoyan mutuamente en el acceso inicial a los objetivos, los servicios de pago y las herramientas o sitios de descifrado o publicación.

Los operadores de ransomware pueden ahora comprar el acceso a organizaciones o redes gubernamentales en línea u obtener credenciales y acceso a través de relaciones interpersonales con intermediarios cuyo principal objetivo es únicamente monetizar el acceso obtenido.

A continuación, los operadores utilizan el acceso adquirido para implementar una carga útil de ransomware comprada a través de mercados o foros de la web oscura. En muchos casos, las negociaciones con las víctimas las lleva a cabo el equipo de RaaS, no los propios operadores. Estas transacciones delictivas son fluidas y los participantes tienen pocas posibilidades de ser detenidos y acusados debido al anonimato de la web oscura y a la dificultad de aplicar las leyes a nivel transnacional.

Un esfuerzo sostenible y exitoso contra esta amenaza requerirá una estrategia de todo el gobierno que se ejecute en estrecha colaboración con el sector privado.



Al contrario de cómo a veces se presenta el ransomware en los medios de comunicación, es poco frecuente que una sola variante de ransomware esté administrada por una "banda de ransomware" de principio a fin. En su lugar, hay entidades separadas que crean el malware, acceden a las víctimas, implementan el ransomware y se encargan de las negociaciones de extorsión. La industrialización del ecosistema delictivo ha llevado a:

- Agentes de acceso que irrumpen y entregan el acceso (acceso como servicio).
- Desarrolladores de malware que venden herramientas.
- Operadores delictivos y afiliados que realizan intrusiones.
- Proveedores de servicios de cifrado y extorsión que se apoderan de la monetización de los afiliados (RaaS).

Todas las campañas de ransomware operadas por humanos comparten dependencias comunes de las debilidades de seguridad. En concreto, los atacantes suelen aprovecharse de la escasa higiene cibernética de una organización, que suele incluir la aplicación de revisiones con poca frecuencia y la no implementación de la autenticación multifactor (MFA).

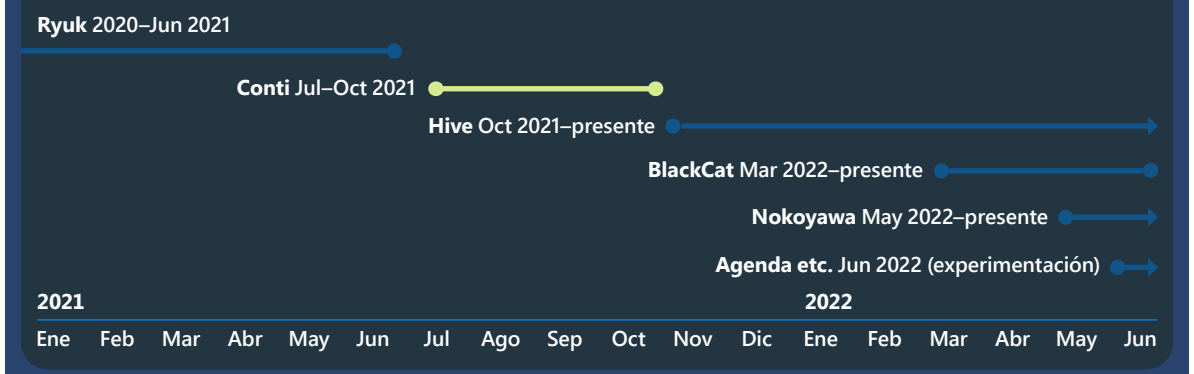
Caso práctico: la disolución de Conti

Conti, una de las variantes de ransomware más importantes de los últimos dos años, comenzó a cerrar sus operaciones a mediados de 2022, y el Centro de inteligencia sobre amenazas de Microsoft (MSTIC) observó un descenso considerable de la actividad a fines de marzo y principios de abril. Observamos las últimas implementaciones de ransomware de Conti a mediados de abril. Sin embargo, al igual que el cierre de otras operaciones de ransomware, la disolución de Conti no tuvo un impacto considerable en la implementación de ransomware, ya que MSTIC observó que los afiliados de Conti pasaron a implementar otras cargas útiles de ransomware, como BlackBasta, Lockbit 2.0, LockbitBlack y HIVE. Esto coincide con los datos de años anteriores y sugiere que cuando las bandas de ransomware se desconectan, resurgen meses después o redistribuyen sus capacidades técnicas y recursos a nuevos grupos.

Nuestros equipos de inteligencia de amenazas de Microsoft rastrean a los actores de amenaza de ransomware como grupos individuales (etiquetados como DEV) basados en sus herramientas específicas, en lugar de rastrearlos por el malware que utilizan. Esto significó que cuando los afiliados de Conti se dispersaron, pudimos continuar el rastreo de estos DEV a través de su uso de otras herramientas o kits RaaS. Por ejemplo:

- DEV-0230, que está afiliado a Trickbot, había sido un prolífico usuario de Conti. A fines de abril, MSTIC lo observó utilizando QuantumLocker.
- DEV-0237 pasó del kit de ransomware de Conti a HIVE y Nokoyawa, incluyendo el uso de HIVE en el ataque del 31 de mayo contra organismos gubernamentales de Costa Rica.
- A DEV-0506, otro prolífico usuario del kit de ransomware Conti, se le observó utilizando BlackBasta.

Ejemplo de un afiliado (DEV-0237) que cambia rápidamente entre los programas de RaaS



Tras el cierre de un programa RaaS como Conti, el ransomware afiliado se desplaza a otro (Hive) casi inmediatamente.

RaaS hace evolucionar el ecosistema del ransomware y dificulta la atribución

Dado que el ransomware operado por humanos está dirigido por operadores individuales, los patrones de ataque varían en función del objetivo y se alternan a lo largo de la duración de un ataque. En el pasado, observamos una estrecha relación entre el vector de entrada inicial, las herramientas y las opciones de carga útil del ransomware en cada campaña de una misma cepa de ransomware. Esto facilitó la atribución. El modelo de afiliación RaaS, sin embargo, desvincula esta relación. Como resultado, Microsoft rastrea a los afiliados de ransomware que implementan cargas útiles en ataques específicos, en lugar de rastrear a los desarrolladores de cargas útiles de ransomware como operadores.

Dicho de otro modo, ya no suponemos que el desarrollador de HIVE es el operador detrás de un ataque de ransomware HIVE; es más probable que sea un afiliado.

La industria de la ciberseguridad ha luchado por captar de forma suficiente esta delimitación entre desarrolladores y operadores. La industria sigue informando a menudo de un incidente de ransomware por el nombre de su carga útil, lo que da la falsa impresión de que una única entidad, o banda de ransomware, está detrás de todos los ataques que utilizan esa carga útil concreta de ransomware, y todos los incidentes asociados a ella comparten técnicas e infraestructura comunes. Para apoyar a los defensores de la red, es importante aprender más sobre las etapas que preceden a los ataques de diferentes afiliados (como la filtración de datos y los mecanismos de persistencia adicionales) ylas oportunidades de detección y protección que pueden existir.

Más que el malware, los atacantes necesitan credenciales para tener éxito en sus operaciones. El éxito de la infección de ransomware operado por humanos de toda una organización se basa en el acceso a una cuenta altamente privilegiada.

Enfoque en los ataques de ransomware operados por humanos

A lo largo del año pasado, los expertos en ransomware de Microsoft llevaron a cabo investigaciones en profundidad de más de 100 incidentes de ransomware de origen humano para rastrear las técnicas de los atacantes y comprender cómo proteger mejor a nuestros clientes.

Es importante tener en cuenta que el análisis que compartimos aquí solo es posible para los dispositivos integrados y administrados. Los dispositivos no integrados ni administrados representan la parte menos segura de los activos de hardware de una organización.

Técnicas de fase de ransomware más frecuentes:

75 %
Usa herramientas de administración.

75 %
Utiliza una cuenta de usuario elevada adquirida y comprometida para propagar cargas malintencionadas a través del protocolo SMB.

99 %
Intenta manipular los productos de seguridad y de copia de seguridad descubiertos mediante herramientas incorporadas al sistema operativo.

El típico ataque operado por humanos

Los ataques de ransomware de origen humano pueden clasificarse en la fase previa al ransomware y la fase de implementación del mismo. Durante la fase previa al ransomware, los atacantes se preparan para infiltrarse en la red conociendo la tipología y la infraestructura de seguridad de la organización.

Detenga a los atacantes antes de que lleguen a la fase de implementación de ransomware	**¡Implementación!**
Antes del ransomware	**Ransomware**
Esta fase puede durar desde unos días hasta varias semanas o meses, aunque se ha ido acortando en los últimos dos años.	Esta fase puede durar solo minutos.
Los atacantes se preparan para infiltrarse en la red aprendiendo todo lo posible sobre la topología y la infraestructura de seguridad. Los atacantes también pueden filtrar los datos en esta fase.	Los atacantes tienen como objetivo cifrar la mayor cantidad de datos posible.

Nuestras investigaciones descubrieron que la mayoría de los actores que están detrás de los ataques de ransomware operados por humanos se aprovechan de debilidades de seguridad similares y comparten patrones y técnicas de ataque comunes.

Una estrategia de seguridad duradera

Combatir y prevenir ataques de esta naturaleza requiere un cambio en la mentalidad de la organización para enfocarse en la protección integral necesaria para frenar y detener a los atacantes antes de que puedan pasar de la fase previa al ransomware a la fase de implementación del mismo.

Las empresas deben aplicar los procedimientos recomendados de seguridad de forma coherente y dinámica en sus redes, con el objetivo de mitigar las clases de ataques. Debido a la toma de decisiones humanas, estos ataques de ransomware pueden generar varias alertas de productos de seguridad, aparentemente dispares, que pueden perderse con facilidad o no responder a tiempo. La fatiga de las alertas es real, y los centros de operaciones de seguridad (SOC) pueden facilitarles la vida observando las tendencias de sus alertas o agrupando las alertas en incidentes para que puedan ver el panorama general. Los SOC pueden entonces mitigar las alertas utilizando capacidades de endurecimiento como las reglas de reducción de la superficie de ataque. El endurecimiento contra las amenazas más comunes no solo puede reducir el volumen de alertas, sino también detener a muchos atacantes antes de que consigan acceder a las redes.

Las organizaciones deben mantener continuamente altos niveles de seguridad e higiene de la red para protegerse de los ataques de ransomware de origen humano.

Información práctica

A los atacantes de ransomware los motivan las ganancias fáciles, por lo que aumentar su costo a través del fortalecimiento de la seguridad es clave para interrumpir la economía de la ciberdelincuencia.

1. Desarrolle protección de las credenciales. Más que el malware, los atacantes necesitan credenciales para tener éxito en sus operaciones. El éxito de la infección por ransomware de toda una organización depende del acceso a una cuenta altamente privilegiada, como la de un administrador de dominio, o de la capacidad de editar una directiva de grupo.
2. Realice auditorías de exposición de credenciales.
3. Dé prioridad a la implementación de actualizaciones de Active Directory.
4. Dé prioridad al endurecimiento de la nube.
5. Reduzca la superficie de ataque.
6. Endurezca los activos orientados a Internet y comprenda su perímetro.
7. Reduzca la fatiga de las alertas del SOC endureciendo su red para reducir el volumen y preservar el ancho de banda para los incidentes de alta prioridad.

Vínculos a más información

- RaaS: comprensión de la economía por encargo de la ciberdelincuencia y cómo protegerse | Blog de seguridad de Microsoft
- Ataques de ransomware operados por humanos: un desastre evitable | Blog de seguridad de Microsoft

Información sobre el ransomware de los responsables de la primera línea de respuesta

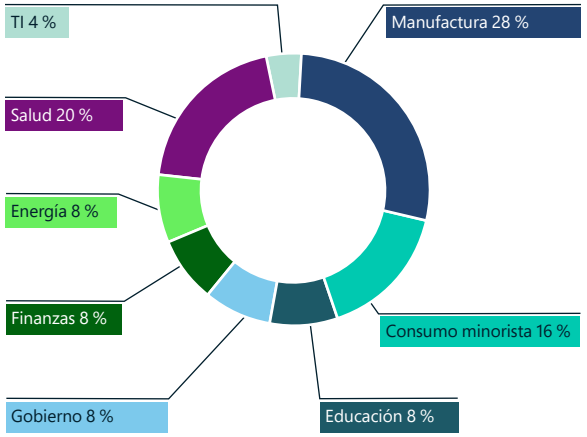
Las organizaciones de todo el mundo experimentaron un crecimiento constante de los ataques de ransomware operados por humanos a partir de 2019. Sin embargo, las operaciones de las fuerzas de seguridad y los acontecimientos geopolíticos del último año tuvieron un impacto significativo en las organizaciones de ciberdelincuentes.

La Línea de servicios de seguridad de Microsoft apoya a los clientes durante un ciberataque completo, desde la investigación hasta la contención exitosa y las actividades de recuperación. Los servicios de respuesta y recuperación se ofrecen a través de dos equipos altamente integrados, uno de los cuales se centra en la investigación y el trabajo de base para la recuperación y el segundo en la contención y la recuperación. En esta sección se presenta un resumen de los hallazgos basados en los compromisos de ransomware durante el año pasado.

93 %

de las investigaciones de Microsoft durante los compromisos de recuperación de ransomware revelaron controles insuficientes de acceso a privilegios y movimiento lateral.

Incidentes de ransomware y compromisos de recuperación por parte de la industria

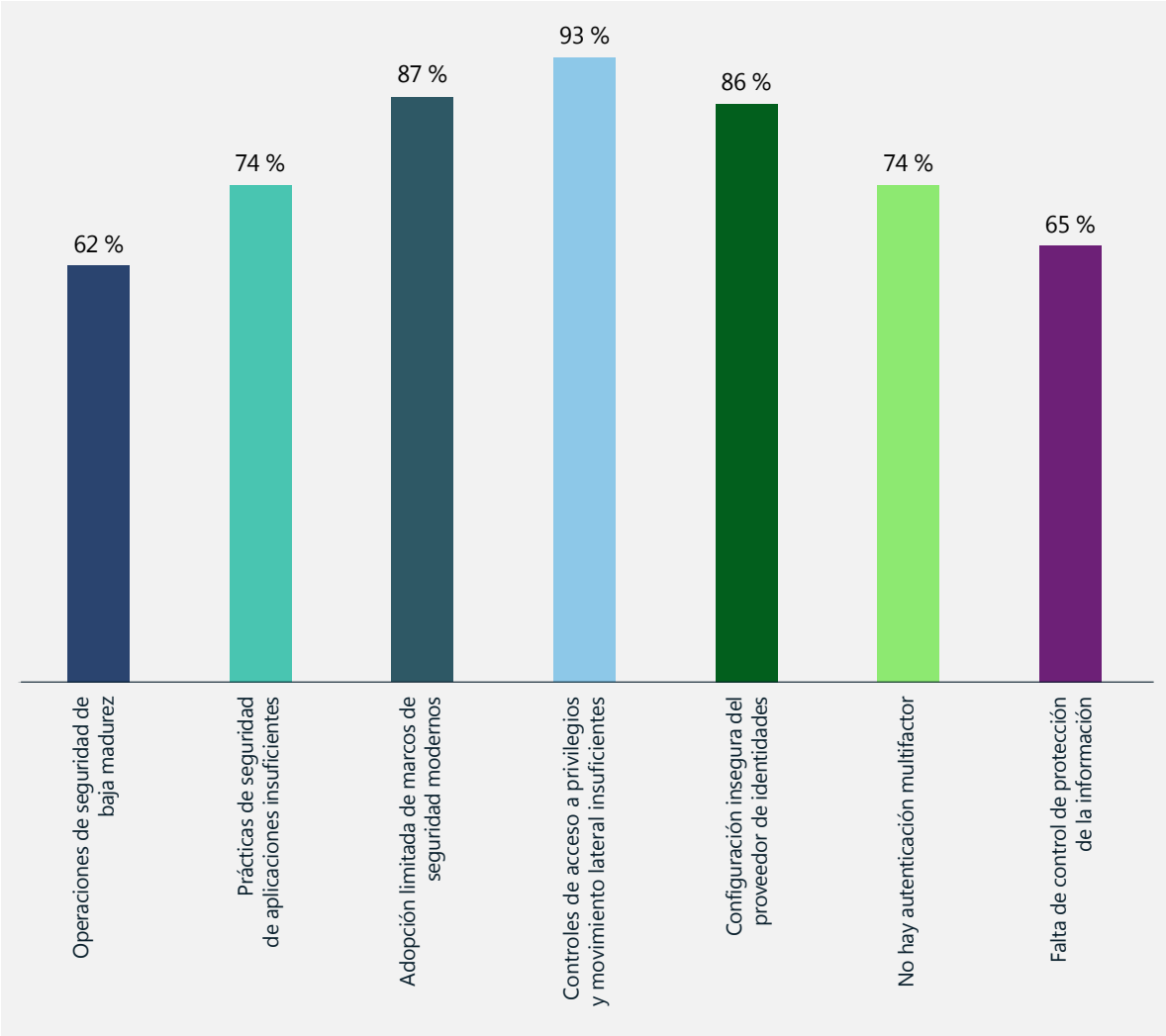


A medida que surgen nuevos grupos pequeños y amenazas, los equipos de defensa deben estar al tanto de la evolución de las amenazas de ransomware, a la vez que se protegen contra familias de ransomware previamente desconocidas. El enfoque de desarrollo rápido utilizado por los grupos delictivos condujo a la creación de ransomware inteligente empaquetado en kits fáciles de usar. Esto permite una mayor flexibilidad a la hora de lanzar ataques generalizados contra un mayor número de objetivos.

En las siguientes páginas se profundiza en los factores que contribuyen más comúnmente a una débil protección contra el ransomware, agrupados en tres categorías de resultados:

1. Controles de identidad débiles
2. Operaciones de seguridad ineficaces
3. Protección de datos limitada

Resumen de los hallazgos más comunes en los compromisos de respuesta al ransomware



El hallazgo más común entre los compromisos de respuesta a incidentes de ransomware fue la insuficiencia de controles de acceso a privilegios y movimiento lateral.

Información sobre el ransomware de los responsables de la primera línea de respuesta

Continuación

Los tres principales factores observados en nuestros compromisos de respuesta in situ:

① **Controles de identidad débiles:** los ataques de robo de credenciales siguen siendo uno de los principales factores que contribuyen

② **Los procesos de operaciones de seguridad ineficaces** no solo presentan una ventana de oportunidad para los atacantes, sino que impactan considerablemente en el tiempo de recuperación

③ Finalmente, todo se reduce a los datos: las organizaciones luchan por poner en práctica una **estrategia de protección de datos** que se ajusta a sus necesidades empresariales

① Controles de identidad débiles

El ransomware operado por humanos sigue evolucionando y emplea métodos de robo de credenciales y movimiento lateral tradicionalmente asociados a los ataques dirigidos. Los ataques exitosos suelen ser el resultado de campañas de larga duración que implican el compromiso de los sistemas de identidad, como Active Directory (AD), que permiten a los operadores humanos robar credenciales, acceder a los sistemas y permanecer en la red.

Active Directory (AD) y seguridad de Azure AD

88 %

de los clientes afectados no emplearon los procedimientos recomendados de seguridad de AD y Azure AD. Esto se ha convertido en un vector de ataque común, ya que los atacantes se aprovechan de las configuraciones erróneas y de las posturas de seguridad más débiles en los sistemas de identidad críticos para obtener un mayor acceso e impacto en las empresas.

Acceso al mínimo privilegio y uso de estaciones de trabajo con acceso con privilegios (PAW)

Ninguna de las organizaciones afectadas aplicó los principios de segregación de credenciales administrativas y de acceso con mínimos privilegios a través de estaciones de trabajo dedicadas durante la administración de sus activos críticos de identidad y de alto valor, como los sistemas propietarios y las aplicaciones críticas para el negocio.

Seguridad de las cuentas privilegiadas

88 %

de los compromisos, la MFA no se implementó para las cuentas sensibles y de alto privilegio, dejando una brecha de seguridad para que los atacantes comprometan las credenciales y pasen a otros ataques usando credenciales legítimas.

84 %

Los administradores del 84 % de las organizaciones no utilizaron controles de identidad de privilegios, como el acceso just-in-time, para evitar el uso nefasto de las credenciales privilegiadas comprometidas.

Información sobre el ransomware de los responsables de la primera línea de respuesta

Continuación

② Operaciones de seguridad ineficaces

Nuestros datos muestran que las organizaciones que han sufrido ataques de ransomware tienen importantes brechas en sus operaciones de seguridad, herramientas y administración del ciclo de vida de los activos de tecnología de la información. A partir de los datos disponibles, lo que más se observó fueron las siguientes brechas:

Aplicación de revisión:

68 %

de las organizaciones afectadas no contaban con un proceso eficaz de administración de vulnerabilidades y revisiones, y la gran dependencia de los procesos manuales frente a la aplicación de revisiones automatizadas provocaba aperturas críticas. La manufactura y las infraestructuras críticas siguen luchando con el mantenimiento y la aplicación de revisiones de los sistemas de tecnología de operaciones (OT) heredados.

Falta de herramientas de operaciones de seguridad:

La mayoría de las organizaciones informaron de la falta de visibilidad de la seguridad de extremo a extremo debido a la falta o a la mala configuración de las herramientas de seguridad, lo que lleva a una disminución de la eficacia de la detección y la respuesta.

60 %

de las organizaciones informaron de que no utilizaban una herramienta EDR[6], una tecnología fundamental para la detección y la respuesta.

60 %

no invirtió en tecnología de administración de eventos e información de seguridad (SIEM), lo que dio lugar a silos de supervisión, una capacidad limitada para detectar amenazas de extremo a extremo y operaciones de seguridad ineficaces. La automatización sigue siendo una brecha clave en las herramientas y procesos del SOC, lo que obliga al personal del SOC a pasar incontables horas dando sentido a la telemetría de seguridad.

84 %

de las organizaciones afectadas no permitieron la integración de sus entornos multinube en sus herramientas de operaciones de seguridad.

Procesos de respuesta y recuperación:

76 %

La falta de un plan de respuesta eficaz fue un área crítica observada en el 76 % de las organizaciones afectadas, lo que impide una preparación adecuada de la organización para la crisis y repercute de forma negativa en el tiempo de respuesta y recuperación.

③ Protección de datos limitada

Muchas organizaciones comprometidas carecían de procesos adecuados de protección de datos, lo que repercutió gravemente en los tiempos de recuperación y en la capacidad de volver a las operaciones comerciales. Las lagunas más comunes que se encuentran son:

Copia de seguridad inmutable:

44 %

de las organizaciones no tenían copias de seguridad inmutables de los sistemas afectados. Los datos también muestran que los administradores no disponían de copias de seguridad ni de planes de recuperación para activos críticos como el AD.

Prevención de pérdida de datos:

Los atacantes suelen encontrar la manera de comprometer los sistemas a través de la explotación de las vulnerabilidades de la organización, filtrando los datos críticos para la extorsión, el robo de la propiedad intelectual o la monetización.

92 %

de las organizaciones afectadas no aplicaron controles eficaces de prevención de la pérdida de datos para mitigar estos riesgos, lo que condujo a la pérdida de datos críticos.

El ransomware disminuyó en algunas regiones y aumentó en otras

Este año hemos observado un descenso en el número total de casos de ransomware notificados a nuestros equipos de respuesta en Norteamérica y Europa en comparación con el año anterior. Al mismo tiempo, aumentaron los casos notificados en América Latina.

Una de las interpretaciones de esta observación es que los ciberdelincuentes se han alejado de las áreas que se perciben como de mayor riesgo de desencadenar el escrutinio de las fuerzas de seguridad en favor de objetivos más suaves. Dado que Microsoft no observó una mejora sustancial en la seguridad de las redes empresariales en todo el mundo para explicar la disminución de las llamadas de soporte relacionadas con el ransomware, creemos que la causa más probable es una combinación de la actividad de las fuerzas de seguridad en 2021 y 2022 que aumentó el costo de la actividad delictiva, junto con algunos acontecimientos geopolíticos de 2022.

Una de las operaciones de RaaS más frecuentes pertenece a un grupo delictivo de habla rusa conocido como REvil (también conocido como Sodinokibi) que ha estado activo desde 2019. En octubre de 2021, los servidores de REvil se desconectaron en el marco de la operación policial internacional GoldDust.[7] En enero de 2022, Rusia detuvo a 14 presuntos miembros de REvil y allanó 25 locales relacionados con ellos.[8] Esta fue la primera vez que Rusia actuó contra los operadores de ransomware en su territorio.

Si bien es probable que las actividades de las fuerzas de seguridad reduzcan la frecuencia de los ataques en 2022, los actores de amenaza podrían desarrollar nuevas estrategias para evitar ser descubiertos en el futuro. Además, la tensión entre Rusia y Estados Unidos por la invasión rusa de Ucrania parece haber puesto fin a la incipiente cooperación rusa en la lucha mundial contra el ransomware. Después de un breve período de incertidumbre tras las detenciones de REvil, Estados Unidos y Rusia dejaron de cooperar en. la persecución de los actores de ransomware, lo que significa que los ciberdelincuentes podrían volver a ver a Rusia como un refugio seguro.

De cara al futuro, prevemos que el ritmo de las actividades de ransomware dependerá del resultado de algunos temas clave:

1. ¿Actuarán los gobiernos para impedir que los delincuentes que se dedican al ransomware operen dentro de sus fronteras, o tratarán de desbaratar a los actores que operan desde suelo extranjero?
2. ¿Cambiarán los grupos de ransomware sus tácticas para eliminar la necesidad del ransomware y recurrir a ataques de tipo extorsivo?
3. ¿Podrán las organizaciones modernizar y transformar sus operaciones de TI más rápido de lo que los delincuentes pueden explotar las vulnerabilidades?
4. ¿Los avances en el seguimiento y rastreo de los pagos de rescates obligarán a los receptores de los mismos a cambiar de táctica y de negociación?

Si bien es probable que las actividades de las fuerzas de seguridad reduzcan la frecuencia de los ataques en 2022, los actores de amenaza podrían desarrollar nuevas estrategias para evitar ser descubiertos en el futuro.

2 veces

Los ataques de ransomware disminuyeron en algunas regiones, pero las peticiones de rescate aumentaron más del doble.

Información práctica

1. Céntrese en estrategias de seguridad holísticas, ya que todas las familias de ransomware se aprovechan de las mismas debilidades de seguridad para afectar a una red.
2. Actualice y mantenga los fundamentos de la seguridad para aumentar el nivel básico de protección de la defensa en profundidad y modernizar las operaciones de seguridad. La migración a la nube permite detectar las amenazas con mayor rapidez y responder más rápido.

Vínculos a más información

- Proteja su organización del ransomware | Seguridad de Microsoft
- 7 Siete maneras de reforzar su entorno contra el peligro | Blog de seguridad de Microsoft
- Mejorar las defensas basadas en la IA para desbaratar el ransomware operado por humanos | Equipo de investigación de Microsoft 365 Defender
- Security Insider: Explore las últimas actualizaciones e información sobre ciberseguridad | Seguridad de Microsoft

La ciberdelincuencia como servicio

La ciberdelincuencia como servicio (CaaS) es una amenaza creciente y en evolución para los clientes de todo el mundo. La Unidad de delitos digitales (DCU) de Microsoft observó un crecimiento continuo del ecosistema CaaS con un número creciente de servicios en línea que facilitan varios ciberdelitos, incluyendo BEC y ransomware operado por humanos. El phishing sigue siendo uno de los métodos de ataque preferidos, ya que los ciberdelincuentes pueden adquirir un valor considerable si consiguen robar y vender el acceso a las cuentas robadas.

En respuesta a la expansión del mercado de CaaS, la DCU mejoró sus sistemas de escucha para detectar e identificar las ofertas de CaaS en todo el ecosistema de Internet, la web profunda, los foros vetados,[9] los sitios web dedicados, los foros de discusión en línea y las plataformas de mensajería.

Los ciberdelincuentes colaboran ahora a través de zonas horarias e idiomas para obtener resultados específicos. Por ejemplo, un sitio web de CaaS administrado por una persona en Asia mantiene operaciones en Europa, y crea cuentas malintencionadas en África. La naturaleza multijurisdiccional de estas operaciones presenta complejos desafíos legales y de aplicación de la ley. En respuesta, la DCU centra sus esfuerzos en desactivar la infraestructura criminal malintencionada utilizada para facilitar los ataques de CaaS y en colaborar con las fuerzas del orden de todo el mundo para que los delincuentes rindan cuentas.

Los ciberdelincuentes usan cada vez más los análisis para maximizar el alcance, el ámbito y las ganancias. Al igual que las empresas legítimas, los sitios web de CaaS deben garantizar la validez de los productos y servicios para mantener una reputación sólida. Por ejemplo, los sitios web de CaaS automatizan habitualmente el acceso a las cuentas comprometidas para garantizar la validez de las credenciales comprometidas. Los ciberdelincuentes suspenderán las ventas de cuentas específicas cuando se restablezcan las contraseñas o se apliquen revisiones a las vulnerabilidades. Cada vez más, identificamos sitios web de CaaS que ofrecen a los compradores una verificación a la carta como proceso de control de calidad. Como resultado, los compradores pueden sentirse seguros de que el sitio web de CaaS vende cuentas y contraseñas activas, a la vez que se reducen los posibles costos para el comerciante de CaaS si las credenciales robadas se corrigen antes de la venta.

La DCU también observó sitios web de CaaS que ofrecían a los compradores la opción de adquirir cuentas comprometidas de ubicaciones geográficas específicas, proveedores de servicios en línea designados y personas, profesiones e industrias seleccionadas de forma específica. Con frecuencia, las cuentas solicitadas se enfocan en profesionales o departamentos que procesan la facturación, como los directores financieros o "cuentas por cobrar". Del mismo modo, las industrias que participan en la contratación pública suelen ser el objetivo debido a la cantidad de información que se pone a disposición a través del proceso de licitación pública.

Las investigaciones de la DCU sobre el CaaS sacaron a la luz una serie de tendencias clave:

El número y la sofisticación de los servicios van en aumento.

Un ejemplo es la evolución de las shells web, que suelen consistir en servidores web comprometidos utilizados para automatizar los ataques de phishing. DCU observó que los revendedores de CaaS simplifican la carga de kits de phishing o malware a través de paneles web especializados. Los vendedores de CaaS a menudo intentan posteriormente vender servicios adicionales al actor de amenaza a través del panel, como servicios de mensajes de correo no deseado y listas de destinatarios de correo no deseado especializadas basadas en atributos definidos, como la ubicación geográfica o la profesión. En algunos casos, observamos que se utilizaba un único shell web en varias campañas de ataque, lo que sugiere que los actores de amenaza podrían mantener un acceso persistente al servidor comprometido. También observamos un aumento de los servicios de anonimización disponibles como parte del ecosistema CaaS, así como ofertas de redes privadas virtuales (VPN) y cuentas de servidores privados virtuales (VPS). En la mayoría de los casos, las VPN/VPS ofrecidas se adquirieron inicialmente a través de tarjetas de crédito robadas. Los sitios web de CaaS también ofrecían un mayor número de protocolos de escritorio remoto (RDP), shell seguro (SSH) y cPanels para utilizarlos como plataforma para orquestar ataques de ciberdelincuencia. Los comerciantes de CaaS configuran el RDP, el SSH y los cPanels con herramientas y scripts apropiados para facilitar varios tipos de ciberataques.

Los servicios de creación de dominios homógrafos exigen cada vez más el pago en criptomonedas.

Los dominios homoglifos suplantan nombres de dominio legítimos utilizando caracteres idénticos o casi idénticos en apariencia a otro carácter. El objetivo es engañar al espectador haciéndole creer que el dominio homogéneo es el auténtico. Estos dominios son una amenaza omnipresente y una gateway para una cantidad importante de ciberdelitos. Los sitios de CaaS ahora venden nombres de dominio homogéneos personalizados, lo que permite a los compradores solicitar nombres de empresas y dominios específicos para hacerse pasar por ellos. Una vez recibido el pago, los comerciantes de CaaS utilizan una herramienta generadora de homoglifos para seleccionar el nombre de dominio y luego registrar el homoglifo malintencionado. El pago de este servicio se realiza casi exclusivamente en criptomoneda.

2 750 000

registros de sitios web bloqueados con éxito por la DCU este año para adelantarse a los actores delictivos que planificaban utilizarlos para participar en la ciberdelincuencia mundial.

La ciberdelincuencia como servicio

Continuación

Los vendedores de CaaS ofrecen cada vez más credenciales comprometidas para su compra.

Las credenciales comprometidas permiten el acceso no autorizado a las cuentas de los usuarios, incluyendo el servicio de mensajería de correo electrónico, los recursos de intercambio de archivos corporativos y OneDrive para la Empresa. Si las credenciales de administrador se ven comprometidas, los usuarios no autorizados podrían acceder a archivos confidenciales, recursos de Azure y cuentas de usuario de la empresa. En muchos casos, las investigaciones de la DCU identificaron el uso no autorizado de la misma credencial en varios servidores como medio para automatizar la verificación de credenciales. Este patrón sugiere que el usuario comprometido podría ser víctima de varios ataques de phishing o tener un malware en el dispositivo que permita a los registradores de pulsaciones de teclas de la red de robots (botnet) recopilar las credenciales.

Están surgiendo servicios y productos de CaaS con características mejoradas para evitar la detección.

Un vendedor de CaaS ofrece kits de phishing con capas crecientes de complejidad y características de anonimato diseñadas para eludir los sistemas de detección y prevención por tan solo USD 6 al día. El servicio ofrece una serie de redireccionamientos que realizan comprobaciones antes de permitir el tráfico a la siguiente capa o sitio. Uno de ellos ejecuta más de 90 comprobaciones para tomar la huella digital del dispositivo, incluyendo si se trata de una máquina virtual, recopilando detalles sobre el navegador y el hardware que se utiliza, y más. Si todas las comprobaciones se superan, el tráfico se envía a una página de aterrizaje utilizada para el phishing.

Los servicios de ciberdelincuencia de extremo a extremo están vendiendo suscripciones a servicios administrados.

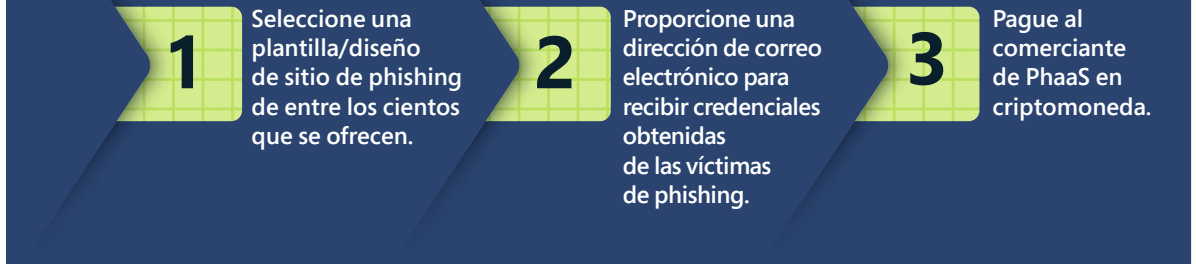
Normalmente, cada paso en la comisión de un delito en línea puede exponer a los actores de amenaza si la seguridad operativa es deficiente. El riesgo de exposición e identificación aumenta si los servicios se compran en varios sitios de CaaS. La DCU observó una tendencia preocupante en la web oscura, en la que aumentan los servicios que ofrecen anonimizar el código del software y anonimizar el texto de los sitios web para reducir su exposición. Los proveedores de servicios de suscripción a la ciberdelincuencia de extremo a extremo administran todos los servicios y garantizan los resultados, lo que reduce aún más los riesgos de exposición para la OCN suscriptora. La reducción del riesgo ha aumentado la popularidad de estos servicios de extremo a extremo.

El phishing como servicio (PhaaS) es un ejemplo de servicio de ciberdelincuencia de extremo a extremo. PhaaS es una evolución de los servicios anteriores conocidos como servicios totalmente indetectables (FUD) y se ofrece por suscripción. Las condiciones típicas de PhaaS incluyen el mantenimiento de los sitios web de phishing durante un mes.

La DCU también identificó a un comerciante de CaaS que ofrecía denegación de servicio distribuido (DDoS) en un modelo de suscripción. Este modelo externaliza la creación y el mantenimiento de la red de robots (botnet) necesaria para llevar a cabo los ataques al comerciante de CaaS. Cada cliente de la suscripción DDoS recibe un servicio cifrado para mejorar la seguridad operativa y un año de soporte 24/7. El servicio de suscripción DDoS ofrece diferentes arquitecturas y métodos de ataque, por lo que un comprador simplemente selecciona un recurso para atacar y el vendedor brinda acceso a una serie de dispositivos comprometidos en su red de robots para llevar a cabo el ataque. El costo de la suscripción a DDoS es de solo USD 500.

El trabajo de la DCU para desarrollar herramientas y técnicas que identifiquen y desbaraten a los ciberdelincuentes de CaaS es continuo. La evolución de los servicios de CaaS presenta importantes desafíos, especialmente en lo que respecta a la alteración de los pagos con criptomonedas.

PhaaS, los ciberdelincuentes ofrecen varios servicios dentro de una única suscripción. Por lo general, un comprador solo necesita realizar tres acciones:



Una vez completados estos pasos, el comerciante de PhaaS crea servicios con tres o cuatro capas de redireccionamiento y recursos de hospedaje para dirigirse a usuarios específicos. Posteriormente, se lanza la campaña y se recogen las credenciales de las víctimas, se verifican y se envían a la dirección de correo electrónico proporcionada por el comprador. Por una prima, muchos comerciantes de PhaaS ofrecen hospedar sitios de phishing en la blockchain pública para que se pueda acceder a ellos desde cualquier navegador y las redirecciones puedan dirigir a los usuarios a un recurso en el libro mayor distribuido.

Uso delictivo de las criptomonedas

A medida que se generaliza la adopción de la criptomoneda, los delincuentes la utilizan cada vez más para eludir las medidas policiales y de lucha contra el lavado de dinero. Esto aumenta el desafío para las fuerzas del orden de rastrear y localizar los pagos de criptomonedas a los ciberdelincuentes.

El gasto mundial en soluciones de blockchain creció aproximadamente un 340 % en los últimos cuatro años, mientras que las nuevas billeteras de criptomonedas crecieron alrededor del 270 %. Hay más de 83 millones de billeteras únicas en todo el mundo, y la capitalización total del mercado de todas las criptomonedas era de aproximadamente USD 1,1 billones a partir del 28 de julio de 2022.[10]

Fuente: Twitter.com—@PeckShieldAlert (PeckShield es una empresa de seguridad blockchain con sede en China).

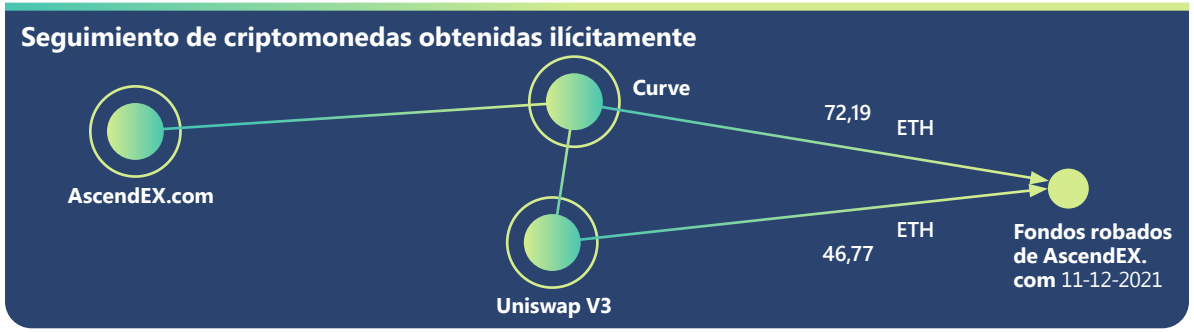
Seguimiento de los pagos del ransomware

El ransomware es una de las mayores fuentes de obtención ilícita de criptomonedas. En un esfuerzo por interrumpir la infraestructura técnica malintencionada utilizada en los ataques de ransomware (por ejemplo, la interrupción de Zloader en abril de 2022[11]), la DCU de Microsoft rastrea las billeteras de los delincuentes para permitir el seguimiento y la recuperación de las criptomonedas.

Los investigadores de la DCU han observado que los actores de ransomware evolucionan sus tácticas de comunicación con las víctimas para ocultar el rastro del dinero. Al principio, los ciberdelincuentes incluían direcciones de Bitcoin en sus notas de rescate. Sin embargo, esto facilitó el seguimiento de las transacciones de pago en blockchain, por lo que los actores de ransomware dejaron de incluir las direcciones de las billeteras y, en su lugar, sumaron direcciones de correo electrónico o vínculos a sitios web de chat para comunicar las direcciones de pago del rescate a las víctimas. Algunos actores incluso crearon páginas web e inicios de sesión únicos para cada víctima con el fin de evitar que los investigadores de seguridad y las fuerzas de seguridad obtuvieran las direcciones de las billeteras de los delincuentes haciéndose pasar por víctimas. A pesar de los esfuerzos de los delincuentes por ocultar su rastro, algunos pagos de rescates pueden recuperarse trabajando con las fuerzas de seguridad y las empresas de criptoanálisis que pueden rastrear los movimientos en blockchain.

Tendencias: lavado a través de DEX de los ingresos ilícitos

Un problema clave para los ciberdelincuentes es la conversión de criptomonedas en moneda fiduciaria. Los ciberdelincuentes tienen varias vías potenciales de conversión, cada una de las cuales conlleva un grado diferente de riesgo. Uno de los métodos utilizados para reducir el riesgo es lavar las ganancias a través de un intercambio descentralizado



Utilizando la herramienta de investigación de criptomonedas Chainalysis, la Unidad de delitos digitales de Microsoft descubrió que los hackers de AcendEX intercambiaron sus fondos robados en una DEX más pequeña llamada Curve, además de Uniswap. Este diagrama ilustra las rutas de lavado que el equipo descubrió. Cada círculo representa un grupo de billeteras y los números de cada línea representan la cantidad total de Ethereum transmitida con fines de lavado.

(DEX) antes de cobrar a través de las opciones de cobro disponibles, como los intercambios centralizados (CEX), de punto a punto (P2P) y los intercambios extrabursátiles (OTC). Los DEX son un lugar atractivo para el lavado porque a menudo no siguen las medidas de ALD.

En diciembre de 2021, unos hackers atacaron la plataforma mundial de comercio de criptomonedas AscendEx y robaron aproximadamente USD 77,7 millones en criptomonedas pertenecientes a sus clientes.[12] AscendEx contrató a empresas de análisis de blockchain y se puso en contacto con otros CEX para que las billeteras que recibían los fondos robados fueran incluidos en la lista negra. Además, las direcciones a las que se enviaron las monedas se etiquetaron como tales en el explorador de blockchain de Ethereum, Etherscan.[13] Para eludir las alertas y las listas negras, los hackers enviaron USD 1,5 millones en Ethereum a Uniswap, uno de los mayores DEX del mundo, el 18 de febrero de 2022.[14]

La adopción de medidas más estrictas de lucha contra el lavado de dinero por parte de DEX podría frenar la actividad de lavado en sus plataformas y obligar a los ciberdelincuentes a utilizar otros métodos de ofuscación, como la caída de monedas o los intercambios sin licencia. Por ejemplo, Uniswap anunció recientemente que empezará a utilizar listas negras para bloquear las billeteras que se sabe que están implicadas en actividades ilícitas para que no puedan realizar transacciones en la bolsa.[15]

Información práctica

1. Si es víctima de un ciberdelito y ha pagado al delincuente con criptomoneda, póngase en contacto con la policía local, que podría ayudarle a rastrear y recuperar los fondos perdidos.
2. Familiarícese con las medidas contra el lavado de dinero en vigor cuando seleccione una DEX.

Vínculos a más información

- Defensa contra amenazas basada en el hardware contra los cada vez más complejos cryptojackers | Equipo de investigación de Microsoft 365 Defender

La evolución del panorama de las amenazas de phishing

Los esquemas de phishing de credenciales están en aumento y siguen siendo una amenaza sustancial para los usuarios de todo el mundo porque se dirigen indiscriminadamente a todas las bandejas de entrada. Entre las amenazas que nuestros investigadores rastrean y contra las que protegen, el volumen de los ataques de phishing es órdenes de magnitud mayor que todas las demás amenazas.

Utilizando los datos de Defender for Office, vemos el correo electrónico malintencionado y la actividad de identidad comprometida. Azure Active Directory Identity Protection brinda aún más información a través de las alertas de eventos de identidad comprometida. Utilizando Defender for Cloud Apps, vemos eventos de acceso a datos de identidad comprometidos, y Microsoft 365 Defender (M365D) ofrece correlación entre productos. La métrica del movimiento lateral proviene de Defender para punto de conexión (alertas y eventos de comportamiento de ataque), Defender for Office (correo electrónico malintencionado) y, de nuevo, M365D para la correlación entre productos).

710 millones

correos electrónicos de phishing bloqueados por semana.

1 hr 12 m

El tiempo medio que tarda un atacante en acceder a sus datos privados si es víctima de un correo electrónico de phishing.[16]

1 hr 42 m

El tiempo medio para que un atacante comience a moverse lateralmente dentro de su red corporativa una vez que un dispositivo está comprometido.[17]

Las credenciales de Microsoft 365 siguen siendo uno de los tipos de cuenta más buscados por los atacantes. Una vez comprometidas las credenciales de inicio de sesión, los atacantes pueden entrar en los sistemas informáticos vinculados a la empresa para facilitar la infección con malware y ransomware, robar datos e información confidencial de la empresa accediendo a los archivos de SharePoint, y continuar con la propagación del phishing enviando más correos electrónicos malintencionados utilizando Outlook, entre otras acciones.

Además de las campañas con objetivos más amplios, el phishing de credenciales, donaciones e información personal, los atacantes se dirigen a empresas selectivas para obtener mayores pagos. Los ataques de phishing por correo electrónico contra empresas para obtener beneficios económicos se denominan colectivamente ataques BEC.

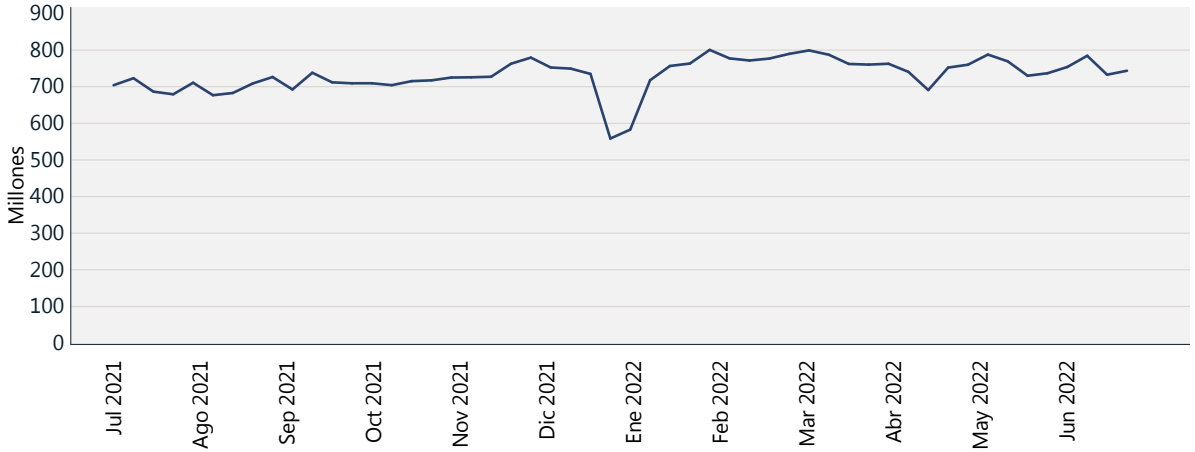
Microsoft detecta millones de correos electrónicos BEC cada mes, lo que equivale al 0,6 % de todos los correos electrónicos de phishing observados. Un informe de IC3[18] publicado en mayo de 2022 indica una tendencia al alza en las pérdidas expuestas debido a los ataques BEC.

Las técnicas utilizadas en los ataques de phishing siguen aumentando en complejidad. En respuesta a las contramedidas, los atacantes se adaptan a nuevas formas de implementar sus técnicas y aumentar la complejidad de cómo y dónde alojan la infraestructura de operación de las campañas. Esto significa que las organizaciones deben volver a evaluar periódicamente su estrategia de implementación de soluciones de seguridad para bloquear los correos electrónicos malintencionados y reforzar el control de acceso a las cuentas individuales de los usuarios.

531 000

Además de las URL bloqueadas por Defender for Office, nuestra Unidad de delitos digitales dirigió la eliminación de 531 000 URL únicas de phishing hospedadas fuera de Microsoft.

Correos electrónicos de phishing detectados



El número de detecciones de phishing por semana sigue aumentando. El descenso en diciembre-enero es una bajada estacional esperada, que también se informó en el informe del año pasado. Fuente: señales de Exchange Online Protection

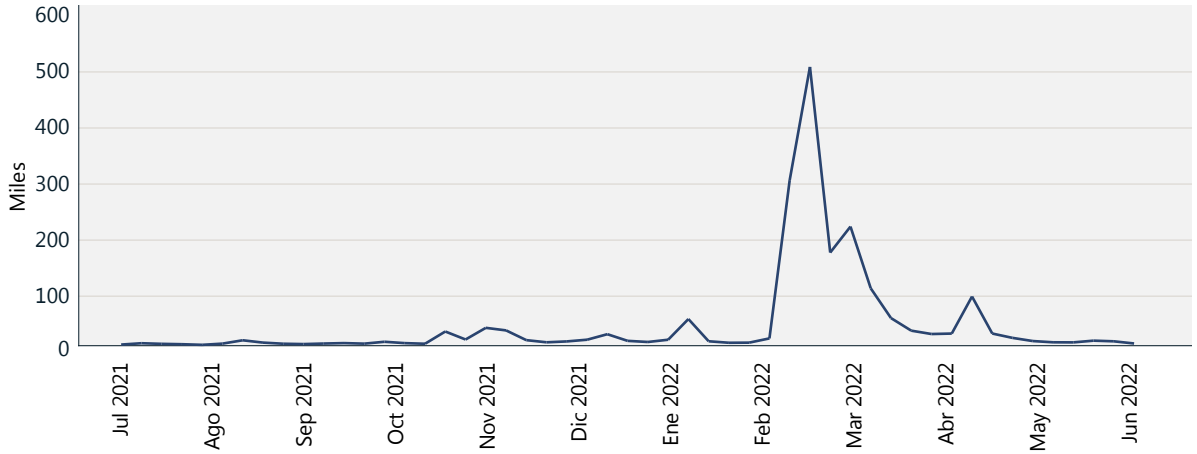
La evolución del panorama de las amenazas de phishing

Continuación

Seguimos observando un aumento constante año tras año de los correos electrónicos de phishing. El cambio hacia el trabajo a distancia en 2020 y 2021 vio un aumento sustancial de los ataques de phishing con el objetivo de capitalizar el entorno de trabajo cambiante. Los operadores de phishing se apresuran a adoptar nuevas plantillas de correo electrónico utilizando señuelos alineados con los principales acontecimientos mundiales, como la pandemia de COVID-19, y temas vinculados a las herramientas de colaboración y productividad, como Google Drive o el intercambio de archivos de OneDrive. Aunque los temas de COVID-19 han disminuido, la guerra en Ucrania se convirtió en un nuevo señuelo a partir de principios de marzo de 2022. Nuestros investigadores observaron un aumento asombroso de correos electrónicos que suplantan a organizaciones legítimas y que solicitan donaciones de criptomonedas en Bitcoin y Ethereum, supuestamente para apoyar a los ciudadanos ucranianos.

Solo unos días después del inicio de la guerra en Ucrania, a fines de febrero de 2022, el número de correos electrónicos de phishing detectados que contenían direcciones de Ethereum encontradas entre los clientes empresariales aumentó drásticamente. El total de encuentros alcanzó su punto máximo en la primera semana de marzo, cuando medio millón de correos electrónicos de phishing contenían una dirección de la billetera de Ethereum. Antes del inicio de la guerra, el número de direcciones de billeteras de Ethereum en otros correos electrónicos detectados como phishing era significativamente menor, con una media de unos pocos miles de correos electrónicos al día.

Correos electrónicos de phishing con direcciones de billetera de Ethereum



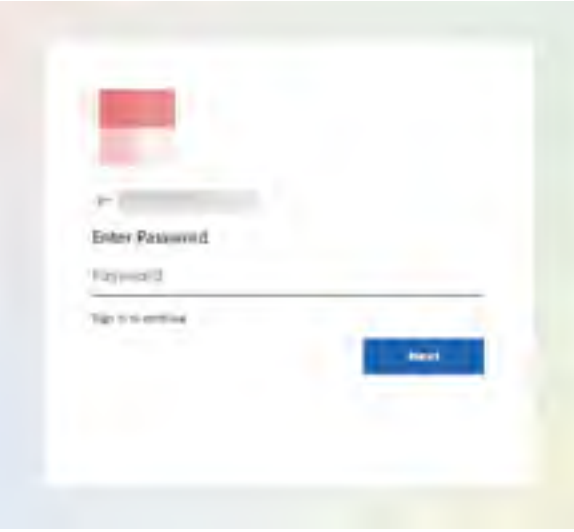
El total de correos electrónicos detectados como phishing que contenían direcciones de billeteras de Ethereum aumentó al comienzo del conflicto entre Ucrania y Rusia y disminuyó tras el impulso inicial.

Más que nunca, los suplantadores de identidad se apoyan en la infraestructura legítima para operar, lo que impulsa un aumento de las campañas de phishing dirigidas a comprometer varios aspectos de una operación para no tener que comprar, alojar u operar la suya propia. Por ejemplo, los correos electrónicos malintencionados pueden provenir de cuentas de remitente comprometidas. Los atacantes se benefician del uso de estas direcciones de correo electrónico, que tienen una mayor puntuación de reputación y se consideran más confiables que las cuentas y dominios de nueva creación. En algunas campañas de phishing más avanzadas, observamos que los atacantes prefieren enviar y suplantar desde dominios que tienen DMARC[19] incorrectamente configurado con una directiva de "no acción", abriendo la puerta a la suplantación del correo electrónico.

Las grandes operaciones de phishing tienden a utilizar servicios en la nube y máquinas virtuales (VM) en la nube para hacer operativos los ataques a gran escala. Los atacantes pueden automatizar por completo el proceso de implementación y entrega de mensajes de correo electrónico desde las máquinas virtuales utilizando los relés de correo electrónico SMTP o la infraestructura de correo electrónico en la nube para beneficiarse de las altas tasas de entrega y la reputación positiva de estos servicios legítimos. Si se permite el envío de correo electrónico malintencionado a través de estos servicios en la nube, los defensores deben confiar en fuertes capacidades de filtrado de correo electrónico para bloquear la entrada de correos electrónicos en su entorno.

Las cuentas de Microsoft siguen siendo un objetivo principal para los operadores de phishing, como demuestran las numerosas páginas de aterrizaje de phishing que suplantan la página de inicio de sesión de Microsoft 365. Por ejemplo, los suplantadores de identidad intentan igualar la experiencia de inicio de sesión de Microsoft en sus kits de phishing generando una URL única personalizada para el destinatario. Esta URL apunta a una página web malintencionada desarrollada para cosechar credenciales, pero un parámetro en la URL contendrá la dirección de correo electrónico del destinatario específico. Una vez que el objetivo navega a la página, el kit de phishing rellena previamente los datos de inicio de sesión del usuario y un logotipo corporativo personalizado para el destinatario del correo electrónico, reflejando la apariencia de la página de inicio de sesión de Microsoft 365 personalizada de la empresa objetivo.

Página de phishing que suplanta un inicio de sesión de Microsoft con contenido dinámico

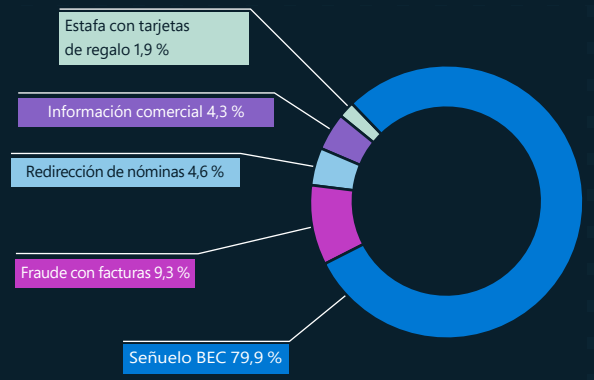


Enfoque en el compromiso de correo electrónico empresarial

Los ciberdelincuentes están desarrollando esquemas y técnicas cada vez más complejas para vencer la configuración de seguridad y dirigirse a individuos, empresas y organizaciones. En respuesta, estamos invirtiendo importantes recursos para mejorar aún más nuestro programa de aplicación de la ley de la BEC.

La BEC es el ciberdelito financiero más costoso, con una estimación de USD 2400 millones en pérdidas ajustadas en 2021, lo que representa más del 59 % de las cinco principales pérdidas por delitos en Internet a nivel mundial.[20] Para entender el alcance del problema y la mejor manera de proteger a los usuarios contra los BEC, los investigadores de seguridad de Microsoft han estado rastreando los temas más comunes utilizados en los ataques.

Temas de BEC (enero-junio de 2022)



Temas de BEC por porcentaje de aparición

Tendencias de BEC

Como punto de entrada, los atacantes de BEC normalmente intentan iniciar una conversación con las víctimas potenciales para establecer una relación. Al hacerse pasar por un colega o un conocido de negocios, el atacante conduce gradualmente la conversación en dirección a una transferencia monetaria. El correo electrónico de introducción, que rastreamos como señuelo de BEC, representa cerca del 80 % de los correos electrónicos de BEC detectados. Otras tendencias identificadas por los investigadores de seguridad de Microsoft en el último año son:

- Las técnicas más utilizadas en los ataques BEC observados en 2022 fueron la suplantación de identidad[21] y la suplantación.[22]
- El subtipo de BEC que provocó el mayor daño financiero a las víctimas fue el fraude de facturas (basado en el volumen y los importes en dólares solicitados vistos en nuestras investigaciones de campañas BEC).
- El robo de información empresarial, como los informes de cuentas por pagar y los contactos de los clientes, permite a los atacantes elaborar fraudes de facturas convincentes.
- La mayoría de las solicitudes de redirección de nóminas se enviaron desde servicios de correo electrónico gratuitos y rara vez desde cuentas comprometidas. El volumen de correos electrónicos procedentes de estos orígenes se dispara en torno a los días 1 y 15 de cada mes, las fechas de pago más habituales.
- A pesar de ser vías de fraude muy conocidas, las estafas con tarjetas de regalo solo representaron el 1,9 % de los ataques BEC detectados.

Información práctica

Defensa contra la suplantación de identidad

Para reducir la exposición de su organización al phishing, se recomienda a los administradores de TI que apliquen las siguientes directivas y funciones:

1. Exigir el uso de MFA en todas las cuentas para limitar el acceso no autorizado.
2. Habilitar las funciones de acceso condicional para las cuentas con grandes privilegios a fin de bloquear el acceso desde países, regiones e IP que no suelen generar tráfico en su organización.
3. Considerar la posibilidad de utilizar claves de seguridad físicas para los ejecutivos, los empleados que participan en actividades de pago o de compra, y otras cuentas con privilegiaos.
4. Imponer el uso de exploradores que admitan servicios como Microsoft SmartScreen para analizar las URL en busca de comportamientos sospechosos y bloquear el acceso a sitios web malintencionados conocidos.[23]
5. Utilizar una solución de seguridad basada en el machine learning que ponga en cuarentena el phishing de alta probabilidad y detone las URL y los archivos adjuntos en un sandbox antes de que el correo electrónico llegue a la bandeja de entrada, como Microsoft Defender para Office 365.[24]
6. Habilitar las funciones de protección contra la suplantación de identidad y la falsificación en toda su organización.
7. Configurar las directivas de acción de DomainKeys Identified Mail (DKIM) y Domain-based Message Authentication Reporting & Conformance (DMARC) para evitar la entrega de mensajes de correo electrónico no autenticados que podrían estar suplantando a remitentes de buena reputación.
8. Auditar las reglas de permiso creadas por el inquilino y el usuario y eliminar las excepciones basadas en el dominio y la IP. Estas reglas a menudo tienen prioridad y pueden permitir que los correos electrónicos malintencionados conocidos pasen por el filtrado de correo electrónico.
9. Ejecute de manera periódica simuladores de phishing para medir el riesgo potencial en su organización e identificar y educar a los usuarios vulnerables.

Vínculos a más información

- Del robo de cookies a BEC: los atacantes utilizan los sitios de phishing AiTM como punto de entrada para continuar con el fraude financiero | Equipo de investigación de Microsoft 365 Defender, Centro de inteligencia sobre amenazas de Microsoft (MSTIC)

Engaño de homoglifos

BEC y phishing son tácticas comunes de la ingeniería social. La ingeniería social desempeña un papel importante en la delincuencia, al persuadir a un objetivo para que interactúe con el delincuente ganando su confianza.

En el comercio físico, las marcas se utilizan para garantizar la confianza en el origen de un producto o servicio, y los productos falsificados son un abuso de la marca. Del mismo modo, los ciberdelincuentes se hacen pasar por un contacto conocido por el objetivo durante un ataque de phishing, utilizando homoglifos para engañar a las víctimas potenciales.

Un homoglifo es un nombre de dominio utilizado para la comunicación por correo electrónico en BEC, en el que se sustituye un carácter por otro de aspecto idéntico o casi idéntico, con el fin de engañar al objetivo.

Técnicas de homoglifos utilizadas en los intentos de BEC

BEC tiene generalmente dos fases, la primera de las cuales implica el compromiso de las credenciales. Estos tipos de fugas de credenciales pueden ser el resultado de ataques de phishing o vulneraciones de datos de gran tamaño. Las credenciales se venden o intercambian en la web oscura.

La segunda fase es la del fraude, en la que los atacantes utilizan las credenciales comprometidas para llevar a cabo una sofisticada ingeniería social utilizando dominios de correo electrónico homoglifos.

Progresión de un ataque BEC

Técnica	% de dominios que muestran la técnica del homoglifo
sub l para I	25 %
sub i para l	12 %
sub q para g	7 %
sub rn para m	6 %
sub .cam para .com	6 %
sub 0 para o	5 %
sub ll para l	3 %
sub ii para i	2 %
sub vv para w	2 %
sub l para ll	2 %
sub e para a	2 %
sub nn para m	1 %
sub ll para I, sub l para i	1 %
sub o para u	1 %

Análisis de más de 1700 dominios homoglifos entre enero y julio de 2022. Mientras que se utilizaron 170 técnicas de homogeneización, el 75 % de los dominios utilizaron solo 14 técnicas.

Un homoglifo en acción

Un dominio homoglifo que parece idéntico aun dominio de correo que la víctima reconoce está registrado en un proveedor de correo con un nombre de usuario que es idéntico. A continuación, se envía un correo electrónico secuestrado desde el dominio secuestrado con nuevas instrucciones de pago.

Aprovechando la inteligencia open source y el acceso a los hilos de correo electrónico, el delincuente identifica a las personas que tienen responsabilidad en la facturación y los pagos. A continuación, crea una suplantación de una dirección de correo electrónico de la persona que envía las facturas. Esta suplantación se compone de un nombre de usuario idéntico y un dominio de correo que es un homoglifo del remitente genuino.

El atacante copia una cadena de correo electrónico que contiene una factura legítima, y luego cambia la factura para que contenga sus propios datos bancarios. Esta nueva factura modificada se reenvía desde el correo electrónico de suplantación de identidad al destinatario. Como el contexto tiene sentido y el correo electrónico parece auténtico, a menudo el objetivo sigue las instrucciones fraudulentas.

Información práctica

1. Imponga el uso de exploradores que admitan servicios de análisis de URL para detectar comportamientos sospechosos y bloquee el acceso a sitios web malintencionados conocidos, como Safe Links y SmartScreen.[25]
2. Utilice una solución de seguridad basada en el machine learning que ponga en cuarentena el phishing de alta probabilidad y detone las URL y los archivos adjuntos en un sandbox antes de que el correo electrónico llegue a la bandeja de entrada.

Vínculos a más información

- Centro de quejas de delitos de Internet (IC3) | Compromiso de correo electrónico empresarial: la estafa de USD 43 mil millones
- Información de inteligencia de suplantación: Office 365 | Microsoft Docs
- Información de suplantación: Office 365 | Microsoft Docs

Una línea de tiempo de la interrupción de las redes de robots (botnet) desde los primeros días de colaboración de Microsoft

Durante más de una década, la DCU ha trabajado para detener de forma proactiva la ciberdelincuencia, que ha dado lugar a 26 programas malintencionados e interrupciones del estado nación. A medida que el equipo de la DCU utiliza tácticas y herramientas más avanzadas para acabar con estas operaciones ilícitas, vemos que los ciberdelincuentes también evolucionan sus planteamientos en un intento de mantenerse a la cabeza. A continuación se presenta una línea de tiempo que muestra un ejemplo de las redes de robots desbaratadas por la DCU y las estrategias que Microsoft adoptó para cerrarlas.

2008

Red de robots Conficker

Descripción: Un gusano de rápida propagación dirigido al sistema operativo Windows, que infectó a millones de equipos y dispositivos en una red común; provocó cortes en la red en todo el mundo.

Colaboración: Formación del grupo de trabajo Conficker, el primer consorcio de este tipo. Microsoft se asoció con 16 organizaciones de todo el mundo para derrotar al bot.

Respuesta de Microsoft: El grupo colaboró en muchas jurisdicciones internacionales y consiguió acabar con Conficker.

2009

Red de robots Waledac

Descripción: Una compleja red de robots de correo no deseado con dominios estadounidenses que recopilaba direcciones de correo electrónico y distribuía correo no deseado que infectaba hasta 90 000 equipos en todo el mundo.[26]

Colaboración: Creación de otro consorcio, el Centro de protección contra malware de Microsoft (MMPC), centrado en una estrecha colaboración con el mundo académico.[27]

Respuesta de Microsoft: Microsoft utilizó el enfoque de interrupción escalonada de C2 y sorprendió a los malos actores con la incautación de dominios basados en Estados Unidos sin previo aviso.[28] Microsoft concedió la propiedad temporal de casi 280 dominios utilizados por los servidores de Waledac.

2011

Se crea la Unidad de delitos digitales de Microsoft

Colaboración: Diseñada para frustrar la ciberdelincuencia que afecta al ecosistema de Microsoft mediante la estrecha integración de un equipo de investigadores, abogados e ingenieros.

Enfoque de Microsoft: El objetivo es comprender mejor los aspectos técnicos de los distintos programas malintencionados y entregar estos conocimientos al equipo jurídico de Microsoft para desarrollar una estrategia de interrupción eficaz.

2013

Red de robots Rustock

Descripción: Un bot de correo electrónico troyano de puerta trasera que utiliza a los proveedores de Internet como C2 principal; diseñado para vender productos farmacéuticos.

Colaboración: Microsoft forjó una asociación con Pfizer Pharmaceuticals para conocer los medicamentos vendidos por Rustock y colaboró estrechamente con las fuerzas del orden holandesas.[29]

Respuesta de Microsoft: Microsoft colaboró con los US Marshalls y las fuerzas de seguridad de los Países Bajos para desmantelar los servidores C2 en ese país. Registró y bloqueó todos los futuros algoritmos generadores de dominios (DGA).

Sirefef/red de robots (botnet) de acceso cero

Descripción: Una red de robots publicitarios diseñada para dirigir a la gente a sitios web peligrosos que instalarían malware o robarían información personal; infectó más de dos millones de equipos y costó a los anunciantes más de USD 2,7 millones al mes; principalmente en Estados Unidos y Europa Occidental.

Colaboración: Trabajó en estrecha colaboración con el FBI y el Centro de delitos informáticos de Europol para derribar la infraestructura de punto a punto.

Respuesta de Microsoft: Se unió a la red de Acceso cero, sustituyó a los servidores C2 delictivos y se apoderó con éxito de los dominios de los servidores de descarga.

2019

Red de robots Trickbot

Descripción: Una sofisticada red de robots con infraestructura fragmentada en todo el mundo que tenía como objetivo la industria de los servicios financieros; dispositivos IoT comprometidos.

Colaboración: Microsoft se asoció con el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC) para acabar con Trickbot.[30]

Respuesta de Microsoft: La DCU creó un sistema para identificar y rastrear la infraestructura de bots y generó notificaciones para los proveedores de Internet activos, teniendo en cuenta las leyes específicas de varios países.

2022

Enfoque continuo en la interrupción

Descripción: Microsoft desbarató la infraestructura de siete actores de amenazas durante el año pasado, impidiéndoles distribuir más malware, controlar los equipos de las víctimas y dirigirse a otras víctimas.

Colaboración: En colaboración con los proveedores de servicios de Internet, los gobiernos, las fuerzas de orden público y la industria privada, Microsoft compartió información para corregir a más de 17 millones de víctimas de malware en todo el mundo.

De cara al futuro

La DCU sigue innovando y pretende utilizar su experiencia en la desarticulación de redes de robots para llevar a cabo operaciones coordinadas que vayan más allá del malware. Nuestro éxito continuado requiere una ingeniería creativa, el intercambio de información, teorías jurídicas innovadoras y asociaciones públicas y privadas.

Abuso de la infraestructura por parte de los ciberdelincuentes

Gateways de Internet como infraestructura de comando y control delictivo

Los dispositivos de IoT se están convirtiendo en un objetivo cada vez más popular para los ciberdelincuentes que utilizan redes de robots generalizadas. Cuando los enrutadores no tienen revisiones y se dejan expuestos directamente a Internet, los actores de amenaza pueden abusar de ellos para obtener acceso a las redes, ejecutar ataques malintencionados e incluso apoyar sus operaciones.

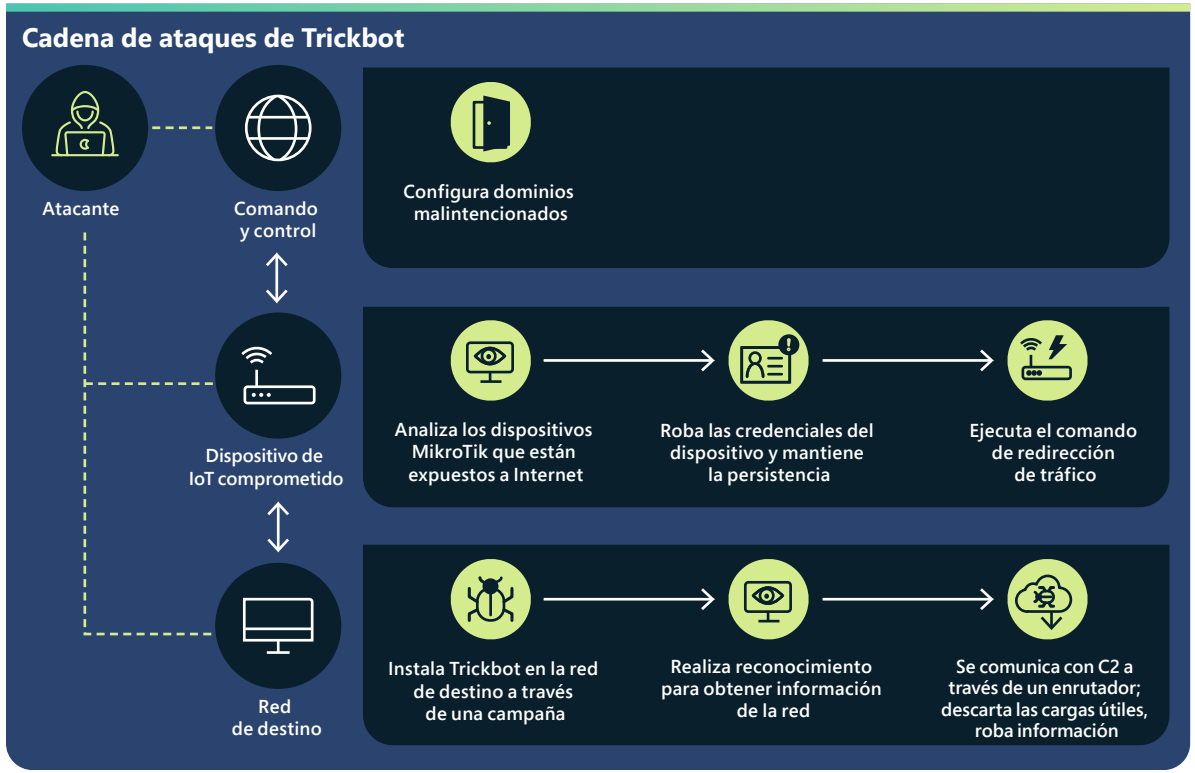
El equipo de Microsoft Defender para IoT realiza investigaciones sobre equipos que van desde controladores de sistemas de control industrial heredados hasta sensores de IoT de vanguardia. El equipo investiga el malware específico de IoT y OT para contribuir a la lista compartida de indicadores de compromiso.

Los enrutadores son vectores de ataque especialmente vulnerables porque son omnipresentes en los hogares y organizaciones conectados a Internet. Hemos estado rastreando la actividad de los enrutadores MikroTik, un enrutador popular en todo el mundo a nivel residencial y comercial, identificando cómo se utilizan para el comando y control (C2), los ataques al sistema de nombres de dominio (DNS) y el secuestro de la minería criptográfica.

Más concretamente, identificamos cómo los operadores de Trickbot utilizan enrutadores MikroTik comprometidos y los reconfiguran para que actúen como parte de su infraestructura C2. La popularidad de estos dispositivos agrava la gravedad de su abuso por parte de Trickbot, y su hardware y software únicos permiten a los actores de amenaza evadir las medidas de seguridad tradicionales, ampliar su infraestructura y comprometer más dispositivos y redes.

Los enrutadores expuestos corren el riesgo de que se exploten sus posibles vulnerabilidades.

Al rastrear y analizar el tráfico que contenía comandos de shell seguro (SSH), observamos que los atacantes utilizaban los enrutadores MikroTik para comunicarse con la infraestructura de Trickbot tras obtener credenciales legítimas para los dispositivos. Estas credenciales pueden obtenerse a través de ataques de fuerza bruta, explotando vulnerabilidades conocidas con revisiones fácilmente disponibles y utilizando contraseñas predeterminadas. Una vez que se accede a un dispositivo, el atacante emite un comando único que redirige el tráfico entre



Cadena de ataque de Trickbot que muestra el uso de dispositivos de IoT MikroTik como servidores proxy para C2.

dos puertos del enrutador, estableciendo la línea de comunicación entre los dispositivos afectados por Trickbot y el C2.

Hemos reunido nuestros conocimientos sobre los diversos métodos de ataque a los dispositivos MikroTik, más allá de Trickbot, así como las vulnerabilidades y exposiciones comunes conocidas (CVE) en una herramienta open source para los dispositivos MikroTik, que puede extraer los artefactos forenses relacionados con los ataques a estos dispositivos.[31]

Los dispositivos que actúan como proxies inversos para el malware C2 no son exclusivos de los enrutadores Trickbot y MikroTik. En colaboración con el equipo de Microsoft RiskIQ, rastreamos el C2 implicado y, mediante la observación de los certificados SSL, identificamos los dispositivos Ubiquiti y LigoWave que también se ven afectados.[32] Esto es un fuerte indicio de que los dispositivos IoT se están convirtiendo en componentes activos de los ataques coordinados de los estados nacionales y en un objetivo popular para los ciberdelincuentes que utilizan redes de robots generalizadas.

Criptodelincuentes que abusan de dispositivos de IoT

Los dispositivos de gateway son un objetivo cada vez más valioso para los actores de amenaza, ya que el número de vulnerabilidades conocidas ha crecido constantemente año tras año. Se están utilizando para la minería de criptomonedas y otros tipos de actividades malintencionadas.

A medida que la criptomoneda se ha hecho más popular, muchas personas y organizaciones han invertido potencia informática y recursos de red de dispositivos como enrutadores para minar monedas en blockchain. Sin embargo, la minería de criptomonedas es un proceso que requiere mucho tiempo y recursos y tiene pocas probabilidades de éxito. Para aumentar la probabilidad de minar una moneda, los mineros se agrupan en redes distribuidas y cooperativas, recibiendo hashes relativos al porcentaje de la moneda que lograron minar con sus recursos conectados.

El año pasado, Microsoft observó un número creciente de ataques que abusan de los enrutadores para redirigir los esfuerzos de minería de criptomonedas. Los ciberdelincuentes comprometen los enrutadores conectados a los grupos de minería y redirigen el tráfico de minería a sus direcciones IP asociadas con ataques de envenenamiento de DNS, que alteran la configuración de DNS de los dispositivos objetivo. Los enrutadores afectados registran una dirección IP errónea en un determinado nombre de dominio, enviando sus recursos de minería (o hashes) a grupos utilizados por los actores de amenaza. Estos grupos pueden minar monedas anónimas asociadas a actividades delictivas o utilizar los hashes legítimos generados por los mineros para adquirir un porcentaje de la moneda que minaron, obteniendo así las recompensas.

Dado que más de la mitad de las vulnerabilidades conocidas encontradas en 2021 carecen de la aplicación de una revisión, la actualización y la seguridad de los enrutadores en las redes corporativas y privadas sigue siendo un desafío importante para los propietarios y administradores de dispositivos.

Dispositivos comprometedores para la minería ilegal de criptomonedas.

Los actores de amenaza roban parte de los hashes del grupo original, o los recursos se transfieren a su grupo, o los enrutadores tienen malware en ellos que roban recursos para la minería.

El envenenamiento del DNS de los dispositivos gateway compromete las actividades legítimas de minería y redirige los recursos a las actividades delictivas de minería.

Máquinas virtuales como infraestructura delictiva

El paso generalizado a la nube incluye a los ciberdelincuentes que aprovechan los activos privados de las víctimas involuntarias obtenidos a través de la suplantación de identidad o la distribución de malware para el robo de credenciales. Muchos ciberdelincuentes están optando por montar sus infraestructuras malintencionadas en máquinas virtuales (VM) basadas en la nube, contenedores y microservicios.

Una vez que el ciberdelincuente tiene acceso, puede producirse una secuencia de eventos para configurar la infraestructura, como una serie de máquinas virtuales mediante scripts y procesos automatizados. Estos procesos automatizados y con scripts se utilizan para lanzar actividades malintencionadas, como ataques de correo no deseado a gran escala por correo electrónico, ataques de phishing y páginas web que hospedan contenido nefasto. Incluso puede incluir la creación de un entorno virtual a escala que lleve a cabo la minería de criptomonedas, provocando a la víctima final una factura de cientos de miles de dólares a final de mes.

Los ciberdelincuentes entienden que su actividad malintencionada tiene una vida limitada antes de su detección y cierre. Como resultado, se han ampliado y ahora operan de forma proactiva teniendo en cuenta las contingencias. Se ha observado que preparan las cuentas comprometidas con antelación y vigilan sus entornos. En cuanto se detecta una cuenta (configurada con cientos de miles de máquinas virtuales), pasan a la siguiente, ya preparada por scripts para su activación inmediata, y su actividad malintencionada continúa sin apenas interrupción.

Al igual que la infraestructura en la nube, la infraestructura local puede utilizarse en ataques con entornos locales virtuales que son desconocidos para el usuario local. Esto requiere que el punto de acceso inicial permanezca abierto y accesible. Los ciberdelincuentes también han abusado de los activos privados locales para iniciar una cadena de infraestructura en la nube, configurada para ofuscar su origen y evitar la detección de la creación de infraestructuras sospechosas.

Información práctica

1. Implemente una buena ciberhigiene e imparta capacitación en ciberseguridad a los empleados con orientaciones para evitar ser objeto de ingeniería social.
2. Realice comprobaciones periódicas automatizadas de las anomalías en la actividad de los usuarios mediante detecciones a escala para ayudar a reducir este tipo de ataques.
3. Actualice y proteja a los enrutadores en las redes corporativas y privadas.

¿El hacktivismo llegó para quedarse?

Aunque el hacktivismo no es un fenómeno nuevo, en la guerra de Ucrania se produjo una oleada de hackers voluntarios, incluidos algunos dirigidos por los gobiernos para implementar herramientas cibernéticas con el fin de dañar la reputación o los activos de opositores políticos, organizaciones e incluso estados nación.

En febrero de 2022, el gobierno ucraniano llamó a los civiles privados de todo el mundo para que llevaran a cabo ciberataques contra Rusia como parte de su "ejército informático" de 300 000 efectivos.[33] Al mismo tiempo, grupos hacktivistas establecidos como Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans y RaidForum2 comenzaron a realizar ataques en apoyo de Ucrania. Otros grupos, incluidos algunos de la banda del ransomware Conti, se pusieron del lado de Rusia.[34]

En los meses siguientes, las actividades de Anonymous fueron muy visibles. Los hackers que actúan en nombre del grupo (o en el de una de sus filiales) desactivaron temporalmente miles de sitios web rusos y bielorrusos, filtraron cientos de gigabytes de datos robados, piratearon los canales de televisión rusos para que reprodujeran contenidos proucranianos e incluso ofrecieron pagar Bitcoin por los tanques rusos entregados.

El auge de los hackers ciudadanos

Las plataformas de los medios sociales permitieron la rápida organización y movilización de miles de aspirantes a hackers ciudadanos, a los que se les proporcionaron instrucciones para llevar a cabo ataques fácilmente ejecutables, como los ataques DDoS. Los organizadores aprovecharon Twitter, Telegram y los foros privados para reunir a los hackers, organizar las operaciones y difundir los manuales de instrucciones de los hackers.

Sin embargo, es probable que la mayoría de estos hackers tengan habilidades limitadas, incluso con instrucción. Esto sugiere dos futuros potenciales: uno en el que cientos o miles de individuos con capacidades técnicas rudimentarias utilicen plantillas de ataque para llevar a cabo futuros ataques hacktivistas coordinados o individuales contra objetivos, o un segundo futuro en el que el término definitivo de las hostilidades en Ucrania les haga dejar atrás su hacktivismo, al menos hasta que el siguiente problema político o social los inspire a actuar.

Politización de los hackers

El mayor riesgo que plantea esta movilización política es el despliegue de hackers expertos en tecnología que podrían seguir realizando ciberataques contra objetivos de gobiernos extranjeros para apoyar sus propias prioridades nacionales, ya sea por iniciativa propia o a instancias de su gobierno.

Irán, China y Rusia ya utilizan el hacktivismo como fuente de reclutamiento para sus grupos de hackers del estado. Por ejemplo, en abril de 2022, el grupo de hackers prorruso Killnet lanzó ataques DDoS contra los ferrocarriles checos, los aeropuertos regionales y el servidor de la administración pública checa, a pesar de que este país no está directamente implicado en la guerra.[35] Al mismo tiempo, algunos gobiernos podrían utilizar el hacktivismo como cubierta de operaciones tradicionales de ciberespionaje o sabotaje; por ejemplo, las actividades iraníes contra Israel.

En un entorno de aumento de los ataques DDoS relacionados con el hacktivismo, la industria tecnológica se enfrenta al desafío de descifrar con rapidez la diferencia entre un flujo de tráfico normal y otro anormal hacia un sitio web. Microsoft y sus socios han desarrollado una colección de herramientas que distinguen el tráfico DDoS malintencionado y lo rastrean hasta su origen. Además, la plataforma Azure de Microsoft puede identificar las máquinas de la plataforma que producen niveles extraordinariamente altos de tráfico saliente y apagarlas.

Surgimiento del software de protesta

El software de protesta surgió como resultado directo de las reacciones emocionales a la guerra entre Rusia y Ucrania. Algunos desarrolladores de software open source utilizaron la popularidad de su software como medio para alzar la voz o tomar medidas contra una situación geopolítica en desarrollo. Esto incluía archivos de texto inofensivos que se abrían en un escritorio o un navegador para difundir mensajes de paz, pero también incluía ataques dirigidos basados en la geolocalización de direcciones IP y acciones destructivas como el borrado de un disco duro. A medida que se desarrollen otros acontecimientos mundiales, podemos esperar que el software de protesta vuelva a salir a la superficie en el futuro. Dado que, por lo general, se trata de casos en los que mantenedores open source muy respetados deciden hacer declaraciones personales utilizando sus propios componentes open source, actualmente no existe ninguna protección que impida que se produzcan este tipo de cambios en los paquetes de archivos de origen y los usuarios deben ser conscientes del impacto potencial.

Las plataformas de los medios sociales permitieron la organización y movilización de miles de aspirantes a hackers ciudadanos, a los que se les proporcionaron instrucciones para llevar a cabo ataques fácilmente ejecutables, como los ataques DDoS.

Información práctica

1. La industria tecnológica debe unirse para diseñar una respuesta integral a esta nueva amenaza.
2. Las principales empresas tecnológicas, como Microsoft, disponen de herramientas para identificar el tráfico malintencionado asociado a los ataques DDoS y desactivar las máquinas responsables.
3. Los usuarios open source deben mantener una mayor vigilancia en tiempos de conflicto geopolítico.

Notas finales

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. Detección y respuesta de puntos de conexión. https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. Un foro vetado es un foro de discusión en línea que requiere que un miembro existente avale la incorporación de un nuevo miembro.
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. Fuente de datos: Defender para Office (correo electrónico malintencionado/actividad de identidad comprometida), Azure Active Directory Identity Protection (eventos/alertas de identidad comprometida), Defender for Cloud Apps (eventos de acceso a datos de identidad comprometida) y M365D (correlación entre productos).
17. Fuente de datos: Defender para punto de conexión (alertas/eventos de comportamiento de ataque), Defender para Office (correo electrónico malintencionado) y M365D (correlación entre productos).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Domain-based Message Authentication, Reporting and Conformance: Un protocolo de autenticación de correo electrónico, directivas e informes diseñado para dar a los propietarios de dominios de correo electrónico la capacidad de proteger su dominio del uso no autorizado.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va. 22 de febrero, 2010).
27. Consulte Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 de septiembre de 2011.
28. En concreto, la Regla 65 de las Reglas Federales de Procedimiento Civil permite a una parte solicitar dicho remedio si 1) la parte sufrirá un daño inmediato e irreparable si no se concede la solución, y 2) la parte intenta notificar a la otra parte de manera oportuna. Además, la ley exige que se aplique una prueba de equilibrio, en la que se compare el derecho del demandado a ser notificado con el grado de perjuicio para el público.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9 de febrero de 2011).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 de agosto de 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Amenazas para los estados nación

Los actores de estado nación lanzan ciberataques cada vez más sofisticados para evadir la detección y promover sus prioridades estratégicas.

Información general de las amenazas para los estados nación

Los actores de estado nación lanzan ciberataques cada vez más sofisticados para evadir la detección y promover sus prioridades estratégicas. La llegada de la implementación de armas cibernéticas en la guerra híbrida de Ucrania es el inicio de una nueva era de conflictos.

Rusia también ha apoyado su guerra con operaciones de influencia informativa, utilizando la propaganda para influir en las opiniones de Rusia, en Ucrania y el resto del mundo. Este primer conflicto híbrido a gran escala ha enseñado otras lecciones importantes. En primer lugar, la seguridad de las operaciones y los datos digitales puede protegerse mejor, tanto en el ciberespacio como en el espacio físico, trasladándose a la nube. Los primeros ataques rusos se dirigieron a servicios locales con malware limpiador, y apuntaron a centros de datos físicos con uno de los primeros misiles lanzados.

Ucrania respondió trasladando con rapidez las cargas de trabajo y los datos a nubes de gran escala hospedadas en centros de datos fuera de Ucrania. En segundo lugar, los avances en la inteligencia de las ciberamenazas y la protección de los puntos de conexión impulsada por los datos y los servicios avanzados de IA y ML en la nube han ayudado a Ucrania a defenderse de los ciberataques rusos.

En otros lugares, los actores de estado nación han aumentado su actividad y están utilizando los avances en la automatización, la infraestructura en la nube y las tecnologías de acceso remoto para atacar un conjunto más amplio de objetivos. Las cadenas de suministro de TI corporativas que permiten el acceso a los objetivos finales fueron atacadas con frecuencia. La higiene de la ciberseguridad se volvió aún más crítica cuando los actores explotaron rápidamente las vulnerabilidades sin revisiones, utilizaron técnicas sofisticadas y de fuerza bruta para robar credenciales y ofuscaron sus operaciones utilizando software open source o legítimo. E Irán se une a Rusia en el uso de ciberarmas destructivas, incluido el ransomware, como elemento básico de sus ataques.

Estos acontecimientos exigen la adopción urgente de un marco global coherente que dé prioridad a los derechos humanos y proteja a las personas del comportamiento imprudente del estado en línea. Todas las naciones deben trabajar juntas para las normas y reglas acordadas para una conducta de estado responsable.

› La defensa de Ucrania: Primeras lecciones de la guerra cibernética: Microsoft On the Issues

Mayor focalización en las infraestructuras críticas, en especial en el sector de la TI, los servicios financieros, los sistemas de transporte y las infraestructuras de comunicación.

› Más información en la página 35

La cadena de suministro de TI se utiliza como gateway a los objetivos.

NOBELIUM

› Más información en la página 36

China está ampliando sus objetivos a nivel mundial, en especial en los países más pequeños del sudeste asiático, para obtener información y ventajas competitivas.

› Más información en la página 44

Irán se volvió cada vez más agresivo tras la transición de poder, amplió los ataques de ransomware más allá de los adversarios regionales a las víctimas de EE. UU. y la UE, y tuvo como objetivo infraestructuras críticas estadounidenses de alto perfil.

› Más información en la página 46

La identificación y rápida explotación de las vulnerabilidades sin revisiones se ha convertido en una táctica clave. La rápida implementación de las actualizaciones de seguridad es la clave de la defensa.

› Más información en la página 39

Corea del Norte atacó a las empresas de defensa y aeroespaciales, a las criptomonedas, a los medios de comunicación, a los desertores y a las organizaciones de ayuda, para lograr los objetivos del régimen: construir la defensa, reforzar la economía y garantizar la estabilidad interna.

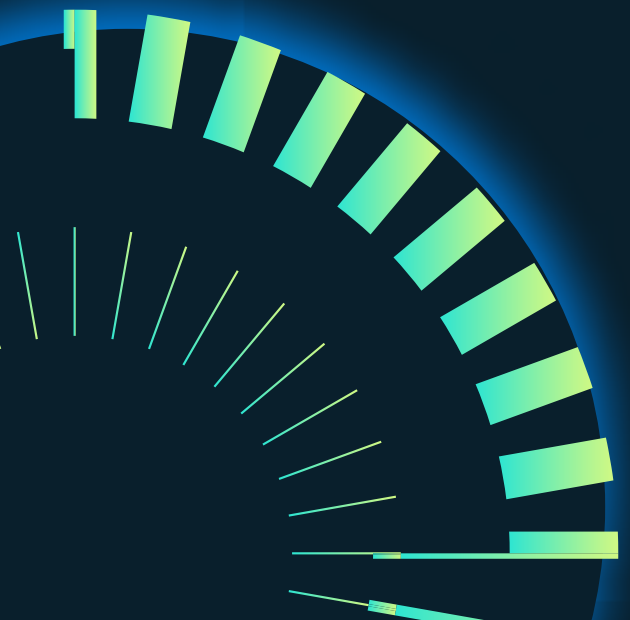
› Más información en la página 49

Los cibermercenarios amenazan la estabilidad del ciberespacio, ya que esta creciente industria de empresas privadas está desarrollando y vendiendo herramientas, técnicas y servicios avanzados para que sus clientes (a menudo gobiernos) puedan irrumpir en redes y dispositivos.

› Más información en la página 52

Introducción

Tras los ataques de alto perfil en 2020 y 2021, los actores de amenaza de los estados nación gastaron importantes recursos para adaptarse a las nuevas protecciones de seguridad implementadas por las organizaciones para defenderse de las amenazas sofisticadas.



Al igual que las organizaciones empresariales, los adversarios comenzaron a utilizar los avances en la automatización, la infraestructura en la nube y las tecnologías de acceso remoto para extender sus ataques contra un conjunto más amplio de objetivos. Estos ajustes tácticos dieron lugar a nuevos enfoques y ataques a gran escala contra las cadenas de suministro de las empresas. La higienez de la seguridad informática adquirió un grado de importancia aún mayor a medida que los actores desarrollaban nuevas formas de explotar con rapidez las vulnerabilidades sin revisiones, ampliaban las técnicas para comprometer las redes corporativas y ofuscaban sus operaciones utilizando software open source o legítimo. Las nuevas técnicas de ataque ofrecen vectores nuevos y más difíciles de detectar para acceder a la red de un objetivo. Por último, a medida que se intensificaban los ataques físicos en tiempos de guerra, vimos cómo los ciberataques adquirían un papel destacado en la actividad militar.

El conflicto en Ucrania ha proporcionado un ejemplo demasiado significativo de cómo los ciberataques evolucionan para impactar en el mundo en paralelo al conflicto militar sobre el terreno. Los sistemas eléctricos, los sistemas de telecomunicaciones, los medios de comunicación y otras infraestructuras críticas se convirtieron en objetivos de ataques físicos y ciberataques. Los intentos de comprometer la red comúnmente observados como parte de las campañas de espionaje y filtración de información se centraron en la guerra híbrida en los ataques destructivos de malware limpiador contra los sistemas de infraestructuras críticas. La conexión de la seguridad de estos sistemas a la nube permitió la detección temprana y la interrupción de ataques potencialmente devastadores.[1]

Por primera vez en un gran evento cibernético, las detecciones de comportamiento que aprovechan el machine learning utilizaron patrones de ataque conocidos para identificar y detener con éxito nuevos ataques sin conocimiento previo del malware subyacente, incluso antes de que los humanos fueran conscientes de las amenazas. También confirmamos el valor de compartir la inteligencia sobre amenazas en tiempo real con los defensores que protegen estos sistemas, dándoles información vital para prever y defenderse de los ataques activos.

Los actores de amenaza de los estados nación de todo el mundo siguen expandiendo sus operaciones de formas nuevas y antiguas. China, Corea del Norte, Irán y Rusia realizaron ataques a clientes de Microsoft. La cadena de suministro de servicios de TI se convirtió en un objetivo común a medida que los actores cambiaron el enfoque a los servicios ascendentes que pueden ser puntos de acceso a múltiples organizaciones. Esperamos que los actores continúen explotando las relaciones de confianza en las cadenas de suministro de las empresas, haciendo hincapié en la importancia de la aplicación exhaustiva de las normas de autenticación, la aplicación de revisiones diligentes y la configuración de cuentas para la infraestructura de acceso remoto, así como las auditorías frecuentes de las relaciones con los socios para comprobar la autenticidad.

Los actores de estado nación, al igual que los operadores delictivos y de ransomware, han respondido al aumento de la exposición dirigiéndose a los sistemas empresariales mal configurados o sin revisiones (infraestructura VPN/VPS, servidores en las instalaciones, software de terceros) para llevar a cabo ataques en vivo. Muchos han incrementado el uso de malware básico y herramientas de equipo rojo open source para ofuscar su actividad malintencionada.

Como resultado, el mantenimiento de una base sólida de higiene de seguridad de TI a través de la aplicación de revisiones prioritarias, la activación de funciones antimanipulación, el uso de herramientas de administración de la superficie de ataque como RiskIQ para obtener una visión externa de una superficie de ataque, y la activación de la autenticación multifactor en toda la empresa se han convertido en fundamentos básicos para defenderse de forma proactiva contra muchos actores sofisticados.

Los actores de estado nación también han aumentado el uso del ransomware como táctica en sus ataques, a menudo reutilizando el malware de rescate creado por ese ecosistema delictivo en sus ataques. Hemos visto a actores con base en Irán y Corea del Norte que aprovechan las herramientas de ransomware para dañar los sistemas objetivo, a menudo incluyendo la infraestructura crítica, dentro de los rivales regionales. Por último, hemos visto la creciente amenaza de los cibermercenarios que desarrollan y venden herramientas, técnicas y servicios para ampliar las vulnerabilidades contra soluciones vulnerables de terceros. La sofisticación y la agilidad de los ataques de los actores de estado nación seguirán evolucionando cada año. Las organizaciones deben responder estando informadas de estos cambios de los actores y evolucionar las defensas en paralelo.

John Lambert
Vicepresidente corporativo e ingeniero distinguido, Centro de inteligencia sobre amenazas de Microsoft

Antecedentes sobre los datos de los estados nación

Las amenazas para los estados nación se definen como actividades de ciberamenazas que se originan en un país específico con la aparente intención de fomentar los intereses nacionales. Los actores de estado nación presentan algunas de las amenazas más avanzadas y persistentes a las que se enfrentan nuestros clientes, como el robo de propiedad intelectual, el espionaje, la vigilancia, el robo de credenciales y los ataques destructivos, entre otros.

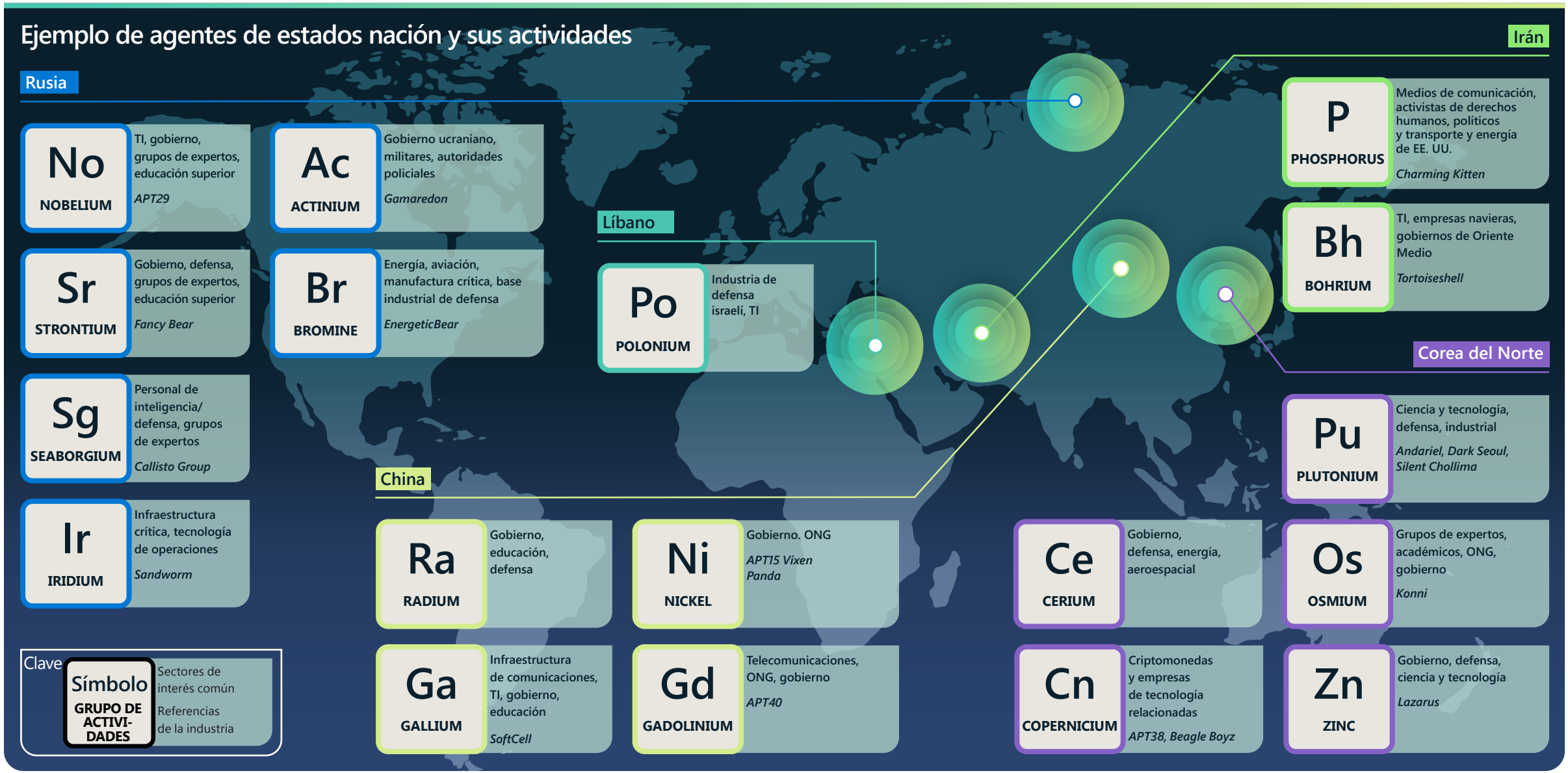
Invertimos importantes recursos en descubrir, comprender y contrarrestar estas amenazas. Cuando una organización o el titular de una cuenta individual es el objetivo o se ve comprometido por actividades observadas de un estado nación, Microsoft envía una alerta en forma de notificación de estado nación (NSN) directamente al cliente, incluyendo la información que necesitan para investigar la actividad. Hasta junio de 2022, habíamos entregado más de 67 000 NSN desde que comenzamos en 2018.

Los datos de las alertas NSN de Microsoft se presentan en este capítulo para ofrecer una visión de la actividad medible. El nivel de actividad del estado-nación que se muestra en los gráficos se basa en el número de NSN que Microsoft ha emitido a los clientes en respuesta a la detección de actores del estado nación que atacan o comprometen al menos una cuenta de la organización del cliente.

Los cuatro principales estados nación cuyos grupos de amenaza incluimos en este informe son Rusia, China, Irán y Corea del Norte. Estos representan los países de origen de los actores más comúnmente observados que se dirigen a los clientes de Microsoft en el último año. El informe también incluye nuestras observaciones sobre los grupos de amenaza del Líbano y de los cibermercenarios, o actores ofensivos del sector privado por encargo.

Microsoft identifica los grupos de estados nación por nombres de elementos químicos (como NOBELIUM), algunos de los cuales se muestran en la siguiente página. Utilizamos las designaciones DEV-#### como un nombre temporal dado a un grupo de actividad de amenaza desconocido, emergente o en desarrollo, que nos permite seguirlo como un conjunto único de información hasta que alcancemos un alto grado de confianza sobre el origen o la identidad del actor que está detrás de la actividad.

Una vez que cumple los criterios, una DEV se convierte en un actor con nombre o se fusiona con los actores existentes. A lo largo de este capítulo, citamos ejemplos de grupos de estado nación y de DEV para brindar una visión más profunda de los objetivos de los ataques, las técnicas y el análisis de las motivaciones. Aunque muchos de estos grupos utilizan las mismas herramientas que los ciberdelincuentes, presentan amenazas únicas en forma de malware a medida, la capacidad de descubrir y aprovechar las vulnerabilidades de día cero y la impunidad legal.


Ejemplo de agentes de estados nación y sus actividades
Rusia
No
NOBELIUM
TI, gobierno, grupos de expertos, educación superior
APT29
Ac
ACTINIUM
Gobierno ucraniano, militares, autoridades policiales
Gamaredon
Sr
STRONTIUM
Gobierno, defensa, grupos de expertos, educación superior
Fancy Bear
Br
BROMINE
Energía, aviación, manufactura crítica, base industrial de defensa
EnergeticBear
Sg
SEABORGIUM
Personal de inteligencia/ defensa, grupos de expertos
Callisto Group
Ir
IRIDIUM
Infraestructura crítica, tecnología de operaciones
Sandworm
Líbano
Po
POLONIUM
Industria de defensa israelí, TI
Irán
P
PHOSPHORUS
Medios de comunicación, activistas de derechos humanos, políticos y transporte y energía de EE. UU.
Charming Kitten
Bh
BOHRIUM
TI, empresas navieras, gobiernos de Oriente Medio
Tortoiseshell
Corea del Norte
Pu
PLUTONIUM
Ciencia y tecnología, defensa, industrial
Andariel, Dark Seoul, Silent Chollima
China
Ra
RADIUM
Gobierno, educación, defensa
Ni
NICKEL
Gobierno. ONG
APT15 Vixen Panda
Ce
CERIUM
Gobierno, defensa, energía, aeroespacial
Os
OSMIUM
Grupos de expertos, académicos, ONG, gobierno
Konni
Ga
GALLIUM
Infraestructura de comunicaciones, TI, gobierno, educación
SoftCell
Gd
GADOLINIUM
Telecomunicaciones, ONG, gobierno
APT40
Cn
COPERNICIUM
Criptomonedas y empresas de tecnología relacionadas
APT38, Beagle Boyz
Zn
ZINC
Gobierno, defensa, ciencia y tecnología
Lazarus
Clave
Símbolo
GRUPO DE ACTIVI-DADES
Sectores de interés común
Referencias de la industria

La evolución del panorama de las amenazas

La misión de Microsoft de rastrear la actividad de los actores de estado nación y notificar a los clientes cuando vemos que están siendo atacados o comprometidos está arraigada en nuestra misión de proteger a nuestros clientes de los ataques.

Esta notificación es una parte crucial de nuestro compromiso de informar a los clientes si los ataques observados se evitan con éxito gracias a las protecciones de nuestros productos de seguridad, o si los ataques son efectivos debido a debilidades de seguridad desconocidas. El seguimiento de las notificaciones a lo largo del tiempo ayuda a Microsoft. a identificar la evolución de las tendencias de las amenazas por parte de los actores y a centrar las protecciones de los productos en la mitigación proactiva de las amenazas para los clientes en todos nuestros servicios en la nube.

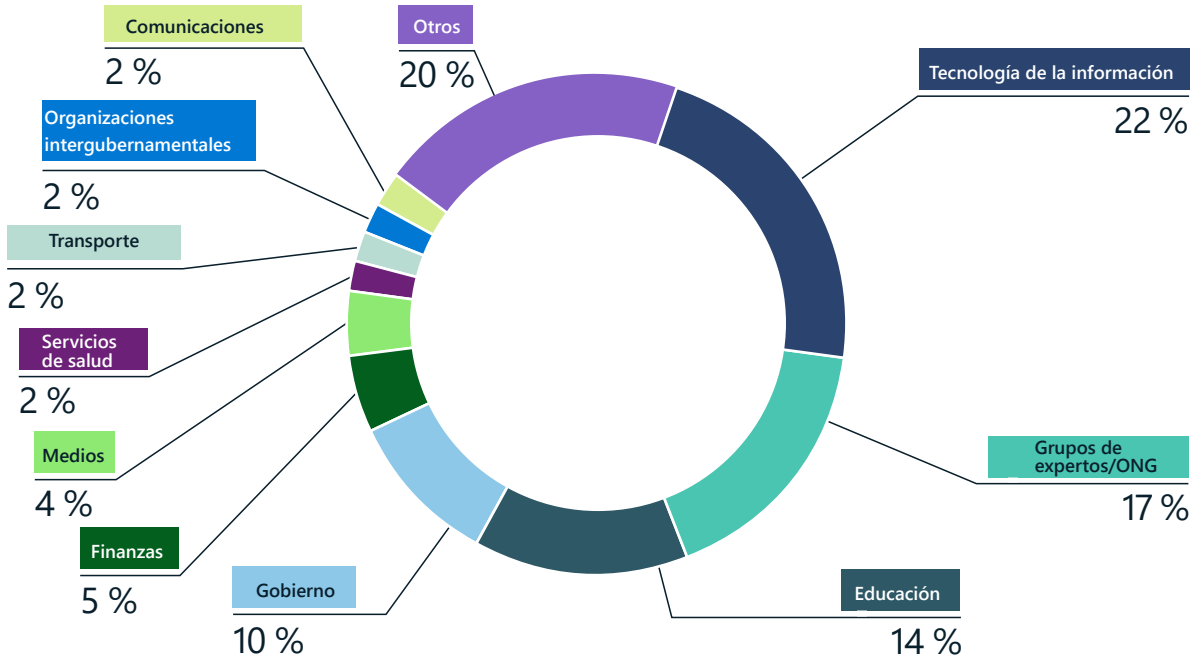
Este seguimiento también nos permite compartir datos e información sobre lo que vemos. Los analistas que rastrean a estos actores y siguen sus ataques se basan en una combinación de indicadores técnicos y conocimientos geopolíticos para comprender las motivaciones de los actores, combinando el contexto técnico y el global en nuevas percepciones. Esta recopilación ofrece una visión única de las prioridades de los actores cibernéticos de los estados nación y de cómo sus motivaciones pueden reflejar las prioridades políticas, militares y económicas de los estados nación que los emplean.

Los acontecimientos políticos del último año han configurado las prioridades y la tolerancia al riesgo de los grupos de amenazas patrocinados por el estado en todo el mundo. A medida que las relaciones geopolíticas se han ido resquebrajando y que los elementos de corte belicista han adquirido más control en algunas naciones, los actores cibernéticos se han vuelto más descarados y agresivos. Por ejemplo:

- Rusia atacó sin descanso al gobierno ucraniano y a las infraestructuras críticas del país para complementar su acción militar sobre el terreno.[2]
- Irán buscó agresivamente incursiones en las infraestructuras críticas de Estados Unidos, como las autoridades portuarias.
- Corea del Norte continuó su campaña de robo de criptomonedas a empresas financieras y tecnológicas.
- China amplió sus operaciones de ciberespionaje mundial.

Aunque los actores del estado nación pueden ser técnicamente sofisticados y emplear una amplia variedad de tácticas,a menudo una buena higiene cibernética puede mitigar sus ataques. Muchos de estos actores confían en medios relativamente poco tecnológicos, como los correos electrónicos de phishing de objetivo definido, para distribuir sofisticados programas malintencionados, en lugar de invertir en el desarrollo de vulnerabilidades personalizadas o en el uso de ingeniería social dirigida para lograr sus objetivos.

Sectores industriales a los que apuntan los actores de estado nación



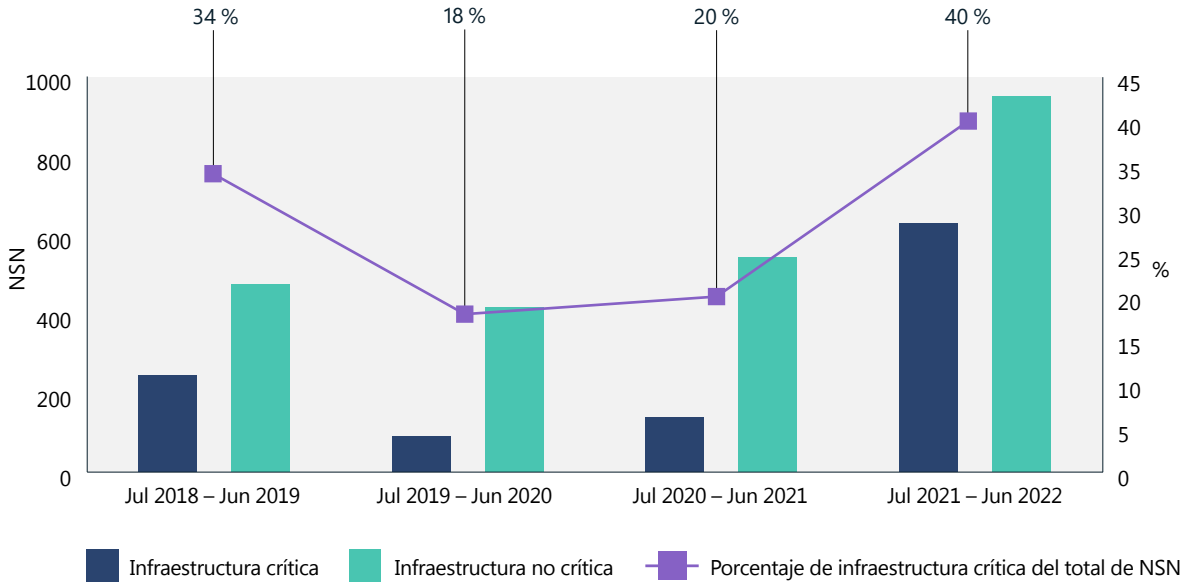
Los grupos de estado nación se dirigieron a una variedad de sectores. Los actores de estado rusos e iraníes apuntaron a la industria de las tecnologías de la información como medio para acceder a los clientes de las empresas de este sector. Los grupos de expertos, las organizaciones no gubernamentales (ONG), las universidades y los organismos gubernamentales siguieron siendo otros objetivos habituales de los actores de estado nación.

Los actores de estado nación tienen una variedad de objetivos que pueden llevar a apuntar a grupos específicos de organizaciones o individuos. En el último año han aumentado los ataques a la cadena de suministro, con especial atención a las empresas de TI. Al comprometer a los proveedores de servicios de TI, los actores de amenaza a menudo son capaces de llegar a su objetivo original a través de una relación de confianza con la empresa que administra los sistemas conectados, o de ejecutar potencialmente ataques a una escala mucho mayor comprometiendo a cientos de clientes posteriores en un solo ataque. Después del sector de TI, las entidades más atacadas fueron los grupos de expertos, los académicos adscritos a universidades y los funcionarios públicos. Se trata de "objetivos blandos" deseables para el espionaje con el fin de recopilar información sobre asuntos geopolíticos.

La evolución del panorama de las amenazas

Continuación

Tendencias de la infraestructura crítica

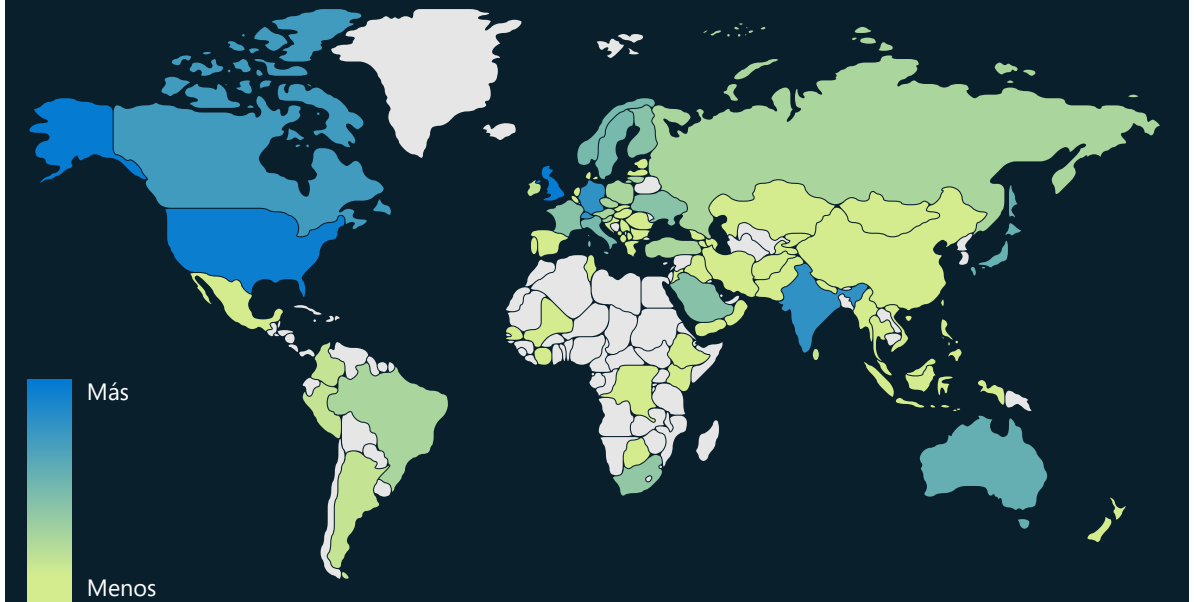


El año pasado aumentaron los objetivos de los grupos de estado nación[3] sobre las infraestructuras críticas, centrándose los actores en las empresas del sector informático, los servicios financieros, los sistemas de transporte y las infraestructuras de comunicaciones.

"Antes de la invasión de Ucrania, los gobiernos pensaban que los datos debían permanecer dentro de un país para estar seguros. Tras la invasión, migrar los datos a la nube y salir de las fronteras territoriales forma parte de la planificación de la resiliencia y el buen gobierno".

Cristin Flynn Goodwin,
Consejero general adjunto, Seguridad y confianza del cliente

La orientación geográfica de los actores de estado nación



El año pasado, los grupos de estado nación atacaron a todo e mundo, con especial atención a las empresas estadounidenses y británicas. Las organizaciones de Israel, los Emiratos Árabes Unidos, Canadá, Alemania, India, Suiza y Japón también se encontraban entre los objetivos más frecuentes, según nuestros datos del NSN.

Información práctica

1. Identifique y proteja sus posibles objetivos de datos de alto valor, las tecnologías de riesgo, la información y las operaciones comerciales que podrían alinearse con las prioridades estratégicas de los grupos de estado nación.
2. Permita que las protecciones en la nube brinden la identificación y mitigación de las amenazas conocidas y nuevas para su red a escala.

La cadena de suministro de TI como gateway al ecosistema digital

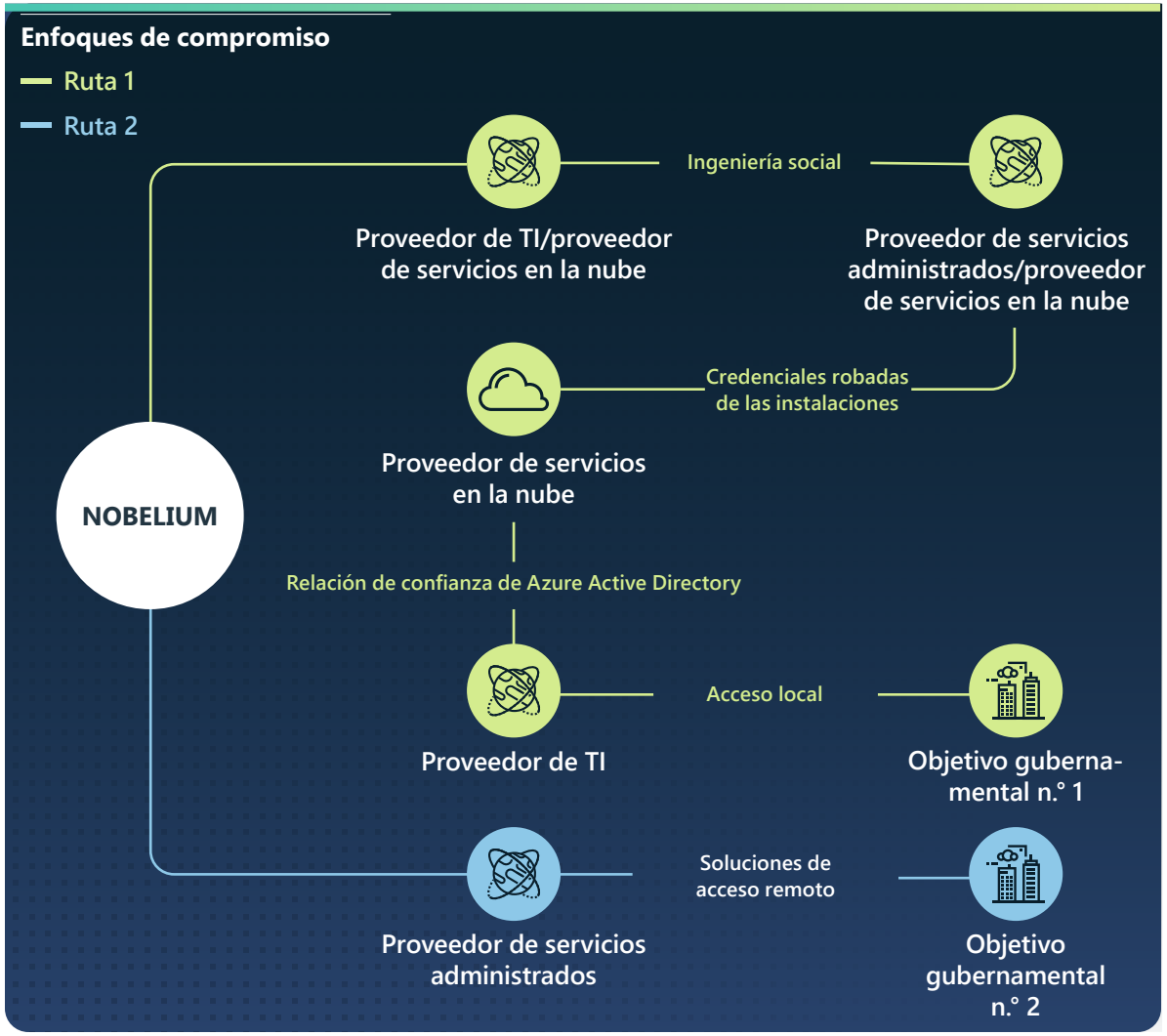
El hecho de que los estados nación apunten a los proveedores de servicios de TI podría permitir a los actores de amenaza explotar otras organizaciones de interés aprovechando la confianza y el acceso concedido a estos proveedores de la cadena de suministro. El año pasado, los grupos de ciberamenaza de estado nación se dirigieron a los proveedores de servicios de TI para atacar objetivos de terceros y obtener acceso a los clientes de los sectores gubernamental, político y de infraestructuras críticas.

Los proveedores de servicios informáticos son objetivos intermediarios atractivos, ya que prestan servicio a cientos de clientes directos y miles de clientes indirectos de interés para los servicios de inteligencia extranjeros. Si se explotan, las prácticas comerciales rutinarias y los privilegios administrativos delegados de los que gozan estas empresas, podrían permitir a los actores malintencionados acceder y manipular las redes de los clientes de los proveedores de servicios de TI sin que se activen inmediatamente las alertas.

El año pasado, NOBELIUM intentó comprometer y aprovechar las cuentas con privilegios de los proveedores de soluciones en la nube y de otros servicios administrados para intentar acceder a clientes políticos y gubernamentales de Estados Unidos y Europa.

NOBELIUM demostró cómo un enfoque de "comprometer a uno para comprometer a muchos" podía dirigirse contra un adversario geopolítico percibido. El año pasado, el actor de amenaza persiguió la intrusión tanto de terceros como directa en organizaciones sensibles con sede en los estados miembro de la Organización del Tratado del Atlántico Norte (OTAN), que el gobierno ruso percibe como una amenaza existencial. Entre julio de 2021 y principios de junio de 2022, el 48 % de las notificaciones de clientes de Microsoft sobre la actividad de amenazas rusas contra clientes de servicios en línea se dirigieron a empresas del sector informático con sede en países miembros de la OTAN, probablemente como puntos de acceso intermediarios. En general, el 90 % de las notificaciones sobre la actividad de las amenazas rusas durante el mismo periodo se dirigieron a clientes con sede en los estados miembro de la OTAN, principalmente en los sectores de las tecnologías de la información, los grupos de expertos y las organizaciones no gubernamentales (ONG), y el gobierno, lo que sugiere una estrategia de búsqueda de múltiples medios de acceso inicial a estos objetivos.

Se ha pasado de explotar la cadena de suministro de software a explotar la cadena de suministro de servicios de TI, dirigiéndose a las soluciones en la nube y a los proveedores de servicios administrados para llegar a los clientes posteriores.



Este diagrama muestra el enfoque multivectorial de NOBELIUM para comprometer sus objetivos finales y los daños colaterales a otras víctimas en el camino. Además de las acciones mostradas con anterioridad, NOBELIUM lanzó ataques de difusión de contraseñas y de phishing contra las entidades implicadas, apuntando incluso a la cuenta personal de a lmenos un empleado del gobierno como otra vía potencial de compromiso.

La cadena de suministro de TI como gateway al ecosistema digital

Continuación

A lo largo del año, el Centro de inteligencia sobre amenazas de Microsoft (MSTIC) detectó un número creciente de actores estatales iraníes y afiliados a Irán que comprometen a las empresas de TI. En muchos casos, se detectó que los actores robaban credenciales de inicio de sesión para acceder a los clientes posteriores con diversos objetivos, desde la recopilación de información hasta los ataques destructivos de represalia.

- En julio y agosto de 2021, DEV-0228 comprometió a un proveedor de software empresarial israelí para luego comprometer a clientes posteriores en los sectores israelíes de defensa, energía y legal.[4]
- Entre agosto y septiembre de 2021, Microsoft detectó un pico de actores estatales iraníes que atacaban a empresas de TI con sede en la India. La ausencia de problemas geopolíticos apremiantes que hubieran provocado ese cambio sugiere que este objetivo es el acceso indirecto a filiales y clientes fuera de la India.
- En enero de 2022, DEV-0198, un grupo que consideramos afiliado al gobierno de Irán, comprometió a un proveedor israelí de soluciones en la nube. Microsoft evalúa que el actor probablemente utilizó credenciales comprometidas del proveedor para autenticarse en una empresa de logística israelí. MSTIC observó que el mismo actor intentaba llevar a cabo un ciberataque destructivo contra la empresa de logística ese mismo mes.
- En abril de 2022, POLONIUM, un grupo con sede en el Líbano que, según evaluamos, colaboraba con grupos estatales iraníes en técnicas de la cadena de suministro de tecnologías de la información, comprometió a otra empresa israelí de TI para obtener acceso a organizaciones legales y de defensa israelíes.[5]

La actividad de este último año demuestra que actores de amenaza como NOBELIUM y DEV-0228 están familiarizándose con el panorama de las relaciones de confianza de una organización mejor que las propias organizaciones. Este aumento de la amenaza pone de relieve la necesidad de que las organizaciones comprendan y endurezcan las fronteras y los puntos de entrada de sus patrimonios digitales. También subraya la importancia de que los proveedores de servicios informáticos supervisen rigurosamente su propia salud en materia de ciberseguridad. Por ejemplo, las organizaciones tienen que implementar la autenticación multifactor y las directivas de acceso condicional que dificultan a los actores malintencionados la captura de cuentas con privilegios o la propagación a través de una red. Llevar a cabo una revisión y una auditoría exhaustivas de las relaciones con los socios ayuda a minimizar cualquier permiso innecesario entre su organización y los proveedores anteriores y a eliminar inmediatamente el acceso a cualquier relación que parezca extraña. Familiarizarse con los registros de actividad y revisar la actividad disponible facilita la detección de anomalías que podrían dar lugar a una investigación más profunda.

> El hecho de que los estados nación apunten a terceros les permite explotar organizaciones sensibles aprovechando la confianza y el acceso en una cadena de suministro.

Información práctica

1. Revise y audite las relaciones con los proveedores de servicios ascendentes y descendentes y los accesos con privilegios delegados para minimizar los permisos innecesarios. Elimine el acceso a las relaciones de socios que parezcan desconocidas o que aún no hayan sido auditadas.[6]
2. Habilite el registro y revise toda la actividad de autenticación para la infraestructura de acceso remoto y las redes privadas virtuales (VPN), centrándose en las cuentas configuradas con autenticación de factor único, para confirmar la autenticidad e investigar la actividad anómala.
3. Habilite la MFA para todas las cuentas (incluidas las de servicio) y asegúrese de que la MFA se aplique a toda la conectividad remota.
4. Utilice soluciones sin contraseña para asegurar las cuentas.[7]

Vínculos a más información

- NOBELIUM se dirige a los privilegios administrativos delegados para facilitar ataques más amplios | Centro de inteligencia sobre amenazas de Microsoft (MSTIC)
- Aumenta el número de objetivos iraníes en el sector de la TI | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft
- Exponer la actividad y la infraestructura de POLONIUM dirigida a organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC)

Explotación rápida de las vulnerabilidades

A medida que las organizaciones refuerzan sus posturas de ciberseguridad, los actores de estado nación responden buscando tácticas nuevas y únicas para realizar ataques y evadir la detección. La identificación y explotación de vulnerabilidades previamente desconocidas (conocidas como vulnerabilidades de día cero) es una táctica clave en este esfuerzo.

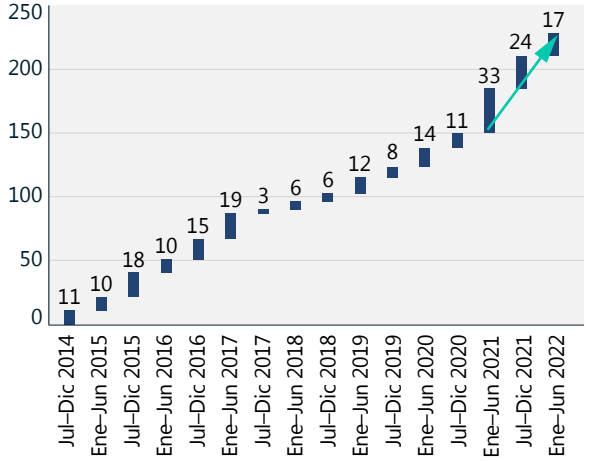
Las vulnerabilidades de día cero son un medio especialmente eficaz para la explotación inicial y, una vez expuestas de manera pública, otros estados nación y actores delictivos pueden reutilizar las vulnerabilidades. El número de vulnerabilidades de día cero divulgadas públicamente durante el año pasado está a la par con las del año anterior, que fue el más alto registrado.

A medida que los actores de ciberamenaza (tanto los estados nación como los delincuentes) se vuelven más hábiles en el aprovechamiento de estas vulnerabilidades, hemos observado una reducción en el tiempo entre el anuncio de una vulnerabilidad y la mercantilización de esa vulnerabilidad. Esto hace que sea esencial que las organizaciones apliquen revisiones en las vulnerabilidades inmediatamente. Del mismo modo, es fundamental que las organizaciones o las personas que descubran nuevas vulnerabilidades las divulguen de forma responsable o las comuniquen a los proveedores afectados lo antes posible, de acuerdo con los procedimientos coordinados de divulgación de vulnerabilidades.

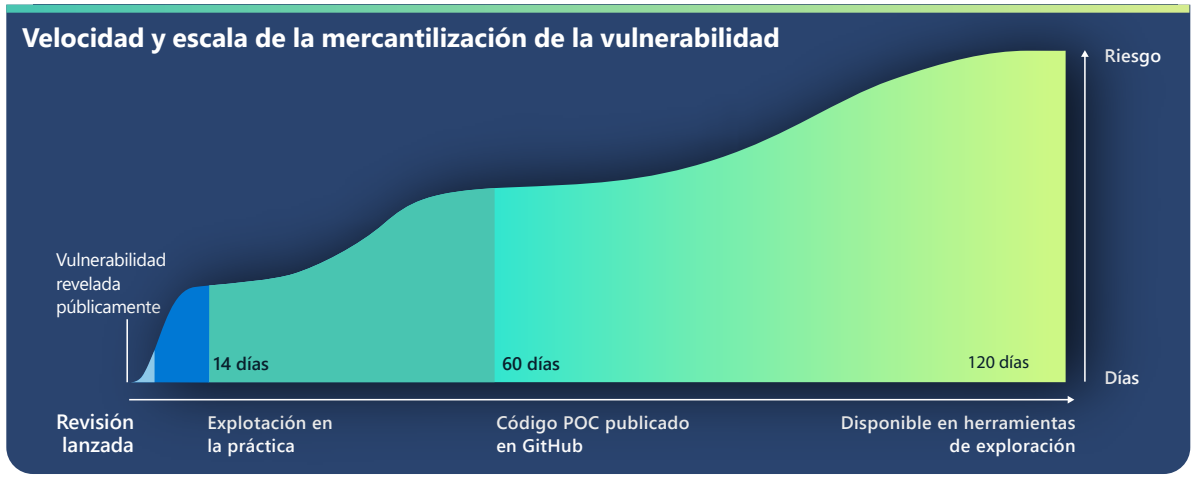
Esto garantiza que se identifiquen las vulnerabilidades y se desarrollen revisiones de manera oportuna para proteger a los clientes de amenazas que antes se desconocían.

Muchas organizaciones suponen que tienen menos probabilidades de ser víctimas de ataques de día cero si la administración de vulnerabilidades forma parte de la seguridad de su red. Sin embargo, la mercantilización de las vulnerabilidades está haciendo que lleguen a un ritmo mucho más rápido. Los exploits de día cero a menudo son descubiertos por otros actores y se reutilizan ampliamente en un corto período de tiempo, lo que deja en riesgo a los sistemas sin revisiones. Aunque la explotación de día cero puede ser difícil de detectar, las acciones de los actores después de la explotación son a menudo más fáciles de detectar y, si provienen de software totalmente revisado, pueden actuar como una señal de advertencia de un compromiso.

Revisiones liberadas para vulnerabilidades de día cero



Número de vulnerabilidades de día cero públicamente reveladas de la Lista de vulnerabilidades y revelaciones comunes (CVE).



Por término medio, solo hacen falta 14 días para que una vulnerabilidad esté disponible en la práctica después de que se divulgue públicamente. Esta vista ofrece un análisis de los plazos de explotación de las vulnerabilidades de día cero, junto con el número de sistemas vulnerables a la vulnerabilidad en cuestión y activos en Internet desde el momento de la primera divulgación pública.

Aunque los ataques de vulnerabilidad de día cero tienden a dirigirse inicialmente a un conjunto limitado de organizaciones, se adoptan con rapidez en el ecosistema más amplio de actores de amenaza. Esto pone en marcha una carrera para que los actores de amenaza exploten la vulnerabilidad lo más ampliamente posible antes de que sus objetivos potenciales instalen las revisiones.

Si bien observamos que muchos actores de estado nación desarrollan vulnerabilidades a partir de puntos débiles desconocidos, los actores de amenaza de estados nación con sede en China son muy competentes en el descubrimiento y desarrollo de vulnerabilidades de día cero. La normativa china sobre notificación de vulnerabilidades entró en vigor en septiembre de 2021, siendo la primera vez en el mundo que un gobierno exige la notificación de vulnerabilidades a una autoridad gubernamental para su revisión antes de que la vulnerabilidad se comparta con el propietario del producto o servicio. Esta nueva normativa podría permitir a elementos del gobierno chino acumular las vulnerabilidades notificadas para convertirlas en armas. El aumento del uso de días cero en el último año por parte de actores con sede en China probablemente refleja el primer año completo de requisitos de divulgación de vulnerabilidades para la comunidad de seguridad china y un paso importante en el uso de vulnerabilidades de día cero como prioridad de estado. Las vulnerabilidades que se describen a continuación las desarrollaron e implementaron por primera vez los actores de estado nación con sede en China en ataques, antes de ser descubiertas y difundidas entre otros actores del ecosistema de amenazas más amplio.

Explotación rápida de las vulnerabilidades

Continuación

Incluso las organizaciones que no son objetivo de ataques de estado nación tienen un período limitado para aplicar revisiones a las vulnerabilidades de día cero en los sistemas afectados antes de que el ecosistema de actores más amplio las explote.

Estos ejemplos de vulnerabilidades recién identificadas demuestran que las organizaciones disponen de un promedio de 60 días desde que se aplica la revisión a una vulnerabilidad y se pone en línea un código de prueba de concepto (POC), que a menudo recopilan otros actores para su reutilización. Del mismo modo, las organizaciones tienen un promedio de 120 días antes de que una vulnerabilidad esté disponible en las herramientas automatizadas de exploración y explotación de vulnerabilidades, como Metasploit, lo que a menudo da lugar a que la vulnerabilidad se utilice de forma masiva. Esto pone de manifiesto que incluso las organizaciones que no son un objetivo de los actores de amenaza de estado nación tienen un período limitado para aplicar revisiones a las vulnerabilidades de día cero en los sistemas afectados antes de que un ecosistema de actores más amplio exploten las vulnerabilidades.

CVE-2021-35211 SolarWinds Serv-U

En julio de 2021, SolarWinds publicó un aviso de seguridad para CVE-2021-35211, atribuyendo a Microsoft la notificación.[8] En ese momento, descubrimos al actor de amenaza alineado con el estado nación DEV-0322 explotando activamente la vulnerabilidad de SolarWinds Serv-U. Nuestro equipo de RiskIQ observó 12 646 direcciones IP que hospedaban versiones conectadas a Internet de los dispositivos afectados entre el 15 de junio y el 9 de julio.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

En septiembre de 2021, nuestros investigadores observaron a actores afiliados a China explotando Zoho ManageEngine en varias entidades con sede en Estados Unidos. La vulnerabilidad se reportó públicamente el 6 de septiembre como CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, que las organizaciones suelen utilizar para administrar el restablecimiento de contraseñas.[9] DEV-0322 explotó la vulnerabilidad a fines de septiembre, utilizándola como vector inicial para afianzarse en las redes y realizando acciones adicionales como el volcado de credenciales, la instalación de binarios personalizados y el lanzamiento de malware para mantener la persistencia. En el momento de la divulgación, RiskIQ observó 4011 casos de estos sistemas activos y en Internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

A fines de octubre de 2021, observamos que DEV-0322 aprovechaba una vulnerabilidad (CVE-2021-44077) en un segundo producto de Zoho ManageEngine, ServiceDesk Plus, un software de soporte informático con administración de activos. DEV-0322 utilizó esta vulnerabilidad para atacar y comprometer entidades de los sectores de la salud, la tecnología de la información, la educación superior y la manufactura crítica. El 2 de diciembre, la Oficina Federal de Investigación (FBI) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) emitieron un aviso conjunto en el que advertían al público sobre los actores de amenaza de estado nación que aprovechaban la vulnerabilidad. En el momento de la divulgación, RiskIQ observó 7,956 casos de estos sistemas activos y en Internet.

CVE-2021-42321 Microsoft Exchange

Se reveló una vulnerabilidad de día cero para una vulnerabilidad de Exchange CVE-2021-42321 durante la Tianfu Cup, una cumbre internacional de ciberseguridad y competición de hacking celebrada el 16 y 17 de octubre de 2021 en Chengdu, China. Los investigadores de seguridad de Microsoft observaron la vulnerabilidad de Exchange utilizada en la práctica el 21 de octubre, solo tres días después de que se revelara la vulnerabilidad. En el momento de la divulgación, RiskIQ observó 61 559 casos de estos sistemas activos y en Internet. Seguimos observando la actividad de explotación en noviembre de 2021.

CVE-2022-26134 Confluence

Un actor afiliado a China probablemente tenía el código de la vulnerabilidad de día cero para la vulnerabilidad Confluence (CVE-2022-26134) cuatro días antes de que esta se hiciera pública el 2 de junio, y es probable que la aprovechó contra una entidad con sede en Estados Unidos. En el momento de la divulgación, RiskIQ observó 53 621 casos de sistemas Confluence vulnerables en Internet.

Las vulnerabilidades se recopilan y explotan a gran escala y en plazos cada vez más cortos.

Información práctica

1. Dé prioridad a la aplicación de revisiones a las vulnerabilidades de día cero tan pronto como se publiquen; no espere al ciclo de administración de revisiones para implementarlas.
2. Documente y haga inventario de todos los activos de hardware y software de la empresa para determinar el riesgo y decidir con rapidez cuándo actuar sobre las revisiones.

Las tácticas cibernéticas de los actores de estado rusos amenazan a Ucrania y a otros países

Este año, los actores de estado rusos lanzaron operaciones cibernéticas para complementar la acción militar durante la invasión rusa de Ucrania, utilizando a menudo las mismas tácticas y técnicas implementadas contra objetivos fuera de Ucrania. Es fundamental que las organizaciones de todo el mundo tomen medidas para reforzar la ciberseguridad contra las amenazas digitales procedentes de los actores de amenaza alineados con Rusia.

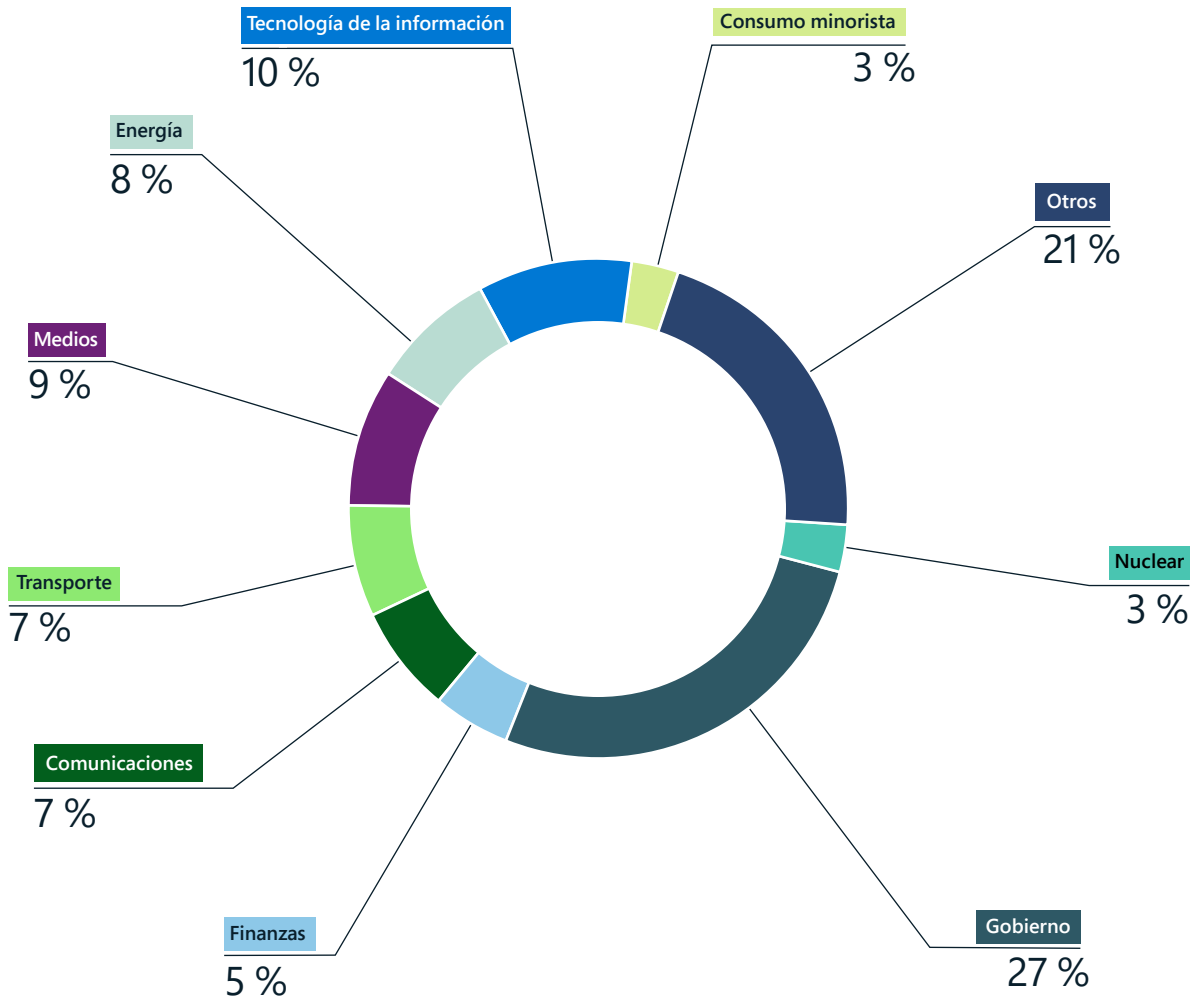
La situación sobre el terreno sigue fluctuando mientras persiste el conflicto militar, y Ucrania y sus aliados deben estar preparados para defenderse si los ciberoperadores de estado rusos aumentan la frecuencia o la intensidad de las intrusiones en función de los objetivos militares. Durante los primeros cuatro meses de la guerra, Microsoft observó que actores de amenaza asociados con el ejército ruso lanzaron múltiples oleadas de ciberataques destructivos contra casi 50 agencias y empresas ucranianas distintas e intrusiones centradas en el espionaje contra muchas otras. Excluyendo las operaciones contra clientes de servicios en línea, el 64 % de la actividad de las amenazas rusas contra objetivos conocidos se dirigió a organizaciones con sede en Ucrania entre fines de febrero y junio.

En cada operación, los actores de amenaza rusos emplearon muchas de las tácticas, técnicas y procedimientos (TTP) que vimos que se utilizaban antes de la invasión contra objetivos tanto dentro como fuera de Ucrania. Estos actores pretendían destruir datos y desequilibrar a los organismos gubernamentales ucranianos en el periodo inicial del conflicto. Desde entonces, han tratado de hacer fracasar el transporte de ayuda militar y humanitaria a Ucrania, interrumpir el acceso público a los servicios y medios de comunicación y robar información de valor económico o de inteligencia a largo plazo para Rusia.

El objetivo del transporte amenaza un área de importancia crítica para los ciudadanos ucranianos que intentan sobrevivir al conflicto. Según una encuesta patrocinada por UNICEF en mayo, los encuestados de las zonas urbanas afectadas por el conflicto estaban más preocupados por el transporte y el combustible, las interrupciones del suministro, la seguridad y el acceso limitado a los alimentos, los servicios médicos y los servicios financieros.[10] En junio, el Coordinador de crisis de la ONU para Ucrania dijo que al menos 15,7 millones de personas en Ucrania necesitaban ayuda humanitaria urgente, y que la cifra aumentaría a medida que la guerra continuara.[11]

Fuera de Ucrania, Microsoft detectó esfuerzos rusos de intrusión en la red contra 128 organizaciones en 42 países entre fines de febrero y junio. Estados Unidos era el objetivo número uno de Rusia. Polonia, por donde transita gran parte de la ayuda militar y humanitaria internacional a Ucrania, fue también un objetivo importante durante este periodo. Actores de amenaza afiliados al estado ruso persiguieron también en abril y mayo a organizaciones de los países bálticos y a redes informáticas de Dinamarca, Noruega, Finlandia y Suecia.

Sectores industriales más atacados en Ucrania desde la invasión



Las organizaciones gubernamentales federales, estatales y locales de Ucrania han seguido siendo objetivos prioritarios para el estado ruso y los grupos de amenaza afiliados al estado durante todo el conflicto. La atención a las organizaciones de los sectores del transporte, la energía, las finanzas y los medios de comunicación pone de manifiesto el riesgo que estas operaciones cibernéticas suponen para los servicios de los que dependen los ciudadanos ucranianos.

Las tácticas cibernéticas de los actores de estado rusos amenazan a Ucrania y a otros países

Continuación

Hemos visto un aumento de actividades similares dirigidas a los ministerios de asuntos exteriores de los países de la OTAN.

El año pasado, los grupos de amenazas estatales rusos siguieron interesados en comprometer las infraestructuras críticas tanto dentro como fuera de Ucrania. IRIDIUM implementó el programa malintencionado Industroyer2 en un intento fallido de dejar sin electricidad a millones de personas en Ucrania. Fuera de Ucrania, BROMINE llevó a cabo intrusiones contra organizaciones relacionadas con la manufactura y los sistemas de control industrial a principios de 2022.

El estado ruso y los actores afiliados al estado dirigieron operaciones cibernéticas contra Ucrania, sus aliados y otros objetivos de valor de inteligencia este año utilizando muchas de las siguientes TTP:

El phishing de objetivo definido con archivos adjuntos o vínculos malintencionados

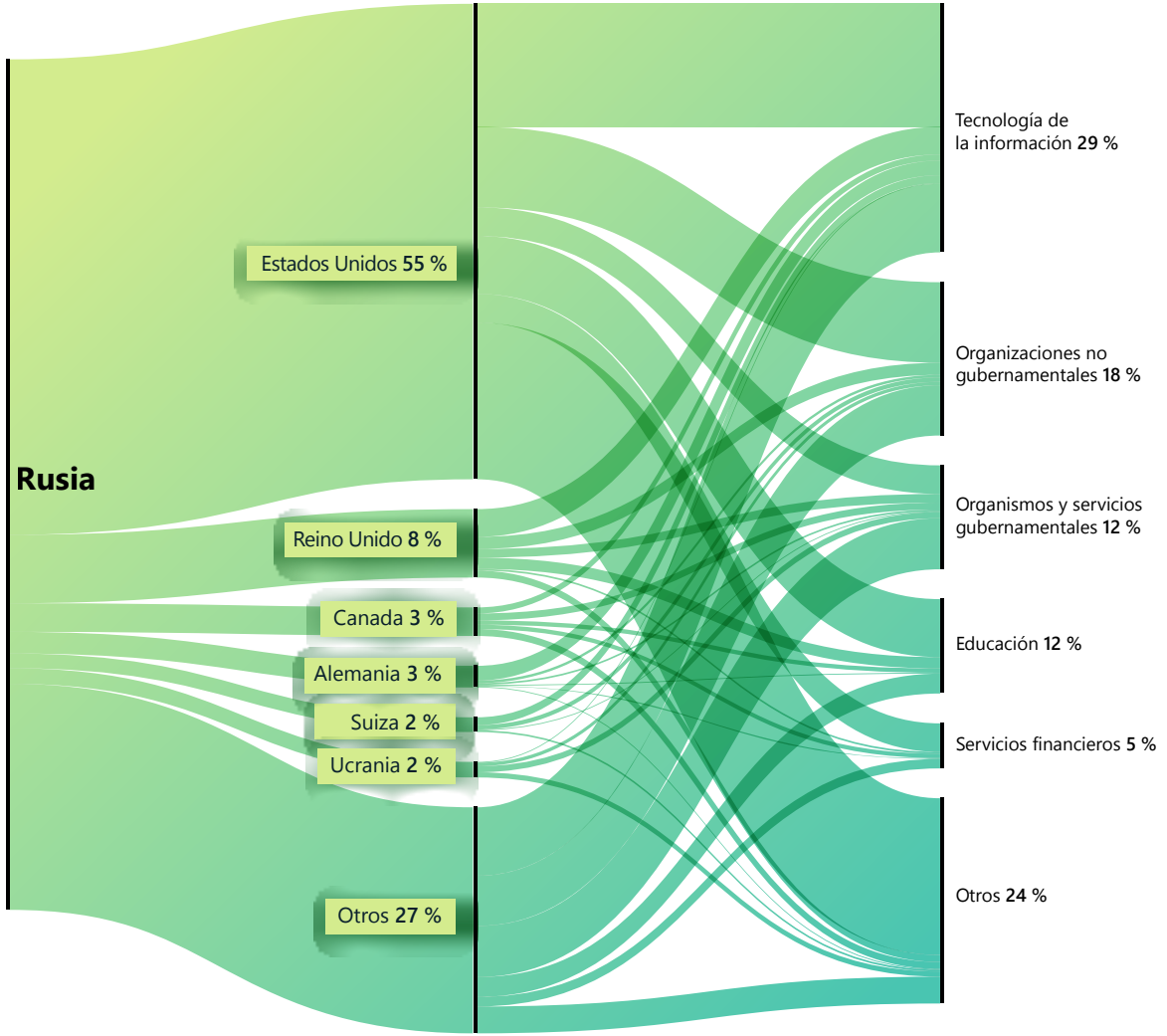
Los grupos de estado rusos y afiliados a Rusia, como ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM e IRIDIUM, utilizaron campañas de phishing para obtener acceso inicial a las cuentas y redes deseadas en organizaciones dentro y fuera de Ucrania. Muchas campañas utilizaron cuentas comprometidas o suplantadas en organizaciones objetivo o dentro de la misma industria y temas convincentes para atraer a las víctimas. NOBELIUM utilizó cuentas diplomáticas comprometidas para enviar correos de phishing disfrazados de comunicaciones diplomáticas a empleados de ministerios de asuntos exteriores de todo el mundo. STRONTIUM creó cuentas falsas basadas en nombres de titulares de cuentas disponibles públicamente en grupos de expertos de Estados Unidos y envió mensajes de phishing para acceder a las cuentas de esos grupos. SEABORGIUM hizo phishing utilizando señuelos relacionados con la información sobre el conflicto de Ucrania para obtener un acceso inicial a cuentas de grupos de expertos sobre asuntos internacionales en los países nórdicos.

Aprovechamiento de la cadena de suministro de los servicios de TI para influir en los clientes posteriores

A fines de 2021, actores de estado rusos comprometieron a los proveedores de servicios informáticos y utilizaron el acceso para facilitar la desfiguración de sitios web y la implementación del malware destructivo Whispergate de DEV-0586 en enero.[12] DEV-0586 también comprometió la red de una empresa de TI que construyó sistemas de administración de recursos para el Ministerio de Defensa de Ucrania y otras organizaciones en los sectores de las comunicaciones y el transporte, lo que indica que el grupo estaba explorando opciones de ataque a terceros también en esos sectores.

En todo el mundo, pero especialmente en Estados Unidos y Europa Occidental, NOBELIUM se dirigió a los proveedores de servicios de TI para obtener acceso a las redes gubernamentales y otras redes sensibles a lo largo de 2021-2022 (consulte el análisis de las vulnerabilidades de la cadena de suministro anteriormente en este capítulo).

Rusia: Principales países y sectores industriales



A pesar de que desde principios de 2022 se ha intensificado la atención a las organizaciones con sede en Ucrania, las empresas con sede en América del Norte y Europa Occidental siguen siendo los clientes de servicios en línea a los que más se dirigen los actores rusos. La campaña de NOBELIUM contra el sector de las tecnologías de la información lo convirtió en el sector más atacado el año pasado.

Las tácticas cibernéticas de los actores de estado rusos amenazan a Ucrania y a otros países

Continuación

Aprovechamiento de las aplicaciones orientadas al público para obtener un acceso inicial a las redes

Desde al menos fines de 2021, STRONTIUM trabajó en el desarrollo y perfeccionamiento de sus capacidades para explotar servicios de cara al público, como los servidores de Microsoft Exchange, para robar información. STRONTIUM explotó servidores Exchange sin revisiones para acceder a cuentas del gobierno ucraniano, así como a organizaciones militares y relacionadas con la industria de la defensa en Estados Unidos, Líbano, Perú y Rumanía, y a otras agencias gubernamentales con sede en Armenia, Bosnia, Kosovo y Malasia. DEV-0586, también afiliado al ejército ruso, explotó las vulnerabilidades del servidor Confluence para obtener acceso inicial a organizaciones del gobierno y del sector de las tecnologías de la información en Ucrania y otros países de Europa del Este.

El estado ruso y los actores de amenaza afiliados utilizan muchas de las mismas TTP para comprometer a las organizaciones de interés en tiempos de guerra y de paz.

Uso de cuentas y protocolos administrativos, y utilidades nativas para el descubrimiento de la red y el movimiento lateral

Después de obtener el acceso inicial a una red, Microsoft observó que los actores de estado rusos aprovechaban las cuentas legítimas y las utilidades de software utilizadas para realizar tareas básicas de mantenimiento con el fin de evadir la detección durante el mayor tiempo posible. Se basaban en identidades comprometidas con capacidades administrativas y protocolos, herramientas y métodos de administración válidos para moverse de forma lateral dentro de las redes sin atraer de inmediato la atención de los monitores automáticos y los defensores de la red.

La ciberhigiene básica y el empleo de herramientas de detección y respuesta de puntos de conexión pueden ayudar a mitigar el impacto negativo de este tipo de operaciones tanto en tiempos de paz como de guerra.

La imprevisibilidad del conflicto en curso exige que las organizaciones de todo el mundo tomen medidas para reforzar la ciberseguridad contra las amenazas digitales procedentes del estado ruso y de los actores de amenaza afiliados a Rusia.

Información práctica

1. Minimice el robo de credenciales y el abuso de cuentas protegiendo las identidades de sus usuarios mediante la implementación de herramientas de protección de identidades MFA y aplicando el acceso de mínimo privilegio para asegurar las cuentas y sistemas más sensibles y privilegiados.
2. Aplique las actualizaciones para asegurarse de que todos sus sistemas reciben el máximo nivel de protección lo antes posible y se mantienen al día.
3. Implemente soluciones antimalware, de detección de puntos de conexión y de protección de la identidad en toda su organización. Una combinación de soluciones de seguridad de defensa en profundidad, junto con personal formado y capacitado, puede empoderar a su organización para identificar, detectar y prevenir las intrusiones que afectan a su negocio.
4. Facilite las investigaciones y la recuperación en caso de que detecte o reciba una notificación de una amenaza para su entorno mediante una copia de seguridad de los sistemas críticos y activando el registro. Se recomienda encarecidamente establecer un plan de respuesta ante incidentes.

Vínculos a más información

- La defensa de Ucrania: Primeras lecciones de la guerra cibernética | Microsoft On the Issues
- La guerra híbrida en Ucrania | Microsoft On the Issues
- Actividad de las ciberamenazas en Ucrania: análisis y recursos | Centro de respuestas de seguridad de Microsoft (MSRC)
- Interrupción de los ciberataques dirigidos a Ucrania | Microsoft On the Issues
- Ataques de malware contra el gobierno de Ucrania | Microsoft On the Issues
- MagicWeb: El truco posterior al compromiso de NOBELIUM para autenticarse como cualquiera | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Equipo de detección y respuesta (DART), Equipo de investigación de Microsoft 365 Defender

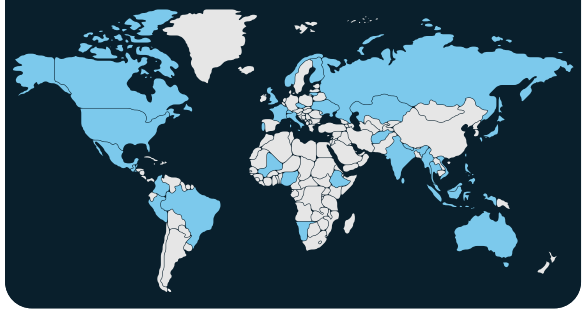
China amplía su objetivo global para obtener una ventaja competitiva

En el complejo clima geopolítico actual, el estado chino y los actores de amenaza afiliados al estado que llevan a cabo operaciones cibernéticas a menudo tienen como objetivo promover los objetivos estratégicos militares, económicos y de relaciones exteriores del país como parte del objetivo de China de conseguir una ventaja competitiva. En el último año, Microsoft ha observado una amplia actividad de amenazas chinas dirigidas a países de todo el mundo.

Desde mediados de 2021, China ha estado maniobrando para garantizar la estabilidad económica y financiera en medio del peor aumento del COVID-19 en dos años.[13] China continuó haciendo malabarismos con su posición en los acontecimientos geopolíticos, como la lucha por equilibrar su asociación "sin límites" con Rusia,[14] y mantener su posición en la escena mundial.[15] Además, la postura de China contra Estados Unidos y sus aliados en relación con Taiwán[16] y el mar de la China Meridional siguió tensando las relaciones exteriores con muchos países.[17]

El estado chino y los grupos de amenaza afiliados al estado aumentaron sus objetivos en las naciones más pequeñas de todo el mundo, centrándose en el sudeste asiático para obtener una ventaja competitiva en todos los frentes.

Países en el punto de mira del estado chino y de los grupos afines al estado

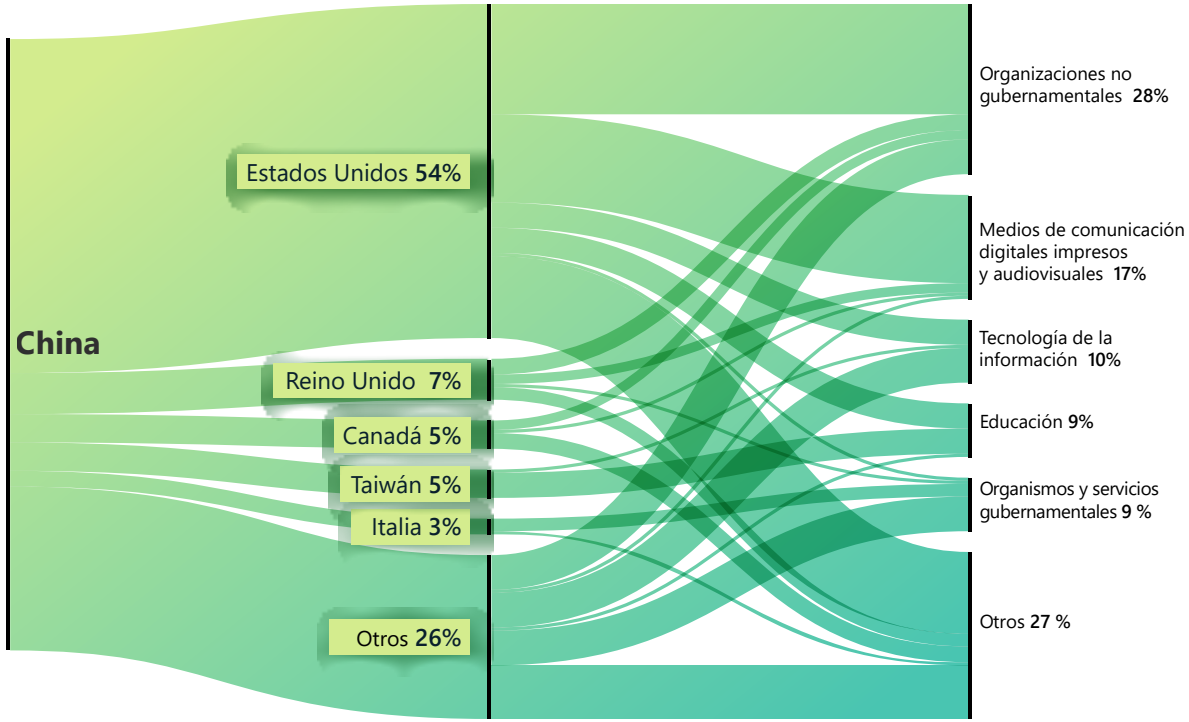


China también continuó ampliando su influencia económica a nivel mundial a través de la Iniciativa de la Franja y la Ruta (BRI, por sus siglas en inglés), previamente establecida, e intentó reactivar un marco de inversión global con la UE,[18] y negociando un nuevo acuerdo comercial regional con 15 países de Asia-Pacífico conocido como Asociación Económica Integral Regional.[19] Microsoft considera que China seguirá utilizando la recopilación cibernética como herramienta para ayudar a avanzar en sus objetivos estratégicos políticos, militares y económicos, debido a las operaciones cibernéticas observadas y a la amplitud de las entidades a las que se dirige.

Los objetivos cibernéticos pueden favorecer los intereses económicos y militares.

Microsoft observó el estado chino y los grupos de amenazas afiliados al estado han atacado de forma generalizada a países más pequeños de todo el mundo, lo que sugiere que China probablemente utiliza el ciberespionaje como un componente de su influencia económica y militar global.

China: Principales países y sectores industriales



Los grupos de expertos/ONG, los medios de comunicación, TI, el gobierno y los sectores de la educación se encuentran entre los sectores más atacados por los grupos de amenazas con base en China, probablemente para la recopilación persistente de información y el reconocimiento.

La gama de objetivos incluía, entre otros, países de África, el Caribe, Oriente Medio, Oceanía y el sur de Asia, con especial atención a los países del sudeste asiático y las islas del Pacífico.

En consonancia con la estrategia de la BRI de China, los grupos de amenazas con base en ese país se dirigieron a entidades de Afganistán, Kazajistán, Mauricio, Namibia y Trinidad y Tobago.[20] Por ejemplo, Trinidad y Tobago fue el primer país del Caribe en respaldar la estrategia BRI de China en 2018, y China lo considera un socio importante en la región. NICKEL ha tenido operaciones de red persistentes dirigidas a Trinidad y Tobago desde 2021. Por ejemplo, en marzo de 2022, NICKEL realizó actividades de reconocimiento dirigidas a un organismo gubernamental, probablemente con fines de recopilación de información.

China amplía su objetivo global para obtener una ventaja competitiva

Continuación

Mientras tanto, Microsoft observó que los grupos de amenazas chinos, tanto del estado como afiliados al estado, centraron sus operaciones de red contra entidades del sudeste asiático y se expandieron a los países de las islas del Pacífico, a medida que China cambiaba sus prioridades militares y económicas para hacer frente a los desafíos del renovado interés de Estados Unidos en la región. En enero de 2022, Microsoft observó que RADIUM tenía como objetivo una empresa energética y un organismo gubernamental asociado a la energía en Vietnam, y un organismo gubernamental indonesio. Las actividades de RADIUM probablemente estén en consonancia con los objetivos estratégicos de China en el Mar de China Meridional.[21] A fines de febrero y principios de marzo, GALLIUM comprometió más de 100 cuentas afiliadas a una importante organización intergubernamental (OIG) de la región del Sudeste Asiático. El momento en que GALLIUM apuntó a la organización intergubernamental en la región coincidió con el anuncio de una reunión programada entre Estados Unidos y los líderes regionales. Es probable que a los actores de GALLIUM se les haya encomendado la tarea de vigilar las comunicaciones y recopilar información antes del evento.

A medida que China ampliaba su influencia en los países de las islas del Pacífico, se sucedían las actividades de los grupos chinos de amenazas. En abril, China y las Islas Salomón firmaron un acuerdo de seguridad destinado a "promover la paz y la seguridad". El acuerdo permite potencialmente a China desplegar policías y militares armados en las Islas Salomón.[22] En mayo, China acogió la segunda reunión de ministros de Asuntos Exteriores de los países insulares del Pacífico (PIC) en Fiyi y propuso avanzar en una "asociación estratégica integral" para promover los intereses políticos, culturales, sociales, de seguridad y de cambio climático, así como para luchar contra la pandemia.[23] Por las mismas fechas, en mayo, Microsoft identificó el malware de GADOLINIUM en los sistemas del gobierno de las Islas Salomón. RADIUM también ejecutó código malintencionado en los sistemas de una empresa de telecomunicaciones de Papúa Nueva Guinea. Consideramos que estas actividades tenían probablemente fines de recopilación de información para apoyar la estrategia regional general de China.

Microsoft interrumpe las operaciones de NICKEL, pero el grupo de amenazas demuestra su persistencia.

En diciembre de 2021, la Unidad de delitos digitales (DCU) de Microsoft presentó alegatos ante el Tribunal de Distrito de los Estados Unidos para el Distrito Este de Virginia solicitando autoridad para incautar 42 dominios de comando y control (C2) controlados por NICKEL. Estos dominios C2 se utilizaron en operaciones contra gobiernos, entidades diplomáticas y ONG en toda América Central y del Sur, el Caribe, Europa y América del Norte desde septiembre de 2019.[24] A través de estas operaciones, NICKEL logró el acceso a largo plazo a varias entidades y filtró constantemente datos de algunas víctimas desde finales de 2019.

A medida que China siga estableciendo relaciones económicas bilaterales con más países, a menudo en acuerdos asociados a la BRI, la influencia mundial de China seguirá creciendo. Consideramos que el estado chino y los actores de amenaza afiliados al estado perseguirán objetivos en sus sectores gubernamental, diplomático y de las ONG para obtener nuevos conocimientos, probablemente en busca de espionaje económico o de objetivos tradicionales de recopilación de información. Desde la interrupción de Microsoft, NICKEL ha apuntado a varios organismos gubernamentales, probablemente tratando de recuperar el acceso perdido. Entre fines de marzo y mayo de 2022, NICKEL volvió a comprometer al menos a cinco organismos gubernamentales de todo el mundo. Esto sugiere que el grupo tenía puntos de entrada adicionales a esas entidades o recuperó el acceso a través de nuevos dominios C2. La persistencia de NICKEL en comprometer repetidamente a los mismos organismos gubernamentales a nivel mundial indica la importancia de la tarea a alto nivel.

China está siendo más asertiva con su postura en política exterior. Evaluamos que es probable que el espionaje económico y la recopilación de información a través de la informática continúen.

Información práctica

1. Impulse la ciberdefensa para mitigar las ciberamenazas de forma proactiva. La persistencia de los actores de amenaza chinos requiere que las organizaciones identifiquen, protejan, detecten y respondan a las posibles intrusiones de manera oportuna.
2. Los actores de amenaza abusan de las tareas programadas[25] como un método común de persistencia y evasión de la defensa, asegúrese de que su entorno emplea directrices de seguridad adicionales para protegerse contra esta técnica comúnmente utilizada.[26]
3. Seguimos observando el uso de las shells web como vector inicial en las redes dirigidas.[27] Las organizaciones deben endurecer sus sistemas contra los ataques de shells web que pueden proporcionar a los atacantes acceso para ejecutar comandos remotos.[28]

Vínculos a más información

- NICKEL se dirige a las organizaciones gubernamentales de América Latina y Europa | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital (DSU) de Microsoft
- Proteger a las personas de los recientes ciberataques | Microsoft On the Issues

Irán se torna cada vez más agresivo tras la transición de poder

Microsoft ha observado que los grupos de estado iraníes y los actores afiliados aumentan el ritmo y el alcance de los ciberataques contra Israel, amplían los ataques de ransomware más allá de los adversarios regionales a las víctimas de EE. UU. y la UE, y apuntan a la infraestructura crítica de EE. UU. de alto perfil para, al menos, preposicionarse para posibles ciberataques destructivos.

La creciente agresión cibernética de los actores de estado iraníes ha seguido a la transición de su poder presidencial. En el verano de 2021, el presidente de línea dura Ibrahim Raisi sustituyó al presidente moderado Hassan Rouhani. A diferencia de Raisi, que es un protegido del Líder Supremo y un estrecho aliado de los Cuerpos de la Guardia Revolucionaria Islámica (CGRI), la inclinación del expresidente Rouhani por la diplomacia a menudo le hizo entrar en conflicto con el Líder Supremo y los altos dirigentes de los CGRI.[29] Las opiniones belicistas del gobierno de Raisi parecen haber aumentado la disposición de los actores iraníes a emprender acciones más audaces contra Israel y Occidente, en particular contra Estados Unidos, a pesar de la reanudación del compromiso diplomático para reactivar el acuerdo nuclear con Irán.

Aumento del ritmo y el alcance de los ciberataques iraníes contra Israel

Pocas semanas después de que Raisi completara la formación de su equipo de política exterior,[30] los actores de estado iraníes reanudaron los ciberataques destructivos contra Israel a un ritmo más rápido que el año anterior. Estos ataques de ransomware y hack-and-leak se produjeron cada pocas semanas a partir de septiembre y en ellos participaron al menos tres actores afiliados a Irán, lo que sugiere que los ataques podrían haber formado parte de una campaña nacional de represalias contra Israel. En al menos un caso, Microsoft evaluó un ataque de ransomware contra una organización israelí a fines de 2021 que pretendía ocultar un ataque de eliminación de datos subyacente. El análisis de malware de Microsoft determinó que el ransomware entregado a la víctima estaba programado para ejecutar el malware limpiador tras el cifrado.

En 2022, los ciberataques iraníes se intensificaron en la selección de objetivos y la forma de los ataques. En febrero, DEV-0198 intentó llevar a cabo un ataque destructivo contra infraestructuras críticas israelíes. Microsoft también evalúa que un actor afiliado a Irán fue probablemente el responsable de un sofisticado ciberataque que activó las sirenas de los cohetes de emergencia en Israel en junio, probablemente utilizando un software que ajusta el audio a través de las redes IP.

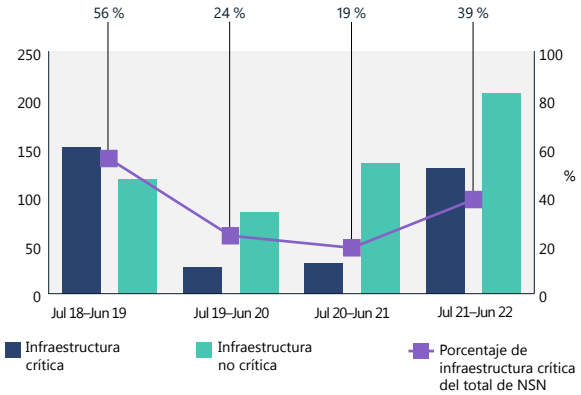
La amenaza iraní a las infraestructuras críticas de EE. UU. e Israel aumentó a lo largo del año

Actores de estado iraníes que, según Microsoft, están afiliados a la IRGC (PHOSPHORUS y DEV-0198) tuvieron como objetivo infraestructuras críticas estadounidenses e israelíes de alto nivel desde fines de 2021 hasta mediados de 2022. El objetivo probable era proporcionar a Teherán opciones para tomar represalias contra los mismos sectores que los altos cargos de los CGRI culparon a Estados Unidos e Israel de haber desbaratado en Irán.[31] Consideramos que esta actividad está vinculada a las declaraciones realizadas a fines de octubre de 2021 por el general de los CGRI Gholamreza Jalali, jefe de la Organización de Defensa Pasiva de Irán, quien se hizo eco de las acusaciones de otras figuras influyentes del régimen de que Estados Unidos e Israel llevaron a cabo ciberataques contra los puertos, ferrocarriles y estaciones de servicio de Irán.[32] Jalali formuló esta acusación por segunda vez en declaraciones preparadas durante un discurso escenificado en la oración del viernes en un podio con la imagen de un misil que golpea las palabras "EE. UU.", lo que sugiere que sus superiores tienen la misma opinión.[33]

PHOSPHORUS comenzó a escanear de forma generalizada las organizaciones estadounidenses en octubre de 2021 en busca de vulnerabilidades sin revisiones de Fortinet y ProxyShell. Una vez comprometidos, estos sistemas sin revisiones se utilizaron para ejecutar ataques de ransomware, en varios casos contra infraestructuras críticas de Estados Unidos y otras naciones occidentales. Se trata de los primeros casos confirmados de ataques de ransomware afiliados al estado iraní fuera de Oriente Medio. Tras el ciberataque contra las estaciones de servicio iraníes a fines de octubre, Microsoft observó un pico de ataques de ransomware iraní contra empresas estadounidenses, lo que sugiere una posible correlación.

Al mismo tiempo, PHOSPHORUS se dedicó a atacar, a menudo a través de phishing de objetivo definido, a empresas de infraestructuras críticas de Estados Unidos de alto nivel, como los principales puertos y aeropuertos de entrada, sistemas de tránsito, empresas de servicios públicos y compañías de petróleo y gas. Este objetivo, a menudo realizado a través de phishing de objetivo definido, duró hasta mediados de 2022. Los objetivos se alinean directamente con los sectores que Teherán ha culpado a Estados Unidos e Israel de atacar en Irán, y probablemente proporcionaron a Irán opciones de represalia. El compromiso de objetivos casi idénticos ofrecería una oportunidad para disuadir esos futuros ataques, al tiempo que se intenta evitar la escalada señalando la causa de los ataques sin admitir la culpabilidad.

Resurgimiento del objetivo de la infraestructura iraní



Los ataques iraníes a infraestructuras críticas aumentaron hasta los niveles más altos observados desde fines de 2018 hasta principios de 2019. Utilizamos la Directiva de Política Presidencial 21 de Estados Unidos (PPD-21) para determinar si una empresa se ajusta a los criterios de infraestructura crítica. (Jul 2021 – Jun 2022).

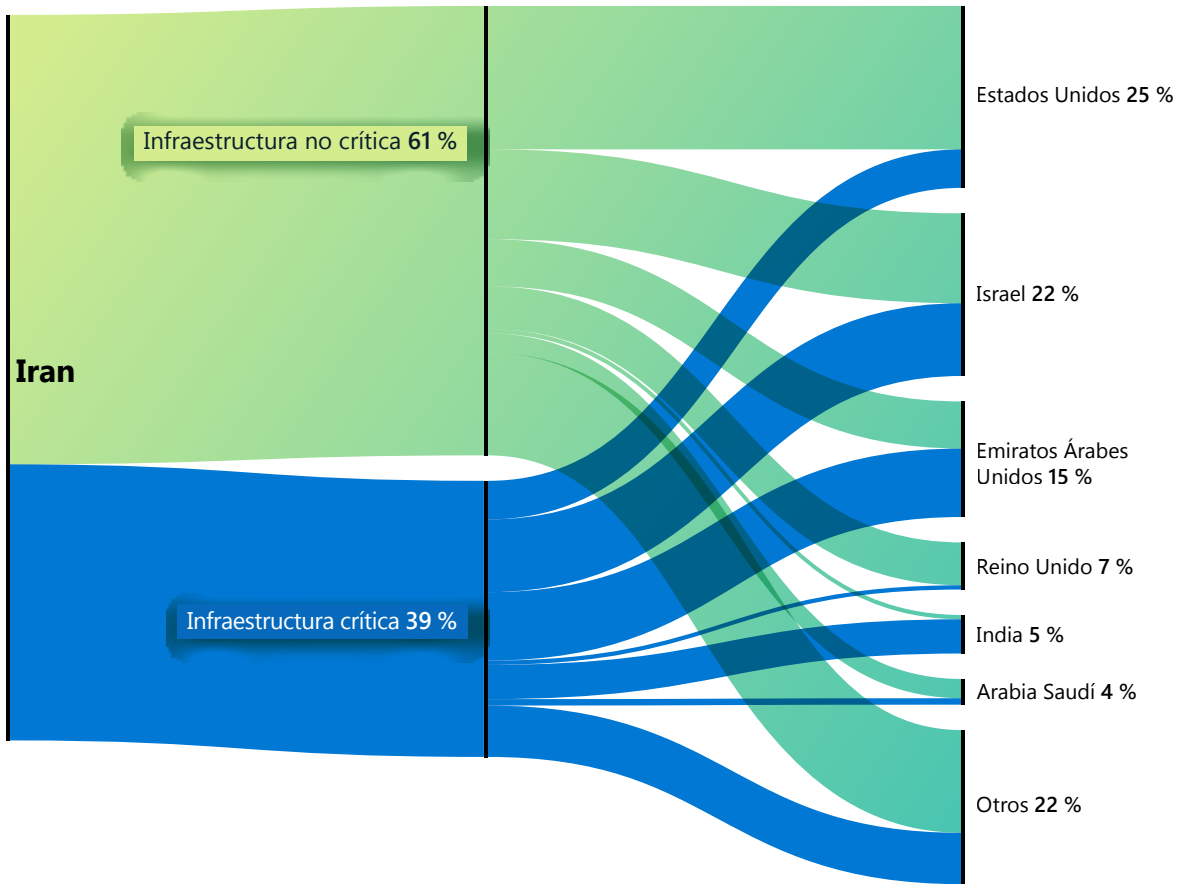
Irán se torna cada vez más agresivo tras la transición de poder

Continuación

En Israel, DEV-0198 se dirigió a los ferrocarriles israelíes, a las empresas de logística, a los proveedores de software de las empresas de logística y a las empresas de combustible, centrándose en las gasolineras. A principios de 2022, el grupo llevó a cabo un ataque perturbador contra la red de una importante empresa logística israelí, que obligó a la compañía a cerrar sus equipos y algunas de sus operaciones para contener el ataque. En otro caso, observamos que el grupo intentó acceder a la red de un importante proveedor de transporte israelí mediante credenciales robadas o reutilizadas. Mientras tanto, otro actor iraní, DEV-0343 (cuyo objetivo son las empresas de defensa, transporte marítimo e imágenes por satélite, sugiere vínculos con el CGRI) comprometió cuentas de entidades israelíes relacionadas con el transporte y los puertos a principios de 2021.

Es probable que los grupos de amenazas iraníes sigan siendo una amenaza para las empresas de transporte y energía estadounidenses e israelíes, sobre todo a medida que los esfuerzos diplomáticos para reactivar el acuerdo nuclear iraní disminuyan y Washington, Tel Aviv y Teherán busquen medios coercitivos alternativos para obtener concesiones.

Objetivos de las infraestructuras críticas iraníes por país



Los ataques iraníes a infraestructuras críticas se produjeron sobre todo contra organizaciones israelíes, emiratíes y estadounidenses.

Es probable que los actores iraníes sigan siendo una amenaza para las empresas de transporte y energía estadounidenses e israelíes en el próximo año.

Los grupos iraníes han ampliado los ataques de ransomware más allá de los adversarios regionales y están apuntando a objetivos de infraestructura crítica de alto perfil de Estados Unidos e Israel.

Información práctica

1. Mejore la ciberhigiene general de su organización habilitando soluciones sin contraseña, como MFA, e imponiendo su uso en toda la conectividad remota para mitigar cualquier credencial potencialmente comprometida.
2. Evalúe la autenticidad de todo el tráfico de correo electrónico entrante para asegurarse de que la dirección del remitente es legítima.
3. Aplique revisiones tempranas y frecuentes.[34]
4. Revise y audite cada una de sus relaciones con los proveedores de servicios para minimizar cualquier permiso innecesario entre su organización y los proveedores anteriores. Microsoft recomienda eliminar inmediatamente el acceso a cualquier relación de socios que parezca desconocida o que aún no haya sido auditada.[35]

Vínculos a más información

- Aumenta el número de objetivos iraníes en el sector de la TI | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital (DSU) de Microsoft
- DEV-0343 vinculado a Irán y dirigido a los sectores de defensa, SIG y marítimo | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital (DSU) de Microsoft

Un grupo con base en el Líbano y vinculado a Irán ataca a Israel

Microsoft supervisa las actividades de las ciberamenazas independientemente de la plataforma, la víctima objetivo o la región geográfica. Mantenemos la visibilidad y la caza activa de amenazas en todo el mundo para escribir mejores detecciones para nuestros clientes.

Aunque las amenazas de Rusia, China, Irán y Corea del Norte representan la mayor parte de nuestra actividad observada de actores estatales, también rastreamos y comunicamos las amenazas de los países miembros de la OTAN y las naciones democráticas. El año pasado, presentamos la actividad de un actor radicado en Turquía (SILICON) y de un actor radicado en Vietnam (BISMUTH). Este año, ampliamos los detalles de un grupo con sede en el Líbano que ya habíamos revelado públicamente.[36]

Microsoft descubrió un grupo con sede en el Líbano que no estaba documentado y que, según nuestra opinión, operaba en coordinación con actores afiliados al Ministerio de Inteligencia y Seguridad de Irán (MOIS). Esta colaboración o dirección de Teherán estaría en consonancia con las revelaciones realizadas desde fines de 2020 de que el gobierno de Irán está utilizando a terceros para llevar a cabo operaciones cibernéticas, lo que probablemente refuerce la negación plausible de Irán.

En la actividad observada, POLONIUM apuntó o comprometió a dos docenas de organizaciones con sede en Israel y a una organización intergubernamental con operaciones en el Líbano entre febrero y mayo de 2022, antes de que Microsoft interrumpiera y revelara públicamente su actividad. Casi la mitad de las organizaciones israelíes formaban parte de la industria de defensa de Israel o tenían vínculos con empresas de defensa israelíes, lo que indica que el grupo tiene un conjunto de intereses similares a los de Irán a la hora de recopilar información sobre Israel o contrarrestarlo directamente.[37]

Los vínculos evaluados por POLONIUM con los grupos MOIS se basan en los solapamientos observados entre las víctimas y la coincidencia de herramientas y técnicas.

- Superposición de víctimas: Un grupo estatal iraní vinculado al MOIS de Irán, que Microsoft rastrea como MERCURY, comprometió previamente a múltiples víctimas de POLONIUM, lo que indica una convergencia de los requisitos de la misión o un posible "traspaso" de víctimas entre grupos.
- Herramientas y técnicas comunes: Al igual que POLONIUM, MSTIC observó que DEV-0588 (también conocido como CopyKittens) suele utilizar AirVPN para sus operaciones y DEV-0133 (también conocido como Lyceum[38]) utiliza OneDrive para C2 y la filtración. Al igual que los actores de estado iraníes, POLONIUM utilizó un proveedor de servicios en la nube para comprometer una empresa de aviación y un bufete de abogados israelíes.[39]

POLONIUM implementó una serie de implantes personalizados que utilizaban servicios en la nube para el C2 y la filtración de datos, especialmente OneDrive y DropBox. POLONIUM a menudo creaba aplicaciones únicas de OneDrive para los objetivos, con el fin de evadir la detección.

A partir de junio de 2022, Microsoft suspendió más de 20 aplicaciones de OneDrive creadas por POLONIUM, notificó a las organizaciones afectadas e implementó una serie de actualizaciones de inteligencia de seguridad para poner en cuarentena las herramientas desarrolladas por POLONIUM.

Microsoft detectó y deshabilitó con éxito el abuso de OneDrive por parte de POLONIUM como C2.

Información práctica

1. Actualice las herramientas antivirus[40] y asegúrese de que la protección de la nube[41] esté activada para detectar los indicadores relacionados.
2. Para los clientes con relaciones con proveedores de servicios, asegúrese de revisar y auditar todas las relaciones con los socios para minimizar los permisos innecesarios entre su organización y los proveedores anteriores.[42] Elimine inmediatamente el acceso a cualquier relación de socios que parezca desconocida o que no haya sido auditada.

Vínculos a más información

- Exponer la actividad y la infraestructura de POLONIUM dirigida a organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital (DSU) de Microsoft
- MERCURY aprovecha las vulnerabilidades de Log4j 2 en sistemas sin revisiones para atacar a organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Equipo de investigación de Microsoft 365 Defender Team, Inteligencia contra amenazas de Microsoft Defender

Capacidades cibernéticas de Corea del Norte empleadas para lograr los tres objetivos principales del régimen

Las prioridades cibernéticas de Corea del Norte durante el año pasado reflejaron las prioridades globales declaradas por el gobierno. Kim Jong Un hizo hincapié en las tres prioridades de construir la capacidad de defensa, reforzar la difícil economía del país y garantizar la estabilidad interna en varios discursos clave.[43] Las acciones llevadas a cabo por los actores estatales norcoreanos demuestran claramente que la cibernética está siendo utilizada para lograr estos tres objetivos.

Los agentes estatales norcoreanos utilizaron diversas tácticas para intentar penetrar en las empresas aeroespaciales de todo el mundo.

Los grupos de amenazas de estado norcoreanos, principalmente CERIUM y ZINC, utilizaron diversas tácticas para intentar penetrar en las redes de las empresas de defensa y aeroespaciales de todo el mundo. Cuando Corea del Norte se embarcó en su período más agresivo de pruebas de misiles en la primera mitad de 2022, utilizó el ciberespionaje para ayudar a los investigadores norcoreanos a obtener una ventaja en el desarrollo de sistemas de defensa autóctonos y contramedidas para los avances de sus adversarios.

Observamos que COPERNICIUM se dirigía a una serie de empresas relacionadas con la criptomoneda en todo el mundo, a menudo con éxito, para ayudar a la difícil economía de Corea del Norte. Aunque no podemos confirmar si el grupo fue capaz de filtrar dinero tras el compromiso, observamos que COPERNICIUM infectó docenas de máquinas enviando documentos malintencionados que se hacían pasar por propuestas de otras empresas de criptomonedas.

Por último, un grupo al que Microsoft rastrea como DEV-0215 trabajó para mantener la estabilidad y la lealtad en Corea del Norte dirigiéndose a las organizaciones de noticias que informan sobre asuntos norcoreanos. Estos medios tienen fuentes tanto en Corea del Norte como en las comunidades de desertores, que Pyongyang considera una amenaza existencial. Además, el grupo se esforzó por acceder a las redes de grupos cristianos de habla coreana, que suelen ser francos contra Corea del Norte y trabajan activamente con los desertores norcoreanos.

Objetivo de las empresas de defensa y aeroespaciales

Los actores de estado norcoreanos, liderados por CERIUM y ZINC, se esforzaron mucho en desarrollar tácticas destinadas a penetrar en las empresas de defensa y aeroespaciales. CERIUM sondeó repetidamente las redes privadas virtuales (VPN) de Corea del Sur descargando clientes y buscando puntos débiles. También descargó aplicaciones comunes utilizadas por clientes militares y gubernamentales surcoreanos, probablemente en busca de vulnerabilidades. El grupo seguía de cerca la actualidad y redactaba nuevos documentos de señuelo que utilizaban temas de gran relevancia como cebo para animar a los objetivos a hacer clic en sus ejecutables y vínculos de malware.

Tanto ZINC como CERIUM utilizaron las redes sociales y la ingeniería social en sus campañas. ZINC era especialmente hábil en la creación de perfiles falsos en LinkedIn y otras redes sociales profesionales, donde sus operadores se hacían pasar por reclutadores de importantes empresas de defensa y aeroespaciales. Utilizando estos perfiles, enviaban vínculos o archivos adjuntos malintencionados a las víctimas potenciales mediante mensajes directos en las redes sociales o por correo electrónico.

Además de los empleados de las empresas, CERIUM también se dirigió ampliamente a los miembros del ejército surcoreano, mostrando especial interés tanto en las academias militares de Corea del Sur como en los militares que trabajan en el ámbito académico.

Apuntar a la criptomoneda para equilibrar las pérdidas

Desde que se impusieron las sanciones de la ONU en 2016, la economía de Corea del Norte ha seguido contrayéndose, agravada por catástrofes naturales como las inundaciones[44] y la sequía,[45] así como por un cierre casi total de las fronteras a las importaciones desde el inicio de la pandemia de COVID-19 a principios de 2020.[46] Aunque Corea del Norte abrió brevemente sus fronteras para el comercio con China a principios de 2022, pronto volvieron a cerrarse.[47] A mediados de mayo, Corea del Norte informó de su primer caso local de COVID-19.[48] Desde entonces, ha aplicado una estrategia de cierre masivo al estilo de China para combatir el virus, que ha afectado negativamente a la ya frágil economía de Corea del Norte.

El grupo de estado norcoreano COPERNICIUM trató de compensar parte de los ingresos perdidos robando dinero, típicamente en forma de criptomonedas, de cualquier empresa en cuyas redes pudiera penetrar. Vimos docenas de máquinas comprometidas pertenecientes a empresas relacionadas con la criptomoneda en Estados Unidos, Canadá, Europa y toda Asia. COPERNICIUM llegó a comprometer máquinas pertenecientes a empresas relacionadas con la criptomoneda dentro del aliado más fuerte de Corea del Norte, China, tanto en el continente como en Hong Kong. El grupo se apoyó en gran medida en las redes sociales para sus primeros reconocimientos y aproximaciones a los objetivos. Los actores construirían perfiles fingiendo ser desarrolladores o altos cargos de empresas relacionadas con la criptomoneda. A continuación, establecían relaciones con las personas del sector, enviando vínculos o archivos malintencionados una vez que habían establecido una relación.

Capacidades cibernéticas de Corea del Norte empleadas para lograr los tres objetivos principales del régimen

Continuación

Un grupo relacionado con PLUTONIUM desarrolla e implementa ransomware

Un grupo de actores con origen en Corea del Norte que Microsoft rastrea como DEV-0530 comenzó a desarrollar y utilizar ransomware en ataques en junio de 2021. Este grupo, que se autodenomina H0lyGh0st, utilizó una carga útil de ransomware con el mismo nombre para sus campañas y logró comprometer a pequeñas empresas en varios países ya en septiembre de 2021.

Microsoft evaluó que DEV-0530 tenía conexiones con otro grupo con sede en Corea del Norte rastreado como PLUTONIUM (también conocido como DarkSeoul o Andariel). Aunque el uso del ransomware H0lyGh0st en las campañas es exclusivo de DEV-0530, MSTIC observó comunicaciones entre ambos grupos, así como que DEV-0530 utilizaba herramientas creadas exclusivamente por PLUTONIUM.

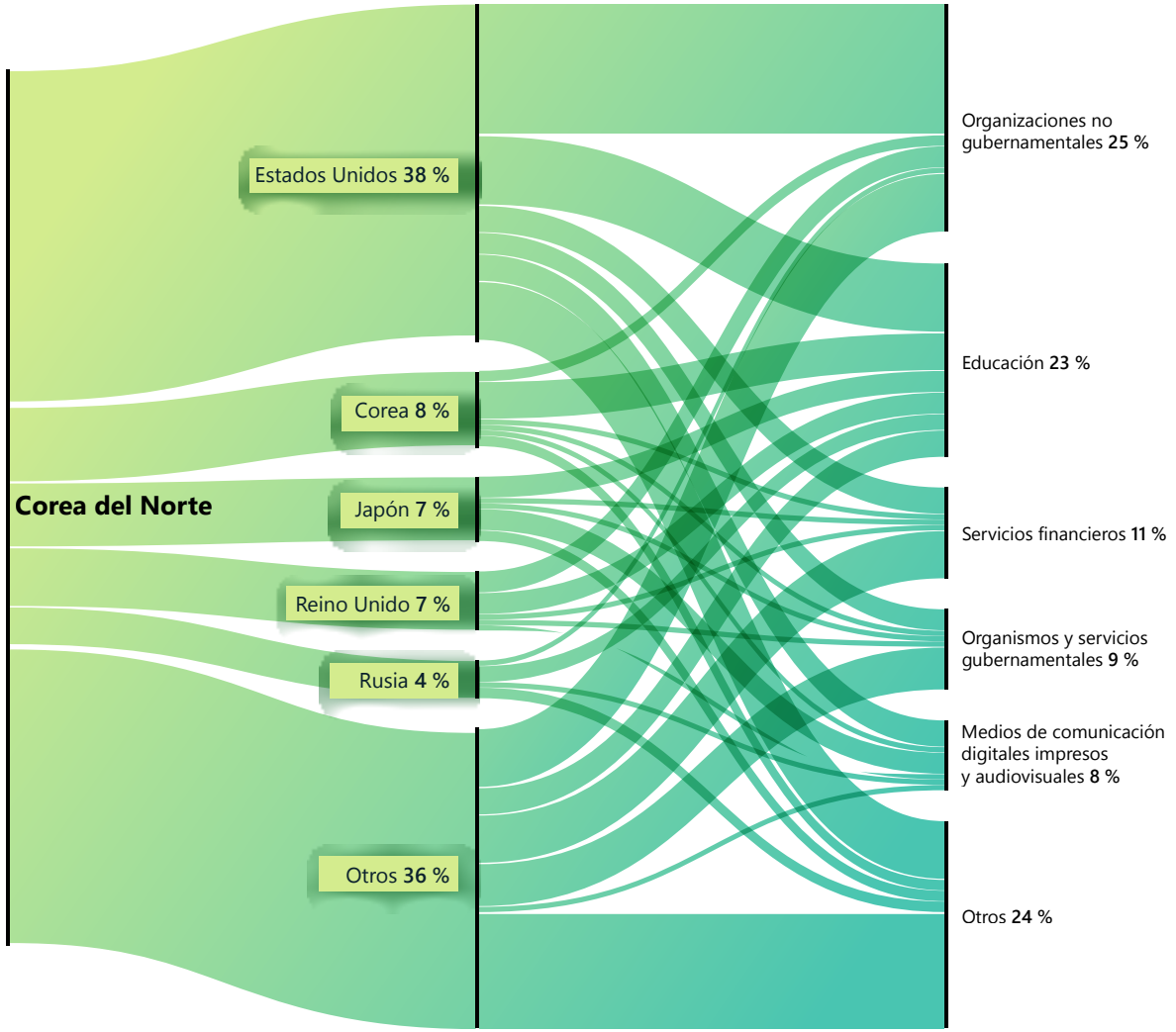
No es seguro que la actividad de DEV-0530 estuviera patrocinada por el gobierno. Aunque los ataques de ransomware podrían haber sido ordenados por el gobierno por la misma razón que patrocina el robo a las empresas de criptomonedas, también es posible que los actores detrás de DEV-0530 estuvieran actuando de forma independiente para ganar dinero para sí mismos. Si se tratara de hackers norcoreanos que operan de forma independiente, eso explicaría por qué la actividad no fue generalizada en comparación con las operaciones de robo patrocinadas por el gobierno contra las empresas de criptomonedas.

Ataque a los medios de comunicación norcoreanos, a los desertores, a los grupos religiosos y a las organizaciones de ayuda.

En el último año, el líder supremo Kim Jong Un se centró públicamente más en la seguridad interna y la lealtad que en los misiles y las armas nucleares. Como reflejo de esta preocupación por los problemas internos, al menos dos grupos de estado norcoreanos se centraron en aspectos que el régimen consideraría como amenazas internas.

El primero fue un grupo que Microsoft rastrea como DEV-0215, cuyo objetivo son las organizaciones de medios de comunicación que siguen de cerca las noticias de Corea del Norte. Una de las razones más probables de esta orientación es que estos medios obtienen sus noticias de desertores norcoreanos, de ciudadanos chinos que trabajan en estrecha colaboración con Corea del Norte e incluso de algunos ciudadanos norcoreanos radicados en el país, que utilizan diversos métodos para comunicarse con el mundo exterior. El gobierno norcoreano ve a estos grupos como una amenaza existencial para su supervivencia, especialmente a los ciudadanos dentro de Corea del Norte que serían vistos como traidores y espías. Es probable que DEV-0215 tratara de identificar las fuentes de estos medios para poder neutralizar las posibles filtraciones de información.

Corea del Norte: Principales países y sectores industriales



Corea del Norte considera a Estados Unidos, Corea del Sur y Japón como sus principales enemigos. Aunque Rusia es un aliado desde hace mucho tiempo, los actores de amenaza norcoreana tienen como objetivo los grupos de expertos, los académicos y los funcionarios diplomáticos rusos para obtener información sobre la visión rusa de los asuntos mundiales.

Capacidades cibernéticas de Corea del Norte empleadas para lograr los tres objetivos principales del régimen

Continuación

Microsoft también vio pruebas de que DEV-0215 se dirigía a las comunidades cristianas de habla coreana. Las iglesias cristianas evangélicas coreanas tienden a ser críticas tanto con Corea del Norte como con los gobiernos surcoreanos que favorecen el compromiso con Corea del Norte. Es probable que estas iglesias lleven a cabo actividades de divulgación entre los desertores, y algunas realizan labores humanitarias con Corea del Norte. Corea del Norte los considera una amenaza porque, aunque el flujo de desertores procedentes de Corea del Norte casi se agotó durante la pandemia,[49] estos grupos cristianos suelen desempeñar un papel fundamental a la hora de ayudar a los desertores a escapar. DEV-0215 ha generado documentos falsos sobre conferencias cristianas para hablantes de coreano como señuelo para atacar al grupo y descubrir quiénes están ayudando a organizar las deserciones.

Por último, el grupo de estado OSMIUM mostró un interés constante en las organizaciones de ayuda internacional a lo largo del año, incluidas las organizaciones que han ayudado a Corea del Norte en el pasado. Aunque Corea del Norte ha rechazado generalmente las ofertas de ayuda del exterior, en especial desde el estallido de COVID-19,[50] es posible que esté considerando aceptar las ofertas de ayuda, pero que desconfíe de las ramificaciones de seguridad que supondría permitir la entrada de trabajadores extranjeros en el país. Es posible que Corea del Norte esté penetrando en las redes de las organizaciones de ayuda de todo el mundo para determinar si permite la entrada de dicha ayuda en su propio país.

Información práctica

1. Los actores de estado norcoreanos son hábiles, implacables y creativos, pero las organizaciones pueden defenderse de ellos.
2. La mayoría de los ataques exitosos pueden detenerse con una higiene cibernética básica, como la autenticación de dos factores o no abrir archivos adjuntos de personas desconocidas en un entorno virtual.

Vínculos a más información

- Un actor de la amenaza norcoreana apunta a las pequeñas y medianas empresas con el ransomware H0lyGh0st | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital (DSU) de Microsoft

Entre los expertos en Corea del Norte se debate desde hace tiempo si el gobierno norcoreano va en serio con sus declaraciones públicas o si se trata de una postura efectista.La alineación de los ciberataques con las prioridades anunciadas por Corea del Norte valida la creencia de que Corea del Norte habla en serio cuando habla públicamente de sus objetivos.

Los cibermercenarios amenazan la estabilidad del ciberespacio

Existe una industria creciente de empresas privadas que desarrollan y venden herramientas, técnicas y servicios que permiten a sus clientes, a menudo gobiernos, entrar en redes, equipos, teléfonos y dispositivos conectados a Internet. Estas entidades, que son un activo para los actores de estado nación, suelen poner en peligro a disidentes, defensores de los derechos humanos, periodistas, defensores de la sociedad civil y otros ciudadanos particulares. Nos referimos a ellos como cibermercenarios o actores ofensivos del sector privado.

Un mundo en el que las empresas del sector privado crean y venden ciberarmas es más peligroso para los consumidores, las empresas de todos los tamaños y los gobiernos. Estas herramientas ofensivas pueden utilizarse de forma incompatible con las normas y los valores del buen gobierno y la democracia. Microsoft cree que la protección de los derechos humanos es una obligación fundamental, que nos tomamos en serio al reducir la "vigilancia como servicio" en todo el mundo.

Microsoft ha evaluado a ciertos actores estatales de regímenes democráticos y autoritarios que subcontratan el desarrollo o el uso de la tecnología de "vigilancia como servicio". Así evitan la rendición de cuentas y la supervisión, además de adquirir capacidades que serían difíciles de desarrollar de forma nativa.

> Estas armas cibernéticas ofrecen a los estados nación capacidades de vigilancia que no habrían podido desarrollar por sí solos.

El mercado en el que operan los cibermercenarios es opaco. Sin embargo, seguimos observando que estos grupos utilizan vulnerabilidades de día cero e incluso vulnerabilidades de clic cero que no requieren ninguna interacción de la víctima, permitiendo la vigilancia como servicio.

Microsoft anunció recientemente un actor ofensivo del sector privado europeo al que llamamos KNOTWEED, una PSOA con sede en Austria llamada DSIRF. Múltiples noticias han vinculado a la empresa con el desarrollo e intento de venta de un conjunto de herramientas de malware llamado Subzero.[51] Entre las víctimas se encuentran bufetes de abogados, bancos y consultorías estratégicas de países como Austria, Reino Unido y Panamá.[52]

Dado que estas capacidades de vigilancia ofensiva ya no son capacidades altamente clasificadas creadas por las agencias de defensa e inteligencia, sino productos comerciales que ahora se ofrecen a empresas y particulares, cualquier régimen regulador de las ciberarmas debe ir más allá del control de las exportaciones. El impacto de estas ciberarmas puede ser devastador.

Cuando un cibermercenario explota una vulnerabilidad en un producto o servicio, pone en riesgo todo el ecosistema informático. Cuando las vulnerabilidades se identifican públicamente, las empresas se encuentran en una carrera contra el tiempo para liberar las protecciones antes de que se produzcan amplios ataques (consulte nuestro anterior análisis de las vulnerabilidades). Se trata de un ciclo peligroso y difícil tanto para los proveedores de software (que deben desarrollar revisiones de forma expeditiva) como para los consumidores de productos (que deben aplicar las revisiones inmediatamente).

Como miembro fundador del Acuerdo Tecnológico de Ciberseguridad[53] (una alianza líder que reúne a más de 150 empresas tecnológicas) Microsoft se ha comprometido a no realizar operaciones ofensivas en línea. Mantenemos ese compromiso y nuestras responsabilidades en materia de derechos humanos en este ámbito. Hemos llevado a cabo interrupciones técnicas y desafíos legales para poner de manifiesto las repercusiones negativas causadas por los servicios prestados por los cibermercenarios y seguiremos protegiendo a nuestros clientes cuando veamos abusos.

> Los cibermercenarios crean y ofrecen capacidades de "vigilancia como servicio" tecnológicamente sofisticadas y de amplia disposición, incluyendo malware avanzado, y una serie de técnicas.

Conocimientos prácticos para los gobiernos

1. Implemente requisitos de transparencia y supervisión para la vigilancia como servicio, especialmente en la contratación, incluyendo la prohibición de estos actores ofensivos, como ha hecho EE. UU. con la lista de empresas del Departamento de Comercio en la Lista de Entidades.
2. Establezca restricciones posteriores al empleo para los antiguos empleados de este sector.
3. Intente aplicar las obligaciones de "conocer al cliente" y animar a las empresas a mantener sus compromisos en materia de derechos humanos.

Vínculos a más información

- Desenredar a KNOTWEED: actor ofensivo europeo del sector privado que utiliza vulnerabilidades de día cero | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Centro de respuestas de seguridad de Microsoft (MSRC), RiskIQ (Inteligencia contra amenazas de Microsoft Defender)
- Continuación de la lucha contra las ciberarmas del sector privado | Microsoft On the Issues

Operacionalización de las normas de ciberseguridad para la paz y la seguridad en el ciberespacio

Necesitamos urgentemente un marco global coherente que dé prioridad a los derechos humanos y proteja a las personas del comportamiento imprudente del estado en línea. En ningún lugar se demuestra esto más claramente que en la actual guerra en Ucrania. Además de un esfuerzo estratégico global, los gobiernos pueden actuar ahora para tener un impacto positivo inmediato.

Hace cinco años, Microsoft pidió una "Convención de Ginebra Digital" para avanzar en las responsabilidades y obligaciones de todos los sectores para defender la paz y la seguridad en línea. El ciberespacio se estaba convirtiendo en un ámbito distinto y volátil de conflicto y competencia entre Estados, con ataques cada vez más frecuentes, incluso en tiempos de paz.

Hoy en día, sigue existiendo una clara necesidad de dicho marco, como demuestran los ciberataques rusos contra Ucrania en el marco de la invasión rusa. Esta guerra ha creado un nuevo frente que es drásticamente distinto de cualquiera que hayamos conocido antes.

Para dar estabilidad al ciberespacio será necesario reforzar y replantear las instituciones de gobernanza mundial para que se adapten a su finalidad. El ciberespacio es fundamentalmente distinto de otros dominios: no tiene fronteras, es sintético y la industria privada lo mantiene en gran medida.

Esto significa pedir a la industria tecnológica que asuma una mayor responsabilidad tanto en la seguridad de los productos y servicios como en el ecosistema digital en general. Aunque se han producido notables avances en todos los frentes, los desafíos han aumentado de forma espectacular.

Debemos redoblar los esfuerzos colectivos para defender la seguridad del ciberespacio. No podemos dar por sentados los derechos y las libertades que hemos llegado a esperar en Internet. Mientras nos esforzamos por hacer frente a los desafíos, los actores malintencionados están planificando cómo y dónde atacar a continuación utilizando la IA, aprovechando la desinformación, y encontrando maneras de socavar el metaverso en ciernes. Los defensores de los derechos humanos, la industria tecnológica y los gobiernos que respetan los derechos deben trabajar juntos hacia una visión afirmativa de un mundo seguro en línea. El camino es largo, pero hay cosas que los gobiernos pueden hacer ahora para mejorar inmediatamente el ecosistema de la ciberseguridad:

- Citar normas, leyes y consecuencias en las atribuciones. Una mejora importante en los últimos cinco años ha sido la rapidez y la coordinación de las atribuciones gubernamentales de los ciberataques. Más allá de nombrar y avergonzar, estas declaraciones deben destacar qué leyes o normas internacionales se han infringido y qué tipo de consecuencias se impondrán para ayudar a reforzar el reconocimiento de las expectativas internacionales.
- Aclarar la interpretación del derecho internacional en línea. Aunque los gobiernos están de acuerdo en que el derecho internacional se aplica en línea, sigue habiendo dudas sobre cómo se aplica en casos concretos. Esto es especialmente pertinente tras la invasión de Ucrania. Los gobiernos pueden contribuir en gran medida a fijar las expectativas, evitar los malentendidos y fomentar la confianza si declaran cómo entienden sus obligaciones en virtud del derecho internacional.
- Consultar con otras partes interesadas. Mientras los foros internacionales siguen descubriendo las mejores formas de facilitar una sólida inclusión de las diversas partes interesadas, los gobiernos pueden apoyar un diálogo informado consultando a las comunidades de las múltiples partes interesadas, en especial a la industria tecnológica, para garantizar que el diálogo se beneficie de quienes tienen una experiencia indispensable.
- Formar un organismo permanente para apoyar el comportamiento responsable de los estados en el ciberespacio. La labor de los foros diplomáticos internacionales para promover el comportamiento responsable de los estados en línea nunca ha sido tan importante. Es evidente la necesidad de un mecanismo permanente de la ONU que se ocupe del ciberespacio como ámbito de conflicto.
- Definir nuevas normas para la evolución de las amenazas. Las amenazas del ciberespacio evolucionan constantemente junto con las innovaciones tecnológicas. Aunque las normas internacionales deberían ser neutrales desde el punto de vista tecnológico, tendrán que actualizarse y atenuarse en función de los cambios en el panorama de las amenazas y en el uso que hacemos de la tecnología. Incluso hoy en día, vemos cómo se abusa de las brechas del marco internacional existente. Los estados tienen que comprometerse a proteger expresamente los procesos básicos que sustentan el ecosistema digital y que en la actualidad no están protegidos, como el proceso de actualización del software. Además, hay zonas específicas que merecen una protección adicional. Por ejemplo, como hemos aprendido en medio de la pandemia, las normas para proteger la asistencia de salud son esenciales.

El volumen y la sofisticación de los actores y ataques de los estados nación están aumentando, creando una situación insostenible.

Hay cosas que los gobiernos pueden hacer ahora para mejorar inmediatamente el ecosistema de la ciberseguridad, incluida la aplicación de normas y reglas acordadas para el comportamiento de los estados en el ciberespacio y la colaboración con la comunidad más amplia de varias partes interesadas para abordar las nuevas deficiencias.

Las instituciones multilaterales deben replantearse para hacer frente al acuciante desafío de los ciberataques de los estados nación.

Vínculos a más información

- Un momento de reflexión: la necesidad de una respuesta fuerte y global en materia de ciberseguridad | Microsoft On the Issues
- Hay que poner fin a los ciberataques dirigidos a la salud | Microsoft On the Issues
- El próximo capítulo de la ciberdiplomacia en las Naciones Unidas está por llegar | Microsoft On the Issues

Notas finales

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. En este capítulo, las infraestructuras críticas se definen en la Directiva Política Presidencial 21 (PPD-21), Critical Infrastructure Security and Resilience (febrero de 2013).
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

Notas finales, continuación

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. En particular, aplique revisiones a los servidores Exchange por las vulnerabilidades de ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065, CVE-2021-34473). Además, asegúrese de aplicar revisiones a los dispositivos Fortinet FortiOS SSL VPN en busca de vulnerabilidades.
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
    https://www.bbc.com/news/world-asia-59845636
    https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the "Subzero" state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, We unveil the state Trojan "Subzero" from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Como se señala en nuestro blog técnico, la identificación de objetivos en un país no significa necesariamente que un cliente de DSIRF resida en el mismo país, ya que la selección de objetivos internacionales es habitual.
53. Página de inicio | Cybersecurity Tech Accord (cybertechaccord.org)

Dispositivos e infraestructura

Con la aceleración de la transformación digital, la seguridad de la infraestructura digital es más importante que nunca.

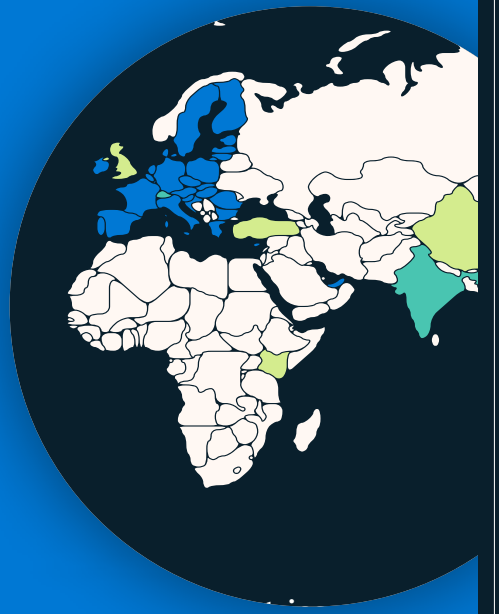
Información general de

los dispositivos y la infraestructura

La pandemia, unida a la rápida adopción de dispositivos de todo tipo conectados a Internet como componente de la aceleración de la transformación digital, ha aumentado de manera considerable la superficie de ataque del mundo digital.

Los ciberdelincuentes y los estados nación se están aprovechando rápidamente. Mientras que la seguridad del hardware y el software de TI se ha reforzado en los últimos años, la seguridad de los dispositivos de la Internet de las Cosas (IoT) y la tecnología de operaciones (OT) no ha seguido el ritmo. Los actores de amenaza están explotando estos dispositivos para establecer el acceso en las redes y permitir el movimiento lateral, para establecer un punto de apoyo en una cadena de suministro, o para interrumpir las operaciones de OT de la organización objetivo.

Los gobiernos de todo el mundo se están trasladando para proteger las infraestructuras críticas mejorando la seguridad de la IoT y de la OT.



Más información en la página 59

Se necesitan directivas de seguridad coherentes e interoperables a nivel mundial para garantizar una amplia adopción.

Más información en la página 59

El malware como servicio se ha trasladado a operaciones a gran escala contra la IoT y la OT expuestas en infraestructuras y servicios públicos, así como en redes corporativas.

Más información en la página 63

Los ataques contra los dispositivos de administración remota van en aumento, con más de 100 millones de ataques observados en mayo de 2022, un aumento de cinco veces en el último año.

Más información en la página 62

Los atacantes aprovechan cada vez más las vulnerabilidades del firmware de los dispositivos de IoT para infiltrarse en las redes corporativas y lanzar ataques devastadores.

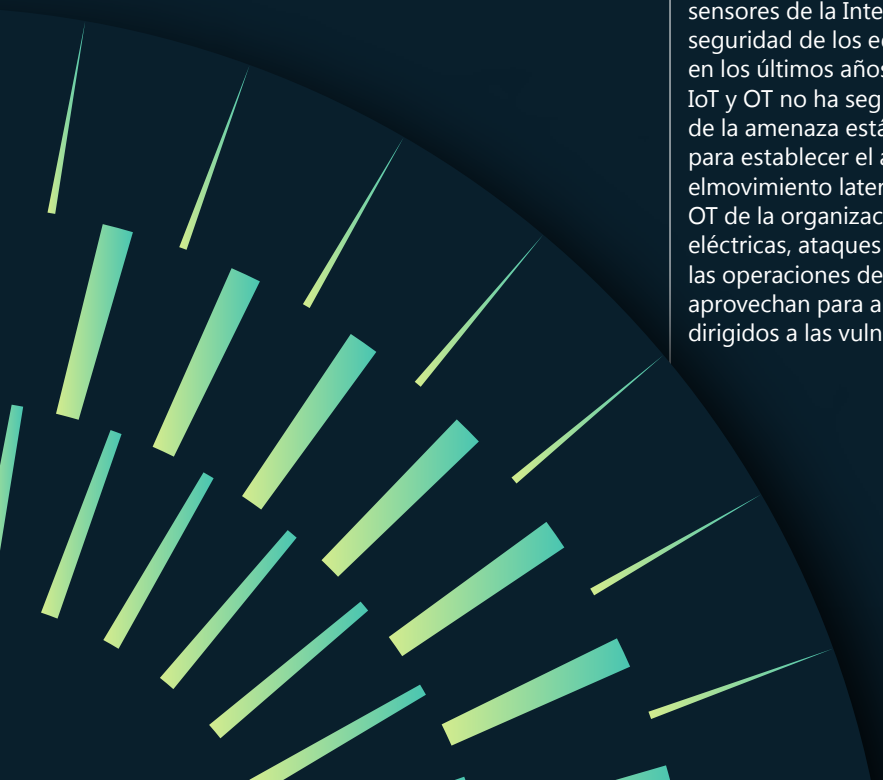
Más información en la página 65

El 32 % de las imágenes de firmware analizadas contenían al menos 10 vulnerabilidades críticas conocidas.

Más información en la página 66

Introducción

La aceleración de la transformación digital ha aumentado el riesgo de ciberseguridad para las infraestructuras críticas y los sistemas ciberfísicos.



En los últimos años se han producido cambios sin precedentes en el mundo digital. Las organizaciones están evolucionando para aprovechar los avances en la capacidad informática tanto de la nube inteligente como del perímetro inteligente. Como resultado de la pandemia que obliga a las entidades a digitalizarse para sobrevivir y del ritmo al que las industrias de todo el mundo están adoptando dispositivos con acceso a Internet, la superficie de ataque del mundo digital está aumentando exponencialmente.

Esta migración rápida ha superado la capacidad de la comunidad de seguridad de mantenerse al día. En el último año, hemos observado que las amenazas explotan dispositivos en todas las partes de la organización, desde equipos de TI tradicionales hasta controladores de tecnología operativa (OT) o simples sensores de la Internet de las Cosas (IoT). Aunque la seguridad de los equipos informáticos se ha reforzado en los últimos años, la seguridad de los dispositivos IoT y OT no ha seguido el mismo ritmo. Los actores de la amenaza están explotando estos dispositivos para establecer el acceso en las redes y permitir elmovimiento lateral o interrumpir las operaciones de OT de la organización. Hemos visto ataques a las redes eléctricas, ataques de ransomware que interrumpen las operaciones de OT, enrutadores de IoT que se aprovechan para aumentar la persistencia y ataques dirigidos a las vulnerabilidades del firmware.

Si bien la prevalencia de las vulnerabilidades de IoT y OT es un desafío para todas las organizaciones, la infraestructura crítica está en mayor riesgo porque los actores de la amenaza han aprendido que la desactivación de los servicios críticos es una palanca poderosa. El ataque de ransomware de 2021 a la empresa Colonial Pipeline Company demostró cómo los delincuentes pueden interrumpir un servicio crítico para aumentar la probabilidad de que se pague un rescate. Y los ciberataques de Rusia contra Ucrania demuestran que algunos estados nación consideran los ciberataques contra infraestructuras críticas como un sabotaje aceptable para lograr sus objetivos militares.

No obstante, hay esperanza en el horizonte. Los legisladores y los defensores de la red están actuando para mejorar la ciberseguridad de las infraestructuras críticas, incluidos los dispositivos de IoT y OT de los que dependen. Los legisladores están acelerando el desarrollo de leyes y reglamentos para fomentar la confianza pública en la ciberseguridad de las infraestructuras y dispositivos críticos.

Microsoft se está asociando con gobiernos de todo el mundo para aprovechar esta oportunidad de mejorar la ciberseguridad y agradecemos cualquier otro compromiso. Sin embargo, nos preocupa que los requisitos incoherentes, a medida o complejos puedan tener efectos no deseados, incluida la disminución de la seguridad en algunos casos al desviar los escasos recursos de seguridad hacia el cumplimiento de múltiples certificaciones duplicadas.

Desde el punto de vista de las operaciones de seguridad, los defensores de la red adoptan varios enfoques para mejorar la postura de seguridad de la IoT/OT de su organización. Uno de los enfoques consiste en implementar la monitorización continua de los dispositivos IoT y OT. Otra es "cambiar a la izquierda"; es decir, exigir y aplicar mejores prácticas de ciberseguridad para los propios dispositivos de IoT y OT. Un tercer enfoque consiste en aplicar una solución de supervisión de la seguridad que abarque tanto las redes de TI como las de OT. Este enfoque holístico tiene la importante ventaja añadida de contribuir a los procesos críticos de la organización, como "romper los silos" entre OT e IT, lo que a su vez permite a la organización alcanzar una postura de seguridad mejorada al tiempo que se cumplen los objetivos empresariales.

Michal Braverman-Blumenstyk
Vicepresidente corporativo, director de Tecnología, nube y seguridad de IA

Los gobiernos actúan para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Los gobiernos de todo el mundo están elaborando y desarrollando políticas para administrar el riesgo de ciberseguridad de las infraestructuras críticas. Muchos también están promulgando políticas para mejorar la seguridad de los dispositivos de IoT y OT. La creciente ola mundial de iniciativas políticas está creando una enorme oportunidad para mejorar la ciberseguridad, pero también plantea desafíos a las partes interesadas de todo el ecosistema.

El desarrollo de una visión holística para la administración de los riesgos cibernéticos de las infraestructuras críticas es fundamental, pero complejo, sobre todo teniendo en cuenta el grado de interconexión entre las tecnologías y los proveedores mundiales, la gama de usos de la tecnología y los riesgos asociados, y la necesidad de invertir en estrategias a corto y largo plazo. Unas directivas de alcance efectivo que impulsen el aprendizaje iterativo y las mejoras, y apoyen la interoperabilidad global e intersectorial, pueden ayudar a administrar la complejidad y permitir una transformación digital más orientada a la seguridad. Sin embargo, un enfoque fragmentado de la legislación podría dar lugar a requisitos reglamentarios superpuestos e incoherentes. Esto podría afectar a los recursos y, en última instancia, socavar los objetivos de seguridad. Por ejemplo, las organizaciones podrían desviar recursos de la innovación y la seguridad a ejercicios de cumplimiento formalistas.

Microsoft busca asociarse con los gobiernos de todo el mundo en la búsqueda de directivas efectivas de ciberseguridad de las infraestructuras críticas, aumentando la comprensión de los desafíos y oportunidades, y apoyando los esfuerzos para mejorar la postura de riesgo colectivo.

Evolución de la directiva de administración de riesgos de ciberseguridad de las infraestructuras críticas

Durante el último año, múltiples jurisdicciones, entre ellas Australia, Chile, la Unión Europea (UE), Japón, Singapur, el Reino Unido (RU) y los Estados Unidos, han desarrollado, actualizado o implementado requisitos de ciberseguridad intersectoriales o específicos del sector.[1] Muchos de estos gobiernos, y otros como el de la India[2] y Suiza[3], ya han emitido o están desarrollando requisitos de notificación de incidentes de ciberseguridad para las infraestructuras críticas y los proveedores de servicios esenciales.[4]

El año pasado se produjeron algunas novedades políticas notables en Australia, la UE, Indonesia y Estados Unidos. Australia promulgó dos leyes para ayudarle a administrar los riesgos de ciberseguridad de las infraestructuras críticas intersectoriales. Las leyes, entre otras cosas, designan nuevos sectores de infraestructuras críticas, exigen la elaboración de planes de administración de riesgos, obligan a informar sobre incidentes de ciberseguridad y facultan al gobierno para intervenir si determina que un operador de infraestructuras críticas no quiere o no puede responder de manera suficiente a un incidente.

La UE trabajó para actualizar su Directiva SRI de 2016, que proporciona un marco para que los Estados miembros de la UE regulen los servicios y productos tecnológicos considerados críticos para su economía y el funcionamiento de la sociedad. La propuesta de NIS 2 incluye revisiones que crearían una nueva categoría de infraestructura digital crítica, aumentarían los requisitos de notificación de ciberincidentes e impondrían requisitos adicionales de administración de riesgos de ciberseguridad, La UE también desarrolló una propuesta de actualización de su Ley de Resiliencia Operativa Digital (DORA), creando nuevos requisitos para las tecnologías de comunicación de la información utilizadas en el sector de los servicios financieros.

En mayo, Indonesia emitió un reglamento presidencial sobre la protección de las infraestructuras de información vitales ("IIV"), que entrará en vigor en mayo de 2024 y abarcará sectores como la energía, el transporte, las finanzas y la salud, entre otros. El objetivo de Indonesia con la normativa es proteger la continuidad de la implementación de la IIV, evitar los ciberataques y aumentar la preparación en la administración de los ciberincidentes. Los proveedores de IIV serán responsables de llevar a cabo una protección segura y confiable, de aplicar una administración eficaz de los riesgos cibernéticos y de informar de los resultados de estos a los organismos gubernamentales correspondientes. El reglamento incluye la obligación de notificar los ciberincidentes en un plazo de 24 horas.

Los gobiernos actúan para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Continuación

El Congreso de los EE. UU. aprobó una ley que autoriza a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) a emitir reglamentos para exigir a los operadores de infraestructuras críticas que informen de los ciberincidentes, y la Administración de Seguridad en el Transporte (TSA) de los EE. UU. emitió nuevos requisitos de ciberseguridad específicos para el sector del transporte. En 2021, la TSA emitió dos directivas de seguridad para los operadores de oleoductos de líquidos peligrosos y gas natural en respuesta al ataque de ransomware a Colonial Pipeline Company:

- La primera directiva exigía a los operadores la designación de un coordinador de ciberseguridad, la notificación de ciberincidentes en un plazo de 12 horas y la realización de una evaluación de la vulnerabilidad de sus sistemas.
- La segunda directiva, que la TSA revisó en 2022, les exigía aplicar medidas de mitigación específicas para protegerse contra los ataques de ransomware y otras amenazas conocidas a los sistemas de TI y OT, desarrollar y aplicar un plan de contingencia y respuesta de ciberseguridad en un plazo de 30 días, y someterse a una revisión anual del diseño de la arquitectura de ciberseguridad.

Basándose en su normativa para oleoductos y gasoductos, la TSA emitió otras dos directivas de seguridad a fines de 2021 que promulgaban requisitos de ciberseguridad para los ferrocarriles de mercancías, las compañías ferroviarias de pasajeros o los sistemas de tránsito ferroviario. Las directivas exigían que los operadores cubiertos designaran un coordinador de ciberseguridad, notificaran los incidentes de ciberseguridad en un plazo de 24 horas, elaboraran y aplicaran un plan de respuesta ante incidentes de ciberseguridad y completaran una evaluación de la vulnerabilidad de la ciberseguridad. La TSA anunció simultáneamente que también actualizaba sus programas de seguridad aérea para exigir a los operadores de aeropuertos y aerolíneas que apliquen las dos primeras disposiciones, designando un coordinador y notificando los incidentes en un plazo de 24 horas.

Desarrollos de directivas en la IoT y la seguridad de los dispositivos OT

En docenas de países, los gobiernos están activos en el desarrollo de requisitos para avanzar en la ciberseguridad de los productos y servicios de tecnología de la información y las comunicaciones (TIC), incluidos los dispositivos de IoT y OT. En el contexto de los productos y servicios de la TIC, las mayores preocupaciones son la seguridad de la cadena de suministro de software y la seguridad de la IoT.

- La Comisión Europea propuso la Ley de resiliencia cibernética, que establecería requisitos de ciberseguridad para el software independiente y los dispositivos conectados y servicios auxiliares.[5] Las prácticas más importantes para los proveedores de software incluyen el aprovechamiento de un ciclo de vida de desarrollo de software seguro[6] y la provisión de una lista de materiales de software.[7] Se aplicarían nuevos requisitos de seguridad a los dispositivos conectados y se encargaría a todos los fabricantes la administración de procesos coordinados de divulgación de vulnerabilidades[8] para los productos liberados.

Los legisladores también han centrado su atención en la continua proliferación de dispositivos de IoT y OT conectados en red.

- En el Reino Unido, el proyecto de Ley de seguridad de los productos e infraestructura de las telecomunicaciones exigirá a los fabricantes de productos conectables por los consumidores, como los televisores inteligentes, que dejen de utilizar contraseñas predeterminadas que son un blanco fácil para los ciberdelincuentes, que establezcan una política de divulgación de vulnerabilidades (como una forma de recibir avisos de los fallos de seguridad) y que ofrezcan transparencia sobre el tiempo mínimo durante el que proporcionarán actualizaciones de seguridad.[9]
- En la UE se están aplicando nuevas normas o requisitos de seguridad a través de múltiples instrumentos legislativos, entre ellos un acto delegado de la Directiva sobre equipos radioeléctricos que se aplica a los dispositivos inalámbricos y pretende mejorar la resiliencia de la red, proteger la privacidad de los consumidores y reducir el riesgo de fraude monetario.[10] Además, podría exigirse el uso de un esquema de certificación de la nube,[11] actualmente en desarrollo como resultado de la Ley. de Ciberseguridad[12] de la UE de 2019.

La necesidad de coherencia

En muchos casos, la gama de actividades entre regiones, sectores, tecnologías y áreas de administración del riesgo operacional se está llevando a cabo simultáneamente, lo que da lugar a un posible solapamiento o incoherencia en el alcance, los requisitos y la complejidad para las organizaciones que tratan de aprovechar la orientación o demostrar el cumplimiento. Sin una definición universalmente aceptada de la IoT, el alcance es muy difícil para las regulaciones de dispositivos IoT y OT. Los ejemplos anteriores se aplican potencialmente a los "productos conectados y servicios auxiliares", los "productos conectables de consumo" y los "dispositivos inalámbricos". Al mismo tiempo, muchos gobiernos pretenden aplicar regímenes de evaluación más sólidos para comprender mejor si las organizaciones y los productos cumplen con los requisitos actuales, emergentes y en evolución, y cómo lo hacen. A medida que estas tendencias se fusionen, la complejidad aumentará. Resulta alentador que las preguntas planteadas durante la consulta sobre la Ley de resiliencia cibernética de la UE exploren cómo la nueva normativa podría interactuar con la regulación de ciberseguridad existente, lo que indica la intención de evitar requisitos de ciberseguridad conflictivos.

Los enfoques iterativos basados en el riesgo y orientados a los resultados o al proceso (en lugar de a la aplicación) podrían fomentar la ciberseguridad y la mejora continua. Del mismo modo, centrarse en permitir la interoperabilidad entre sectores, regiones y áreas políticas podría elevar sistemáticamente la ciberseguridad en las cadenas de suministro mundiales interconectadas.

Los gobiernos actúan para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Continuación

Cada vez son más complejas las directivas de ciberseguridad de las infraestructuras críticas que se están desarrollando en todas las regiones, sectores y áreas temáticas. Esta actividad conlleva grandes oportunidades e importantes retos. La forma de proceder de los gobiernos será crucial para el futuro de la transformación digital y la seguridad de todo el ecosistema.

Acelerar las inversiones de todo el ecosistema en la seguridad de la cadena de suministro de software y la arquitectura de Confianza cero

La Orden Ejecutiva (OE) 14028 de EE. UU. sobre la mejora de la ciberseguridad ha sido un catalizador para acelerar las iniciativas en curso de Microsoft para invertir en nuestra propia seguridad de la cadena de suministro y de todo el ecosistema y para permitir que nuestros clientes cumplan los objetivos de Confianza cero.

Llevamos mucho tiempo creyendo que para mejorar la cadena de suministro de software es necesario compartir los aprendizajes y los procedimientos recomendados, empezando por nuestra publicación del Ciclo de vida de desarrollo de seguridad de Microsoft hace unos 15 años.

Además, estamos colaborando estrechamente con el Centro Nacional de Excelencia en Ciberseguridad para demostrar los enfoques de la arquitectura de Confianza cero aplicados tanto a la tecnología local como a lade la nube, y estableciendo nuevas capacidades de producto, incluida la capacidad de aplicar la autenticación resiliente al phishing para entornos híbridos y multinube.

Hoy, vamos a ir más allá de los requisitos de la EO para demostrar la conformidad con los requisitos de seguridad de la cadena de suministro de software y proporcionar información de la lista de materiales de software (SBOM) de dos maneras:

1. En primer lugar, compartimos una versión open source de nuestra herramienta generadora de SBOM, que hemos creado para que se integre con facilidad a los canales de CI/CD que admiten compilaciones en plataformas Windows, Linux, Mac, iOS y Android.[13]
2. En segundo lugar, contribuiremos al desarrollo de normas industriales para la integridad, la transparencia y la confianza en la cadena de suministro (SCITT). Esto permitirá el intercambio automatizado de información verificable sobre la cadena de suministro, incluidos los artefactos que demuestran la conformidad con los requisitos, como los resultantes de la guía de la cadena de suministro de software de EO.

Información práctica

1. Las instituciones multilaterales deben replantearse para hacer frente al acuciante desafío de los ciberataques de los estados nación.
2. Desarrolle directivas de ciberseguridad que sean coherentes e interoperables entre regiones, sectores y áreas temáticas.

Vínculos a más información

- Inversiones continuas en la seguridad de la cadena de suministro en apoyo de la Orden ejecutiva sobre ciberseguridad | Microsoft Tech Community
- El gobierno de EE. UU. establece la estrategia y los requisitos de la arquitectura de Confianza cero | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Integridad, transparencia y confianza en la cadena de suministro | github.com
- Implementación de una arquitectura de Confianza cero | NCCoE (nist.gov)

IoT y OT expuestas: Tendencias y ataques

El mundo digital, cada vez más conectado, implica que los dispositivos se conectan rápidamente, se comunican con sistemas más amplios, recopilan datos y crean visibilidad en espacios antes oscuros. Esto supone una oportunidad tanto para las organizaciones como para los actores de las amenazas, ya que el negocio de la ciberdelincuencia se está convirtiendo en una industria multimillonaria y en un riesgo.

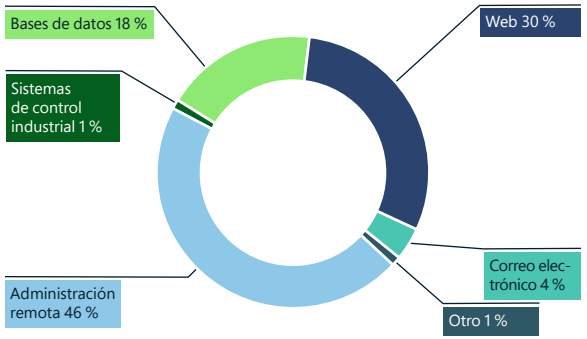
Los dispositivos IoT, que incluyen desde impresoras hasta cámaras web, dispositivos de control climático y controles de acceso a edificios, suponen riesgos de seguridad únicos para las personas, las organizaciones y las redes. Aunque son fundamentales para las operaciones de muchas organizaciones, pueden convertirse con rapidez en una responsabilidad y un riesgo para la seguridad. La rápida adopción de soluciones de IoT en casi todas las industrias ha aumentado el número de vectores de ataque yel riesgo de exposición de las organizaciones.

El malware como servicio se ha trasladado a las operaciones a gran escala contra la infraestructura civil y los servicios públicos (incluidos los hospitales, el petróleo y el gas, las redes eléctricas, los servicios de transporte y otras infraestructuras críticas), así como las redes corporativas. Los actores de las amenazas deben realizar importantes esfuerzos de investigación para descubrir yexplotar la configuración de los entornos operativos y los dispositivos IoT yOT integrados.

Los dispositivos IoT plantean riesgos de seguridad únicos como puntos de entrada y cambio en la red. Millones de dispositivos IoT no tienen revisiones o están expuestos.

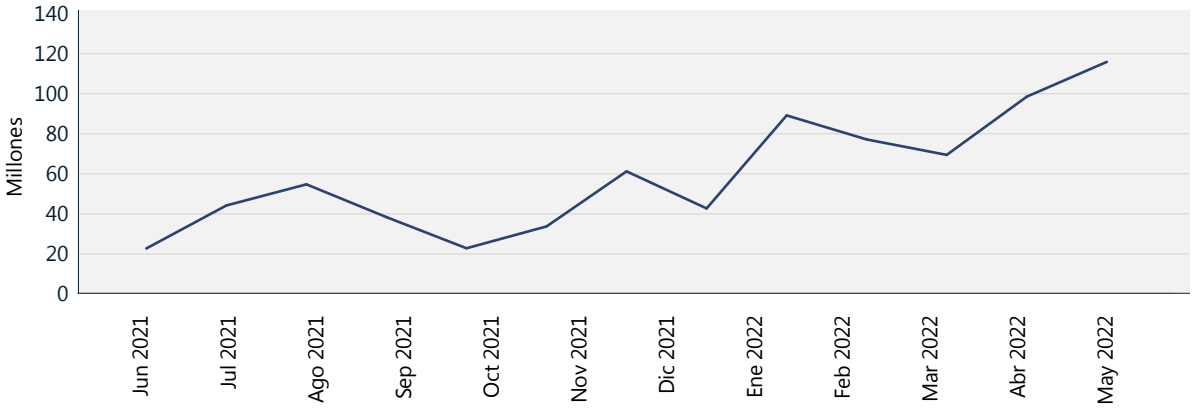
Los dispositivos expuestos pueden ser descubiertos a través de herramientas de búsqueda en Internet, identificando los servicios que escuchan en los puertos de red abiertos. Estos puertos se usan habitualmente para la administración remota de dispositivos.
Si no se asegura correctamente, un dispositivo IoT expuesto puede utilizarse como punto de cambio en otra capa de la red de la empresa, ya que los usuarios no autorizados pueden acceder remotamente a los puertos. Hemos observado una variedad de actores de amenaza que intentan explotar las vulnerabilidades de los dispositivos expuestos a Internet, desde cámaras hasta enrutadores y termostatos. Sin embargo, a pesar del riesgo, millones de dispositivos siguen sin revisiones o expuestos.

Resumen de los tipos de ataque en la IoT/OT



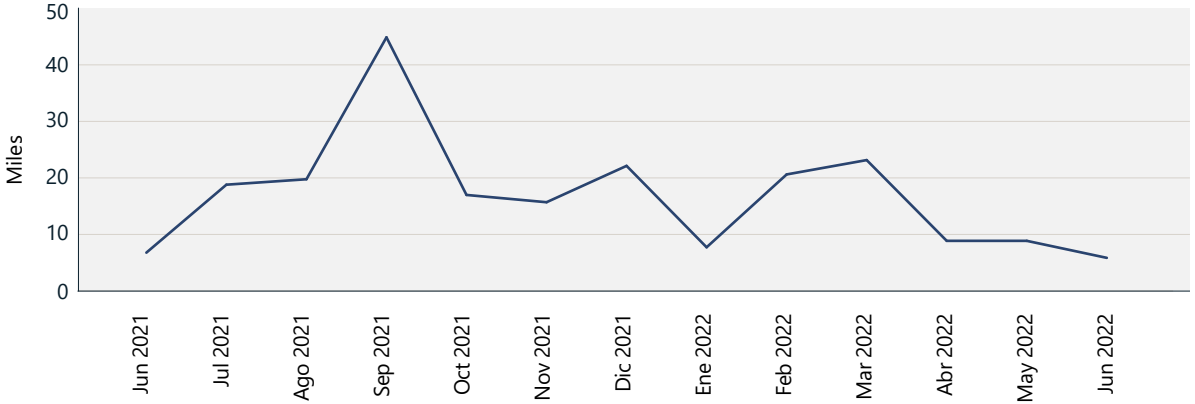
Tipos de ataques observados a través de la red de sensores MSTIC. Los más frecuentes fueron los ataques contra dispositivos de administración remota, los ataques vía web y los ataques a bases de datos (fuerza bruta o vulnerabilidades).

Ataques contra dispositivos de administración remota



Aumento de los ataques a los puertos de administración remota a lo largo del tiempo, como se observa en la red de sensores MSTIC.

Ataques web contra la IoT y OT



Volumen de ataques web a lo largo del tiempo, visto a través de la red de sensores MSTIC. A medida que el número de dispositivos conectados directamente a la web sigue disminuyendo, los atacantes podrían acabar siendo menos propensos a sondearlos.

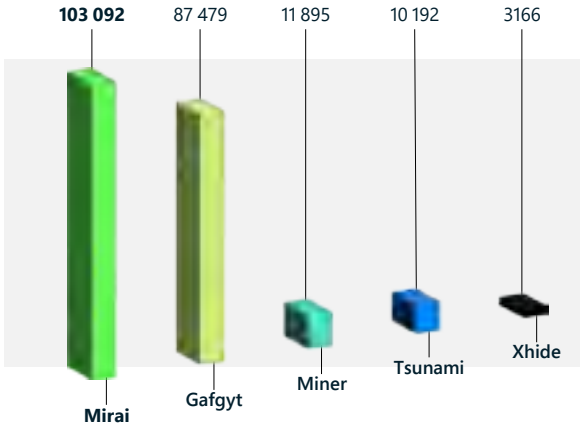
IoT y OT expuestas: Tendencias y ataques

Continuación

Utilidad de malware renovada

A medida que los grupos de ciberdelincuentes han ido evolucionando, también lo ha hecho su implementación de malware y la elección de sus objetivos. El año pasado, observamos que los ataques contra protocolos comunes de la IoT (como Telnet) disminuyeron significativamente, en algunos casos hasta un 60 %. Al mismo tiempo, los grupos de ciberdelincuentes y los agentes de los estados nación reutilizaron las redes de robots. La persistencia del malware, como Mirai, pone de manifiesto la modularidad de estos ataques y la adaptabilidad de las amenazas existentes.

El principal malware de IoT detectado en la práctica



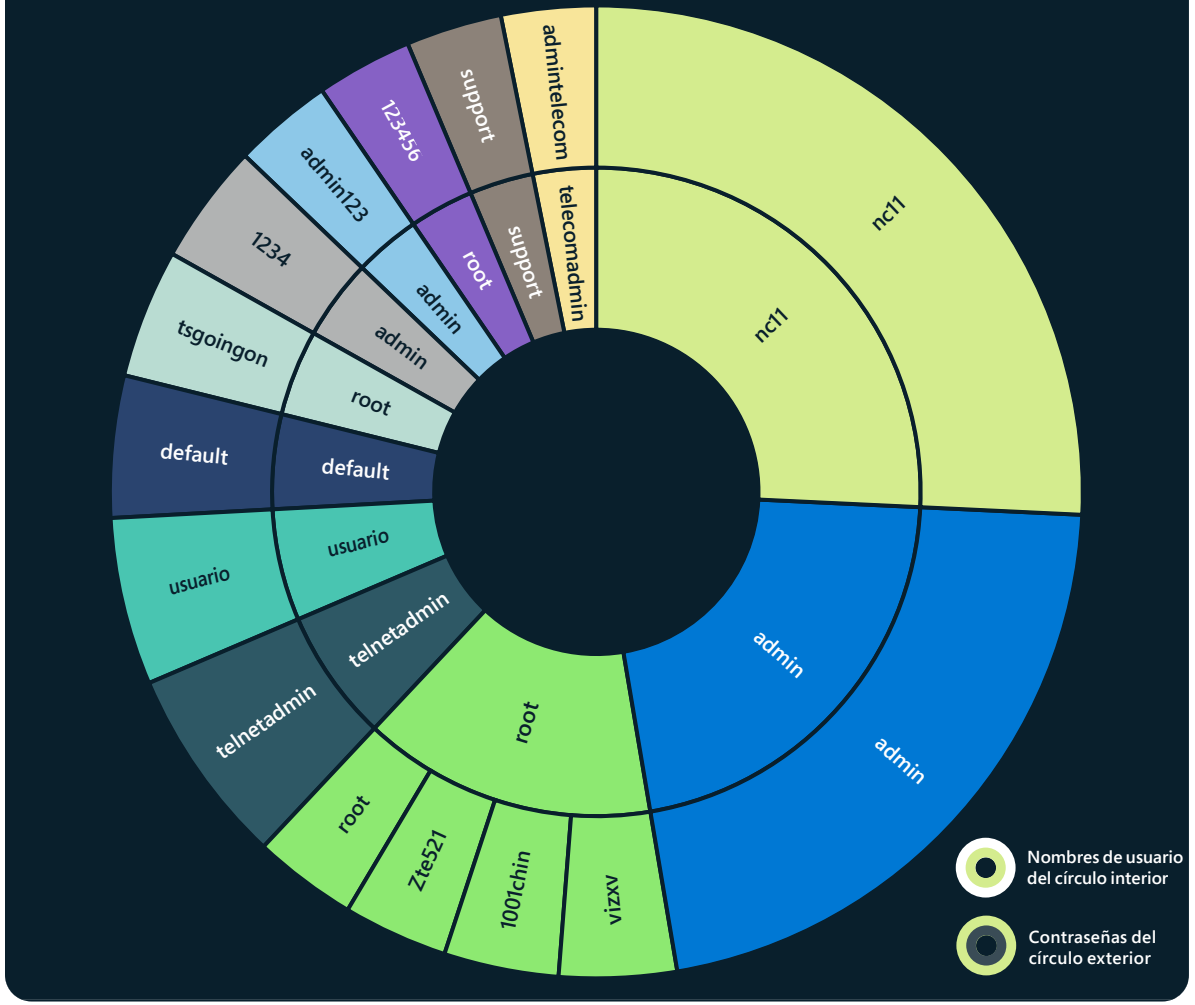
Mirai evolucionó para infectar una amplia gama de dispositivos IoT, incluyendo cámaras de protocolo de Internet, grabadores de video digital de cámaras de seguridad y enrutadores. El vector de ataque eludió los controles de seguridad heredados y supone un riesgo para los puntos de conexión de la red al explotar vulnerabilidades adicionales y desplazarse lateralmente. Mirai se rediseñó en múltiples ocasiones, con variantes que se adaptan a diferentes arquitecturas y explotan vulnerabilidades conocidas y de día cero para comprometer nuevos vectores de ataque.

El uso de Mirai creció entre las arquitecturas de CPU x86 de 32 y 64 bits durante el año pasado, y el malware recibió nuevas capacidades que los grupos delictivos y de estados nación adoptaron con rapidez. Los ataques del estado nación aprovechan ahora las nuevas variantes de las redes de robots existentes en los ataques de denegación de servicio distribuidos (DDoS) contra adversarios extranjeros.

A medida que los ingresos de los ataques contra los dispositivos IoT disminuyeron en 2022, observamos que varios grupos de actores de amenaza abusan de las vulnerabilidades (como Log4j y Spring4Shell) para entregar una carga útil malintencionada a dispositivos como servidores, infectándolos y reclutándolos en grandes redes de robots que realizan ataques DDoS. La renovada utilidad del malware diseñado para dirigirse a los dispositivos vulnerables de la IoT tiene graves implicaciones tanto para las organizaciones como para los países, ya que el movimiento lateral puede exponer puertas traseras a cargas útiles adicionales y a otros dispositivos en las redes.

Muchos protocolos de los sistemas de control industrial no están supervisados y, por tanto, son vulnerables a los ataques específicos de la OT. Esto puede significar un mayor riesgo para las infraestructuras críticas.

Prevalencia relativa de los pares de nombre de usuario y contraseña observados entre los dispositivos IoT/OT en 45 días de señales de sensores.



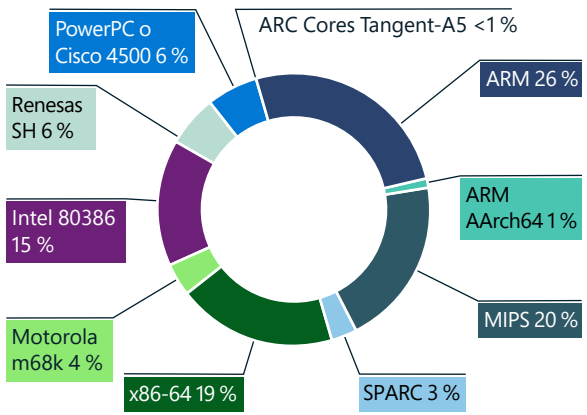
El uso de pares de nombres de usuario y contraseñas comunes incrementa el riesgo de compromiso. Sobre la base de una muestra de más de 39 millones de dispositivos IoT y OT, los que utilizaban nombres de usuario y contraseñas idénticos representaban alrededor del 20 %.

IoT y OT expuestas: Tendencias y ataques

Continuación

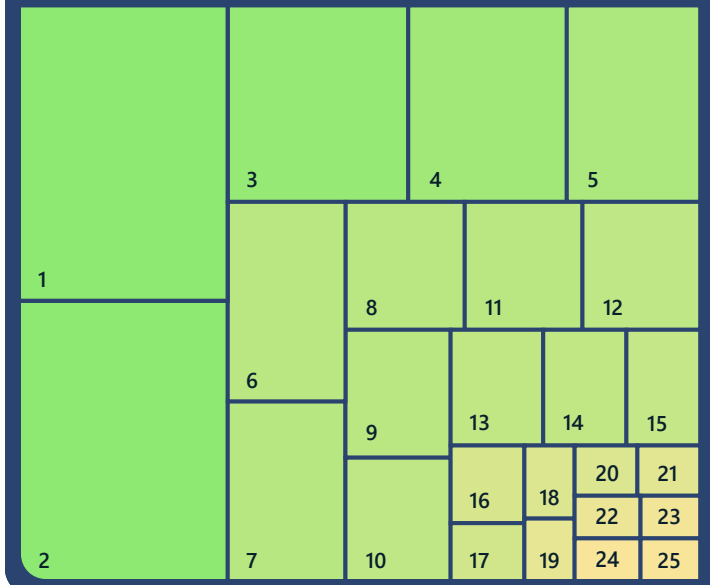
Aunque las configuraciones débiles y las credenciales predeterminadas siguen suponiendo un riesgo para las redes, Microsoft ha observado muchas vulnerabilidades basadas en web que utilizan HTTP. Hemos observado este aumento de los ataques a los servicios basados en web mediante redes de robots heredadas. Mientras tanto, disminuyó el número de puertos telnet abiertos en Internet, un signo positivo para la seguridad de la red, ya que las redes de robots que suponían un riesgo histórico para los dispositivos están perdiendo relevancia. Mientras tanto, disminuyó el número de puertos telnet abiertos en Internet, un signo positivo para la seguridad de la red, ya que las redes de robots que suponían un riesgo histórico para los dispositivos están perdiendo relevancia.

Distribución del malware de IoT por arquitectura de CPU



Microsoft ha observado que los dispositivos IoT que funcionan con ARM son los más atacados por el malware, seguidos por los MIPS, X86-64 e Intel 80386 CPU.

Prevalencia del protocolo del sistema de control industrial



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet en tiempo real
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Agente Siemens WinCC
10. EtherNet/IP O/O
11. Acceso a datos de control de Honeywell
12. MMS
13. IEC-60870
14. Diagnóstico de Honeywell FDA
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Vulnerabilidades del protocolo del sistema de control industrial

Examinamos los datos de OT de nuestros sensores conectados a la nube, revelando los protocolos más comunes del sistema de control industrial (ICS). Estos protocolos permiten conocer la naturaleza de estos dispositivos y su superficie de ataque. Esto es muy relevante para la seguridad de las infraestructuras críticas. Algunos aprendizajes clave son:

1. La mayoría de los protocolos representados son propietarios, por lo que las herramientas estándar de supervisión de TI no tendrán una visibilidad de seguridad suficiente en estos dispositivos y protocolos. Como resultado, las redes quedan sin supervisión y, por tanto, son más vulnerables a los ataques específicos de la OT.
2. Existe una gran variedad de protocolos específicos de los proveedores. Esto significa que las soluciones de seguridad específicas del proveedor no podrán cubrir de manera suficiente toda la red. Microsoft da prioridad a un enfoque agnóstico del proveedor, para ofrecer cobertura de seguridad para la amplia variedad de dispositivos diferentes.
3. Las organizaciones tienen que asegurarse de que estos protocolos no están expuestos directamente a Internet desde sus redes. Esta exposición podría suponer un importante riesgo para la seguridad debido a las vulnerabilidades y a la naturaleza insegura de estos protocolos.

El malware como Mirai persiste desarrollando nuevas capacidades y está siendo adoptado por grupos de ciberdelincuentes y actores de estado nación, aprovechando nuevas variantes de redes de robots existentes en ataques DDoS a adversarios extranjeros.

Información práctica

1. Asegúrese de que los dispositivos son robustos aplicando revisiones, cambiando las contraseñas predeterminadas y los puertos SSH predeterminados.
2. Reduzca la superficie de ataque eliminando las conexiones a Internet innecesarias y los puertos abiertos, restringiendo el acceso remoto mediante el bloqueo de puertos, denegando el acceso remoto y utilizando servicios VPN.
3. Utilice una solución de detección y respuesta de red (NDR) con conciencia de IoT/OT y una solución de administración de eventos e información de seguridad (SIEM)/orquestación y respuesta de seguridad (SOAR) para supervisar los dispositivos en busca de comportamientos anómalos o no autorizados, como la comunicación con hosts desconocidos.
4. Segmentar las redes para limitar la capacidad de un atacante de moverse lateralmente y comprometer los activos después de la intrusión inicial. Los dispositivos de IoT y las redes de OT deben aislarse de las redes de TI corporativas a través del uso de firewalls.
5. Asegúrese de que los protocolos de ICS no se expongan directamente a Internet.

Cadena de suministro y hackeo del firmware

Casi todos los dispositivos conectados a Internet tienen firmware, que es un software incrustado en el hardware ola placa de circuito del dispositivo. En los últimos años, hemos visto un aumento de la selección de firmware para lanzar ataques devastadores. Como es probable que el firmware siga siendo un objetivo valioso para los actores de amenaza, las organizaciones deben protegerse contra la piratería del firmware.

El firmware es responsable de las funciones principales de un dispositivo, como la conexión al a red o el almacenamiento de datos. El firmware se encuentra en enrutadores, cámaras, televisores y otros dispositivos utilizados en las empresas (IoT) junto con equipos de control industrial (OT) utilizados en infraestructuras críticas. Históricamente, el firmware se ha escrito con código no seguro, creando importantes vulnerabilidades que pueden ser explotadas para tomar el control del dispositivo o inyectar código malintencionado en el firmware.

Este riesgo se agrava cuando se trata de la cadena de suministro. La mayoría de los dispositivos se construyen con componentes de software y hardware de numerosos fabricantes, así como con bibliotecas open source. En muchos casos, los operadores de dispositivos no cuentan con visibilidad de la lista de materiales de hardware y software (H/SBOM) para evaluar el riesgo de la cadena de suministro de los dispositivos en su red. En junio de 2020, se revelaron vulnerabilidades en una pila de red utilizada por muchos fabricantes diferentes que afectaban a cientos de millones de dispositivos IoT en el espacio de los equipos industriales y de consumo.[14] En algunos casos, la pila de red fue renombrada por otros proveedores y no había ninguna indicación de que un dispositivo fuera vulnerable. Vemos una amenaza creciente de actores malintencionados que apuntan a esta cadena de suministro de software y hardware de dispositivos IoT/OT para comprometer a las organizaciones.

El proceso de actualización del firmware varía mucho según los dispositivos, y la complejidad y el desafío logístico que supone su realización influyen en la frecuencia de actualización. No siempre es posible determinar si un dispositivo está ejecutando el último firmware, lo que dificulta a los profesionales de la seguridad supervisar y garantizar la postura de seguridad en sus dispositivos IoT y OT. Además, algunos dispositivos tienen un firmware que no está firmado criptográficamente, lo que permite su actualización sin la verificación del usuario. Estos puntos débiles abren aún más los dispositivos a los ataques a lo largo de la cadena de producción y distribución.

Para hacer frente a estas amenazas, Microsoft invierte significativamente en garantizar la seguridad e integridad del firmware a medida que avanza por las distintas etapas de la cadena de suministro, y en certificar en todo momento que no se ha manipulado durante su ingesta o a lo largo del camino. Esto nos permitirá validar la confianza entre cada segmento de la tubería y entregar una cadena de custodia certificada y comprobable de extremo a extremo para cada componente que enviamos a los clientes. Estamos trabajando con nuestros socios para llevar esta seguridad del chip a la nube a todos los dispositivos de la red empresarial y OT.

"Los proveedores de infraestructuras ICT son cada vez más objetivos, ya que permiten la replicación generalizada de un mismo ataque. Al mismo tiempo, la legislación mundial, la reglamentación y las exigencias de los clientes en cuanto a la seguridad y la resiliencia de la cadena de suministro van en aumento, a menudo con requisitos divergentes.

La solución es la asociación. Junto con los proveedores y los gobiernos mundiales, Microsoft se compromete a abordar la seguridad en todo el ecosistema de nuestra cadena de suministro, superando las exigencias de los clientes y de los reguladores. Para ello, estamos impulsando un enfoque integral de la seguridad y la resiliencia operativa que se implementa con flexibilidad en toda la cadena de suministro.

Impulsar la integridad del firmware desde el diseño hasta el funcionamiento del dispositivo es la clave de nuestro enfoque colectivo. Garantizar los procesos de SDL de los proveedores e implementar la innovación de la raíz de confianza del hardware son ejemplos de cómo podemos "construir" la integridad de la cadena de suministro.

Nuestra comunidad está aprovechando la investigación y el desarrollo colectivos que abarcan nuevas técnicas antimanipulación y mecanismos criptográficos, combinados con la supervisión continua y la detección de anomalías. Juntos, estamos avanzando para minimizar el atractivo de la cadena de suministro como superficie de ataque".

Edna Conway,
Vicepresidente, agente de Seguridad y riesgo, Infraestructura en la nube

Enfoque en las vulnerabilidades del firmware

Los atacantes aprovechan cada vez más las vulnerabilidades del firmware de los dispositivos de IoT para infiltrarse en las redes corporativas. A diferencia de los puntos de conexión de TI tradicionales que utilizan agentes XDR para identificar las debilidades, la identificación de vulnerabilidades dentro de los dispositivos de IoT/OT es mucho más esquiva.

Un reciente estudio realizado por Microsoft y el Instituto Ponemon pone de manifiesto tanto la oportunidad como el desafío de la seguridad de los dispositivos IoT/OT en una empresa.[15] Aunque el 68 % de los encuestados cree que la adopción de IoT/OT es fundamental para su transformación digital estratégica, el 60 % reconoce que la seguridad de IoT/OT es uno de los aspectos menos seguros de la infraestructura de TI/OT.

Un ejemplo de atacantes que utilizan las vulnerabilidades del firmware de los dispositivos IoT para infiltrarse en una red es el troyano Trickbot, que aprovechó las contraseñas predeterminadas y las vulnerabilidades de los enrutadores Mikrotik[16] para eludir los sistemas de defensa corporativos. El desafío fundamental del firmware de los dispositivos IoT es la falta de visibilidad de la postura de seguridad y las vulnerabilidades de los dispositivos.

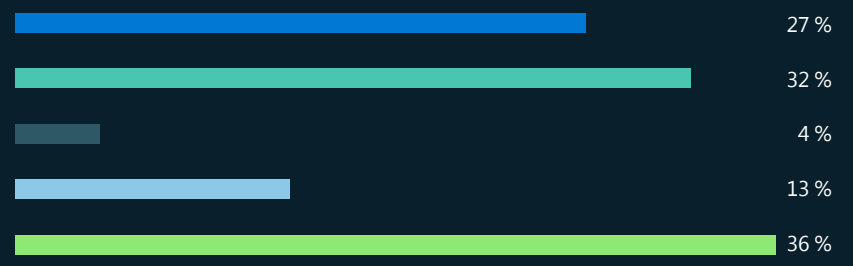
Aunque hay soluciones disponibles para crear dispositivos seguros, hay miles de millones de dispositivos ya en el mercado e implementados en las empresas. Estos dispositivos se conocen como "sistema antiguo". En 2021, Microsoft adquirió ReFirm Labs para poner de relieve la seguridad de los dispositivos antiguos y permitir a los fabricantes de dispositivos mejorar la seguridad de sus productos. ReFirm Labs analiza la imagen binaria del firmware de un dispositivo y elabora un informe detallado sobre posibles fallos de seguridad.[17] Esta tecnología se está incorporando a una futura versión de Microsoft Defender for IoT.

Durante el año pasado, examinamos los resultados agregados del firmware único escaneado por nuestros clientes. Aunque no todos los puntos débiles descubiertos pueden explotarse, ponen de manifiesto el desafío fundamental de la seguridad del firmware de los dispositivos.

Tenga en cuenta que los tipos de debilidades que existen en los dispositivos IoT/OT nunca serían aceptables en los puntos de conexión tradicionales de Windows o Linux.

- Contraseñas débiles: El 27 % de las imágenes de firmware analizadas contenían cuentas con contraseñas codificadas con algoritmos débiles (MD5/DES), que los atacantes pueden romper fácilmente.

Se analizan los puntos débiles de seguridad en las imágenes del firmware



- Vulnerabilidades conocidas: Al igual que otros sistemas, el firmware de los dispositivos IoT/OT aprovecha ampliamente las bibliotecas open source. Sin embargo, los dispositivos suelen venir con versiones desfasadas de estos componentes. En nuestro análisis, el 32 % de las imágenes contenían al menos 10 vulnerabilidades conocidas (CVE) calificadas como críticas (9,0 o más). El 4 % contenía al menos 10 vulnerabilidades críticas con más de seis años de antigüedad.
- Certificados caducados: Los certificados se utilizan para autenticar conexiones e identidades, así como para proteger datos sensibles, pero el 13 % de las imágenes analizadas contenían al menos 10 certificados que habían caducado hace más de tres años.
- Componentes de software: El 36 % de las imágenes contienen componentes de software que Microsoft recomienda excluir en los dispositivos IoT, como herramientas de captura de paquetes (tcpdump, libpcap), que pueden aprovecharse para el reconocimiento de la red como parte de una cadena de ataque.

Ataques de firmware en la práctica

Viasat: Uso de una vulnerabilidad de firmware para atacar la comunicación por satélite

En febrero de 2022, un incidente en la red de satélites desconectó una red de comunicación estratégica con repercusiones en toda Europa. El sistema KA-SAT de Viasat recibió una gran cantidad de tráfico que desconectó muchos módems y se inició un ataque de denegación de servicio contra la red. Al interrumpirse la banda ancha fija, miles de aerogeneradores quedaron inaccesibles a distancia para los operadores y se implementó un malware malintencionado en los módems afectados. La interrupción afectó a más de 30 000 terminales de satélite utilizados por empresas y organizaciones para la comunicación.

Cyclops Blink: Uso de un ataque a la cadena de suministro de firmware para atacar las gateways de los firewall

Para los actores de amenaza, el desarrollo y la expansión de la infraestructura de comando y control (C2) y de ataque es un componente crucial del éxito. A medida que crece la necesidad de una infraestructura C2 estable, los enrutadores se han convertido en un vector de ataque deseable debido a su infrecuente aplicación de revisiones y a la falta de soluciones de seguridad integrales.

Microsoft se está asociando con el gobierno y la industria en la tecnología de análisis de firmware para aportar una mayor visibilidad a la seguridad de los dispositivos y ofrecer seguridad en todo el ciclo de vida para los constructores y operadores de dispositivos.

Desde junio de 2019, un grupo de amenazas persistentes avanzadas (APT) afiliado a un estado nación utilizó el malware modular Cyclops Blink para dirigirse a los dispositivos de firewall vulnerables de WatchGuard y a los enrutadores de ASUS mediante la ejecución de actualizaciones de firmware malintencionadas y el reclutamiento para una gran red de robots. El malware infecta con éxito los dispositivos explotando una vulnerabilidad conocida que permite una escalada de privilegios, lo que permite a los actores de la amenaza administrar el dispositivo. Una vez infectado, el malware permite la instalación de otros módulos y evade las actualizaciones del firmware. Se han observado dispositivos comprometidos que se conectan a servidores C2 hospedados en otros dispositivos WatchGuard. Al emitir muchos certificados SSL para su C2 en varios puertos TCP, los operadores de Cyclops Blink obtuvieron acceso remoto con privilegios a las redes a través de la ejecución de actualizaciones de firmware malintencionadas y la evasión de los métodos de seguridad tradicionales, como el escaneo.

Cómo mejora Microsoft la seguridad de la cadena de suministro

Microsoft se está asociando con el gobierno y la industria para abordar estos desafíos de seguridad de los dispositivos IoT y OT (consulte la discusión en la página 66). Nuestra contribución incluirá el aprovechamiento de la tecnología de análisis de firmware para proporcionar a los operadores de dispositivos visibilidad sobre la postura de seguridad de los dispositivos en su red. Esto permitirá a los clientes identificar y priorizar los dispositivos que necesitan protecciones adicionales, actualizaciones o sustituciones, e impulsar la demanda de los fabricantes de dispositivos para que inviertan en su seguridad. Al mismo tiempo, apoyamos a los creadores con soluciones integrales para diseñar dispositivos seguros y adoptar ciclos de vida de desarrollo seguros.

Otro componente clave es brindar a los constructores y operadores una infraestructura sólida que permita actualizar el firmware de los dispositivos a medida que se descubren y resuelven los problemas de seguridad. Microsoft reúne el análisis de firmware y Defender for IoT con Device Update for IoT Hub para ofrecer una solución que aborde el ciclo de vida completo de la seguridad de los dispositivos IoT y OT. Estos son pasos importantes para hacer realidad nuestra visión de que los clientes aseguren la infraestructura mediante la adopción de dispositivos que apoyen un enfoque de Confianza cero en sus soluciones de IoT y OT.[18]

Los atacantes apuntan cada vez más las vulnerabilidades del firmware de los dispositivos de IoT para infiltrarse en las redes corporativas.

Información práctica

1. Obtenga una visibilidad más profunda de los dispositivos IoT/OT en su red y priorícelos por riesgo para la empresa si se ven comprometidos.
2. Utilice herramientas de escaneo de firmware para conocer los posibles puntos débiles de seguridad y colabore con los proveedores para identificar cómo mitigar los riesgos de los dispositivos de alto riesgo.
3. Influya positivamente en la seguridad de los dispositivos IoT/OT exigiendo a sus proveedores la adopción de los procedimientos recomendados del ciclo de vida de desarrollo seguro.

Vínculos a más información

- Evaluación de las cadenas de suministro críticas que apoyan a la industria estadounidense de las tecnologías de la información y la comunicación

Ataques de OT basados en el reconocimiento

Las cadenas de suministro complejas utilizan información de diseño específica para planificar el sistema real. De la miríada de activos que componen esta información de diseño, el más sensible es el archivo de proyecto, que define el entorno y sus activos. Este archivo es un objetivo estratégico crucial para los actores de amenaza que buscan obtener acceso e implementar un ataque exitoso totalmente adaptado al entorno.

Dirigirse a los sistemas industriales para perturbar los procesos operativos implica dos pasos.

1. Primero, el atacante debe acceder a la red de OT. Esto puede hacerse entrando a través de los dispositivos IoT en el lado de la red de la empresa (nivel 4 del modelo Purdue) y cruzando la frontera entre TI y IoT, tradicionalmente separada por firewalls y equipos de red, hacia los niveles de operación y control.
2. Segundo, hay que identificar los dispositivos de la red. Los sistemas industriales utilizan dispositivos y componentes estándar en arquitecturas personalizadas diseñadas específicamente para sus entornos. Uno de estos dispositivos estándar es el controlador lógico programable (PLC). Cada fabricante desarrolla interfaces y funciones únicas para sus PLC, que son un componente crucial de los sistemas industriales, y estos dispositivos se configuran además con esquemas personalizados diseñados de forma específica para los entornos del cliente.

La configuración única de cada PLC se describe en el archivo de proyecto, que contiene la definición del entorno y sus activos, la lógica de escalera, etc.

En la mayoría de los entornos que muestran pruebas de un ataque, el análisis muestra que la línea de tiempo que precede al ataque supera con creces la duración del propio ataque. Los actores de las amenazas a menudo invierten meses en simular el entorno y sus activos de forma remota, haciendo muchos intentos para construir un modelo y preparar su ataque dirigido. A medida que los entornos cambian continuamente e integran nuevos dispositivos, se crean vulnerabilidades específicamente en torno a los datos de los archivos de proyecto y configuración. El robo ataque en semanas o meses y permitir a los atacantes modelar el entorno objetivo con rapidez y precisión, lo que aumenta la dificultad para detectar la actividad malintencionada.

Industroyer e Incontroller

Hemos observado un aumento de los ataques a organizaciones, infraestructuras críticas y objetivos gubernamentales por parte de actores patrocinados por el estado que utilizan malware modular y marcos de ataque. Los nuevos intentos de interferir en las operaciones críticas de Ucrania ponen de manifiesto la creciente amenaza de los ataques de OT basados en el reconocimiento y muy adaptados a sus entornos de destino. Las prolongadas fases de reconocimiento e investigación llevadas a cabo por los actores cibernéticos de los estados nación apuntan a una estrategia de uso de la ciberguerra para paralizar las infraestructuras remotamente con el fin de alcanzar objetivos estratégicos u operativos específicos en operaciones cibercinéticas combinadas con la estrategia política.

Hemos observado una amenaza creciente de ataques de OT basados en el reconocimiento que están altamente adaptados a sus entornos objetivo.

Ataques de OT basados en el reconocimiento

Continuación

A principios de 2022, se identificaron dos ataques críticos de OT adaptables. Un ataque ciberfísico contra subestaciones eléctricas y relés de protección en Ucrania se llevó a cabo con malware personalizado, incluida una variante de Industroyer, un malware conocido por haber causado cortes de energía en Ucrania tras su implementación en 2016.

Industroyer2 es la primera reimplementación conocida de malware de ataque a OT en un nuevo objetivo. Utilizó el complemento del protocolo IEC104 (protocolo estándar para la monitorización y el control de sistemas de energía) desarrollado para Industroyer y dirigido principalmente a unidades terminales remotas tipo PLC con número de modelo ABB RTU540/560. El autor de este malware utilizó el conocimiento del entorno de la víctima para emitir comandos de manera repetida a salidas predeterminadas, asegurándose de que no pudieran encenderse manualmente. Esto aseguraba cortes de energía más duraderos y un impacto más dañino.

Incontroller, un marco de ataque modular identificado durante el mismo período, es un conjunto de herramientas modulares que reduce de forma considerable el tiempo de espera para penetrar y atacar los dispositivos OT, eludiendo las soluciones de seguridad heredadas. El kit de herramientas de propósito general tiene capacidades de recopilación de datos, reconocimiento y ataque que son altamente personalizables para diferentes entornos y pueden tener un gran impacto en la fase de investigación para un ataque de OT, lo que reduce el tiempo necesario para realizar el reconocimiento, apoya la simulación de entornos mediante la extracción de información sobre los dispositivos y sus configuraciones.

El marco de trabajo de Incontroller es compatible con los protocolos de los PLC de Schneider Electric y Omron y recoge información, como la versión del firmware, eltipo de modelo y los dispositivos conectados. El kit de herramientas puede emitir comandos para cambiar las configuraciones y encender y apagar las salidas. Una vez que se accede a un entorno, el marco admite la implantación de puertas traseras en los dispositivos para la entrega de más cargas útiles, la emisión de vulnerabilidades para aumentar los puntos de acceso, la carga de lógica de escalera y la capacidad de iniciar ataques DoS. La naturaleza genérica del conjunto de herramientas permite a un actor de amenaza atacar un entorno con rapidez sin necesidad de escribir nuevos ataques para cada PLC o ubicación. Esto permite al actor interactuar de forma sencilla con diferentes tipos de máquinas potencialmente en muchas industrias.

Información práctica

1. Evite transferir archivos que contengan definiciones del sistema a través de canales no seguros, o a personal no esencial.
2. Cuando la transferencia de este tipo de archivos sea inevitable, asegúrese de supervisar la actividad en la red y garantizar la seguridad de los activos.
3. Proteja las estaciones de ingeniería mediante la supervisión con soluciones EDR.
4. Lleve a cabo de forma proactiva la respuesta ante incidentes en las redes OT.
5. Implantar una monitorización continua, como Defender for IoT.

Notas finales

1. Consulte, por ejemplo, Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Ley de modificación de la legislación en materia de seguridad (Protección de infraestructura crítica) de 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | Publicación de prensa | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Ley sobre telecomunicaciones (Seguridad) 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In: página de inicio
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Consulte, por ejemplo, sin título (house.gov)
5. Ley de ciberresiliencia | Configurar el futuro digital de Europa (europa.eu)
6. Consulte, por ejemplo, Ciclo de vida de desarrollo de seguridad de Microsoft
7. Consulte, por ejemplo, Generación de listas de materiales de software (SBOM) con SPDX en Microsoft: Engineering@Microsoft; consulte también, por ejemplo, The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Consulte, por ejemplo, https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill—product security factsheet—GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)
12. Certification — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub - microsoft/sbom-tool: The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. La innovación en IoT/OT es fundamental, pero conlleva importantes riesgos (diciembre de 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. Descubrimiento del uso de dispositivos IoT por parte de Trickbot en la infraestructura C2 (marzo de 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. Episodio del programa de IoT en Channel 9 sobre el escaneo del firmware de IoT (mayo de 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. Cómo aplicar un enfoque de Confianza cero a sus soluciones de IoT (mayo de 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Operaciones de influencia cibernética

Las operaciones de influencia extranjera actuales utilizan nuevos métodos y tecnologías, lo que hace que sus campañas destinadas a erosionar la confianza sean más eficientes y eficaces.

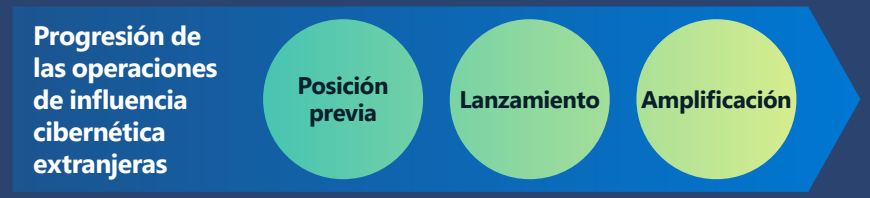
Información general de

las operaciones de influencia cibernética

Las operaciones de influencia extranjera actuales utilizan nuevos métodos y tecnologías, lo que hace que sus campañas destinadas a erosionar la confianza sean más eficientes y eficaces.

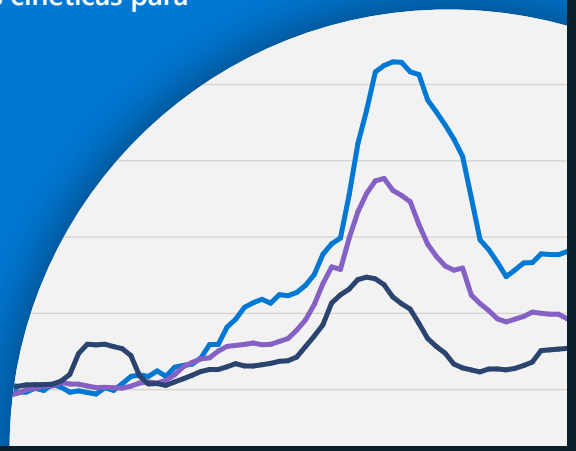
Los estados nación recurren cada vez más a sofisticadas operaciones de influencia para distribuir propaganda e influir en la opinión pública, tanto en el nivel nacional como en el internacional. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos. Los actores expertos en manipulación persistente avanzada están utilizando los medios de comunicación tradicionales junto con Internet y las redes sociales para aumentar enormemente el alcance, la escala y la eficacia de sus campañas, así como el impacto desmesurado que están teniendo en el ecosistema informativo mundial. En el último año, hemos visto cómo estas operaciones se han utilizado como parte de la guerra híbrida de Rusia en Ucrania, pero también hemos visto cómo Rusia y otras naciones, incluidas China e Irán, recurren cada vez más a las operaciones de propaganda impulsadas por las redes sociales para ampliar su influencia global.

Las operaciones de ciberinfluencia son cada vez más sofisticadas, ya que cada vez más gobiernos y estados nación utilizan estas operaciones para moldear la opinión, desacreditar a los adversarios y promover la discordia.



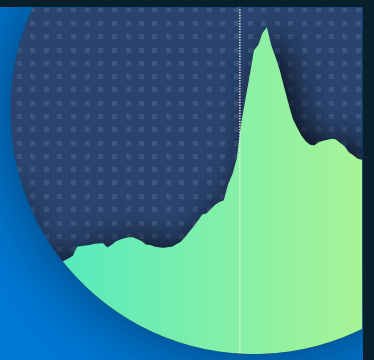
Más información en la página 74

La invasión rusa de Ucrania demuestra las operaciones de influencia cibernética integradas con ciberataques más tradicionales y operaciones militares cinéticas para maximizar el impacto.



Más información en la página 76

Rusia, Irán y China emplearon campañas de propaganda e influencia a. lo largo de la pandemia de COVID-19, a menudo como un dispositivo estratégico para lograr objetivos políticos más amplios.



Más información en la página 76

Los medios sintéticos son cada vez más frecuentes debido a la proliferación de herramientas que crean y difunden fácilmente imágenes, videos y audio artificiales de gran realismo. La tecnología de procedencia digital que certifica el origen de los activos de los medios de comunicación es prometedora para combatir el uso indebido.

Más información en la página 80

Un enfoque holístico para protegerse de las operaciones de influencia cibernética

Microsoft está aprovechando su ya madura infraestructura de inteligencia sobre ciberamenazas para combatir las operaciones de ciberinfluencia. Nuestra estrategia consiste en detectar, interrumpir, defender y disuadir las campañas de propaganda de los agresores extranjeros.

Más información en la página 83

Introducción

La democracia necesita información confiable para prosperar. Un área clave de atención para Microsoft son las operaciones de influencia que desarrollan y perpetúan los estados nación. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos.

Las operaciones de influencia extranjera siempre han sido una amenaza para el ecosistema de la información. Sin embargo, lo que difiere en la era de Internet y los medios sociales es el enorme aumento del alcance, la escala y la eficacia de las campañas, y el enorme impacto que pueden tener en la salud del ecosistema informativo mundial.

El viejo adagio de que "una mentira recorre medio mundo antes de que la verdad tenga la oportunidad de ponerse los zapatos" se confirma ahora con datos. Un estudio del Instituto Tecnológico de Massachusetts (MIT)[1] descubrió que las falsedades tienen un 70 % más de probabilidades de ser retuiteadas que la verdad y llegan seis veces más rápido a las primeras 1500 personas. El ecosistema de la información se ha vuelto cada vez más turbio a medida que las campañas de propaganda florecen en Internet y en las redes sociales y socavan la confianza en las noticias tradicionales. En un estudio de 2021,[2] solo el 7 % de los adultos estadounidenses dijo tener "mucha" confianza en la información de los periódicos, la televisión y la radio, mientras que el 34 % dijo no tener "ninguna".

Microsoft ha estado trabajando para identificar los principales actores, amenazas y tácticas en el espacio de influencia cibernética extranjera y para compartir las lecciones aprendidas. En junio de este año, publicamos un informe exhaustivo sobre las lecciones aprendidas de Ucrania, que contenía un análisis detallado de las operaciones de influencia cibernética de Rusia.[3]

También estamos estudiando cómo las tecnologías avanzadas, como "deep fake" o falsificaciones profundas, pueden convertirse en armas y socavar la credibilidad de los periodistas. Y estamos trabajando con la industria, el gobierno y el mundo académico para desarrollar mejores formas de detectar los medios sintéticos y restaurar la confianza, como los sistemas de inteligencia artificial (IA) que pueden detectar las falsificaciones.

La naturaleza rápidamente cambiante del ecosistema de la información y de la propaganda en línea de los estados nación, incluida la fusión de los ciberataques tradicionales con las operaciones de influencia y la interferencia en las elecciones democráticas, requiere un enfoque de toda la sociedad para mitigar las amenazas a la democracia tanto en línea como fuera de ella.

Microsoft se dedica a apoyar un ecosistema informativo saludable en el que prosperen las noticias y la información de confianza. Estamos desarrollando herramientas y capacidades de detección de amenazas para combatir el riesgo cambiante y creciente de las operaciones de influencia impulsadas por el estado nación. Para que este trabajo sea posible, adquirimos recientemente Miburo Solutions, nos asociamos con validadores de terceros como el Global Disinformation Index y NewsGuard, y participamos y a veces lideramos asociaciones de múltiples partes interesadas, como la Coalition for Content Provenance and Authenticity (C2PA). Solo trabajando juntos podremos conseguir enfrentarnos a quienes pretenden socavar los procesos y las instituciones democráticas.

Teresa Hutson
Vicepresidenta, Tecnología y responsabilidad corporativa

Tendencias en las operaciones de influencia cibernética

Las operaciones de ciberinfluencia son cada vez más sofisticadas, ya que la tecnología evoluciona al mismo ritmo. Estamos asistiendo a una superposición y ampliación de las herramientas utilizadas en los ciberataques tradicionales que se aplican a las operaciones de ciberinfluencia. Además, estamos asistiendo a una mayor coordinación y amplificación entre los estados nación.

Microsoft invirtió este año en la lucha contra las operaciones de influencia extranjera mediante la adquisición de Miburo Solutions, una empresa especializada en el análisis de operaciones de influencia extranjera. Mediante la combinación de estos analistas con los analistas de contexto de amenazas de Microsoft, se formó el Centro de análisis de amenazas digitales (DTAC). DTAC analiza e informa sobre las amenazas de estado nación, incluyendo tanto los ciberataques como las operaciones de influencia, combinando la información y la inteligencia de las amenazas con el análisis geopolítico para brindar conocimientos e informar sobre la respuesta y las protecciones eficaces.

Más de tres cuartas partes de las personas de todo el mundo afirmaron estar preocupadas por la militarización de la información,[4] y nuestros datos respaldan estas preocupaciones. Microsoft y sus socios han estado rastreando el modo en que los actores de estado nación usan las operaciones de influencia para lograr sus objetivos estratégicos y metas políticas. Además de los ciberataques destructivos y los esfuerzos de ciberespionaje, los regímenes autoritarios emplean cada vez más las operaciones de ciberinfluencia para moldear la opinión, desacreditar a los adversarios, incitar al miedo, promover la discordia y distorsionar la realidad.

Estas operaciones de ciberinfluencia extranjera suelen tener tres fases:

Posición previa

Al igual que el posicionamiento previo de malware en la red informática de una organización, las operaciones de ciberinfluencia extranjeras posicionan previamente narraciones falsas en el dominio público de Internet. La táctica de posicionamiento previo ha ayudado durante mucho tiempo a las actividades cibernéticas más tradicionales, sobre todo si los administradores de TI analizan su actividad de red más reciente. El malware que permanece latente durante un tiempo prolongado en una red puede hacer que su uso posterior sea más eficaz. Las narraciones falsas que pasan inadvertidas en Internet pueden hacer que las referencias posteriores parezcan más creíbles.

Lanzamiento

A menudo, en el momento más beneficioso para lograr los objetivos del actor, se lanza una campaña coordinada para propagar las narraciones a través de los medios de comunicación respaldados e influenciados por el gobierno y los canales de las redes sociales.

Amplificación

Por último, los medios de comunicación controlados por el estado y sus apoderados amplifican las narraciones dentro de las audiencias objetivo. A menudo, los facilitadores tecnológicos involuntarios amplían el alcance de las narraciones. Por ejemplo, la publicidad en línea puede ayudar a financiar actividades y los sistemas coordinados de entrega de contenidos pueden inundar los motores de búsqueda.

Este enfoque de tres pasos se aplicó a fines de 2021 para apoyar la falsa narración rusa en torno a supuestas armas biológicas y biolaboratorios en Ucrania. Esta narración se subió por primera vez a YouTube el 29 de noviembre de 2021 como parte de un programa habitual en inglés de un expatriado estadounidense afincado en Moscú que afirmaba que los laboratorios biológicos financiados por Estados Unidos en Ucrania estaban relacionados con las armas biológicas. La historia pasó prácticamente inadvertida durante meses. El 24 de febrero de 2022, justo cuando los tanques rusos cruzaron la frontera, la narración se envió a la batalla. Un equipo de análisis de datos de Microsoft identificó 10 sitios de noticias controlados o influenciados por Rusia que publicaron de manera simultánea informes el 24 de febrero apuntando al "informe del año pasado" y tratando de darle credibilidad. Además, funcionarios rusos del Ministerio de Asuntos Exteriores celebraron conferencias de prensa que sembraron aún más las falsas afirmaciones sobre los biolaboratorios estadounidenses en el entorno informativo. Los equipos patrocinados por Rusia trabajaron entonces para amplificar la narración en las redes sociales y en los sitios de Internet de manera más amplia.

Estamos viendo cómo los regímenes autoritarios de todo el mundo colaboran para contaminar el ecosistema de la información en beneficio mutuo. Por ejemplo, a lo largo de la pandemia de COVID-19, Rusia, Irán y China emplearon operaciones de propaganda e influencia utilizando una combinación de métodos de difusión abiertos, semiclandestinos y encubiertos para atacar a las democracias y promover objetivos geopolíticos (se analiza en profundidad en la página 76). Los tres regímenes aprovecharon los ecosistemas de mensajes e información de los demás para promover las narraciones preferidas. Gran parte de esta cobertura consistió en críticas o teorías conspirativas sobre Estados Unidos y sus aliados, difundidas por figuras gubernamentales en declaraciones oficiales, al tiempo que promovían sus propias vacunas y respuestas al COVID-19 como superiores a las de Estados Unidos y otras democracias. Al amplificarse mutuamente, los medios de comunicación estatales crearon un ecosistema en el que la cobertura negativa de las democracias (o la cobertura positiva de Rusia, Irán y China) producida por un medio de comunicación estatal se vio reforzada por otros.

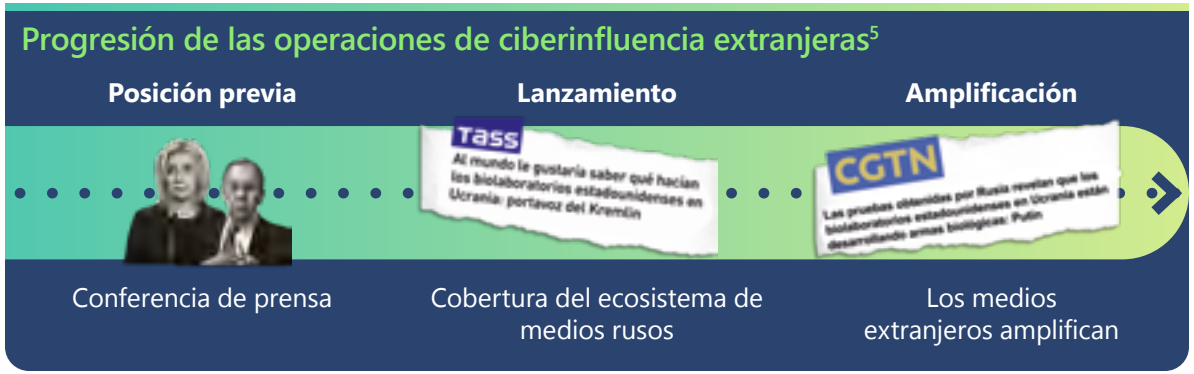


Ilustración de cómo las narraciones sobre los biolaboratorios y las armas biológicas de Estados Unidos se difunden a través de las tres amplias fases de muchas operaciones de influencia extranjera: posición previa, lanzamiento y amplificación.

Tendencias en las operaciones de influencia cibernética

Continuación

Por si fuera poco, las entidades tecnológicas del sector privado podrían facilitar estas campañas sin saberlo. Los facilitadores pueden ser empresas que registran dominios de Internet, hospedan sitios web, promueven material en las redes sociales y sitios de búsqueda, canalizan el tráfico y ayudan a pagar estos ejercicios mediante la publicidad digital. Las organizaciones deben conocer las herramientas y los métodos empleados por los regímenes autoritarios para las operaciones de ciberinfluencia, de modo que puedan detectar y luego prevenir la propagación de las campañas. También existe una necesidad creciente de ayudar a los consumidores a desarrollar una capacidad más sofisticada para identificar las operaciones de influencia extranjeras y limitar el compromiso con sus narrativas o contenidos.

Las operaciones de ciberinfluencia, incluida la propaganda autoritaria, son una amenaza para las democracias de todo el mundo, ya que erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos.

Es necesario aumentar la coordinación y el intercambio de información entre el gobierno, el sector privado y la sociedad civil para aumentar la transparencia y exponer y desbaratar estas campañas de influencia.

En todo el mundo, más de tres cuartas partes de las personas se preocupan por la forma en que la información se convierte en un arma.

Enfoque en las operaciones de influencia durante el COVID-19 y la invasión rusa de Ucrania

Los estados nación que intentan controlar el entorno de la información a lo largo de la pandemia y durante la invasión rusa de Ucrania proporcionan ejemplos descarnados de cómo los regímenes autoritarios mezclan las operaciones cibernéticas y de información.

Propaganda de COVID-19

Rusia, Irán y China emplearon campañas de propaganda e influencia durante la pandemia de COVID-19. El COVID-19 ocupó un lugar destacado en estas campañas de dos maneras principales:

1. Representaciones de la pandemia en sí.
2. Campañas que utilizaron COVID-19 como un dispositivo estratégico para lograr objetivos políticos más amplios.

El objetivo general de este tipo de campañas es doble: en primer lugar, socavar las democracias, las instituciones democráticas y la imagen de Estados Unidos y sus aliados en la escena mundial; y en segundo lugar, reforzar su propia posición a nivel nacional e internacional.

Un ejemplo de esto puede verse en los mensajes de las cuentas y organizaciones mediáticas rusas conocidas que se dirigen a los lectores de lengua inglesa frente a la forma en que el gobierno ruso se comunicó con su propio pueblo en relación con la vacuna y la gravedad del COVID-19.

Temas cubiertos por las 10 historias sobre el coronavirus más vistas en RT.com
(Oct 2021 - Abr 2022)

La propaganda contra las vacunas se dirige a los lectores no rusos

Ruso (Traducido al español)	Inglés (traducido al español)
"Los bloqueos y los refuerzos impiden la transmisión"	"Las vacunas no consiguen frenar la transmisión y son ineficaces contra las nuevas cepas"
"Los personajes públicos rusos dan positivo en las pruebas"	"La vacuna de Pfizer tiene efectos secundarios peligrosos"
"Los casos y las muertes están aumentando en Rusia"	"La vacunación masiva tiene una motivación política"
"La vacuna Sputnik V es muy eficaz"	"Pfizer y Moderna realizan ensayos no regulados"
"Se necesita la prueba de la vacuna en el transporte público"	

La mensajería rusa sobre el COVID-19 difiere según el idioma.

Las campañas que pretendían ocultar el origen del virus COVID-19 ofrecen otro ejemplo. Desde el comienzo de la pandemia, la propaganda rusa, iraní y china de COVID-19 impulsó la cobertura de los demás para amplificar estos temas centrales. Gran parte de esta cobertura consistió en promover críticas o teorías conspirativas sobre Estados Unidos. Al amplificarse mutuamente de forma periódica, los medios de comunicación estatales desarrollaron un ecosistema en el que la cobertura negativa de las democracias (o la cobertura positiva de Rusia, Irán y China) producida por un medio de comunicación estatal se vio reforzada por otros.

Un ejemplo de ello es la temprana sugerencia de los medios de comunicación estatales rusos e iraníes de que el COVID-19 podría ser un arma biológica creada por Estados Unidos. Esta afirmación circuló en sitios web de conspiraciones marginales a principios de la pandemia después de una entrevista con un profesor de derecho que afirmó que creía que el COVID-19 fue creado como un arma.[6] Después de que la entrevista se publicara en algunos sitios web de alcance limitado, los medios de comunicación estatales recogieron la historia. PressTV, un medio de comunicación iraní en inglés y francés patrocinado por el gobierno iraní,[7] publicó un artículo en inglés en febrero de 2020 titulado "¿Es el coronavirus un arma de guerra biológica estadounidense como cree Francis Boyle?". El artículo sugería que Estados Unidos estaba detrás del brote de COVID-19, y escribía: "en todas las guerras de Estados Unidos se utilizan armas radiológicas, químicas, biológicas y otras prohibidas, que infligen un daño devastador a la población de las zonas objetivo".[8] Los medios de comunicación estatales rusos y las cuentas del gobierno chino se hicieron eco de este sentimiento. Russia Today (RT), un medio de comunicación estatal conocido por su papel en la difusión de la propaganda del Kremlin[9], publicó al menos una noticia que promovía declaraciones de funcionarios iraníes en las que se afirmaba que el COVID-19 podría ser un "producto de un 'ataque biológico' estadounidense dirigido a Irán y China"[10] y publicó mensajes en las redes sociales sugiriendo lo mismo. Por ejemplo, un tweet de RT del 27 de febrero de 2020, decía: "Que levante la mano quien no se va a sorprender si alguna vez se revela que el #coronavirus es una arma biológica?"[11]

La guerra en Ucrania: la propaganda como arma de guerra

La invasión rusa de Ucrania es un claro ejemplo de cómo las operaciones de ciberinfluencia pueden combinarse con ciberataques más tradicionales y operaciones militares sobre el terreno para maximizar su impacto.

En el período previo a la invasión de Ucrania, los analistas de inteligencia de amenazas de Microsoft vieron que al menos seis actores distintos alineados con Rusia lanzaron más de 237 ciberataques contra Ucrania. Estas campañas buscaban degradar los servicios e instituciones, interrumpir el acceso de los ucranianos a información fiable y sembrar dudas sobre el liderazgo del país.

Enfoque en las operaciones de influencia durante el COVID-19 y la invasión rusa de Ucrania

Continuación

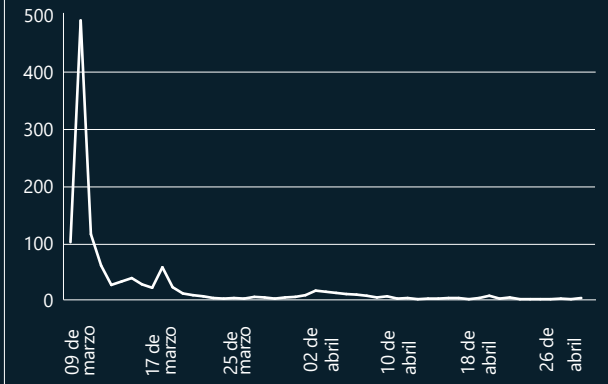
En un informe de Microsoft publicado en abril de 2022, mostramos cómo, en un aparente intento de controlar el entorno informativo en Kiev, Rusia lanzó un ataque con misiles contra una torre de televisión en Kiev el mismo día que lanzó un destructivo programa malintencionado contra una importante empresa de medios de comunicación ucraniana.[12]

En otro ejemplo de cómo convergen los ciberataques y las operaciones de influencia, un actor de amenazas ruso envió a ciudadanos ucranianos correos electrónicos que pretendían ser de residentes de Mariupol, culpando al gobierno ucraniano de la escalada de la guerra y llamando a sus compatriotas a contraatacar al gobierno. Estos correos electrónicos se dirigían específicamente (por su nombre) a quienes los recibían, indicando que podrían haber sufrido el robo de su información en un ciberataque anterior relacionado con el espionaje. No se incluyeron vínculos malintencionados, lo que sugiere que la intención eran puras operaciones de influencia.

La presentación de material supuestamente pirateado, filtrado o sensible es una táctica común utilizada por los actores rusos en las operaciones de influencia. A lo largo de la guerra en Ucrania, los canales de medios sociales prorrusos han promovido lo que afirman que son materiales filtrados o sensiblesde fuentes ucranianas. Los canales y medios de comunicación social prorrusos utilizan el material filtrado o sensible como parte de una estrategia de influencia más amplia para degradar la confianza en las instituciones y poner en duda las narraciones principales. Esta información puede manipularse para crear propaganda contra Ucrania y Occidente, disminuir la confianza en la seguridad digital y erosionar el apoyo a la ayuda occidental a Ucrania.

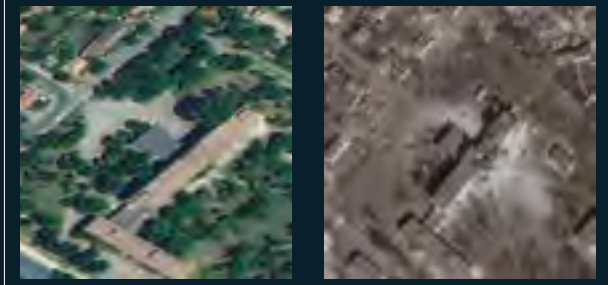
Rusia utilizó otros ataques informativos para moldear la opinión pública después de los acontecimientos sobre el terreno para oscurecer o socavar los hechos. Por ejemplo, el 7 de marzo, Rusia predijo, mediante una presentación ante la Organización de las Naciones Unidas (ONU), que un hospital de maternidad de Mariupol (Ucrania) se había desocupado y se estaba usando como sitio militar. El 9 de marzo, Rusia bombardeó el hospital. Tras conocerse la noticia del bombardeo, el representante de Rusia en la ONU, Dmitry Polyanskiy, tuiteó que la cobertura del bombardeo era una "noticia falsa" y citó las afirmaciones anteriores de Rusia sobre su supuesto uso como emplazamiento militar. A continuación, Rusia difundió este relato en los sitios web controlados por Rusia durante las dos semanas siguientes al ataque al hospital.

Dominios con tráfico
(9 de marzo de 2022 al 30 de abril de 2022)



Los sitios web de propaganda publicaron historias sobre la maternidad durante unas dos semanas, con una breve reactivación a partir del 1 de abril de 2022. Fuente: Microsoft AI for Good Lab.

Imágenes por satélite de un hospital perinatal en Mariupol en febrero y marzo de 2022



El propio análisis de imágenes por satélite de Microsoft mostró el bombardeó al hospital perinatal. La primera foto es del 24 de febrero de 2022 y la segunda es del 24 de marzo de 2022. Fuente de la foto: Planet Labs.

El encubrimiento de las atrocidades por parte de Rusia ha continuado a medida que avanzaba la guerra. Por ejemplo, a fines de junio de 2022, los medios de comunicación rusos y las personas influyentes presentaron el bombardeo de un centro comercial como algo justificado y necesario, afirmando falsamente que no se utilizaba como centro comercial, sino como arsenal de las fuerzas de defensa territorial ucranianas.[13] Varios blogueros pro-Kremlin en Telegram publicaron y amplificaron contenidos que reforzaban la narración de "falsa bandera", con blogueros que señalaban supuestos indicadores de fabricación, como la presencia de personas con uniforme militar en las imágenes del lugar de los hechos[14] y la ausencia de mujeres en el metraje.[15] Rusia lanzó campañas apoyándose en un sistema construido de mensajeros y medios de propaganda. La amplificación de estas historias en línea proporciona a Rusia la capacidad de desviar la culpa en la escena internacional y evitar la responsabilidad.

Los Estados nación como Rusia comprenden el valor de utilizar la información derivada de fuentes cerradas para influir en las percepciones del público, utilizando campañas de "hackeo y filtración" para difundir narraciones contrarias y sembrar la desconfianza.

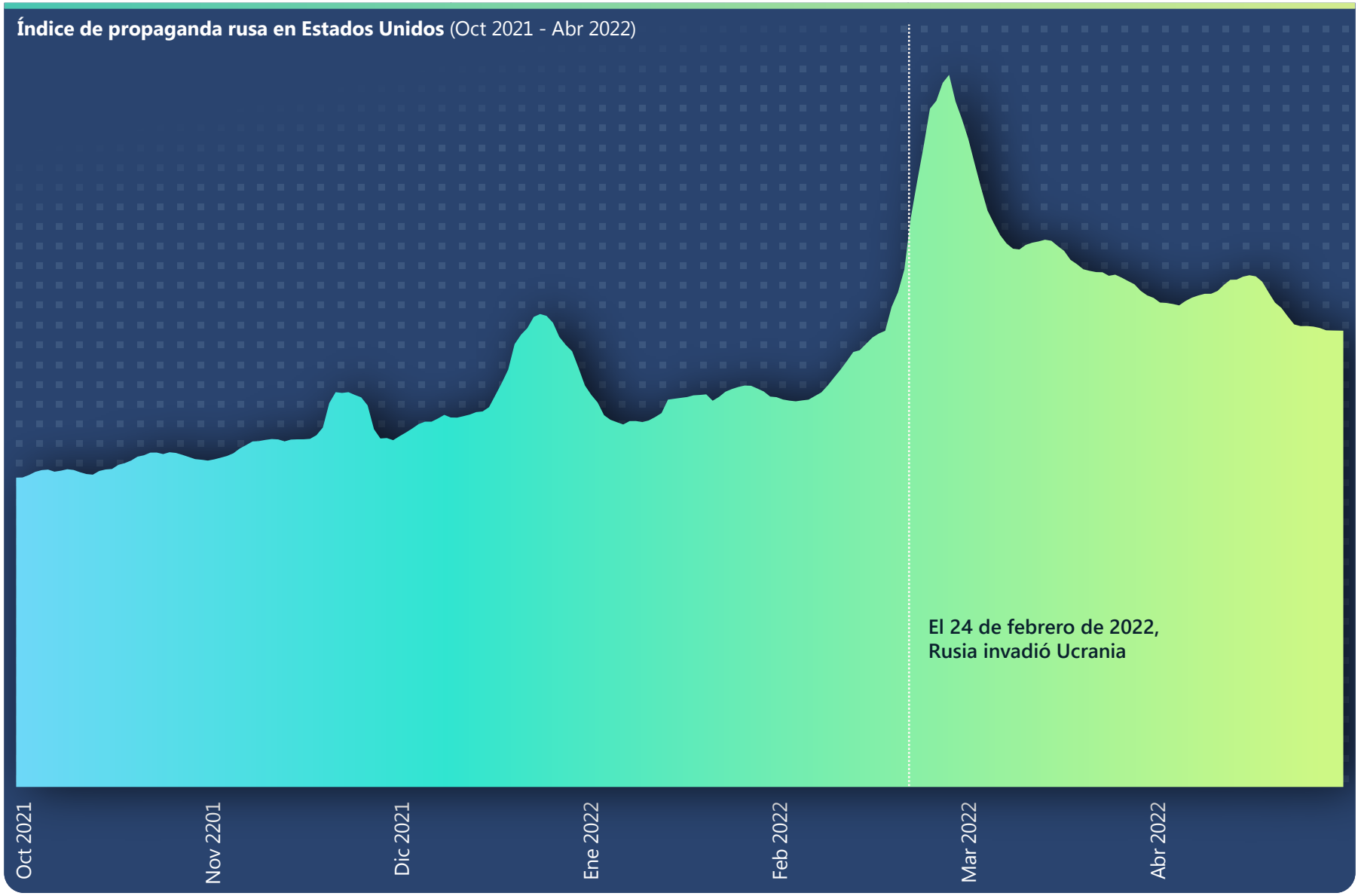
Vínculos a más información

- La defensa de Ucrania: Primeras lecciones de la guerra cibernética | Microsoft On the Issues
- Resumen de la actividad de ciberataques de Rusia en Ucrania | Microsoft Special Report
- Interrupción de los ciberataques dirigidos a Ucrania | Microsoft On the Issues

Seguimiento del Índice de propaganda rusa

En enero de 2022, casi mil sitios web estadounidenses remitían tráfico a sitios web de propaganda rusa. Los temas más comunes de los sitios web de propaganda rusa dirigidos a un público estadounidense fueron la guerra en Ucrania, la política interna de Estados Unidos (ya sea a favor de Trump o de Biden) y las narraciones relacionadas con el COVID-19 y las vacunas.

El Índice de propaganda rusa (IPR) supervisa el flujo de noticias de los medios de comunicación y amplificadores rusos, controlados y patrocinados por el estado, como proporción del tráfico total de noticias en Internet. El RPI puede utilizarse para trazar el consumo de propaganda rusa en Internet y en diferentes zonas geográficas en una línea de tiempo precisa. Sin embargo, Microsoft señala que solo podemos observar la propaganda rusa publicada en sitios web previamente identificados. No tenemos información sobre la propaganda en otros tipos de sitios web, incluidos los sitios web de noticias autorizadas, los sitios web no identificados y los grupos de redes sociales.



Seguimiento del Índice de propaganda rusa

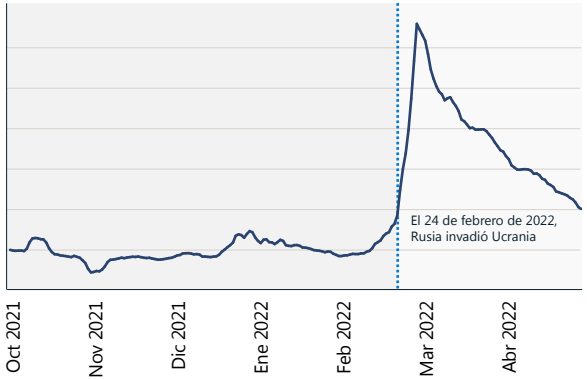
Continuación

Índice de propaganda rusa: Ucrania

Cuando comenzó la guerra de Ucrania, vimos un aumento del 216 % en la propaganda rusa, que alcanzó su punto máximo el 2 de marzo. El gráfico siguiente muestra cómo este repentino aumento coincidió con la invasión. Los dos gráficos muestran cómo la propaganda rusa se disparó poco después del inicio de la invasión.

RPI, Ucrania

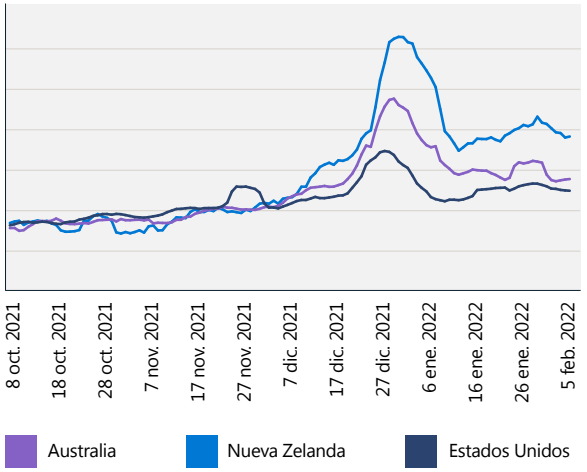
(7 de octubre de 2021 al 30 de abril de 2022)



Índice de propaganda rusa: Nueva Zelanda frente a Australia y Estados Unidos

Una evaluación del RPI en Nueva Zelanda mostró un pico a finales de 2021 que estaba relacionado con la propaganda de COVID-19. Este repunte del consumo de propaganda rusa en Nueva Zelanda precedió a un aumento de las protestas públicas a principios de 2022 en Wellington. Un segundo pico estuvo claramente relacionado con la invasión rusa de Ucrania y superó los RPI de Australia y Estados Unidos.

RPI, Nueva Zelanda frente a Australia y los Estados Unidos



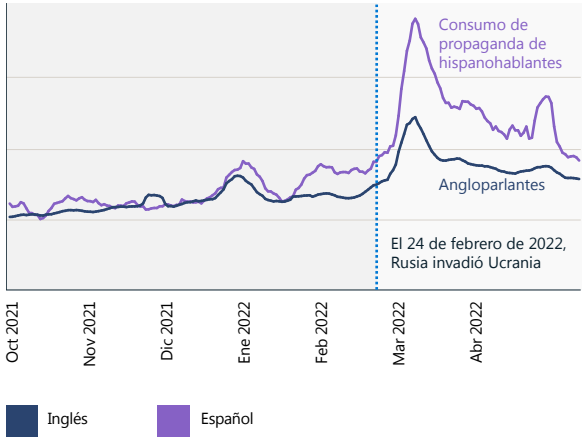
El consumo de propaganda rusa en Nueva Zelanda es similar al de Australia hasta la primera semana de diciembre de 2021. Después de diciembre, el consumo de propaganda rusa en Nueva Zelanda aumentó más del 30 % en relación con el consumo en Australia y Estados Unidos.

Índice de propaganda rusa en los Estados Unidos: inglés y español

El RPI también hace un seguimiento de la propaganda en todas las lenguas. Múltiples medios, como RT y Sputnik News, están disponibles en más de 20 idiomas. Entre ellos están el inglés, el español, el alemán, el francés, el griego, el italiano, el checo, el polaco, el serbio, el letón, el lituano, el moldavo, el bielorruso, el armenio, el osetio, el georgiano, el azerí, el árabe, el turco, el persa y el dari.

El siguiente gráfico muestra que el RPI de las noticias en español en Estados Unidos es mucho mayor que el de las noticias en inglés.

El consumo de propaganda rusa es 2 veces mayor entre los hispanohablantes



El consumo de propaganda rusa en Estados Unidos es dos veces mayor entre los hispanohablantes.

La propaganda rusa es alta en Latinoamérica

RT en español es el medio de comunicación internacional con mayor número de páginas vistas y de seguidores en Facebook.

Fuente: Microsoft AI for Good Research Lab

Medios sintéticos

Estamos entrando en una era dorada para la creación y manipulación de medios con IA. Los analistas de Microsoft señalan que esto se debe a dos tendencias clave: la proliferación de herramientas y servicios fáciles de usar para crear artificialmente imágenes, videos, audio y texto sintéticos de gran realismo, y la capacidad de difundir con rapidez contenidos optimizados para audiencias específicas.

Ninguno de estos desarrollos es intrínsecamente problemático por sí mismo. La tecnología basada en la IA puede utilizarse para crear contenidos digitales divertidos y emocionantes, ya sea creando material puramente sintético o mejorando el existente. Estas herramientas están siendo muy utilizadas por las empresas para la publicidad y la comunicación y por los particulares para crear contenidos atractivos para sus seguidores. Sin embargo, los medios de comunicación sintéticos, cuando se crean y distribuyen con la intención de dañar, tienen el potencial de causar graves daños a las personas, las empresas, las instituciones y la sociedad. Microsoft ha sido una fuerza impulsora en el desarrollo de tecnologías y prácticas, tanto a nivel interno como en todo el ecosistema de los medios de comunicación, para limitar este daño.

Esta sección explora las ideas del análisis de Microsoft sobre el estado actual de la tecnología para crear contenido sintético perjudicial, los daños que pueden surgir si este contenido se difunde de forma amplia, y las mitigaciones técnicas que pueden defender contra las ciberamenazas basadas en medios sintéticos.

Creación de medios sintéticos

El campo del texto y los medios de comunicación sintéticos está avanzando a una velocidad increíble, ya que técnicas que antes solo eran posibles con los vastos recursos informáticos de los grandes estudios cinematográficos se integran ahora en aplicaciones para teléfonos. Al mismo tiempo, las herramientas son cada vez más fáciles de usar y pueden generar contenidos con un nivel de realismo que puede engañar incluso a los especialistas en medios forenses. Estamos muy cerca de alcanzar el punto en el que cualquiera puede crear un video sintético de cualquier persona diciendo o haciendo cualquier cosa. No es descabellado pensar que estamos entrando en una era en la que una cantidad importante de los contenidos que vemos en Internet son total o parcialmente sintéticos mediante técnicas de IA.

> Con la disponibilidad de herramientas más sofisticadas, fáciles de usar y ampliamente disponibles, la creación de contenidos sintéticos va en aumento y pronto será indistinguible de la realidad.

Hay muchas herramientas de edición de imagen, video y audio, gratuitas y comerciales, de gran calidad. Estas herramientas pueden utilizarse para realizar cambios sencillos pero potencialmente perjudiciales en los contenidos digitales, como agregar texto engañoso, intercambiar caras y eliminar o alterar el contexto. Estas "falsificaciones baratas" se utilizan ampliamente para difundir contenidos nefastos, promover ideologías políticas y dañar la reputación. Un ejemplo conocido es el video de 2019[16] de la presidenta de la Cámara de Representantes de Estados Unidos, Nancy Pelosi, arrastrando las palabras y pareciendo ebria. Aunque se determinó con rapidez que el video estaba ralentizado para crear el efecto, la "falsificación barata" se difundió mucho antes de que salieran a la luz el video original y el contexto.

Los enfoques más sofisticados para alterar el contenido de los medios de comunicación incluyen la aplicación de técnicas avanzadas de IA para (a) crear medios de comunicación puramente sintéticos, y (b) realizar ediciones más sofisticadas de los medios existentes. El término "deepfake" se utiliza a.menudo para los medios sintéticos que se crearon mediante técnicas de IA de vanguardia (el nombre proviene de las redes neuronales profundas que a veces se utilizan). Estas tecnologías se están desarrollando como aplicaciones, herramientas y servicios independientes y se están integrando en herramientas de edición comerciales y de código abierto.

Estas tecnologías se utilizan como armas por los malos actores que esperan dañar a las personas e instituciones. Algunos ejemplos de técnicas de "deepfake" son:

- **Intercambio de caras (video, imágenes)**: reemplazar una cara en un video por otra. Esta técnica puede utilizarse para intentar chantajear a una persona, empresa o institución, o para colocar a personas en lugares o situaciones embarazosas.
- **Titiriteros (video, imágenes)**: usar un video para animar una imagen fija o un segundo video. Esto puede hacer que parezca que una persona ha dicho algo vergonzoso o engañoso.
- **Redes generativas antagónicas (video, imágenes)**: una familia de técnicas para generar imágenes fotorrealistas.
- **Modelos de transformadores (video, imágenes, texto)**: crear imágenes ricas a partir de descripciones de texto.

Estas técnicas avanzadas basadas en la IA todavía no se utilizan de forma generalizada en las campañas de ciberinfluencia, pero esperamos que el problema crezca a medida que las herramientas sean más fáciles de usar y estén más disponibles.

El impacto de la manipulación de los medios sintéticos

El uso de operaciones de información para causar daño o ampliar la influencia no es nuevo. Sin embargo, la velocidad con la que se difunde la información y nuestra incapacidad para distinguir con rapidez la realidad de la ficción hacen que el impacto y el daño provocado por las falsificaciones y otros medios malintencionados generados de forma sintética puedan ser mucho mayores, como se ha demostrado con el ejemplo de Pelosi.

Hay varias categorías de daños que consideramos: manipulación del mercado, fraude en los pagos, vishing, su plantación de identidad, daño a la marca, daño a la reputación y redes de robots. Muchas de estas categorías tienen ejemplos del mundo real ampliamente difundidos, lo que podría socavar nuestra capacidad de separar los hechos de la ficción.

Una amenaza más a largo plazo y más insidiosa es la que se cierne sobre nuestra comprensión de la verdad si ya no podemos confiar en lo que vemos y oímos. Por ello, cualquier imagen, audio o video comprometedor de un personaje público o privado puede descartarse como falso, un resultado conocido como "El dividendo del mentiroso".[17] Investigaciones recientes[18] muestran que este abuso de la tecnología ya se está utilizando para atacar los sistemas financieros, aunque hay muchos otros escenarios de abuso que son plausibles.

Medios sintéticos

Continuación

Detección de medios sintéticos

La industria, el gobierno y el mundo académico se esfuerzan por desarrollar mejores formas de detectar y mitigar los medios sintéticos y restaurar la confianza. Hay varias vías prometedoras para avanzar, así como barreras que merecen consideración.

Uno de los enfoques consiste en crear sistemas basados en la IA que puedan detectar las falsificaciones, es decir, sistemas de IA "defensivos"3para contrarrestar los sistemas d IA ofensivos. Se trata de un área de investigación activa en la que los sistemas actuales de creación de audio y video sintéticos dejan artefactos reveladores que analistas forenses capacitados de medios y herramientas automatizadas pueden detectar.

Por desgracia, aunque las falsificaciones actuales tienen fallas reveladoras, los artefactos precisos tienden a ser específicos de una herramienta o algoritmo concreto. Esto significa que el entrenamiento con falsificaciones conocidas no suele generalizarse a otros algoritmos, como se demostró en un concurso abierto de 2020 para construir detectores de "deepfake".[19] Resulta tentador aumentar la inversión en el desarrollo de detectores más avanzados, pero Microsoft es muy escéptica de que esto se traduzca en mejoras significativas por dos razones:

En primer lugar, disponemos de excelentes modelos físicos que reflejan el mundo real. Los actuales creadores de falsificaciones recortan las distancias, lo que da lugar a artefactos detectables, pero los nuevos modelos serán cada vez más realistas. No hay nada inherentemente especial en una escena del mundo real captada por una cámara que no pueda modelarse con un equipo.

En segundo lugar, los algoritmos avanzados de creación de falsificaciones utilizan una técnica llamada Redes generativas antagónicas (GAN) como parte del proceso de creación. Una GAN enfrenta a dos sistemas de IA utilizando un generador para crear la falsificación y un discriminador para detectar las imágenes falsas y entrenar al generador. Cualquier inversión en el desarrollo de un mejor detector solo permitirá al generador mejorar la calidad de las falsificaciones.

Panorama de los medios sintéticos

Factores Baja barrera de entrada	Herramientas fáciles de usar	Herramientas más sofisticadas	Fácil distribución	
Productores Usos buenos y perjudiciales	Organizaciones e instituciones	Personas y consumidores	Actores malintencionados para causar daños	
Distribución Velocidad sin precedentes	Amplificación de redes sociales	Correos electrónicos dirigidos y anuncios	Archivos de audio a través de correo de voz	Directo desde el origen
Efectos Erosión de la confianza	Daño a la reputación individual	Fraude y otros daños financieros	Daño a la organización o marca	Manipulación del mercado
Mitigación Soluciones prometedoras	Sistemas avanzados de IA para la detección	Procedencia digital	Esfuerzos entre las industrias	

Medios sintéticos

Continuación

Procedencia de los activos digitales

Si la detección de falsificaciones no es confiable, ¿qué se puede hacer para protegerse de los usos nocivos de los medios sintéticos? Una importante tecnología emergente es la procedencia digital, un mecanismo que permite a los creadores de medios digitales certificar un activo y ayuda a los consumidores a identificar si el activo digital se manipuló o no. La procedencia digital es muy importante en el contexto de las redes sociales actuales, dada la velocidad con la que los contenidos pueden recorrer Internet y la posibilidad de que los malos actores manipulen con facilidad los contenidos.

900 %

de aumento interanual de la proliferación de "deepfakes" desde 2019.[20]

La tecnología de procedencia digital es una versión moderna de la firma criptográfica de documentos, diseñada para capturar el origen, el historial de edición y los metadatos de los objetos a medida que fluyen por la web actual. Un equipo interdisciplinario de investigadores y científicos de Microsoft desarrolló la visión y los métodos técnicos para hacer posible este tipo de certificación de extremo a extremo a prueba de manipulaciones de los medios. Codirigimos una asociación intersectorial destinada a dar vida a la tecnología de procedencia de los medios en Project Origin (fundado por Microsoft, BBC, CBC/Radio-Canada y el New York Times) y participamos en la Iniciativa de autenticidad de los contenidos (fundada por Adobe). Microsoft también ha colaborado con socios de servicios tecnológicos y de medios de comunicación para crear la Coalition for Content Provenance and Authenticity (C2PA). C2PA es una organización de normalización que ha publicado hace poco la especificación de procedencia digital más avanzada para utilizar con activos de medios de comunicación como imágenes, videos, audio y texto.

Un objeto habilitado para C2PA lleva un manifiesto que protege el objeto y los metadatos de la manipulación, y elcertificado que lo acompaña identifica al editor.

Los medios sintéticos no se diseñaron originalmente para causar daño, pero los malos actores están utilizándolos como armas para socavar la confianza en las personas e instituciones.

La procedencia digital es una prometedora tecnología emergente que tiene el potencial de ayudar a restaurar la confianza de la gente en los contenidos de los medios de comunicación en línea al certificar el origen de un activo de medios.

Las soluciones disponibles públicamente basadas en la especificación C2PA están apareciendo como una nueva función en los productos existentes o como nuevas aplicaciones y servicios independientes. Esperamos que la mayoría de las herramientas de captura, edición y creación más utilizadas estén habilitadas para C2PA en unos años. Esto supone una oportunidad para que las empresas determinen sus necesidades y usos de la procedencia digital en la actualidad, y exijan esta capa adicional de protección en las herramientas que utilizan en los flujos de trabajo existentes.

Información práctica

1. Tome medidas proactivas para proteger a su organización contra las amenazas de desinformación mediante la consideración proactiva de sus respuestas de relaciones públicas y comunicación.
2. Utilice la tecnología de procedencia para proteger las comunicaciones oficiales.

Vínculos a más información

- Un avance prometedor en materia de desinformación | Microsoft On the Issues
- A Milestone Reached, 31 de enero de 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Explore los detalles técnicos del sistema que utiliza Project Origin para la autentificación de medios | Microsoft ALT Innovation

Un enfoque holístico para protegerse de las operaciones de influencia cibernética

Microsoft está aprovechando su ya madura infraestructura de inteligencia sobre ciberamenazas para desarrollar una visión más amplia e inclusiva de las operaciones de ciberinfluencia.

Utilizamos un marco para sugerir estrategias de respuesta y mitigación para combatir la amenaza que suponen las operaciones, que puede dividirse en cuatro pilares clave: detectar, interrumpir, defender y disuadir.

Además, Microsoft ha adoptado cuatro principios para anclar nuestro trabajo en este espacio. Lo primero es el compromiso de respetar la libertad de expresión y defender la capacidad de nuestros clientes para crear, publicar y buscar información a través de nuestras plataformas, productos y servicios. En segundo lugar, trabajamos de forma proactiva para evitar que nuestras plataformas y productos se utilicen para amplificar sitios y contenidos extranjeros de ciberinfluencia. En tercer lugar, no nos beneficiaremos voluntariamente de contenidos o actores extranjeros de ciberinfluencia. Por último, damos prioridad ala aparición de contenidos para contrarrestar las operaciones de ciberinfluencia extranjeras utilizando datos internos y de terceros de confianza sobre nuestros productos.

Detección

Al igual que en el caso de la ciberdefensa, el primer paso para contrarrestar las operaciones de ciberinfluencia extranjeras es desarrollar la capacidad de detectarlas. Ninguna empresa u organización puede esperar realizar individualmente los progresos necesarios. Será crucial una nueva y más amplia colaboración en el sector tecnológico, y los avances en el análisis y la denuncia de las operaciones de ciberinfluencia dependerán en gran medida del papel de la sociedad civil, incluso en instituciones académicas y organizaciones sin ánimo de lucro.

Reconociendo este papel, los investigadores Jake Shapiro y Alicia Wanless de la Universidad de Princeton y la Fundación Carnegie para la Paz Internacional, respectivamente, han trazado planes para lanzar el nuevo "Institute for Research on the Information Environment" (IRIE, Instituto de investigación sobre el entorno de la información). Con el apoyo de Microsoft, la Fundación Knight y Craig Newmark Philanthropies, el IRIE creará una institución de investigación inclusiva con varias partes interesadas, siguiendo el modelo de la Organización Europea para la E Investigación Nuclear (CERN). Combinará la experiencia en el procesamiento y análisis de datos para acelerar y ampliar los nuevos descubrimientos en este espacio. Los resultados se compartirán para informar a los responsables políticos, las empresas tecnológicas y los consumidores en general.

Defensa

El segundo pilar estratégico es reforzar las defensas democráticas, una prioridad de larga data que necesita inversión e innovación. Debe tener en cuenta los desafíos que la tecnología ha creado para la democracia, y las oportunidades que la tecnología ha creado para defender las sociedades democráticas con mayor eficacia.

El marco estratégico de Microsoft tiene como objetivo ayudar a las partes interesadas intersectoriales a detectar, interrumpir, defender y disuadir de la propaganda, en especial de las campañas de agresores extranjeros.

Conviene empezar por uno de los grandes desafíos tecnológicos de nuestra época: el impacto de Internet y la publicidad digital en el periodismo tradicional. Desde el año 1700, una prensa libre e independiente ha desempeñado un papel especial en el apoyo a todas las democracias del planeta, descubriendo la corrupción, documentando las guerras e iluminando los mayores desafíos sociales de esta y otras épocas. Sin embargo, Internet ha destruido las noticias locales al devorar los ingresos por publicidad y atraer a los suscriptores de pago. Muchos periódicos locales se han hundido. Una de las tantas conclusiones de nuestro reciente trabajo es que las ciudades que carecen de periódico están expuestas, sin saberlo, a un volumen de propaganda extranjera superior a la media. Por estos motivos, uno de los pilares defensivos de la democracia debe fortalecer el periodismo tradicional y la prensa libre, sobre todo a nivel local. Esto requiere una inversión e innovación constantes que deben reflejar las necesidades locales de los distintos países y continentes. Estas cuestiones no son fáciles y requieren enfoques de varias partes interesadas, que Microsoft y otras empresas tecnológicas apoyan cada vez más. También necesitamos nuevas innovaciones en las políticas públicas, que deben ser una prioridad pública. Esto puede incluir leyes que permitan a los editores negociar los ingresos publicitarios de forma colectiva con las empresas tecnológicas, y legislación que proporcione créditos fiscales para aliviar a las redacciones locales de una parte de sus impuestos sobre las nóminas de los periodistas que emplean. Los periodistas necesitan muchas otras herramientas para su oficio, incluida la capacidad de separar los contenidos de fuentes legítimas y fraudulentas.

También existe la necesidad de ayudar a los consumidores a desarrollar una capacidad más sofisticada para identificar las operaciones de información impulsadas por el estado nación. Aunque esto pueda parecer desalentador, se asemeja al trabajo que el sector tecnológico lleva a cabo desde hace tiempo para combatir otras ciberamenazas. Considere la posibilidad de educar a los consumidores para que miren con más atención una dirección de correo electrónico para ayudar a detectar el correo no deseado u otras comunicaciones fraudulentas. Las iniciativas en Estados Unidos, como el News Literacy Project y el Trusted Journalism

Una amenaza más a largo plazo y más insidiosa es la que se cierne sobre nuestra comprensión de la verdad si ya no podemos confiar en lo que vemos y oímos.

Un enfoque holístico para protegerse de las operaciones de influencia cibernética

Continuación

Program, están ayudando a desarrollar consumidores de noticias e información mejor informados. A nivel mundial, una nueva tecnología como el complemento para explorador de NewsGuard puede ayudar a que este esfuerzo avance mucho más rápido.

Esto también debería recordarnos que parte de la base de la democracia es la educación cívica. Como siempre, este esfuerzo debe comenzar en las escuelas. Pero vivimos en un mundo que requiere que recibamos una educación cívica continua a lo largo de nuestra vida. El nuevo compromiso de Civismo en el trabajo, liderado por el Centro de Estudios Estratégicos e Internacionales (Center for Strategic and International Studies), y del que Microsoft fue uno de los firmantes y socios inaugurales, pretende revitalizar la alfabetización cívica en las comunidades empresariales. Es un buen ejemplo de la amplitud de oportunidades para reforzar nuestras defensas democráticas.

Interrupción

En los últimos años, la Unidad de delitos digitales (DCU) de Microsoft ha perfeccionado las tácticas y desarrollado herramientas para desbaratar ciberamenazas que van desde el ransomware hasta las redes de robots y los ataques de estados nación. Hemos aprendido muchas lecciones fundamentales, empezando por el papel de la interrupción activa para contrarrestar una amplia gama de ciberataques.

Al pensar en contrarrestar las operaciones de ciberinfluencia, la interrupción podría desempeñar un papel aún más importante y el mejor enfoque de la interrupción se está aclarando. El antídoto más eficaz contra el engaño generalizado es la transparencia. Por este motivo, Microsoft ha aumentado su capacidad para detectar e interrumpir las operaciones de influencia de los estados nación mediante la adquisición de Miburo Solutions, una empresa líder en análisis e investigación de ciberamenazas especializada en la detección y respuesta a las operaciones de ciberinfluencia extranjeras.

Nuestra experiencia ha demostrado que los gobiernos, las empresas tecnológicas y las ONG deben atribuir los ciberataques con cuidado y con amplias pruebas. Comprender el impacto de dicha perturbación es vital y puede ser aún más útil para desbaratar la influencia cibernética. El intercambio de información por parte del gobierno de EE. UU. en el período previo a la invasión rusa de Ucrania puso en práctica la transparencia, al exponer los planes rusos, incluyendo campañas específicas, como un complot para utilizar un video gráfico falso.

Como se muestra en la publicación del verano pasado del CyberPeace Institute de Ginebra sobre los ciberataques en curso dentro y fuera de Ucrania, existe una oportunidad para que una amplia gama de organizaciones de la sociedad civil y del sector privado promuevan la transparencia en relación con las operaciones de ciberinfluencia. Los informes confiables sobre operaciones recién descubiertas y bien documentadas pueden ayudar al público a evaluar mejor lo que lee, ve y oye, sobre todo en Internet. Para ello, Microsoft se basará en sus actuales informes cibernéticos y los ampliará, y publicará nuevos informes, datos y actualizaciones relacionados con lo que descubramos sobre las operaciones de ciberinfluencia, incluyendo declaraciones de atribución cuando proceda. Publicaremos un informe anual que utilice un enfoque basado en datos para examinar en toda la empresa la prevalencia de las operaciones de información en el extranjero y los próximos pasos para garantizar una mejora progresiva. También estudiaremos otras medidas que se basen en este tipo de transparencia.

El papel de la publicidad digital es de suma importancia, por ejemplo, ya que la publicidad puede ayudar a financiar las operaciones extranjeras y, al mismo tiempo, crear una apariencia de legitimidad para los sitios de propaganda patrocinados por el extranjero. Serán necesarios nuevos esfuerzos para interrumpir estos flujos financieros.

Disuasión

Por último, no podemos esperar que las naciones cambien de comportamiento si no hay responsabilidad por la infracción de las normas internacionales. La aplicación de esta responsabilidad pertenece exclusivamente al gobierno. No obstante, cada vez más, la acción de las varias partes interesadas está desempeñando un papel importante en el fortalecimiento y la ampliación de las normas internacionales. Más de 30 plataformas, anunciantes y editores en línea (entre ellos Microsoft) han firmado el recién actualizado Código de buenas prácticas en materia de desinformación de la Comisión Europea, acordando compromisos reforzados para hacer frente a este creciente desafío. Al igual que el reciente Llamado de París, el Llamado de Christchurch y la Declaración sobre el futuro de Internet, la acción multilateral y de varias partes interesadas puede reunir a los gobiernos y al público de las naciones democráticas. Los gobiernos pueden entonces basarse en estas normas y leyes para promover la responsabilidad que las democracias del mundo necesitan y merecen.

A través de una rápida transparencia radical, los gobiernos y las sociedades democráticas pueden contrarrestar con eficacia las campañas de influencia atribuyendo el origen de los ataques del estado nación, informando al público y creando confianza en las instituciones.

> Hemos aumentado la capacidad técnica para detectar y desbaratar operaciones de influencia extranjera y nos comprometemos a informar de forma transparente sobre estas operaciones, al igual que lo hacemos con los ciberataques.

Información práctica

1. Implemente sólidas prácticas de higiene digital en toda su organización.
2. Considere las formas de reducir cualquier habilitación involuntaria de las campañas de ciberinfluencia por parte de sus empleados o de sus prácticas empresariales. Esto incluye la reducción del suministro a sitios de propaganda extranjeros conocidos.
3. Apoye las campañas de alfabetización informativa y compromiso cívico como componente clave para ayudar a las sociedades a defenderse de la propaganda y la influencia extranjera.
4. Comprométase directamente con los grupos correspondientes para su industria que trabajan para abordar las operaciones de influencia.

Notas finales

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. La defensa de Ucrania: Primeras lecciones de la guerra cibernética (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_ FullReport pdf
5. La portavoz del Ministerio de Asuntos Exteriores ruso, Maria Zakharova: https://tass.com/politics/1401777; Lavrov:https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Russia's Kremenchuk Claims Versus the Evidence—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas, and Kristjan Peterson, octubre de 2020

Resiliencia cibernética

Comprender los riesgos y las recompensas de la modernización resulta crucial para un enfoque holístico de la resiliencia.

Información general de la resiliencia cibernética

La seguridad cibernética es un factor clave del éxito tecnológico. La innovación y la mejora de la productividad solo pueden conseguirse al introducir medidas de seguridad que hagan a las organizaciones lo más resilientes posible contra los ataques modernos.

La pandemia nos ha desafiado a dar un giro a nuestras prácticas y tecnologías de seguridad para proteger a los empleados de Microsoft dondequiera que trabajen. El año pasado, los actores de amenaza continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido administrar la prevalencia y la complejidad de diversos métodos de ataque y el aumento de la actividad de los estados nación.

Una resiliencia cibernética eficaz requiere un enfoque holístico y adaptable para resistir las amenazas cambiantes a los servicios e infraestructuras básicos.

Más información en la página 89

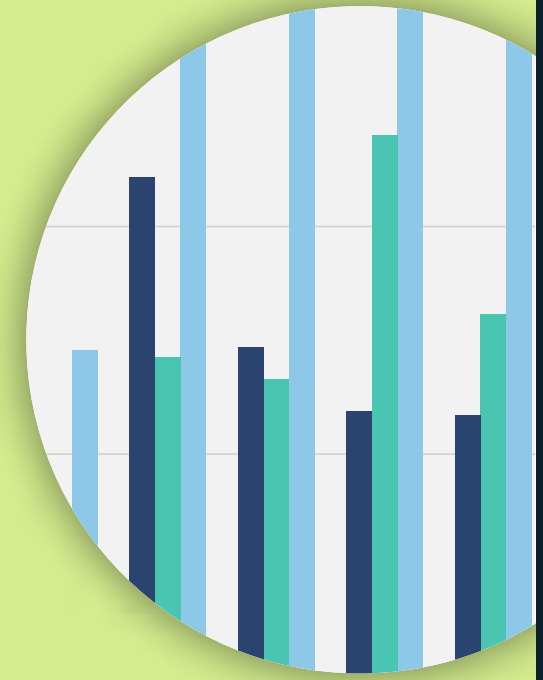
La modernización de los sistemas y la arquitectura son importantes para administrar las amenazas en un mundo hiperconectado.

Más información en la página 90

La postura de seguridad básica es un factor determinante en la eficacia de las soluciones avanzadas.

Más información en la página 92

Aunque los ataques basados en contraseñas siguen siendo la principal fuente de compromiso de la identidad, están surgiendo otros tipos de ataques.



Más información en la página 93

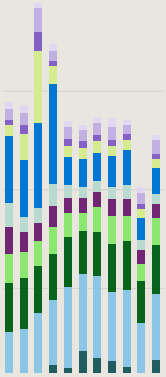
La dimensión humana de la resiliencia a las operaciones de ciberinfluencia es nuestra capacidad para colaborar y cooperar.

Más información en la página 102

La gran mayoría de los ciberataques que tienen éxito podrían evitarse utilizando una higiene de seguridad básica.

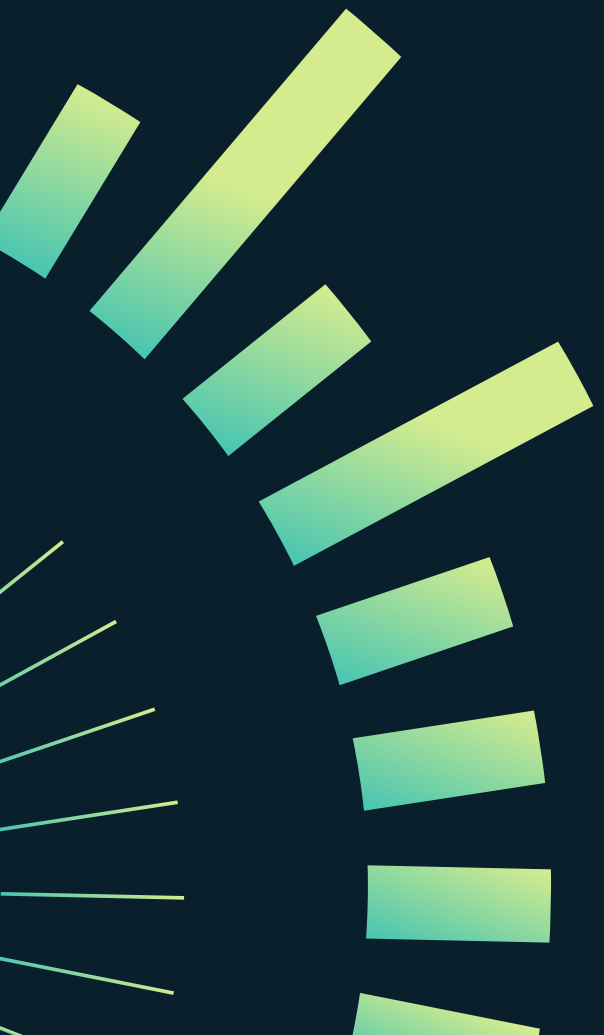
Más información en la página 108

Durante el año pasado, el mundo experimentó una actividad DDoS sin precedentes en cuanto a volumen, complejidad y frecuencia.



Más información en la página 98

Introducción



La pandemia nos desafió a dar un giro a nuestras prácticas y tecnologías de seguridad para proteger a los empleados de Microsoft dondequiera que trabajen. El año pasado, los actores de amenaza continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y. el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido administrar la prevalencia y la complejidad de diversos métodos de ataque y el aumento de la actividad de los estados nación.

La actividad de las amenazas digitales y el nivel de sofisticación de los ciberataques aumenta cada día. Muchos de los complejos ataques actuales se centran en comprometer las arquitecturas de identidad, las cadenas de suministro y las terceras partes con diversos grados de controles de seguridad. En especial, hemos observado que los ataques de suplantación de identidad (phishing) son una amenaza clara y presente. Sin embargo, este tipo de ataques suelen no tener éxito con una buena administración de identidades, control de phishing y prácticas de administración de puntos de conexión. Por lo tanto, debemos recordar lo básico: el 98 % de los ataques pueden detenerse con medidas básicas de higiene. En Microsoft, administramos las identidades y los dispositivos como parte de nuestro enfoque de Confianza cero, que incluye el acceso menos privilegios y las credenciales resistentes al phishing para detener eficazmente a los actores de amenaza y mantener nuestros datos protegidos.

Hoy en día, incluso los actores de amenaza que carecen de conocimientos técnicos sofisticados pueden lanzar ataques increíblemente destructivos, ya que el acceso a tácticas, técnicas y procedimientos avanzados está ampliamente disponible en la economía de la ciberdelincuencia. La guerra en Ucrania demostró cómo los actores de los estados nación han intensificado sus operaciones cibernéticas ofensivas a través del aumento del uso de ransomware. El ransomware es ahora una industria sofisticada, con actores de amenazas que utilizan tácticas de doble o triple extorsión para extraer un pago y desarrolladores que ofrecen ransomware como servicio (RaaS). Con RaaS, los actores de las amenazas utilizan una red de afiliados para llevar a cabo los ataques, reduciendo la barrera de entrada para los ciberdelincuentes menos cualificados y, en última instancia, ampliando el grupo de atacantes.

En consecuencia, Microsoft diseñó un programa de eliminación de ransomware. El objetivo del programa es subsanar las deficiencias en los controles y la cobertura, contribuir a la mejora de las funciones de los servicios y desarrollar manuales de recuperación para nuestro centro de operaciones de seguridad y los equipos de ingeniería en caso de ataque de ransomware.

Los recientes ataques a la cadena de suministro y a los proveedores externos indican un importante punto de inflexión en el sector. Los trastornos que estos ataques provocan a nuestros clientes, socios, gobiernos y a Microsoft siguen aumentando, lo que ilustra la importancia de centrar la atención en la resiliencia cibernética y la colaboración entre las partes interesadas en la seguridad. Los adversarios también atacan los sistemas locales, lo que refuerza la necesidad de que las organizaciones administren las vulnerabilidades que plantean los sistemas heredados mediante la modernización y el traslado de la infraestructura a la nube, donde la seguridad es más sólida.

Vivimos en una época en la que la seguridad es un factor clave del éxito tecnológico. La innovación y la mejora de la productividad solo pueden conseguirse al introducir medidas de seguridad que hagan a las organizaciones lo más resilientes posible contra los ataques modernos. A medida que las amenazas digitales aumentan y evolucionan, es crucial incorporar la resiliencia cibernética en el tejido de cada organización.

Bret Arsenault
Director de seguridad de la información

Resiliencia cibernética: Una base crucial para una sociedad conectada

La revolución de la tecnología digital ha hecho que las organizaciones se transformen para estar cada vez más conectadas tanto en su funcionamiento como en los servicios que ofrecen. A medida que crecen las amenazas en el panorama cibernético, el desarrollo de la resiliencia cibernética en el tejido de la organización es tan esencial como la resiliencia financiera y operativa.

La transformación digital ha alterado para siempre la forma en que las organizaciones interactúan con los clientes, los socios, los empleados y otras partes interesadas. Las nuevas tecnologías ofrecen enormes oportunidades para relacionarse con las personas, transformar los productos y optimizar las operaciones. La pandemia aceleró la transformación digital al impulsar tecnologías innovadoras que permiten a las personas colaborar de nuevas maneras y desde cualquier lugar.

A medida que las ciberamenazas se vuelven endémicas, se torna más difícil evitar que comprometan a una organización en nuestro mundo "siempre conectado". La resiliencia cibernética representa la capacidad de una organización para continuar con las operaciones y mantener la aceleración del crecimiento a pesar del aluvión de ataques. La prevención tiene que equilibrarse con la capacidad de supervivencia y recuperación, y los gobiernos y las empresas están desarrollando modelos integrales que van más allá de la seguridad y la privacidad para proteger los activos, los datos y otros recursos como parte de la resiliencia cibernética.

Desarrollar un enfoque integral para la resiliencia cibernética

La resiliencia cibernética requiere un enfoque holístico, adaptable y global que pueda resistir las amenazas cambiantes a los servicios e infraestructuras básicos, lo que incluye:

- La higiene cibernética básica descrita en nuestra curva de campana de la resiliencia cibernética.
- La comprensión y administración de la relación riesgo/recompensa de la transformación digital.
- Las capacidades de respuesta en tiempo real que permiten la detección proactiva de amenazas y vulnerabilidades.
- La protección contra ataques conocidos y actividad preventiva contra los vectores de ataque nuevos y previstos, incluida la capacidad de corrección automática.
- El menor impacto de los ataques y desastres mediante el aislamiento y la segmentación de las fallas.
- La recuperación automática y redundancia en caso de interrupción.
- La priorización de las pruebas operativas para encontrar las brechas y comprender las responsabilidades compartidas y las dependencias de los recursos externos, como las soluciones de seguridad basadas en la nube.

Un programa eficaz de resiliencia cibernética comienza con los fundamentos de los recursos, como conocer los servicios disponibles y tener un catálogo confiable de recursos a los que se puede recurrir en caso de interrupción. Partiendo de esta base, el programa debe ser capaz de evaluar su propia eficacia, medir el rendimiento de los servicios críticos y sus dependencias, probar y validar las capacidades en los servicios locales y en la nube, y alimentar la mejora continua en todo el ciclo de vida digital de la organización.

Para ofrecer un enfoque integral, nos asociamos con las organizaciones para identificar sus servicios locales y en línea, procesos empresariales, dependencias, personal, vendedores y proveedores más críticos. También buscamos identificar los activos y recursos asociados a las expectativas de los clientes y del mercado, las obligaciones reglamentarias y contractuales y las operaciones internas. A medida que se identifican estos recursos críticos, los esfuerzos paralelos tienen que detectar y supervisar las amenazas, las interrupciones, los posibles vectores de ataque y las vulnerabilidades de los sistemas y procesos. La capacidad de hacer esto en el marco de la actual escasez de competencias requiere rigor en la priorización basada en el riesgo global que supone para la organización.

Este tipo de enfoque holístico tiene que ser adaptable en un contexto de un panorama de amenazas en continua evolución, con el objetivo de impulsar una mejora medible del rendimiento, reducir el tiempo de detección, respuesta y recuperación, y reducir el radio de impacto en caso de interrupción. El enfoque también tiene que reconocer la creciente conexión de las amenazas. Por ejemplo, un incidente de seguridad puede dar lugar a una vulneración de datos con implicaciones para la privacidad, lo que requiere que muchos equipos internos y externos trabajen juntos para responder con celeridad y minimizar el impacto.

La resiliencia cibernética es la capacidad de una empresa para continuar las operaciones y mantener la aceleración del crecimiento a pesar de las interrupciones, incluidos los ciberataques.

Información práctica

1. Cree y administre sistemas tecnológicos que limiten el impacto de una brecha y les permitan seguir operando con seguridad y eficacia, incluso si una brecha tiene éxito. Enfóquese en los activos críticos comunes, apoye la agilidad y realice una arquitectura para la adaptabilidad (por ejemplo, nube híbrida y multinube, multiplataforma), reduzca las superficies de ataque (por ejemplo, elimine las aplicaciones no utilizadas y los derechos de acceso sobreaprovisionados), suponga recursos comprometidos y espere que los adversarios evolucionen.
2. A la hora de planificar los proyectos digitales, hay que tener en cuenta las posibles amenazas junto con las oportunidades, así como las responsabilidades compartidas en materia de resiliencia en toda la cadena de suministro de tecnología digital, incluidas las soluciones de seguridad basadas en la nube.
3. Cree sistemas para integrar la seguridad por diseño y tomar medidas para prever, detectar, resistir, adaptar y responder a futuras amenazas en evolución.
4. Asegúrese de que los líderes empresariales consulten con los equipos de seguridad cuando sea necesario para comprender los riesgos asociados a los nuevos desarrollos. Del mismo modo, los equipos de seguridad deben considerar los objetivos empresariales y asesorar a los líderes sobre cómo alcanzarlos de forma segura.
5. Garantice la existencia de prácticas y procedimientos operativos claros para la resiliencia de la organización en caso de incidentes cibernéticos.

La importancia de modernizar los sistemas y la arquitectura

A medida que desarrollamos nuevas capacidades para un mundo hiperconectado, tenemos que administrar las amenazas que plantean los sistemas y el software heredados.

Los sistemas heredados, aquellos que se desarrollaron antes de que las herramientas modernas de conectividad, como los teléfonos inteligentes, las tabletas y los servicios en la nube, se convirtieran en la norma, representan un riesgo para una organización que todavía los utiliza. Esta exposición al riesgo se ve reforzada por las conclusiones del equipo de Servicios de seguridad de Microsoft para la respuesta ante incidentes, un grupo de profesionales de la seguridad que ayuda a los clientes a responder y recuperarse de los ataques.

A lo largo del año pasado, los problemas detectados entre los clientes que se recuperaban de los ataques estaban relacionados con seis categorías, como se muestra en el gráfico de esta página. En la siguiente página se describen las medidas que pueden adoptarse para mejorar la resiliencia.

Más del 80 % de los incidentes de seguridad pueden deberse a unos pocos elementos que faltan y que podrían abordarse mediante enfoques de seguridad modernos.

Problemas clave que afectan a la resiliencia cibernética

Este gráfico muestra el porcentaje de clientes afectados que carecen de controles de seguridad básicos que son fundamentales para aumentar la resiliencia cibernética de la organización. Los hallazgos se basan en los compromisos de Microsoft durante el último año.

"Los líderes tienen que pensar en la resiliencia cibernética como una faceta crítica de la resiliencia empresarial. Tienen que planificar las interrupciones cibernéticas del mismo modo que lo hacen con las catástrofes naturales u otros acontecimientos imprevistos y reunir a las partes interesadas internas, como los departamentos de operaciones, comunicaciones y jurídico, entre otros, para elaborar estrategias. De este modo, las organizaciones se aseguran de que sus sistemas empresariales críticos vuelvan a estar en línea lo antes posible para reanudar el funcionamiento normal de la empresa.

Pero no se detiene allí. Dado que muchas organizaciones dependen de proveedores de terceros y proveedores de servicios, los líderes tienen que ampliar la planificación de la resiliencia cibernética a su cadena de valor de extremo a extremo para garantizar aún más la continuidad del negocio y la resiliencia".

Ann Johnson,
Vicepresidente corporativo de Desarrollo empresarial de seguridad, cumplimiento, identidad y administración

La importancia de modernizar los sistemas y la arquitectura

Continuación

Hay áreas claras que las organizaciones pueden abordar para modernizar su enfoque y protegerse de las amenazas:

Problema	Pasos prácticos
Configuración insegura del proveedor de identidades La configuración errónea y la exposición de las plataformas de identidad y sus componentes son un vector común para obtener acceso no autorizado de alto privilegio.	Siga las líneas básicas de configuración de seguridad y los procedimientos recomendados al implementar y mantener sistemas de identidad como la infraestructura de AD y Azure AD. Implementar restricciones de acceso mediante la aplicación de la segregación de privilegios, el acceso de mínimo privilegio y la utilización de estaciones de trabajo de acceso privilegiado (PAW) para la administración de los sistemas de identidad.
Controles de acceso a privilegios y movimiento lateral insuficientes Los administradores tienen excesivos permisos en el entorno digital y a menudo exponen las credenciales administrativas en las estaciones de trabajo sujetas a riesgos de Internet y productividad.	Asegure y limite el acceso administrativo para hacer el entorno más resiliente y limitar el alcance de un ataque. Emplee controles de administración de acceso a privilegios, como el acceso Just-In-Time y la administración justa.
No hay autenticación multifactor (MFA) Los atacantes de hoy en día no entran por la fuerza, sino que inician sesión.	MFA es un control de acceso de usuarios crítico y fundamental que todas las organizaciones tienen que habilitar. Junto con el acceso condicional, MFA puede ser inestimable para luchar contra las ciberamenazas.
Operaciones de seguridad de baja madurez La mayoría de las organizaciones afectadas utilizaban herramientas tradicionales de detección de amenazas y no disponían de información pertinente para responder y corregir a tiempo.	Una estrategia integral de detección de amenazas requiere inversiones en detección y respuesta extendida (XDR) y modernas herramientas nativas de la nube que emplean el machine learning para separar el ruido de las señales. Modernice las herramientas de operaciones de seguridad mediante la incorporación de XDR, que puede entregar una visión profunda de la seguridad en todo el panorama digital.
Falta de control de protección de la información Las organizaciones siguen luchando por establecer controles holísticos de protección de la información que tengan una cobertura total en todas las ubicaciones de los datos, que sigan siendo eficaces durante todo el ciclo de vida de la información y que estén alineados con la criticidad empresarial de los datos.	Identifique los datos críticos de su empresa y dónde se encuentran. Revise los procesos del ciclo de vida de la información y aplique la protección de los datos garantizando la continuidad del negocio.
Adopción limitada de marcos de seguridad modernos La identidad es el nuevo perímetro de seguridad, que permite el acceso a servicios digitales y entornos informáticos dispares. La integración de los principios de Confianza cero, la seguridad de las aplicaciones y otros marcos cibernéticos modernos permite a las organizaciones administrar de forma proactiva riesgos que, de otro modo, les costaría prever.	Los marcos de Confianza cero aplican los conceptos de mínimo privilegio, verificación explícita de todos los accesos y suponen siempre un compromiso. Las organizaciones también tienen que implementar controles y prácticas de seguridad en los procesos de DevOps y del ciclo de vida de las aplicaciones para obtener mayores niveles de garantía en sus sistemas empresariales.

La postura de seguridad básica es un factor determinante en la eficaciade las soluciones avanzadas

A través de nuestro análisis, descubrimos un predominio de puntos ciegos comunes en las defensas de las organizaciones que permiten a los atacantes obtener un acceso inicial, establecer un punto de apoyo e implementar un ataque, incluso en presencia de soluciones de seguridad avanzadas.

En muchos casos, el resultado de un ciberataque está determinado mucho antes de que este comience. Los atacantes aprovechan los entornos vulnerables para obtener el acceso inicial, llevar a cabo la vigilancia y causar estragos mediante el movimiento lateral y el cifrado o la filtración. Detener a un atacante en una fase temprana aumenta en gran medida la oportunidad de reducir el impacto global.

Microsoft estudió configuraciones específicas en posturas de seguridad para identificar las deficiencias más comunes en la práctica real de estos entornos. Esto nos permitió ver las vulnerabilidades más comunes explotadas durante los ataques de ransomware operados por humanos que permitieron a los actores de la amenaza obtener acceso y viajar a través de una red sin ser detectados.

Las configuraciones básicas de seguridad deben estar activadas

Los dispositivos de una organización que no están incorporados o están obsoletos (tanto en relación con las vulnerabilidades como con el estado de los agentes de seguridad) sirven como potenciales puntos de entrada y rutas de establecimiento de acceso para los atacantes. Descubrimos que, si bien es cierto que los dispositivos de la organización cuentan con una detección y respuesta de puntos de conexión[1] (EDR) actualizada y la solución de la plataforma de protección de puntos de conexión[2] (EPP) es un paso importante, no está garantizado que detenga el ransomware.

Las soluciones avanzadas, como el EDR y el EPP, son fundamentales para detectar a un atacante en una fase temprana del flujo de ataque y permitir la reparación y protección automáticas. Sin embargo, como estas soluciones avanzadas se basan en una capacidad fundamental para detectar un ataque, requieren que se activen las configuraciones básicas de seguridad. De hecho, observamos un predominio de escenarios con soluciones avanzadas en funcionamiento que se veían mermadas por la ausencia de configuraciones básicas de seguridad.

Los procedimientos recomendados en las configuraciones de seguridad son un mayor indicador de resiliencia que el tiempo de respuesta de los analistas del centro de operaciones de seguridad (SOC)

Hemos observado una reducción del 70 % en el tiempo que tarda un analista del SOC en ver y actuar sobre una alerta pertinente durante un periodo de seis meses en toda nuestra población de clientes y socios. Esta mayor concienciación es una buena señal. Sin embargo, mientras que la visibilidad de la configuración de seguridad mejoró el rendimiento de los analistas del SOC, la habilitación de la visibilidad del producto mediante la incorporación y la actualización de los dispositivos de la organización fue un mayor predictor de la prevención exitosa.

Riesgo que suponen los dispositivos desconocidos

A diferencia de las redes en la nube, en las que los clientes saben qué activos se ejecutan en cada sistema operativo, las redes locales pueden contener una gran variedad de dispositivos como IoT, equipos, servidores y dispositivos de red que no son supervisados ni administrados por la organización.

La red empresarial promedio tiene más de 3500 dispositivos conectados que no están protegidos por un agente EDR y que pueden tener acceso a los recursos de la empresa o incluso a activos de gran valor. Microsoft Defender para punto de conexión (MDE) utiliza la inspección de la red para descubrir dispositivos y entregar información sobre las clasificaciones de los dispositivos conectados a la red, como el nombre del dispositivo, la distribución del sistema operativo y el tipo de dispositivo.

3500

es el número promedio de dispositivos conectados en una empresa que no están protegidos por un agente de detección y respuesta de puntos de conexión.

En el caso de los dispositivos no admitidos por un agente EDR, al menos hay que conocer su existencia y actuar para protegerlos evaluando las vulnerabilidades, así como restringiendo el acceso a la red.

Información práctica

1. Incluso las soluciones avanzadas pueden verse perjudicadas por la ausencia de configuraciones básicas de seguridad.
2. Invierta en los procedimientos recomendados de configuración de la postura de seguridad para protegerse de futuros ataques. Estos ajustes básicos producen un enorme retorno de la inversión en términos de la capacidad de una organización para defenderse de los ataques.
3. Incorpore todos los dispositivos aplicables a una solución EDR.
4. Asegúrese de actualizar los agentes de seguridad y garantizar la protección contra la manipulación para permitir una mayor visibilidad y una protección más completa de los productos.

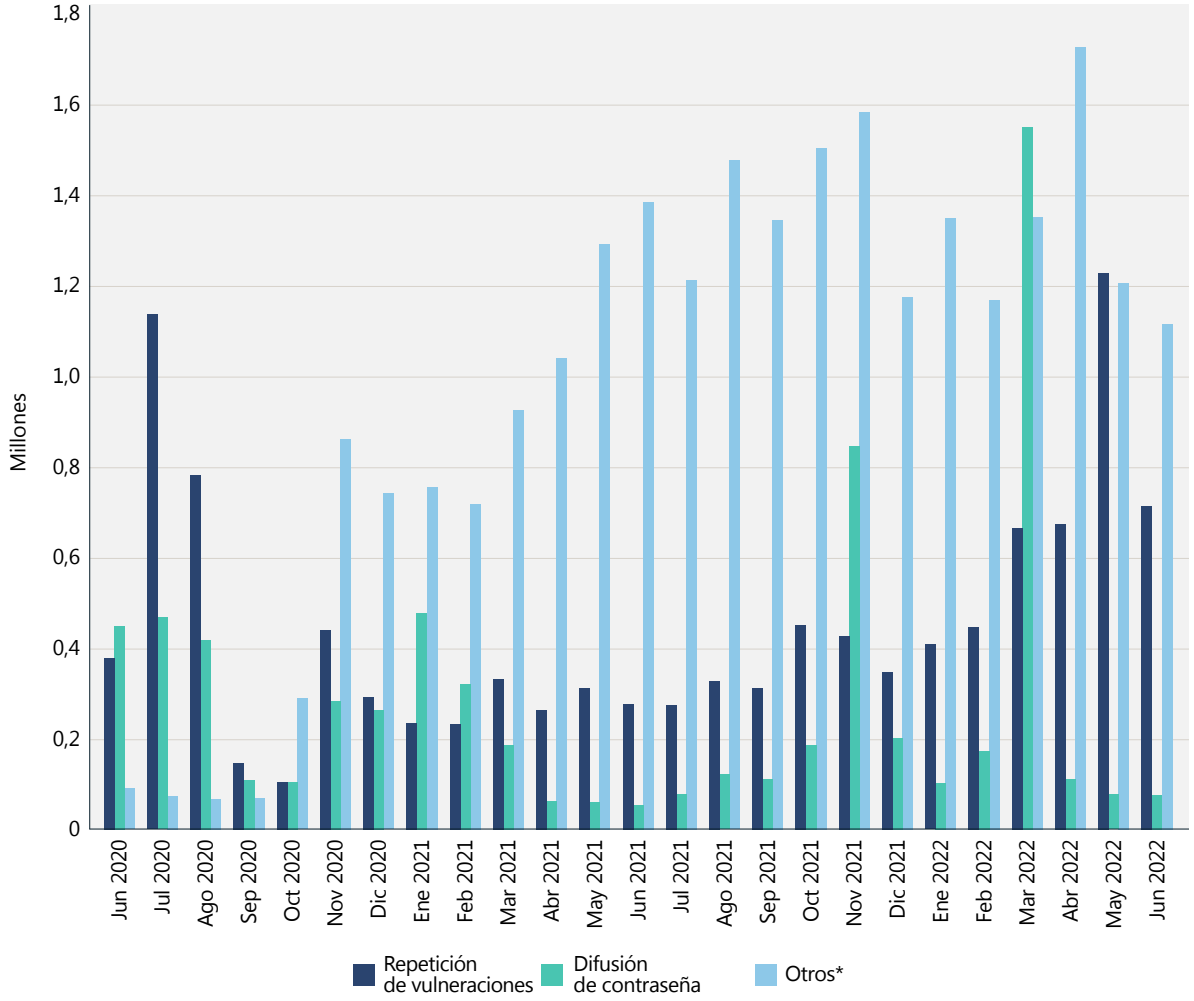
El mantenimiento del estado de la identidad es fundamental para el bienestar de la organización

La protección de la identidad es más importante que nunca. Aunque los ataques basados en contraseñas siguen siendo la principal fuente de compromiso de la identidad, están surgiendo otros tipos de ataques. El volumen de ataques sofisticados sigue aumentando en relación con la norma anterior de difusión de contraseñas y repetición de infracciones.

Los ataques basados en contraseñas siguen siendo comunes, y más del 90 % de las cuentas comprometidas a través de estos métodos no están protegidas con una autenticación fuerte. La autenticación fuerte utiliza más de un factor de autenticación, por ejemplo, contraseña + SMS y claves de seguridad FIDO2.

Hemos observado un aumento de los ataques de difusión de contraseñas dirigidos, con alzas muy grandes en el volumen de tráfico de los atacantes repartidos entre miles de direcciones IP.

Usuarios comprometidos por categoría de ataque



Usuarios comprometidos por mes por categoría de ataque. Los volúmenes de ataques de difusión de contraseñas fueron muy volátiles, como se observa en los picos de noviembre de 2021 y marzo de 2022. Estos picos representan miles de usuarios y miles de direcciones IP tocadas. *"Otros" indica ataques diferentes a la difusión de contraseñas y a la repetición de infracciones, incluyendo phishing, malware, "man-in-the-middle", compromiso del emisor de tokens en las instalaciones, y otros. Fuente: Azure AD Identity Protection.

4500

En el tiempo que se tarda en leer esta declaración, nos hemos defendido de 4500 ataques con contraseña.

El mantenimiento del estado de la identidad es fundamental para el bienestar de la organización

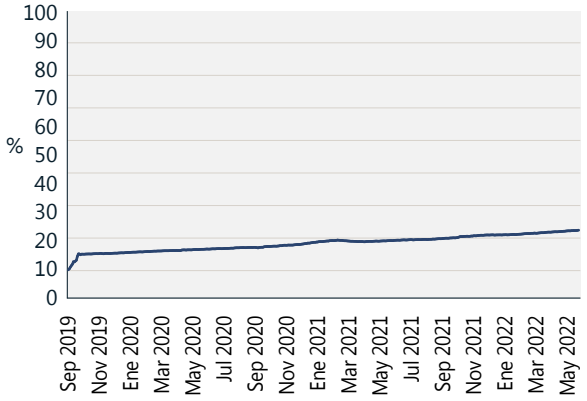
Continuación

Adopción de autenticación sólida

Como nota positiva, estamos viendo un crecimiento constante en la adopción de la autenticación fuerte entre la base de clientes empresariales de Azure Active Directory (Azure AD). En el caso de Azure AD, los usuarios activos mensuales (MAU) de autenticación fuerte crecieron del 19 % al 26 % en el último año, mientras que los MAU de autenticación fuerte para las cuentas administrativas crecieron del 30 % al 33 % aproximadamente.

Esta tendencia es positiva, pero aún se necesita un crecimiento significativo para alcanzar una cobertura mayoritaria de la autenticación fuerte; los clientes que aún no utilizan la autenticación fuerte en sus entornos deberían empezar a planificar e implementar la autenticación fuerte para proteger a sus usuarios.[3] A la hora de diseñar la implementación de la autenticación fuerte, debería considerarse la autenticación sin contraseña, ya que ofrece la experiencia de uso más segura, eliminando el riesgo de ataques con contraseña.

Uso de una autenticación sólida
(Sep 2019–May 2022)

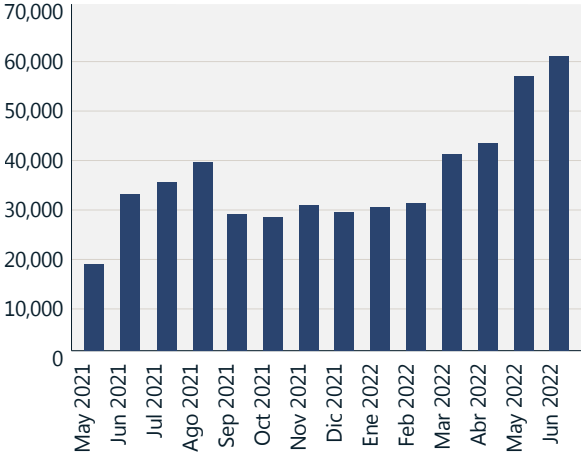


Aunque el uso de la autenticación fuerte se ha duplicado desde 2019, solo el 26 % de los usuarios y el 33 % de los administradores utilizan la autenticación fuerte. Fuente: Azure Active Directory.

Aumento constante de los ataques de repetición de tokens

La proporción de otras formas de ataque aumentó en 2022. Vimos un aumento de los ataques dirigidos que evitan específicamente la autenticación basada en contraseñas para reducir la posibilidad de detección. Estos ataques aprovechan las cookies de inicio de sesión único (SSO) del explorador o los tokens de actualización obtenidos a través de malware, phishing y otros métodos. En algunos casos, los atacantes eligen infraestructuras en lugares cercanos a la ubicación geográfica del usuario objetivo para reducir aún más las posibilidades de detección. Hemos visto un aumento constante de los ataques de repetición de token, llegando a más de 40 000 detecciones al mes en Azure AD Identity Protection. La repetición de tokens es el uso de tokens que se emitieron a un usuario legítimo por parte de un atacante que tiene la posesión de dichos tokens. Los tokens se obtienen comúnmente a través de malware, por ejemplo filtrando las cookies del explorador del usuario o a través de métodos avanzados de phishing.

Volumen de ataques de repetición de tokens detectados



Ataques de repetición de tokens detectados por mes. Fuente: Azure AD Identity Protection, sesiones únicas marcadas por la detección de tokens anómalos.

El mantenimiento del estado de la identidad es fundamental para el bienestar de la organización

Continuación

Extracción de tokens

Más que el malware, los atacantes necesitan credenciales para lograr sus objetivos. De hecho, el 100 % de los ataques de ransomware operados por humanos incluyen credenciales robadas. Muchas intrusiones sofisticadas incluyen credenciales compradas en la web oscura, inicialmente robadas a un malware de robo de credenciales poco sofisticado y de amplia distribución. Esta clase de malware ha evolucionado para robar tokens, incluyendo la información de la sesión y las reclamaciones MFA. Esto significa que las infecciones en los sistemas domésticos, donde los usuarios se conectan a los activos corporativos, pueden conducir a graves incidentes en las redes corporativas.

Los atacantes también pueden extraer tokens de los dispositivos de las víctimas a través de ataques tipo "man-in-the-middle", en los que la víctima hace clic en un vínculo malintencionado en un correo electrónico o mensaje instantáneo de phishing y se le dirige a un sitio web que se parece la página legítima de inicio de sesión del proveedor de identidad. En realidad, es un servicio web creado por el atacante que retransmite e intercepta todo el tráfico entre el usuario y el proveedor de identidad. El atacante puede interceptar el nombre de usuario y la contraseña y también retransmitir los desafíos MFA; los tokens resultantes emitidos por el proveedor de identidad e interceptados por el atacante podrían contener afirmaciones MFA que el atacante puede utilizar para satisfacer los requisitos MFA.

Microsoft Defender for Cloud Apps ha detectado un promedio de 895 ataques de este tipo al mes desde principios de 2022. Esta forma de ataque puede evitarse con los factores de MFA resistentes al phishing, como la autenticación basada en certificados, Windows Hello para empresas o las claves de seguridad FIDO2.

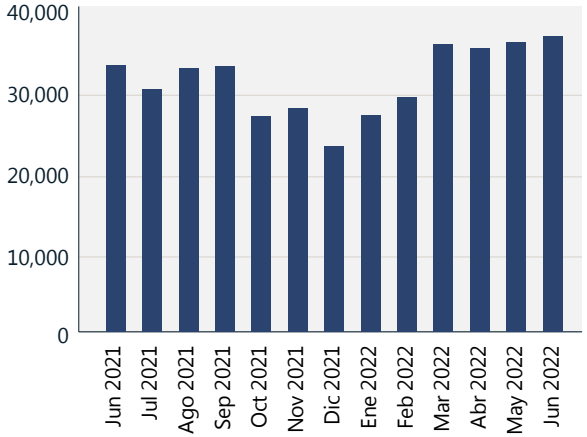
> Los ataques basados en contraseñas son el principal método por el que se comprometen las cuentas.

Fatiga de MFA

Utilizando el concepto de "fatiga de MFA", los atacantes generan varias solicitudes de MFA al dispositivo de la víctima, esperando que esta acepte la solicitud, ya sea de forma involuntaria o como resultado de la fatiga. Este ataque puede evitarse utilizando aplicaciones modernas de autenticación, como Microsoft Authenticator, combinadas con funciones como la coincidencia de números[4] y la habilitación de contexto adicional.[5] Azure AD Identity Protection calcula que se producen 30 000 ataques de fatiga de MFA al mes.

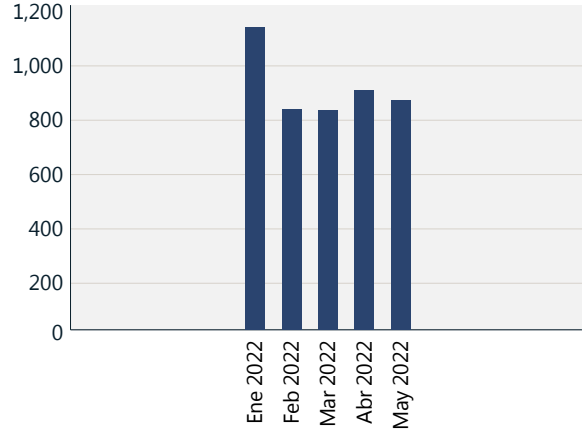
> La proporción de ataques sofisticados sigue aumentando, lo que subraya la necesidad de contar con factores de autenticación multifactor resistentes al phishing.

Instancias estimadas de ataques de fatiga de MFA



Fuente: Azure AD Identity Protection.

Casos detectados de phishing seguidos de ataques tipo "man-in-the-middle"



Fuente: Microsoft Defender for Cloud Apps.

Información práctica

1. Asegúrese de que todas las cuentas de su organización están protegidas por medidas de autenticación sólidas.
2. La autenticación sin contraseña ofrece la experiencia más segura y fácil de usar, eliminando el riesgo de ataques con contraseña.
3. Deshabilite la autenticación heredada en toda su organización.
4. Proteja las cuentas administrativas y de alto valor con formas de autenticación fuerte resistentes al phishing.
5. Modernice de un proveedor de identidades local a un proveedor de identidades en la nube y conecte todas sus aplicaciones al proveedor de identidades en la nube para obtener una experiencia de usuario y una seguridad coherentes.

Vínculos a más información

- En el Día Mundial de la Contraseña, considere la posibilidad de prescindir de las contraseñas | Seguridad de Microsoft

Configuración de seguridad predeterminada del sistema operativo

Con el panorama de las amenazas a la seguridad en continua evolución, vemos una creciente necesidad de seguridad informática configurada de manera predeterminada para mejorar la resiliencia cibernética. Aunque la seguridad de los sistemas operativos es más urgente, compleja y crítica para la empresa que nunca, puede ser un desafío acertar y administrar.

En el pasado, la seguridad de los equipos y dispositivos incluía funciones de seguridad integradas que el cliente o el profesional de TI debía configurar a su propio nivel. Este enfoque ya no es suficiente, ya que los atacantes están utilizando herramientas más avanzadas de automatización, infraestructura en la nube y tecnologías de acceso remoto para lograr sus objetivos. Se ha convertido en algo fundamental que todas las capas de seguridad, desde el chip hasta la nube, estén configuradas de manera predeterminada. Microsoft ha evolucionado para configurar la seguridad del sistema operativo Windows de manera predeterminada.[6]

Los clientes que adoptan una defensa en profundidad (incluida una postura de seguridad en capas, nuevas funciones de seguridad, revisiones y actualizaciones periódicas y constantes, así como capacitación en seguridad y concienciación para denunciar el phishing y otras estafas) pueden esperar menos malware.

Para simplificar la defensa en profundidad, Windows 11 cuenta con protecciones de hardware y software estrechamente integradas y activadas de manera predeterminada, como la integridad de la memoria, el arranque seguro y un Módulo de plataforma de confianza 2.0. Los usuarios de Windows 10 con hardware capaz también pueden activar estas funciones en la aplicación Configuración de Windows o en el menú de la BIOS.

Los dispositivos más antiguos en general no suelen tener una alineación tan fuerte entre la seguridad del hardware y las técnicas de seguridad del software. Para los dispositivos en los que la seguridad no está activada de manera predeterminada, configúrelos manualmente en los ajustes siempre que sea posible.[7]

Para los dispositivos en los que la seguridad no está activada de manera predeterminada, Microsoft recomienda la configuración manual en los ajustes siempre que sea posible.

Sea proactivo a la hora de aplicar actualizaciones continuas del sistema operativo y revisiones de seguridad que ayuden a brindar protección a lo largo del ciclo de vida del hardware y el software.

Información práctica

1. Utilice una solución sin contraseña que vincule las credenciales de inicio de sesión en el Módulo de plataforma de confianza; en concreto, busque una solución sin contraseña que cumpla el estándar de la industria Faster Identity Online (FIDO) Alliance[8].
2. Realice una limpieza oportuna de todos los ejecutables no utilizados y obsoletos que se encuentran en los dispositivos de las organizaciones.
3. Proteja los ataques avanzados al firmware activando la integridad de la memoria, el arranque seguro y la el Módulo de plataforma de confianza 2.0, si no está activado de manera predeterminada, que endurece el arranque utilizando las capacidades incorporadas en las CPU modernas.
4. Active el cifrado de datos y la protección de credenciales.
5. Habilite los controles de aplicaciones y exploradores para mejorar la protección frente a aplicaciones no confiables y otras protecciones integradas contra vulnerabilidades.
6. Habilite la protección de acceso a la memoria para ayudar a proteger contra ataques físicos ocasionales, como que alguien conecte un dispositivo malintencionado a los puertos de acceso externo.

Vínculos a más información

- Libro de seguridad de Windows | Comercial
- Las nuevas características de seguridad de Windows 11 ayudarán a proteger el trabajo híbrido | Microsoft Security Blog

Centralidad de la cadena de suministro de software

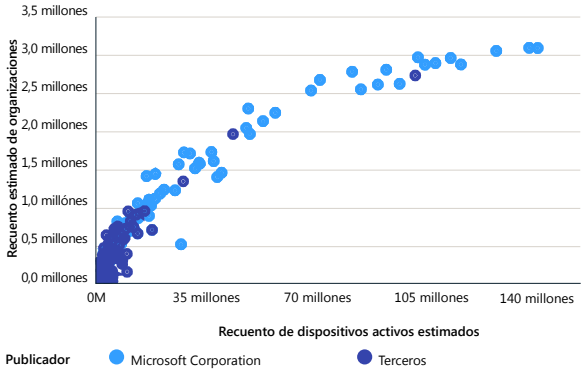
Los ataques a aplicaciones, complementos y extensiones de terceros pueden erosionar la confianza de los clientes en los proveedores que desempeñan un papel central en el ecosistema de suministro. El uso de la teoría de redes para observar la centralidad del software ayuda a iluminar la criticidad de las revisiones, sobre todo para las aplicaciones centrales.

La Red de aplicaciones de Windows, compuesta por 18 millones de ejecutables de aplicaciones, está instalada y se utiliza en cinco millones de organizaciones, lo que brinda una visión de alto nivel de nuestro ecosistema de software. De las 100 000 aplicaciones más utilizadas, el 97 % las producen organizaciones de terceros, cuyas actualizaciones y revisiones de seguridad son responsabilidad de ellas. Esto ilustra dos rasgos importantes de nuestro ecosistema de aplicaciones comerciales.

En primer lugar, está la centralidad en el ecosistema de aplicaciones comerciales de Windows. Solo las 100 000 aplicaciones más importantes (de las 18 millones) se utilizan en 1000 o más dispositivos. En otras palabras, poco más de la mitad del 1 % de estas aplicaciones tienen este tipo de efecto de amplio alcance entre el ecosistema de dispositivos.

En segundo lugar, hay diversidad en la administración de esas aplicaciones, donde los 10 000 principales proveedores de aplicaciones administran las actualizaciones y las revisiones de seguridad de estas aplicaciones comerciales más utilizadas. Esto demuestra la interdependencia que tiene una empresa en un conjunto diverso de controles de seguridad, cumplimiento y administración de los proveedores de software.

Penetración comercial de las aplicaciones más utilizadas



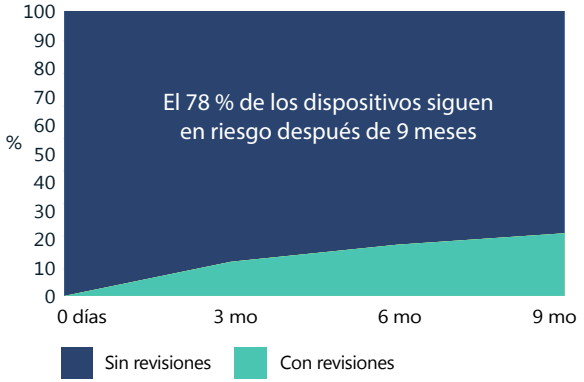
Las principales aplicaciones son utilizadas por millones de organizaciones y decenas de millones de dispositivos. Como son casi omnipresentes, los adversarios están en constante búsqueda para explotar las vulnerabilidades de estas aplicaciones principales, que pueden afectar a millones de dispositivos de la base de usuarios.

Observamos que millones de dispositivos comerciales siguen utilizando versiones de aplicaciones vulnerables muchos meses después de la publicación de la revisión o incluso años después del fin del soporte del producto. Por ejemplo, hay más de un millón de dispositivos comerciales de Windows activos que ejecutan la versión de un lector de PDF que no es compatible desde 2017.

Las versiones antiguas de las aplicaciones que no son compatibles siguen en uso activo en millones de dispositivos comerciales. En consecuencia, las organizaciones corren el riesgo de tener vulnerabilidades a las que no se aplicarán revisiones.

En el caso de las versiones de aplicaciones en soporte, observamos un estancamiento de la velocidad de adopción de revisiones críticas, que es lo contrario de la tendencia que impulsará la resiliencia. En cambio, la curva debería mostrar una adopción exponencial ascendente de revisiones mes a mes, para lograr la resiliencia necesaria.

Tasa de implementación de revisiones críticas



Tras examinar una vulnerabilidad crítica que afectaba a 134 versiones de un conjunto de navegadores, descubrimos que el 78 %, es decir, millones de dispositivos, seguían utilizando una de las versiones afectadas nueve meses después de la publicación de la revisión.

Utilizamos el conjunto de herramientas InterpretML[9] para identificar las características correlacionadas con las organizaciones que son más propensas a tener dispositivos con versiones de aplicaciones más antiguas. Entre los factores de predicción más importantes se encuentran: las bajas horas de dedicación a los dispositivos; zonas geográficas como Asia-Pacífico y América Latina; e industrias como la del automóvil, los productos químicos, las telecomunicaciones, el transporte y la logística, los pagadores de salud (encargados de las reclamaciones) y los seguros.

El mantenimiento de la resiliencia del software debe incluir la desactivación o desinstalación periódica de las aplicaciones no utilizadas.

La seguridad y el cumplimiento de las normas de una organización dependen de sus propios esfuerzos y delos de sus proveedores de software.

Información práctica

1. Realice actualizaciones oportunas de todas las aplicaciones y puntos de conexión de su organización.
2. Realice una limpieza oportuna de todos los ejecutables no utilizados y obsoletos que se encuentran en los dispositivos de las organizaciones.

Vínculos a más información

- Documentación de Microsoft Intune | Microsoft Docs
- Administración de aplicaciones | Microsoft Docs
- Microsoft Defender para punto de conexión | Seguridad de Microsoft
- Marco de cadena de suministro seguro de OSS | Ingeniería de seguridad de Microsoft
- Marco de cadena de suministro seguro de software open source Microsoft | GitHub

Creación de resiliencia a los nuevos ataques DDoS, a las aplicaciones web y a la red

La acelerada transformación digital ha puesto fin al modelo tradicional de red y perímetro de seguridad. Pasar a la nube significa que las empresas tienen que adoptar una seguridad de red nativa de la nube para proteger los activos digitales.

La complejidad, la frecuencia y el volumen de los ataques siguen creciendo y ya no se limitan a las temporadas de vacaciones, lo que indica un cambio hacia ataques durante todo el año. Esto pone de manifiesto la importancia de la protección continua más allá de las tradicionales temporadas de mayor tráfico.

Ataques de denegación de servicio distribuido (DDoS)

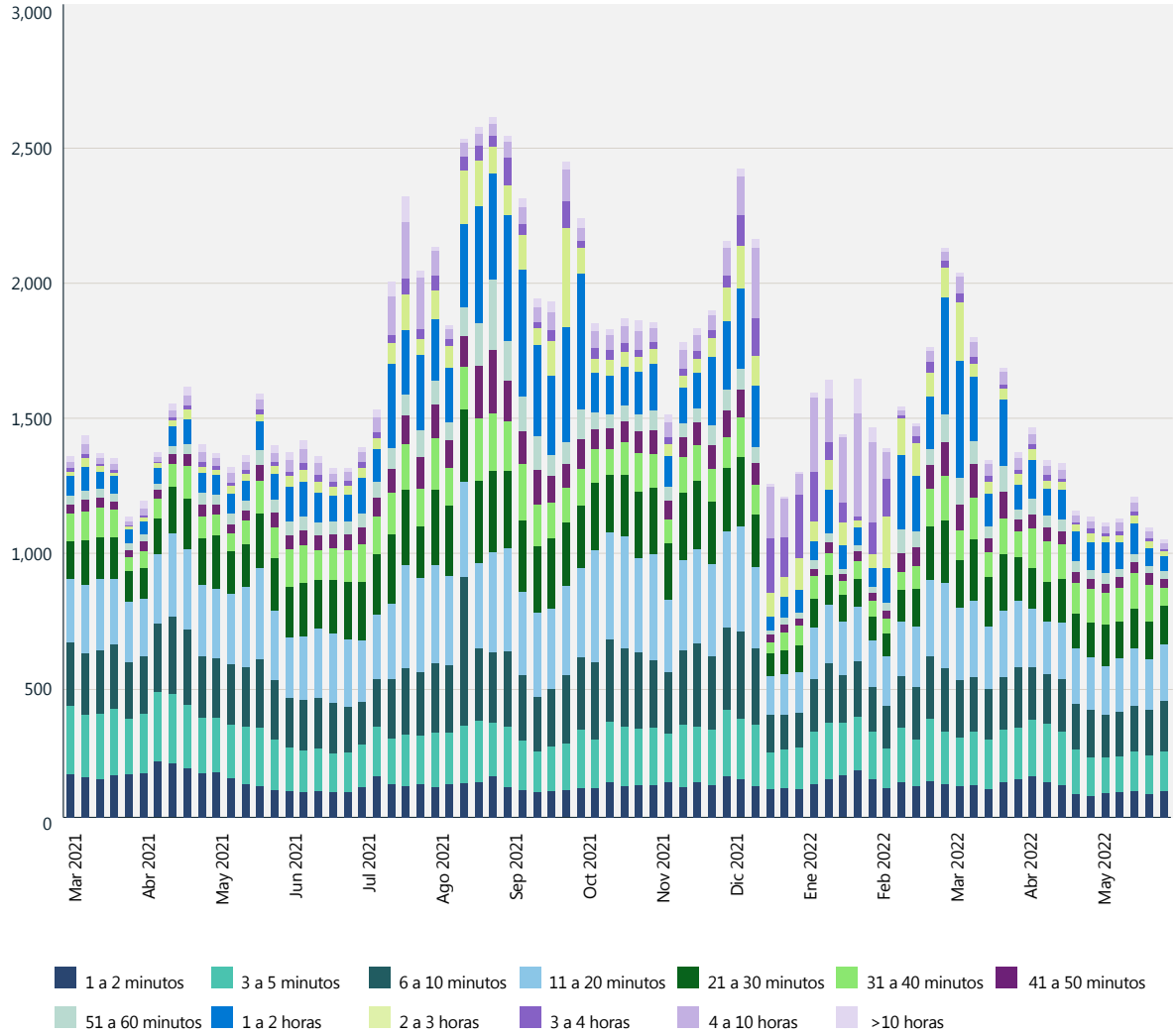
Durante el año pasado, el mundo experimentó una actividad DDoS sin precedentes en cuanto a volumen, complejidad y frecuencia. Esta explosión de DDoS se vio impulsada por un aumento considerable de los ataques de estado nación y la continua proliferación de servicios de DDoS de bajo costo. Microsoft mitigó un promedio de 1955 ataques al día, lo que supone un aumento del 40 % respecto al año anterior. Con anterioridad, el número máximo de ataques se producía normalmente durante la temporada de vacaciones de fin de año. Este año, no obstante, la mayor cantidad registrada en un día fue el 10 de agosto de 2021. Esto podría indicar un cambio hacia los ataques durante todo el año y pone de manifiesto la importancia de la protección continua más allá de las tradicionales temporadas de mayor tráfico.

En noviembre de 2021, Microsoft frustró un ataque DDoS volumétrico con un rendimiento de 3,4 terabits por segundo (Tbps) procedente de aproximadamente 10 000 fuentes que abarcaban varios países. En 2022 se mitigaron ataques similares de gran volumen por encima de los 2+Tbps, lo que pone de manifiesto que no solo aumenta la complejidad y la frecuencia de los ataques, sino también su volumen (ancho de banda).

Duración del ataque

La mayoría de los ataques observados durante este último año fueron de corta duración. Aproximadamente el 28 % de los ataques duraron menos de 10 minutos, el 26 % entre 10 y 30 minutos y el 14 % entre 31 y 60 minutos. El 32 % de los ataques duraron más de una hora.

Número de ataques DDoS y distribución de la duración
(Mar 2021–May 2022)



La mayoría de los ataques del último año fueron de corta duración. Aproximadamente el 28 % de los ataques duraron menos de 10 minutos.

Creación de resiliencia a los nuevos ataques DDoS, a las aplicaciones web y a la red

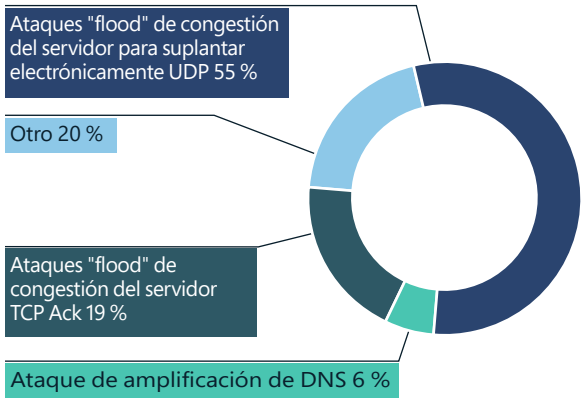
Continuación

Vectores de ataque DDoS

El año pasado, los vectores de ataque comúnmente empleados fueron el reflejo del Protocolo de datagramas de usuario (UDP) en el puerto 80 utilizando el protocolo simple de descubrimiento de servicios (SSDP), el protocolo ligero de acceso a directorios sin conexión (CLDAP), el sistema de nombres de dominio (DNS) y el protocolo de tiempo de red (NTP) que comprende un solo valor máximo. También se observó un aumento de los ataques DDoS en la capa de aplicación dirigidos a sitios web, con 16,3 millones de RPS (solicitudes por segundo) máximos y 9,89 Tbps de tráfico máximo.

En 2022, Microsoft mitigó casi 2000 ataques DDoS diarios y frustró el mayor ataque DDoS registrado en la historia.

Vectores de ataque DDoS



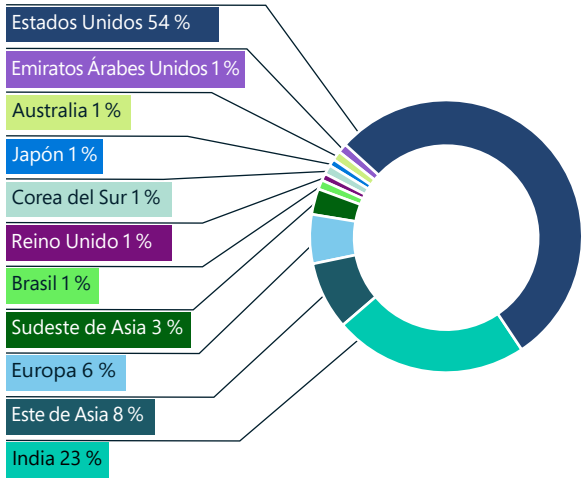
El ataque "flood" de congestión del servidor para suplantar electrónicamente UDP subió al primer vector en la primera mitad de 2022, del 16 % al 55 %. El ataque "flood" de congestión del servidor TCP ACK disminuyó del 54 % al 19 %.

El sector del juego sigue siendo el principal objetivo de los ataques DDoS, en su mayoría procedentes de mutaciones de la red de robots Mirai y de ataques de bajo volumen del protocolo UDP. Dado que el UDP se utiliza habitualmente en aplicaciones de juegos y streaming, una abrumadora mayoría de los vectores de ataque eran ataques "flood" de congestión del servidor para suplantar electrónicamente UDP, mientras que una pequeña parte eran ataques de reflejo y amplificación UDP.

Regiones de destino geográficas

De los ataques DDoS detectados durante el año pasado, el 54 % se realizaron contra objetivos en Estados Unidos, una tendencia que podría explicarse en parte por el hecho de que la mayoría de los clientes de Azure y Microsoft están en Estados Unidos. También hemos visto un fuerte aumento de los ataques contra la India, que ha pasado del 2 % de todos los ataques en el segundo semestre de 2021 al 23 % en el primer semestre de 2022. Asia oriental, y Hong Kong en particular, sigue siendo un objetivo popular, con un 8 %. En el caso de Europa, se produjeron concentraciones de ataques contra las regiones de Ámsterdam, Viena, París y Fráncfort.

Destino de ataque DDoS

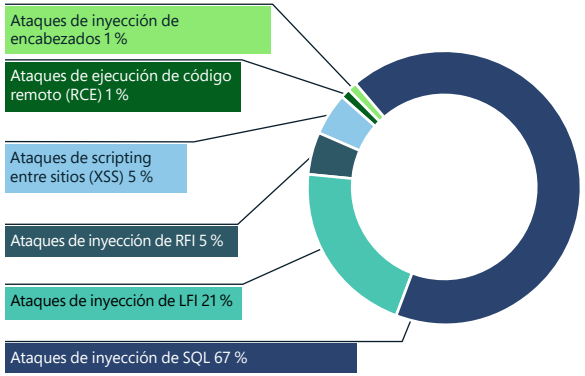


Atribuimos el alto volumen de ataques en Asia a la enorme presencia de juegos en la región, sobre todo en China, Japón, Corea del Sur e India. Esta huella continuará expandiéndose a medida que la creciente penetración de los teléfonos inteligentes impulsa la popularidad de los juegos móviles, lo que sugiere que este objetivo geográfico solo seguirá creciendo.

Vulnerabilidades de aplicaciones web

El firewall de aplicaciones web (WAF), en combinación con la protección DDoS, es parte integral de la estrategia de defensa en profundidad para proteger los activos de la web y la interfaz de programación de aplicaciones (API). Microsoft observó más de 300 000 millones de reglas WAF activadas al mes a través de los WAF de Azure.

Distribución de los tipos de ataque más frecuentes



Azure WAF detecta diariamente miles de millones de ataques Open Web Application Security Project (OWASP) Top 10[10]. Según nuestras señales, los atacantes intentaron en su mayoría ataques de inyección SQL, seguidos de ataques de inyección de archivos locales y de inyección de archivos remotos. Esto coincide con la lista OWASP Top Ten que muestra los ataques de inyección como el tercer tipo más común de ataques web.

También se ha producido un aumento de los ataques de bots contra las aplicaciones web de Azure, con un promedio de 1700 millones de solicitudes de bots al mes y un 4,6 % de ese tráfico formado por bots malos.

Creación de resiliencia a los nuevos ataques DDoS, a las aplicaciones web y a la red

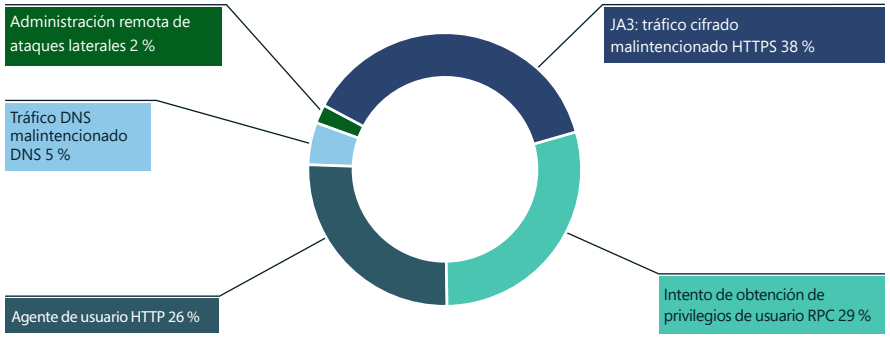
Continuación

Debido al creciente número de bots que realizan ataques de relleno de credenciales, fraude con tarjetas de crédito, campañas de ciberinfluencia y ataques a la cadena de suministro, esperamos ver un aumento constante de los ataques de bots contra las aplicaciones web.

Intrusiones en la red: detección y prevención

Hemos observado un aumento significativo de las vulnerabilidades de la capa de red, en particular del malware, en 2022. El sistema de detección y prevención de intrusiones (IDPS) de Azure Firewall bloqueó más de 150 millones de conexiones solo en el mes de junio.

Motivo de denegación del tráfico IDPS



Motivos de alerta de tráfico IDPS

El análisis del tráfico de alerta y denegación de IDPS muestra los siguientes enfoques utilizados por los atacantes. En el tráfico de denegación, estamos viendo que los atacantes utilizan SSL para ocultar sus actividades y los ataques de ejecución remota son cada vez más comunes. En el tráfico de alerta, estamos viendo que se utilizan los protocolos SMB/SMB2 para realizar ataques de ejecución remota.

Información práctica

1. Inspeccione todo el tráfico entre sistemas dentro de un centro de datos o servicio en la nube, y el tráfico que intenta acceder a ellos.
2. Desarrollar una sólida estrategia de respuesta a la seguridad de la red durante todo el año.
3. Utilice los servicios de seguridad nativos de la nube para implementar una sólida postura de seguridad de red de Confianza cero.

Vínculos a más información

- Mejore sus defensas de seguridad para los ataques de ransomware con Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Anatomía de un ataque de amplificación DDoS | Microsoft Security Blog
- Protección inteligente de aplicaciones desde el perímetro hasta la nube con Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Desarrollo de un enfoque equilibrado de la seguridad de los datos y la resiliencia cibernética

La transformación digital ha impulsado una gran expansión de los activos de datos y un aumento de los riesgos de seguridad, cumplimiento y privacidad. Las organizaciones con capacidad de resiliencia cibernética tienen que equilibrar las inversiones en protección de datos, cumplimiento de la normativa y capacidades de recuperación, e integrarlas con procesos de respuesta normativa especializados para hacer frente a distintos tipos de infracciones.

Las vulneraciones de datos no son una cuestión de "si", sino de "cuándo". El estudio "Cost of a Data Breach, 2021" de IBM y Ponemon Institute informa de un costo promedio mundial de la vulneración de datos de USD 4,24 millones (un 10 % más que el año anterior) y de USD 9,05 millones en Estados Unidos. Los errores de cumplimiento se encontraron como el principal factor de amplificación de costos. Por el contrario, las reducciones de los costos de las infracciones se asociaron a los procedimientos recomendados, como la planificación de la respuesta ante incidentes (IR), la madurez de la implementación de Confianza cero, la IA y la automatización de la seguridad, y el uso del cifrado.

Las vulneraciones de datos son inevitables. Las organizaciones que adopten un enfoque de resiliencia equilibrado reducirán la frecuencia, el impacto y el costo de las infracciones.

La gobernanza de los datos, la seguridad, el cumplimiento y la privacidad son interdependientes

En los últimos años hemos visto cómo los datos han ganado protagonismo como motor crucial de creación de valor para las organizaciones. Al mismo tiempo, el aumento de las normativas sobre privacidad que exigen tanto la gobernanza de los datos como la seguridad han difuminado las líneas entre los roles de riesgo. Mientras que las nuevas funciones de los altos ejecutivos, como el Director de datos (CDO) o los Directores de privacidad (CPO), tienen un gran interés en la seguridad y el cumplimiento, la aplicación y puesta en marcha de la protección de datos a menudo depende de los equipos dirigidos por los Directores de información (CIO) o el Director de seguridad de la información (CISO). No se trata de una vía de sentido único, ya que las iniciativas de gobernanza de datos dirigidas por los CDO también tienen beneficios en materia de seguridad. Como resultado de esta interconexión, los equipos de TI, de gobernanza de datos, de seguridad, de cumplimiento y de privacidad deben trabajar cada vez más estrechamente para lograr la eficiencia y administrar el riesgo.

Las plataformas unificadas de administración del riesgo de datos para todo el patrimonio de datos de la organización son el futuro

Alinear los procesos de administración de TI, gobernanza de datos, seguridad, cumplimiento y privacidad es difícil en un entorno de aplicaciones a medida para cada disciplina y una cobertura uniforme a través de la típica organización híbrida, la dispersión de datos en varias nubes. Creemos que las organizaciones necesitan un único panel para localizar y conocer sus datos, proteger sus datos, gobernar el acceso, el uso y el ciclo de vida de los datos, y prevenir la pérdida de datos en todo el patrimonio de datos. Trabajar a partir de la misma información sobre el inventario de datos y la actividad facilita los procesos entre equipos, ofrece una imagen de riesgo más completa y permite a las organizaciones prepararse mejor y agilizar su respuesta ante una infracción.

El "panel único" debe actuar como un prisma. Los equipos que tienen un interés en la seguridad, el cumplimiento y la privacidad de los datos necesitan vistas diferentes pero coherentes del mismo inventario de datos y de la actividad para alinearse y colaborar. La actividad de los datos incluye eventos de acceso, modificación y movimiento de datos, que son una parte valiosa de la ecuación de seguridad de los datos.

La gobernanza eficaz de los datos, la seguridad, el cumplimiento y la privacidad son interdependientes y requieren la colaboración de todos los equipos.

Información práctica

1. Equilibre la defensa con la recuperación y minimice el impacto de la vulneración de datos invirtiendo en el cumplimiento, la protección de datos y las capacidades de respuesta.
2. Desarrolle y adopte procesos y herramientas que trasciendan los silos de riesgo de los datos y abarquen todo el conjunto de datos.

Vínculos a más información

- Microsoft Purview: Soluciones de protección de datos | Seguridad de Microsoft
- El futuro del cumplimiento y el gobierno de los datos ya está aquí: Presentación de Microsoft Purview | Microsoft Security Blog

Resiliencia a las operaciones de influencia cibernética: la dimensión humana

En los últimos cinco años, los avances en materia de gráficos y machine learning han introducido herramientas fáciles de usar, capaces de generar rápidamente contenidos realistas de alta calidad que pueden difundirse ampliamente en Internet en cuestión de segundos.

Cuando se trata de acontecimientos comunicados a través de contenidos textuales, sonoros y visuales, hemos llegado a un punto en el que ni los humanos ni los algoritmos pueden distinguir de forma confiable los hechos de la ficción. La proliferación de estas herramientas y sus resultados están poniendo en duda la confiabilidad de todos los medios de comunicación digitales, perturbando nuestra comprensión de los acontecimientos locales y mundiales. Las nuevas maneras de operaciones de influencia que permiten losa vances tecnológicos tienen graves implicaciones para los procesos democráticos.[11]

Surgen preguntas sobre lo que podemos hacer para prepararnos para un futuro más resiliente contra estas operaciones de ciberinfluencia. La tecnología es solo una parte del rompecabezas. Se necesitarán varios esfuerzos, incluida la educación dirigida a la alfabetización mediática, la concienciación y la vigilancia, las inversiones en periodismo de calidad (con periodistas de confianza, en el nivel local, nacional e internacional), las redes de intercambio y alerta sobre las operaciones de influencia, y nuevos tipos de regulaciones que penalicen a los actores malintencionados que generan o manipulan los medios digitales con el objetivo de engañar.

También reconocemos que restablecer la confianza en los contenidos digitales es un objetivo ambicioso que requerirá diversas perspectivas y participación. No hay ninguna empresa, ni institución, ni gobierno que pueda resolver estas amenazas por sí solo. Nuestro superpoder como humanos es la capacidad de colaborar y cooperar. Esto es de suma importancia ahora porque requerirá que todo el mundo (gobiernos de todo el mundo, industrias, academias y sobre todo organizaciones de noticias, sociales y de medios de comunicación) trabajen juntos para la mejora y la salud de nuestra sociedad.

Vínculos a más información

- Aplicaciones de la inteligencia artificial en las misiones cibernéticas del Departamento de Defensa | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (3 de mayo de 2022; Testimonio de Eric Horvitz)

Fortalecimiento del factor humano con la capacitación

Abordar el factor humano es un componente clave de cualquier estrategia de capacitación en ciberseguridad. Según un estudio de Kaspersky sobre el factor humano en la seguridad informática,[12] el 46 % de los incidentes de ciberseguridad implican a personal descuidado o uniformado que facilita el ataque de forma inadvertida.

El equipo de Educación y Concienciación de Microsoft en la organización de Seguridad digital y resiliencia es responsable de fortalecer el factor humano de la ciberseguridad mediante la capacitación a los empleados para asegurar nuestros propios sistemas y datos y los de nuestros clientes. Nuestros objetivos son:

- Reducir el riesgo para Microsoft y nuestros clientes mediante la creación de un conjunto de habilidades de seguridad centralizado para toda la empresa en toda la población de empleados.
- Fortalecer los conocimientos de seguridad de losempleados mediante un enfoque de refuerzo de la capacitación en varias fases para apoyar los resultados de comportamiento deseados.
- Fomentar el cambio de cultura haciendo que la mentalidad de seguridad sea una parte intrínseca de la cultura de Microsoft a través de la capacitación y los eventos de seguridad requeridos anualmente.
- Promover un recurso web centralizado para los procedimientos recomendados, la información sobre la directiva de la empresa y la notificación de incidentes para todo lo relacionado con la ciberseguridad.

Un programa de capacitación en ciberseguridad centralizado y específico llega a todos los empleados de Microsoft al menos una vez al año. Las ofertas de capacitación están optimizadas para apoyar las iniciativas actuales de ciberseguridad y ofrecer resultados medibles de comportamiento. El Consejo de administración de riesgos de la información (IRMC) de Microsoft desempeña un papel fundamental en la identificación de los resultados importantes del cambio de comportamiento en materia de ciberseguridad que debe abordar la capacitación.

Con todos nuestros programas de capacitación en ciberseguridad, medimos la eficiencia, la eficacia y los resultados de la solución cuando es posible. Por ejemplo, nuestra oferta de capacitación sobre amenazas internas tiene un 95 % de cumplimiento de la capacitación, una satisfacción excepcional de los alumnos y ha dado lugar a un aumento considerable de los gerentes que informan de posibles casos de amenazas internas a través de la herramienta Report It Now de la empresa. El programa incluye:

Security Foundations: capacitación centralizada de concienciación y cumplimiento de la ciberseguridad en toda la empresa que aborda las principales prácticas de seguridad y privacidad. Esta esperada serie de capacitación emplea un modelo de entretenimiento educativo o "edutainment" para hacer que el aprendizaje sobre ciberseguridad sea atractivo e interesante.

STRIKE: capacitación técnica exigida por Microsoft para los ingenieros que crean y mantienen soluciones de línea de negocio. Esta capacitación por invitación aborda áreas oportunas y críticas de los procedimientos recomendados de higiene de ciberseguridad y utiliza un modelo de entrega híbrido en vivo adaptado a las necesidades de la audiencia.

Programa específico: los programas de capacitación específicos apoyan iniciativas de ciberseguridad como Shadow IT, Insider Threat y Microsoft Federal. Estas ofertas están estrechamente integradas en la estrategia general de compromiso para sus respectivas iniciativas de ciberseguridad mediante el patrocinio ejecutivo y la presentación de informes de puntuación para evitar un enfoque de capacitación de "marcar la casilla".

MSProtect: el recurso web centralizado de Microsoft ofrece procedimientos recomendados, información sobre la directiva de la empresa y notificación de incidentes para todo lo relacionado con la ciberseguridad. Este recurso on-demand es el más utilizado por los empleados fuera de la oferta de capacitación formal.

La capacitación en seguridad no debe verse como una actividad de cumplimiento, de marcar la casilla. En su lugar, hay que centrarse en el cambio de comportamiento para poder supervisar los resultados en los comportamientos objetivo identificados, y establecer sistemas de escucha para determinar el impacto de las ofertas.

Información práctica

1. Brinde capacitación y recursos de seguridad a los empleados cuando y donde lo necesiten.
2. Desarrolle una estrategia de capacitación centralizada informada por las partes interesadas de toda la empresa.
3. Garantice el seguimiento y el análisis del impacto de la capacitación en cuanto a la eficiencia (cantidad), la eficacia (calidad) y los resultados (impacto empresarial).

Vínculos a más información

- Microsoft pone en marcha la siguiente fase de su iniciativa de capacitación tras ayudar a 30 millones de personas

Información de nuestro programa de eliminación de ransomware

Microsoft ha emprendido su propio recorrido de Confianza cero[13] en los últimos cinco años para garantizar que las identidades y los dispositivos se administren de forma sólida y saludable. A medida que aumenta el riesgo de ransomware, hemos desarrollado una visión profunda para apoyar nuestro enfoque de protección de nosotros mismos y de nuestros clientes.

Tras una evaluación interna en profundidad, creamos un programa de eliminación de ransomware para corregir las deficiencias en los controles y la cobertura, contribuir a la mejora de las funciones de servicios como Defender para punto de conexión, Azure y M365, y desarrollar manuales para nuestros equipos de SOC e ingeniería sobre cómo recuperarse en caso de un ataque de ransomware.

El primer paso fue comprender el alcance de nuestra protección contra un ataque de ransomware dirigido a Microsoft. Los esfuerzos ya estaban en marcha para implementar Defender para punto de conexión y garantizar que todos los dispositivos se administran y cumplen con nuestras directivas de Confianza cero, pero necesitábamos encontrar una forma de comprender todas las facetas de la interrogante más amplia de si podríamos recuperarnos eficazmente de un ataque. Para obtener información, evaluamos el NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile,[14] que se alinea con nuestra directiva general de la empresa contra nuestra lista conocida de controles. Este análisis identificó rápidamente las brechas en la cobertura.

A continuación, priorizamos las brechas en las funciones de identificación, detección, protección, respuesta y recuperación del CSF. Encontramos una alineación estratégica con Confianza cero y otros programas y también descubrimos brechas que no tenían una línea de trabajo existente. Una vez evaluada la cantidad de trabajo y el esfuerzo necesario para corregir estas deficiencias, las separamos en dos pilares:

- **Proteger la empresa (PtE):** defina los elementos de trabajo que debemos hacer como empresa para protegernos y poder recuperarnos de un ataque, en caso de que este tenga éxito.
- **Proteger al cliente (PtC):** incorpore capacidades a nuestra oferta para proteger tanto a nuestros clientes como a nuestro negocio.

Incorporación de resultados en nuestra propia empresa

Para corregir los principales riesgos y proteger nuestros servicios críticos contra un ataque de ransomware, planificamos enfocar las inversiones en los próximos 6 a 12 meses en la consecución de los cinco escenarios siguientes como parte de un programa dedicado al ransomware. Una vez que tengamos éxito en cada uno de los escenarios, ampliaremos de manera gradual el alcance del programa para llegar a todas las partes de la empresa.

Escenario 1: Los miembros del equipo de seguridad comprenden el riesgo global asociado a un ataque de ransomware y tienen un proceso establecido para dar a conocer a los ejecutivos las brechas de control y el estado del riesgo.

Escenario 2: Los miembros del equipo de seguridad tienen acceso a los manuales diseñados para ayudarles a ellos y a otros equipos de Microsoft a responder y recuperar los servicios críticos de un ataque de ransomware.

Escenario 3: Los miembros del equipo de resiliencia de la empresa tienen una norma que seguir para la copia de seguridad de los sistemas críticos. Existen manuales y se realizan ejercicios periódicos de copia de seguridad y recuperación para garantizar que los datos puedan recuperarse en caso de ataque de ransomware.

Escenario 4: Los propietarios de los servicios comprenden e implementan los controles y directivas de seguridad y operativos necesarios para proteger sus servicios, los datos de los clientes, los puntos de conexión y los activos de red contra los ataques de ransomware, con especial atención a los servicios priorizados como servicios críticos de Microsoft.

Escenario 5: Todos los empleados pueden acceder a recursos educativos y de capacitación que describen cómo reconocer un ataque de ransomware y cómo notificar al equipo de seguridad e iniciar la respuesta.

Información práctica

1. Documente y valide las actividades de recuperación y reparación de extremo a extremo relacionadas con los ataques de ransomware contra servicios críticos.
2. Involucre a las partes interesadas en la actualización de sus manuales de administración de crisis de la empresa para incluir actividades específicas de ransomware y un proceso de decisión y orientación para determinar si se debe pagar por el ransomware y cuándo.
3. Mejore la cobertura de detección y protección habilitando las capacidades disponibles en sus productos de seguridad implementados (por ejemplo, las reglas de reducción de la superficie de ataque de Defender para puntos de conexión).
4. Trabajar con el equipo de normas de seguridad para definir una línea de base para la protección contra un ataque de ransomware, y proporcionar capacitación y documentación a los equipos de ingeniería sobre cómo protegerse contra un ataque de ransomware.
5. Poner en marcha la automatización para facilitar la implementación de las directivas de seguridad y operaciones a los equipos de DevOps y garantizar que si un sistema se desvía del cumplimiento se señale con rapidez y se corrija.

Vínculos a más información

- Cómo se protege Microsoft contra el ransomware | Microsoft Inside Track

Cómo actuar ahora sobre las implicaciones de la seguridad cuántica

Existe presión para administrar la amenaza que la computación cuántica supone para la criptografía actual y todo lo que protege. El recientemente publicado Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] se basa en el Decreto 10428 de EE. UU.[16] para mejorar la ciberseguridad del país destaca que la seguridad de la cadena de suministro de software es fundamental para hacer frente a futuros ataques de estados nación.

¿Qué son los equipos cuánticos?

Los ordenadores cuánticos son máquinas que utilizan las propiedades de la física cuántica para almacenar datos y realizar cálculos. Esto puede ser muy ventajoso para determinadas tareas en las que podrían superar ampliamente incluso a nuestros mejores superequipos. La computación cuántica ya está abriendo nuevos horizontes para el cifrado y el procesamiento de datos. Los estudios predicen que la computación cuántica se convertirá en una industria multimillonaria ya en 2030.[17] De hecho, la computación y la comunicación cuánticas están a punto de tener un efecto transformador en varias industrias, desde la salud y la energía hasta las finanzas y la seguridad.

La computación cuántica es una amenaza para la criptografía actual y todo lo que protege.

La amenaza a la criptografía actual

Con el algoritmo de Shor de 1994 y un equipo cuántico a escala industrial de más de unos pocos millones de qubits físicos, todos nuestros algoritmos criptográficos de clave pública actuales y ampliamente implementados podrían romperse de manera eficaz. Es fundamental considerar, evaluar y normalizar criptosistemas "seguros desde el punto de vista cuántico" que sean eficientes, ágiles y seguros frente a un ataque adversario cuántico. La migración del software a la "criptografía poscuántica", es decir, la robustez de los algoritmos y protocolos clásicos existentes frente a los ataques cuánticos, tardará años, si no una década o más, en lograrse.[18]

Esto significa que existe presión para administrar la amenaza para la criptografía actual y todo lo que protege. Los adversarios pueden grabar datos cifrados ahora y explotarlos más tarde, cuando dispongan de un equipo cuántico. Esperar a que llegue la computación cuántica para abordar sus implicaciones criptográficas será demasiado tarde.

Como la criptografía se utiliza en todo el ecosistema cibernético, esto significa que nuestros servicios de seguridad basados en criptografía podrían verse comprometidos. Por ejemplo, esto incluye servicios de comunicaciones (TLS, IPSec), mensajería (correo electrónico, conferencias web), administración de identidad y acceso, navegación web, firma decódigo, transacciones de pago y otros servicios que dependen de la criptografía para su protección.

A medida que los equipos cuánticos se conviertan en una realidad, los componentes de software de terceros que contengan implementaciones de algoritmos y capacidades criptográficas requerirán también un escrutinio adicional. Esto requiere que todas las organizaciones a lo largo de la cadena de valor pongan de su parte para garantizar que la cadena siga siendo segura. Los organismos de la industria y los gobiernos están incrementando sus esfuerzos para definir los requisitos de seguridad de la cadena de suministro de software y, en algunos casos, introduciendo nuevos mandatos para asegurar la cadena. National Security Memorandum NSM-8[19] establece requisitos y plazos para implementar la criptografía poscuántica en los Sistemas de Seguridad Nacional (NSS). Establece un plazo de 180 días para "la planificación de la modernización, el uso de cifrado no compatible, los protocolos exclusivos para misiones aprobados, los protocolos resistentes al cuanto y la planificación del uso de criptografía resistente al cuanto cuando sea necesario".

La normalización es una actividad que requiere mucho tiempo en la transición hacia una criptografía segura desde el punto de vista cuántico.Los organismos de normalización que trabajan en normas que utilizan criptografía de clave pública deben empezar ya a experimentar y adaptarse a los algoritmos poscuánticos.

El Post-Quantum Standardization Project del NIST está revisando nuevos algoritmos de criptografía poscuántica (PQC), algoritmos clásicos que se consideran resistentes a los ataques cuánticos.[20] Este trabajo influirá en los esfuerzos globales de los organismos de normalización. Aunque habrá cierto solapamiento con las selecciones de algoritmos del gobierno de EE. UU., las distintas opciones de organismos nacionales/reguladores para los algoritmos conformes podrían plantear desafíos internacionales. Esta fragmentación complicará a su vez la ingeniería de productos y servicios.

Se están revisando nuevos algoritmos de criptografía poscuántica a través del programa Post-Quantum Cryptography Standardization del NIST. Este trabajo influirá en los esfuerzos globales de los organismos de normalización.

Información práctica

Junto con SAFECode y los miembros asociados, la industria debería emprender actividades inmediatas a más corto plazo para preparar la transición al PQC.[21] Estos incluyen:

1. Hacer un inventario de sus productos/ códigos que utilizan criptografía.
2. Implementar una estrategia de agilidad criptográfica en toda su organización que incluya la minimización del cambio de código necesario cuando cambia la criptografía.
3. Dirigir el uso de algoritmos candidatos a la seguridad cuántica en sus productos o servicios que utilicen criptografía.
4. Estar preparado para utilizar diferentes algoritmos de clave pública para el cifrado, el intercambio de claves y las firmas.
5. Probar en sus aplicaciones el impacto de claves, cifrados y firmas de gran tamaño.

Vínculos a más información

- Microsoft ha demostrado la física subyacente necesaria para crear un nuevo tipo de qubit | Microsoft Research

Integración de la empresa, la seguridad y la TI para una mayor resiliencia

Una resiliencia cibernética robusta depende de que los líderes empresariales trabajen con los equipos de seguridad para implementar la seguridad. Según la experiencia de Microsoft, el liderazgo en seguridad es una disciplina difícil que requiere el apoyo de los líderes de la organización para protegerla de la forma más eficaz.

Los líderes de seguridad se enfrentan a una serie de desafíos dinámicos que abarcan temas relacionados con el riesgo, la tecnología, la economía, los procesos organizativos, los modelos empresariales, la transformación cultural, los intereses geopolíticos, el espionaje y el cumplimiento de las sanciones internacionales. Cada uno de ellos conlleva matices que hay que comprender y administrar de cerca.

Los líderes de la seguridad también tienen la tarea de frustrar tanto a los atacantes humanos inteligentes, bien financiados y muy motivados, como a los ciberdelincuentes poco cualificados, pero eficaces. Sus equipos deben defender complejos patrimonios técnicos, a menudo construidos de forma incremental a lo largo de 30 o más años, cuando la seguridad era una prioridad baja o inexistente. Las decisiones tomadas hace años pueden plantear riesgos hoy, hasta que paguemos la deuda técnica y abordemos las brechas de seguridad.

Los líderes de las organizaciones y los legisladores pueden tener un impacto positivo significativo en la seguridad apoyando activamente a los líderes de seguridad y ayudando a construir un puente entre la seguridad integrada y el resto de la organización. Cuando Microsoft trabaja con clientes que tienen esta alineación, vemos que construyen una organización más resiliente y también mejoran su agilidad para adaptarse e innovar.

El liderazgo organizativo puede apoyar a los líderes de seguridad centrándose en tres áreas clave:

1. Crear seguridad desde el diseño

A veces, la seguridad se considera un obstáculo o una idea tardía en los procesos empresariales, y a menudo solo se tiene en cuenta en las decisiones cuando ya es demasiado tarde para evitar un riesgo o solucionarlo de forma barata y sencilla.

Los líderes de las organizaciones y los legisladores políticos deben asegurarse de que:

Se incluya la seguridad desde el principio en las nuevas iniciativas. Las nuevas iniciativas digitales y la adopción de la nube deben dar prioridad a la seguridad para garantizar que el riesgo organizativo no aumente con cada nueva aplicación o capacidad digital. Una vez incluida la seguridad de forma confiable, puede utilizar esos procesos para modernizar los sistemas heredados y obtener al mismo tiempo ventajas de seguridad y productividad.

Se normalice el mantenimiento preventivo de la seguridad. Garantice que el mantenimiento básico de la seguridad (como la aplicación de actualizaciones y revisiones de seguridad y las configuraciones seguras) cuente con todo el apoyo organizativo asignado (incluidos presupuestos, tiempos de inactividad programados, requisitos de adquisición para la asistencia de productos de proveedores).

Por desgracia, muchas organizaciones retrasan, aplazan o aplican solo de manera parcial estas prácticas comunes. Esto ofrece a los atacantes amplias oportunidades de explotación. La necesidad de normalización de la seguridad se recoge en el documento US NIST 800-40.[22]

2. Comprometerse con la seguridad

Los líderes de la organización deben participar activamente en los procesos clave de seguridad y patrocinarlos para garantizar la priorización de los recursos y la preparación ante catástrofes de seguridad. Esto incluye participar en:

La identificación de los activos empresariales críticos. Los responsables y equipos de seguridad deben saber qué activos son críticos para la empresa, a fin de centrar los recursos de seguridad en lo que más importa. A menudo se trata de un nuevo ejercicio que incluye plantear y responder a nuevas preguntas que no se han abordado con anterioridad.

Ejercicios de continuidad del negocio y recuperación ante desastres en materia de ciberseguridad. Los ciberataques pueden convertirse en grandes acontecimientos que interrumpan o paralicen la mayor parte o la totalidad de las operaciones empresariales. Garantizar que los equipos de toda la organización estén preparados para hacer frente a estas situaciones reducirá el tiempo necesario para restablecer las operaciones comerciales, limitará los daños a la organización y ayudará a mantener la confianza de clientes, ciudadanos y electores. Esto debería integrarse en un proceso existente de continuidad del negocio y recuperación ante desastres.

La mejor forma de tomar decisiones sobre los riesgos de seguridad es que lo hagan los responsables de la empresa o la misión, que tienen una visibilidad completa de todos los riesgos y oportunidades.

Integración de la empresa, la seguridad y la TI para una mayor resiliencia

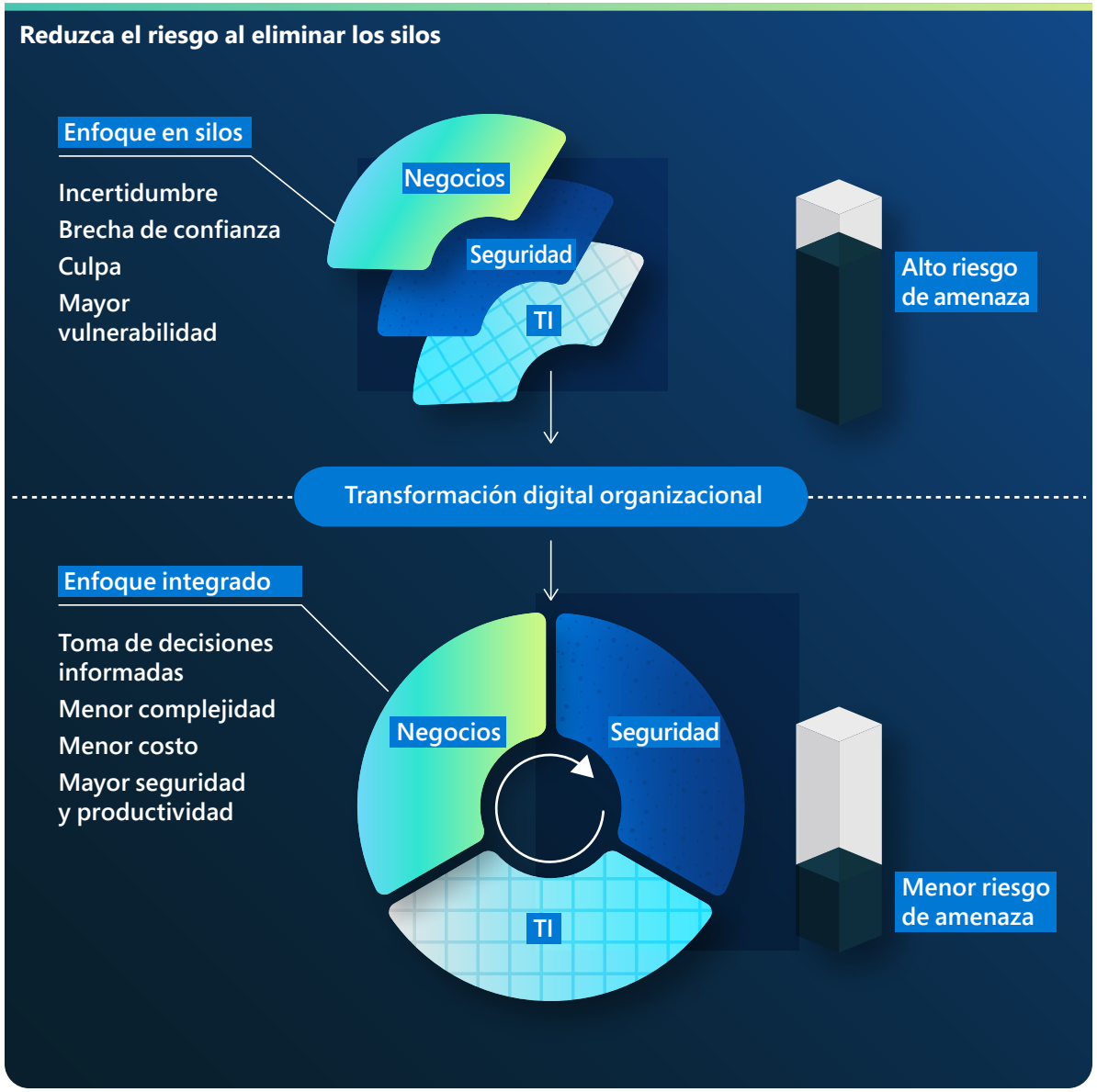
Continuación

3. Posicionar correctamente la seguridad

La forma en que las organizaciones estructuran la rendición de cuentas sobre los riesgos de seguridad a menudo las predispone a tomar decisiones poco acertadas. La mejor forma de tomar decisiones sobre riesgos es que las tomen los responsables de la empresa o la misión, que tienen plena visibilidad de todos los riesgos y oportunidades, pero las organizaciones suelen asignar (implícita o explícitamente) la responsabilidad de los riesgos de seguridad a los expertos en la materia del equipo de seguridad. Esto supone una carga insana para los equipos de seguridad, al tiempo que priva a los propietarios de las empresas de visibilidad y control sobre un riesgo clave para su negocio. Las organizaciones pueden corregir esto mediante la:

Preparación de los empresarios: eduque a los empresarios sobre los riesgos de seguridad en general y sobre cómo estas amenazas pueden afectar y afectarán a su negocio. Implicar directamente a los equipos de seguridad en este esfuerzo también aumenta la relación de colaboración con la seguridad y la agilidad general de la empresa.

Asignación del riesgo de seguridad a los empresarios: a medida que los propietarios de las empresas estén lo suficientemente informados como para comprender y aceptar los riesgos de seguridad, la organización debería transferirles explícitamente la responsabilidad de los riesgos de seguridad, sin dejar de responsabilizar a los equipos de seguridad de la administración de dichos riesgos y de proporcionar conocimientos y orientación al propietario.



"La resiliencia cibernética se sitúa en una escala móvil que va desde la continuidad del negocio y recuperación ante desastres, empezando por una buena copia de seguridad de los datos, pasando por la capacidad de recuperación de los procesos, la tecnología y sus dependencias (incluidas las personas y terceros), hasta los servicios siempre activos y autorrecuperables, la resiliencia de las funciones críticas y las conmutaciones por error de terceros críticos. Las organizaciones más resilientes fomentan la integración entre los profesionales de TI, los responsables de negocio y los de seguridad. Una gran capacidad de resiliencia incluye el diseño de la resiliencia desde el principio, la administración segura de los cambios y el aislamiento granular de los errores. La resiliencia cibernética es solo un escenario en un buen programa de planificación para todo tipo de riesgos. A medida que aumentan los riesgos cibernéticos y la intersección entre ciberseguridad y resiliencia se hace más importante, la conexión del director de Seguridad de la Información (CISO) con el programa de resiliencia de la empresa se hace más fuerte. Cada año, más CISO asumen la responsabilidad de la resiliencia en toda la empresa".

Lisa Reshaur
Gerente general, Administración de Riesgos, Microsoft

Vínculos a más información

- De la resiliencia a la perseverancia digital: Cómo las organizaciones están utilizando la tecnología digital para dar un giro en tiempos sin precedentes | Official Microsoft Blog
- Cómo pueden colaborar los equipos informáticos y de seguridad para mejorar la seguridad de los puntos de conexión | Seguridad de Microsoft

La curva de la campana de la resiliencia cibernética

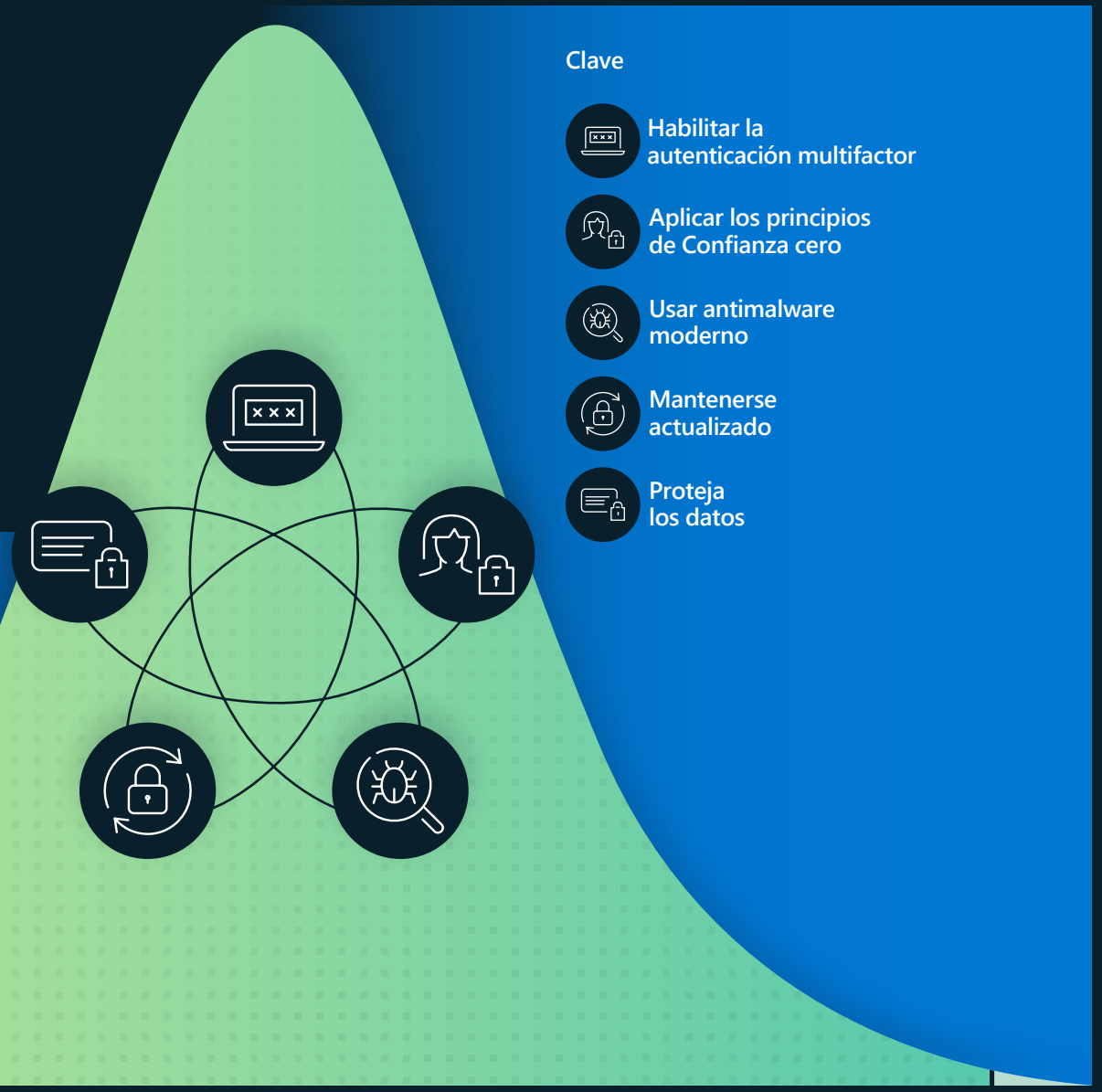
Factores de éxito de la resiliencia que toda organización debe adoptar

Como hemos visto, muchos ciberataques tienen éxito simplemente porque no se ha seguido una higiene de seguridad básica. Las normas mínimas que toda organización tiene que adoptar son:

- **Habilitar la autenticación multifactor (MFA):** para proteger contra contraseñas de usuario comprometidas y ayuda a proporcionar resiliencia adicional para las identidades.
- **Aplicar principios de Confianza cero:** la piedra angular de cualquier plan de resiliencia que limite el impacto en una organización. Estos principios son:
  1. – Comprobar explícitamente: asegúrese de que los usuarios y dispositivos están en buen estado antes de permitir el acceso a los recursos.
  2. – Usar el acceso con privilegios mínimos: solo permita el privilegio necesario para acceder a un recurso y nada más.
  3. – Suponer una vulneración: suponga que las defensas del sistema se infringieron y que los sistemas podrían estar comprometidos. Esto significa vigilar constantemente el entorno en busca de posibles ataques.
- **Utilizar antimalware de detección y respuesta extendidas:** implemente software para detectar y bloquear automáticamente los ataques y entregar información a las operaciones de seguridad. Supervisar la información de los sistemas de detección de amenazas es esencial para poder responder a las amenazas a tiempo.
- **Mantenerse actualizado:** los sistemas sin revisiones y desactualizados son una de las principales razones por las que muchas organizaciones son víctimas de un ataque. Garantice que todos los sistemas se mantienen actualizados, incluidos el firmware, el sistema operativo y las aplicaciones.
- **Proteger los datos:** conocer sus datos importantes, dónde se encuentran y si se han implementado los sistemas adecuados es crucial para aplicar la protección apropiada.

98 %

La higiene de seguridad básica aún protege contra el 98 % de los ataques



Notas finales

1. La detección y respuesta de puntos de conexión (EDR) es una plataforma de seguridad de punto de conexión empresarial diseñada para ayudar a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas. La detección y respuesta de punto de conexión ofrece detecciones avanzadas de ataques que son prácticas y casi en tiempo real. Los analistas de seguridad pueden priorizar las alertas con eficacia, obtener visibilidad de todo el alcance de una vulneración y tomar medidas de respuesta para corregir las amenazas.
2. Una plataforma de protección de puntos de conexión (EPP) es una solución que se implementa en los dispositivos de los puntos de conexión para evitar el malware basado en archivos, detectar y bloquear la actividad malintencionada de aplicaciones confiables y no confiables, y ofrecer las capacidades de investigación y corrección necesarias para responder de manera dinámica a los incidentes y alertas de seguridad.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Libro de seguridad de Windows: Comercial
7. Las nuevas características de seguridad de Windows 11 ayudarán a proteger el trabajo híbrido | Microsoft Security Blog
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Orden ejecutiva 14028 Improving the Nation's Cybersecurity
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. "The Long Road Ahead to Transition to Post-Quantum Cryptography", https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Equipos colaboradores

Equipos colaboradores

Un grupo diverso de profesionales centrados en la seguridad, que trabajan en diferentes equipos de Microsoft entregan los datos y las perspectivas de este informe. En conjunto, su objetivo es proteger a Microsoft, sus clientes y al mundo en general de la amenaza de los ciberataques. Nos enorgullece compartir estos conocimientos como un acto de transparencia, con el objetivo común de convertir el mundo en un lugar más seguro para todos.

AI for Good Research Lab: aprovechar el poder de los datos y la IA para abordar muchos de los desafíos del mundo. El laboratorio colabora con organizaciones ajenas a Microsoft, aplicando la IA para mejorar los medios de subsistencia y el medioambiente. Entre sus áreas de interés figuran la seguridad en línea (desinformación, ciberseguridad, seguridad infantil), la respuesta ante desastres, la sostenibilidad y la IA para la salud.

Azure Edge y seguridad de plataformas, empresas y sistemas operativos: responsable de la seguridad del sistema operativo central y de la plataforma en Windows, Azure y otros productos de Microsoft. El equipo crea soluciones de seguridad y hardware líderes del sector en las plataformas de Microsoft para reducir los riesgos de vulnerabilidades, identidad y malware desde el chip hasta la nube. Creadores de la plataforma de núcleo protegido de Microsoft en PC, Edge y Server, el procesador de seguridad Microsoft Pluton y mucho más.

Azure Networking, Core: un equipo de redes en la nube centrado en la WAN de Microsoft, las redes de centros de datos y la infraestructura de redes definidas por software de Azure, incluida la plataforma DDoS, la plataforma de perímetro de red y los productos de seguridad de red como Azure WAF, Azure Firewall y Azure DDoS Protection Standard.

Equipo de investigación sobre seguridad en la nube: al proteger la nube de Microsoft, crear características y productos de seguridad innovadores y llevar a cabo investigaciones, este equipo protege y capacita a los clientes de Microsoft para transformar de manera segura sus organizaciones.

Seguridad y confianza de los clientes (CST): un equipo que impulsa la mejora continua de la seguridad del cliente en los productos y servicios en línea de Microsoft. Al trabajar con equipos de ingeniería y seguridad en toda la empresa, CST garantiza el cumplimiento, mejora la seguridad y ofrece más transparencia para proteger a nuestros clientes y promover la confianza global en Microsoft.

Éxito del cliente: Los equipos de seguridad de Éxito del cliente trabajan directamente con los clientes para compartir procedimientos recomendados, lecciones aprendidas y orientación para acelerar la transformación y modernización de la seguridad. Este equipo reúne y organiza los procedimientos recomendados y las lecciones aprendidas del recorrido de Microsoft, así como de nuestros clientes, en estrategias, arquitecturas y planes de referencia, etc.

Centro de operaciones de ciberdefensa (CDOC): la instalación de ciberseguridad y defensa de Microsoft es un centro de fusión que reúne a profesionales de seguridad de toda la empresa para proteger nuestra infraestructura corporativa y la infraestructura en la nube a la que los clientes tienen acceso. Los responsables de responder a los incidentes colaboran con científicos de datos e ingenieros de seguridad de todos los grupos de servicios, productos y dispositivos de Microsoft para ayudar a proteger, detectar y responder a las amenazas las 24 horas, los 7 días de la semana.

Iniciativa de democracia para el futuro: un equipo de Microsoft que trabaja para preservar, proteger y promover los fundamentos de la democracia mediante el fomento de un ecosistema de información saludable, salvaguardando procesos democráticos abiertos y seguros y abogando por la responsabilidad cívica de las empresas.

Unidad de delitos digitales (DCU): un equipo de abogados, investigadores, científicos de datos, ingenieros, analistas y profesionales empresariales dedicados a luchar contra la ciberdelincuencia a escala mundial mediante el uso de tecnología, análisis forense, acciones civiles, remisiones penales y asociaciones tanto públicas como privadas.

Diplomacia digital: un equipo internacional de antiguos diplomáticos, legisladores y expertos jurídicos que trabajan para fomentar un ciberespacio pacífico, estable y seguro frente a los crecientes conflictos entre estados nación.

Seguridad digital y resiliencia (DSR): una organización dedicada a permitir a Microsoft crear los dispositivos y servicios más confiables, manteniendo al mismo tiempo la seguridad de nuestra empresa y la protección de nuestros datos y los de nuestros clientes.

Unidad de seguridad digital (DSU): un equipo de abogados y analistas de ciberseguridad que aportan conocimientos jurídicos, geopolíticos y técnicos para proteger a Microsoft y a sus clientes. La DSU fomenta la confianza en las defensas de seguridad empresarial de Microsoft frente a ciberadversarios avanzados de todo el mundo.

Centro de análisis de amenazas digitales (DTAC): un equipo de expertos que analiza e informa sobre las amenazas de los estados nación, incluidos los ciberataques y las operaciones de influencia. El equipo combina información e inteligencia sobre ciberamenazas con análisis geopolíticos para entregar información a nuestros clientes y a Microsoft que sirva de base para una respuesta y protección eficaces.

Empresa y seguridad: un equipo centrado en brindar una plataforma moderna, segura y administrable para la nube inteligente y el perímetro inteligente.

Movilidad empresarial: un equipo que ayuda a brindar un lugar de trabajo moderno y una administración moderna para mantener la seguridad de los datos, en la nube y en las instalaciones. Endpoint Manager incluye los servicios y herramientas que Microsoft y sus clientes usan para administrar y supervisar dispositivos móviles, equipos.de escritorio, máquinas virtuales, dispositivos integrados y servidores.

Equipos colaboradores

Continuación

Administración de riesgos empresariales: un equipo que trabaja en todas las unidades de negocio para dar prioridad a los debates sobre riesgos con los altos directivos de Microsoft. ERM conecta múltiples equipos de riesgo operativo, administra el marco de riesgo empresarial de Microsoft y facilita la evaluación de la seguridad interna de la empresa utilizando el Marco de ciberseguridad de NIST.

Directiva global de ciberseguridad: un equipo que trabaja con gobiernos, ONG y socios de la industria para promover políticas públicas de ciberseguridad que permitan a los clientes fortalecer su seguridad y resiliencia cuando adoptan y usan la tecnología de Microsoft.

Seguridad de identidad y acceso a la red (IDNA): un equipo que trabaja para proteger a todos los clientes de Microsoft de accesos no autorizados y fraudes. Seguridad de IDNA es un equipo interdisciplinario de ingenieros, gerentes de productos, científicos de datos e investigadores de seguridad.

Seguridad de M365: organización que desarrolla soluciones de seguridad, como Microsoft Defender para punto de conexión (MDE) y Microsoft Defender for Identity (MDI), entre otras, para proteger a los clientes empresariales.

IA, Ética y Efectos en Ingeniería e Investigación (AETHER) de Microsoft: un consejo asesor de Microsoft cuya misión es garantizar que las nuevas tecnologías se desarrollen y apliquen de forma responsable.

Búsqueda y distribución de Microsoft Bing: un equipo dedicado a ofrecer un motor de búsqueda en Internet de primera clase, que permite a los usuarios de todo el mundo encontrar con rapidez resultados de búsqueda e información confiables, incluido el seguimiento de los temas y las tendencias que les interesan, al tiempo que les da el control de su privacidad.

Soluciones para socios y clientes de Microsoft: Organización comercial unificada de comercialización de Microsoft responsable de funciones de campo como especialistas y asesores de ventas técnicas y de seguridad.

Expertos de Microsoft Defender: la mayor organización mundial de Microsoft de investigadores de seguridad centrados en productos, científicos aplicados y analistas de inteligencia de amenazas. Expertos de Defender ofrece capacidades innovadoras de detección y respuesta en productos de seguridad de Microsoft 365 y servicios administrados de Expertos de Microsoft Defender.

Microsoft Defender for IoT: un equipo compuesto por investigadores expertos en la materia especializados en ingeniería inversa de malware, protocolos y firmware de IoT/OT. El equipo busca amenazas IoT/OT para descubrir tendencias y campañas malintencionadas.

Inteligencia sobre amenazas de Microsoft Defender (RiskIQ): un equipo que produce inteligencia táctica mediante el análisis de la amplia recopilación de telemetría externa de Microsoft, trazando el panorama de las amenazas a medida que evoluciona para descubrir infraestructuras de amenazas desconocidas hasta ahora, y añadiendo contexto a los actores y campañas de amenazas. El equipo publica de forma periódica investigaciones puntuales y distintivas para brindar a los defensores información táctica crucial.

Equipo de desarrollo empresarial de seguridad de Microsoft: un equipo que dirige la estrategia de crecimiento de la ciberseguridad, las asociaciones y las inversiones estratégicas de Microsoft.

Centro de respuestas de seguridad de Microsoft (MSRC): un equipo comprometido con los investigadores de seguridad que trabajan para proteger a los clientes y al ecosistema de socios de Microsoft. MSRC, una parte integral del Centro de operaciones de ciberdefensa (CDOC) de Microsoft, reúne a expertos en respuesta de seguridad para detectar y responder a las amenazas en tiempo real.

Servicios de seguridad de Microsoft para la respuesta ante incidentes: un equipo de expertos en ciberseguridad que ayuda a los clientes durante todo el ciberataque, desde la investigación hasta la contención con éxito y las actividades relacionadas con la recuperación. Los servicios se ofrecen a través de dos equipos altamente integrados, el Equipo de detección y respuesta (DART), centrado en la investigación y los preparativos para la recuperación, y la Práctica de seguridad de recuperación de compromiso (CRSP), que se centra en los aspectos de contención y recuperación.

Centro de inteligencia sobre amenazas de Microsoft (MSTIC): un equipo enfocado en la identificación, el seguimiento y la recopilación de inteligencia relacionada con los adversarios más sofisticados y avanzados que impactan a los clientes de Microsoft, incluidas las amenazas de estado de nación, el malware y el phishing.

One Engineering System (1ES): un equipo con la misión de ofrecer herramientas de primera clase para ayudar a los desarrolladores de Microsoft a ser lo más productivos y seguros posible. El equipo dirige la estrategia central para asegurar la cadena de suministro de software de Microsoft de extremo a extremo.

Centro de inteligencia sobre amenazas operativas (OpTIC): el equipo responsable de administrar y difundir la información sobre ciberamenazas que respalda la misión del Centro de operaciones de ciberdefensa (CDOC) de Microsoft para proteger a Microsoft y a nuestros clientes.

Microsoft

Iluminar el panorama de las amenazas y potenciar una defensa digital.

- Más información: **https://microsoft.com/mddr**
- Profundice: **https://blogs.microsoft.com/on-the-issues/**
- Manténgase conectado: **@msftissues y @msftsecurity**