Microsoft

Relatório de Defesa Digital da Microsoft de 2022

A iluminar o panorama de ameaças e a capacitar uma defesa digital.

Índice

Os dados, os insights e os eventos neste relatório são de julho de 2021 a junho de 2022 (Ano fiscal da Microsoft de 2022), exceto se indicado de outra forma.

Para uma melhor experiência de visualização e navegação neste relatório, recomendamos a utilização do Adobe Reader, disponível para download gratuito a partir do site da Adobe.

Introdução por Tom Burt

Vice-Presidente Empresarial, Segurança e Confiança do Cliente

"Os biliões de sinais que analisamos a partir do nosso ecossistema de produtos e serviços em todo o mundo revelam a ferocidade, o âmbito e a dimensão das ameaças digitais globalmente"

Um instantâneo do nosso panorama...

Âmbito e dimensão do panorama de ameaças

O volume de ataques de palavra-passe aumentou para cerca de 921 ataques a cada segundo, um aumento de 74% em apenas um ano.

Desmantelar o cibercrime

Até à data, a Microsoft removeu mais de 10.000 domínios utilizados por cibercriminosos e 600 utilizados por atores estatais.

Resolver vulnerabilidades

93% dos nossos compromissos de resposta a incidentes de ransomware revelaram controlos insuficientes sobre o acesso privilegiado e o movimento lateral.

Em 23 de fevereiro de 2022, o mundo da cibersegurança entrou numa nova era, a era da guerra híbrida. Nesse dia, horas antes de os mísseis serem lançados e os tanques atravessarem as fronteiras, os atores russos lançaram um ciberataque destrutivo contra o governo ucraniano, a tecnologia e os objetivos do setor financeiro. Pode ler mais sobre estes ataques e as lições a aprender com os mesmos no capítulo das Ameaças de Estado-nação desta terceira edição anual do Relatório de Defesa Digital da Microsoft (MDDR). A lição chave é que a cloud oferece a melhor segurança física e lógica contra os ciberataques e permite avanços na análise de informações de ameaças e na proteção de endpoints que provaram o seu valor na Ucrânia.

Apesar de qualquer desenvolvimento do ano em cibersegurança devesse começar aí, o relatório deste ano fornece uma visão muito mais aprofundada. No primeiro capítulo do relatório, concentramo-nos nas atividades dos cibercriminosos, enquanto que o segundo capítulo aborda as ameaças de Estado-nação. Ambos os grupos aumentaram significativamente a sofisticação dos seus ataques, o que aumentou drasticamente o impacto das suas ações. Enquanto a Rússia dirigia as manchetes, os atores iranianos escalaram os seus ataques após uma transição do poder presidencial, lançando ataques destrutivos direcionados a Israel e operações de ransomware e de acesso ilícito e fuga, visando a infraestrutura crítica nos Estados Unidos. A China também aumentou os seus esforços de espionagem no sudeste asiático e em outras partes do sul do globo, procurando contrariar a influência dos EUA e roubar dados e informações críticas.

Os atores estrangeiros também estão a utilizar técnicas altamente eficazes para possibilitar a influência das operações de propaganda em regiões em todo o mundo, conforme abordado no terceiro capítulo. Por exemplo, a Rússia trabalhou arduamente para convencer os seus cidadãos e os cidadãos de muitos outros países de que a sua invasão à Ucrânia se justificava, ao mesmo tempo que semeava a propaganda a desacreditar as vacinas contra a COVID no Ocidente e, simultaneamente, a promover a sua eficácia em casa. Além disso, os atores estão cada vez mais a visar dispositivos de controlo da Internet of Things (IoT) ou dispositivos de tecnologia operacional (OT) como pontos de entrada para redes e uma infraestrutura crítica que é discutida no capítulo quatro. Finalmente, no último capítulo, fornecemos os insights e as lições que aprendemos ao longo do ano passado ao defender os ataques dirigidos à Microsoft e aos nossos clientes à medida que revemos os desenvolvimentos do ano em resiliência cibernética.

Cada capítulo fornece as principais lições aprendidas e insights com base no ponto de vantagem exclusivo da Microsoft. Os biliões de sinais que analisamos a partir do nosso ecossistema de produtos e serviços em todo o mundo revelam a ferocidade, o âmbito e a dimensão das ameaças digitais globalmente. A Microsoft está a tomar medidas para defender os nossos clientes e o ecossistema digital contra estas ameaças, e pode ler mais sobre a nossa tecnologia que identifica e bloqueia biliões de tentativas de phishing, roubos de identidade e outras ameaças aos nossos clientes.

Introdução por Tom Burt

Continuação

Também utilizamos meios jurídicos e técnicos para apreender e encerrar a infraestrutura utilizada por cibercriminosos e atores do estado-nação, e notificar os clientes quando estão a ser ameaçados ou atacados por um ator do estado-nação. Trabalhamos para desenvolver funcionalidades e serviços cada vez mais eficazes que utilizam a tecnologia de IA/ML para identificar e impedir que as ciberameaças e os profissionais de segurança se defendam e identifiquem intrusões cibernéticas de forma mais rápida e eficaz.

Talvez o mais importante seja, em todo o MDDR, o facto de oferecermos os nossos melhores conselhos sobre os passos que as pessoas, as organizações e as empresas podem individualmente adotar para se defenderem contra estas ameaças digitais crescentes. A adoção de boas práticas de higiene cibernética é a melhor defesa e pode reduzir significativamente o risco de ciberataques.

O estado do cibercrime

Os cibercriminosos continuam a atuar como empresas de lucro sofisticadas. Os atacantes estão a adaptar-se e a encontrar novas formas de implementar as suas técnicas, aumentando a complexidade da forma e do local onde alojam a infraestrutura de operações de campanha. Ao mesmo tempo, os cibercriminosos estão a tornar-se mais frugais. Para reduzir as suas despesas gerais e aumentar a aparência de legitimidade, os atacantes estão a comprometer as redes de negócio e os dispositivos para alojar campanhas de phishing, malware ou inclusivamente para utilizar o seu poder de computação para minerar criptomoedas.

Saiba mais na pág. 6

"O advento da implementação de armas cibernéticas na guerra híbrida na Ucrânia é o início de uma nova era de conflito."

Ameaças de estado-nação

Os atores do estado-nação estão a lançar ataques cibernéticos cada vez mais sofisticados, concebidos para evitar a sua deteção e reforçar as suas prioridades estratégicas. O advento da implementação de armas cibernéticas na guerra híbrida na Ucrânia é o início de uma nova era de conflito. A Rússia também apoiou a guerra com operações de influência da informação, utilizando propaganda para criar impacto nas opiniões na Rússia, na Ucrânia e globalmente. Fora da Ucrânia, os atores do Estado-nação aumentaram a atividade e começaram a utilizar os avanços na automatização, na infraestrutura de cloud e nas tecnologias de acesso remoto para atacarem um conjunto mais amplo de alvos. As cadeias de abastecimento empresariais de TI que permitem o acesso aos alvos finais foram frequentemente atacadas. A higiene da segurança cibernética tornou-se ainda mais crítica à medida que os atores exploravam rapidamente vulnerabilidades não corrigidas, utilizavam tanto técnicas sofisticadas, como de força bruta para roubarem as credenciais e ofuscaram as suas operações através da utilização de software open source ou legítimo. Além disso, o Irão junta-se à Rússia na utilização de armas cibernéticas destrutivas, incluindo o ransomware, como um elemento essencial dos seus ataques.

Estes desenvolvimentos exigem a adoção urgente de um enquadramento global consistente que dê prioridade aos direitos humanos e proteja as pessoas contra o comportamento online imprudente do Estado. Todas as nações devem trabalhar em conjunto para implementar normas e regras para uma conduta responsável do Estado.

Saiba mais na pág. 30

Dispositivos e infraestrutura

A pandemia, aliada à rápida adoção de todos os tipos de dispositivos com acesso à Internet no âmbito da aceleração da transformação digital, aumentou significativamente a superfície de ataque do nosso universo digital. Como resultado, os cibercriminosos e os Estados-nação estão rapidamente a tirar partido dessa situação. Apesar do reforço da segurança de hardware e de software de TI nos últimos anos, a segurança da IoT e dos dispositivos de OT não acompanhou o ritmo. Os atores das ameaças estão a explorar estes dispositivos para aceder às redes e permitir o movimento lateral, para criar uma base forte na cadeia de fornecimento ou para perturbar as operações de OT da organização alvo.

Saiba mais na pág. 56

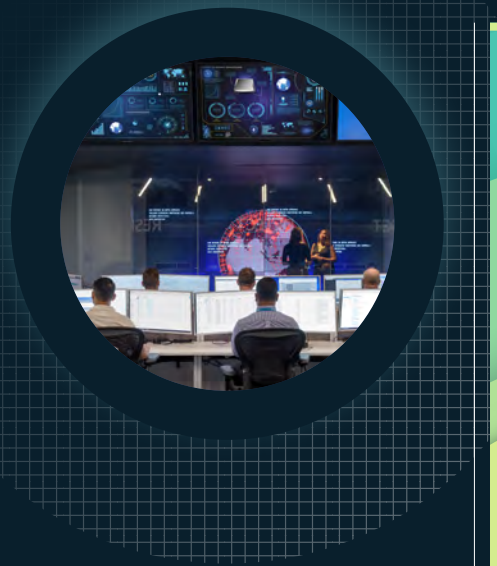
Introdução por Tom Burt

Continuação

Operações de ciberinfluência

Os estados-nação estão a utilizar cada vez mais operações sofisticadas de influência para distribuir propaganda e criar impacto na opinião pública, tanto a nível nacional como internacional. Estas campanhas corroem a confiança, aumentam a polarização e ameaçam os processos democráticos. Os habilidosos atores Manipuladores Persistentes Avançados estão a utilizar os meios de comunicação tradicionais juntamente com a internet e as redes sociais para aumentarem significativamente o âmbito, a dimensão e a eficiência das suas campanhas, e o impacto de grande dimensão que estão a ter no ecossistema de informações global. No ano passado, vimos estas operações utilizadas como parte da guerra híbrida da Rússia na Ucrânia, mas também vimos a Rússia e outras nações, incluindo a China e o Irão, a implementarem cada vez mais operações de propaganda alimentadas por redes sociais para alargarem a sua influência global numa série de assuntos.

Saiba mais na pág. 71



Resiliência cibernética

A segurança é um fator-chave para o sucesso tecnológico. A inovação e a melhoria da produtividade só podem ser alcançadas através da introdução de medidas de segurança que tornem as organizações o mais resilientes possível contra ataques modernos. A pandemia desafiou-nos a mudar as nossas práticas e tecnologias de segurança na Microsoft para protegermos os nossos colaboradores onde quer que trabalhem. No ano passado, os atores de ameaças continuaram a tirar partido das vulnerabilidades expostas durante a pandemia e da mudança para um ambiente de trabalho híbrido. Desde então que o nosso principal desafio tem sido gerir a prevalência e a complexidade de vários métodos de ataque e aumentar a atividade do Estado-nação. Neste capítulo, abordamos em detalhe os desafios que enfrentamos e as defesas que mobilizamos em resposta aos nossos mais de 15.000 parceiros.

Saiba mais na pág. 86

O nosso ponto de vantagem exclusivo

37 biliões
de ameaças de e-mail bloqueadas

34,7 biliões
de ameaças de identidade bloqueadas

43 biliões
de sinais sintetizados diariamente, utilizando análises de dados sofisticadas e algoritmos de IA para compreender e proteger contra as ameaças digitais e a ciberatividade criminosa.

+ de 8.500
engenheiros, investigadores, cientistas de dados, especialistas em cibersegurança, caçadores de ameaças, analistas geopolíticos, investigadores e equipas de inquiridos da linha de frente em 77 países.

+ de 15.000
parceiros no nosso ecossistema de segurança que aumentam a resiliência cibernética para os nossos clientes.

2,5 biliões
de sinais de endpoint analisados diariamente

De 1 de julho de 2021 a 30 de junho de 2022

Introdução por Tom Burt

Continuação

Acreditamos que a Microsoft, de forma independente e através de estreitas parcerias com o setor privado, governo e sociedade civil, tem a responsabilidade de proteger os sistemas digitais que sustentam o tecido social da nossa sociedade e promover ambientes de computação seguros e protegidos para cada pessoa, onde quer que estejam localizadas. Esta responsabilidade é a razão pela qual publicamos o MDDR todos os anos desde 2020. O relatório é o ponto culminante da imensidão de dados e da investigação abrangente da Microsoft. O relatório partilha os nossos insights exclusivos sobre a forma como o panorama de ameaças digitais está a evoluir e as ações cruciais que podem ser tomadas hoje mesmo para melhorar a segurança do ecossistema.

Esperamos incutir um sentimento de urgência, para que os leitores tomem medidas imediatas com base nos dados e nos insights que apresentamos aqui e nas nossas inúmeras publicações de cibersegurança ao longo do ano. À medida que consideramos a gravidade da ameaça para o panorama digital, e a sua tradução para o mundo físico, é importante lembrar que todos estamos habilitados a tomar medidas para nos protegermos, às nossas organizações e às empresas contra as ameaças digitais.

Obrigado por ter disponibilizado o seu tempo para analisar o Relatório de Defesa Digital da Microsoft deste ano. Esperamos que perceba que fornece sugestões e insights valiosos para nos ajudar a defender coletivamente o ecossistema digital.

Tom Burt
Vice-Presidente Empresarial,
Segurança e Confiança do Cliente

O nosso objetivo com este relatório é ambivalente:

1. Iluminar o panorama de ameaças digitais em evolução para os nossos clientes, parceiros e intervenientes que abrangem o ecossistema mais amplo, esclarecendo os novos ciberataques e a evolução das tendências em ameaças historicamente persistentes.
2. Capacitar os nossos clientes e parceiros para melhorarem a sua resiliência cibernética e responderem a estas ameaças.

O Estado do Cibercrime

À medida que as defesas cibernéticas melhoram e mais organizações adotam uma abordagem proativa à prevenção, os atacantes vão adaptando as suas técnicas.

Uma descrição geral do

Estado do Cibercrime

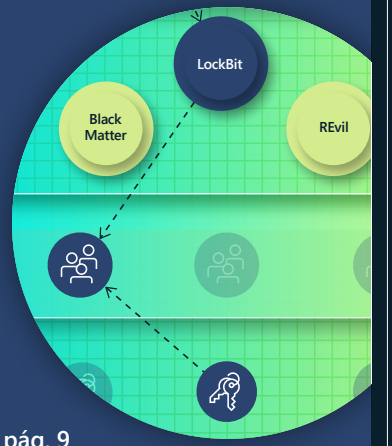
À medida que as defesas cibernéticas melhoram e mais organizações adotam uma abordagem proativa à prevenção, os atacantes vão adaptando as suas técnicas.

Os cibercriminosos continuam a atuar como empresas de lucro sofisticadas. Os atacantes estão a adaptar-se e a encontrar novas formas de implementar as suas técnicas, aumentando a complexidade da forma e do local onde alojam a infraestrutura de operações de campanha. Ao mesmo tempo, os cibercriminosos estão a tornar-se mais frugais. Para reduzir as suas despesas gerais e aumentar a aparência de legitimidad os atacantes estão a comprometer as redes de negócio e os dispositivos para alojar campanhas de phishing, malware ou inclusivamente para utilizar o seu poder de computação para minerar criptomoedas.

O cibercrime continua a aumentar à medida que a industrialização da economia do cibercrime reduz a barreira de competências à entrada, fornecedor maior acesso às ferramentas e à infraestrutura.

Saiba mais na pág. 18

A ameaça do ransomware e de extorsão está a tornar-se mais ousa com ataques dirigidos a governos, empresas e infraestruturas críticas.



Saiba mais na pág. 9

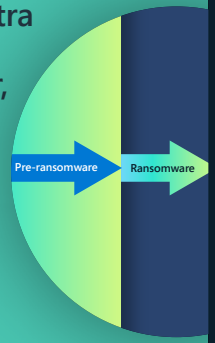
Os atacantes ameaçam cada vez mais a divulgar dados confidenciais para encorajar o pagamento de resgates.

Saiba mais na pág. 10

O ransomware operado pelo homem é o mais prevalente, uma vez que um terço dos alvos são comprometidos com sucesso por criminosos que utilizam estes ataques e 5% dos mesmos são resgatados.

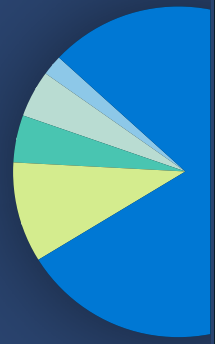
Saiba mais na pág. 9

A defesa mais eficaz contra o ransomware inclui a autenticação multifator, patches de segurança frequentes e princípios de Confiança Zero em toda a arquitetura de rede.



Saiba mais na pág. 13

Os esquemas de phishing de credenciais que visam indiscriminadamente todas as caixas de entrada estão em crescimento e o compromisso de e-mail empresarial, incluindo a fraude de faturas, representa um risco de cibercriminalidade significativo para as empresas.



Saiba mais na pág. 21

Para revolucionar as infraestruturas maliciosas dos cibercriminosos e dos atores do estado-nação, a Microsoft baseia-se em abordagens jurídicas inovadoras e nas nossas parcerias públicas e privadas.

Saiba mais na pág. 25

Introdução

O cibercrime continua a crescer, com aumentos tanto nos ataques aleatórios, como nos direcionados.

À medida que as defesas cibernéticas melhoram e mais governos e empresas têm uma abordagem proativa à prevenção, vemos os atacantes a utilizar duas estratégias para obter o acesso necessário para facilitar o cibercrime. Uma abordagem é uma campanha com alvos abrangentes que depende do volume. A outra utiliza a vigilância e objetivos mais seletivos para aumentar a taxa de retorno. Mesmo quando a geração de receitas não é o objetivo, como é o caso das atividades do Estado-nação para fins geopolíticos, são utilizados ataques aleatórios e direcionados. No ano passado, os cibercriminosos continuaram a contar com a engenharia social e a exploração de problemas tópicos para maximizar o sucesso das campanhas. Por exemplo, enquanto os engodos de phishing com a temática da COVID foram sendo utilizados com menor frequência, observamos o aumento dos engodos que solicitam doações para apoiar os cidadãos da Ucrânia.

Os atacantes estão a adaptar-se e a encontrar novas formas de implementar as suas técnicas, aumentando a complexidade da forma e do local onde alojam a infraestrutura de operações de campanha. Observamos que os cibercriminosos estão a tornar-se mais frugais e os atacantes já não estão a pagar pela tecnologia. Para reduzir as suas despesas gerais e aumentar a aparência de legitimidade, alguns atacantes procuram cada vez mais comprometer os negócios a alojar campanhas de phishing, malware ou inclusivamente a utilizar o seu poder de computação para minerar criptomoedas.

Neste capítulo, também examinamos o aumento do acesso ilícito, uma perturbação causada por cidadãos privados que realizam ciberataques a novos objetivos sociais ou políticos. Milhares de pessoas em todo o mundo, tanto especialistas como novatos, mobilizaram-se para lançarem ataques desde fevereiro de 2022, como a desativação de websites e a fuga de dados roubados como parte da guerra entre a Rússia e a Ucrânia. É muito cedo para prever se esta tendência vai continuar após o fim das hostilidades ativas.

As organizações têm de rever e reforçar regularmente os controlos de acesso e implementar estratégias de segurança para se defenderem contra ciberataques. No entanto, não é só isso que podem fazer. Explicamos como a nossa Unidade de Crimes Digitais (DCU) utilizou os processos civis para apreender a infraestrutura maliciosa utilizada pelos cibercriminosos e os atores do estado-nação. Temos de combater esta ameaça juntos através de parcerias públicas e privadas. Esperamos que, ao partilhar o que aprendemos ao longo dos últimos 10 anos, ajudemos os outros a compreender e a considerar as medidas proativas que podem adotar para se protegerem a si próprios e ao ecossistema mais amplo contra a crescente ameaça do cibercrime.

Amy Hogan-Burney
Diretor Geral, Unidade de Crimes Digitais

Ransomware e extorsão: uma ameaça de nível nacional

Os ataques de ransomware representam um risco acrescido para todos os indivíduos, uma vez que a infraestrutura crítica, as empresas de todas as dimensões e os governos estatais e municipais são alvo de criminosos que aproveitam um ecossistema crescente de cibercrime.

Nos últimos dois anos, os incidentes de ransomware de perfil elevado, como os que envolvem infraestrutura crítica, cuidados de saúde e fornecedores de serviços de TI, atraíram grande atenção do público. À medida que os ataques de ransomware se tornaram mais audazes no seu âmbito, os seus efeitos tornaram-se mais amplos. Seguem-se alguns exemplos de ataques já vistos em 2022:

- Em fevereiro, um ataque a duas empresas afetou os sistemas de processamento de pagamentos de centenas de postos de gasolina no norte da Alemanha.[1]
- Em março, um ataque contra o serviço postal da Grécia interrompeu temporariamente a entrega de e-mails e afetou o processamento de transações financeiras.[2]
- No final de maio, um ataque de ransomware contra agências do governo da Costa Rica forçou uma a declaração de emergência nacional depois de os hospitais serem encerrados e interrompida a cobrança de taxas aduaneiras e tributárias.[3]
- Também em maio, um ataque causou atrasos e cancelamentos de voos numa das maiores companhias aéreas da Índia, deixando centenas de passageiros retidos.[4]

O sucesso destes ataques e a extensão dos seus impactos no mundo real são o resultado de uma industrialização da economia do cibercrime, permitindo o acesso a ferramentas e infraestrutura e expandindo as capacidades dos cibercriminosos ao reduzir a sua barreira de competências à entrada.

Nos últimos anos, o ransomware mudou de um modelo no qual um único "gangue" iria desenvolver e distribuir uma carga de ransomware para o modelo de ransomware como um serviço (RaaS). O RaaS permite a um grupo gerir o desenvolvimento da carga de ransomware e prestar serviços de pagamento e extorsão através da fuga de dados para outros cibercriminosos (aqueles que realmente lançam os ataques de ransomware), referidos como "afiliados" para uma redução dos lucros. Este franchising da economia do cibercrime aumentou o conjunto de atacantes. A industrialização de ferramentas de cibercriminosos facilitou a execução de intrusões, a extração de dados e a implementação de ransomware aos atacantes.

O ransomware operado por humanos[5], um termo cunhado por investigadores da Microsoft para descrever as ameaças conduzidas por humanos que tomam decisões em todas as fases dos ataques com base no que descobrem na rede do seu alvo e delineiam a ameaça dos ataques de ransomware de produtos, continua a ser uma ameaça significativa para as organizações.

Modelo baseado nos dados do Microsoft Defender para Endpoint (EDR) (de janeiro a junho de 2022).

Ransomware e extorsão: uma ameaça ao nível da nação

Continuação

Os ataques de ransomware tornaram-se ainda mais impactantes porque a adoção de uma estratégia de monetização de extorsão dupla se tornou numa prática padrão. Isto implica a extração de dados a partir de dispositivos comprometidos, encriptando os dados nos dispositivos e, em seguida, publicando ou ameaçando publicar os dados roubados publicamente para pressionar as vítimas a pagarem um resgate.

Apesar de a maioria dos atacantes de ransomware o implementar de forma oportunista em qualquer rede a que obtém acesso, alguns adquirem acesso de outros cibercriminosos, alavancando as ligações entre os mediadores de acesso e os operadores de ransomware.

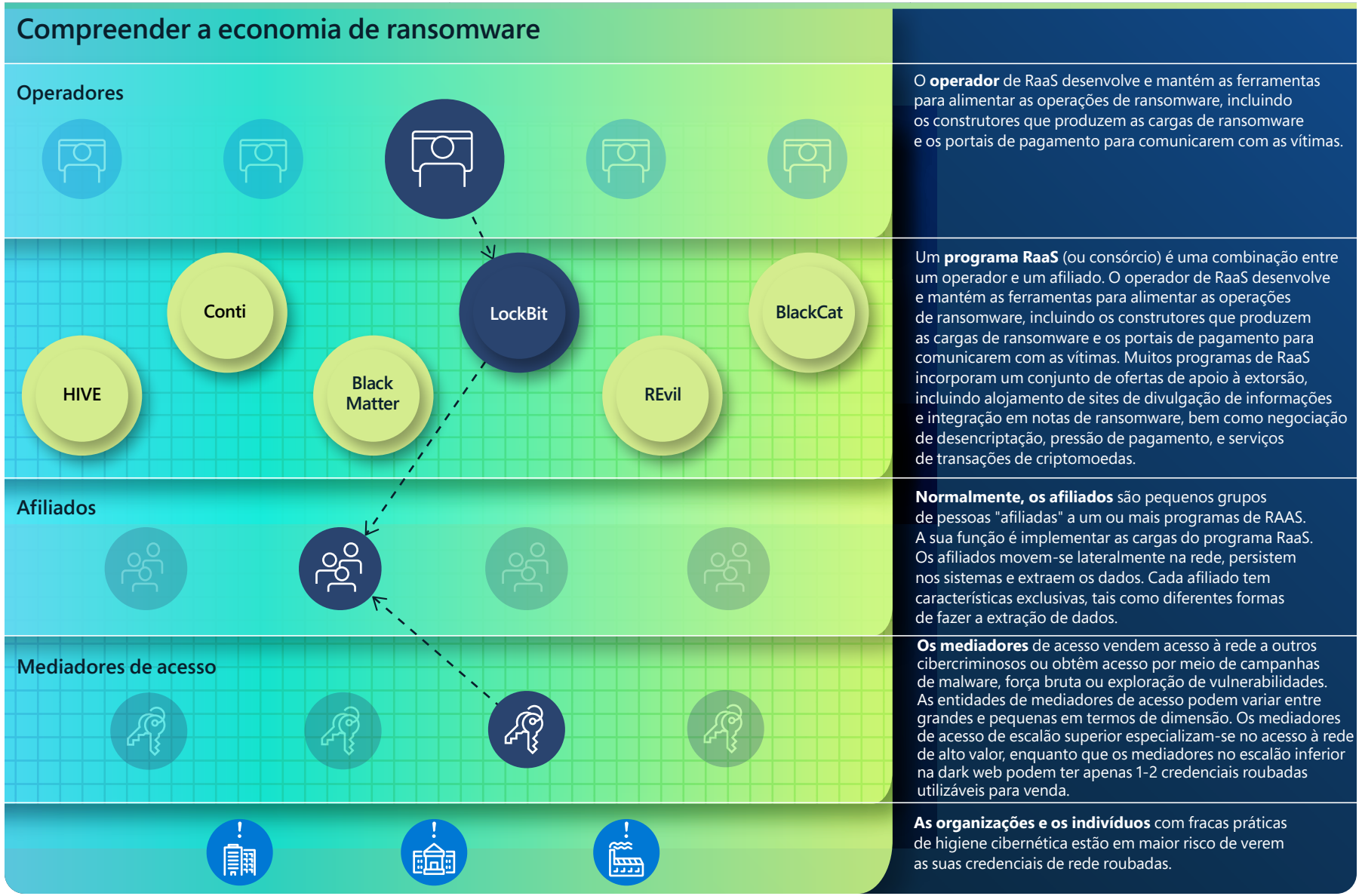
A nossa amplitude de inteligência de sinais exclusiva é recolhida a partir de várias origens (identidade, e-mail, endpoints e cloud) e fornece insights sobre a economia de ransomware crescente, juntamente com um sistema de afiliados que inclui ferramentas concebidas para os atacantes tecnicamente menos competentes.

A expansão das relações entre cibercriminosos especializados aumentou o ritmo, a sofisticação e o sucesso dos ataques de ransomware. Isto impulsionou a evolução do ecossistema de cibercriminosos em atores ligados com diferentes técnicas, objetivos e conjuntos de competências que se apoiam mutuamente no acesso inicial a alvos, serviços de pagamento e ferramentas ou sites de desencriptação ou publicação.

Os operadores de ransomware podem agora adquirir acesso a organizações ou redes governamentais online ou obter credenciais e acesso através de relações interpessoais com mediadores cujo objetivo principal é rentabilizar exclusivamente o acesso que adquiriram.

Em seguida, os operadores utilizam o acesso adquirido para implementar uma carga de ransomware comprada através de mercados ou fóruns da Dark Web. Em muitos casos, as negociações com as vítimas são conduzidas pela equipa RaaS, e não pelos próprios operadores. Estas transações criminosas são totalmente integradas e os participantes arriscam muito pouco ao serem detidos e se for apresentada queixa devido ao anonimato da Dark Web e às dificuldades em aplicar as leis transnacionais.

Um esforço sustentável e bem-sucedido contra esta ameaça vai exigir a execução de toda uma estratégia governamental em estreita parceria com o setor privado.



Contrariamente à forma como o ransomware é por vezes retratado nos meios de comunicação, é raro uma única variante de ransomware ser gerida por um "gangue de ransomware" de ponta a ponta. Por sua vez, existem entidades separadas que criam malware, obtêm acesso às vítimas, implementam ransomware e tratam de negociações de extorsão. A industrialização do ecossistema criminal levou a:

- Mediadores de acesso que entram e divulgam o acesso (acesso como um serviço).
- Programadores de malware que vendem ferramentas.
- Atores criminosos e afiliados que conduzem intrusões.
- Fornecedores de serviços de encriptação e extorsão que fazem a monetização dos afiliados (RaaS).

Todas as campanhas de ransomware operado por humanos partilham dependências comuns nas fraquezas da segurança. Em termos específicos, os atacantes costumam tirar partido da má higiene cibernética de uma organização, que muitas vezes inclui a aplicação de correções esporádicas e a falha na implementação da autenticação multifator (MFA).

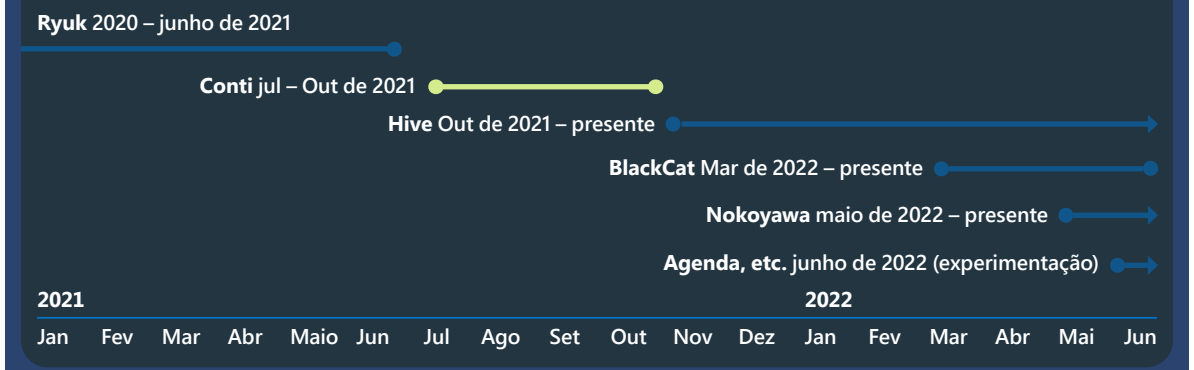
Caso prático: a dissolução do Conti

A Conti, uma das principais variantes de ransomware nos últimos dois anos, começou a encerrar as operações em meados de 2022, com o Centro de Informações Sobre Ameaças da Microsoft (MSTIC) a observar uma redução significativa da atividade no final de março e início de abril. Observámos as últimas implementações de ransomware do Conti em meados de abril. No entanto, tal como a cofragem de outras operações de ransomware, a dissolução do Conti não teve um impacto significativo nas implementações de ransomware, porque o MSTIC verificou a dinamização dos afiliados do Conti para implementar outras cargas de ransomware, incluindo BlackBasta, Lockbit 2,0, LockbitBlack e HIVE. Isto é consistente com os dados dos anos anteriores e sugere que, quando os gangues de ransomware ficam offline, voltam a surgir meses mais tarde ou a redistribuir as suas capacidades técnicas e recursos para novos grupos.

As nossas equipas de análise de informações de ameaças da Microsoft monitoriza os atores de ameaças de ransomware como grupos individuais (rotulados como DEV) com base nas suas ferramentas específicas, em vez de os monitorizar pelo malware que utilizam. Isto significava que, quando os afiliados do Conti se dispersavam, conseguíamos continuar a monitorizar estes programadores através da utilização de outras ferramentas ou kits de RaaS. Por exemplo:

- O DEV-0230, que é afiliado com o Trickbot, tinha sido um utilizador prolífico do Conti. No final de abril, o MSTIC observou-o a usar o QuantumLocker.
- O DEV-0237 passou do kit de ransomware do Conti para HIVE e Nokoyawa, incluindo a utilização de HIVE no ataque de 31 de maio contra as agências governamentais da Costa Rica.
- O DEV-0506, outro utilizador prolífico do kit de ransomware do Conti, foi observado com o BlackBasta.

Exemplo de um afiliado (DEV-0237) a mudar rapidamente entre programas RaaS



Depois de um programa RaaS, como o Conti, ser encerrado, o afiliado de ransomware muda para outro (Hive) quase imediatamente.

O RaaS evolui o ecossistema de ransomware e dificulta a atribuição

Como o ransomware operado por humanos é impulsionado por operadores individuais, os padrões de ataque variam de acordo com o destino e são alternados ao longo da duração de um ataque. No passado, observámos uma estreita relação entre o vetor de entrada inicial, as ferramentas e as opções de carga de ransomware em cada campanha de uma única estirpe de ransomware. Isto facilitou a atribuição. No entanto, o modelo de filial RaaS desassocia esta relação. Como resultado, a Microsoft controla os afiliados de ransomware que implementam cargas em ataques específicos, em vez de monitorizar os programadores de carga de ransomware como operadores.

Por outro lado, já não assumimos que o programador HIVE é o operador por detrás de um ataque de ransomware HIVE; o mais provável é que seja um afiliado.

O setor da cibersegurança tem lutado para capturar adequadamente esta delimitação entre programadores e operadores. O setor ainda relata com frequência um incidente de ransomware pelo seu nome de carga, o que dá a falsa impressão de que uma única entidade, ou gangue de ransomware, está por trás de todos os ataques utilizando essa carga de ransomware específica, e todos os incidentes associados ao mesmo partilham técnicas e infraestrutura comuns. Para dar suporte aos defensores de rede, é importante saber mais sobre as fases que precedem os ataques de diferentes afiliados, como a extração de dados e os mecanismos de persistência adicionais, e as oportunidades de deteção e proteção que poderão existir.

Mais do que o malware, os atacantes precisam de credenciais para serem bem sucedidos nas suas operações. A infeção com sucesso de ransomware operado por humanos de toda uma organização depende do acesso a uma conta altamente privilegiada.

Destaque sobre ataques de ransomware operado por humanos

Durante o último ano, os especialistas em ransomware da Microsoft realizaram investigações profundas sobre mais de 100 incidentes de ransomware operado por humanos para monitorizar as técnicas dos atacantes e compreender como proteger melhor os nossos clientes.

É importante ter em atenção que a análise que partilhamos aqui só é possível para dispositivos integrados e geridos. Os dispositivos não geridos e não integrados representam a parte menos segura dos ativos de hardware de uma organização.

Técnicas de fase de ransomware mais prevalentes:

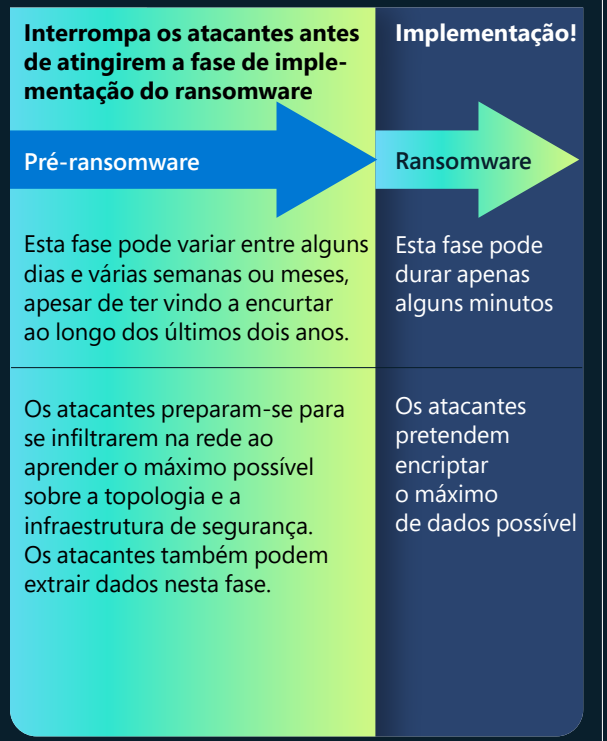
75%
Utilizam ferramentas de administração.

75%
Utilizam a conta de utilizador adquirida elevada e comprometida para espalhar cargas maliciosas através do protocolo SMB.

99%
Tentam adulterar a segurança e produtos de cópia de segurança descobertos através de ferramentas integradas no SO.

O típico ataque operado por humanos

Os ataques de ransomware operados por humanos podem ser categorizados na fase pré-ransomware e na fase de implementação do ransomware. Durante a fase pré-ransomware, os atacantes preparam-se para se infiltrarem na rede ao aprender sobre a tipologia e a infraestrutura de segurança da organização.



As nossas investigações constataram que a maioria dos atores por detrás dos ataques de ransomware operado por humanos tiram partido das fraquezas de segurança semelhantes e partilham padrões de ataque e técnicas comuns.

Uma estratégia de segurança duradoura

Combater e prevenir ataques desta natureza exige uma mudança na mentalidade de uma organização para se concentrar na proteção abrangente necessária para abrandar e parar os atacantes antes de poderem migrar da fase pré-ransomware para a fase de implementação do ransomware.

As empresas têm de aplicar as melhores práticas de segurança de forma consistente e agressiva às suas redes, com o objetivo de mitigar as classes de ataques. Devido à tomada de decisão humana, estes ataques de ransomware podem gerar múltiplos alertas de produtos de segurança aparentemente díspares, que podem ser facilmente perdidos ou não respondidos a tempo. A fadiga de alerta é real e os centros de operações de segurança (SOC) podem facilitar as suas vidas observando as tendências nos respetivos alertas ou agrupando alertas em incidentes para que possam ver o panorama geral. Em seguida, os SOC podem mitigar alertas através de funcionalidades de fortalecimento, como regras de redução da superfície de ataque. O fortalecimento contra as ameaças comuns pode não só reduzir o volume de alerta, mas também deter muitos atacantes antes de obterem acesso às redes.

As organizações têm de manter elevados padrões contínuos de postura de segurança e higiene de rede para se protegerem dos ataques de ransomware operado por humanos.

Insights acionáveis

Os atacantes de ransomware são motivados por lucros fáceis, pelo que aumentar os seus custos através do reforço da segurança é fundamental para perturbar a economia cibercriminosa.

1. Criar higiene de credenciais. Mais do que o malware, os atacantes precisam de credenciais para serem bem sucedidos nas suas operações. A infeção com sucesso de ransomware operado por humanos de toda uma organização depende do acesso a uma conta altamente privilegiada, como um Administrador de Domínio, ou capacidades para editar uma Política de Grupo.
2. Auditar a exposição das credenciais.
3. Priorize a implementação de atualizações do Active Directory.
4. Priorize o fortalecimento da cloud.
5. Reduza a superfície de ataque.
6. Fortaleça os ativos com acesso Internet e compreenda o seu perímetro.
7. Reduza a fadiga de alerta do SOC ao fortalecer a sua rede para reduzir o volume e preservar a largura de banda para incidentes de alta prioridade.

Ligações para mais informações

- RaaS: compreender a economia gig do cibercrime e como se proteger | Blogue Microsoft Security
- Ataques de ransomware operado por humanos: um desastre evitável | Blogue Microsoft Security

Insights de ransomware dos inquiridos da linha de frente

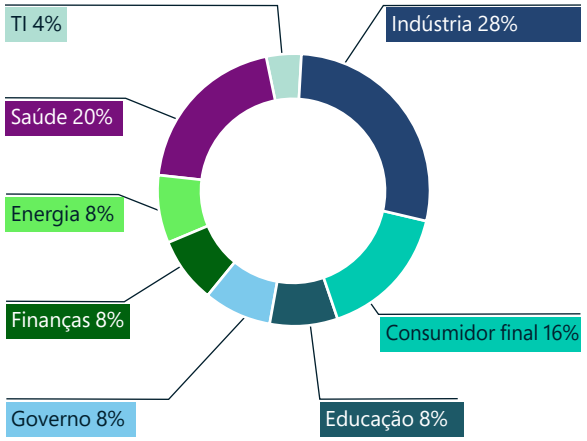
As organizações em todo o mundo registaram um crescimento constante nos ataques de ransomware operado por humanos a partir de 2019. No entanto, as operações de entrada em vigor da lei e os eventos geopolíticos no último ano tiveram um impacto significativo nas organizações cibercriminosas.

A Linha de Serviços de Segurança da Microsoft apoia os clientes durante um ciberataque completo, desde a investigação às atividades de contenção e recuperação bem-sucedidas. Os serviços de resposta e recuperação são oferecidos através de duas equipas altamente integradas, com uma a concentrar-se na investigação e nas bases para a recuperação e a segunda a focar-se na contenção e recuperação. Esta secção apresenta um resumo das conclusões baseadas nos compromissos de ransomware ao longo do ano passado.

93%

das investigações da Microsoft durante os compromissos de recuperação de ransomware revelaram acesso privilegiado insuficiente e controlos laterais dos movimentos.

Incidentes de ransomware e compromissos de recuperação por setor

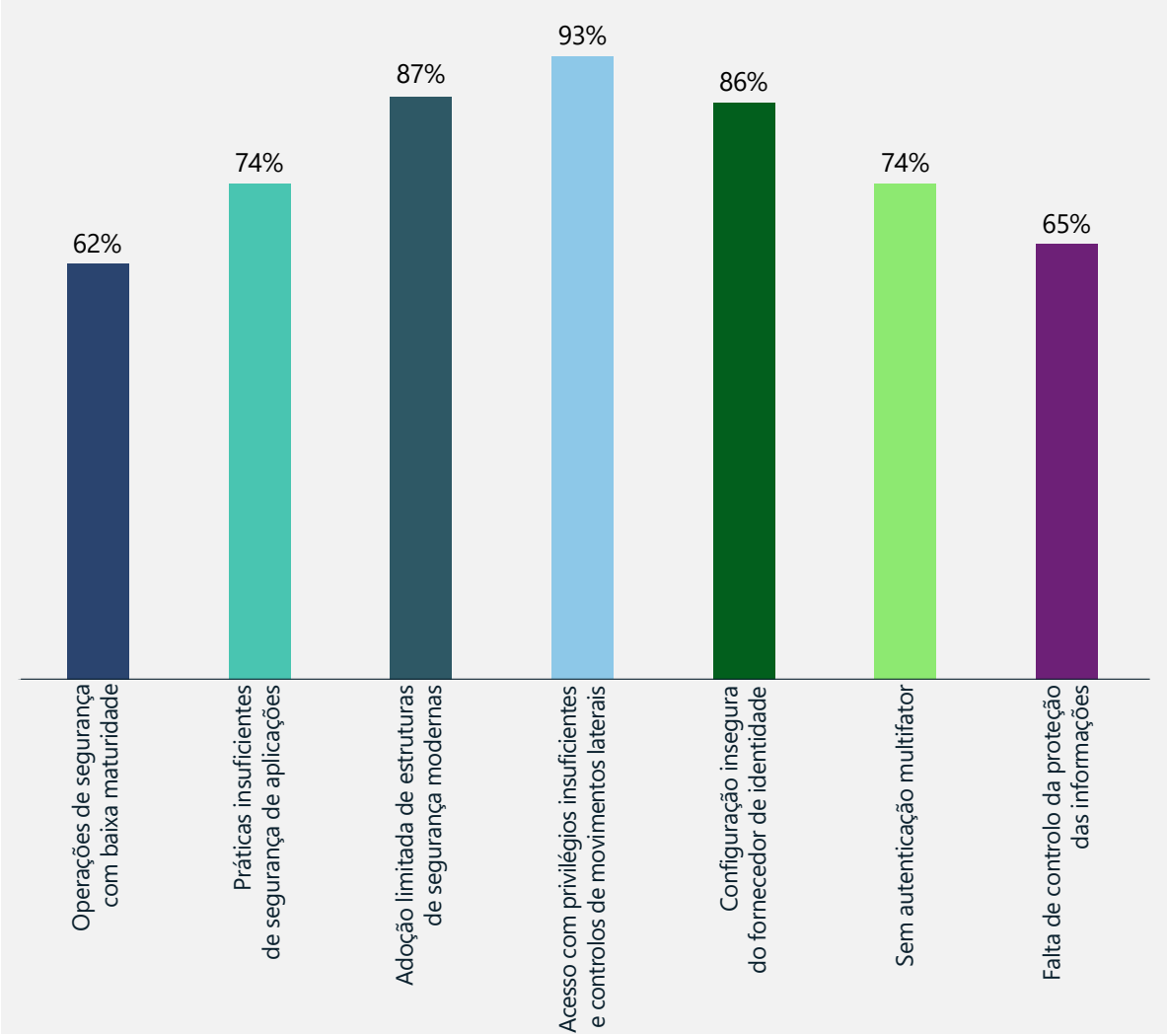


À medida que surgem novas ameaças e grupos pequenos, as equipas de defesa têm de estar cientes da evolução das ameaças de ransomware enquanto protegem contra famílias de malware de ransomware que antes eram desconhecidas. A abordagem de rápido desenvolvimento utilizada por grupos criminosos levou à criação de ransomware inteligente embalado em kits de fácil utilização. Isto permite uma maior flexibilidade para lançar ataques generalizados a um maior número de alvos.

As páginas seguintes fornecem uma visão mais aprofundada dos fatores mais observados e que contribuíram para uma fraca proteção contra o ransomware, agrupados em três categorias de resultados:

1. Fracos controlos de identidade
2. Operações de segurança ineficazes
3. Proteção limitada de dados

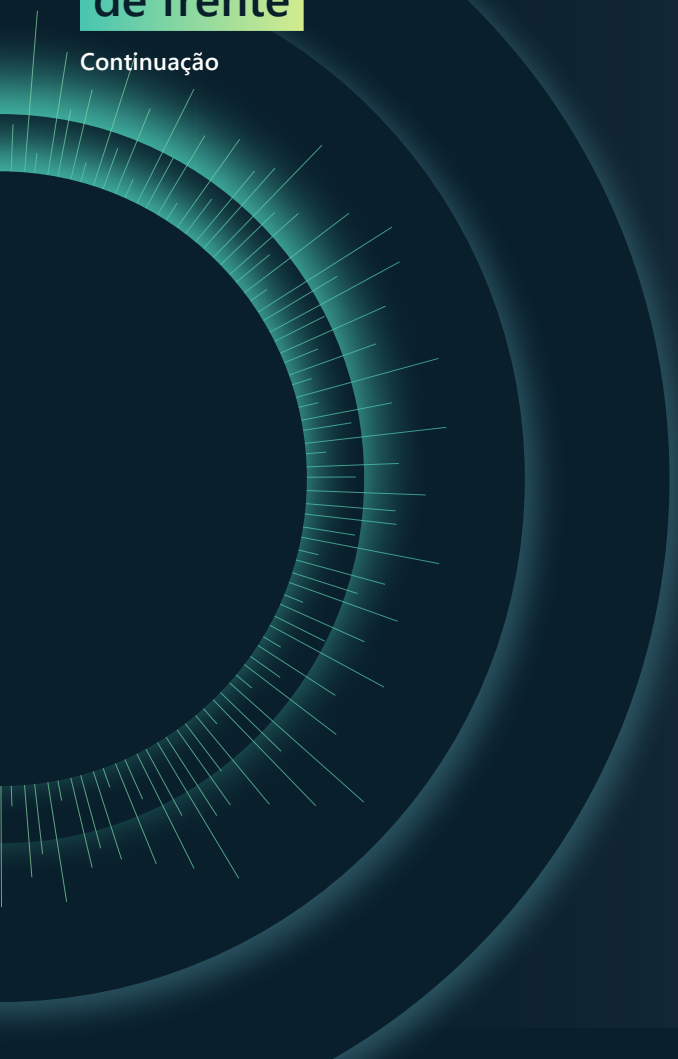
Resumo das conclusões mais comuns nos compromissos de resposta ao ransomware



A conclusão mais comum entre os compromissos de resposta a incidentes de ransomware foi o acesso privilegiado insuficiente e os controlos laterais dos movimentos.

Insights de ransomware dos inquiridos da linha de frente

Continuação



Os três principais fatores de contribuição observados nos nossos compromissos de resposta no local:

① **Fracos controlos de identidade:** os ataques de roubo de credenciais continuam a ser um dos principais fatores contribuintes

② **Os processos de operações de segurança ineficazes** não apresentam apenas uma janela de oportunidade para os atacantes, mas afetam significativamente o tempo de recuperação

③ Eventualmente, tudo se resume aos dados: as organizações lutam para implementar uma **estratégia de proteção de dados** eficaz que se alinha com as suas necessidades de negócio

① Fracos controlos de identidade

O ransomware operado por humanos continua a evoluir e a utilizar o roubo de credenciais e os métodos de movimento laterais tradicionalmente associados aos ataques direcionados. Os ataques bem-sucedidos são muitas vezes o resultado de campanhas de longa duração que envolvem o comprometimento de sistemas de identidade, como o Active Directory (AD), que permitem aos operadores humanos roubar credenciais, sistemas de acesso e permanecer persistentes na rede.

Segurança do Active Directory (AD) e do Azure AD

88%

dos clientes impactados não aplicaram as melhores práticas de segurança do AD e do Azure AD. Isto tornou-se um vetor de ataque comum à medida que os atacantes exploram as configurações erradas e as posturas de segurança mais fracas nos sistemas de identidade críticos para obter acesso e criar impacto mais amplamente nas empresas.

Menos privilégios acesso e utilização de Estações de Trabalho de Acesso Privilegiado (PAW)

Nenhuma das organizações impactadas implementou a segregação de credenciais administrativas adequada e os princípios de acesso menos privilegiados através de estações de trabalho dedicadas durante a gestão da sua identidade crítica e ativos de elevado valor, como sistemas proprietários e aplicações críticas para o negócio.

Segurança da conta com privilégios

88%

dos compromissos, a MFA não foi implementada para as contas confidenciais sensíveis e com altos privilégios, deixando uma lacuna de segurança para os atacantes comprometerem as credenciais e dinamizarem outros ataques através de credenciais legítimas.

84%

Os administradores em 84% das organizações não utilizam controlos de identidades privilegiados, como o acesso just-in-time para evitar mais utilizações nefastas de credenciais privilegiadas comprometidas.

Insights de ransomware dos inquiridos da linha de frente

Continuação

② Operações de segurança ineficazes

Os nossos dados mostram que as organizações que sofreram ataques de ransomware têm lacunas significativas nas suas operações de segurança, ferramentas e gestão do ciclo de vida do ativo de tecnologias da informação. Com base nos dados disponíveis, foram mais observadas as seguintes lacunas:

Aplicação de patches:

68%

das organizações impactadas não tiveram um processo de vulnerabilidade e gestão de patches eficaz, e uma elevada dependência de processos manuais versus correções automatizadas levou a aberturas críticas. A indústria e a infraestrutura crítica continuam a lutar contra a manutenção e a aplicação de patches de sistemas de tecnologia operacional legados (OT).

Falta de ferramentas de operações de segurança:

A maioria das organizações reportou uma falta de visibilidade de segurança integral devido a uma falta ou configuração incorreta das ferramentas de segurança, o que levou a uma diminuição na eficácia de deteção e resposta.

60%

das organizações não referiram a utilização de uma ferramenta EDR[6], uma tecnologia fundamental para deteção e resposta.

60%

não investiu na tecnologia de gestão de informações e eventos de segurança (SIEM) que conduz a silos de monitorização, capacidade limitada para detetar ameaças integrais e operações de segurança ineficientes. A automatização continua a ser uma lacuna chave nas ferramentas e processos do SOC, forçando a equipa SOC a passar inúmeras horas a compreender a telemetria de segurança.

84%

das organizações impactadas não permitem a integração dos seus ambientes multicloud nas suas ferramentas de operações de segurança.

Processos de resposta e recuperação:

76%

A falta de um plano de resposta eficaz era uma área crítica observada em 76% das organizações impactadas, impedindo a preparação adequada de crises organizacionais e influenciando negativamente o tempo de resposta e recuperação.

③ Proteção limitada de dados

Muitas organizações comprometidas careciam de processos de proteção de dados adequados que conduzissem a um impacto severo nos tempos de recuperação e na capacidade de retorno às operações de negócio. As lacunas mais comuns encontradas incluem:

Cópia de segurança imutável:

44%

das organizações não possuíam cópias de segurança imutáveis para os sistemas impactados. Os dados também mostram que os administradores não possuíam cópias de segurança e planos de recuperação para ativos críticos, como o AD.

Prevenção de perda de dados:

Normalmente, os atacantes encontram uma forma de comprometer os sistemas através da exploração de vulnerabilidades na organização, extraindo dados críticos para extorsão, roubo de propriedade intelectual ou monetização.

92%

das organizações impactadas não implementaram controlos de prevenção de perda de dados eficazes para mitigar estes riscos, o que levou a uma perda de dados crítica.

O ransomware diminuiu em algumas regiões e aumentou noutras

Este ano, observámos uma redução no número global de casos de ransomware comunicados às nossas equipas de resposta na América do Norte e na Europa, comparativamente com o ano anterior. Ao mesmo tempo, os casos relatados na América Latina aumentaram.

Uma interpretação desta observação é que os cibercriminosos se afastam das áreas que se percebem terem um maior risco de acionar o escrutínio da aplicação da lei em prol de alvos mais brandos. Dado que a Microsoft não observou uma melhoria substancial na segurança das redes empresariais em todo o mundo, para explicar a redução das chamadas de suporte relacionadas com o ransomware, acreditamos que a causa mais provável é uma combinação da atividade de aplicação da lei em 2021 e 2022 que aumentou o custo da atividade criminosa, juntamente com alguns eventos geopolíticos de 2022.

Uma das operações de RaaS mais prevalentes pertence a um grupo criminoso de língua russa, conhecido como REvil (também conhecido como Sodinokibi), que atua desde 2019. Em outubro de 2021, os servidores da REvil foram colocados offline como parte da aplicação da lei internacional da Operação GoldDust.[7] Em janeiro de 2022, a Rússia prendeu 14 alegados membros do REvil e invadiu 25 localizações associadas aos mesmos.[8] Esta foi a primeira vez que a Rússia agiu contra os operadores de ransomware no seu território.

Apesar de as atividades de aplicação da lei terem provavelmente diminuído a frequência dos ataques em 2022, os atores de ameaças podem desenvolver novas estratégias para evitar serem apanhados no futuro. Além disso, a tensão entre a Rússia e os Estados Unidos por causa da invasão da Rússia à Ucrânia parece ter colocado um ponto final na cooperação nascente da Rússia na luta global contra o ransomware. Após um breve período de incerteza que se seguiu às prisões de REvil, os Estados Unidos e a Rússia cessaram a cooperação na prossecução dos atores de ransomware, o que significa que os cibercriminosos poderão ver, mais uma vez, a Rússia como porto seguro.

Olhando para o futuro, prevemos que o ritmo das atividades de ransomware vá depender do resultado de algumas perguntas chave:

1. Os governos vão tomar medidas para impedir que os criminosos de ransomware operem dentro das suas fronteiras ou procuram perturbar os atores que operam a partir de territórios estrangeiros?
2. Os grupos de ransomware vão mudar as táticas para eliminar a necessidade de ransomware e recorrer a ataques do tipo extorsão?
3. As organizações vão conseguir modernizar e transformar as suas operações de TI mais depressa do que os criminosos podem explorar vulnerabilidades?
4. Os avanços na monitorização e rastreio dos pagamentos de resgate forçam os beneficiários de resgate a mudarem as táticas e as negociações?

Apesar de as atividades de aplicação da lei terem provavelmente diminuído a frequência dos ataques em 2022, os atores de ameaças podem desenvolver novas estratégias para evitar serem apanhados no futuro.

2X

Os ataques de ransomware diminuíram em algumas regiões, mas as exigências de resgate aumentaram mais do que o dobro.

Insights acionáveis

1. Concentre-se nas estratégias de segurança holística, à medida que todas as famílias de ransomware tiram partido das mesmas fraquezas de segurança para afetar uma rede.
2. Atualize e mantenha noções básicas de segurança para aumentar o nível básico de proteção em profundidade e modernizar as operações de segurança. A migração para a cloud permite detetar ameaças de forma mais rápida e responder mais rapidamente.

Ligações para mais informações

- Proteja a sua organização contra o ransomware | Microsoft Security
- 7 formas de fortalecer o seu ambiente contra comprometimento | Blogue Microsoft Security
- Melhorar as defesas baseadas na IA para interromper o ransomware operado pelo homem | Equipa de Investigação do Microsoft 365 Defender
- Security Insider: explore os mais recentes insights e atualizações de cibersegurança | Microsoft Security

Cibercrime como um serviço

O cibercrime como um serviço (CaaS) é uma ameaça crescente e em constante evolução para os clientes em todo o mundo. A Unidade de Crimes Digitais (DCU) da Microsoft observou o crescimento contínuo do ecossistema de CaaS com um número crescente de serviços online que facilitam vários cibercrimes, incluindo o BEC e o ransomware operado por humanos. O phishing continua a ser um método de ataque preferencial porque os cibercriminosos podem adquirir um valor significativo desde o roubo e a venda de acesso a contas roubadas com êxito.

Em resposta à expansão do mercado de CaaS, a DCU aprimorou os sistemas de escuta para detetar e identificar ofertas de CaaS em todo o ecossistema da Internet, na web profunda, nos fóruns controlados,[9] websites dedicados, fóruns de discussão online e em plataformas de mensagens.

Os cibercriminosos estão agora a colaborar em fusos horários e idiomas para fornecer resultados específicos. Por exemplo, um site de CaaS administrado por um indivíduo na Ásia mantém operações na Europa e cria contas maliciosas em África. O carácter multijurisdicional destas operações apresenta desafios complexos em matéria de legislação e imposição da lei. Em resposta, a DCU concentra os seus esforços na desativação da infraestrutura criminosa maliciosa utilizada para facilitar os ataques de CaaS e na colaboração com os organismos responsáveis pela aplicação da lei em todo o mundo para responsabilizar os criminosos.

Os cibercriminosos estão a utilizar cada vez mais a análise de dados para maximizar o alcance, o âmbito e os ganhos. Como as empresas legítimas, os websites de CaaS têm de assegurar a validade dos produtos e dos serviços para manterem uma reputação sólida. Por exemplo, os sites de CaaS automatizam de forma rotineira o acesso a contas comprometidas para assegurar a validade das credenciais comprometidas. Os cibercriminosos irão interromper as vendas de contas específicas quando as palavras-passe forem repostas ou as vulnerabilidades forem corrigidas. Cada vez mais, identificámos websites de CaaS que fornecem aos compradores a verificação on-demand como um processo de controlo de qualidade. Como resultado, os compradores podem ter a certeza de que o site de CaaS vende contas ativas e palavras-passe, ao mesmo tempo que reduz os custos potenciais para o comerciante de CaaS se as credenciais roubadas forem corrigidas antes da venda.

A DCU também observou websites de CaaS que ofereciam aos compradores a opção de adquirir contas comprometidas de localizações geográficas específicas, fornecedores de serviços online designados e indivíduos, profissões e indústrias direcionados especificamente. As contas frequentemente pedidas concentram-se nos profissionais ou departamentos que processam a faturação, como os CFO ou as "Contas a Receber".

Da mesma forma, as indústrias que participam na contratação pública são muitas vezes o alvo devido à quantidade de informações disponibilizadas através do processo de licitação pública.

As investigações da DCU sobre o CaaS surgiram de várias tendências principais:

O número e a sofisticação dos serviços estão a aumentar.

Um exemplo é a evolução de shells Web que normalmente consistem em servidores Web comprometidos utilizados para automatizar ataques de phishing. A DCU observou os revendedores de CaaS a simplificarem o carregamento de kits de phishing ou malware através de dashboards Web especializados. Muitas vezes, os vendedores de CaaS tentam posteriormente vender serviços adicionais ao agente de ameaças através do dashboard, como serviços de mensagens de spam e listas de destinatários de spam especializadas, com base nos atributos definidos, incluindo a localização geográfica ou a profissão. Em alguns casos, observamos um único shell Web a ser utilizado em várias campanhas de ataque, o que sugere que os atores de ameaças podem manter o acesso persistente ao servidor comprometido. Também observamos um aumento nos serviços de anonimização disponíveis como parte do ecossistema de CaaS, bem como ofertas para redes privadas virtuais (VPN) e contas de servidor privado virtual (VPS). Na maioria dos casos, as VPN/VPS oferecidas foram inicialmente obtidas através de cartões de crédito roubados. Os websites de CaaS também ofereceram um maior número do protocolo de ambiente de trabalho remoto (RDP), shell de segurança (SSH) e cPanels para utilização como uma plataforma para orquestrar ataques de cibercrime. Os comerciantes de CaaS configuram o RDP, SSH e cPanels com ferramentas e scripts adequados para facilitar vários tipos de ciberataques.

Os serviços de criação de domínios homógrafos exigem cada vez mais o pagamento em criptomoedas.

Os domínios homógrafos personificam nomes de domínio legítimos ao utilizar caracteres idênticos ou praticamente idênticos a outro caracter em termos de aparência. O objetivo é induzir o espetador a pensar que o domínio homógrafo é o domínio genuíno. Estes domínios são uma ameaça omnipresente e um gateway para uma quantidade significativa de cibercrime. Os sites de CaaS vendem agora nomes de domínio de homógrafos personalizados, o que permite aos compradores solicitarem nomes de domínios e empresas específicos para personificar. Depois de recebido o pagamento, os comerciantes de CaaS utilizam uma ferramenta geradora de homógrafos para selecionar o nome do domínio e, em seguida, registar o homógrafo malicioso. O pagamento deste serviço é quase exclusivamente feito em criptomoedas.

2.750.000

de registos no site bloqueados com êxito pela DCU, este ano, para se antecipar aos atores criminosos que planeavam utilizar os mesmos para se envolverem no cibercrime global.

Cibercrime como um serviço

Continuação

Os vendedores de CaaS oferecem cada vez mais credenciais comprometidas para compra.

As credenciais comprometidas permitem o acesso não autorizado a contas de utilizador, incluindo o serviço de mensagens de e-mail, recursos de partilha de ficheiros empresariais e o OneDrive para empresas. Se as credenciais do administrador forem comprometidas, os utilizadores não autorizados poderão obter acesso a ficheiros confidenciais, recursos de Azure e contas de utilizador da empresa. Em muitos casos, as investigações da DCU identificaram a utilização não autorizada da mesma credencial em vários servidores como uma forma de automatizar as credenciais de verificação. Este padrão sugere que o utilizador comprometido pode ser vítima de vários ataques de phishing ou ter malware de dispositivo que permite aos keyloggers do botnet recolher credenciais.

Os serviços e produtos de CaaS com funcionalidades avançadas estão a emergir para evitar a deteção.

Um vendedor de CaaS oferece kits de phishing com maiores níveis de complexidade e funcionalidades de anonimização concebidas para contornar os sistemas de deteção e prevenção pelo valor de 6 USD por dia. O serviço oferece uma série de redirecionamentos que executam verificações antes de permitir o tráfego para a camada ou o site seguinte. Um destes executa mais de 90 verificações para impressão digital do dispositivo, incluindo se é uma máquina virtual, reunindo detalhes sobre o browser e o hardware que estão a ser utilizados e muito mais. Se todas as verificações passarem, o tráfego é enviado para uma página de destino utilizada para phishing.

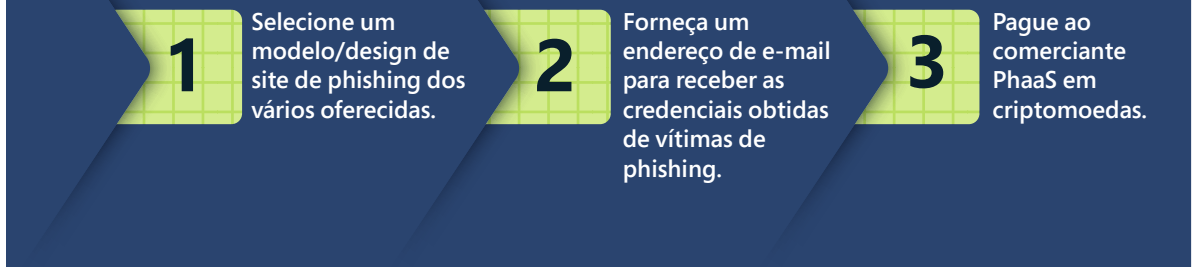
Os serviços de cibercrime de ponta a ponta estão a vender subscrições aos serviços geridos.

Normalmente, se a segurança operacional for fraco, cada passo na comissão de um crime online pode expor os atores de ameaças. O risco de exposição e de identificação aumenta se os serviços forem adquiridos a partir de vários sites de CaaS. A DCU observou uma tendência preocupante na dark web, segundo a qual existe um aumento na oferta de serviços para anonimizar o código de software e tornar o texto do website genérico para reduzir a exposição. Os fornecedores de serviços de subscrição de cibercrimes de ponta a ponta gerem todos os seus serviços e garantem os resultados que reduzem ainda mais os riscos de exposição à OCN de subscrição. A redução do risco aumentou a popularidade destes serviços de ponta a ponta.

O phishing como serviço (PhaaS) é um exemplo de um serviço de cibercrime de ponta a ponta. O PhaaS é uma evolução dos serviços anteriores conhecidos como serviços totalmente indetetáveis (FUD) e é oferecido numa base de subscrição. Os termos de PhaaS típicos incluem a manutenção de sites de phishing ativos durante um mês.

A DCU também identificou um comerciante de CaaS que oferecia uma oferta de negação de serviço distribuída (DDoS) num modelo de subscrição. Este modelo terceiriza a criação e a manutenção do botnet necessário para efetuar ataques ao comerciante de CaaS. Cada cliente de subscrição DDoS recebe um serviço encriptado para melhorar a segurança operacional e um ano de suporte 24 horas por dia, 7 dias por semana. O serviço de subscrições DDoS oferece diferentes arquiteturas e métodos de ataque, para que um comprador selecione simplesmente um recurso para atacar e o vendedor forneça acesso a uma série de dispositivos comprometidos no seu botnet para efetuar o ataque. O custo para a subscrição de DDoS é de apenas 500 USD.

PhaaS, os cibercriminosos oferecem vários serviços numa única subscrição. Em geral, um comprador tem de adotar apenas três ações:



Depois de concluídos estes passos, o comerciante PhaaS cria serviços com três ou quatro camadas de recursos de redirecionamento e alojamento para alvejar utilizadores específicos. A campanha é posteriormente lançada e as credenciais das vítimas são recolhidas, verificadas e enviadas para o endereço de e-mail fornecido pelo comprador. Como prémio, muitos comerciantes PhaaS oferecem-se para alojar sites de phishing na blockchain pública para poderem ser acedidos por qualquer browser e os redirecionamentos podem apontar os utilizadores para um recurso no livro razão distribuído.

O trabalho da DCU para desenvolver ferramentas e técnicas que identificam e perturbam os cibercriminosos de CaaS está em curso. A evolução dos serviços CaaS apresenta desafios significativos, sobretudo na interrupção dos pagamentos de criptomoedas.

Utilização criminosa de criptomoedas

À medida que a adoção de criptomoedas se torna na corrente dominante, os criminosos estão a utilizá-las cada vez mais para evitar medidas de aplicação da lei e combate ao branqueamento de capitais (AML). Isto aumenta o desafio da aplicação da lei para monitorizar e rastrear pagamentos de criptomoedas a cibercriminosos.

Os gastos mundiais em soluções de blockchain cresceram cerca de 340% nos últimos quatro anos, enquanto as novas carteiras de criptomoedas cresceram cerca de 270%. Existem mais de 83 milhões de carteiras exclusivas globalmente e a capitalização total de mercado de todas as criptomoedas foi de aproximadamente 1,1 trilião de USD em 28 de julho de 2022.[10]

Fonte: Twitter.com—@PeckShieldAlert (PeckShield é uma empresa de segurança blockchain baseada na China).

Monitorizar pagamentos de ransomware

O ransomware é uma das maiores fontes de criptomoedas obtidas ilegalmente. Num esforço para interromper a infraestrutura técnica maliciosa utilizada nos ataques de ransomware, como por exemplo, a interrupção do Zloader em abril de 2022[11], a DCU da Microsoft monitorizou as carteiras criminosas para ativar as capacidades de monitorização e recuperação de criptomoedas.

Os investigadores da DCU observaram atores de ransomware a evoluir as suas táticas de comunicação com as vítimas para ocultar o rasto do dinheiro. Originalmente, os cibercriminosos incluíam endereços de Bitcoin nas suas notas de resgate. No entanto, isto facilitou a continuação das transações de pagamento na blockchain, pelo que os atores de ransomware pararam de incluir endereços de carteiras e, em vez disso, anexaram endereços de e-mail ou ligações a sites de chat para comunicarem endereços de pagamento de resgates às vítimas. Alguns atores até criaram páginas web e inícios de sessão únicos para cada vítima para impedir que os investigadores de segurança e a aplicação da lei obtivessem os endereços da carteira dos criminosos que se faziam passar por vítimas. Apesar dos esforços dos criminosos para esconderem o seu rasto, ainda podem ser recuperados alguns pagamentos de resgate ao trabalharem com empresas de imposição da lei e de análise de criptomoedas que consigam monitorizar o movimento na blockchain.

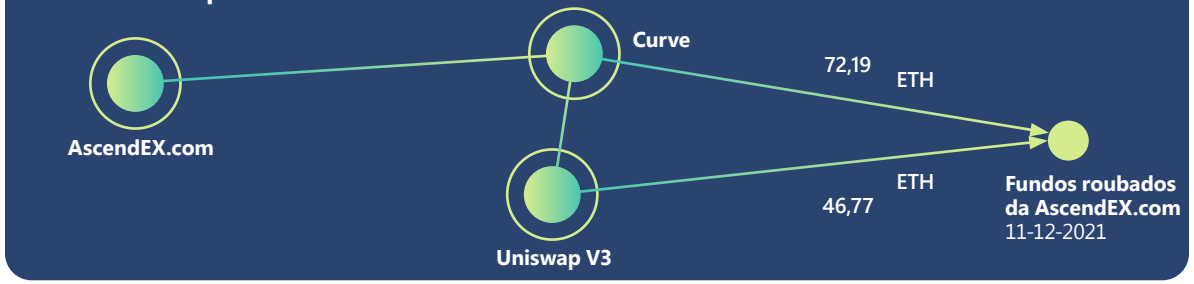
Tendências: lavagem de DEX de receitas ilícitas

Um problema chave para os cibercriminosos é a conversão de criptomoedas em moeda fiduciária. Os cibercriminosos têm vários potenciais caminhos de conversão, em que cada um tem um grau de risco diferente. Um método utilizado para reduzir o risco consiste em fazer a lavagem de recursos através de uma troca descentralizada (DEX) antes de retirar o dinheiro através das opções de levantamento disponíveis, como as trocas centralizadas (CEX), as trocas peer-to-peer (P2P) e venda livre (OTC). As DEX são uma localização de lavagem atrativa já que muitas vezes não seguem as medidas de AML.

Em dezembro de 2021, os hackers atacaram a plataforma de negociação de criptomoedas global AscendEx e roubaram cerca de 77.7 milhões de USD em criptomoedas que pertenciam aos seus clientes.[12] A AscendEx contratou empresas de análise de blockchain e contactou outras CEX para que as carteiras que recebiam fundos roubados pudessem ser colocadas na lista negra. Além disso, os endereços para onde as moedas foram enviadas foram rotulados como tal no explorador Etherscan de blockchain do Ethereum.[13] Para contornar os alertas e as listas negras, os hackers enviaram 1.5 milhões de USD no Ethereum para a Uniswap, uma das maiores DEX do mundo, a 18 de fevereiro de 2022.[14]

A adoção de medidas de AML mais fortes pelas DEX poderia conter a atividade de lavagem nas suas plataformas e forçar os cibercriminosos a utilizarem outros métodos de obscurecimento, como a queda de moedas ou as trocas não licenciadas.

Monitorizar criptomoedas obtidas ilicitamente



Utilizando a ferramenta de análise de dados de criptomoedas Chainalysis, a Unidade de Crimes Digitais da Microsoft descobriu que os hackers da AcendEx trocaram os seus fundos roubados por uma DEX menor chamada Curve, além da Uniswap. Este diagrama ilustra as rotas de branqueamento que a equipa descobriu. Cada círculo representa um cluster de carteiras e os números em cada linha representam a quantidade total de Ethereum transmitida para fins de lavagem.

Como exemplo, a Uniswap anunciou recentemente que irá começar a utilizar listas negras para bloquear carteiras conhecidas por estarem envolvidas em atividades ilícitas de transação na troca.[15]

Insights acionáveis

1. Se for vítima de cibercrime e se pagou ao criminoso através de criptomoedas, contacte as autoridades policiais locais para que possam ajudar a monitorizar e a recuperar os fundos perdidos.
2. Familiarize-se com as medidas de ALM em vigor ao selecionar uma DEX.

Ligações para mais informações

- Defesa contra ameaças baseada em hardware contra cryptojackers cada vez mais complexos | Equipa de Investigação do Microsoft 365 Defender

O panorama em evolução de ameaças de phishing

Os esquemas de phishing de credenciais estão em crescimento e continuam a ser uma ameaça substancial para os utilizadores em todo o mundo porque visam todas as caixas de entrada de forma indiscriminada. Entre as ameaças que os nossos investigadores monitorizam e protegem, o volume de ataques de phishing é de magnitude maior do que todas as outras ameaças.

Utilizando os dados do Defender para o Office, vemos o e-mail malicioso e a atividade de identidade comprometida. A Proteção de Identidades do Azure Active Directory fornece ainda mais informações através de alertas de eventos de identidades comprometidos. Utilizando o Defender para Aplicações na Cloud, vemos eventos de acesso a dados de identidade comprometidos e o Microsoft 365 Defender (M365D) fornece correlação entre produtos. A métrica de movimento lateral provém do Defender para Endpoint (alertas e eventos de comportamento de ataque), Defender para o Office (e-mail malicioso) e novamente o M365D para correlação entre produtos).

710 milhões
e-mails de phishing bloqueados por semana.

1h12m
A mediana de tempo necessário para um atacante aceder aos seus dados privados se for vítima de um e-mail de phishing.[16]

1h42m
A mediana de tempo para um atacante se começar a mover lateralmente dentro da sua rede empresarial quando um dispositivo é comprometido.[17]

As credenciais do Microsoft 365 continuam a ser um dos tipos de conta mais procurados para os atacantes. Depois de as credenciais de início de sessão estarem comprometidas, os atacantes podem iniciar sessão em sistemas informáticos vinculados às empresas para facilitar a infeção com malware e ransomware, roubar informações e dados da empresa confidenciais ao aceder aos ficheiros do SharePoint e continuar a propagação do phishing ao enviar e-mails maliciosos adicionais através do Outlook, entre outras ações.

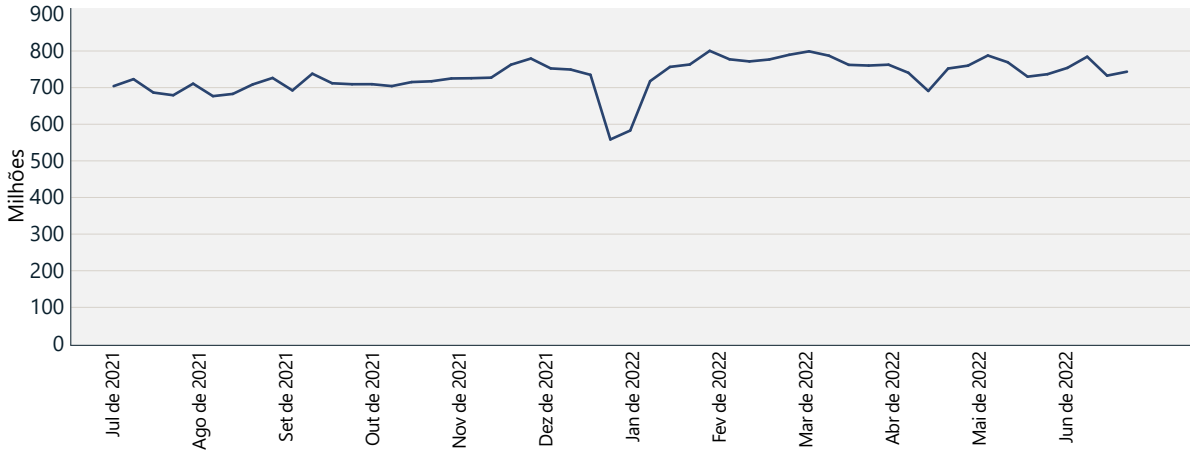
Além de campanhas com metas mais amplas, phishing para credenciais, doações e informações pessoais, os atacantes estão a visar empresas seletivas para pagamentos maiores. Os ataques de phishing por e-mail contra empresas para obter ganhos financeiros são coletivamente referidos como ataques BEC.

A Microsoft deteta milhões de e-mails BEC todos os meses, o que equivale a 0,6% de todos os e-mails de phishing observados. Um relatório da IC3[18] publicado em maio de 2022 indica uma tendência ascendente nas perdas expostas devido aos ataques BEC.

As técnicas utilizadas nos ataques de phishing continuam a aumentar em complexidade. Como resposta a contramedidas, os atacantes adaptam novas formas de implementar as suas técnicas e aumentam a complexidade da forma e do local onde alojam a infraestrutura de operações de campanha. Isto significa que as organizações têm de reavaliar regularmente a sua estratégia de implementação de soluções de segurança para bloquear e-mails maliciosos e reforçar o controlo de acesso às contas de utilizador individuais.

531.000
Além dos URL bloqueados pelo Defender para o Office, a nossa Unidade de Crimes Digitais dirigiu a remoção de 531.000 URL de phishing exclusivos alojados fora da Microsoft.

E-mails de phishing detetados



O número de deteções de phishing por semana continua a aumentar. A redução em dezembro – janeiro é uma queda sazonal esperada, também relatada no relatório do ano passado. Fonte: Sinais de Proteção do Exchange Online.

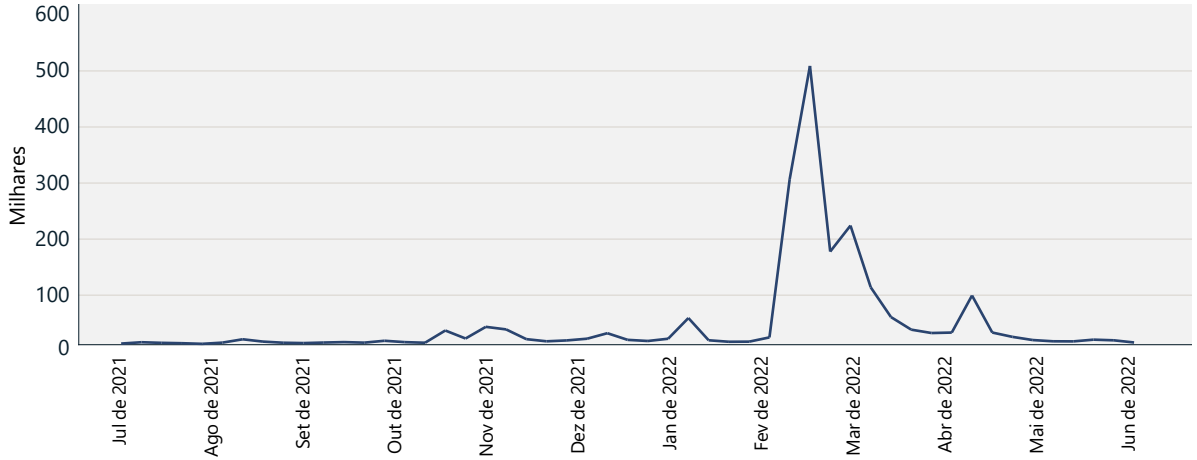
O panorama em evolução de ameaças de phishing

Continuação

Continuamos a observar um aumento estável ano após ano em e-mails de phishing. A mudança para o trabalho remoto em 2020 e 2021 assistiu a um aumento substancial dos ataques de phishing com o objetivo de capitalizar o ambiente de trabalho em mudança. Os operadores de phishing são rápidos a adotar novos modelos de e-mail com iscos alinhados com os principais eventos mundiais, como a pandemia da COVID-19 e os temas ligados às ferramentas de colaboração e produtividade, como a partilha de ficheiros do Google Drive ou do OneDrive. Apesar de os temas sobre a COVID-19 terem diminuído, a guerra na Ucrânia transformou-se num novo chamariz a partir do início de março de 2022. Os nossos investigadores observaram um aumento assombroso de e-mails que representavam organizações legítimas que aliciavam doações de criptomoedas em Bitcoin e Ethereum, alegadamente para suportarem os cidadãos ucranianos.

Apenas alguns dias após o início da guerra na Ucrânia no final de fevereiro de 2022, o número de e-mails de phishing detetados que contêm endereços Ethereum encontrados em clientes empresariais aumentou drasticamente. O total de casos atingiu o pico na primeira semana de março, quando meio milhão de e-mails de phishing continham um endereço da carteira do Ethereum. Antes do início da guerra, o número de endereços da carteira Ethereum noutros e-mails detetados como hosts era significativamente menor, com uma média de alguns milhares de e-mails por dia.

E-mails de phishing com endereços da carteira do Ethereum



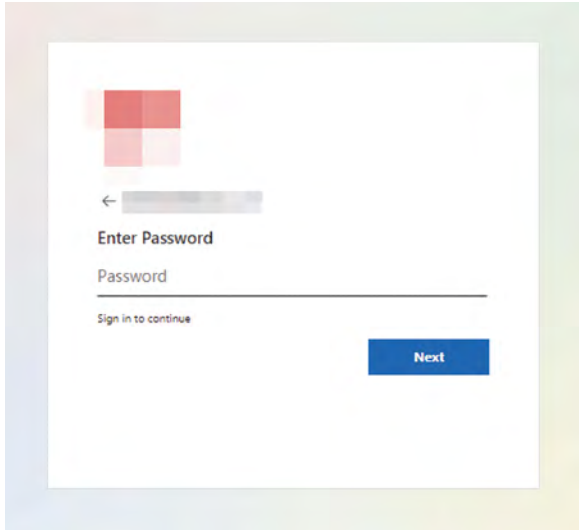
Os e-mails totais detetados como phish que contêm endereços da carteira Ethereum aumentaram no início do conflito entre a Ucrânia e a Rússia e abrandaram após o empurrão inicial.

Mais do que nunca, os phishers estão a contar com a infraestrutura legítima para operar, impulsionando um aumento de campanhas de phishing que visam comprometer vários aspetos de uma operação para que não tenham de comprar, alojar ou operar as suas próprias. Por exemplo, os e-mails maliciosos podem vir de contas de remetente comprometidas. Os hackers beneficiam da utilização destes endereços de e-mail que têm uma pontuação de reputação superior e são vistos como mais fiáveis do que as contas e domínios recentemente criados. Em algumas campanhas de phishing mais avançadas, observámos que os atacantes preferiam enviar e falsificar a partir de domínios que têm DMARC[19] incorretamente configurados com uma política "sem ação", abrindo a porta para a falsificação de e-mails.

As grandes operações de phishing tendem a utilizar serviços de cloud e máquinas virtuais de cloud (VM) para operacionalizarem ataques em grande escala. Os atacantes podem automatizar totalmente o processo de implementação e entrega de e-mails de VM através de relés de e-mail SMTP ou da infraestrutura de e-mail na cloud para tirar partido das elevadas taxas de entrega e da boa reputação destes serviços legítimos. Se for permitido que o e-mail malicioso seja enviado através destes serviços Cloud, os defensores têm de contar com fortes capacidades de filtragem de e-mail para impedir que os e-mails entrem no seu ambiente.

As contas Microsoft continuam a ser um dos principais alvos dos operadores de phishing, como evidenciado pelas inúmeras páginas de destino de phishing que personificam a página de início de sessão do Microsoft 365. Por exemplo, os phishers tentam corresponder à experiência de início de sessão da Microsoft nos seus kits de phishing ao gerar um URL exclusivo personalizado para o destinatário. Este URL aponta para uma página web maliciosa desenvolvida para obter credenciais, mas um parâmetro no URL irá conter o endereço de e-mail do destinatário específico. Quando o alvo navega para a página, o kit de phishing vai pré-povoar os dados de início de sessão de utilizador e um logotipo empresarial personalizado para o destinatário do e-mail, espelhando a aparência da página de início de sessão personalizada do Microsoft 365 da empresa alvo.

Página de phishing a personificar o início de sessão da Microsoft com conteúdo dinâmico

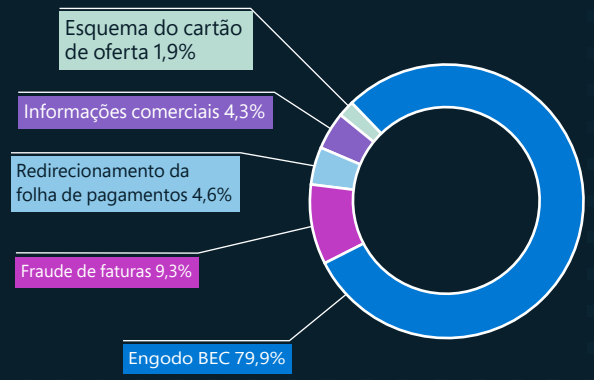


Destaque para o compromisso de e-mail empresarial

Os cibercriminosos estão a desenvolver esquemas e técnicas cada vez mais complexos para derrotar as definições de segurança e visar indivíduos, empresas e organizações. Estamos a investir recursos significativos para melhorar ainda mais o nosso programa de imposição de BEC em resposta.

O BEC é o cibercrime financeiro mais caro, com 2,4 biliões de USD estimados em perdas ajustadas em 2021, o que representa mais de 59% das cinco principais perdas de crimes na Internet a nível mundial.[20] Para compreender o âmbito do problema e qual a melhor forma de proteger os utilizadores contra o BEC, os investigadores de segurança da Microsoft têm vindo a monitorizar os temas mais comuns utilizados nos ataques.

Temas BEC (janeiro a junho de 2022)



Temas BEC por percentagem de ocorrência

Tendências BEC

Como ponto de entrada, os atacantes do BEC tentam normalmente iniciar uma conversação com potenciais vítimas para estabelecerem relações. Posando como um colega ou conhecido de negócio, o atacante lidera gradualmente a conversação no sentido de uma transferência monetária. O e-mail de introdução, que acompanhamos como um isco do BEC, representa cerca de 80% dos e-mails detetados do BEC. Outras tendências identificadas pelos investigadores de segurança da Microsoft no último ano incluem:

- As técnicas mais frequentemente utilizadas nos ataques BEC observados em 2022 foram o spoofing[21] e a representação.[22]
- O subtipo de BEC que causou mais danos financeiros às vítimas foi a fraude de faturas (com base no volume e nos montantes de dólar solicitados observados nas nossas investigações de campanha do BEC).
- O roubo de informações de negócio, como relatórios de contas a pagar e contactos com clientes, permite que os atacantes elaborem fraudes convincentes de faturas.
- A maioria dos pedidos de redirecionamento da folha de pagamentos foram enviados a partir de serviços de e-mail gratuitos e raramente de contas comprometidas. O volume de e-mail destas origens aumentou junto ao primeiro e décimo quinto dia de cada mês, as datas de pagamento mais comuns.
- Apesar de serem rotas bem conhecidas para fraudes, os golpes de cartões de presente só constituíram 1,9% dos ataques de BEC detetados.

Insights acionáveis

Defender contra phishing

Para reduzir a exposição da sua organização ao phishing, os administradores de TI são incentivados a implementar as seguintes políticas e funcionalidades:

1. Exigir a utilização da MFA em todas as contas para limitar o acesso não autorizado.
2. Ativar funcionalidades de acesso condicional para contas altamente privilegiadas para bloquear o acesso de países, regiões e IP que normalmente não geram tráfego na sua organização.
3. Ponderar a utilização de chaves de segurança física para executivos, colaboradores envolvidos em atividades de pagamento ou aquisição e outras contas privilegiadas.
4. Impor a utilização de browsers que suportam serviços como o Microsoft SmartScreen para analisar URL em termos de comportamentos suspeitos e bloquear o acesso a sites maliciosos conhecidos.[23]
5. Utilizar uma solução de segurança baseada em machine learning que coloca em quarentena a probabilidade de phishing e detona URL e anexos numa sandbox antes de o e-mail chegar à caixa de entrada, como o Microsoft Defender para o Office 365.[24]
6. Ativar as funcionalidades de proteção contra personificação e falsificação em toda a sua organização.
7. Configurar as políticas de ação de DomainKeys Identified Mail (DKIM) e Relatórios e Conformidade de Autenticação de Mensagens baseadas em domínios (DMARC) para evitar a entrega de e-mails não autenticados que possam ser falsificação por remetentes com reputação.
8. O inquilino de auditoria e o utilizador criado permitem regras e removem exceções baseadas no domínio amplo e no IP. Estas regras têm muitas vezes precedência e podem permitir e-mails maliciosos conhecidos através da filtragem de e-mails.
9. Executar regularmente simuladores de phishing para avaliar o risco potencial em toda a sua organização e para identificar e educar os utilizadores vulneráveis.

Ligações para mais informações

- Desde o roubo de cookies até ao BEC: os atacantes utilizam sites de phishing AiTM como ponto de entrada para mais fraudes financeiras | Equipa de Investigação do Microsoft 365, Centro de Informações Sobre Ameaças da Microsoft (MSTIC)

Engano de homoglifo

O BEC e o phishing são táticas comuns de engenharia social. A engenharia social desempenha um papel importante no crime, persuadindo um alvo a interagir com o criminoso ao ganhar a sua confiança.

No comércio físico, as marcas registadas são utilizadas para garantir a confiança na origem relativamente a um produto ou serviço, e os produtos falsificados são um abuso da marca registada. Da mesma forma, os cibercriminosos apresentam-se como um contacto familiar para o alvo durante um ataque de phishing, utilizando homógrafos para enganar as potenciais vítimas.

Um homógrafo é um nome de domínio utilizado para a comunicação por e-mail no BEC, em que um caracter é substituído por outro idêntico ou praticamente idêntico em termos de aparência, para enganar o alvo.

Técnicas de homógrafo utilizadas nas tentativas de BEC

Normalmente, o BEC tem duas fases, a primeira das quais envolve o comprometimento de credenciais. Estes tipos de fugas de credenciais podem resultar de ataques de phishing ou de grandes violações de dados. As credenciais são então vendidas ou negociadas na dark web.

A segunda fase é a fase de fraude, em que os atacantes utilizam credenciais comprometidas para se envolverem em engenharia social sofisticada através de domínios de e-mail de homoglifo.

Progressão de um ataque BEC

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

Análise de mais de 1.700 domínios de homógrafo entre janeiro e julho de 2022. Apesar de terem sido utilizadas 170 técnicas de homógrafo, 75% dos domínios utilizaram apenas 14 técnicas.

Um homógrafo em ação

Um domínio de homógrafo que é idêntico a um domínio de e-mail que a vítima reconhece estar registado num fornecedor de e-mail com um nome de utilizador idêntico. Em seguida, é enviado um e-mail sequestrado do domínio sequestrado com novas instruções de pagamento.

Aproveitando a análise de informações open source e o acesso às conversações de e-mail, o criminoso identifica os indivíduos que têm a responsabilidade da faturação e dos pagamentos. Em seguida, criam uma personificação de um endereço de e-mail do indivíduo que envia faturas. Esta personificação é composta por um domínio de nome de utilizador e e-mail idêntico que é um homógrafo do remetente genuíno.

O atacante copia uma cadeia de e-mail que contém uma fatura legítima e, em seguida, altera a fatura para conter os próprios dados bancários. Esta nova fatura modificada é então reenviada a partir do e-mail de personificação de homógrafo para o destino. Como o contexto faz sentido e o e-mail parece genuíno, muitas vezes o alvo segue as instruções fraudulentas.

Insights acionáveis

1. Impor a utilização de browsers que suportam serviços para analisar URL em termos de comportamentos suspeitos e bloquear o acesso a sites maliciosos, como as Ligações Seguras ou o SmartScreen.[25]
2. Utilizar uma solução de segurança baseada em machine learning que coloca em quarentena a probabilidade de phishing e detona URL e anexos numa sandbox antes de o e-mail chegar à caixa de entrada.

Ligações para mais informações

- Centro de Denúncias de Crimes na Internet (IC3) | Comprometimento de E-mail Empresarial: o esquema de 43 biliões de USD
- Insights inteligentes sobre spoofing — Office 365 | Microsoft Docs
- Insights sobre representação — Office 365 | Microsoft Docs

Um cronograma de disrupção de botnet dos primeiros dias de colaboração da Microsoft

Durante mais de uma década, a DCU trabalhou para parar proativamente o cibercrime, resultando em 26 disrupções de malware e de estado-nação. À medida que a equipa da DCU utiliza ferramentas e táticas avançadas para encerrar estas operações ilícitas, vemos que os cibercriminosos também evoluem com as suas abordagens na tentativa de se manterem um passo à frente. Eis uma cronologia que mostra um exemplo dos botnets interrompidos pela DCU e as estratégias da Microsoft adotadas para os encerrar.

2008

Botnet Conficker

Descrição: um verme que se espalha rapidamente tendo como alvo o SO Windows, infetando milhões de computadores e dispositivos numa rede comum; criou falhas de rede em todo o mundo.

Colaboração: formação do Conficker Working Group, o primeiro consórcio deste tipo. A Microsoft estabeleceu uma parceria com 16 organizações em todo o mundo para derrotar o bot.

Resposta da Microsoft: O grupo colaborou em várias jurisdições internacionais e foi bem-sucedido ao encerrar a Conficker.

2009

Botnet Waledac

Descrição: um botnet de spam complexo com domínios norte-americanos que recolheram endereços de e-mail e distribuíram spam, infetando até 90.000 computadores em todo o mundo.[26]

Colaboração: criação de outro consórcio, o Centro de Proteção contra Malware da Microsoft (MMPC) com foco na estreita colaboração com académicos.[27]

Resposta da Microsoft: a Microsoft utilizou a abordagem de interrupção por escalões do C2 e surpreendeu os maus atores ao apreender domínios baseados nos EUA sem aviso prévio.[28] A Microsoft transferiu temporariamente a propriedade de quase 280 domínios utilizados pelos servidores do Waledac.

2011

A Unidade de Crimes Digitais da Microsoft está formada

Colaboração: concebido para frustrar o cibercrime que afeta o ecossistema Microsoft através de uma estreita integração numa equipa de investigadores, advogados e engenheiros.

Abordagem da Microsoft: o objetivo é compreender melhor os aspetos técnicos de vários malwares e fornecer estes insights à equipa jurídica da Microsoft para desenvolver uma estratégia de perturbação eficaz.

2013

Botnet Rustock

Descrição: um bot de e-mail de spam de troJan de backdoor que utiliza fornecedores de internet como C2S primários; concebido para vender produtos farmacêuticos.

Colaboração: a Microsoft forjou uma parceria com a Pfizer Pharmaceuticals para compreender os medicamentos vendidos pela Rustock e trabalhou em estreita colaboração com os atores policiais holandeses.[29]

Resposta da Microsoft: a Microsoft trabalhou com os US Marshalls e a aplicação da lei nos Países Baixos para derrubar os servidores de C2 nesse país. Registados e bloqueados todos os algoritmos de gerador de domínios futuros (DGA).

Botnet de acesso Sirefef/Zero

Descrição: um botnet de publicidade concebido para direcionar as pessoas para sites perigosos que instalariam malware ou roubariam informações pessoais; infetou mais de 2 milhões computadores e custou mais de 2,7 milhões de USD por mês aos anunciantes; sobretudo nos EUA e na Europa Ocidental.

Colaboração: trabalho em estreita colaboração com o FBI e o Centro de Cibercrime da Europol para reduzir a infraestrutura ponto-a-ponto.

Resposta da Microsoft: adesão à rede de Acesso Zero, substituição dos servidores C2 criminosos e apreensão com êxito dos domínios de servidor de download.

2019

Botnet Trickbot

Descrição: um botnet sofisticado com uma infraestrutura fragmentada em todo o mundo que visava o setor dos serviços financeiros; dispositivos IoT comprometidos.

Colaboração: a Microsoft estabeleceu uma parceria com o Centro de Partilha e Análise de Informações dos Serviços Financeiros (FS-ISAC) para derrubar o Trickbot.[30]

Resposta da Microsoft: A DCU criou um sistema para identificar e monitorizar a infraestrutura do bot e gerou notificações para os fornecedores de Internet ativos, tendo em conta as leis específicas em vários países.

2022

Foco contínuo na interrupção

Descrição: a Microsoft interrompeu a infraestrutura de sete atores de ameaças ao longo do último ano, impedindo-os de distribuírem malware adicional, controlarem os computadores das vítimas e alvejar outras vítimas.

Colaboração: em parceria com os fornecedores de serviços de internet, os governos, a aplicação da lei e a indústria privada, a Microsoft partilhou informações para remediar o problema em mais de 17 milhões de vítimas de malware em todo o mundo.

Olhar para o futuro

A DCU continua a inovar e está a tentar utilizar a sua experiência em interrupções de botnet para efetuar operações coordenadas que vão além do malware. O nosso sucesso contínuo exige engenharia criativa, partilha de informações, teorias jurídicas inovadoras e parcerias públicas e privadas.

Utilização abusiva da infraestrutura pelos cibercriminosos

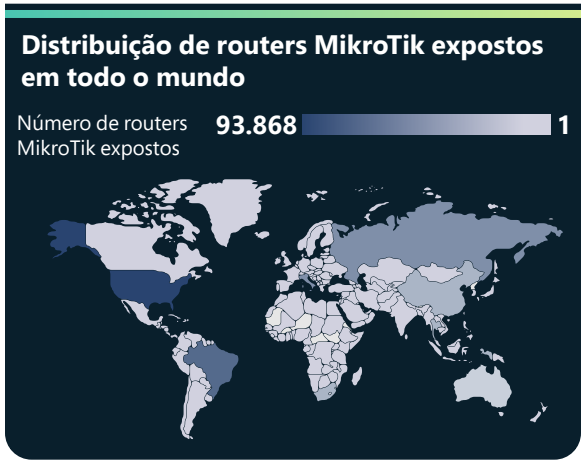
Gateways de Internet como infraestrutura de comando e controlo criminal

Os dispositivos IoT estão a tornar-se num alvo cada vez mais popular para os cibercriminosos através de botnets generalizados. Quando os routers não são corrigidos e ficam expostos diretamente à Internet, os atores de ameaças podem abusar dos mesmos para obter acesso às redes, executar ataques maliciosos e até mesmo suportar as suas operações.

A equipa do Microsoft Defender para IoT realiza estudos em equipamentos que vão desde controladores de sistemas de controlo industrial legados até sensores de IoT de última geração. A equipa investiga malware específico de IoT e OT para contribuir para a lista partilhada de indicadores de comprometimento.

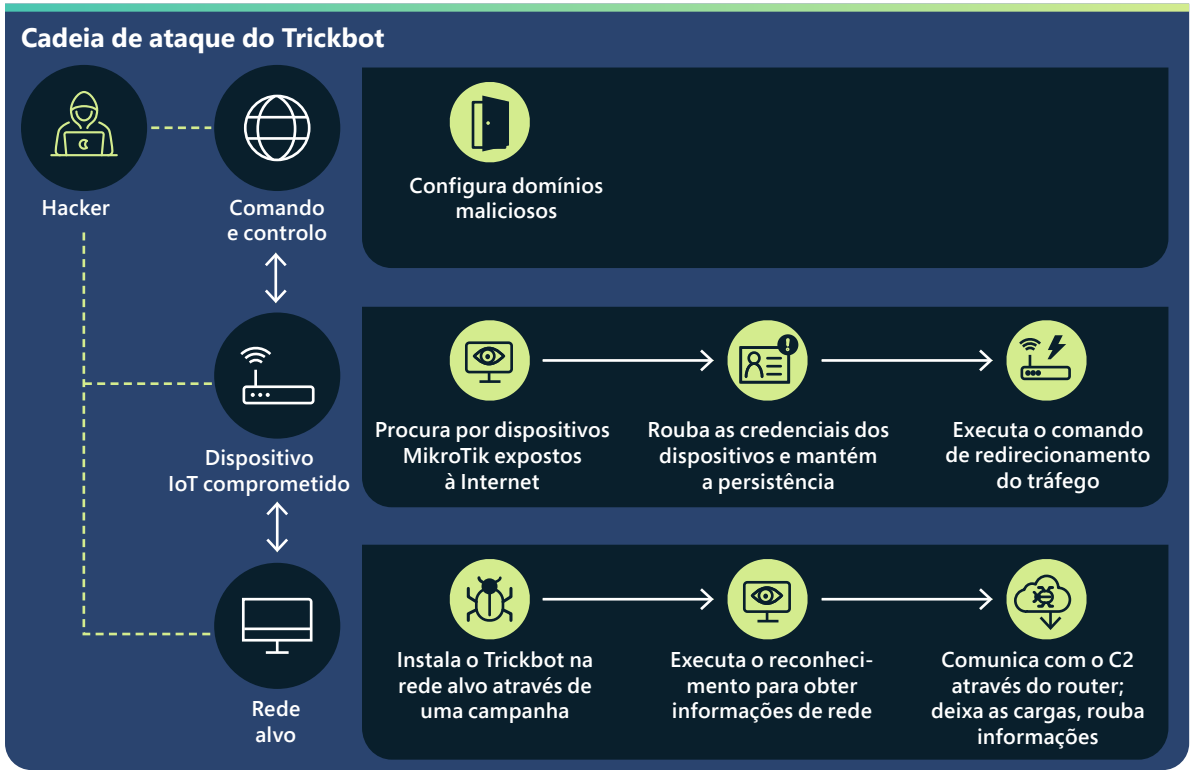
Os routers são vetores de ataque particularmente vulneráveis porque são omnipresentes em todas as organizações e residências com ligação à Internet. Temos vindo a monitorizar a atividade dos routers MikroTik, um router popular em todo o mundo, tanto em residências como em negócios, identificando como são utilizados para comandos e controlo (C2), ataques do sistema de nomes de domínio (DNS) e sequestro de mineração de criptomoedas.

Mais especificamente, identificámos como os operadores de Trickbot utilizam routers MikroTik comprometidos e os reconfiguram para atuarem como parte da sua infraestrutura C2. A popularidade destes dispositivos compõe a gravidade do seu abuso pelo Trickbot, e o seu hardware e software exclusivos permitem aos atores de ameaças escaparem às medidas de segurança tradicionais, expandirem a sua infraestrutura e comprometerem mais dispositivos e redes.



Os routers expostos estão em risco de verem as suas potenciais vulnerabilidades exploradas.

Ao monitorizar e analisar o tráfego que contém comandos de shell seguros (SSH), observamos que os atacantes utilizam routers MikroTik para comunicar com a infraestrutura do Trickbot depois de obterem credenciais legítimas para dispositivos. Estas credenciais podem ser obtidas através de ataques de força bruta, explorando vulnerabilidades conhecidas com correções prontamente disponíveis e utilizando palavras-passe predefinidas. Depois de um dispositivo ser acedido, o atacante emite um comando exclusivo que redireciona o tráfego entre duas portas no router, estabelecendo a linha de comunicação entre os dispositivos afetados pelo Trickbot e o C2.



Cadeia de ataque do Trickbot que mostra a utilização de dispositivos IoT do MikroTik como servidores proxy para o C2.

Agregámos os nossos conhecimentos sobre os vários métodos de ataque aos dispositivos MikroTik, além do Trickbot, bem como as vulnerabilidades e exposições comuns conhecidas (CVE) numa ferramenta open source para dispositivos MikroTik, que pode extrair os artefactos forenses relacionados com ataques nestes dispositivos.[31]

Os dispositivos que atuam como proxies inversos para malware C2 não são exclusivos dos routers Trickbot e MikroTik. Em colaboração com a equipa RiskIQ da Microsoft, localizámos o C2 envolvido e, através da observação de certificados SSL, identificámos dispositivos Ubiquiti e LigoWave que também sofreram impacto.[32] Esta é uma forte indicação de que os dispositivos IoT estão a tornar-se componentes ativos dos ataques coordenados de estados-nação e um alvo popular para os cibercriminosos que utilizam botnets generalizados.

Criminosos criptográficos que abusam de dispositivos IoT

Os dispositivos de gateway são um alvo cada vez mais valioso para os atores de ameaças, à medida que o número de vulnerabilidades conhecidas cresce consistentemente de ano para ano. Estão a ser utilizados para a mineração de criptomoedas e outros tipos de atividade maliciosa.

À medida que as criptomoedas se tornaram mais populares, muitas pessoas e organizações investiram recursos de rede e poder computa-cional a partir de dispositivos, como routers, para extrair moedas no blockchain. No entanto, a mineração de criptomoedas é um processo intensivo em termos de tempo e recursos com uma baixa probabilidade de sucesso. Para aumentar a probabilidade de mineração de uma moeda, os mineiros reúnem-se em redes cooperativas distribuídas, recebendo hashes em relação à percentagem da moeda que conseguiram na mineração com os seus recursos interligados.

No ano passado, a Microsoft observou um número crescente de ataques que abusavam dos routers para redirecionar os esforços de mineração de criptomoedas. Os cibercriminosos comprometem os routers ligados a conjuntos de mineração e redirecionam o tráfego de mineração para os endereços IP associados com ataques de envenenamento do DNS, que alteram as definições DNS dos dispositivos direci`onados. Os routers afetados registam o endereço IP errado num determinado nome de domínio, enviando os seus recursos de mineração, ou hashes, para conjuntos utilizados por atores de ameaças. Estes conjuntos podem extrair moedas anónimas associadas a atividades criminosas ou utilizar hashes legítimos gerados pelos mineiros para adquirirem uma percentagem da moeda que extraíram, colhendo assim as recompensas.

Com mais de metade das vulnerabi-lidades conhecidas encontradas em 2021 com falta de patches, a atualização e proteção dos routers nas redes empresariais e privadas continua a ser um desafio significativo para os administradores e proprietários de dispositivos.

Dispositivos comprometidos para a mineração ilegal de criptomoedas.

O envenenamento do DNS dos dispositivos de gateway compromete as atividades de mineração legítimas e redireciona os recursos para atividades de mineração criminal.

Máquinas virtuais como infraestrutura criminosa

A mudança generalizada para a cloud inclui cibercriminosos que aproveitam os recursos privados de vítimas inconscientes obtidos através do phishing ou da distribuição de ladrões de credenciais de malware. Muitos cibercriminosos estão a optar por configurar as suas infraestruturas maliciosas em máquinas virtuais (VM) baseadas na cloud, containers e microsserviços.

Depois de o cibercriminoso ter acesso, pode ocorrer uma sequência de eventos para configurar a infraestrutura, como uma série de máquinas virtuais através de scripts e de processos automatizados. Estes processos automatizados com scripts são utilizados para lançar atividades maliciosas, incluindo ataques de spam de e-mail em grande escala, ataques de phishing e páginas web que alojam conteúdos nefastos. Pode inclusivamente incluir a criação de um ambiente virtual dimensionado que realiza a mineração de criptomoedas, o que causa à vítima final uma fatura de centenas de milhares de dólares no final do mês.

Os cibercriminosos entendem que a sua atividade maliciosa tem um período de vida limitado antes de ser detetada e desligada. Como resultado, aumentaram a sua dimensão e agora operam de forma proativa com as contingências como prioridade. Têm sido observados a preparar contas comprometidas antes do tempo e a monitorizar os seus ambientes. Assim que é detetada uma conta (configurada com centenas de milhares de máquinas virtuais), os cibercriminosos passam para a conta seguinte, já preparada por scripts para ser ativada imediatamente, e a sua atividade maliciosa continua com pouca ou nenhuma interrupção.

Como a infraestrutura de cloud, a infraestrutura on-premises pode ser utilizada em ataques com ambientes virtuais locais que são desconhecidos para o utilizador local. Isto exige que o ponto de acesso inicial permaneça aberto e acessível. Os ativos privados on-premises também foram utilizados de forma abusiva por cibercriminosos para iniciar uma cadeia de infraestrutura na cloud configurada para ofuscar a sua origem para evitar a deteção da criação de infraestrutura suspeita.

Insights acionáveis

1. Implemente uma boa higiene cibernética e forneça formação em cibersegurança aos colaboradores com orientação para evitar a sua engenharia social.
2. Efetue verificações automatizadas de anomalias de atividade do utilizador regularmente através de deteções à escala para ajudar a reduzir estes tipos de ataques.
3. Atualize e proteja os routers em redes empresariais e privadas.

A prática de acesso ilícito veio para ficar?

Apesar de a prática de acesso ilícito não ser um novo fenómeno, a guerra na Ucrânia assistiu a um surto de hackers voluntários, incluindo alguns dirigidos por governos para implementar ferramentas cibernéticas para danificar a reputação ou os ativos dos opositores políticos, das organizações e até dos estados-nação.

Em fevereiro de 2022, o governo ucraniano convocou civis privados em todo o mundo para conduzirem ciberataques contra a Rússia como parte do seu forte "exército de TI" de 300.000 pessoas.[33] Ao mesmo tempo, grupos de atores de acesso ilícito estabelecidos, como o Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans e o RaidForum2 começaram a realizar ataques de apoio à Ucrânia. Outros grupos, incluindo alguns do gangue de ransomware Conti, tomaram o partido da Rússia.[34]

Nos meses que se seguiram, as atividades do Anonymous foram altamente visíveis. Os hackers que atuam em nome do grupo, ou no de um dos seus afiliados, inativaram temporariamente milhares de sites russos e bielorrussos, com a fuga de centenas de gigabytes de dados roubados, acederam ilicitamente canais de televisão russos para reproduzirem conteúdo pró-ucraniano e até ofereceram o pagamento de Bitcoins pelos tanques russos que se renderam.

O surgimento dos hackers cidadãos

As plataformas de redes sociais permitiram a rápida organização e mobilização de milhares de hackers cidadãos, que receberam instruções para a realização de ataques facilmente executáveis, como ataques DDoS. Os organizadores aproveitaram o Twitter, o Telegram e os fóruns privados para reunir hackers, organizar operações e disseminar manuais de instruções de hacking.

No entanto, a maioria destes hackers tem provavelmente competências limitadas, mesmo com instruções. Isto sugere dois potenciais futuros: um em que centenas ou milhares de indivíduos com capacidades técnicas rudimentares utilizam modelos de ataque para conduzirem futuros ataques de acesso ilícito coordenados ou individuais contra alvos, ou um segundo em que o fim final das hostilidades na Ucrânia os vê a deixarem a sua atividade de acesso ilícito, pelo menos até que o próximo conflito político ou social os inspire à ação.

Politização de hackers

O maior risco representado por esta mobilização política é a implementação de hackers conhecedores da tecnologia que poderão continuar a conduzir ciberataques contra alvos de governos estrangeiros para suportarem as suas próprias prioridades nacionais, quer de uma base autoiniciada ou a mando do seu governo.

O Irão, a China e a Rússia já utilizam o acesso ilícito como fonte do recrutamento para os seus grupos de hackers estatais. Por exemplo, em abril de 2022, o grupo de hackers pró-russo Killnet lançou ataques de DDoS contra a ferrovia Chéquia, os aeroportos regionais e o servidor do serviço civil da Chéquia, apesar de o país não estar diretamente envolvido na guerra.[35] Ao mesmo tempo, alguns governos podem utilizar o acesso ilícito como cobertura para as operações de sabotagem e espionagem cibernética tradicionais, por exemplo, as atividades iranianas contra Israel.

Num ambiente de aumento dos ataques de DDoS ligados ao acesso ilícito, o setor da tecnologia é desafiado a decifrar rapidamente a diferença entre o fluxo de tráfego normal e anormal para um site. A Microsoft e os seus parceiros desenvolveram uma coleção de ferramentas que distingue o tráfego de DDoS malicioso e o rastreiam de volta à sua origem. Além disso, a plataforma de Azure da Microsoft pode identificar as máquinas que produzem níveis extraordinariamente elevados de tráfego de saída na plataforma e encerra-as.

Emergência de protestware

O protestware emergiu como resultado direto das reações emocionais à guerra entre a Rússia e a Ucrânia. Alguns programadores de software open source utilizaram a popularidade do seu software como um meio para afirmar ou tomar medidas contra uma situação geopolítica em desdobramento. Isto incluía ficheiros de texto inofensivos abertos num ambiente de trabalho ou browser para espalhar mensagens de paz, mas também incluía ataques direcionados baseados na geolocalização de endereços IP e ações destrutivas, como a limpeza de um disco rígido. À medida que outros eventos globais se desenrolam, é expectável voltar a ver a superfície de protestware no futuro. Uma vez que estes são geralmente os casos em que os responsáveis de código aberto bem respeitados decidem fazer declarações pessoais com os seus próprios componentes open source, atualmente não há proteção no local para impedir que estes tipos de alterações ocorram nos pacotes de ficheiros de origem e os utilizadores devem manter a consciência do potencial impacto.

As plataformas de redes sociais permitiram a organização e mobilização de milhares de hackers cidadãos, que receberam instruções para a realização de ataques facilmente executáveis, como ataques DDoS.

Insights acionáveis

1. O setor da tecnologia tem de se reunir para conceber uma resposta abrangente a esta nova ameaça.
2. As principais empresas de tecnologia, incluindo a Microsoft, têm ferramentas para identificar o tráfego malicioso associado aos ataques de DDoS e desativar as máquinas responsáveis.
3. Os utilizadores open source devem manter vigilância elevada durante os períodos de conflito geopolítico.

Notas finais

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. Deteção e resposta de endpoints. 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. Um Fórum Supervisionado é um fórum de discussão online que exige que um membro existente confirme a adição de um novo membro.
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. Origem de dados: Defender para o Office (e-mail malicioso/atividade de identidade comprometida), Proteção de Identidade do Azure Active Directory (eventos de identidade/ alertas comprometidos), Defender para Aplicações na Cloud (eventos de acesso a dados de identidade comprometidos) e M365D (correlação entre produtos).
17. Origem de dados: Defender para Endpoint (alertas/eventos de comportamento de ataque), Defender para o Office (e-mail malicioso) e M365D (correlação entre produtos).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Autenticação, Relatórios e Conformidade de Mensagens baseadas no domínio: uma autenticação de e-mail, uma política e um protocolo de relatórios concebidos para dar aos proprietários de domínios de e-mail a capacidade de protegerem o seu domínio contra a utilização não autorizada.
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 fevereiro de 2010).
27. Consultar Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 de setembro de 2011.
28. Especificamente, a Regra 65 das Regras Federais do Processo Civil permite a uma parte procurar tal remédio se: 1) a parte sofrer danos imediatos e irreparáveis se o alívio não for concedido e 2) a parte tentar fornecer o outro aviso prévio de forma atempada. Além disso, a lei exige a aplicação de um teste de equilíbrio, que equilibra o direito de aviso do réu relativamente ao quantum de danos ao público.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9 de fevereiro 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: Dispositivos Ubiquiti Comprometidos e Utilizados como Proxies Inversos do Malware C2 | Edição da Comunidade RiskIQ
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

Ameaças de Estado-Nação

Os atores do estado-nação estão a lançar ataques cibernéticos cada vez mais sofisticados, para evitar a sua deteção e reforçar as suas prioridades estratégicas.

Uma descrição geral das

Ameaças de Estado-Nação

Os atores do estado-nação estão a lançar ataques cibernéticos cada vez mais sofisticados, para evitar a sua deteção e reforçar as suas prioridades estratégicas. O advento da implementação de armas cibernéticas na guerra híbrida na Ucrânia é o início de uma nova era de conflito.

A Rússia também apoiou a guerra com operações de influência da informação, utilizando propaganda para criar impacto nas opiniões na Rússia, na Ucrânia e globalmente. Este primeiro conflito híbrido de grande escala ensinou outras lições importantes. Em primeiro lugar, a segurança das operações e dos dados digitais pode ser protegida de melhor forma, tanto no ciberespaço como no espaço físico, na migração para a cloud. Os ataques russos iniciais visaram serviços on-premises com malware limpador de dados e datacenters físicos direcionados com um dos primeiros mísseis lançados.

A Ucrânia reagiu através da rápida migração de workloads e de dados para clouds de hiperescala alojadas em datacenters fora da Ucrânia. Em segundo lugar, os avanços na análise de informações de ameaças cibernéticas e a proteção de endpoints pelos dados e serviços avançados de IA e ML na cloud ajudaram a Ucrânia a defender-se dos ciberataques russos.

Noutro local, os atores do Estado-nação aumentaram a atividade e estão a utilizar os avanços na automatização, na infraestrutura de cloud e nas tecnologias de acesso remoto para atacarem um conjunto mais amplo de alvos. As cadeias de abastecimento empresariais de TI que permitem o acesso aos alvos finais foram frequentemente atacadas. A higiene da segurança cibernética tornou-se ainda mais crítica à medida que os atores exploravam rapidamente vulnerabilidades não corrigidas, utilizavam tanto técnicas sofisticadas, como de força bruta para roubarem as credenciais e ofuscaram as suas operações através da utilização de software open source ou legítimo. E o Irão junta-se à Rússia na utilização de armas cibernéticas destrutivas, incluindo o ransomware, como um elemento essencial dos seus ataques.

Estes desenvolvimentos exigem a adoção urgente de um enquadramento global consistente que dê prioridade aos direitos humanos e proteja as pessoas contra o comportamento online imprudente do Estado. Todas as nações devem trabalhar para implementar as normas e regras acordadas para uma conduta responsável do Estado.

Defender a Ucrânia: as primeiras lições da ciberguerra — Microsoft On the Issues

Aumento do alvejamento de infraestrutura crítica particularmente no setor das TI, serviços financeiros, sistemas de transporte e infraestrutura de comunicações.

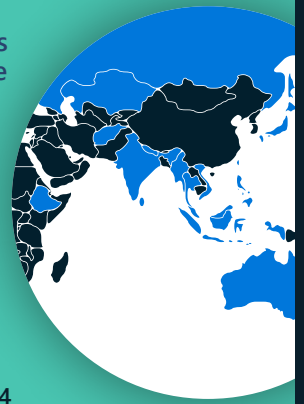
Saiba mais na pág. 35

Cadeia de fornecimento de TI a ser utilizada como um gateway para aceder aos alvos.

NOBELIUM

Saiba mais na pág. 36

A China expande os respetivos objetivos globais, especialmente as nações mais pequenas no sudeste asiático, para obter informações e vantagem competitiva.

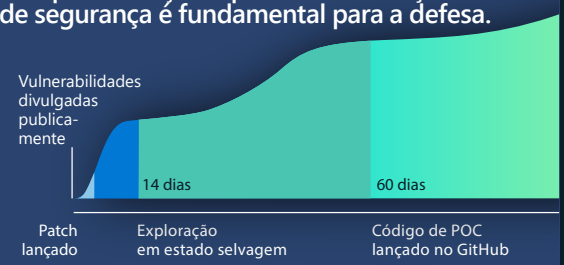


Saiba mais na pág. 44

O Irão tornou-se cada vez mais agressivo depois da transição de energia, expandiu os ataques de ransomware além dos adversários regionais para vítimas dos EUA e da UE e alvejou a infraestrutura crítica norte-americana.

Saiba mais na pág. 46

A identificação e a rápida exploração das vulnerabilidades não corrigidas transformaramse numa tática chave. A implementação rápida de atualizações de segurança é fundamental para a defesa.



Saiba mais na pág. 39

A Coreia do Norte tinha como alvo empresas de defesa e aeroespaciais, criptomoedas, agências de notícias, desertores e organizações de ajuda, para atingir os objetivos do regime: sustentar a defesa, fomentar a economia e garantir a estabilidade doméstica.

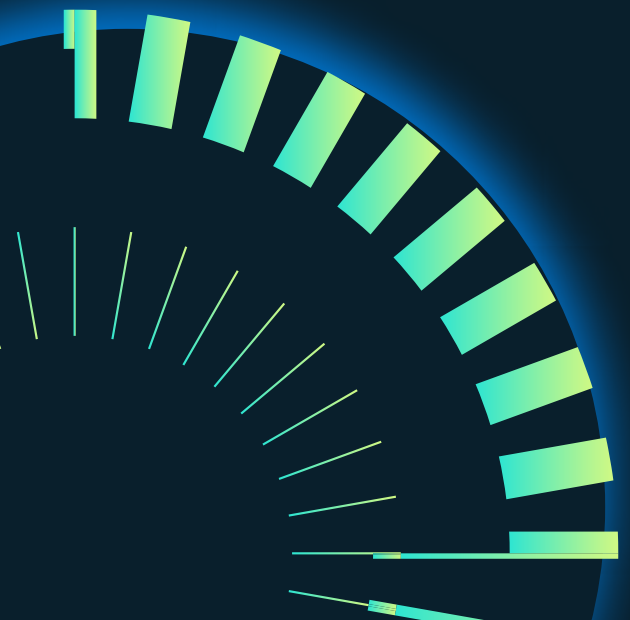
Saiba mais na pág. 49

Os mercenários cibernéticos ameaçam a estabilidade do ciberespaço, uma vez que esta indústria crescente de empresas privadas está a desenvolver e a vender ferramentas, técnicas e serviços avançados para permitir que os seus clientes (muitas vezes governos) invadam redes e dispositivos.

Saiba mais na pág. 52

Introdução

Após os ataques de grande visibilidade em 2020 e 2021, os atores de ameaças do Estado-nação gastaram recursos significativos a adaptarem-se às novas proteções de segurança implementadas pelas organizações para se defenderem contra ameaças sofisticadas.



Como as organizações empresariais, os adversários começaram a utilizar os avanços na automatização, na infraestrutura de cloud e nas tecnologias de acesso remoto para aumentarem os seus ataques contra um conjunto de alvos mais amplo. Estes ajustamentos táticos resultaram em novas abordagens e em ataques de grande escala contra as cadeias de fornecimento empresariais. A higiene da segurança de Ti assumiu um grau de importância ainda maior à medida que os atores desenvolveram novas formas de explorar rapidamente as vulnerabilidades não corrigidas, expandir as técnicas para comprometer as redes empresariais e ofuscar as suas operações através da utilização do software open source ou legítimo. As novas técnicas de ataque forneceram vetores novos e mais difíceis de detetar para obterem acesso à rede de um alvo. Finalmente, à medida que os ataques físicos em tempo de guerra se intensificaram, vimos que os ciberataques têm um papel proeminente na atividade militar.

O conflito na Ucrânia forneceu um exemplo extremamente contundente de como os ciberataques evoluem para afetar o mundo paralelamente aos conflitos militares no terreno. Os sistemas de energia, sistemas de telecomunicações, meios de comunicação e outras infraestruturas críticas tornaram-se alvos de ataques físicos e ciberataques. As tentativas de comprometimento da rede habitualmente observadas como parte das campanhas de espionagem e de extração de informações focaram-se na guerra híbrida contra ataques de malware de limpador de software destrutivo contra sistemas de infraestrutura críticos. A ligação entre a segurança destes sistemas e a cloud resultou na deteção precoce e na interrupção de ataques potencialmente devastadores.[1]

Pela primeira vez num grande evento cibernético, as deteções comportamentais que aproveitam o machine learning utilizaram padrões de ataque conhecidos para identificarem e pararem com êxito os ataques sem conhecimentos prévios do malware subjacente, mesmo antes de os humanos estarem cientes das ameaças. Também confirmámos o valor da partilha de informações sobre ameaças em tempo real com os defensores que protegem estes sistemas, fornecendo-lhes informações vitais para se anteciparem e se defenderem contra os ataques ativos.

Os atores de ameaças do Estado-nação em todo o mundo continuam a expandir as suas operações de formas novas e antigas. A China, a Coreia do Norte, o Irão e a Rússia executaram ataques a clientes Microsoft. A cadeia de fornecimento de serviços de TI tornou-se um alvo comum, uma vez que os atores mudaram o foco para os serviços a montante que podem ser pontos de acesso para várias organizações. Esperamos que os atores continuem a explorar as relações fidedignas nas cadeias de fornecimento empresariais, enfatizando a importância da aplicação abrangente de regras de autenticação, correções diligentes e configuração de contas para a infraestrutura de acesso remoto, e auditorias frequentes das relações com os parceiros para verificação da autenticidade.

Os atores do Estado-nação, assim como o ransomware e os operadores criminosos, responderam ao aumento da exposição ao moverem-se para alvejar sistemas empresariais mal configurados ou não corrigidos (infraestrutura VPN/VPS, servidores on-premises, software de terceiros) para executar ataques "living of the land". Muitos têm aumentado a utilização de malware de produtos e ferramentas open source Red Team para ofuscar as suas atividades maliciosas.

Como resultado, a manutenção de uma linha de base de segurança de TI forte através da aplicação de correções prioritárias, permitindo funcionalidades antiadulteração, utilizando ferramentas de gestão de superfície de ataque como o RiskIQ para obter uma visão externa de uma superfície de ataque e permitindo a autenticação multifator em toda a empresa tornaram-se os conceitos básicos para se defender proativamente contra muitos atores sofisticados.

Os atores do estado-nação também aumentaram a utilização de ransomware como tática nos seus ataques, muitas vezes reutilizando o malware de resgate criado por esse ecossistema criminoso nos seus ataques. Vimos tanto atores baseados na Coreia do Sul como no Irão a alavancar ferramentas de ransomware de produtos para danificar sistemas direcionados, muitas vezes incluindo infraestrutura crítica, nos rivais regionais. Finalmente, vimos a crescente ameaça dos mercenários cibernéticos que desenvolvem e vendem ferramentas, técnicas e serviços para expandir explorações contra as soluções de terceiros vulneráveis. A sofisticação e a agilidade dos ataques dos atores do Estado-nação irão continuar a evoluir a cada ano. As organizações devem responder ao serem informadas destas alterações aos atores e a desenvolver defesas em paralelo.

John Lambert
Vice-Presidente Empresarial e Ilustre Engenheiro, Centro de Informações Sobre Ameaças da Microsoft

Antecedentes sobre os dados de estado-nação

As ameaças de estado-nação são atividades de ciberameaças que têm origem num país específico com a aparente intenção de fomentar os interesses nacionais. Os atores do estado-nação apresentam algumas das ameaças mais avançadas e persistentes que os nossos clientes enfrentam, incluindo o roubo de propriedade intelectual, espionagem, vigilância, roubo de credenciais, ataques destrutivos e muito mais.

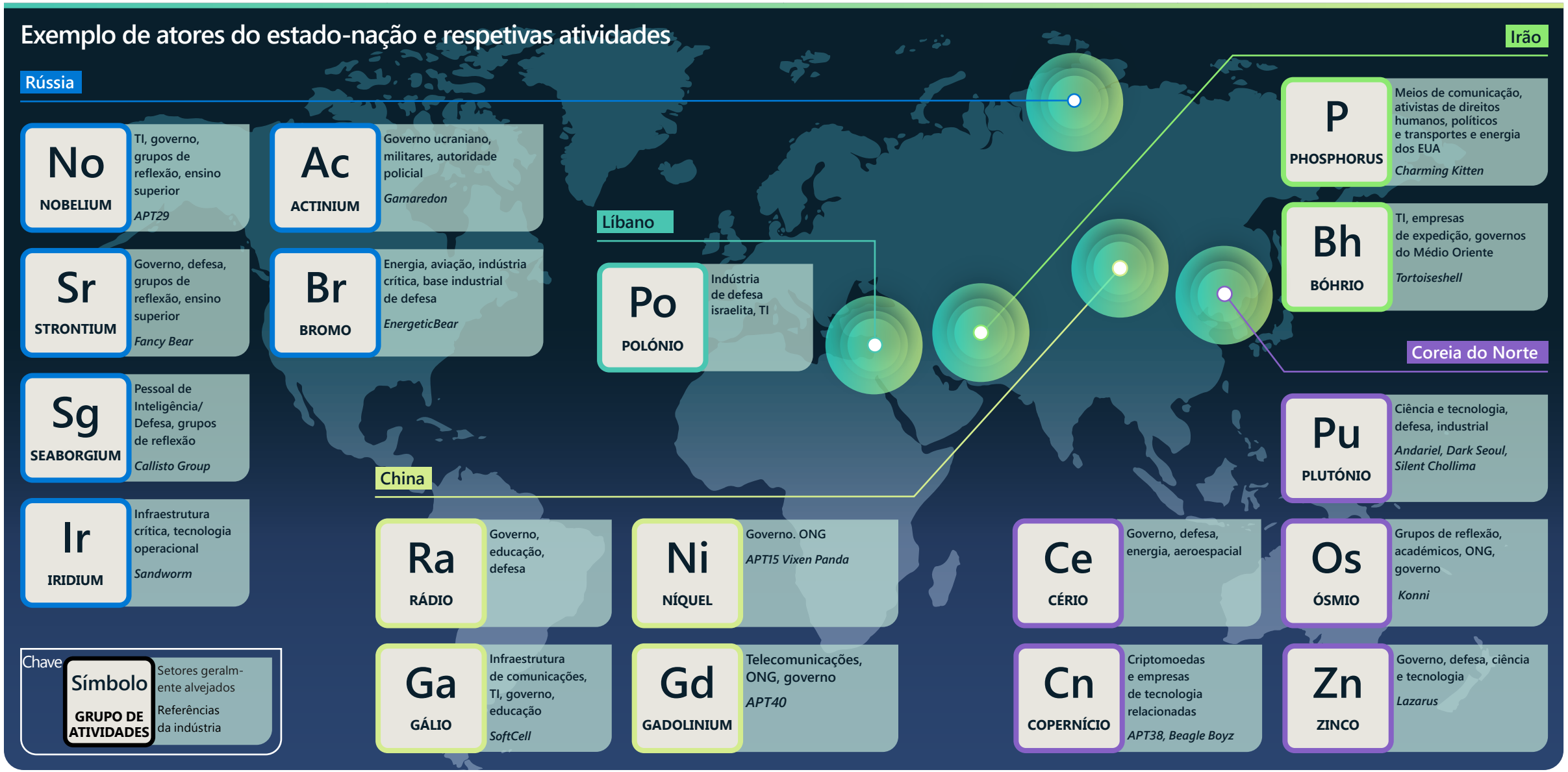
Investimos recursos significativos na descoberta, compreensão e neutralização destas ameaças. Quando uma organização ou titular de uma conta individual é alvejado ou comprometido por atividades observadas do Estado-nação, a Microsoft envia um alerta sob a forma de uma notificação de Estado-nação (NSN) diretamente ao cliente, incluindo as informações que precisam para investigar a atividade. A partir de junho de 2022, tínhamos enviado mais de 67.000 NSN desde que começámos em 2018.

Os dados de alerta NSN da Microsoft são apresentados neste capítulo para fornecer uma visão da atividade mensurável. O nível de atividade do Estado-nação mostrado nos gráficos baseia-se no número de NSN da Microsoft emitidos aos clientes em resposta à deteção de atores do Estado-nação que visam ou comprometem pelo menos uma conta na organização do cliente.

Os quatro Estados-nação primários cujos grupos de ameaças incluímos neste relatório são a Rússia, a China, o Irão e a Coreia do Norte. Estes representam os países de origem dos atores mais comumente observados direcionados para os clientes Microsoft ao longo do ano passado. O relatório também inclui as nossas observações sobre grupos de ameaças do Líbano e de mercenários cibernéticos, ou atores ofensivos do setor privado para serem contratados.

A Microsoft identifica os grupos de Estado-nação por nomes de elementos químicos (como o NOBELIUM), e na página seguinte apresentamos apenas alguns dos mesmos. Utilizamos as designações DEV-#### como um nome temporário dado a um cluster de ameaças desconhecido, emergente ou em desenvolvimento, o que nos permite monitorizá-lo como um conjunto exclusivo de informações até chegarmos a um elevado grau de confiança sobre a origem ou a identidade do agente por detrás da atividade.

Uma vez que cumpre os critérios, um DEV é convertido num ator nomeado ou fundido com os atores existentes. Ao longo deste capítulo, citamos exemplos de grupos de estado-nação e de DEV para fornecer uma visão mais aprofundada dos alvos de ataque, técnicas e análise de motivações. Apesar de muitos destes grupos utilizarem as mesmas ferramentas que os cibercriminosos, apresentam ameaças exclusivas sob a forma de malware personalizado, a capacidade de descobrir e capitalizar as vulnerabilidades de dia zero e a impunidade legal.


Exemplo de atores do estado-nação e respetivas atividades
Rússia
No
NOBELIUM
TI, governo, grupos de reflexão, ensino superior
APT29
Ac
ACTINIUM
Governo ucraniano, militares, autoridade policial
Gamaredon
Sr
STRONTIUM
Governo, defesa, grupos de reflexão, ensino superior
Fancy Bear
Br
BROMO
Energia, aviação, indústria crítica, base industrial de defesa
EnergeticBear
Sg
SEABORGIUM
Pessoal de Inteligência/ Defesa, grupos de reflexão
Callisto Group
Ir
IRIDIUM
Infraestrutura crítica, tecnologia operacional
Sandworm
Líbano
Po
POLÓNIO
Indústria de defesa israelita, TI
Irão
P
PHOSPHORUS
Meios de comunicação, ativistas de direitos humanos, políticos e transportes e energia dos EUA
Charming Kitten
Bh
BÓHRIO
TI, empresas de expedição, governos do Médio Oriente
Tortoiseshell
Coreia do Norte
Pu
PLUTÓNIO
Ciência e tecnologia, defesa, industrial
Andariel, Dark Seoul, Silent Chollima
China
Ra
RÁDIO
Governo, educação, defesa
Ni
NÍQUEL
Governo. ONG
APT15 Vixen Panda
Ce
CÉRIO
Governo, defesa, energia, aeroespacial
Os
ÓSMIO
Grupos de reflexão, académicos, ONG, governo
Konni
Ga
GÁLIO
Infraestrutura de comunicações, TI, governo, educação
SoftCell
Gd
GADOLINIUM
Telecomunicações, ONG, governo
APT40
Cn
COPERNÍCIO
Criptomoedas e empresas de tecnologia relacionadas
APT38, Beagle Boyz
Zn
ZINCO
Governo, defesa, ciência e tecnologia
Lazarus
Chave
Símbolo
GRUPO DE ATIVIDADES
Setores geralmente alvejados
Referências da indústria

O panorama em evolução de ameaças

A missão da Microsoft para monitorizar a atividade do ator do estado-nação e notificar os clientes quando os vemos a ser alvejados ou comprometidos está enraizada na nossa missão de proteger os nossos clientes contra ataques.

Esta notificação é uma parte crucial do nosso compromisso de informar os clientes se os ataques observados são prevenidos com êxito pelas nossas proteções de produtos de segurança ou se os ataques são eficazes devido a falhas de segurança desconhecidas. O controlo das notificações ao longo do tempo ajuda a Microsoft a identificar as tendências de ameaças em evolução por atores e concentrar as proteções dos produtos na mitigação proativa das ameaças aos clientes nos nossos serviços de cloud.

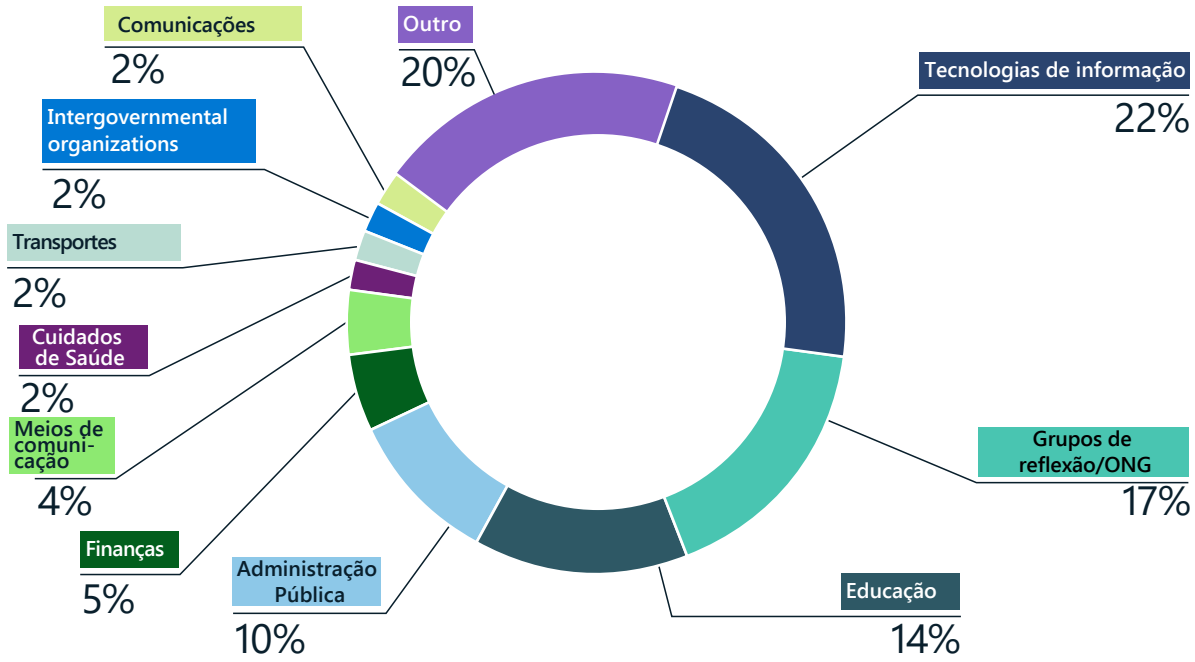
Este controlo também nos permite partilhar dados e insights sobre o que vemos. Os analistas que monitorizam estes atores e seguem os seus ataques baseiam-se numa combinação de indicadores técnicos e conhecimentos geopolíticos para compreender as motivações dos atores, combinando o contexto técnico e global com novos insights. Esta curadoria fornece uma visão única sobre as prioridades dos atores cibernéticos do Estado-nação e como as suas motivações podem espelhar as prioridades políticas, militares e económicas dos Estados-nação que as empregam.

Os desenvolvimentos políticos no ano passado moldaram as prioridades e a tolerância aos riscos dos grupos de ameaças patrocinados pelo estado em todo o mundo. À medida que as relações geopolíticas foram divididas e os elementos tipo falcão adquiriram mais controlo em algumas nações, os atores cibernéticos tornaram-se mais descarados e agressivos. Por exemplo:

- A Rússia visava incansavelmente o governo ucraniano e a infraestrutura crítica do país para complementar a sua ação militar no terreno.[2]
- O Irão procurou agressivamente incursões na infraestrutura crítica norte-americana, como as autoridades portuárias.
- A Coreia do norte continuou a sua campanha de roubo de criptomoedas de empresas financeiras e tecnológicas.
- A China expandiu as suas operações de espionagem cibernética global.

Apesar de os atores dos Estados-nação poderem ser tecnicamente sofisticados e empregar uma ampla variedade de táticas, os seus ataques podem muitas vezes ser mitigados por uma boa higiene cibernética. Muitos destes atores dependem de meios relativamente pouco tecnológicos, como e-mails de spear-phishing de lança, para oferecer malware sofisticado em vez de investirem no desenvolvimento de explorações personalizadas ou na utilização de engenharia social direcionada para atingirem os seus objetivos.

Setores da indústria direcionados por atores do Estado-nação



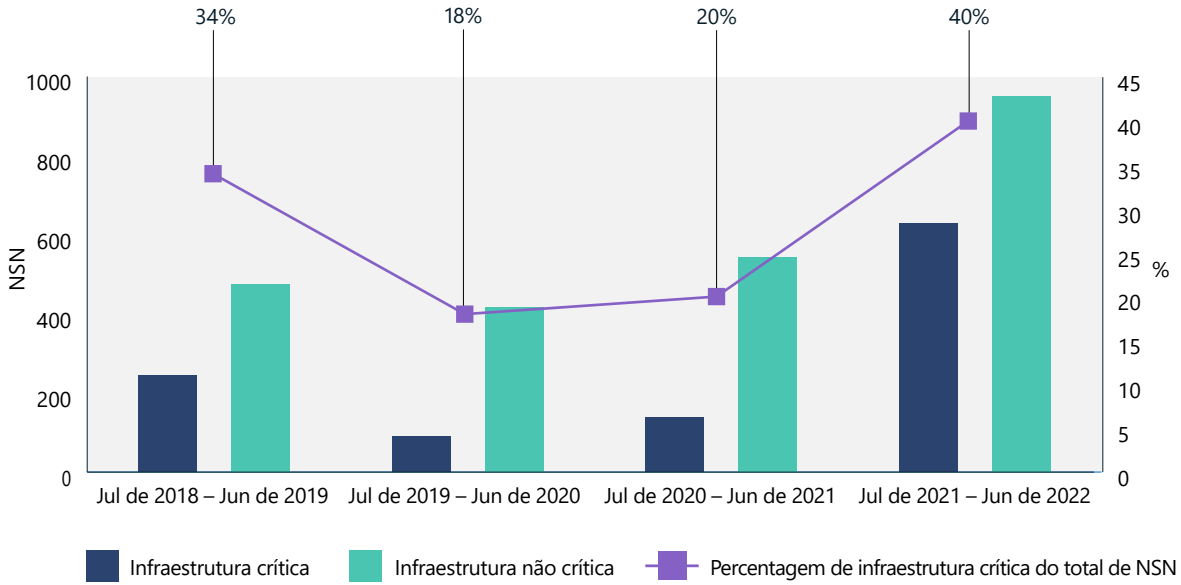
Os grupos de Estado-nação visaram uma série de setores. Os atores estatais russos e iranianos visaram o setor de TI como um meio de acesso aos clientes das empresas de TI. Os grupos de reflexão, as organizações não governamentais (ONG), as universidades e as agências governamentais permaneceram como outros alvos comuns dos atores do estado-nação.

Os intervenientes do Estado-nação têm uma variedade de objetivos que podem resultar no alvejamento de grupos específicos de organizações ou indivíduos. No último ano, os ataques à cadeia de fornecimento aumentaram, com um foco específico nas empresas de TI. Ao comprometer os fornecedores de serviços de TI, os atores de ameaças são muitas vezes capazes de alcançar o seu objetivo original através de uma relação de confiança com a empresa que gere sistemas ligados ou executam potencialmente ataques a uma escala muito maior ao comprometer centenas de clientes a jusante num único ataque. Depois do setor de TI, as entidades mais frequentemente orientadas foram os grupos de reflexão, académicos ligados a universidades e funcionários do governo. Estes são "alvos vulneráveis" desejáveis para a espionagem para recolher informações sobre problemas geopolíticos.

O panorama em evolução de ameaças

Continuação

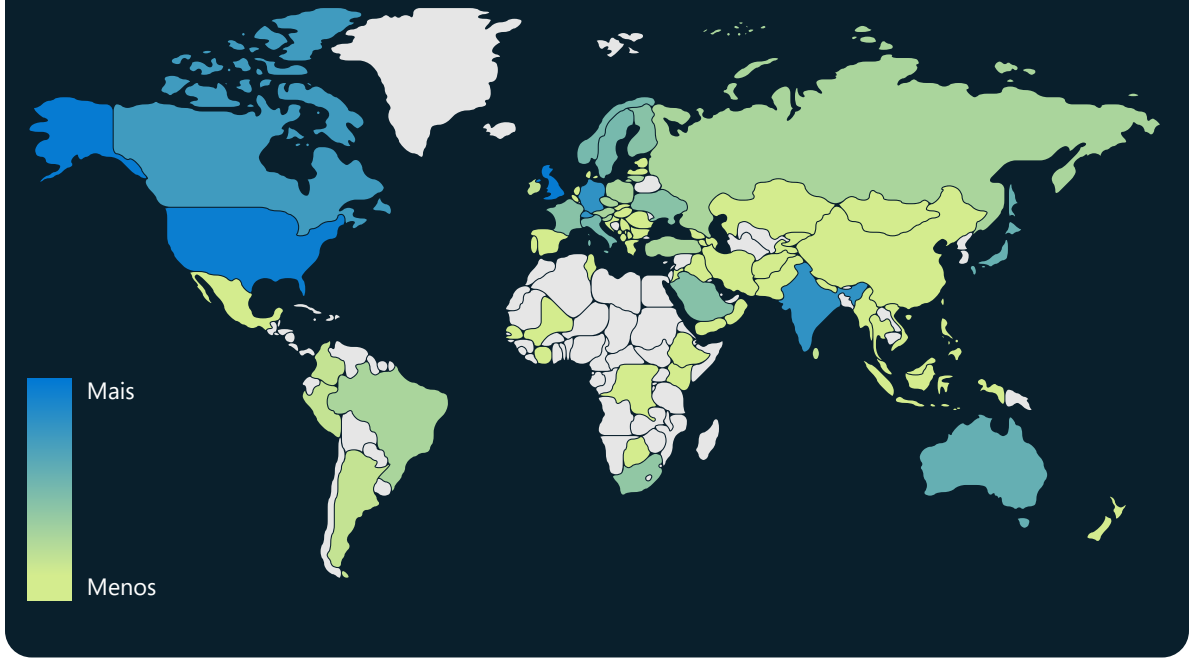
Tendências de infraestrutura crítica



Os objetivos de infraestrutura crítica dos grupos do estado-nação[3] aumentaram no último ano, com os atores a concentrarem-se em empresas do setor de TI, serviços financeiros, sistemas de transporte e infraestrutura de comunicações.

> "Antes da invasão da Ucrânia, os governos pensavam que os dados precisavam de permanecer dentro de um país para estarem seguros. Depois da invasão, a migração de dados para a cloud e a mudança para fora das fronteiras territoriais fazem agora parte do planeamento da resiliência e da boa governação."
>
> **Cristin Flynn Goodwin,**
> Conselheiro Geral Adjunto, Segurança e Confiança do Cliente

Objetivos geográficos dos atores do estado-nação



O alvejamento cibernético dos grupos do Estado-nação atravessou o mundo no ano passado, com um foco particularmente pesado nas empresas britânicas e norte-americanas. As organizações em Israel, nos Emirados Árabes Unidos, no Canadá, na Alemanha, na Índia, na Suíça e no Japão também estavam entre algumas das mais frequentemente alvejadas, segundo os nossos dados do NSN.

Insights acionáveis

1. Identifique e proteja os seus potenciais alvos de dados de elevado valor, as tecnologias de risco, as informações e as operações de negócio que possam estar alinhadas com as prioridades estratégicas dos grupos de Estados-nação.
2. Ative as proteções da cloud para fornecer a identificação e mitigação de ameaças conhecidas e novas para a sua rede, à escala.

A cadeia de fornecimento de TI como gateway do ecossistema digital

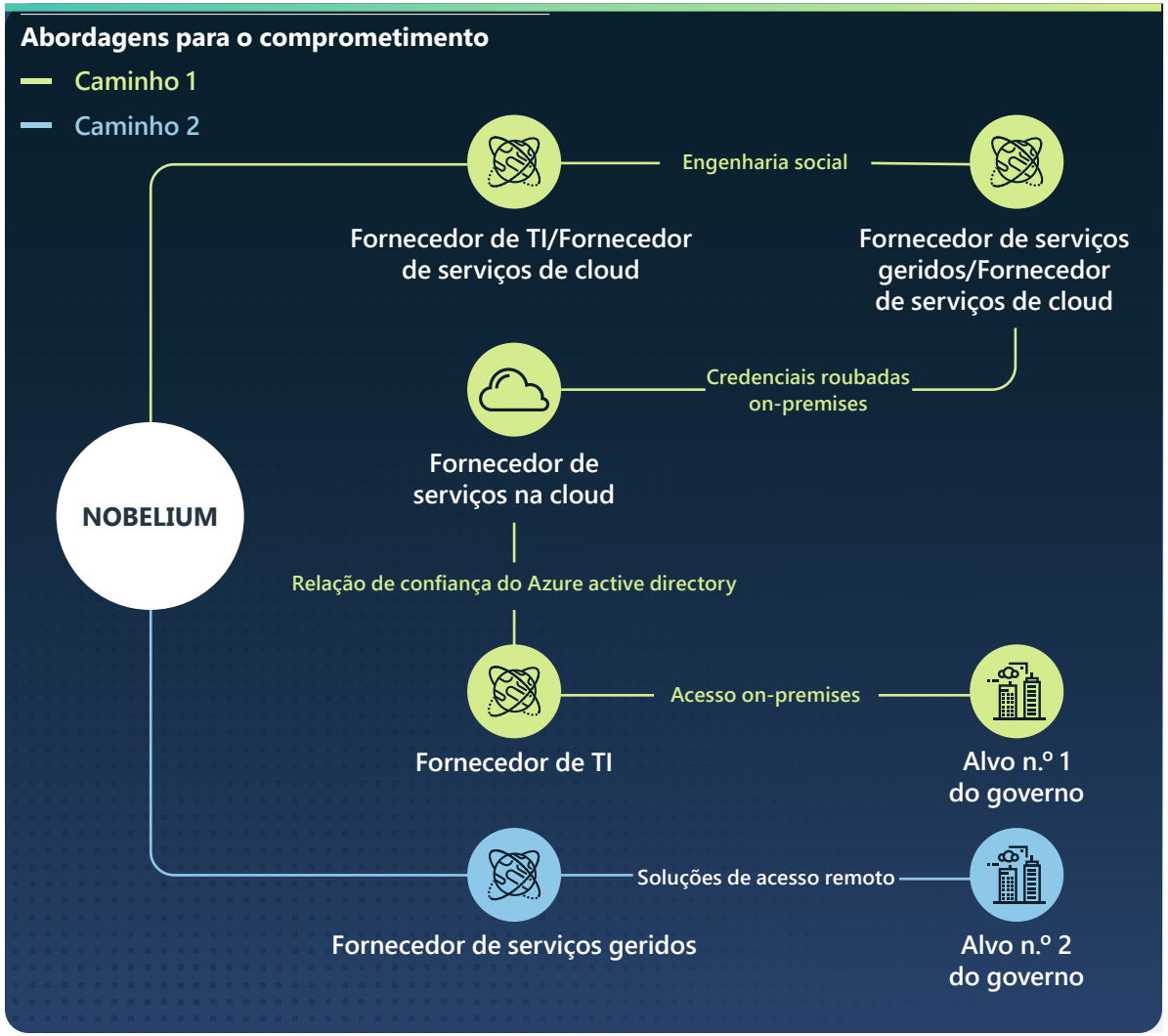
Os ataques de estado-nação a fornecedores de serviços de TI podem permitir que os atores de ameaças explorem outras organizações de interesse ao tirarem partido da confiança e do acesso concedidos a estes fornecedores de cadeias de fornecimento. No ano passado, os grupos de ciberameaças de estado-nação alvejaram os fornecedores de serviços de TI para atacarem alvos de terceiros e obterem acesso a clientes a jusante nos setores governamental, político e de infraestrutura crítica.

Os fornecedores de serviços de TI são alvos intermediários atraentes ao servirem centenas de clientes diretos e milhares de clientes indiretos de interesse para os serviços de inteligência estrangeiros. Se exploradas, as práticas de negócio de rotina e os privilégios administrativos delegados de que estas empresas usufruem, poderão permitir que os atores maliciosos acedam e manipulem as redes de cliente do fornecedor de serviços de Ti sem acionar alertas imediatamente.

No ano passado, o NOBELIUM tentou comprometer e tirar partido das contas privilegiadas em soluções de cloud e outros fornecedores de serviços geridos para tentar obter acesso a jusante alvejando principalmente clientes governamentais e políticos dos EUA e da Europa.

O NOBELIUM demonstrou como uma abordagem de "comprometer um para comprometer muitos" pode ser dirigida contra um adversário geopolítico percebido. No ano passado, o ator de ameaças procurou intrusões diretas e de terceiros em organizações confidenciais com base nos Estados membros da Organização do Tratado do Atlântico Norte (NATO), que o governo russo percebe como uma ameaça existencial. Entre julho de 2021 e início de junho de 2022, 48% das notificações de clientes da Microsoft de atividade de ameaças russas contra serviços online, os clientes foram para as empresas de setor de Ti com base nos países membros da NATO, provavelmente como pontos de acesso intermediários. Globalmente, 90% das notificações sobre a atividade de ameaças russas durante o mesmo período foram para os clientes com sede nos Estados membros da NATO, principalmente nas áreas de TI, grupos de reflexão e organizações não governamentais (ONG) e setores do governo, sugerindo uma estratégia de busca de múltiplos meios de acesso inicial a estes alvos.

Houve uma mudança da exploração da cadeia de fornecimento de software para a exploração da cadeia de fornecimento de serviços de TI, visando soluções de cloud e fornecedores de serviços geridos para chegarem aos clientes a jusante.



Este diagrama retrata a abordagem multicanal do NOBELIUM para comprometer os seus alvos finais e os danos colaterais a outras vítimas ao longo do caminho. Além das ações mostradas acima, o NOBELIUM lançou spray de palavras-passe e ataques de phishing contra as entidades envolvidas, visando mesmo a conta pessoal de pelo menos um funcionário público como outra rota potencial para o comprometimento.

A cadeia de fornecimento de TI como gateway do ecossistema digital

Continuação

Ao longo do ano, o Centro de Informações Sobre Ameaças da Microsoft (MSTIC) detetou um número cada vez maior de atores ligados ao estado iraniano e ao Irão que comprometem as empresas de TI. Em muitos casos, os atores foram detetados a roubar credenciais de início de sessão para obter acesso aos clientes a jusante para uma série de objetivos, desde a recolha de informações aos ataques destrutivos de retaliação.

- Em julho e agosto de 2021, o DEV-0228 comprometeu um fornecedor de software de negócio israelita a comprometer mais tarde os clientes a jusante nos setores de defesa, energia e legal israelitas.[4]
- Entre agosto e setembro de 2021, a Microsoft detetou um aumento de atores estatais iranianos que se destinava a empresas de TI com base na índia. A ausência de problemas geopolíticos urgentes que teriam motivado tal mudança sugere que este alvejamento seja destinado a acesso indireto a subsidiárias e clientes fora da Índia.
- Em janeiro de 2022, o DEV-0198, um grupo que avaliamos como afiliado do governo do Irão, comprometeu um fornecedor de soluções de cloud israelitas. A Microsoft avalia o ator que utilizou provavelmente credenciais comprometidas do fornecedor para autenticar uma empresa de logística israelita. O MSTIC observou o mesmo ator a tentar conduzir um ciberataque destrutivo contra a empresa de logística no final do mês.
- Em abril de 2022, o POLÓNIO, um grupo que avaliámos baseado no Líbano, colaborou com grupos estatais iranianos sobre técnicas de cadeia de fornecimento de TI, comprometeu outra empresa israelita de TI a obter acesso às organizações legais e de defesa israelitas.[5]

No ano anterior, a atividade demonstra que atores de ameaças como o NOBELIUM e o DEV-0228 estão a conhecer melhor o panorama das relações fidedignas de uma organização do que as próprias organizações. Esta maior ameaça enfatiza a necessidade de as organizações compreenderem e fortalecerem as fronteiras e os pontos de entrada das suas propriedades digitais. Além disso, sublinha a importância de os fornecedores de serviços de TI monitorizarem rigorosamente o seu próprio estado de segurança cibernética. Por exemplo, as organizações devem implementar políticas de autenticação multifator e acesso condicional que dificultam a captura de contas privilegiadas por parte de atores mal-intencionados ou a disseminação através de uma rede.

A realização de uma análise completa e a auditoria de relações com os parceiros ajuda a minimizar quaisquer permissões desnecessárias entre a sua organização e os fornecedores a montante e remove imediatamente o acesso a quaisquer relações que não pareçam familiares. A crescente familiaridade com os registos de atividade e a análise da atividade disponível facilitam a deteção de anomalias que podem desencadear investigações adicionais.

> Os ataques de estado-nação a terceiros permitem-lhes explorar organizações sensíveis ao tirarem partido da confiança e do acesso numa cadeia de fornecimento.

Insights acionáveis

1. Analise e audite as relações do fornecedor de serviços a montante e a jusante e os acessos privilegiados delegados para minimizar as permissões desnecessárias. Remova o acesso a quaisquer relações com parceiros que não pareçam familiares ou que ainda não tenham sido auditadas.[6]
2. Ative o registo e analise toda a atividade de autenticação para infraestruturas de acesso remoto e redes privadas virtuais (VPN), com foco nas contas configuradas com a autenticação de fator único, para confirmar a autenticidade e investigar atividades anómalas.
3. Ative a MFA para todas as contas (incluindo as contas de serviço) e certifique-se de que a MFA está em vigor para toda a conectividade remota.
4. Utilize soluções sem palavras-passe para proteger as contas.[7]

Ligações para mais informações

- O NOBELIUM visa privilégios administrativos delegados para facilitar ataques mais amplos | Centro de Informações Sobre Ameaças da Microsoft (MSTIC)
- Alvejamento iraniano no setor de TI em crescimento | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft
- Expor a atividade e a infraestrutura do POLÓNIO dirigidas às organizações israelitas | Centro de Informações Sobre Ameaças da Microsoft (MSTIC)

Exploração rápida da vulnerabilidade

À medida que as organizações fortalecem as suas posturas de cibersegurança, os atores do estado-nação respondem perseguindo novas e exclusivas táticas para gerar ataques e evitar a deteção. A identificação e exploração de vulnerabilidades anteriormente desconhecidas, conhecidas como vulnerabilidades de dia zero, são uma tática chave neste esforço.

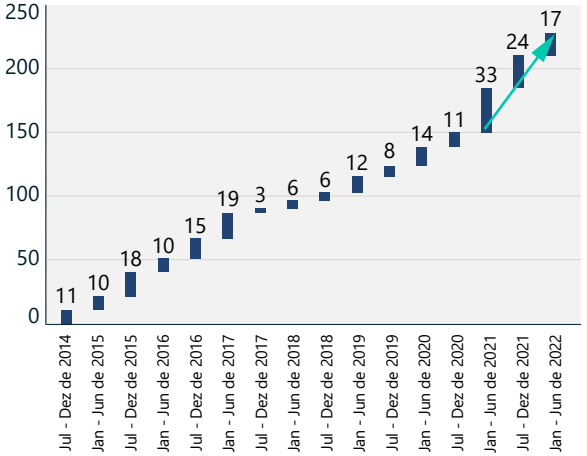
As vulnerabilidades de dia zero são um meio particularmente eficaz para a exploração inicial e, uma vez expostas publicamente, as vulnerabi-lidades podem ser rapidamente reutilizadas por outros atores estatais e criminosos. O número de vulnerabilidades de dia zero divulgadas publicamente no último ano está a par dos do ano anterior, que foi o número mais alto registado.

À medida que os atores de ameaças cibernéticas, tanto estatais como criminosos, se tornam mais aptos a tirar partido destas vulnerabilidades, observamos uma redução no tempo entre o anúncio de uma vulnerabilidade e a mercantilização dessa vulnerabilidade. Isto torna essencial que as organizações corrijam imediatamente as explorações. Da mesma forma, é fundamental que as organizações ou indivíduos que descobrem novas vulnerabilidades as divulguem ou relatem de forma responsável aos fornecedores afetados o mais rapidamente possível, de acordo com os procedimentos de divulgação de vulnerabilidades coordenadas.

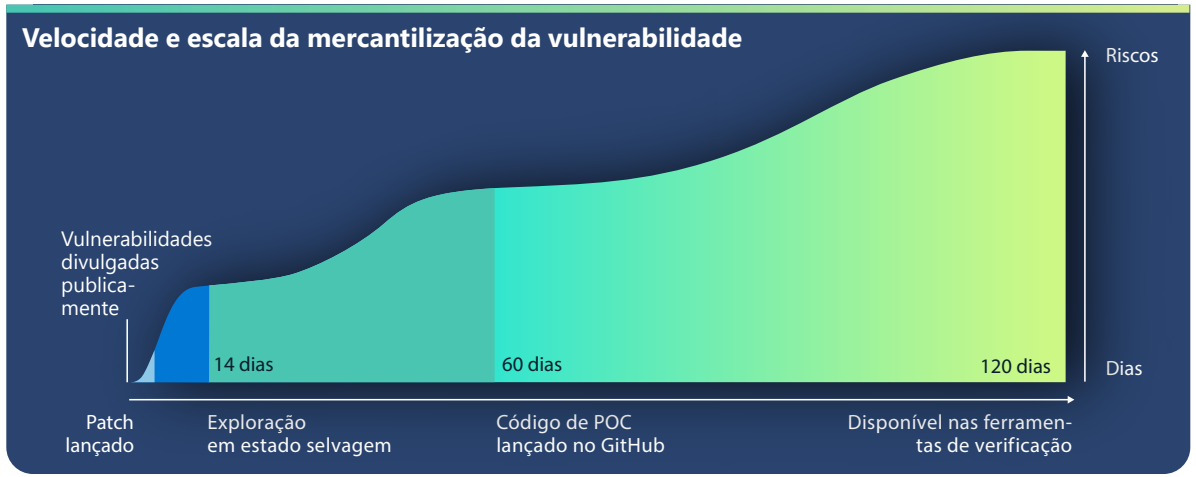
Isto garante que as vulnerabilidades são identificadas e os patches desenvolvidos de forma atempada para proteger os clientes contra ameaças anteriormente desconhecidas.

Muitas organizações assumem que têm menos probabilidades de serem vítimas de ataques de exploração de dia zero se a gestão de vulnerabilidades for essencial para a sua segurança de rede. No entanto, a mercantilização de explorações está a fazer com que cheguem a um ritmo muito mais rápido. As explorações de dia zero são muitas vezes descobertas por outros atores e reutilizadas amplamente num curto período de tempo, o que deixa em risco os sistemas não corrigidos. Apesar de a exploração de dia zero poder ser difícil de detetar, as ações pós-exploração dos atores são muitas vezes mais fáceis de detetar e, se forem provenientes de software totalmente corrigido, podem agir como um sinal de alerta de um comprometimento.

Correções lançadas para vulnerabilidades de dia-zero



Números de explorações de dia zero divulgadas publicamente na Lista das Vulnerabilidades e Divulgações Comuns (CVE).



Em média, leva apenas 14 dias para que uma exploração esteja disponível depois de uma vulnerabilidade ser divulgada publicamente. Esta vista fornece uma análise dos prazos de exploração das vulnerabilidades de dia zero, juntamente com o número de sistemas vulneráveis à dita exploração e ativa na Internet desde o primeiro momento da divulgação pública.

Embora os ataques de vulnerabilidade de dia zero tendam inicialmente a visar um conjunto limitado de organizações, são rapidamente adotados no ecossistema de atores de ameaças maior. Isto inicia uma corrida para os atores de ameaças explorarem a vulnerabilidade o mais amplamente possível antes de os seus potenciais alvos instalarem patches.

Enquanto observamos muitos atores estatais da nação a desenvolverem explorações a partir de vulnerabilidades desconhecidas, os atores de ameaças de Estado-nação baseados na China são particularmente proficientes na descoberta e no desenvolvimento de explorações de dia zero. O regulamento de relatórios de vulnerabilidades da China entrou em vigor em setembro de 2021, marcando o primeiro lugar no mundo para um governo exigir a denúncia de vulnerabilidades a uma autoridade governamental para análise antes de a vulnerabilidade ser partilhada com o produto ou o proprietário do serviço. Este novo regulamento pode permitir que os elementos no governo chinês armazenem vulnerabilidades reportadas para as transformar em armas. O aumento da utilização de dia zero no último ano a partir de atores baseados na China reflete provavelmente o primeiro ano completo dos requisitos de divulgação de vulnerabilidades da China para a comunidade de segurança chinesa e um passo importante na utilização de explorações de dia zero como prioridade do estado. As vulnerabilidades descritas abaixo foram inicialmente desenvolvidas e implementadas por atores de Estado-nação baseados na China em ataques, antes de serem descobertas e distribuídas por outros atores no ecossistema de ameaças de tamanho maior.

Exploração rápida da vulnerabilidade

Continuação

Mesmo as organizações que não são alvo de ataques de estado-nação têm um período limitado para corrigir vulnerabilidades de dia zero em sistemas impactados antes de serem exploradas pelo ecossistema mais amplo de atores.

Estes exemplos de vulnerabilidades recentemente identificadas demonstram que as organizações têm, em média, 60 dias a partir do momento em que uma vulnerabilidade é corrigida e é disponibilizado online um código de prova de conceito (POC) e muitas vezes são recolhidos por outros atores para reutilização. Da mesma forma, as organizações têm, em média, 120 dias antes de uma vulnerabilidade estar disponível em ferramentas automatizadas de verificação e exploração de vulnerabilidades, como o Metasploit, que resulta, muitas vezes, na utilização da exploração em grande escala. Isto evidencia que mesmo as organizações que não são alvo de atores de ameaças de Estado-nação têm um período limitado para corrigir vulnerabilidades de dia zero em sistemas impactados antes de as vulnerabilidades serem exploradas pelo ecossistema mais amplo de atores.

CVE-2021-35211 SolarWinds Serv-U

Em julho de 2021, a SolarWinds lançou um comunicado de segurança para o CVE-2021-35211, creditando a Microsoft com a notificação.[8] Na altura, descobrimos o ator de ameaças DEV-0322 alinhado com o Estado-nação a explorar ativamente a vulnerabilidade do Serv-U da SolarWinds. A nossa equipa RiskIQ observou 12.646 endereços IP de alojamento de versões ligadas à Internet dos dispositivos afetados entre 15 de junho e 9 de julho.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

Em setembro de 2021, os nossos investigadores observaram atores afiliados da China que exploravam o Zoho ManageEngine em várias entidades baseadas nos EUA. A vulnerabilidade foi comunicada publicamente a 6 de setembro como CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, que as organizações normalmente utilizam para processar redefinições de palavra-passe.[9] O DEV-0322 explorou a vulnerabilidade mais tarde, em setembro, utilizando-o como um vetor inicial para obter uma posição nas redes e executar ações adicionais, incluindo o dumping de credenciais, a instalação de binários personalizados e a queda de malware para manter a persistência. No momento da divulgação, o RiskIQ observou 4.011 instâncias destes sistemas ativos e na Internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

No final de outubro de 2021, observámos o DEV-0322 a tirar partido de uma vulnerabilidade (CVE-2021-44077) num segundo produto Zoho ManageEngine, ServiceDesk Plus, um software de suporte técnico de TI com gestão de ativos. O DEV-0322 utilizou esta vulnerabilidade para alvejar e comprometer as entidades no setor da saúde, tecnologias da informação, ensino superior e setores industriais críticos. A 2 de dezembro, o Federal Bureau of Investigation (FBI) e a Cybersecurity and Infrastructure Security Agency (CISA) emitiram um aviso consultivo conjunto para o público sobre os atores de ameaças de Estado-nação que aproveitam a vulnerabilidade. No momento da divulgação, o RiskIQ observou 7.956 instâncias destes sistemas ativos e na Internet.

CVE-2021-42321 Microsoft Exchange

Uma exploração de dia zero para uma vulnerabilidade CVE -2021-42321 do Exchange foi revelada durante a Tianfu Cup, uma cimeira internacional de cibersegurança e uma competição de acesso ilícito que ocorreu a 16 e 17 de outubro de 2021 em Chengdu, China. Os investigadores de segurança na Microsoft observaram a exploração para a vulnerabilidade do Exchange utilizada no estado selvagem a 21 de outubro, apenas três dias depois de a vulnerabilidade ter sido revelada. No momento da divulgação, o RiskIQ observou 61.559 instâncias destes sistemas ativos e na Internet, no momento da divulgação. Continuámos a observar a atividade de exploração em novembro de 2021.

CVE-2022-26134 Confluence

Um ator afiliado da China tinha provavelmente o código de exploração de dia zero para a vulnerabilidade Confluence (CVE -2022-26134) quatro dias antes de a vulnerabilidade ter sido divulgada publicamente a 2 de junho e provavelmente deve tê-lo aproveitado contra uma entidade baseada nos EUA. No momento da divulgação, o RiskIQ observou 53.621 instâncias destes sistemas Confluence vulneráveis na Internet.

As vulnerabilidades estão a ser retiradas e exploradas em grande escala e em prazos cada vez mais curtos.

Insights acionáveis

1. Priorize a aplicação de correções nas vulnerabilidades de dia zero assim que forem lançadas; não espere que o ciclo de gestão de patches seja implementado.
2. Documente e inventarie todos os ativos de hardware e software da empresa para determinar o risco e definir rapidamente quando agir em patches.

As táticas cibernéticas dos atores russos em tempo de guerra ameaçam a Ucrânia e não só

Este ano, os atores estatais russos lançaram operações cibernéticas para complementarem a ação militar durante a invasão da Ucrânia pela Rússia, muitas vezes utilizando as mesmas táticas e técnicas implementadas contra alvos fora da Ucrânia. É fundamental que as organizações em todo o mundo tomem medidas para fortalecer a cibersegurança contra as ameaças digitais resultantes dos atores de ameaças alinhados com a Rússia.

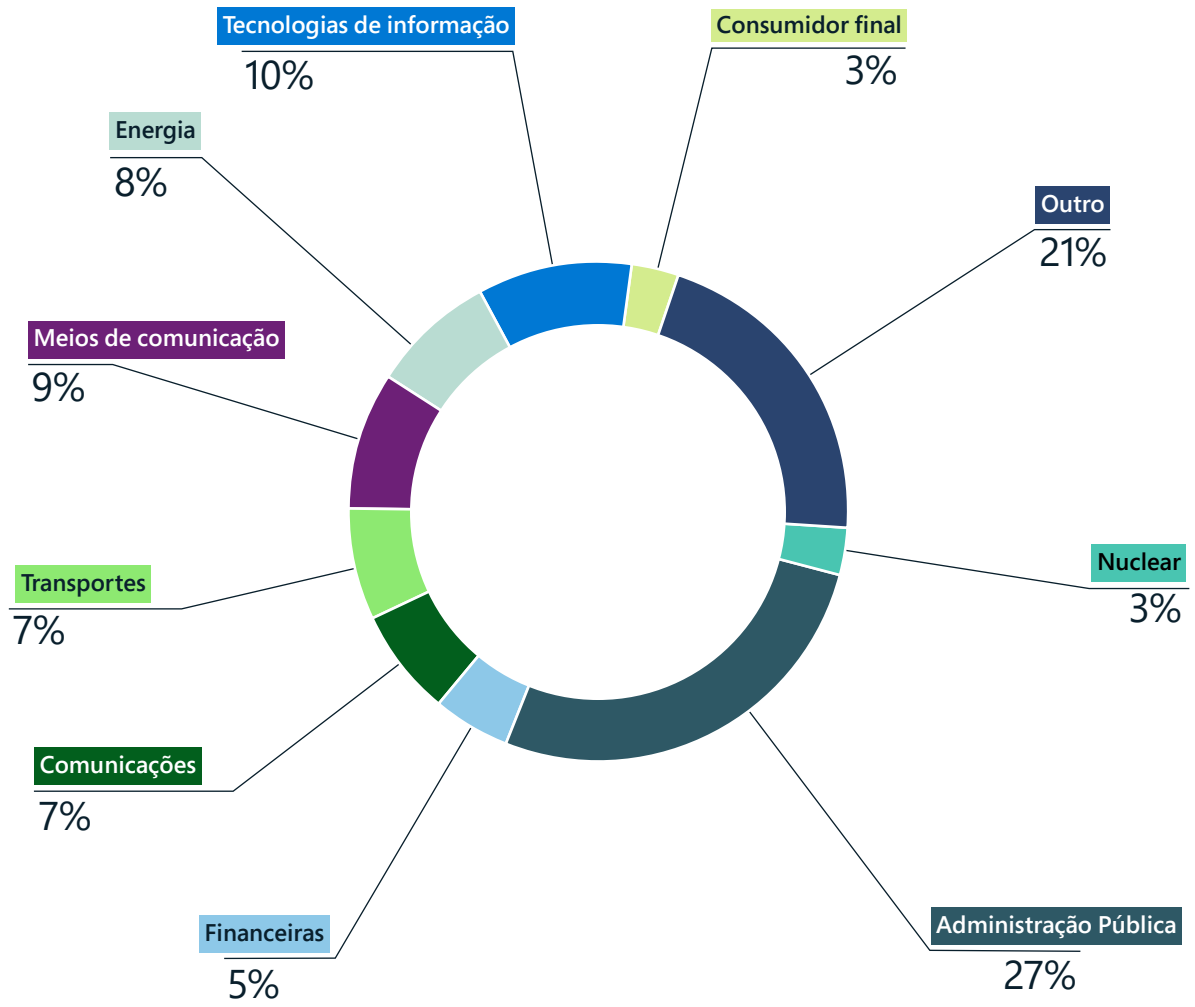
A situação no terreno continua a flutuar à medida que persiste o conflito militar, e a Ucrânia e os seus aliados devem estar preparados para se defenderem se os operadores cibernéticos do estado russo aumentarem a frequência ou a intensidade das intrusões em conformidade com os objetivos militares. Durante os primeiros quatro meses da guerra, a Microsoft observou atores de ameaças associados às forças armadas russas lançaram várias ondas de ciberataques destrutivos contra quase 50 agências e empresas ucranianas distintas e intrusões focadas na espionagem contra muitas outras. Excluindo as operações contra os clientes dos serviços online, 64% da atividade de ameaças russas contra alvos conhecidos era dirigida a organizações baseadas na Ucrânia, entre final de fevereiro e junho.

Em cada operação, os atores de ameaças russos empregaram muitas das táticas, técnicas e procedimentos (TTP) que observámos serem utilizados antes da invasão contra alvos dentro e fora da Ucrânia. Estes atores pretendiam destruir os dados e desequilibrar os órgãos do governo ucraniano no período inicial do conflito. Desde então, procuraram descarrilar o transporte de ajuda humanitária e militar para a Ucrânia, perturbar o acesso público aos serviços e aos meios de comunicação, e roubar informações sobre a inteligência a longo prazo ou o valor económico para a Rússia.

O alvejamento dos transportes ameaça uma área de importância crítica para os cidadãos ucranianos que tentam sobreviver ao conflito. De acordo com um inquérito patrocinado pela UNICEF em maio, os inquiridos nas áreas urbanas afetadas pelo conflito estavam mais preocupados com o transporte e o combustível, as interrupções no aprovisionamento, a segurança e o acesso limitado aos alimentos, aos serviços médicos e aos serviços financeiros.[10] Em junho, o Coordenador de Crises da ONU para a Ucrânia disse que pelo menos 15,7 milhões de pessoas na Ucrânia precisavam urgentemente de ajuda humanitária e o número iria crescer à medida que a guerra continuasse.[11]

Fora da Ucrânia, a Microsoft detetou esforços de intrusão da rede russos contra 128 organizações em 42 países entre o fins de fevereiro e junho. Os Estados Unidos foram os alvos número um da Rússia. A Polónia, através da qual é transportada a maior parte da ajuda humanitária e militar internacional para a Ucrânia, foi também um alvo significativo durante este período. Os atores de ameaças afiliados ao Estado russo perseguiram organizações nos países bálticos e redes informáticas na Dinamarca, Noruega, Finlândia e Suécia em abril e também em maio.

Setores da indústria mais alvejados na Ucrânia desde a invasão



As organizações governamentais federais, estatais e locais na Ucrânia mantiveram-se como alvos prioritários para os grupos de ameaças do estado russo e afiliados da Rússia ao longo do conflito. O foco nas organizações do setor dos transportes, energia, finanças e meios de comunicação destaca o risco que estas operações cibernéticas representam para os serviços nos quais os cidadãos ucranianos confiam.

As táticas cibernéticas dos atores russos em tempo de guerra ameaçam a Ucrânia e não só

Continuação

Assistimos a um aumento da atividade semelhante cujo alvo são os ministérios dos negócios estrangeiros dos países da NATO.

Os grupos de ameaças do Estado russo mantiveram-se interessados em comprometer a infraestrutura crítica dentro e fora da Ucrânia no ano passado. O IRIDIUM implantou o malware Industroyer2 num esforço falhado para deixar milhões de pessoas na Ucrânia sem energia. Fora da Ucrânia, o BROMO realizou intrusões contra organizações envolvidas na indústria e sistemas de controlo industrial no início de 2022.

Os atores estatais russos e afiliados da Rússia dirigiram operações cibernéticas contra a Ucrânia, os seus aliados e outros alvos de valor de análise de informações este ano utilizando muitas das seguintes TTP:

Spear phishing com anexos ou hiperligações maliciosas

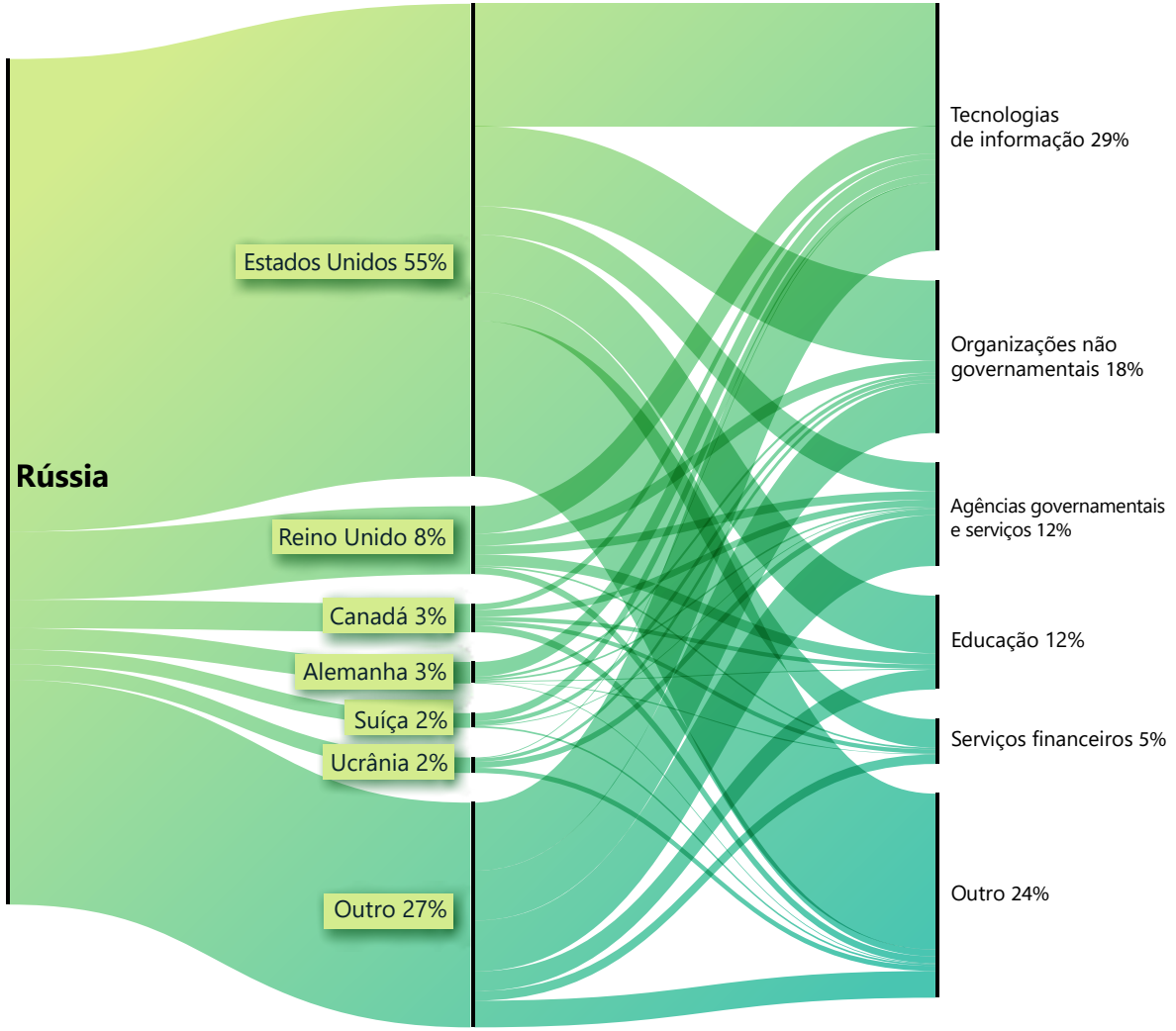
O Estado russo e os grupos afiliados da Rússia, como o ACTINIUM, o NOBELIUM, o STRONTIUM, o DEV-0257, o SEABORGIUM e o IRIDIUM, utilizaram campanhas de phishing para obterem acesso inicial às contas e redes desejadas nas organizações dentro e fora da Ucrânia. Muitas campanhas utilizaram contas comprometidas ou falsificadas em organizações alvo ou no mesmo setor e temas apelativos para atrair as vítimas. O NOBELIUM utilizou contas diplomáticas comprometidas para enviar e-mails de phishing disfarçados de comunicações diplomáticas a colaboradores do Ministério dos Negócios Estrangeiros em todo o mundo. O STRONTIUM criou contas falsificadas baseadas em nomes disponíveis publicamente dos titulares de contas em grupos de reflexão nos Estados Unidos e enviou mensagens de phishing para obter acesso a contas nesses grupos de reflexão. O SEABORGIUM utilizou o phishing com iscos relacionados com a elaboração de relatórios sobre o conflito na Ucrânia para obter acesso inicial às contas nos grupos de reflexão de assuntos internacionais nos países nórdicos.

Exploração da cadeia de fornecimento de serviços de TI para afetar os clientes a jusante

No final de 2021, os atores estatais russos comprometeram os fornecedores de serviços de TI e utilizaram o acesso para facilitar as deformações no website e a implementação do malware destruidor Whispergate pelo DEV-0586 em janeiro.[12] O DEV-0586 também comprometeu a rede de uma empresa de TI que criou sistemas de gestão de recursos para o Ministério da Defesa da Ucrânia e outras organizações nos setores das comunicações e dos transportes, indicando que o grupo estava a explorar também opções de ataque de terceiros nesses setores.

Em todo o mundo, mas sobretudo nos Estados Unidos e na Europa Ocidental, o NOBELIUM visava fornecedores de serviços de TI para obter acesso ao governo e a outras redes sensíveis durante 2021-2022 (consulte o debate sobre as vulnerabilidades da cadeia de fornecimento anteriormente neste capítulo).

Rússia: principais países visados e setores da indústria



Apesar de um foco intenso nas organizações baseadas na Ucrânia desde o início de 2022, as empresas sediadas na América do Norte e na Europa Ocidental ainda eram os principais clientes de serviço online que os atores russos tinham como alvo. A campanha do NOBELIUM contra o setor das TI transformou-o no setor mais alvejado no ano passado.

As táticas cibernéticas dos atores russos em tempo de guerra ameaçam a Ucrânia e não só

Continuação

Exploração de aplicações destinadas ao público para obter acesso inicial às redes

Desde, pelo menos, o final de 2021, o STRONTIUM trabalhou para desenvolver e refinar as suas capacidades para explorar serviços destinados ao público, como os servidores do Microsoft Exchange, para roubar informações. O STRONTIUM explorou servidores Exchange sem patches para aceder a contas do governo ucraniano, bem como a organizações militares e de defesa nos Estados Unidos, no Líbano, no Peru e na Roménia, e noutros organismos da administração pública sediados na Arménia, Bósnia, Kosovo e Malásia. O DEV-0586, também afiliada das forças armadas russas, explorou as vulnerabilidades do servidor Confluence para obter acesso inicial a organizações governamentais e do setor das TI na Ucrânia e noutros países da Europa Oriental.

O estado russo e os atores de ameaças afiliados utilizam muitas das mesmas TTP para comprometerem as organizações de interesse durante os períodos de guerra e paz.

Utilização de contas e protocolos administrativos, e utilidades nativas para a deteção de rede e o movimento lateral

Depois de obter acesso inicial a uma rede, a Microsoft observou atores estatais russos a aproveitarem as contas legítimas e os utilitários de software utilizados para executar tarefas de manutenção básica para evitar a sua deteção durante o máximo de tempo possível. Contavam com identidades comprometidas com capacidades administrativas e protocolos, ferramentas e métodos de administração válidos para se moverem lateralmente dentro das redes sem atrair imediatamente a atenção dos monitores automatizados e dos defensores de rede.

A higiene cibernética básica e o emprego da deteção de endpoints e das ferramentas de resposta podem ajudar a mitigar o impacto negativo destes tipos de operações em tempo de paz, bem como durante os períodos de guerra.

A imprevisibilidade do conflito contínuo exige que as organizações em todo o mundo tomem medidas para fortalecer a cibersegurança contra as ameaças digitais resultantes dos atores de ameaça ligados ao Estado russo e à Rússia.

Insights acionáveis

1. Minimize o roubo de credenciais e o abuso de contas ao proteger as identidades dos seus utilizadores através da implementação de ferramentas de proteção de identidades MFA e da imposição de acesso com menos privilégios para proteger as contas e sistemas mais sensíveis e privilegiados.
2. Aplique atualizações para assegurar que todos os seus sistemas obtêm o mais alto nível de proteção o mais rapidamente possível e que se mantêm atualizados.
3. Implemente soluções antimalware, deteção de endpoints e proteção de identidades em toda a sua organização. Uma combinação de soluções de segurança de defesa aprofundadas, combinadas com pessoal formado e capaz, pode capacitar a sua organização para identificar, detetar e evitar intrusões que afetam o seu negócio.
4. Ative as investigações e a recuperação no caso de detetar ou receber notificações de uma ameaça ao seu ambiente ao fazer a cópia de segurança dos sistemas críticos e ao permitir o registo. É altamente recomendado o estabelecimento de um plano de resposta a incidentes.

Ligações para mais informações

- Defender a Ucrânia: As Primeiras Lições da Ciberguerra | Microsoft On the Issues
- A guerra híbrida na Ucrânia | Microsoft On the Issues
- Atividade de ciberameaças na Ucrânia: análise e recursos | Centro de Resposta de Segurança da Microsoft (MSRC)
- Interromper ataques cibernéticos direcionados à Ucrânia | Microsoft On the Issues
- Ataques de malware direcionados ao governo da Ucrânia | Microsoft On the Issues
- MagicWeb: o truque pós-comprometimento do NOBELIUM para se autenticar como qualquer pessoa | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Equipa de Deteção e Resposta (DART), Equipa de Investigação do Microsoft 365 Defender

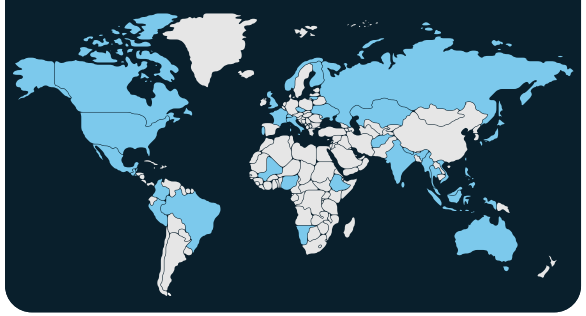
A China expande os objetivos globais para obter uma vantagem competitiva

No atual clima geopolítico complexo, os atores de ameaças estatais chineses e afiliados da China que conduzem operações cibernéticas, têm muitas vezes como objetivo promover os objetivos estratégicos militares, económicos e das relações externas do país, como parte do objetivo da China de obter uma vantagem competitiva. No ano passado, a Microsoft observou uma ampla atividade de ameaças chinesas dirigidas aos países em todo o mundo.

Desde meados de 2021, a China tem vindo a criar manobras para garantir a estabilidade económica e financeira entre o pior surto de COVID-19 em dois anos.[13] A China continuou a conciliar a sua posição em eventos geopolíticos, como a luta para equilibrar a sua parceria "ilimitada" com a Rússia,[14] e manter a sua posição no cenário mundial.[15] Além disso, a posição da China em relação aos Estados Unidos e aos seus aliados sobre Taiwan[16] e ao mar da China Meridional continuou a pôr em causa as relações exteriores com muitos países.[17]

Os grupos de ameaças estatais chineses e afiliados da China aumentaram o alvejamento em nações mais pequenas em todo o mundo com um foco maior no Sudeste Asiático para obter uma vantagem competitiva em todas as frentes.

Países visados pelo estado chinês e grupos chineses afiliados

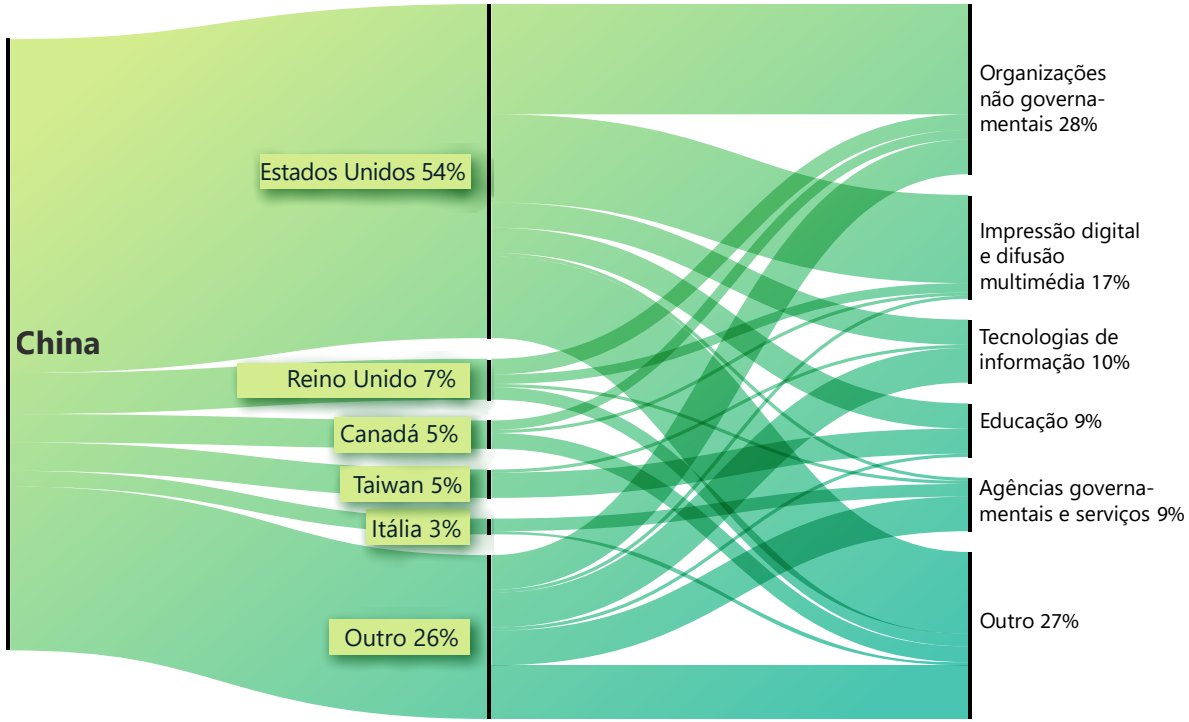


A China também continuou a expandir a sua influência económica globalmente através de iniciativas anteriormente estabelecidas na Nova Rota da Seda (BRI), tentando reavivar um quadro de investimento abrangente com a UE,[18] e negociando um novo acordo comercial regional com 15 países na região da Ásia-Pacífico conhecida como a Parceria Económica Regional Abrangente.[19] A Microsoft avalia que a China vai continuar a utilizar a recolha cibernética como uma ferramenta para ajudar a promover os seus objetivos estratégicos políticos, militares e económicos devido às operações cibernéticas observadas e à amplitude de entidades alvejadas.

Alvejamento cibernético suscetível de promover os interesses económicos e militares.

A Microsoft observou o alvejamento generalizado em nações mais pequenas em todo o mundo por grupos de ameaças estatais chineses e afiliados da China, sugerindo que está provavelmente a utilizar a espionagem cibernética como um componente da sua influência económica e militar global.

China: principais países alvos e setores da indústria



Os setores dos grupos de reflexão/ONG, meios de comunicação, TI, governo e da educação estavam entre os setores mais alvejados para grupos de ameaças baseados na China, provavelmente para a recolha e o reconhecimento de informações persistentes.

O intervalo de alvos incluía, mas não se limitava a, países na África, no Caribe, no Médio Oriente, Oceania e sul da Ásia, com foco particular naqueles países no sudeste asiático e nas ilhas do Pacífico.

De acordo com a estratégia de BRI da China, os grupos de ameaças baseados na China visaram entidades no Afeganistão, Cazaquistão, Maurícias, Namíbia e Trinidad e Tobago.[20] Por exemplo, Trinidad e Tobago foi o primeiro país caribenho a endossar a estratégia de BRI da China em 2018, e a China considera-o um parceiro importante na região. O NÍQUEL tem tido operações de rede persistentes dirigidas a Trinidad e TobAgo desde 2021. Por exemplo, em março de 2022, o NÍQUEL conduziu atividades de reconhecimento dirigidas a uma agência governamental, provavelmente para fins de recolha de informações.

A China expande os objetivos globais para obter uma vantagem competitiva

Continuação

Entretanto, a Microsoft observou grupos de ameaças do estado chinês e afiliados da China que concentram as suas operações de rede contra entidades no sudeste asiático e a expansão para países das Ilhas do Pacífico à medida que a China deslocou as suas prioridades militares e económicas para enfrentar os desafios do interesse renovado dos Estados Unidos na região. Em janeiro de 2022, a Microsoft observou que o RÁDIO visava uma empresa de energia e um órgão governamental associado à energia no Vietname, e uma agência governamental da Indonésia. As atividades do RÁDIO estavam provavelmente alinhadas com os objetivos estratégicos da China no mar da China Meridional.[21] No final de fevereiro e início de março, o GÁLIO comprometeu mais de 100 contas afiliadas a uma organização intergovernamental de destaque (IGO) na região do Sudeste Asiático. O tempo de alvejamento da IGO na região pelo GÁLIO coincidiu com o anúncio de uma reunião agendada entre os Estados Unidos e os líderes regionais. Os atores do GÁLIO ficaram provavelmente encarregados de monitorizar as comunicações e recolher informações antes do evento.

À medida que a China expandiu a sua influência nos países das ilhas do Pacífico, seguiram-se as atividades dos grupos de ameaças chineses. Em abril, a China e as Ilhas Salomão assinaram um contrato de segurança com o objetivo de "promover a paz e a segurança". O acordo permite potencialmente que a China implemente a polícia armada e militares nas Ilhas Salomão.[22] Em maio, a China organizou o segundo encontro de Ministros dos Negócios Estrangeiros dos países das ilhas da China-Pacífico (PIC) nas Fiji e propôs avançar com uma "parceria estratégica abrangente" para promover os interesses políticos, culturais, sociais, de segurança e de mudança climática, e também para combater a pandemia.[23] Por volta da mesma altura, em maio, a Microsoft identificou o malware do GADOLÍNIO nos sistemas governamentais das Ilhas Salomão. O RÁDIO também executou código malicioso nos sistemas de uma empresa de telecomunicações na Papua-Nova Guiné. Concluímos que estas atividades eram prováveis para fins de recolha de informações para suportar a estratégia regional global da China.

A Microsoft interrompe as operações do NíQUEL, mas o grupo de ameaças mostra a sua persistência.

Em dezembro de 2021, a Unidade de Crimes Digitais da Microsoft (DCU) apresentou alegações com o Tribunal Distrital dos EUA para o Distrito Leste da Virgínia que procuram autoridade para apreender 42 domínios de comando e controlo (C2) controlados pelo NÍQUEL. Estes domínios de C2 foram utilizados nas operações contra governos, entidades diplomáticas e ONG na América Central e do Sul, Caribe, Europa e América do Norte desde setembro de 2019.[24] Através destas operações, o NÍQUEL obteve acesso a longo prazo a várias entidades e extraiu consistentemente os dados de algumas vítimas desde o final de 2019.

À medida que a China continua a estabelecer relações económicas bilaterais com mais países, muitas vezes em acordos associados com o BRI, a influência global da China vai continuar a crescer. Avaliámos que os atores de ameaças do estado chinês e afiliados da China vão perseguir os alvos nos seus setores governamental, diplomático e de ONG para obter novos insights, provavelmente em busca de espionagem económica ou objetivos tradicionais de recolha de informações. Desde a disrupção da Microsoft, o NÍQUEL tem como alvo várias agências governamentais, provavelmente a tentar recuperar o acesso perdido. Entre o final de março e maio de 2022, o NÍQUEL voltou a comprometer pelo menos cinco agências governamentais em todo o mundo. Isto sugere que o grupo tinha pontos de entrada adicionais para essas entidades ou recuperou o acesso através de novos domínios C2. A persistência do NÍQUEL em comprometer repetidamente os mesmos organismos públicos globalmente indica a importância da tarefa a um nível elevado.

A China está a ser mais assertiva no seu posicionamento na política externa. Concluímos que a espionagem económica e a recolha de informações cibernéticas irão, provavelmente, continuar.

Insights acionáveis

1. Impulsione a defesa cibernética para mitigar proativamente as ciberameaças. A persistência dos atores de ameaças chineses exige que as organizações identifiquem, protejam, detetem e respondam atempadamente a possíveis intrusões.
2. Utilização abusiva por parte dos atores de ameaças de tarefas agendadas[25] como um método comum de persistência e evasão de defesa. Certifique-se de que o seu ambiente aplica as diretrizes de segurança adicionais para se proteger contra esta técnica comumente utilizada.[26]
3. Continuamos a observar a utilização de shells Web como um vetor inicial em redes alvejadas.[27] As organizações devem fortalecer os seus sistemas contra ataques de shells Web que podem fornecer aos atacantes acesso para executar comandos remotos.[28]

Ligações para mais informações

- NÍQUEL visa organizações governamentais em toda a América Latina e Europa | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft (DSU)
- Proteger as pessoas dos ataques cibernéticos recentes | Microsoft On the Issues

O Irão torna-se cada vez mais agressivo após a transição de energia

A Microsoft observou que os grupos estatais iranianos e os atores afiliados aumentam o ritmo e o âmbito dos ciberataques contra Israel, expandem os ataques de ransomware além dos adversários regionais para as vítimas dos EUA e da UE, e visam uma infraestrutura crítica dos EUA para, pelo menos, se posicionar previamente para potenciais ataques cibernéticos destrutivos.

A crescente agressão cibernética dos atores estatais iranianos acompanhou uma transição do seu poder presidencial. No Verão de 2021, o inflexível Presidente Ibrahim Raisi substituiu o moderado Presidente Hassan Rouhani. Em nítido contraste com Raisi, que é um protegido do Líder Supremo e um aliado próximo da Corporação de Guarda Revolucionária Islâmica (IRGC), a propensão do ex-presidente Rouhani para a diplomacia levou, muitas vezes, a desacordo com o líder supremo e os líderes seniores do IRGC.[29] As visões de falcão da administração Raisi parecem ter suscitado a vontade dos atores iranianos de tomar medidas mais ousadas contra Israel e o Ocidente, em particular os Estados Unidos, apesar da retoma da interação diplomática para reviver o acordo nuclear com o Irão.

Aumento do ritmo e do âmbito dos ciberataques iranianos contra Israel

Algumas semanas após Raisi concluir a formação da sua equipa de política externa,[30] os atores do estado iraniano retomaram os ciberataques destrutivos contra Israel a um ritmo mais rápido do que no ano anterior. Estes ataques de ransomware e de fugas de informações foram realizados de poucas em poucas semanas, a partir de setembro, e envolveram pelo menos três atores afiliados ao Irão, sugerindo que os ataques poderiam ter feito parte de uma campanha nacional de retaliação contra Israel. Em pelo menos um caso, a Microsoft avaliou um ataque de ransomware contra uma organização israelita no final de 2021 que foi concebido para ocultar um ataque de eliminação de dados subjacente. A análise de malware da Microsoft determinou que o ransomware entregue à vítima estava programado para executar malware limpador de dados após a encriptação.

Em 2022, os ciberataques iranianos aumentaram na seleção de alvos e na forma de ataques. Em fevereiro, o DEV-0198 tentou conduzir um ataque destrutivo contra a infraestrutura crítica israelita. A Microsoft também avalia que um ator afiliado do Irão foi provavelmente responsável por um ciberataque sofisticado que disparou sirenes de foguetes de emergência em Israel em junho, provavelmente utilizando software que ajusta o áudio sobre as redes IP.

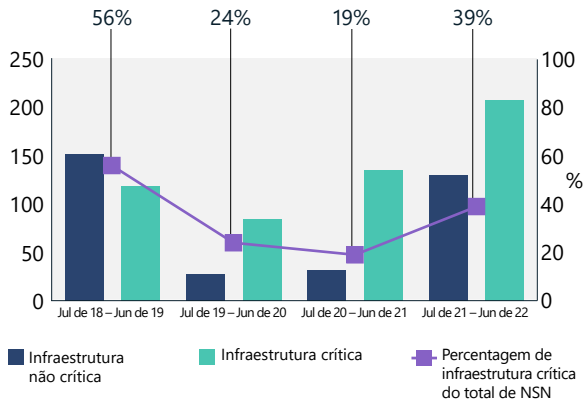
Ameaça iraniana a infraestrutura crítica americana e israelita montada ao longo do ano

Os atores estatais iranianos que a Microsoft avalia são afiliados com da IRGC (FÓSFORO e DEV-0198) alvos de alto perfil da infraestrutura crítica dos EUA e de Israel, desde o final de 2021 até meados de 2022. O objetivo provável era fornecer a Teerão opções para retaliar contra os mesmos setores que os altos funcionários da IRGC culparam os Estados Unidos e Israel pela disrupção do Irão.[31] Concluímos que esta atividade está vinculada às declarações no final de outubro de 2021 pelo General da IRGC Gholamreza Jalali, diretor da Organização de Defesa Passiva do Irão, que repetiu as acusações de outras figuras influentes no regime de que os Estados Unidos e Israel conduziram ataques cibernéticos aos portos, ferrovias e estações de abastecimento do Irão.[32] Jalali entregou esta acusação uma segunda vez em comentários preparados durante um discurso de oração de sexta-feira encenado num pódio com a imagem de um míssil a atingir as palavras "EUA", sugerindo que os seus seniores tinham a mesma vista.[33]

O FÓSFOR começou a verificação generalizada das organizações dos EUA em outubro de 2021 para vulnerabilidades sem correções do Fortinet e do ProxyShell. Uma vez comprometidos, estes sistemas não corrigidos foram utilizados para executar ataques de ransomware, em vários casos contra a infraestrutura crítica nos Estados Unidos e noutras nações ocidentais. Estes marcaram os primeiros casos confirmados de ataques de ransomware de Estados iranianos afiliados fora do Médio Oriente. Após o ciberataque contra os postos de abastecimento do Irão no final de outubro, a Microsoft observou um aumento nos ataques de ransomware iranianos contra empresas dos EUA, o que sugere uma possível correlação.

Ao mesmo tempo, o FÓSFORO mudou para o alvejamento direcionado, muitas vezes através de spear phishing, de empresas de infraestrutura crítica dos de alto nível dos EUA, incluindo grandes portos marítimos e aeroportos de entrada, sistemas de trânsito, empresas de serviços públicos e empresas de petróleo e gás. Este alvejamento, muitas vezes conduzida via spear phishing, durou até meados de 2022. Os alvos alinham diretamente com os setores que Teerão culpou os Estados Unidos e Israel por atacarem no Irão, e provavelmente forneceu ao Irão opções de retaliação. O compromisso de alvos próximos praticamente idênticos iria fornecer uma oportunidade para deter tais ataques futuros, ao mesmo tempo que procurava evitar o agravamento ao sinalizar a causa dos ataques sem admitir a culpa.

Ressurgimento do alvejamento da infraestrutura iraniana



Os objetivos iranianos de infraestruturas críticas aumentou para os níveis mais elevados observados desde o final de 2018 até ao início de 2019. Utilizámos a Diretiva 21 de Políticas Presidenciais dos EUA (PPD-21) para determinar se uma empresa se ajusta aos critérios de infraestrutura crítica. (julho de 2021 – junho de 2022).

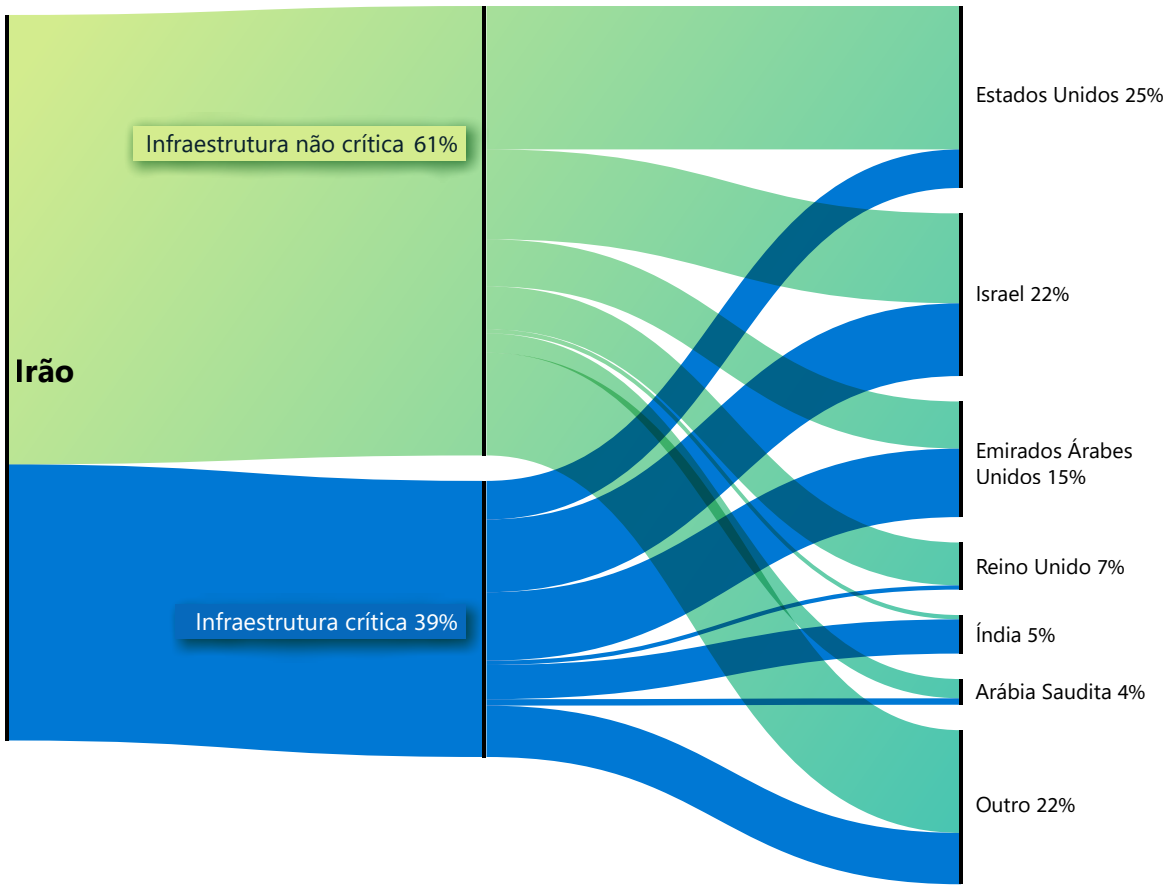
O Irão torna-se cada vez mais agressivo após a transição de energia

Continuação

Em Israel, o DEV-0198 alvejou ferrovias, empresas de logística, fornecedores de software de empresas de logística e empresas de combustível israelitas com foco nos postos de gasolina. No início de 2022, o grupo conduziu um ataque disruptivo à rede de uma grande empresa de logística israelita, o que forçou a empresa a encerrar os seus computadores e algumas das suas operações para deter o ataque. Noutro caso, observámos o grupo a tentar aceder à rede de um importante fornecedor de transporte israelita através de credenciais roubadas ou reutilizadas. Enquanto isso, outro ator iraniano, o DEV-0343, cujo alvo é o setor de defesa, de transportes marítimos e empresas de imagens de satélite sugere ligações com a IRGC, contas comprometidas em transportes israelitas e entidades relacionadas com portos no início de 2021.

É provável que os grupos de ameaças iranianos continuem a ser uma ameaça para as empresas de transporte e energia dos EUA e israelitas, particularmente porque os esforços diplomáticos para reavivar o acordo nuclear iraniano diminuem e Washington, Tel Aviv, e Teerão procuram meios coercivos alternativos para alavancar as concessões.

Objetivos iranianos de infraestruturas críticas por país



O alvejamento iraniano de infraestruturas críticas ocorreu de forma mais proeminente contra organizações israelitas, dos Emirados e dos Estados Unidos.

É provável que os atores iranianos continuem a ameaçar as empresas de transporte e energia dos EUA e de Israel no próximo ano.

Os grupos iranianos expandiram os ataques de ransomware para além dos adversários regionais e estão a visar alvos de infraestrutura críticos nos EUA e em Israel.

Insights acionáveis

1. Melhore a higiene cibernética global da sua organização, permitindo soluções sem palavra-passe, como a MFA, e impondo a sua utilização para toda a conectividade remota para mitigar quaisquer credenciais potencialmente comprometidas.
2. Avalie a autenticidade de todo o tráfego de e-mails de entrada para assegurar que o endereço do remetente é legítimo.
3. Aplique correções com antecedência e frequentemente.[34]
4. Analise e audite cada uma das suas relações de parceria com fornecedores de serviços para minimizar quaisquer permissões desnecessárias entre a sua organização e os fornecedores a montante. A Microsoft recomenda a remoção imediata do acesso a quaisquer relações de parceria que não pareçam familiares ou que ainda não tenham sido auditadas.[35]

Ligações para mais informações

- Os objetivos iraniano no setor de TI em crescimento | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft (DSU)
- DEV-0343 ligado ao Irão que visa a defesa, o GIS e os setores marítimos | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft (DSU)

Grupo baseado no Líbano com ligações ao Irão a alvejar Israel

A Microsoft monitoriza as atividades de ciberameaças independentemente da plataforma, vítima alvejada ou região geográfica. Mantemos a visibilidade e a caça às ameaças ativas em todo o mundo para redigir melhores deteções para os nossos clientes.

Apesar de as ameaças da Rússia, da China, do Irão e da Coreia do Norte representarem a maioria da nossa atividade observada dos atores de Estados-nação, também monitorizamos e comunicamos as ameaças de países membros da NATO e de nações democráticas. No ano passado, destacámos a atividade de um ator baseado na Turquia (SILICON) e de um ator baseado no Vietname (BISMUTH). Este ano, estamos a expandir os detalhes de um grupo baseado no Líbano que divulgámos antes publicamente.[36]

A Microsoft descobriu um grupo com base no Líbano, que não tinha sido documentado anteriormente e avaliámos com confiança moderada que operava em coordenação com atores afiliados do Ministério da Inteligência e Segurança do Irão (MOIS). Tal colaboração ou direção de Teerão estariam alinhadas com as revelações desde o final de 2020, de que o governo do Irão está a utilizar terceiros para efetuar operações cibernéticas, provavelmente para melhorar a negação plausível do Irão.

Na atividade observada, o POLÓNIO alvejou ou comprometeu duas dúzias de organizações baseadas em Israel e uma IGO com operações no Líbano entre fevereiro e maio de 2022, antes de a Microsoft interromper e revelar publicamente a sua atividade.

Quase metade das organizações israelitas fazia parte da indústria de defesa de Israel ou tinha ligações a empresas de defesa israelitas, indicando que o grupo tem um conjunto interesses semelhante ao Irão na recolha de informações e/ou diretamente contra Israel.[37]

As ligações avaliadas do POLÓNIO aos grupos MOIS baseiam-se nas sobreposições observadas de vítimas e na convergência de ferramentas e técnicas.

- Sobreposição de vítimas: um grupo estatal iraniano ligado ao MOIS do Irão, que a Microsoft rastreou como MERCÚRIO, comprometeu anteriormente várias vítimas do POLÓNIO, indicando uma convergência dos requisitos de missão ou uma possível "transferência" das vitimas entre grupos.
- Ferramentas e técnicas comuns: semelhante ao POLÓNIO, o MSTIC observou o DEV-0588 (também conhecida como CopyKittens) que utiliza normalmente a AirVPN para operações e o DEV-0133 (também conhecida como Lyceum[38]) a utilizar o OneDrive para C2 e extração de dados. Semelhante aos atores estatais iranianos, o POLÓNIO utilizou um fornecedor de serviços de cloud para comprometer uma empresa de aviação israelita e uma empresa de advogados.[39]

O POLÓNIO implementou uma série de implantes personalizados utilizando serviços de cloud para C2 e extração de dados, nomeadamente o OneDrive e a DropBox. O POLÓNIO criava frequentemente aplicações exclusivas do OneDrive para os alvos, provavelmente para evitar a deteção.

A partir de junho de 2022, a Microsoft suspendeu mais de 20 aplicações do OneDrive criadas pelo POLONIUM, notificou as organizações afetadas e implementou uma série de atualizações de inteligência de segurança para colocar em quarentena as ferramentas desenvolvidas pelo POLONIUM.

A Microsoft detetou e desabilitou com êxito o abuso de POLÓNIO do OneDrive como um C2.

Insights acionáveis

1. Atualize as ferramentas de antivírus[40] e certifique-se de que a proteção da cloud[41] está ativada para detetar os indicadores relacionados.
2. Para os clientes com relações com fornecedores de serviços, certifique-se que analisa e audita todas as relações de parcerias para minimizar as permissões desnecessárias entre a sua organização e os fornecedores.[42] Remova imediatamente o acesso a quaisquer relações de parceria que pareçam não familiares ou que não tenham sido auditadas.

Ligações para mais informações

- Expor a atividade e a infraestrutura do POLÓNIO dirigidas às organizações israelitas | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft (DSU)
- MERCÚRIO a aproveitar vulnerabilidades Log4j 2 em sistemas não corrigidos para visar organizações israelitas | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Equipa de Investigação do Microsoft 365 Defender, Informações sobre Ameaças do Microsoft Defender

Recursos cibernéticos da Coreia do Norte utilizados para alcançar os três principais objetivos do regime

As prioridades cibernéticas da Coreia do Norte ao longo do último passado refletiam as prioridades globais declaradas pelo governo. Kim Jong Un sublinhou as três prioridades da capacidade de criação de defesa, reforçando a economia em dificuldades do país e garantindo a estabilidade doméstica em vários endereços chave.[43] As ações tomadas pelos atores estatais norte-coreanos mostram claramente que o cibernética está a ser utilizada para alcançar estes três objetivos.

Os atores estatais da Coreia do Norte utilizaram várias táticas para tentarem penetrar as empresas aeroespaciais em todo o mundo.

Os grupos de ameaças do estado norte-coreano, principalmente o CÉRIO e o ZINCO, utilizaram uma variedade de táticas para tentarem penetrar nas redes de empresas de defesa e aeroespaciais em todo o mundo. À medida que a Coreia do Norte embarcou no seu período mais agressivo de testes de mísseis no primeiro semestre de 2022, utilizou a espionagem cibernética para ajudar os investigadores norte-coreanos a ganharem uma vantagem no desenvolvimento de sistemas de defesa indígena e contramedidas para os avanços que os seus adversários tinham alcançado.

Observámos o COPERNÍCIO a visar uma variedade de empresas relacionadas com criptomoedas em todo o mundo, muitas vezes com sucesso, para ajudar a suportar a economia em dificuldades da Coreia do Norte. Apesar de não podermos confirmar se o grupo conseguiu extrair dinheiro após o comprometimento, observámos que o COPERNÍCIO infeta dezenas de máquinas ao enviar documentos maliciosos disfarçados de propostas de outras empresas de criptomoedas.

Finalmente, um grupo que a Microsoft monitoriza como DEV-0215 trabalhou para manter a estabilidade e a lealdade na Coreia do Norte, ao visar as organizações de notícias que reportam os problemas da Coreia do Norte. Estes estabelecimentos têm origens na Coreia do Norte e nas comunidades de desertores, com Pyongyang a ser vista como uma ameaça existencial. Além disso, o grupo trabalhou para obter acesso a redes de grupos cristãos de língua coreana, que tendem a ser francos no seu posicionamento contra a Coreia do Norte e a trabalhar ativamente com desertores norte-coreanos.

Alvejamento das empresas de defesa e aeroespaciais

Os atores estatais norte-coreanos liderados pelo CERIUM e o ZINC fizeram significativos esforços no desenvolvimento de táticas que visam penetrar nas empresas de defesa e aeroespaciais. O CÉRIO sondou repetidamente redes privadas virtuais (VPN) sul-coreanas ao fazer download dos clientes e procurar fraquezas. Também fez download de aplicações comuns utilizadas por clientes militares e governamentais da Coreia do Sul, provavelmente à procura de vulnerabilidades. O grupo acompanhou de perto os eventos atuais e escreveu novos documentos de engodo que utilizaram tópicos de alto perfil como isco para encorajar os alvos a clicarem nas suas ligações e executáveis de malware.

Tanto o ZINCO como o CÉRIO utilizaram as redes sociais e a engenharia social nas suas campanhas. O ZINCO foi particularmente adepto da criação de perfis falsos no LinkedIn e noutros sites de redes sociais profissionais, onde os seus operadores representavam recrutadores para as principais empresas de defesa e aeroespaciais. Utilizando estes perfis, enviavam ligações ou anexos de ficheiros maliciosos para as potenciais vítimas através de mensagens diretas nas redes sociais ou no e-mail.

Além dos colaboradores das empresas, o CÉRIO também se interessou amplamente por membros das forças armadas da Coreia do Sul, demonstrando especial interesse nas academias militares da Coreia do Sul e militares que trabalham no setor académico.

Alvejamento de criptomoedas para equilibrar as perdas

Dado que as sanções da ONU foram cobradas em 2016, a economia da Coreia do Norte continuou a contrair-se, agravada por catástrofes naturais, como inundações[44] e a seca[45], bem como um bloqueio quase total das fronteiras às importações desde o início da pandemia da COVID-19 no início de 2020.[46] Apesar de a Coreia do Norte abrir brevemente as suas fronteiras ao comércio com a China no início de 2022, foram logo fechadas novamente.[47] Em meados de maio, a Coreia do Norte comunicou o seu primeiro caso doméstico de COVID-19.[48] Desde então, aplicou uma estratégia de "COVID zero" ao estilo da China, com confinamentos em massa para combater o vírus que tinha impactado negativamente a já frágil economia da Coreia do Norte.

O grupo estatal da Coreia do Norte COPERNÍCIO tentou compensar algumas das receitas perdidas ao roubar dinheiro, normalmente sob a forma de criptomoedas, a partir de qualquer empresa cujas redes pudessem penetrar. Vimos dezenas de máquinas comprometidas que pertenciam a empresas relacionadas com criptomoedas nos Estados Unidos, no Canadá, na Europa e em toda a Ásia. O COPERNÍCIO até comprometeu máquinas pertencentes a empresas relacionadas com criptomoedas no mais forte aliado da Coreia do Norte, a China, tanto no continente como em Hong Kong. O grupo baseou-se fortemente nas redes sociais para obter os seus primeiros reconhecimentos e abordagens aos alvos. Os atores criam perfis em que fingem ser programadores ou oficiais seniores em empresas relacionadas com criptomoedas. Em seguida, estabeleceriam relações com as pessoas no setor, enviando ligações ou ficheiros maliciosos depois de terem criado empatia.

Recursos cibernéticos da Coreia do Norte utilizados para alcançar os três principais objetivos do regime

Continuação

Um grupo relacionado com o PLUTONIUM desenvolve e implementa ransomware

Um grupo de atores com origem na Coreia do Norte que a Microsoft monitoriza como DEV-0530 começou a desenvolver e utilizar o ransomware em ataques em junho de 2021. Este grupo, que se chamava H0lyGh0st, utilizou uma carga de ransomware com o mesmo nome para as suas campanhas e comprometeu com sucesso as pequenas empresas em vários países, no início de setembro de 2021.

A Microsoft concluiu que o DEV-0530 tinha ligações a outro grupo baseado na Coreia do Norte, monitorizado como PLUTÓNIO (também conhecido como DarkSeoul ou Andariel). Apesar de a utilização do ransomware H0lyGh0st em campanhas ser exclusiva do DEV-0530, o MSTIC observou as comunicações entre os dois grupos, bem como do DEV-0530, através de ferramentas criadas exclusivamente pelo PLUTÓNIO.

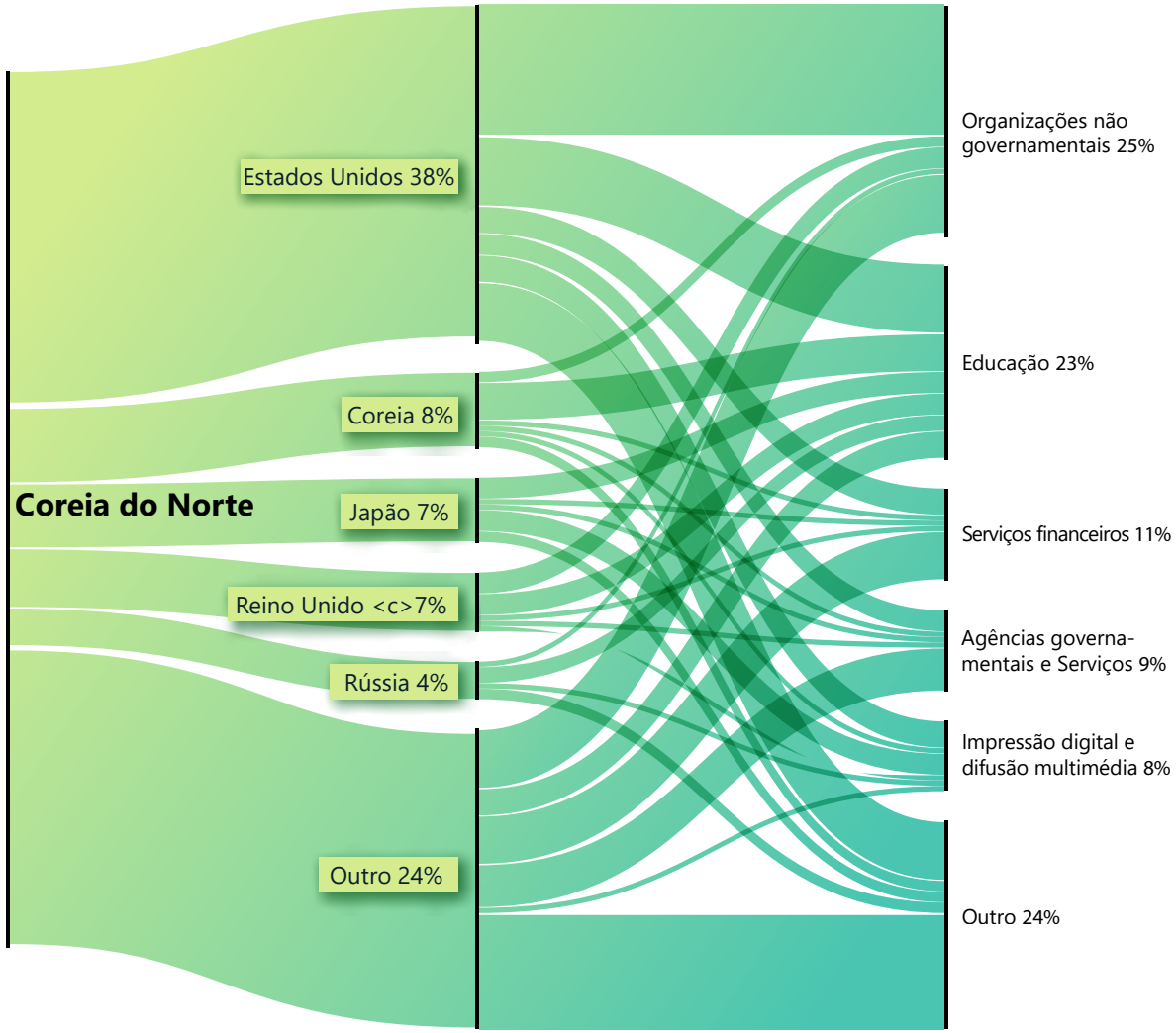
Não é certo que a atividade do DEV-0530 fosse patrocinada pelo governo. Apesar de os ataques de ransomware poderem ter sido ordenados pelo governo pelo mesmo motivo que patrocina o roubo de empresas de criptomoedas, também é possível que os atores por detrás do DEV-0530 atuavam de forma independente para ganharem dinheiro. Se fossem os hackers norte-coreanos a operar de forma independente, isso explicaria por que motivo a atividade não era generalizada em comparação com as operações de roubo patrocinadas pelo governo contra empresas de criptomoedas.

Alvejamento dos estabelecimentos noticiosos, desertores, grupos religiosos e organizações de ajuda da Coreia do Norte

No ano passado, o Líder Supremo Kim Jong Un estava publicamente mais focado na segurança interna e na lealdade do que nos mísseis e nas armas nucleares. Refletindo esta preocupação com questões internas, pelo menos dois grupos estatais da Coreia do Norte centraram-se nos aspetos que o regime considera ameaças domésticas.

O primeiro foi um grupo que a Microsoft monitoriza como DEV-0215, que visa organizações de meios de comunicação que acompanham de perto as notícias da Coreia do Norte. Uma razão provável para este alvejamento é que estas empresas de meios de comunicação obtêm as suas notícias de desertores norte-coreanos, cidadãos chineses que trabalham em estreita colaboração com a Coreia do Norte e até alguns cidadãos norte-coreanos baseados no interior do país, utilizando uma variedade de métodos para comunicar com o mundo exterior. O governo norte-coreano encara estes grupos como uma ameaça existencial à sua sobrevivência, particularmente os cidadãos na Coreia do Norte que seriam vistos como traidores e espiões. É provável que o DEV-0215 procurou identificar as fontes destes estabelecimentos para poderem neutralizar as potenciais fugas de informações.

Coreia do Norte: Principais países e setores da indústria visados



A Coreia do Norte vê os Estados Unidos, a Coreia do Sul e o Japão como os seus principais inimigos. Apesar de a Rússia ser aliada há muito tempo, os atores de ameaças da Coreia do Norte têm como alvo os grupos de reflexão russos, os académicos e os funcionários diplomáticos para obterem informações dos pontos de vista russos sobre assuntos globais.

Recursos cibernéticos da Coreia do Norte utilizados para alcançar os três principais objetivos do regime

Continuação

A Microsoft também viu indícios do DEV-0215 a visar comunidades cristãs de língua coreana. As igrejas cristãs coreanas evangélicas tendem a ser críticas da Coreia do Norte e dos governos sul-coreanos que favorecem a interação com a Coreia do Norte. É provável que estas Igrejas realizem atividades de sensibilização para os desertores e que alguns se envolvam em trabalho humanitário com a Coreia do Norte. A Coreia do Norte vê-os como uma ameaça porque, enquanto o fluxo de desertores provenientes da Coreia do Norte quase que parou durante a pandemia,[49] estes grupos cristãos desempenham muitas vezes um papel fundamental para ajudar os desertores a escaparem. O DEV-0215 gerou documentos falsos sobre conferências cristãs para oradores coreanos como engodos para direcionar o grupo e descobrir quem está a ajudar a organizar as deserções.

Finalmente, o grupo estatal ÓSMIO demonstrou um interesse constante nas organizações de ajuda internacional ao longo do ano, incluindo as organizações que ajudaram a Coreia do Norte no passado. Enquanto a Coreia do Norte tem geralmente evitado ofertas de ajuda externa, especialmente desde o surto de COVID-19,[50] é possível que esteja a considerar aceitar essa ajuda, mas é necessário estar atento às ramificações de segurança de permitir a ajuda de trabalhadores estrangeiros no país. A Coreia do Norte pode estar a penetrar nas redes de organizações de ajuda em todo o mundo para determinar se permite tal ajuda no seu próprio país.

Insights acionáveis

1. Os atores estatais da Coreia do Norte são habilidosos, implacáveis e criativos, mas as organizações podem defender-se contra eles.
2. A maioria dos ataques bem-sucedidos pode ser interrompida com a higiene cibernética básica, como a autenticação de dois fatores ou não abrindo anexos de indivíduos desconhecidos num ambiente virtual.

Ligações para mais informações

- Ator de ameaças norte-coreano visa pequenas e médias empresas com ransomware H0lyGh0st | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Unidade de Segurança Digital da Microsoft (DSU)

Entre os especialistas da Coreia do Norte, há muito que se debate sobre se o governo norte-coreano está a ser sincero nas suas declarações públicas ou se adotou apenas essa postura para o efeito. O alinhamento dos ciberataques com as prioridades anunciadas da Coreia do Norte valida a convicção de que a Coreia do Norte está a ser explícita quando fala publicamente sobre os seus objetivos.

Os mercenários cibernéticos ameaçam a estabilidade do ciberespaço

Existe um setor cada vez maior de empresas privadas que desenvolvem e vendem ferramentas, técnicas e serviços que permitem aos seus clientes, muitas vezes governos, invadir redes, computadores, telemóveis e dispositivos ligados à Internet. Uma vantagem para os atores dos Estados-nação, estas entidades põem muitas vezes em perigo os dissidentes, os defensores dos direitos humanos, os jornalistas, os defensores da sociedade civil e outros cidadãos privados. Referimo-nos a estes como mercenários cibernéticos ou atores ofensivos do setor privado.

Um mundo em que as empresas do setor privado criam e vendem armas virtuais é mais perigoso para os consumidores, empresas de todas as dimensões e governos. Estas ferramentas ofensivas podem ser utilizadas de formas incompatíveis com as normas e os valores da boa governação e da democracia. A Microsoft acredita que a proteção dos direitos humanos é uma obrigação fundamental e que levamos a sério ao restringir a "vigilância como serviço" em todo o mundo.

A Microsoft avaliou alguns atores estatais em regimes democráticos e autoritários a externalizarem o desenvolvimento ou a utilização da tecnologia "vigilância como serviço". É assim que evitam a responsabilização e a supervisão, bem como adquirem capacidades que seriam difíceis de desenvolver de forma nativa.

> Estas armas cibernéticas fornecem aos Estados-nação capacidades de vigilância que não conseguiriam desenvolver sozinhos.

O mercado em que os mercenários cibernéticos operam é opaco. No entanto, continuamos a observar estes grupos através de explorações de dia zero e até de explorações com cliques zero que não exigem nenhuma interação com as vítimas, o que permite a vigilância como serviço.

A Microsoft anunciou recentemente um ator ofensivo do setor privado europeu que chamámos de KNOTWEED, um PSOA baseado na Áustria denominado DSIRF. Vários relatórios noticiosos ligaram a empresa ao desenvolvimento e à tentativa de venda de um conjunto de ferramentas de malware denominado Subzero.[51] As vítimas incluem escritórios de advocacia, bancos e consultorias estratégicas em países como a Áustria, o Reino Unido e o Panamá.[52]

Dado que estas capacidades de vigilância ofensiva já não são potencialidades altamente classificadas criadas por agências de defesa e de inteligência, mas sim produtos comerciais agora oferecidos a empresas e indivíduos, qualquer regime regulamentar para as armas cibernéticas precisa de ir mais além do controlo das exportações. O impacto destas armas cibernéticas pode ser devastador.

Quando um mercenário cibernético explora uma vulnerabilidade num produto ou serviço, coloca todo o ecossistema informático em risco. Quando as vulnerabilidades são publicamente identificadas, as empresas estão a correr contra o tempo para libertarem as proteções antes de os ataques com uma base ampla se desenvolverem (consulte a nossa discussão anterior sobre as explorações de vulnerabilidades). Este é um ciclo perigoso e difícil para os fornecedores de software (que têm de desenvolver patches rapidamente) e os consumidores de produtos (que têm de implementar os patches imediatamente).

Como membro fundador do Acordo Tecnológico de Cibersegurança[53], uma aliança líder que reúne mais de 150 empresas de tecnologia, a Microsoft comprometeu-se a não participar em operações ofensivas online. Defendemos esse compromisso e as nossas responsabilidades em matéria de direitos humanos nesta área. Temos participado em interrupções técnicas e desafios legais para realçar os impactos negativos causados pelos serviços prestados por mercenários cibernéticos e continuaremos a proteger os nossos clientes quando vemos abusos.

> Os cibermercenários criam e fornecem capacidades de "vigilância como serviço" tecnologicamente sofisticadas e amplamente disponíveis, incluindo malware avançado e um vasto leque de técnicas.

Insights acionáveis para governos

1. Implemente requisitos de transparência e supervisão para a vigilância como serviço, sobretudo na aquisição, incluindo a interdição destes atores ofensivos, como os EUA fizeram com a lista de empresas do Departamento de Comércio na Lista de Entidades.
2. Estabeleça restrições pós-emprego para ex-colaboradores neste setor.
3. Vise implementar obrigações de "conhecer o seu cliente" e encorajar as empresas a defenderem os seus compromissos em direitos humanos.

Ligações para mais informações

- Desenredar o KNOTWEED: ator ofensivo do setor privado europeu usa explorações de dia 0 | Centro de Informações Sobre Ameaças da Microsoft (MSTIC), Centro de Resposta de Segurança da Microsoft (MSRC), RiskIQ (Informações sobre Ameaças do Microsoft Defender)
- Continuar a lutar contra as armas cibernéticas do setor privado | Microsoft On the Issues

Instrumentalização das normas de cibersegurança em prol da paz e da segurança no ciberespaço

Necessitamos urgentemente de um enquadramento global consistente que dê prioridade aos direitos humanos e proteja as pessoas contra o comportamento online imprudente dos Estados. Em nenhum outro lugar este sentimento de urgência é mais claramente demonstrado do que na guerra em curso na Ucrânia. Além de um esforço estratégico global, os governos podem agir de imediato no sentido de produzirem um impacto positivo imediato.

Há cinco anos atrás, a Microsoft apelou a uma "Convenção de Genebra Digital" para promover as responsabilidades e obrigações de todos os setores para defender a paz e a segurança online. O ciberespaço começava a emergir como um domínio distinto e instável de conflito e concorrência entre os Estados, com os ataques a tornarem-se mais comuns, mesmo em tempos de paz.

Atualmente, continua a ser evidente a necessidade de um tal enquadramento, conforme demonstram os ciberataques russos contra a Ucrânia no âmbito da invasão da Rússia. Esta guerra criou uma nova linha da frente que é substancialmente diferente de qualquer uma das anteriores até aqui conhecidas.

O regresso da estabilidade ao ciberespaço exigirá o reforço e a redefinição das instituições de governação global para as adaptar ao fim a que se destinam. O ciberespaço é fundamentalmente diferente quando comparado com outros domínios: não tem fronteiras, é sintético e é mantido em grande parte pelo setor privado.

Isto significa pedir ao setor das tecnologias que assuma uma maior responsabilidade não só em relação à segurança dos produtos e dos serviços como no que diz respeito ao ecossistema digital na sua aceção mais ampla. Apesar dos progressos assinaláveis em todas as frentes, os desafios aumentaram drasticamente.

Temos de redobrar os esforços coletivos de defesa da segurança do ciberespaço. Não podemos assumir como garantidos os direitos e as liberdades que nos habituámos a ter online. Enquanto nos esforçamos por responder aos desafios, existem atores maliciosos a planear como e onde atacar a seguir fazendo uso da IA, a tirar partido da desinformação e a desvendar formas de minar o metaverso em ascensão. Os defensores dos direitos humanos, o setor das tecnologias e os governos que respeitam os direitos devem trabalhar em conjunto em prol de uma visão positiva de um mundo online seguro e protegido. O caminho a percorrer é longo, mas há medidas que os governos podem tomar agora mesmo para melhorar imediatamente o ecossistema da cibersegurança:

- Citar as normas, as leis e as consequências nas atribuições. Uma melhoria importante verificada nos últimos cinco anos diz respeito à rapidez e coordenação das atribuições dos ciberataques por parte dos governos. Para além da simples denúncia e responsabilização, estas declarações devem realçar as leis ou normas internacionais que foram violadas e as consequências que serão impostas para ajudar a reforçar o reconhecimento das expectativas internacionais.
- Esclarecer a interpretação do direito internacional online. Apesar de os governos concordarem que o direito internacional é aplicável online, subsistem dúvidas quanto à forma como o mesmo se aplica em casos específicos. Isto é particularmente pertinente no rescaldo da invasão da Ucrânia. Os governos podem dar um enorme contributo no que toca a definir expectativas, evitar mal-entendidos e promover a confiança ao estabelecerem uma interpretação clara das suas obrigações ao abrigo da legislação internacional.
- Consultar outros intervenientes. Paralelamente aos esforços desenvolvidos pelos fóruns internacionais no sentido de identificar as melhores formas de simplificar o envolvimento sólido e inclusivo dos múltiplos intervenientes, os governos podem promover o diálogo informado ao consultarem as comunidades compostas por múltiplos intervenientes, em particular o setor das tecnologias, para assegurar as vantagens de dialogar com quem dispõe de competências indispensáveis.
- Formar um órgão permanente de apoio ao comportamento responsável dos Estados no ciberespaço. O trabalho dos fóruns diplomáticos internacionais para promover o comportamento responsável dos Estados online nunca foi tão importante. Existe uma clara necessidade de um mecanismo permanente das Nações Unidas para gerir o ciberespaço como um domínio de conflito.
- Definir novas normas para as ameaças em evolução. As ameaças do ciberespaço estão em constante evolução, tal como acontece com as inovações tecnológicas. Ainda que as normas internacionais devam ser neutras no plano da tecnologia, deverão ser atualizadas e atenuadas em função das alterações verificadas no panorama das ameaças e na forma como utilizamos a tecnologia. Ainda hoje, constatamos a exploração abusiva das lacunas que existem no atual enquadramento internacional. Os Estados devem empenhar-se em proteger expressamente os processos de base subjacentes ao ecossistema digital que estão atualmente desprovidos de proteção, nomeadamente o processo de atualização de software. Além disso, existem áreas específicas que merecem proteções adicionais. Por exemplo, tal como foi possível aprender com a pandemia, as normas de proteção dos cuidados de saúde são essenciais.

O volume e nível de sofisticação dos ataques e dos atores do estado-nação estão a aumentar, o que cria uma situação insustentável.

A tomada de medidas imediatas é um imperativo. Existem medidas que os governos podem aplicar hoje mesmo para melhorar de imediato o ecossistema da cibersegurança, incluindo a implementação de normas e regras acordadas no que se refere ao comportamento do Estado no ciberespaço e a colaboração com a comunidade mais alargada de múltiplos intervenientes no sentido de dar resposta às lacunas emergentes.

As instituições multilaterais têm de ser repensadas para enfrentar o desafio premente dos ciberataques dos Estados-nação.

Ligações para mais informações

- Momento da verdade: a necessidade de uma resposta forte e global em matéria de cibersegurança | Microsoft On the Issues
- Os ciberataques que visam os cuidados de saúde têm de parar | Microsoft On the Issues
- A exigência de um novo capítulo para a ciberdiplomacia nas Nações Unidas | Microsoft On the Issues

Notas finais

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. A infraestrutura crítica referida neste capítulo é definida com base na Diretiva de Política Presidencial 21 (PPD-21), Critical Infrastructure Security and Resilience (fevereiro de 2013) dos Estados Unidos.
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 finais – Continuação

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. Em particular, aplique o patch aos servidores Exchange para corrigir as vulnerabilidades ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 e CVE-2021-27065, CVE-2021-34473). Além disso, aplique o patch aos dispositivos Fortinet FortiOS SSL VPN para corrigir as 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. Conforme indicado no nosso blogue técnico, a identificação de alvos num país não significa necessariamente que um cliente de DSIRF resida nesse país, uma vez que a definição de alvos internacionais é uma prática comum.
53. Home | Cybersecurity Tech Accord (cybertechaccord.org)

Dispositivos e Infraestrutura

Com a aceleração da transformação digital, a segurança da infraestrutura digital é mais importante do que nunca.

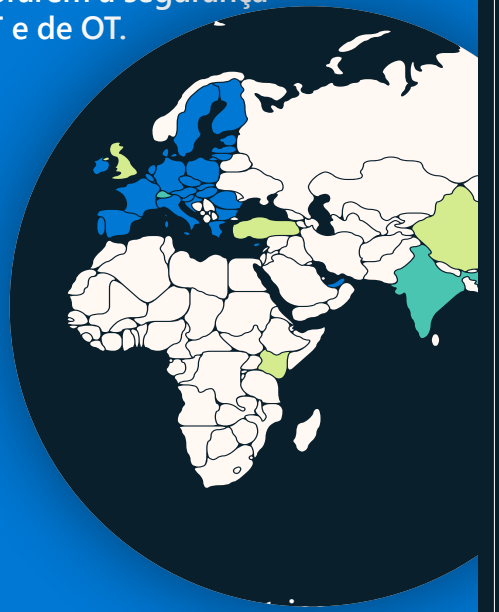
Descrição geral de

Dispositivos e Infraestrutura

A pandemia, aliada à rápida adoção de todos os tipos de dispositivos com acesso à Internet no âmbito da aceleração da transformação digital, aumentou significativamente a superfície de ataque do universo digital.

Os cibercriminosos e os Estados-nação estão a tirar rapidamente partido da situação. Apesar do reforço da segurança do hardware e do software de TI nos últimos anos, a segurança da Internet das Coisas (IoT) e dos dispositivos de tecnologia operacional (OT) não acompanhou o ritmo. Os atores das ameaças estão a explorar estes dispositivos para aceder às redes e permitir o movimento lateral, para criar uma base forte na cadeia de fornecimento ou para perturbar as operações de OT da organização alvo.

Governos do mundo inteiro estão a tomar medidas para proteger a infraestrutura crítica ao melhorarem a segurança da IoT e de OT.

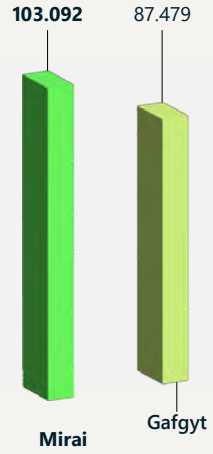


Saiba mais na pág. 59

São necessárias políticas de segurança globalmente consistentes e interoperáveis para assegurar uma adoção generalizada.

Saiba mais na pág. 59

O malware como serviço avançou para operações em grande escala contra a IoT e OT expostas nas infraestruturas e nos serviços públicos, bem como nas redes empresariais.



Saiba mais na pág. 63

Os ataques contra dispositivos de gestão remota estão a aumentar, com mais de 100 milhões ataques observados em maio de 2022, um volume cinco vezes superior ao do ano passado.

Saiba mais na pág. 62

Os atacantes tiram cada vez mais partido das vulnerabilidades no firmware dos dispositivos de IoT para se infiltrarem nas redes empresariais e lançar ataques devastadores.

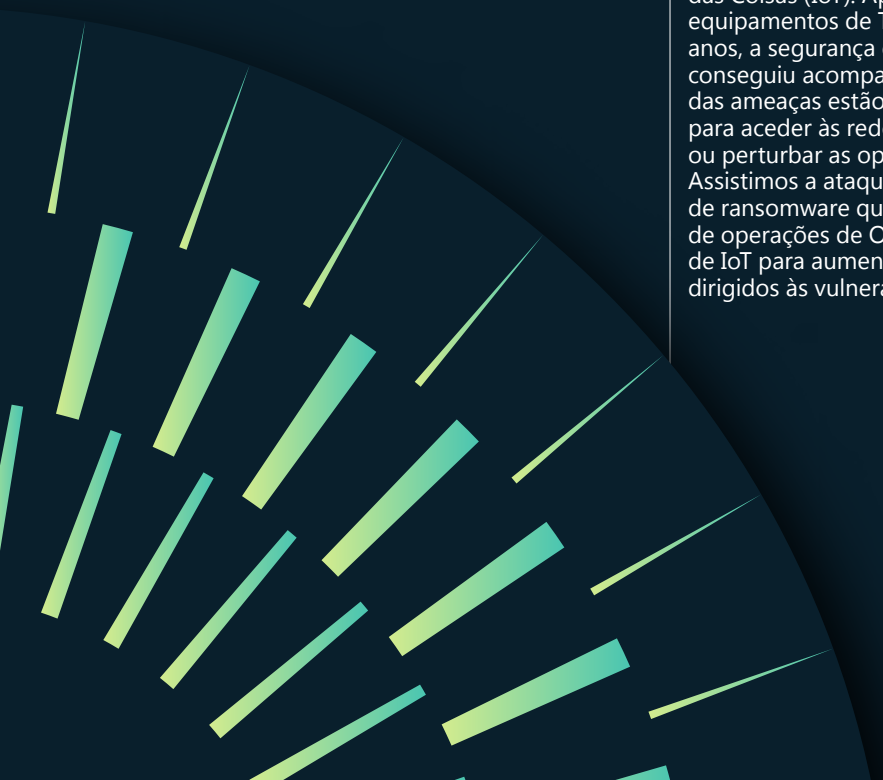
Saiba mais na pág. 65

32% das imagens de firmware analisadas continham pelo menos 10 vulnerabilidades críticas conhecidas.

Saiba mais na pág. 66

Introdução

A aceleração da transformação digital aumentou o risco de cibersegurança para a infraestrutura crítica e os sistemas ciberfísicos.



Os últimos anos têm sido palco de uma mudança sem precedentes no universo digital. As organizações estão a evoluir no sentido de capitalizar os avanços na capacidade de computação da cloud inteligente e da periferia inteligente. Como resultado da pandemia, que forçou as entidades a digitalizar para sobreviverem, e do ritmo com que os setores da indústria de todo o mundo estão a adotar dispositivos com acesso à Internet, a superfície de ataque do universo digital está a aumentar exponencialmente.

A rapidez desta migração ultrapassou a capacidade de a comunidade de segurança acompanhar o seu ritmo. No decorrer do último ano, observámos ameaças que exploram dispositivos de todos os setores da organização, desde os equipamentos de TI tradicionais aos controladores de tecnologia operacional (OT) ou os simples sensores da Internet das Coisas (IoT). Apesar de a segurança dos equipamentos de TI ter sido reforçada nos últimos anos, a segurança dos dispositivos de IoT e OT não conseguiu acompanhar o mesmo ritmo. Os atores das ameaças estão a explorar estes dispositivos para aceder às redes e permitir o movimento lateral ou perturbar as operações de OT da organização. Assistimos a ataques a redes elétricas, a ataques de ransomware que resultaram na interrupção de operações de OT, ao aproveitamento de routers de IoT para aumentar a persistência e a ataques dirigidos às vulnerabilidades do firmware.

Apesar de a prevalência das vulnerabilidades da IoT e OT constituir um desafio para todas as organizações, a infraestrutura crítica corre um risco maior porque os atores das ameaças perceberam que a desativação dos serviços críticos é uma arma poderosa. O ataque de ransomware contra a Colonial Pipeline Company, em 2021, demonstrou como os criminosos podem interromper um serviço critico para aumentar a probabilidade de pagamento de um resgate. Por sua vez, os ciberataques da Rússia contra a Ucrânia demonstram que alguns Estados-nação encaram os ciberataques contra infraestruturas críticas como uma medida de sabotagem aceitável para atingirem os seus objetivos militares.

No entanto, há esperança no horizonte. Os legisladores e os defensores das redes estão a agir no sentido de melhorar a cibersegurança das infraestruturas críticas, incluindo os dispositivos IoT e OT de que dependem. Os legisladores estão a acelerar a elaboração de leis e regulamentos para promover a confiança dos cidadãos na cibersegurança das infraestruturas e dos dispositivos críticos.

A Microsoft está a colaborar com governos do mundo inteiro para aproveitar esta oportunidade de melhorar a cibersegurança e está disponível para ampliar a sua participação. No entanto, preocupa-nos o facto de a existência de requisitos inconsistentes, complexos ou demasiado específicos poder ter efeitos não intencionais, incluindo a redução da segurança em alguns casos, ao desviar os já de si escassos recursos de segurança para assegurar a conformidade com várias certificações redundantes.

Do ponto de vista das operações de segurança, os defensores das redes adotam várias abordagens para melhorar a postura de segurança de IoT/OT da respetiva organização. Uma abordagem consiste em implementar a monitorização contínua dos dispositivos de IoT e OT. Outra abordagem é uma solução conhecida como "shift-left", ou seja, exigir e implementar melhores práticas de cibersegurança para os dispositivos de IoT e OT propriamente ditos. Uma terceira abordagem consiste em implementar uma solução de monitorização da segurança que abranja as redes de TI e OT. Esta abordagem holística tem a importante vantagem acrescida de contribuir para processos organizacionais críticos, como "romper os silos" entre a OT e a TI, o que por sua vez permite que a organização atinja uma postura de segurança avançada ao mesmo tempo que cumpre os objetivos empresariais.

Michal Braverman-Blumenstyk
Vice-Presidente Executivo, Diretor de Tecnologia, Segurança da Cloud e IA

Governos tomam medidas para melhorar a segurança e a resiliência da infraestrutura crítica

Os governos a nível mundial estão a desenvolver e ampliar políticas para gerir o risco de cibersegurança das infraestruturas críticas. Muitos também estão a promulgar políticas para melhorar a segurança dos dispositivos de IoT e OT. A crescente vaga global de iniciativas políticas está a criar uma enorme oportunidade para melhorar a cibersegurança, mas também coloca desafios aos intervenientes de todo o ecossistema.

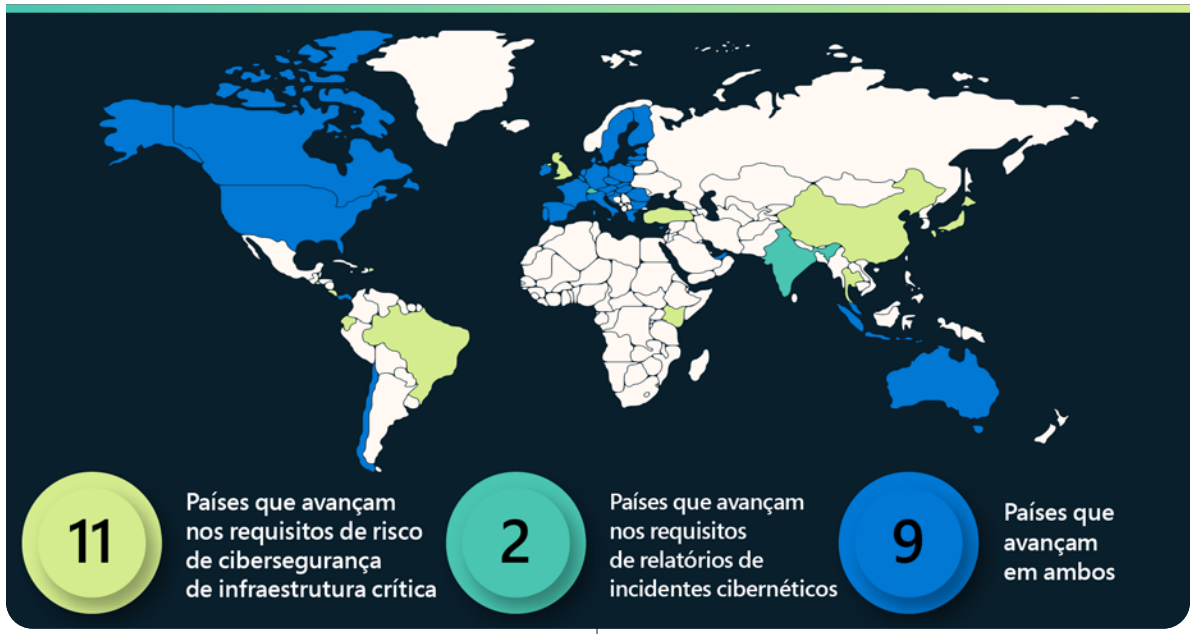
O desenvolvimento de uma visão holística para gerir o risco cibernético das infraestruturas críticas é um processo essencial, mas complexo, sobretudo tendo em conta o grau de interligação entre as tecnologias e os fornecedores globais, a gama de utilizações tecnológicas e os riscos associados, bem como a necessidade de investir em estratégias a curto e longo prazo. A definição de políticas eficazes que favorecem a aprendizagem iterativa e as melhorias, e suportam a interoperabilidade global e intersetorial, pode ajudar a gerir a complexidade e permitir uma transformação digital mais centrada na segurança. No entanto, uma abordagem fragmentada da legislação pode dar origem a requisitos regulamentares inconsistentes e sobrepostos. Isto pode afetar os recursos e, em última análise, minar os objetivos de segurança. Por exemplo, as organizações podem desviar recursos da inovação e da segurança para exercícios de conformidade formalistas.

A Microsoft procura criar parcerias com governos do mundo inteiro na busca de políticas de cibersegurança eficazes para as infraestruturas críticas , com o objetivo de aumentar a compreensão dos desafios e das oportunidades, e apoiar os esforços para melhorar a postura de risco coletivo.

Desenvolvimentos de políticas para a gestão de riscos de cibersegurança de infraestruturas críticas

Durante o último ano, várias jurisdições, incluindo a Austrália, o Chile, a União Europeia (UE), o Japão, a Singapura, o Reino Unido (RU) e os Estados Unidos, desenvolveram, atualizaram ou implementaram requisitos de cibersegurança intersetoriais ou específicos do setor.[1] Muitos destes governos, e outros como a Índia[2] e a Suíça[3], já emitiram ou estão a desenvolver requisitos de relatórios de incidentes de cibersegurança para infraestruturas críticas e fornecedores de serviços essenciais.[4]

Durante o último ano, produziram-se alguns desenvolvimentos assinaláveis em matéria de políticas na Austrália, na UE, na Indonésia e nos Estados Unidos. A Austrália promulgou duas leis para ajudar a gerir os riscos de cibersegurança de infraestruturas críticas intersetoriais. As leis, entre outras determinações, designam novos setores de infraestruturas críticas, requerem o desenvolvimento de planos de gestão de riscos, impõem a comunicação de incidentes de cibersegurança e concedem ao governo meios para intervir se este determinar que o operador de uma infraestrutura crítica não está disposto ou é incapaz de responder adequadamente a um incidente.



A UE trabalhou para atualizar a sua diretiva NIS de 2016, que fornece um enquadramento para os Estados-membros da UE regulamentarem os serviços e produtos tecnológicos considerados críticos para a respetiva economia e o funcionamento da sociedade. A NIS 2 proposta inclui revisões que criam uma nova categoria de infraestrutura digital crítica, aumentam os requisitos para a comunicação de incidentes cibernéticos e impõem requisitos adicionais de gestão de riscos de cibersegurança. A UE também desenvolveu uma proposta de atualização para a sua Lei da Resiliência Operacional Digital (DORA), criando novos requisitos para as tecnologias de comunicação de informações utilizadas no setor dos serviços financeiros.

Em maio, a Indonésia promulgou um regulamento presidencial sobre a proteção da infraestrutura de informações vitais ("IIV"), que irá entrar em vigor em maio de 2024 e irá abranger setores como o da energia, dos transportes, das finanças e da saúde, entre outros. Com este regulamento, a Indonésia pretende proteger a continuidade da implementação da IIV, impedir os ciberataques e aumentar o grau de preparação para lidar com incidentes cibernéticos. Os fornecedores de IIV serão responsáveis por levar a cabo uma proteção segura e fiável, implementar uma gestão de riscos cibernéticos eficaz e comunicar os resultados dos riscos cibernéticos aos organismos públicos competentes. O regulamento inclui um requisito que prevê a comunicação dos incidentes cibernéticos no prazo de 24 horas.

Governos tomam medidas para melhorar a segurança e a resiliência da infraestrutura crítica

Continuação

O Congresso dos E.U.A. aprovou uma lei que autoriza a Agência de Segurança de Infraestruturas e Cibersegurança (CISA) a promulgar regulamentos para exigir a comunicação de incidentes cibernéticos por parte dos operadores de infraestruturas críticas e a Administração da Segurança dos Transportes (TSA) dos E.U.A. emitiu novos requisitos de cibersegurança específicos para o setor dos transportes. Em 2021, a TSA emitiu duas diretivas de segurança para operadores de condutas de gás natural e líquidos perigosos em resposta ao ataque de ransomware lançado contra a Colonial Pipeline Company:

- A primeira diretiva exige que os operadores designem um coordenador de cibersegurança, comuniquem os incidentes cibernéticos num prazo de 12 horas e realizem uma avaliação das vulnerabilidades dos respetivos sistemas.
- A segunda diretiva, que a TSA reviu em 2022, exige que os operadores implementem medidas de mitigação específicas de proteção contra ataques de ransomware e outras ameaças conhecidas aos sistemas de TI e OT, desenvolvam e implementem um plano de contingência e resposta de cibersegurança num prazo de 30 dias e se submetam a uma revisão anual da conceção da arquitetura de cibersegurança.

Com base nos seus regulamentos para gasodutos e oleodutos, a TSA emitiu duas diretivas de segurança adicionais mais tarde, em 2021, que promulgam os requisitos de cibersegurança para os sistemas de transporte ferroviário de mercadorias e passageiros ou de trânsito ferroviário. As diretivas exigem que os operadores abrangidos designem um coordenador de cibersegurança, comuniquem os incidentes de cibersegurança num prazo de 24 horas, desenvolvam e implementem um plano de resposta a incidentes de cibersegurança e levem a cabo uma avaliação das vulnerabilidades de cibersegurança. A TSA anunciou simultaneamente a atualização dos seus programas de segurança para a aviação no sentido de exigir a implementação das duas primeiras disposições aos operadores de aeroportos e linhas aéreas, nomeadamente a designação de um coordenador e a comunicação de incidentes num prazo de 24 horas.

Evolução das políticas de segurança para dispositivos de IoT e OT

Em dezenas de países, os governos estão ativamente envolvidos no desenvolvimento de requisitos para melhorar a cibersegurança dos produtos e serviços das tecnologias de informação e comunicação (TIC), incluindo os dispositivos de IoT e OT. No contexto dos produtos e serviços de TIC, as maiores preocupações são a segurança da cadeia de fornecimento de software e a segurança da IoT.

- A Comissão Europeia propôs a Lei da Resiliência Cibernética, que estabelece requisitos de cibersegurança para o software autónomo e os dispositivos ligados e serviços complementares.[5] As práticas relevantes para os fornecedores de software incluem tirar partido de um ciclo de vida de desenvolvimento de software seguro[6] e fornecer uma Nomenclatura de Software.[7] Os novos requisitos de segurança seriam aplicáveis aos dispositivos ligados e todos os fabricantes ficariam incumbidos de gerir processos coordenados de divulgação de vulnerabilidades[8] para os produtos lançados.

Os legisladores também centraram a sua atenção na proliferação contínua de dispositivos de IoT e dispositivos de OT ligados.

- No Reino Unido, o Projeto de Lei de Segurança de Produtos e Infraestruturas de Telecomunicações exige que os fabricantes de produtos passíveis de ligação destinados ao consumidor, como as smart TVs, deixem de utilizar palavras-passe predefinidas, que são um alvo fácil para os cibercriminosos, estabeleçam uma política de divulgação das vulnerabilidades (como uma forma de receber um aviso de falhas de segurança) e sejam transparentes em relação ao período mínimo de tempo durante o qual fornecem atualizações de segurança.[9]
- Na UE, estão a ser implementadas novas normas ou requisitos de segurança através de vários instrumentos legislativos, incluindo um ato delegado ao abrigo da Diretiva relativa aos Equipamentos de Rádio que se aplica aos dispositivos sem fios e visa melhorar a resiliência da rede, proteger a privacidade dos consumidores e reduzir o risco de fraude monetária.[10] Além disso, poderá se necessário utilizar um plano de certificação na cloud,[11] atualmente em desenvolvimento no seguimento da Lei de Cibersegurança da UE, de 2019[12].

A necessidade de consistência

Em muitos casos, o leque de atividades é desenvolvido em simultâneo em diversas regiões, setores, tecnologias e áreas de gestão de riscos operacionais, o que resulta numa potencial sobreposição ou inconsistência em termos de âmbito, requisitos e complexidade para as organizações que procuram tirar partido das orientações ou demonstrar conformidade. Sem uma definição de IoT universalmente aceite, é particularmente difícil delimitar o âmbito dos regulamentos para dispositivos de IoT e OT. Os exemplos acima indicados aplicam-se potencialmente a "dispositivos ligados e serviços complementares", "produtos passíveis de ligação destinados ao consumidor" e "dispositivos sem fios". Ao mesmo tempo, muitos governos pretendem implementar regimes de avaliação mais robustos para melhor compreender se e como as organizações e os produtos cumprem os requisitos atuais, emergentes e em constante evolução. A fusão gradual destas tendências comporta um aumento da complexidade. Um aspeto encorajador diz respeito às perguntas colocadas durante a consulta sobre a Lei da Resiliência Cibernética da UE, as quais analisaram a potencial interação da nova regulamentação com a regulamentação existente em matéria de cibersegurança, indicando a intenção de evitar requisitos de cibersegurança contraditórios.

As abordagens iterativas baseadas nos riscos e orientadas para os resultados ou os processos (por oposição à implementação específica) podem reforçar a cibersegurança e favorecer uma melhoria contínua. Da mesma forma, um enfoque na viabilização da interoperabilidade entre setores, regiões e áreas políticas poderia melhorar sistematicamente a cibersegurança nas cadeias de fornecimento globais interligadas.

Governos tomam medidas para melhorar a segurança e a resiliência da infraestrutura crítica

Continuação

Estão a ser desenvolvidas políticas de cibersegurança de infraestruturas críticas cada vez mais complexas nas diferentes regiões, setores e áreas temáticas. Esta atividade oferece grandes oportunidades e desafios significativos. A forma de atuação dos governos será crucial para o futuro da transformação digital e da segurança em todo o ecossistema.

Acelerar os investimentos na segurança da cadeia de fornecimento de software e na Arquitetura de Confiança Zero em todo o ecossistema

A Ordem Executiva (EO) 14028 dos E.U.A. sobre a melhoria da cibersegurança serviu de catalisador para acelerar as iniciativas em curso da Microsoft de investir na segurança da cadeia de fornecimento interna e de todo o ecossistema, bem como permitir que os respetivos clientes cumpram os objetivos de Confiança Zero.

Há muito acreditamos que a melhoria da cadeia de fornecimento de software exige a partilha de conhecimentos e melhores práticas, a começar pela divulgação pública do Ciclo de Vida de Desenvolvimento Centrado na Segurança da Microsoft há cerca de 15 anos.

Além disso, estamos a trabalhar em estreita colaboração com o National Cybersecurity Center of Excellence para demonstrar as abordagens à Arquitetura de Confiança Zero aplicadas à tecnologia on-premises e na cloud, e estabelecer novas funcionalidades de produtos, incluindo a capacidade de impor a autenticação resistente ao phishing para ambientes híbridos e multicloud.

Atualmente, estamos a ir além dos requisitos da Ordem Executiva para demonstrar a conformidade com os requisitos de segurança da cadeia de fornecimento de software e fornecer informações de Nomenclaturas de Software (SBOM) de duas formas:

1. Em primeiro lugar, estamos a partilhar uma versão open source da nossa ferramenta de geração de SBOM, criada para ser facilmente integrada nos pipelines de CI/CD que suportam as compilações nas plataformas Windows, Linux, Mac, iOS e Android.[13]
2. Em segundo lugar, estamos a contribuir para o desenvolvimento de normas do setor para a Integridade, Transparência e Fidedignidade da Cadeia de Fornecimento (SCITT). Isto permitirá o intercâmbio automatizado de informações verificáveis da cadeia de fornecimento, incluindo artefactos que demonstrem a conformidade com requisitos como os resultantes das diretrizes da Ordem Executiva sobre a cadeia de fornecimento de software.

Insights acionáveis

1. As instituições multilaterais têm de ser repensadas para enfrentar o desafio premente dos ciberataques dos Estados-nação.
2. Desenvolva políticas de cibersegurança consistentes e interoperáveis entre regiões, setores e áreas temáticas.

Ligações para mais informações

- Investimentos contínuos na segurança da cadeia de fornecimento para apoiar a Ordem Executiva sobre cibersegurança | Microsoft Tech Community
- Governo dos EU.A. estipula os requisitos e a estratégia da arquitetura de Confiança Zero | Blogue Microsoft Security
- CYBER EO | Microsoft Federal
- Integridade, Transparência e Fidedignidade da Cadeia de Fornecimento | github.com
- Implementar uma Arquitetura de Confiança Zero | NCCoE (nist.gov)

Exposição da IoT e OT: tendências e ataques

O universo digital está cada vez mais ligado, o que significa que os dispositivos ficam disponíveis online de forma muito rápida, comunicam com sistemas maiores, recolhem dados e criam visibilidade em espaços anteriormente obscuros. Isto representa uma oportunidade tanto para as organizações como para os atores das ameaças, numa altura em que o negócio do cibercrime está a converter-se simultaneamente numa indústria e num risco de vários mil milhões de dólares.

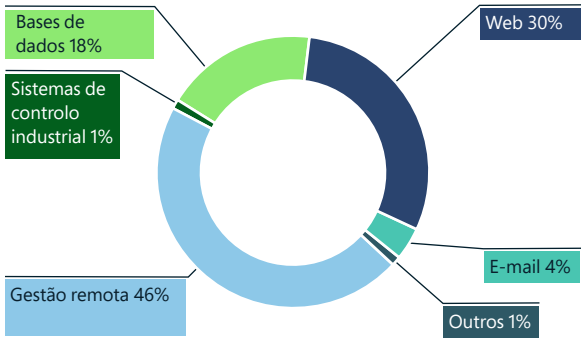
Os dispositivos de IoT, que incluem todo o tipo de dispositivos, desde impressoras a câmaras Web, dispositivos de controlo da temperatura e controlos de acesso a edifícios, colocam riscos de segurança únicos para as pessoas, organizações e redes. Apesar de serem imprescindíveis para as operações de muitas organizações, podem transformar-se rapidamente numa responsabilidade e num risco de segurança. A rápida adoção de soluções de IoT em praticamente todos os setores da indústria aumentou o número de vetores de ataque e o risco de exposição das organizações.

O malware como serviço avançou para operações em grande escala contra as infraestruturas civis e os serviços públicos (incluindo hospitais, infraestruturas de petróleo e gás, redes elétricas, serviços de transporte e outras infraestruturas críticas), bem como contra as redes empresariais. Os atores das ameaças têm de investir grandes esforços de investigação para detetar e explorar a configuração dos ambientes operativos e dos dispositivos de IoT e OT incorporados.

Os dispositivos de IoT colocam riscos de segurança únicos como pontos de entrada e pontos dinâmico na rede. Há milhões de dispositivos de IoT desprovidos de patches ou expostos.

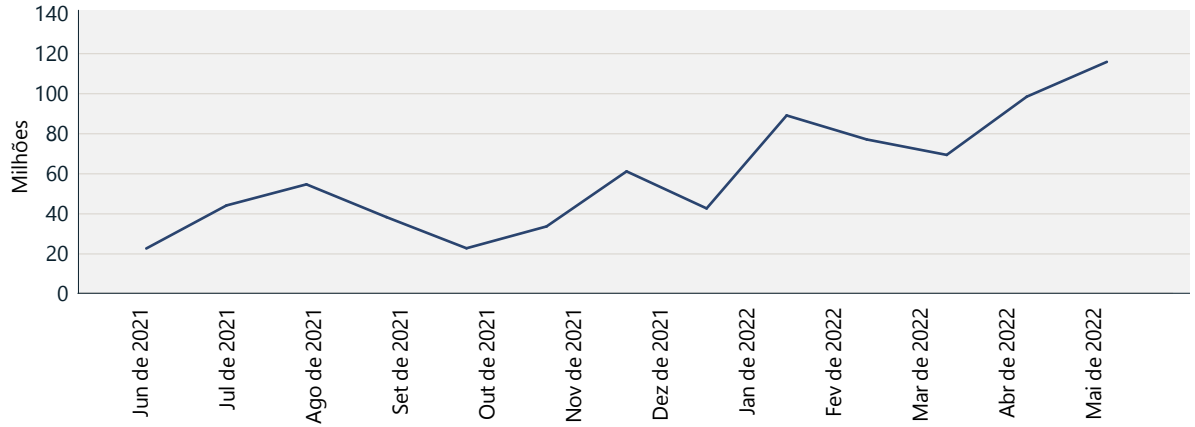
Os dispositivos expostos podem ser detetados através de ferramentas de pesquisa na Internet mediante a identificação de serviços de escuta em portas de rede abertas. Estas portas são normalmente utilizadas para a gestão remota de dispositivos. Se não estiver protegido corretamente, um dispositivo de IoT exposto pode ser utilizado como um ponto dinâmico noutra camada da rede empresarial, já que os utilizadores não autorizados podem aceder remotamente às portas. Temos observado uma variedade de atores das ameaças que tentam explorar as vulnerabilidades dos dispositivos com acesso à Internet, desde câmaras a routers e termostatos. No entanto, apesar do risco, milhões de dispositivos permanecem desprovidos de patches ou expostos.

Resumo de tipos de ataque na IoT/OT



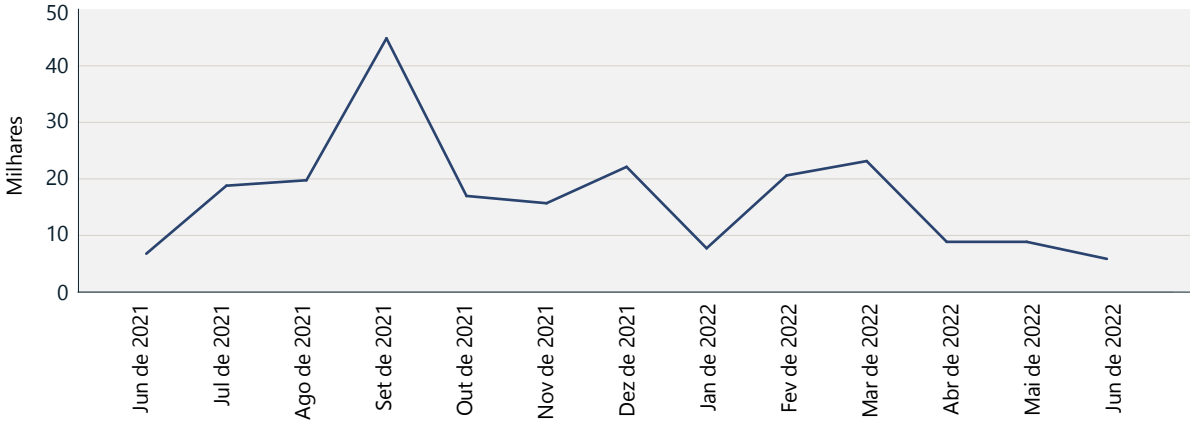
Tipos de ataques observados através da rede de sensores do MSTIC. Os mais predominantes foram ataques contra dispositivos de gestão remota, ataques via Web e ataques a bases de dados (força bruta ou exploits).

Ataques contra dispositivos de gestão remota



Aumento dos ataques contra portas de gestão remota ao longo do tempo, conforme verificado através da rede de sensores do MSTIC.

Ataques via Web contra a IoT e OT



Volume de ataques via Web ao longo do tempo, conforme verificado através da rede de sensores do MSTIC. À medida que o número de dispositivos ligados diretamente à Web continua a cair, os atacantes poderão estar menos dispostos a investigá-los.

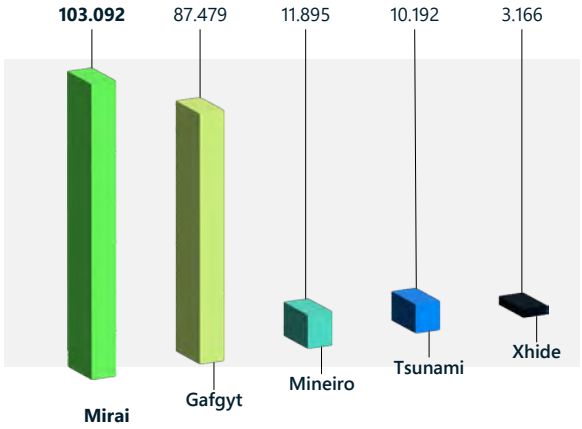
Exposição da IoT e OT: tendências e ataques

Continuação

Utilidade renovada do malware

Os grupos de cibercrime evoluíram ao mesmo ritmo que a respetiva implementação de malware e escolha de alvos. No ano passado, observámos uma diminuição significativa do número de ataques contra protocolos comuns de IoT, como o Telnet, em alguns casos na ordem dos 60%. Ao mesmo tempo, os botnets foram reaproveitados pelos grupos de cibercrime e por atores dos Estados-nação. A persistência do malware, como o Mirai, realça a modularidade destes ataques e a capacidade de adaptação das ameaças existentes.

Principal malware de IoT detetado no mundo real



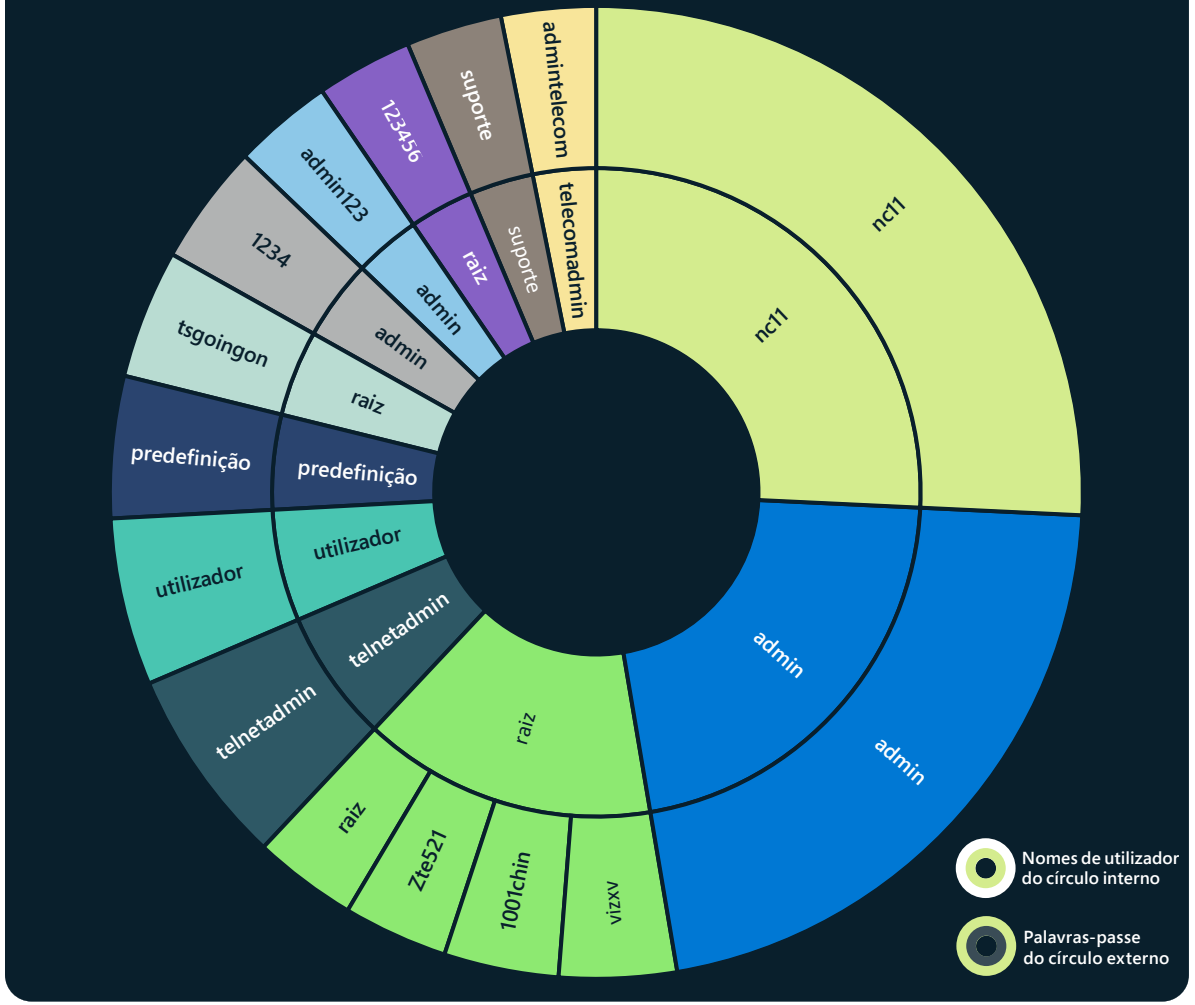
O Mirai evoluiu para infetar uma vasta gama de dispositivos de IoT, incluindo câmaras com protocolo Internet, gravadores de vídeo digitais de câmaras de segurança e routers. O vetor de ataque contornou os controlos de segurança legados e representa um risco para os endpoints na rede ao explorar vulnerabilidades adicionais e mover-se lateralmente. O Mirai foi reformulado várias vezes, com variantes que se adaptam às diferentes arquiteturas e exploram as vulnerabilidades conhecidas e de dia zero de modo a comprometerem novos vetores de ataque.

A utilização do Mirai aumentou nas arquiteturas de CPU x86 de 32 e 64 bits ao longo do último ano, tendo o malware sido dotado de novas capacidades que foram rapidamente adotadas quer pelos Estados-nação, quer por grupos criminosos. Os ataques dos Estados-nação tiram agora partido de novas variantes dos botnets existentes nos ataques denial of service (DDoS) distribuídos contra os adversários estrangeiros.

À medida que as receitas dos ataques contra dispositivos de IoT diminuíram em 2022, observámos como vários grupos de atores das ameaças se aproveitaram de vulnerabilidades, como Log4J e Spring4Shell, para colocar um payload malicioso em dispositivos, como servidores, infetando-os e incorporando-os nos botnets de grandes dimensões que levam a cabo os ataques DDoS. A utilidade renovada do malware concebido para visar dispositivos de IoT vulneráveis tem sérias implicações tanto para as organizações como para os estados-nação, na medida em que o movimento lateral pode expor backdoors a payloads adicionais e outros dispositivos nas redes.

Muitos protocolos de sistemas de controlo industrial não são monitorizados, o que os torna vulneráveis a ataques específicos de OT. Isto pode implicar um maior risco para a infraestrutura crítica.

Prevalência relativa de pares nome de utilizador e palavra-passe observada nos dispositivos de IOT/OT em 45 dias de sinais dos sensores



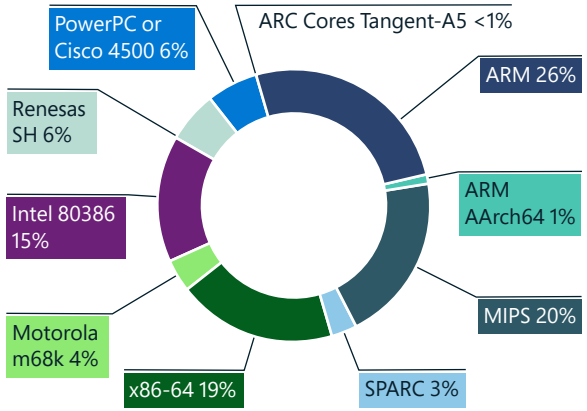
A utilização de pares comuns de nome de utilizador e palavra-passe aumenta o risco de comprometimento. De acordo com uma amostra de mais de 39 milhões dispositivos de IoT e OT, cerca de 20% utilizam nomes de utilizador e palavras-passe idênticos.

Exposição da IoT e OT: tendências e ataques

Continuação

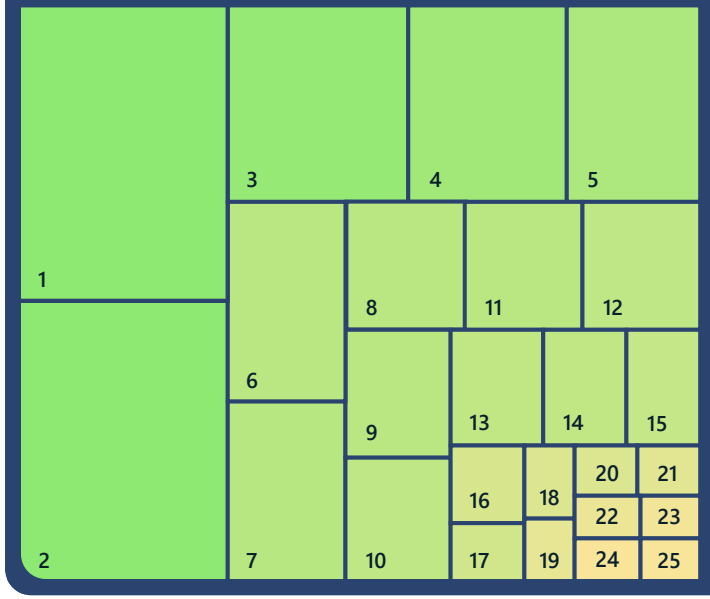
Apesar de as configurações fracas e credenciais predefinidas ainda representarem um risco para as redes, a Microsoft observou que muitos exploits baseados na Web utilizavam o protocolo HTTP. Observámos este aumento de ataques contra serviços baseados na Web através de botnets legados. Entretanto, foi registada uma redução no número de portas de Telnet abertas na Internet, um sinal positivo para a segurança de rede uma vez que os botnets, que sempre representaram um risco histórico para os dispositivos, estão a perder relevância. Apesar desta redução de portas de Telnet abertas, continuamos a observar botnets persistentes nas redes de sensores.

Distribuição do malware de IoT por arquitetura de CPU



A Microsoft observou que os dispositivos de IoT em execução no ARM são os mais visados pelo malware, seguido das CPUs MIPS, X86-64 e Intel 80386.

Prevalência de protocolos de sistemas de controlo industrial



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

Vulnerabilidades de protocolos de sistemas de controlo industrial

Analisámos os dados de OT dos nossos sensores ligados à cloud, o que nos revelou os protocolos de sistemas de controlo industrial (ICS) mais comuns. Estes protocolos fornecem insights sobre a natureza destes dispositivos e a respetiva superfície de ataque. Isto é especialmente relevante para a segurança da infraestrutura crítica. Seguem-se alguns pontos-chave a reter:

1. A maioria dos protocolos representados são proprietários, pelo que as ferramentas de monitorização de TI padrão não têm visibilidade suficiente da segurança destes dispositivos e protocolos. Por conseguinte, as redes não são monitorizadas e, como tal, são mais vulneráveis a ataques específicos de OT.
2. Existe uma grande variedade de protocolos específicos do fornecedor. Isto significa que as soluções de segurança específicas do fornecedor não serão capazes de abarcar adequadamente toda a rede. A Microsoft dá prioridade a uma abordagem independente do fornecedor, para proporcionar cobertura de segurança à ampla variedade de diferentes dispositivos.
3. As organizações devem assegurar que estes protocolos não estão diretamente expostos à Internet a partir das respetivas redes. Esta exposição poderia representar um grande risco de segurança devido às vulnerabilidades e à natureza insegura destes protocolos.

O malware, como o Mirai, persiste graças ao desenvolvimento de novas capacidades e está a ser adotado por grupos de cibercriminosos e atores de estados-nação, que tiram partido de novas variantes dos botnets existentes nos ataques DDoS contra adversários estrangeiros.

Insights acionáveis

1. Certifique-se de que os dispositivos são robustos ao aplicar patches e alterar as palavras-passe e as portas SSH predefinidas.
2. Reduza a superfície de ataque ao eliminar ligações de Internet desnecessárias e portas abertas, restringir o acesso remoto mediante o bloqueio de portas, negar o acesso remoto e utilizar serviços de VPN.
3. Utilize uma solução de deteção e resposta de rede (NDR) com suporte para IoT/OT e uma solução de gestão de eventos e informações de segurança (SIEM)/orquestração e resposta de segurança (SOAR) para monitorizar os dispositivos em busca de comportamentos anómalos ou não autorizados, como a comunicação com hosts desconhecidos.
4. Segmente as redes para limitar a capacidade de um atacante mover-se lateralmente e comprometer os ativos após a intrusão inicial. Os dispositivos de IoT e as redes de OT devem ser isolados das redes de TI corporativas através de firewalls.
5. Certifique-se de que os protocolos ICS não estão diretamente expostos à Internet.

Cadeia de fornecimento e acesso ilícito ao firmware

Praticamente todos os dispositivos ligados à Internet têm firmware, ou seja, software incorporado no hardware ou na placa de circuitos do dispositivo. Ao longo dos últimos anos, o firmware tem sido cada vez mais um alvo privilegiado para o lançamento de ataques devastadores. É muito provável que o firmware se mantenha um alvo valioso para os atores das ameaças, razão pela qual as organizações devem proteger-se contra o acesso ilícito ao firmware.

O firmware é responsável pelas principais funções de um dispositivo, como a ligação a uma rede ou o armazenamento de dados. O firmware está presente em routers, câmaras, televisões e outros dispositivos utilizados nas empresas (IoT), juntamente com o equipamento de controlo industrial (OT) utilizado na infraestrutura crítica. Historicamente, o firmware tem sido escrito com código inseguro, criando vulnerabilidades significativas que podem ser exploradas para assumir o controlo do dispositivo ou injetar código malicioso no firmware.

Este risco é agravado quando se trata da cadeia de fornecimento. A maioria dos dispositivos são criados com componentes de software e hardware de vários fabricantes, bem como bibliotecas open source. Em muitos casos, os operadores de dispositivos não têm visibilidade sobre a nomenclatura do hardware e software (H/SBOM) para avaliar o risco da cadeia de fornecimento dos dispositivos da respetiva rede. Em junho de 2020, foram divulgadas vulnerabilidades numa networking stack utilizada por inúmeros fabricantes diferentes, afetando centenas de milhões de dispositivos de IoT no domínio dos equipamentos industriais e de consumo.[14] Em alguns casos, a marca da networking stack foi mudada por outros fornecedores e não havia nenhuma indicação de que um dispositivo estava vulnerável. Vemos uma ameaça cada vez maior de atores maliciosos que atacam esta cadeia de fornecimento de software e hardware de dispositivos de IoT/OT com o objetivo de comprometer as organizações.

O processo de atualização de firmware varia amplamente entre dispositivos e a complexidade e o desafio logístico inerente à sua execução afeta a frequência da atualização. Nem sempre é possível determinar se um dispositivo está a executar o firmware mais recente, o que dificulta a capacidade de os profissionais de segurança monitorizarem e garantirem a postura de segurança nos respetivos dispositivos de IoT e OT. Além disso, alguns dispositivos têm firmware que não está assinado criptograficamente, o que permite que sejam atualizados sem a verificação do utilizador. Estas fragilidades expõem ainda mais os dispositivos a ataques de cadeia de fornecimento em toda a cadeia de produção e distribuição.

Para fazer face a estas ameaças, a Microsoft investe significativamente no sentido de garantir a segurança e integridade do firmware, à medida que este transita pelas várias fases da cadeia de fornecimento, e atestar a par e passo que o mesmo não foi adulterado durante a ingestão ou o processo em si. Isto irá permitir-nos validar a confiança entre cada segmento do pipeline e proporcionar uma cadeia de custódia ponto a ponto certificada e demonstrável para cada componente que enviamos aos clientes. Estamos a trabalhar com os nossos parceiros para levar esta segurança do chip à cloud a todos os dispositivos da empresa e da rede de OT.

"Os fornecedores de infraestruturas de TIC são cada vez mais alvo de ataques já que permitirem a replicação generalizada de um único ataque. Ao mesmo tempo, a legislação e regulamentação globais e as exigências dos clientes em termos de segurança e resiliência da cadeia de fornecimento estão a aumentar, divergindo muitas vezes em matéria de requisitos.

A solução passa pela criação de parcerias. Em conjunto com os fornecedores e governos de todo o mundo, a Microsoft está empenhada em abordar a segurança do seu ecossistema da cadeia de fornecimento, excedendo as exigências dos clientes e dos reguladores. Para tal, estamos a impulsionar uma abordagem abrangente à segurança e à resiliência operacional, implementada de forma flexível em toda a cadeia de fornecimento.

Promover a integridade do firmware, desde a conceção ao funcionamento do dispositivo, é algo fundamental para a nossa abordagem coletiva. Garantir os processos de SDL dos fornecedores e implementar a inovação radicada na confiança depositada no hardware são exemplos de como podemos "promover" a integridade da cadeia de fornecimento.

A nossa comunidade está a tirar partido da investigação e desenvolvimento coletivos que abrangem novas técnicas antiadulteração e mecanismos criptográficos, combinados com a monitorização contínua e deteção de anomalias. Em conjunto, estamos a fazer progressos no sentido de minimizar os atrativos da cadeia de fornecimento como uma superfície de ataque."

Edna Conway,
Vice-Presidente, Diretor de Segurança e Riscos, Infraestrutura da Cloud

Destaque para as vulnerabilidades de firmware

Os atacantes tiram cada vez mais partido das vulnerabilidades no firmware dos dispositivos de IoT para se infiltrarem nas redes empresariais. Ao contrário dos endpoints de TI tradicionais que utilizam agentes XDR para identificar os pontos fracos, a identificação de vulnerabilidades nos dispositivos de IoT/OT é muito mais difícil.

Uma pesquisa recente realizada pela Microsoft e pelo Ponemon Institute destaca a oportunidade e o desafio de segurança dos dispositivos de IoT/OT numa empresa.[15] Apesar de 68% dos inquiridos acreditar que a adoção de IoT/OT é imprescindível para a sua transformação digital estratégica, 60% reconhece que a segurança de IOT/OT é um dos aspetos menos seguros da infraestrutura de IoT/OT.

Um exemplo de atacantes que utilizam as vulnerabilidades no firmware de um dispositivo de IoT para se infiltrarem numa rede é o trojan Trickbot, que tirou partido das palavras-passe predefinidas e das vulnerabilidades nos routers Mikrotik[16] para contornar os sistemas de defesa empresariais. O desafio fundamental do firmware dos dispositivos de IoT prende-se com a falta de visibilidade sobre a postura de segurança e as vulnerabilidades dos dispositivos.

Apesar de existirem soluções disponíveis para criar dispositivos seguros, existem milhares de milhões de dispositivos já no mercado e implementados nas empresas. Estes são conhecidos como dispositivos "brownfield" (ou seja, pré-existentes). Em 2021, a Microsoft adquiriu o ReFirm Labs para lançar alguma luz sobre a segurança dos dispositivos "brownfield" e conceder aos fabricantes de dispositivos a possibilidade de melhorarem a segurança dos respetivos produtos. O ReFirm Labs analisa a imagem binária do firmware de um dispositivo e produz um relatório detalhado sobre os potenciais pontos fracos da segurança.[17] Esta tecnologia vai ser incorporada numa versão futura do Microsoft Defender para IoT.

No ano passado, examinámos os resultados agregados do firmware exclusivo analisado pelos nossos clientes. Apesar de nem todos os pontos fracos identificados poderem ser explorados de forma ilícita, os resultados sublinham o desafio fundamental subjacente à segurança do firmware dos dispositivos.

É de realçar que os tipos de pontos fracos existentes nos dispositivos de IoT/OT nunca seriam aceitáveis nos endpoints tradicionais do Windows ou do Linux.

- Palavras-passe fracas: 27% das imagens de firmware analisadas continham contas com palavras-passe codificadas com algoritmos fracos (MD5/DES), facilmente decifrados pelos atacantes.

Pontos fracos da segurança nas imagens de firmware analisadas

- Vulnerabilidades conhecidas: à semelhança de outros sistemas, o firmware dos dispositivos de IoT/OT fez um amplo aproveitamento das bibliotecas open source. No entanto, os dispositivos são muitas vezes fornecidos com versões desatualizadas destes componentes. Na nossa análise, 32% das imagens continha pelo menos 10 vulnerabilidades conhecidas (CVEs) classificadas como críticas (9 ou superior). 4% continha pelo menos 10 vulnerabilidades críticas com mais de seis anos.
- Certificados expirados: os certificados são utilizados para autenticar ligações e identidades, bem como para proteger dados confidenciais, mas 13% das imagens analisadas continha pelo menos 10 certificados que haviam expiraram há mais de três anos.
- Componentes de software: 36% das imagens continha componentes de software cuja exclusão dos dispositivos de IoT é recomendada pela Microsoft, como ferramentas de captura de pacotes (tcpdump, libpcap), que podem ser exploradas para o reconhecimento da rede no âmbito de uma cadeia de ataque.

Ataques de firmware no mundo real

Viasat: utilização de uma vulnerabilidade de firmware para atacar as comunicações por satélite

Em fevereiro de 2022, um incidente na rede de satélites desligou uma rede de comunicações estratégica, com efeitos sido sentidos em toda a Europa. O sistema KA-SAT da Viasat recebeu uma grande quantidade de tráfego que desligou muitos modems. A seguir, foi lançado um ataque denial of service contra a rede. Assim que a banda larga fixa foi interrompida, milhares de turbinas eólicas ficaram remotamente inacessíveis aos operadores, ao que se seguiu a implementação de malware malicioso de supressão de dados nos modems afetados. A interrupção afetou mais de 30.000 terminais de satélite utilizados por empresas e organizações para fins de comunicação.

Cyclops Blink: utilizar um ataque de cadeia de fornecimento de firmware para os gateways de firewall de destino

Para os atores das ameaças, o desenvolvimento e a expansão da infraestrutura de comando e controlo (C2) e de ataque são componentes cruciais para o sucesso. Com a crescente necessidade de uma infraestrutura de C2 estável, os routers transformaram-se num vetor de ataque desejável porque a aplicação de patches é pouco frequente e as soluções de segurança abrangentes são escassas.

A Microsoft está a colaborar com o setor público e a indústria em matéria de tecnologia de análise de firmware no sentido de melhorar a visibilidade da segurança dos dispositivos e fornecer uma segurança do ciclo de vida completo aos fabricantes e operadores dos dispositivos.

Desde junho de 2019, um grupo de ameaças avançadas persistentes (APT) afiliado a um Estado-nação utilizou o malware modular Cyclops Blink para atacar dispositivos de firewall WatchGuard vulneráveis e routers ASUS mediante a execução de atualizações de firmware maliciosas e respetiva incorporação num botnet de grandes dimensões. O malware infeta os dispositivos ao explorar uma vulnerabilidade conhecida que permite um escalamento de privilégios, o que abre caminho à gestão dos dispositivos por parte dos atores das ameaças. Uma vez concretizada a infeção, o malware permite a instalação de mais módulos e ilude as atualizações do firmware. Foram observados dispositivos comprometidos a ligar-se a servidores C2 alojados noutros dispositivos WatchGuard. Graças à emissão de numerosos certificados SSL para o respetivo C2 em várias portas TCP, os operadores do Cyclops Blink obtinham acesso remoto com privilégios às redes ao executarem atualizações de firmware maliciosas e iludirem os métodos de segurança tradicionais, como a análise.

Como Microsoft está a melhorar a segurança da cadeia de fornecimento

A Microsoft está a colaborar com o setor público e a indústria no sentido de resolver estes desafios de segurança de dispositivos de IoT e OT (consulte o debate na página 66). O nosso contributo irá incluir a utilização de tecnologia de análise de firmware para fornecer aos operadores dos dispositivos visibilidade ao nível da postura de segurança dos dispositivos nas respetivas redes. Isto permitirá aos clientes identificar e priorizar os dispositivos que precisam de proteções adicionais, atualizações ou de ser substituídos, bem como sensibilizar os fabricantes de dispositivos para a necessidade premente de investirem na segurança dos dispositivos. Ao mesmo tempo, damos suporte aos fabricantes com soluções completas para projetar dispositivos seguros e adotar ciclos de vida de desenvolvimento seguros.

Outro componente chave consiste em fornecer aos fabricantes e operadores uma infraestrutura robusta que permita a atualização do firmware dos dispositivos à medida que os problemas de segurança são detetados e resolvidos. A Microsoft está a aliar a análise de firmware e o Defender para IoT com a Atualização de Dispositivos para IoT Hub para disponibilizar uma solução que permita dar resposta ao ciclo de vida completo da segurança de dispositivos de IoT e OT. Estes são passos importantes para concretizar a nossa visão na qual os clientes protegem a infraestrutura através da adoção de dispositivos que suportem uma abordagem de Confiança Zero às respetivas soluções de IoT e OT.[18]

Os atacantes visam cada vez mais as vulnerabilidades no firmware dos dispositivos de IoT para se infiltrarem nas redes empresariais.

Insights acionáveis

1. Obtenha uma visibilidade mais aprofundada dos dispositivos de IoT/OT na sua rede e atribua-lhes prioridades consoante o risco para a empresa se forem comprometidos.
2. Utilize ferramentas de análise de firmware para compreender os potenciais pontos fracos da segurança e colaborar com os fornecedores para identificar formas de mitigar os riscos para dispositivos de alto risco.
3. Influencie a segurança dos dispositivos de IoT/OT de forma positiva ao exigir a adoção de melhores práticas seguras para o ciclo de vida de desenvolvimento por parte seus fornecedores.

Ligações para mais informações

- Avaliação das Cadeias de Fornecimento Críticas de Suporte ao Setor das Tecnologias de Informação e Comunicações dos E.U.A.

Ataques de OT baseados no reconhecimento

As cadeias de fornecimento complexas utilizam informações de conceção específicas para planear o sistema real. Entre os inúmeros ativos que compõem estas informações de conceção, o mais delicado é o ficheiro de projeto, que define o ambiente e os respetivos ativos. Este ficheiro é um alvo estratégico crucial para os atores das ameaças que procuram obter acesso e lançar um ataque bem-sucedido totalmente adaptado ao ambiente.

O ataque aos sistemas industriais para interromper os processos operacionais envolve dois passos.

1. Em primeiro lugar, o atacante tem de aceder à rede de OT. Para tal, basta que se infiltre através de dispositivos de IoT no lado empresarial da rede (nível 4 do modelo Purdue) e transponha o limite de TI-OT, tradicionalmente separado por firewalls e equipamento de rede, até chegar aos níveis de operações e controlo.
2. Em segundo lugar, os dispositivos de rede têm de ser identificados. Os sistemas industriais utilizam componentes e dispositivos padrão em arquiteturas personalizadas concebidas especificamente para os respetivos ambientes. Um destes dispositivos padrão é o controlador lógico programável (PLC). Cada fabricante desenvolve interfaces e funções exclusivas para os respetivos PLCs, que constituem um componente crucial dos sistemas industriais. Por sua vez, estes dispositivos são configurados com esquemas personalizados adicionais concebidos especificamente para os ambientes do cliente.

A configuração exclusiva de cada PLC é descrita no ficheiro de projeto, que contém a definição do ambiente e dos respetivos ativos, a linguagem ladder e muito mais.

Na maioria dos ambientes que evidenciam provas de um ataque, a análise demonstra que a linha cronológica que precede o ataque excede em muito a duração do ataque em si. Muitas vezes, os atores das ameaças investem meses a simular o ambiente e os respetivos ativos remotamente, realizando muitas tentativas de construir um modelo e preparar o seu ataque direcionado. À medida que os ambientes vão sendo alterados e vão integrando continuamente novos dispositivos, são criadas vulnerabilidades especificamente em torno dos dados nos ficheiros de projeto e de configuração. O roubo de um ficheiro de projeto pode fazer avançar um ataque em termos de semanas ou meses e permitir que os atacantes modelem o ambiente de destino de forma rápida e precisa, o que dificulta ainda mais a deteção da atividade maliciosa.

Industroyer e Incontroller

Temos observado um aumento dos ataques contra organizações, infraestruturas críticas e objetivos governamentais por parte de atores patrocinados por Estados-nação que utilizam malware e estruturas de ataque modulares. As novas tentativas de interferência em operações críticas na Ucrânia sublinham a ameaça crescente de ataques de OT baseados no reconhecimento que são altamente adaptados aos ambientes de destino. As fases prolongadas de reconhecimento e investigação realizadas por ciberatores de estados-nação apontam para uma estratégia que utiliza a ciberguerra para paralisar as infraestruturas remotamente com vista a atingir objetivos estratégicos ou operacionais específicos num contexto de operações cibercinéticas e estratégias políticas combinadas.

Ataques de OT baseados no reconhecimento

Continuação

No início de 2022, foram identificados dois ataques de OT críticos adaptáveis. Um ataque ciberfísico a subestações elétricas e relés de proteção na Ucrânia foi realizado com malware personalizado, incluindo uma variante do Industroyer, um malware conhecido por ter causado falhas de energia na Ucrânia após a sua implementação em 2016.

O Industroyer2 é a primeira reimplementação conhecida de malware malicioso para ataques de OT num novo alvo. Utilizou o plug-in de protocolo IEC104 (protocolo padrão para a monitorização e controlo de sistemas de alimentação) desenvolvido para o Industroyer e atacou sobretudo unidades de terminal remotas do tipo PLC com o número de modelo ABB RTU540/560. O autor deste malware utilizou as informações sobre o ambiente da vítima para emitir repetidamente comandos para saídas pré-determinadas, assegurando de que estas não poderiam ser ativadas manualmente. Esta estratégia garantiu falhas de energia mais prolongadas e um impacto mais prejudicial.

O Incontroller, uma estrutura de ataque modular identificada durante o mesmo período, é um toolkit modular que reduz significativamente o tempo de penetração e ataque de dispositivos de OT, contornando as soluções de segurança legadas. O toolkit para fins gerais tem capacidades de recolha de dados, reconhecimento e ataque altamente personalizáveis para diferentes ambientes e pode afetar significativamente a fase de investigação de um ataque de OT, reduzindo o tempo necessário para executar o reconhecimento e suportando a simulação dos ambientes ao extrair informações sobre os dispositivos e as respetivas configurações.

A estrutura do Incontroller suporta protocolos para os PLCs Schneider Electric e OMRON, e recolhe informações, como a versão de firmware, o tipo de modelo e os dispositivos ligados. O toolkit pode emitir comandos para alterar as configurações e ativar e desativar as saídas. Quando um ambiente é acedido, a estrutura permite a implementação de backdoors em dispositivos para a entrega de mais payloads, a emissão de vulnerabilidades para aumentar os pontos de acesso, o carregamento da linguagem ladder e a capacidade de iniciar ataques DoS. A natureza genérica do toolkit permite que um ator da ameaça ataque rapidamente um ambiente sem precisar de escrever novos ataques para cada PLC ou localização. Isto permite que o ator interaja facilmente com diferentes tipos de máquinas, potencialmente em muitos setores da indústria.

Insights acionáveis

1. Evite transferir ficheiros que contenham definições de sistema através de canais não seguros ou de pessoal não essencial.
2. Quando a transferência de tais ficheiros for inevitável, certifique-se de que monitoriza a atividade na rede e garanta que os ativos estão seguros.
3. Proteja as estações de engenharia através da monitorização com soluções EDR.
4. Conduza a resposta a incidentes para redes de OT de forma proativa.
5. Implemente a monitorização contínua, como o Defender para IoT.

Notas finais

1. Consulte, por exemplo, 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; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | 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); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST
2. Cert-In – Home Page
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Consulte, por exemplo, sem título (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Consulte, por exemplo, Microsoft Security Development Lifecycle
7. Consulte, por exemplo, Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft – Engineering@Microsoft; consulte também, por exemplo, The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Consulte, por exemplo, 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: o SBOM é uma ferramenta altamente dimensionável preparada para empresas que permite a criação de SBOMs compatíveis com SPDX 2.2 para qualquer variedade de artefacto.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. A inovação IoT/OT é essencial, mas comporta riscos significativos (dezembro 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. Descobrir a utilização de dispositivos de IoT da Trickbot na infraestrutura C2 (março 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show no Channel 9 – Episódio sobre análise do firmware de IoT (maio de 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. Como aplicar uma abordagem de Confiança Zero às suas soluções de IoT (maio 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Operações de Ciberinfluência

As operações de influência estrangeira de hoje em dia utilizam novos métodos e tecnologias, que aumentam o grau de eficiência e eficácia das suas campanhas concebidas para minar a confiança das pessoas.

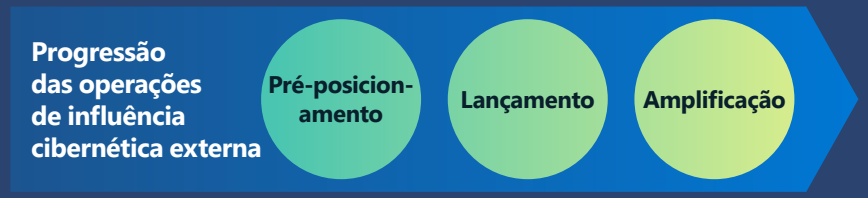
Uma descrição geral das

Operações de Ciberinfluência

As operações de influência estrangeira de hoje em dia utilizam novos métodos e tecnologias, que aumentam o grau de eficiência e eficácia das suas campanhas concebidas para minar a confiança das pessoas.

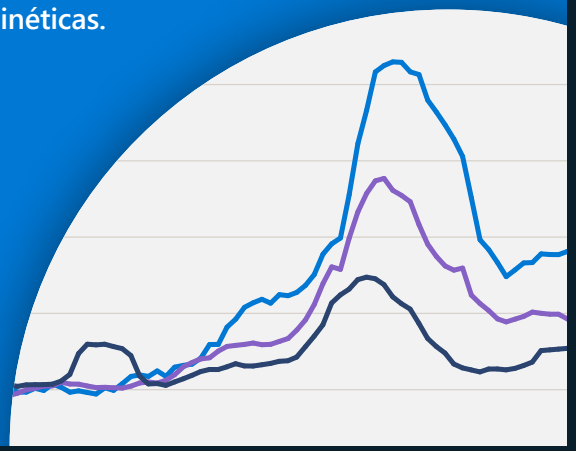
Os estados-nação estão a utilizar cada vez mais operações sofisticadas de influência para distribuir propaganda e criar impacto na opinião pública, tanto a nível nacional como internacional. Estas campanhas corroem a confiança, aumentam a polarização e ameaçam os processos democráticos. Os habilidosos atores Manipuladores Persistentes Avançados estão a utilizar os meios de comunicação tradicionais juntamente com a internet e as redes sociais para aumentarem significativamente o âmbito, a dimensão e a eficiência das suas campanhas, e o impacto de grande dimensão que estão a ter no ecossistema de informações global. No ano passado, vimos estas operações utilizadas como parte da guerra híbrida da Rússia na Ucrânia, mas também vimos a Rússia e outras nações, incluindo a China e o Irão, a adotar cada vez mais operações de propaganda alimentadas pelas redes sociais para alargarem a sua influência global.

As operações de ciberinfluência estão a tornar-se cada vez mais sofisticadas, à medida que mais governos e estados-nação utilizam estas operações para moldar opiniões, desacreditar os adversários e promover a discórdia.



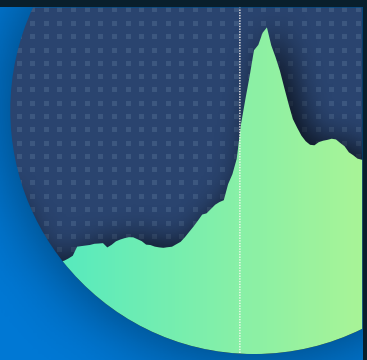
Saiba mais na pág. 74

A invasão da Ucrânia pela Rússia ilustra o enorme impacto da integração entre operações de ciberinfluência, ciberataques mais tradicionais e operações militares cinéticas.



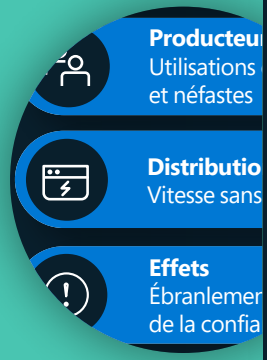
Saiba mais na pág. 76

A Rússia, o Irão e a China recorreram a campanhas de propaganda e influência ao longo de toda a pandemia da COVID-19, muitas vezes como um instrumento estratégico para alcançar objetivos políticos mais amplos.



Saiba mais na pág. 76

Os conteúdos multimédia sintéticos estão a tornar-se cada vez mais predominantes devido à proliferação de ferramentas que criam e disseminam facilmente imagens, vídeos e áudio artificiais altamente realistas. A tecnologia de proveniência digital que certifica a origem dos ativos de multimédia promete combater o uso indevido.



Saiba mais na pág. 80

Uma abordagem holística para se proteger contra as operações de ciberinfluência

A Microsoft continua a desenvolver a sua já consolidada infraestrutura de informações sobre ciberameaças para combater as operações de ciberinfluência. A nossa estratégia consiste em detetar, interromper, defender e desencorajar campanhas de propaganda levadas a cabo por agressores estrangeiros.

Saiba mais na pág. 83

Introdução

A democracia precisa de informações fidedignas para prosperar. Uma área de particular interesse para a Microsoft são as operações de influência que estão a ser desenvolvidas e perpetuadas por estados-nação. Estas campanhas corroem a confiança, aumentam a polarização e ameaçam os processos democráticos.

As operações de influência estrangeira foram, desde sempre, uma ameaça ao ecossistema de informações. No entanto, a grande diferença da era da Internet e das redes sociais em relação ao passado prende-se com o enorme aumento do âmbito, da escala e da eficiência das campanhas, e o vasto impacto que podem exercer sobre a integridade do ecossistema de informações globais.

O velho ditado segundo o qual "uma mentira chega quase ao outro lado do mundo primeiro que a verdade tenha a oportunidade de se manifestar" está agora a ser comprovado com dados. Um estudo realizado pelo Massachusetts Institute of Technology (MIT)[1] constatou que as falsidades têm uma probabilidade 70% maior de serem retweetadas do que a verdade e atingem as primeiras 1500 pessoas seis vezes mais rápido. O ecossistema de informações tornou-se cada vez mais obscuro à medida que as campanhas de propaganda prosperam na Internet e nas redes sociais, minando a confiança depositada nas notícias tradicionais. Um estudo de 2021[2] revelou que apenas 7% dos adultos norte-americanos afirmaram terem "uma grande dose de confiança" nas notícias veiculadas através dos jornais, da televisão e da rádio, enquanto 34% afirmaram não terem "nenhuma confiança mesmo".

A Microsoft tem vindo a desenvolver esforços no sentido de identificar os principais atores, ameaças e táticas no domínio da ciberinfluência estrangeira e partilhar as conclusões tiradas. Em junho deste ano, publicámos um relatório abrangente sobre as conclusões tiradas do conflito na Ucrânia, que continha uma análise detalhada das operações de ciberinfluência da Rússia.[3]

Também estamos a estudar a forma como as tecnologias avançadas, como os "deepfakes", podem ser transformadas em armas e minar a credibilidade dos jornalistas. Além disso, estamos a colaborar com o setor público, a indústria e as instituições académicas no sentido de desenvolver métodos melhores de deteção de conteúdos multimédia sintéticos e restaurar a confiança, como sistemas de inteligência artificial (IA) capazes de identificar falsificações.

A natureza em rápida mudança do ecossistema de informações e a propaganda online levada a cabo por Estados-nação, incluindo a fusão dos ciberataques tradicionais com as operações de influência e a interferência nas eleições democráticas, exigem uma abordagem que envolva toda a sociedade para mitigar as ameaças online e offline à democracia.

A Microsoft está empenhada em dar suporte a um ecossistema de informações saudável, no qual prosperam as notícias e informações fidedignas. Estamos a desenvolver ferramentas e capacidades de deteção de ameaças para combater a evolução e a expansão do risco das operações de influência orientadas por Estados-nação. Para facilitar este trabalho, adquirimos recentemente a Miburo Solutions, estabelecemos parcerias com validadores externos, como a Global Disinformation Index e a NewsGuard, e participamos e, por vezes, lideramos parcerias com vários intervenientes, incluindo a Coalition for Content Provenance and Authenticity (C2PA). Somente se trabalharmos em conjunto seremos capazes de enfrentar aqueles que procuram minar as instituições e os processos democráticos.

Teresa Hutson

Vice-Presidente, Tecnologia e Responsabilidade Empresarial

Tendências das operações de ciberinfluência

As operações de ciberinfluência estão a tornar-se cada vez mais sofisticadas à medida que a tecnologia evolui. Estamos a assistir a uma sobreposição e expansão das ferramentas utilizadas nos ciberataques tradicionais, as quais estão a ser aplicadas às operações de ciberinfluência. Além disso, estamos a ver sinais de uma maior coordenação e amplificação entre Estados-nação.

A Microsoft investiu no combate às operações de influência estrangeira este ano mediante a aquisição da Miburo Solutions, uma empresa especializada na análise de operações de influência estrangeira. Ao combinar estes analistas com os analistas do contexto das ameaças da Microsoft, a Microsoft formou o Digital Threat Analysis Center (DTAC). O DTAC analisa e assinala as ameaças de Estados-nação, incluindo os ciberataques e as operações de influência, combinando informações e dados sobre ameaças com a análise geopolítica para oferecer insights e propor uma resposta e medidas de proteção eficazes.

Mais de três quartos das pessoas de todo o mundo manifestaram estar preocupadas com o uso da informação como uma arma,[4] e os nossos dados confirmam estas preocupações. A Microsoft e os seus parceiros têm vindo a monitorizar a forma como os atores dos Estados-nação estão a utilizar as operações de influência para atingirem os seus objetivos estratégicos e políticos. Além dos ciberataques destrutivos e dos esforços de ciberespionagem, os regimes autoritários estão a utilizar cada vez mais as operações de ciberinfluência para moldar opiniões, desacreditar os adversários, incitar o medo, promover a discórdia e distorcer a realidade.

Normalmente, estas operações de ciberinfluência estrangeira desenrolam-se em três fases:

Pré-posicionamento

À semelhança do que acontece com o pré-posicionamento do malware na rede informática de uma organização, as operações de ciberinfluência estrangeira pré-posicionam as falsas narrativas no domínio público da Internet. A tática de pré-posicionamento há muito que ajuda as atividades cibernéticas mais tradicionais, sobretudo se os administradores de TI analisarem a atividade de rede mais recente. O malware que permanece inativo durante um período prolongado numa rede pode tornar a sua posterior utilização mais eficaz. As falsas narrativas que passam despercebidas na Internet podem fazer com que as referências subsequentes pareçam mais credíveis.

Lançamento

Muitas vezes, no momento mais benéfico para atingir os objetivos do ator, é lançada uma campanha coordenada para propagar narrativas através de meios de comunicação e canais de redes sociais influenciados e apoiados por governos.

Amplificação

Por último, os meios de comunicação e mandatários controlados pelos Estados-nação amplificam as narrativas no seio de audiências específicas. Muitas vezes, alguns utilizadores tecnológicos involuntários ampliam o alcance das narrativas. Por exemplo, a publicidade online pode ajudar a financiar atividades e os sistemas de entrega de conteúdos coordenados podem inundar os motores de busca.

Esta abordagem em três passos foi aplicada no final de 2021 para apoiar a falsa narrativa russa em torno de supostas armas e laboratórios biológicos na Ucrânia. Esta narrativa foi carregada pela primeira vez no YouTube a 29 de novembro de 2021, como parte de um programa habitual em inglês de um expatriado norte-americano sediado em Moscovo que alegava que laboratórios biológicos financiados pelos E.U.A. na Ucrânia estariam ligados a armas biológicas. A história passou despercebida durante largos meses. Em 24 de fevereiro de 2022, assim que os tanques russos cruzaram a fronteira, a narrativa foi introduzida no campo de batalha. Uma equipa de analistas de dados da Microsoft identificou 10 sites de notícias controlados ou influenciados pela Rússia que publicaram relatórios em simultâneo a 24 de fevereiro a apontar para o "relatório do ano passado", procurando dar-lhe credibilidade. Além disso, os funcionários do Ministério dos Negócios Estrangeiros da Rússia realizaram conferências de imprensa destinadas a reforçar a disseminação de notícias falsas sobre laboratórios biológicos dos E.U.A. no ambiente mediático. Equipas patrocinadas pela Rússia trabalharam em seguida para ampliar ainda mais a narrativa nas redes sociais e em sites da Internet.

Estamos a observar uma articulação de esforços de regimes autoritários do mundo inteiro no sentido de contaminar o ecossistema de informações para seu benefício mútuo. Por exemplo, ao longo de toda a pandemia da COVID-19, a Rússia, o Irão e a China recorreram a operações de propaganda e influência utilizando uma combinação de métodos de disseminação declarados, semissecretos e secretos para atacar as democracias e promover objetivos geopolíticos (analisados em maior detalhe na página 76). Os três regimes contribuíram reciprocamente para promover as respetivas narrativas preferenciais nos vários ecossistemas de mensagens e de informações. Grande parte desta cobertura consistiu em críticas ou teorias da conspiração sobre os Estados Unidos e seus aliados, as quais foram propagadas por figuras do governo em declarações oficiais, ao mesmo tempo que promoviam as suas próprias vacinas e respostas à COVID-19 como sendo superiores às dos Estados Unidos e de outras democracias. Ao amplificarem as respetivas narrativas de forma mútua, os meios de comunicação estatais criaram um ecossistema no qual a cobertura negativa das democracias, ou a cobertura positiva da Rússia, do Irão e da China, produzida por um meio de comunicação estatal, era reforçada pelas restantes.

Ilustração de como as narrativas sobre laboratórios biológicos dos E.U.A. e armas biológicas se espalharam através das três fases gerais de muitas operações de influência estrangeira: pré-posicionamento, lançamento e amplificação.

Tendências das operações de ciberinfluência

Continuação

Acresce a este desafio o facto de as entidades tecnológicas do setor privado poderem ativar involuntariamente estas campanhas. Os facilitadores podem incluir empresas que registam domínios da Internet, alojam sites, promovem material nas redes sociais e sites de pesquisa, canalizam tráfego e ajudam a pagar estas atividades com publicidade digital. As organizações têm de estar cientes das ferramentas e dos métodos utilizados pelos regimes autoritários para as operações de ciberinfluência para poderem detetar e, em seguida, evitar a propagação de campanhas. Também existe uma necessidade crescente de ajudar os consumidores a desenvolverem uma capacidade mais sofisticada de identificarem as operações de influência estrangeira e limitarem a interação com as respetivas narrativas ou conteúdos.

As operações de ciberinfluência, incluindo a propaganda autoritária, são uma ameaça para as democracias em todo o mundo, à medida que minam a confiança, aumentam a polarização e ameaçam os processos democráticos.

É necessária uma maior coordenação e partilha de informações entre o governo, o setor privado e a sociedade civil para aumentar a transparência e expor e interromper estas campanhas de influência.

A nível mundial, mais de três quartos das pessoas estão preocupadas com a forma como a informação está a ser usada como uma arma.

Operações de influência durante a pandemia da COVID-19 e a invasão da Ucrânia pela Rússia

Os Estados-nação que procuraram controlar o ambiente de informação ao longo da pandemia e durante a invasão russa da Ucrânia fornecem exemplos categóricos da forma como os regimes autoritários conjugam as operações de cibersegurança e de informação.

Propaganda sobre a COVID-19

A Rússia, o Irão e a China recorreram a campanhas de propaganda e influência ao longo da pandemia da COVID-19. A COVID-19 protagonizou estas campanhas de forma proeminente de duas formas centrais:

1. Representações da pandemia propriamente dita.
2. Campanhas que utilizaram a COVID-19 como um instrumento estratégico para alcançar objetivos políticos mais amplos.

O objetivo geral destes tipos de campanhas é duplo: em primeiro lugar, minar as democracias, as instituições democráticas e a imagem dos Estados Unidos e dos seus aliados no plano global; e, em segundo lugar, reforçar a sua própria posição a nível nacional e internacional.

Um exemplo claro pode ser visto nas mensagens difundidas por contas e organizações de meios de comunicação russas conhecidas que visavam os leitores da língua inglesa em contraste com a forma como o governo russo comunicou com os seus cidadãos sobre a vacina e a gravidade da COVID-19.

Tópicos abordados pelas 10 principais histórias sobre o coronavírus mais vistas em RT.com
(outubro de 2021 – abril de 2022)

Propaganda antivacinas dirigida a leitores não russos

Russo (traduzido abaixo do inglês)	Inglês
"Os confinamentos e as doses de reforço impedem a transmissão"	"As vacinas não conseguem travar a transmissão e são ineficazes contra as novas estirpes"
"Figuras públicas russas estão a testar positivo"	"A vacina Pfizer tem efeitos secundários perigosos"
"Os casos e as mortes estão a aumentar na Rússia"	"A vacinação em massa tem motivações políticas"
"A vacina Sputnik V é altamente eficaz"	"A Pfizer e a Moderna realizam ensaios não regulamentados"
"Comprovativo de vacinação necessário nos transportes públicos"	

As mensagens russas sobre a COVID-19 diferem consoante o idioma.

As campanhas que procuraram ocultar a origem do vírus da COVID-19 oferecem outro exemplo. Desde o início da pandemia, a propaganda russa, iraniana e chinesa sobre a COVID-19 reforçou a cobertura de outros países para ampliar estes temas centrais. Grande parte desta cobertura consistiu em promover críticas ou teorias da conspiração sobre os Estados Unidos. Ao amplificarem as respetivas narrativas de forma mútua e regular, os meios de comunicação estatais desenvolveram um ecossistema no qual a cobertura negativa das democracias, ou a cobertura positiva da Rússia, do Irão e da China, produzida por um meio de comunicação estatal, era reforçada pelas restantes vezes sem conta.

Um exemplo é a sugestão inicial dos meios de comunicação estatais russos e iranianos de que a COVID-19 poderia ser uma arma biológica criada pelos Estados Unidos. Esta alegação circulou em sites de conspiração marginais no início da pandemia após uma entrevista com um professor de direito que afirmava acreditar que a COVID-19 fora criada como uma arma.[6] Depois de a entrevista ter sido publicada em alguns sites com alcance limitado, a história foi veiculada pelos meios de comunicação estatais. A PressTV, um canal de notícias iraniano de expressão francesa e inglesa patrocinada pelo governo iraniano,[7] publicou uma história em língua inglesa em fevereiro 2020 intitulada "Será o coronavírus uma arma de guerra biológica dos E.U.A. como acredita Francis Boyle?" O artigo sugeria que os Estados Unidos estavam por detrás do surto da COVID-19, ao escrever que "em todas as guerras dos E.U.A. haviam sido utilizadas armas radiológicas, químicas, biológicas e outras armas proibidas, infligindo um efeito devastador nas pessoas de determinadas zonas".[8] Os meios de comunicação estatais russos e as contas governamentais chinesas fizeram eco do sentimento. A Russia Today (RT), um canal de notícias estatal conhecido pelo seu papel na disseminação do propaganda do Kremlin[9], publicou pelo menos uma história que promovia declarações de autoridades iranianas com alegações de que a COVID-19 poderia ser um "produto do ataque biológico dos E.U.A. contra o Irão e a China"[10], tendo publicado diversas mensagens nas redes sociais com o mesmo género de insinuação. Por exemplo, num tweet da RT de 27 de fevereiro de 2020 podia ler-se: "Levante a mão quem não ficará surpreso se alguma vez for revelado que o #coronavirus é uma arma biológica?"[11]

A guerra na Ucrânia: propaganda como arma de guerra

A invasão da Ucrânia pela Rússia oferece um exemplo eloquente de como as operações de ciberinfluência podem ser combinadas com ciberataques mais tradicionais e com operações militares no terreno para maximizar o seu impacto.

No período imediatamente anterior à invasão da Ucrânia, analistas de informações sobre ameaças da Microsoft viram pelo menos seis atores separados afiliados da Rússia lançar mais de 237 ciberataques contra a Ucrânia. Estas campanhas procuraram denegrir os serviços e as instituições, perturbar o acesso dos ucranianos a informações fiáveis e semear dúvidas sobre a liderança do país.

Operações de influência durante a pandemia da COVID-19 e a invasão da Ucrânia pela Rússia

Continuação

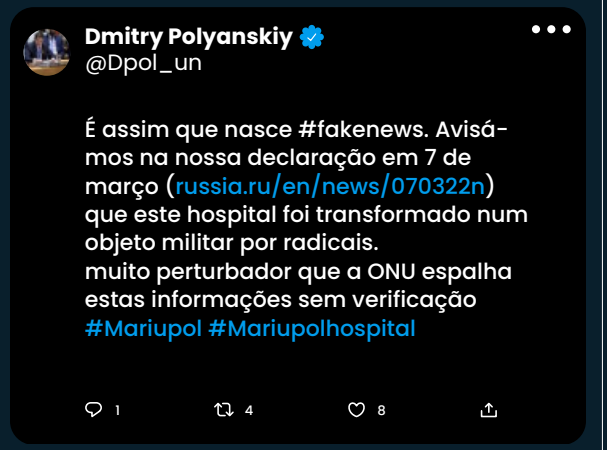
Num relatório da Microsoft publicado em abril de 2022, demonstrámos como, numa aparente tentativa de controlar o ambiente de informação em Kiev, a Rússia lançou um ataque com mísseis contra uma torre de televisão em Kiev no mesmo dia em que lançou um malware destrutivo contra uma importante empresa de meios de comunicação ucraniana.[12]

Noutro exemplo de convergência entre os ciberataques e as operações de influência, um ator de ameaças russo enviou e-mails aos cidadãos ucranianos como se tivessem sido enviados por residentes de Mariupol, culpando o governo ucraniano pela escalada da guerra e convidando os seus compatriotas a protestar contra o governo. Estes e-mails foram endereçados especificamente (por nome) aos que receberam o e-mail, o que indica que as suas informações poderiam ter sido roubadas num ciberataque relacionado com espionagem anterior. Não foram incluídas ligações maliciosas, o que sugere que o objetivo era levar a cabo uma operação de influência pura.

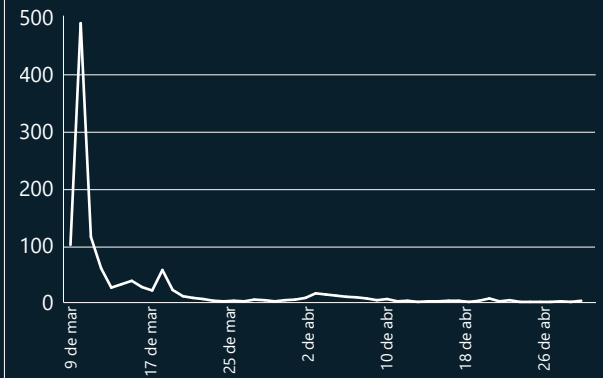
A utilização de materiais supostamente pirateados, divulgados ou de caráter confidencial, é uma tática comum utilizada por atores russos em operações de influência. Ao longo da guerra na Ucrânia, os canais de redes sociais pró-Rússia têm promovido o que alegam ser materiais divulgados ou de caráter confidencial provenientes de fontes ucranianas. Os materiais divulgados ou confidenciais são utilizados pelos canais de redes sociais e meios de comunicação pró-Rússia como parte de uma estratégia de influência mais ampla para deteriorar a confiança nas instituições e lançar dúvidas sobre as narrativas convencionais.

Estas informações podem ser manipuladas para criar propaganda dirigida à Ucrânia e ao Ocidente, diminuir a confiança na segurança digital e minar o apoio à ajuda ocidental à Ucrânia.

A Rússia utilizou outros ataques de informação para moldar a opinião pública após os eventos no terreno para encobrir ou escamotear os factos. Por exemplo, a 7 de março, a Rússia pré-posicionou uma narrativa através de um registo junto das Nações Unidas (NU) de que uma maternidade em Mariupol, na Ucrânia, havia sido evacuada e estava a ser utilizada como base militar. A 9 de março, a Rússia bombardeou o hospital. Após a notícia do bombardeamento, o representante da Rússia nas Nações Unidas, Dmitry Polyanskiy, tweetou que a cobertura do bombardeamento era uma "fake news" e citou as alegações anteriores da Rússia sobre a suposta utilização do local como uma base militar. Em seguida, a Rússia difundiu esta narrativa por todos os sites controlados pela Rússia durante as duas semanas que se seguiram ao ataque ao hospital.



Domínios com tráfego
(9 de março de 2022 – 30 de abril de 2022)



Sites de propaganda publicaram histórias sobre a maternidade durante cerca de duas semanas, com um breve ressurgimento em 1 de abril de 2022. Fonte: Microsoft AI for Good Lab.

Imagens de satélite de um hospital perinatal em Mariupol em fevereiro e março de 2022

A análise de imagens de satélite da Microsoft mostrou que o hospital perinatal foi bombardeado. A primeira fotografia é de 24 de fevereiro de 2022 e a segunda é de 24 de março de 2022. Fonte da fotografia: Planet Labs.

O branqueamento das atrocidades da Rússia continuou com o decurso da guerra. Por exemplo, no final de junho de 2022, os meios de comunicação e os influenciadores russos retrataram o bombardeamento de um centro comercial como justificado e necessário, alegando falsamente que não estava a ser utilizado para esse fim, mas sim como um arsenal para as forças de defesa territorial ucranianas.[13] Vários bloguistas pró-Kremlin no Telegram publicaram e amplificaram conteúdos que reforçavam a narrativa de "operações sob falsa bandeira", apontando para supostos indicadores de manipulação, incluindo a presença de pessoas com uniformes militares[14] e a ausência de mulheres nas filmagens.[15] A Rússia lançou as campanhas com base num sistema elaborado de mensagens e meios de propaganda. A amplificação destas histórias online proporciona à Rússia a capacidade de desviar as culpas na arena internacional e evitar a responsabilização.

Estados-nação, como a Rússia, compreendem o valor de utilizar informações obtidas de fontes estanques para influenciar a perceção pública, recorrendo a campanhas do tipo "piratear e divulgar" para difundir narrativas contrárias e semear a desconfiança.

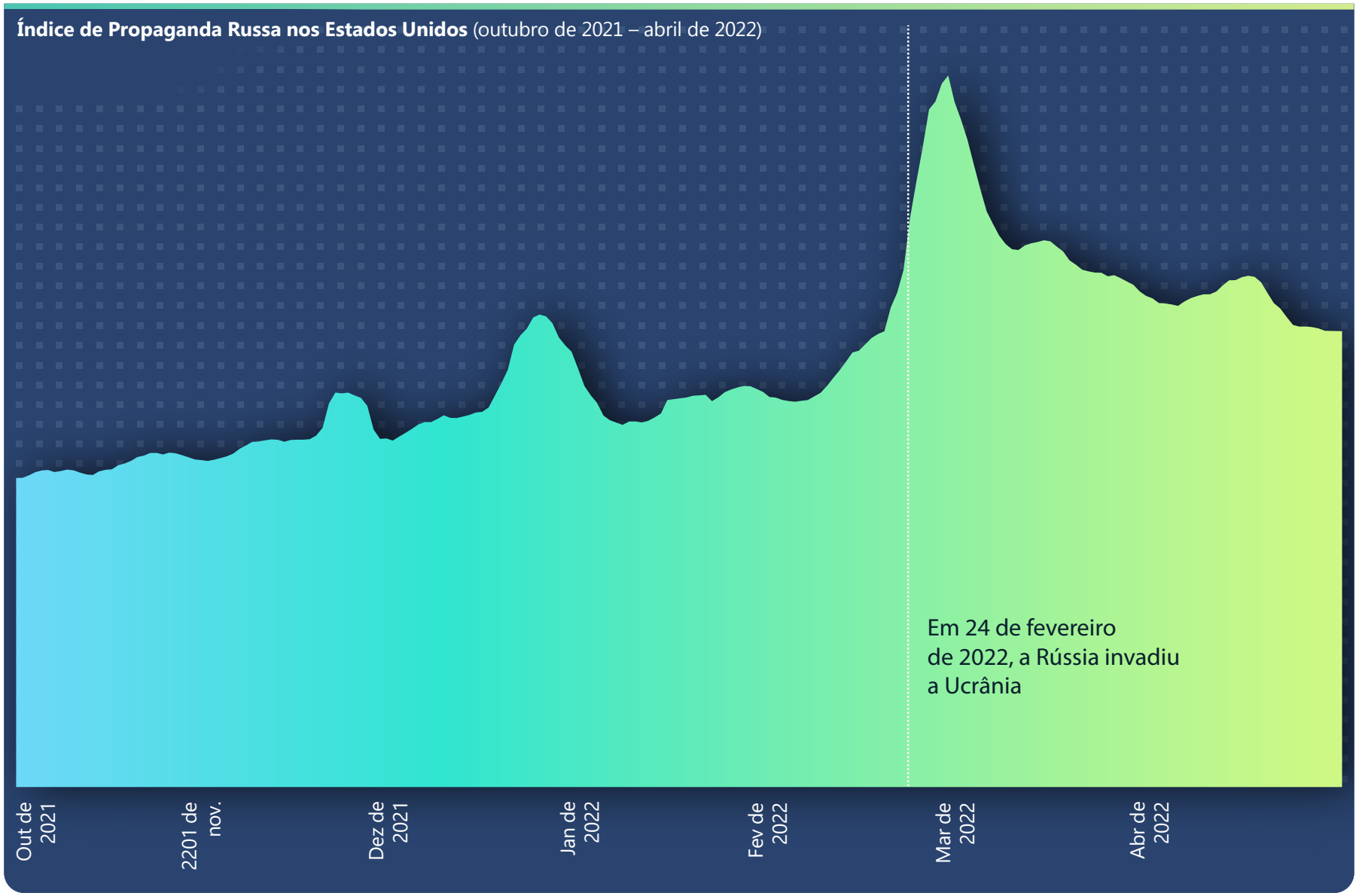
Ligações para mais informações

- Defender a Ucrânia: As Primeiras Lições da Ciberguerra | Microsoft On the Issues
- Uma perspetiva da atividade dos ciberataques da Rússia na Ucrânia | Relatório Especial da Microsoft
- Interromper ataques cibernéticos direcionados à Ucrânia | Microsoft On the Issues

Monitorizar o Índice de Propaganda Russa

Em janeiro de 2022, quase mil sites dos E.U.A. reenviavam tráfego para sites de propaganda russos. Os tópicos mais comuns dos sites de propaganda russos dirigidos a uma audiência norte-americana giravam em torno da guerra na Ucrânia, da política interna dos E.U.A. (pró-Trump ou pró-Biden) e de narrativas relacionadas com a COVID-19 e a vacina.

O Índice de Propaganda Russa (RPI) monitoriza o fluxo de notícias dos meios de comunicação e amplificadores patrocinados e controlados pelo Estado russo como uma parte do tráfego global de notícias na Internet. O RPI pode ser utilizado para cartografar o consumo de propaganda russa através da Internet e em diferentes zonas geográficas numa linha cronológica precisa. A Microsoft assinala, no entanto, que só é possível observar a propaganda russa publicada em sites previamente identificados. Não dispomos de insights sobre a propaganda noutros tipos de sites, incluindo sites de notícias autorizados, sites não identificados e grupos de redes sociais.



Monitorizar o Índice de Propaganda Russa

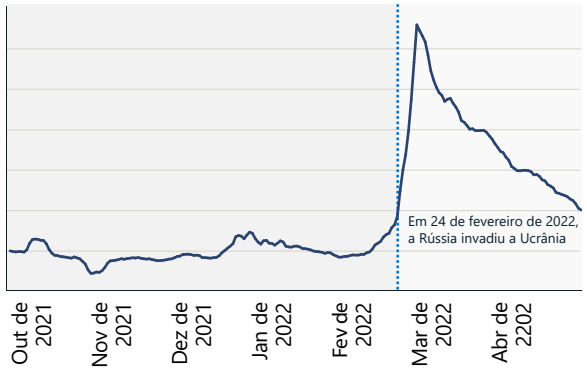
Continuação

Índice de Propaganda Russa: Ucrânia

Quando a guerra da Ucrânia começou, constatámos um aumento de 216% na propaganda russa, atingindo o pico a 2 de março. O gráfico abaixo mostra como este aumento repentino coincidiu com a invasão. Os dois gráficos mostram o súbito aumento da propaganda russa pouco depois da invasão.

RPI, Ucrânia

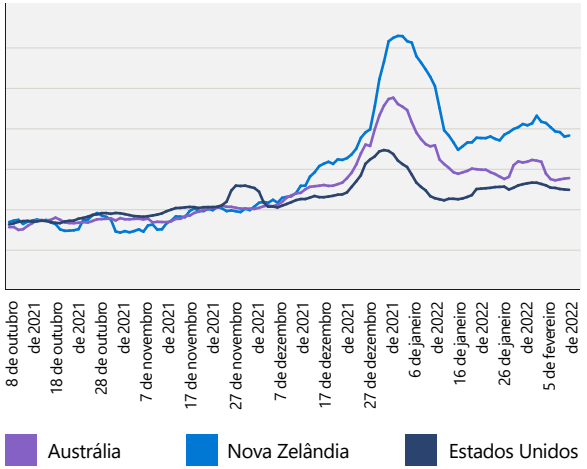
(7 de outubro de 2021 – 30 de abril de 2022)



Índice de Propaganda Russa: Nova Zelândia versus Austrália e Estados Unidos

Uma avaliação do RPI na Nova Zelândia mostrou um pico no final 2021 relacionado com a propaganda sobre a COVID-19. Este pico no consumo de propaganda russa na Nova Zelândia antecedeu uma onda de protestos públicos no início de 2022, em Wellington. Um segundo pico esteve claramente relacionado com a invasão russa da Ucrânia e excedeu os RPIs da Austrália e dos Estados Unidos.

RPI, Nova Zelândia versus Austrália e Estados Unidos



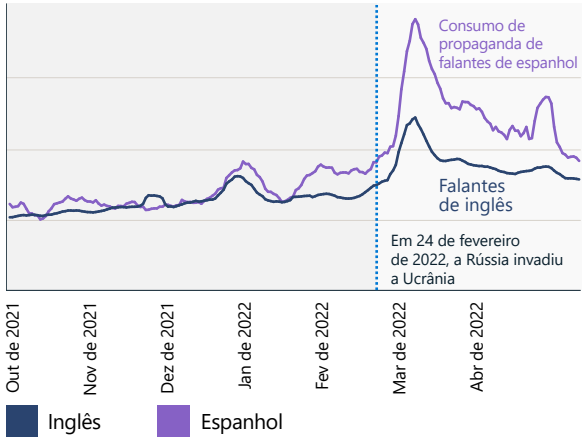
O consumo de propaganda russa na Nova Zelândia é semelhante ao da Austrália até à primeira semana de dezembro de 2021. Depois de dezembro, o consumo de propaganda russa na Nova Zelândia aumentou mais de 30% em relação ao consumo na Austrália e nos Estados Unidos.

Índice de Propaganda Russa nos Estados Unidos: inglês e espanhol

O RPI também monitoriza a propaganda em vários idiomas. Existem vários meios noticiosos, incluindo a RT e a Sputnik News, disponíveis em mais de 20 idiomas. Estes incluem: inglês, espanhol, alemão, francês, grego, italiano, checo, polaco, sérvio, letão, lituano, moldavo, bielorrusso, arménio, osseto, georgiano, azerbaijano, árabe, turco, persa e dari.

O gráfico seguinte mostra que o RPI para o noticiário em espanhol nos Estados Unidos é muito maior do que para o noticiário em inglês.

O consumo de propaganda russa é duas vezes superior entre os falantes de espanhol



O consumo de propaganda russa nos Estados Unidos é duas vezes superior entre os falantes de espanhol.

A propaganda russa é elevada na América Latina

A RT em espanhol é o canal de notícias internacional com o maior número de visualizações de páginas e seguidores do Facebook.

Fonte: Microsoft AI for Good Research Lab

Conteúdos multimédia sintéticos

Estamos a entrar numa era dourada para a criação e manipulação de conteúdos multimédia baseadas na IA. Os analistas da Microsoft observam que este fenómeno é impulsionado por duas tendências-chave: a proliferação de ferramentas e serviços de fácil utilização para criar artificialmente imagens, vídeos, áudio e texto sintéticos altamente realistas, bem como a capacidade de disseminar rapidamente conteúdos otimizados para audiências específicas.

Nenhum destes desenvolvimentos é inerentemente problemático por si só. A tecnologia baseada em IA pode ser utilizada para criar conteúdos digitais divertidos e entusiasmantes, seja para criar materiais puramente sintéticos ou para melhorar o material existente. Estas ferramentas estão a ser amplamente utilizadas pelas empresas para fins de publicidade e comunicação, bem como por indivíduos a fim de criar conteúdos envolventes para os seus seguidores. No entanto, os conteúdos multimédia sintéticos, quando criados e distribuídos com a intenção de causar danos, têm o potencial de provocar sérios prejuízos a indivíduos, às empresas, às instituições e à sociedade. A Microsoft tem sido uma força motriz no desenvolvimento de tecnologias e práticas, tanto internamente como em todo o ecossistema de conteúdos multimédia, para limitar estes danos.

Esta secção explora os insights da análise da Microsoft sobre o estado atual da tecnologia de vanguarda para a criação de conteúdos sintéticos prejudiciais, os problemas que podem surgir se este conteúdo for disseminado em larga escala e as mitigações técnicas que podem oferecer uma defesa contra as ciberameaças baseadas em conteúdos multimédia sintéticos.

Criar conteúdos multimédia sintéticos

O campo do texto e conteúdo multimédia sintéticos está a dar passos gigantes, à medida que as técnicas que antes só eram possíveis com os vastos recursos informáticos dos grandes estúdios de cinema estão agora integradas nas aplicações para telemóveis. Ao mesmo tempo, as ferramentas estão a tornar-se mais fáceis de utilizar e podem gerar conteúdo com um nível de realismo capaz de enganar até os especialistas forenses de multimédia. Estamos muito perto de chegar ao ponto em que qualquer pessoa pode criar um vídeo sintético de qualquer pessoa a dizer ou fazer algo. Não é insensato pensar que estamos a entrar numa era em que uma quantidade significativa do conteúdo que vemos online é total ou parcialmente sintética graças à utilização de técnicas de IA.

> Com a disponibilização de ferramentas mais sofisticadas, fáceis de utilizar e amplamente disponíveis, a criação de conteúdos multimédia sintéticos está a aumentar e, em breve, não será possível distingui-los da realidade.

Existem muitas ferramentas comerciais de edição de imagem, vídeo e áudio gratuitas e de alta qualidade. Estas ferramentas podem ser utilizadas para fazer alterações simples, mas potencialmente prejudiciais ao conteúdo digital, como adicionar texto enganador, trocar o rosto e remover ou alterar o contexto. Estas "cheap fakes" são amplamente utilizadas para disseminar conteúdos nefastos, promover ideologias políticas e comprometer reputações. Um exemplo bem conhecido é o vídeo de 2019[16] em que a Presidente da Câmara dos Comuns dos E.U.A., Nancy Pelosi, parece estar inebriada e com um discurso arrastado. Apesar de ter sido rapidamente apurado que a velocidade do vídeo havia sido retardada para criar o efeito, este "cheap fake" espalhou-se por todo o lado antes de o vídeo e o contexto originais verem a luz.

As abordagens mais sofisticadas à alteração de conteúdo multimédia incluem a aplicação de técnicas avançadas de IA para (a) criar conteúdos multimédia puramente sintéticos e (b) fazer edições mais sofisticadas de conteúdos multimédia existentes. O termo "deepfake" é muitas vezes utilizado para os conteúdos multimédia sintéticos criados com técnicas de IA de vanguarda (o nome provém das redes neurais profundas que, por vezes, são utilizadas). Estas tecnologias estão a ser desenvolvidas como aplicações, ferramentas e serviços autónomos e a ser integradas em ferramentas de edição open source e comerciais estabelecidas.

Estas tecnologias são transformadas em armas por atores de má índole com o objetivo de prejudicar indivíduos e instituições. Seguem-se alguns exemplos de técnicas de "deepfake":

- **Troca de rosto (vídeo, imagens):** substituição de um rosto por outro num vídeo. Esta técnica pode ser utilizada para tentar chantagear um indivíduo, uma empresa ou uma instituição ou para colocar indivíduos em situações ou locais embaraçosos.
- **"Puppeteering" (vídeo, imagens):** utilização de um vídeo para animar uma imagem fixa ou um segundo vídeo. Isto pode fazer com que pareça que um indivíduo disse algo embaraçoso ou enganador.
- **Redes generativas antagónicas (vídeo, imagens):** um conjunto de técnicas para gerar imagens fotorrealistas.
- **Modelos de transformadores (vídeo, imagens, texto):** criação de imagens avançadas a partir de descrições de texto.

Estas técnicas avançadas baseadas em IA ainda não são amplamente utilizadas nas campanhas de ciberinfluência da atualidade, mas é expectável que o problema aumente à medida que as ferramentas se forem tornando mais fáceis de utilizar e estiverem mais amplamente disponíveis.

O impacto da manipulação de conteúdos multimédia sintéticos

A utilização de operações de informação para causar danos ou ampliar a influência não é uma novidade. No entanto, a velocidade com que as informações podem alastrar e a nossa incapacidade para separar rapidamente os factos da ficção significam que o impacto e os danos causados pelas falsificações e por outros conteúdos multimédia maliciosos gerados de forma sintética podem ser muito maiores, como demonstrado com o exemplo de Nancy Pelosi.

Existem várias categorias de danos a considerar: manipulação do mercado, fraude de pagamentos, vishing, usurpação de identidades, danos à marca, danos à reputação e botnets. Muitas destas categorias têm relatado amplos exemplos reais, o que pode minar a nossa capacidade de separar os factos da ficção.

Uma ameaça a mais longo prazo e mais insidiosa é à nossa compreensão do que é verdadeiro se já não conseguirmos confiar naquilo que vemos e ouvimos. Devido a isto, qualquer imagem, áudio ou vídeo comprometedor de uma figura pública ou privada pode ser descartado como falso, um resultado conhecido como Liar's Dividend.[17] Pesquisas recentes[18] mostram que esta utilização abusiva da tecnologia já está em curso para atacar os sistemas financeiros, apesar de serem plausíveis muitos outros cenários de utilização abusiva.

Conteúdos multimédia sintéticos

Continuação

Detetar conteúdos multimédia sintéticos

Estão a decorrer esforços ao nível da indústria, do setor público e das instituições académicas para desenvolver melhores formas de detetar e mitigar os conteúdos multimédia sintéticos e restaurar a confiança. Existem vários caminhos promissores no horizonte, mas também obstáculos dignos de reflexão.

Uma das abordagens passa por criar sistemas baseados em IA capazes de identificar "falsidades", ou seja, sistemas essencialmente "defensivos" para combater os sistemas de IA ofensivos. Esta é uma área de investigação ativa na qual os sistemas atuais para a criação de áudio e vídeo sintéticos deixam os artefactos reveladores que podem ser detetados por analistas forenses de multimédia qualificados e ferramentas automatizadas.

Infelizmente, apesar de as falsificações atuais demonstrarem falhas reveladoras, os artefactos precisos tendem a ser específicos de uma ferramenta ou algoritmo em particular. Isto significa que a formação em falsificações conhecidas não é normalmente generalizada para outros algoritmos, conforme demonstrado num concurso aberto, ocorrido em 2020, para a criação de detetores de imagens deepfake.[19] É tentador aumentar o investimento no desenvolvimento de detetores mais avançados, mas a Microsoft tem sérias dúvidas de que tal irá resultar em melhorias significativas por duas razões:

Em primeiro lugar, dispomos de excelentes modelos físicos que refletem o mundo real. Os atuais criadores de conteúdos falsos fazem atalhos, o que resulta em artefactos detetáveis, mas os modelos mais recentes vão tornar-se cada vez mais realistas. Não há nada inerentemente especial numa cena do mundo real capturada por uma câmara que não possa ser modelada por um computador.

Em segundo lugar, os algoritmos avançados de criação de conteúdos falsos utilizam uma técnica denominada Redes Generativas Antagónicas (GANs) como parte do processo de criação. Uma GAN reproduz dois sistemas de IA antagónicos através de um gerador para criar o elemento falso e um discriminador para detetar imagens falsas e treinar o gerador. Qualquer investimento no desenvolvimento de um detetor melhor só irá permitir ao gerador melhorar a qualidade das falsificações.

Conteúdos multimédia sintéticos

Continuação

Proveniência dos ativos digitais

Se a deteção de falsificações não é fiável, o que pode ser feito para se proteger contra as utilizações nocivas dos meios de comunicação sintéticos? Uma tecnologia emergente importante é a proveniência digital, um mecanismo que permite aos criadores de meios de comunicação digitais certificarem um ativo e ajuda os consumidores a identificarem se o ativo digital foi ou não adulterado. A proveniência digital é particularmente importante no contexto das redes sociais nos dias de hoje, dada a velocidade com que os conteúdos conseguem percorrer a Internet e a oportunidade para os atores mal-intencionados de manipularem facilmente os conteúdos.

900%

de aumento na proliferação de deepfakes todos os anos desde 2019.[20]

A Tecnologia de Proveniência Digital é uma versão moderna da assinatura criptográfica de documentos, concebida para captar a origem, editar o histórico e os metadados dos objetos à medida que fluem na Internet dos dias de hoje. A visão e os métodos técnicos para permitir este tipo de certificação integral inviolável de meios de comunicação social foram desenvolvidos entre equipas de investigadores e cientistas na Microsoft. Co-lideramos uma parceria entre setores com o objetivo de dar vida à tecnologia de proveniência de meios de comunicação social no Project Origin (criado pela Microsoft, BBC, CBC/Radio-Canada e o The New York Times) e fazemos parte da Content Authenticity Initiative (criada pela Adobe). A Microsoft também trabalhou com parceiros em serviços multimédia e de tecnologia para criar a The Coalition for Content Provenance and Authenticity (C2PA). A C2PA é uma organização de normas que publicou, recentemente, a especificação de proveniência digital mais avançada a utilizar com ativos multimédia, incluindo imagens, vídeos, áudio e texto.

Um objeto compatível com C2PA contém um manifesto que protege o objeto e os metadados contra a adulteração, sendo o certificado que o acompanha que identifica o editor.

Os meios de comunicação sintéticos não foram, originalmente, criados para causar danos, mas estão a ser usados com arma pelos agentes mal-intencionados para minar a confiança nas pessoas e instituições.

A proveniência digital é uma tecnologia emergente promissora que tem o potencial de ajudar a restaurar a confiança das pessoas no conteúdo multimédia online, uma vez que certifica a origem de um ativo de multimédia.

As soluções disponíveis publicamente baseadas na especificação C2PA estão a surgir como uma nova funcionalidade nos produtos existentes ou em novas aplicações e serviços autónomos. Esperamos que a maioria das ferramentas de captura, edição e criação de aplicações mais utilizadas seja compatível com a C2PA dentro de alguns anos. Isto representa uma oportunidade para as empresas determinarem as suas necessidades e utilizações atuais para a proveniência digital e para solicitarem esta camada de proteção adicional nas ferramentas que utilizam nos workflows existentes.

Insights acionáveis

1. Tome medidas proativas para proteger a sua organização contra as ameaças de desinformação, através da ponderação proativa das suas respostas de comunicação e RP.
2. Utilize a tecnologia de proveniência para proteger as comunicações oficiais.

Ligações para mais informações

- Um passo promissor para a desinformação | Microsoft On the Issues
- A Milestone Reached, 31 de janeiro de 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Explore os detalhes técnicos sobre as utilizações do Project Origin do sistema para a autenticação dos meios de comunicação | Microsoft ALT Innovation

Uma abordagem holística para se proteger contra as operações de ciberinfluência

A Microsoft está a consolidar a sua infraestrutura de informações sobre ciberameaças já madura para desenvolver uma visão mais abrangente e inclusiva das operações de ciberinfluência.

Utilizamos uma estrutura para estratégias de resposta e mitigação sugeridas para combater a ameaça representada pelas operações. Esta estrutura pode ser dividida em quatro importantes pilares: detetar, perturbar, defender e impedir.

Além disso, a Microsoft adotou quatro princípios para ancorar o nosso trabalho neste espaço. Primeiro, é um compromisso para respeitar a liberdade de expressão e manter a capacidade dos nossos clientes para criar, publicar e procurar informações através das nossas plataformas, produtos e serviços. Em segundo lugar, trabalhamos proativamente para evitar que as nossas plataformas e produtos sejam utilizados para amplificar os conteúdos e sites de ciberinfluência estrangeiros. Em terceiro lugar, não iremos lucrar deliberadamente com atores ou conteúdos de ciberinfluência estrangeiros. Por fim, damos prioridade à deteção de conteúdos para combater as operações de ciberinfluência estrangeira, graças à utilização dados de terceiros, internos e fidedignos, sobre os nossos produtos.

Detetar

Tal como com a ciberdefesa, o primeiro passo para combater as operações de ciberinfluência estrangeira é desenvolver a capacidade de podermos detetá-las. Nenhuma empresa ou organização sozinha consegue evoluir o necessário sem ajuda. Será crucial uma colaboração nova e mais alargada no setor tecnológico, com a evolução na análise e denúncia das operações de ciberinfluência a depender fortemente do papel da sociedade civil, incluindo instituições académicas e organizações sem fins lucrativos.

Ao reconhecerem este papel, os investigadores Jake Shapiro e Alicia Wanless, da Universidade de Princeton e do Carnegie Endowment for International Peace, respetivamente, definiram os planos para lançar o novo "Institute for Research on the Information Environment" (IRIE). Com o apoio da Microsoft, da Knight Foundation e da Craig Newmark Philanthropies, a IRIE irá criar uma instituição de investigação inclusiva com vários intervenientes com base no modelo da Organização Europeia para a Pesquisa Nuclear (CERN). A instituição irá combinar a especialização no processamento e análise de dados para acelerar e escalar novas descobertas neste espaço. Os resultados serão partilhados, de forma mais ampla, com políticos, empresas tecnológicas e consumidores.

Defender

O segundo pilar estratégico consiste em reforçar as defesas democráticas, uma prioridade de longa data que precisa de investimento e inovação. Deve ter em conta os desafios que a tecnologia criou para a democracia e as oportunidades que a mesma criou para defender as sociedades democráticas de forma mais eficaz.

O modelo estratégico da Microsoft visa ajudar os intervenientes de vários setores a detetar, perturbar, defender e impedir a propaganda, nomeadamente campanhas de agressores estrangeiros.

É adequado começar por um dos grandes desafios tecnológicos da nossa era: o impacto da Internet e da publicidade digital no jornalismo tradicional. Desde o século XVIII que uma imprensa livre e independente tem desempenhado um papel especial no apoio a cada democracia no planeta: descobrir corrupção, documentar guerras e realçar os maiores desafios sociais da atualidade e do passado. No entanto, a Internet tem arrasado os meios de comunicação locais, devorando as receitas publicitárias e atraindo subscritores pagos. Muitos jornais locais colapsaram. Um dos muitos insights no nosso trabalho mais recente é que as cidades que não têm um jornal estão inevitavelmente, e sem saberem, muito mais expostas a propaganda estrangeira do que a média. Por estas razões, um dos pilares de defesa críticos da democracia tem de ser o reforço do jornalismo tradicional e uma imprensa livre, sobretudo a nível local. Isto exige investimento e inovação contínuos que têm de refletir as necessidades locais dos diferentes países e continentes. Estes problemas não são fáceis de resolver e requerem abordagens com vários intervenientes, que a Microsoft e outras empresas de tecnologia estão, cada vez mais, a apoiar.

Também precisamos de novas inovações nas políticas públicas, o que tem de ser uma prioridade pública. Isto pode incluir leis que permitam aos editores negociarem as receitas publicitárias coletivamente com empresas de tecnologia e legislação que forneça benefícios fiscais para aliviar as redações locais, nomeadamente sobre a sua parte dos impostos sobre os salários dos jornalistas que empregam. Os jornalistas precisam de muitas outras ferramentas para trabalhar, incluindo a capacidade de separar os conteúdos de origens legítimas e fraudulentas.

Existe também uma necessidade cada vez mais célere de ajudar os consumidores a desenvolverem uma capacidade mais sofisticada de identificar as operações de informação orientadas por estados-nação. Apesar de isto poder parecer assustador, é muito parecido com o trabalho que o setor tecnológico tem feito para combater outras ciberameaças. Considere educar os consumidores para olharem mais atentamente para um endereço de e-mail, de forma a ajudar a identificar spam ou outras comunicações fraudulentas. Tenha como exemplo iniciativas nos Estados Unidos, como o projeto News Literacy Project e o Trusted Journalism.

Uma ameaça a mais longo prazo e mais insidiosa é à nossa compreensão do que é verdadeiro se já não conseguirmos confiar naquilo que vemos e ouvimos.

Uma abordagem holística para se proteger contra as operações de ciberinfluência

Continuação

Program: ambos estão a ajudar a desenvolver consumidores mais bem informados sobre as notícias e a informação. Globalmente, as novas tecnologias, como o plug-in de browser da NewsGuard, podem ajudar a fazer avançar este esforço muito mais depressa.

Isto também deve lembrar-nos de que parte das bases da democracia passa por uma educação cívica. Como sempre, este esforço tem de começar nas escolas. Contudo, vivemos num mundo que exige uma educação cívica contínua ao longo da nossa vida. O novo compromisso Civics at Work, liderado pelo Center for Strategic and International Studies, e do qual a Microsoft foi signatária e parceira desde o início, procura revitalizar a literacia cívica nas comunidades empresariais. Este é um bom exemplo da amplitude de oportunidades para reforçar as nossas defesas democráticas.

Perturbar

Nos últimos anos, a Unidade de Crimes Digitais (DCU) da Microsoft aperfeiçoou as táticas e desenvolveu ferramentas para perturbar as ciberameaças que vão desde o ransomware aos botnets e ataques de estados-nação. Aprendemos muitas lições importantes, começando pelo papel da perturbação ativa na luta contra um vasto leque de ciberataques.

À medida que pensamos em combater as operações de ciberinfluência, a perturbação pode desempenhar um papel ainda mais importante e a melhor abordagem às perturbações está a tornar-se mais clara. O antídoto mais eficaz para a maior das mentiras é a transparência. Por isso, a Microsoft aumentou a sua capacidade de detetar e perturbar as operações de ciberinfluência de estados-nação através da aquisição da Miburo Solutions, uma empresa líder em análise e investigação de ciberameaças especializada na deteção e resposta a operações de ciberinfluência estrangeira.

A nossa experiência demonstrou que os governos, empresas de tecnologia e ONGs devem atribuir os ciberataques de forma cuidadosa e com base em muitas provas. Compreender o impacto destas perturbações é vital e pode ser ainda mais útil para perturbar a ciberinfluência. Veja a partilha de informações do governo dos EUA, no período que antecedeu a invasão da Rússia na Ucrânia, como um bom exemplo de como usar a transparência de forma eficaz: expor os planos russos, incluindo campanhas específicas, como um plano para utilizar um vídeo falso.

Tal como mostrado na publicação do CyberPeace Institute no último verão, em Genebra, sobre os ciberataques contínuos dentro e fora da Ucrânia, existe uma oportunidade para um grande número de organizações da sociedade civil e do setor privado de promover a transparência relacionada com as operações de ciberinfluência. Relatórios fiáveis sobre as operações recém-descobertas e bem documentadas podem ajudar o público a avaliar melhor o que lê, vê e ouve, sobretudo na Internet. Para este efeito, a Microsoft irá criar e expandir os relatórios cibernéticos existentes e lançar novos relatórios, dados e atualizações relacionados com o que descobrimos sobre as operações de ciberinfluência, incluindo as declarações de atribuição, quando apropriado. Publicaremos um relatório anual que utiliza uma abordagem orientada por dados para analisar a prevalência de operações de informação estrangeiras na empresa e os próximos passos para assegurar uma melhoria incremental. Também vamos considerar os passos adicionais que se baseiam neste tipo de transparência.

O papel da publicidade digital é especialmente importante, uma vez que a publicidade pode, por exemplo, ajudar a financiar as operações externas, ao mesmo tempo que cria uma aparência de legitimidade para os sites de propaganda patrocinados por estrangeiros. Serão necessários novos esforços para perturbar estes fluxos financeiros.

Impedir

Por fim, não podemos esperar que as nações alterem o comportamento se não houver responsabilização pela violação das regras internacionais. A imposição dessa responsabilização é uma responsabilidade exclusivamente governamental. No entanto, as ações dos vários intervenientes estão, cada vez mais, a desempenhar um papel importante no fortalecimento e alargamento das normas internacionais. Mais de 30 plataformas online, anunciantes e editores, incluindo a Microsoft, assinaram o Código de Conduta sobre Desinformação, recentemente atualizado, da Comissão Europeia, concordando em reforçar os compromissos para enfrentar este desafio cada vez maior. Como no recente Paris Call, Christchurch Call e na Declaração para o Futuro da Internet, a ação multilateral e com vários intervenientes pode unir os governos e o público entre as nações democráticas. Os governos podem, depois, basear-se nestas normas e leis para promoverem a responsabilização que as democracias do mundo precisam e merecem.

Através da rápida transparência radical, os governos e as sociedades democráticas podem, efetivamente e sem rodeios, influenciar as campanhas ao atribuir a origem dos ataques de estados-nação, informar o público e construir a confiança nas instituições.

Aumentámos a capacidade técnica para detetar e perturbar as operações de influência estrangeira e estamos empenhados em denunciar, de forma transparente, estas operações, como nos nossos relatórios sobre ciberataques.

Insights acionáveis

1. Implemente práticas de higiene digital sólidas em toda a sua organização.
2. Considere formas de reduzir qualquer ativação indesejada de campanhas de ciberinfluência por parte dos seus colaboradores ou das suas práticas empresariais. Isto inclui a redução do fornecimento a conhecidos sites de propaganda estrangeiros.
3. Apoie a literacia informativa e as campanhas de interação cívica como um componente fundamental para ajudar as sociedades a defenderem-se contra a propaganda e influência estrangeiras.
4. Interaja diretamente com grupos relevantes para o seu setor que lidem com operações de influência.

Notas finais

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. Defender a Ucrânia: as primeiras lições da ciberguerra (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Porta-voz do Ministério dos Negócios Estrangeiros da Rússia, 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. Alegações da Rússia sobre Kremenchuk versus as Provas - bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Verificação de factos: Vídeo de Nancy Pelosi "embriagada" é manipulado | 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. Resultados do desafio de deteção do deepfakes: uma iniciativa aberta para promover a IA (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas e Kristjan Peterson, outubro de 2020

Resiliência Cibernética

Compreender os riscos e recompensas da modernização torna-se crucial para uma abordagem holística à resiliência.

Uma descrição geral da

Resiliência Cibernética

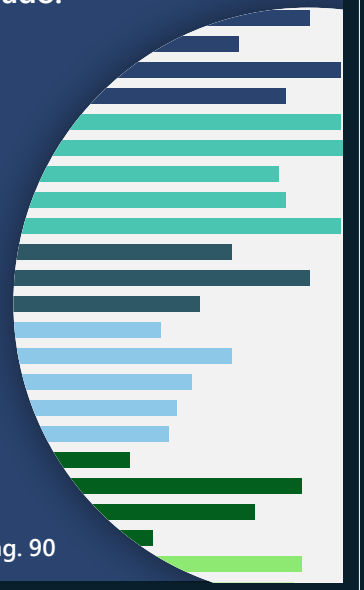
A cibersegurança é um fator-chave para o sucesso tecnológico. A inovação e a melhoria da produtividade só podem ser alcançadas através da introdução de medidas de segurança que tornem as organizações o mais resilientes possível contra ataques modernos.

A pandemia desafiou-os a mudar as nossas práticas e tecnologias de segurança para proteger os colaboradores da Microsoft onde quer que estivessem a trabalhar. No ano passado, os atores de ameaças continuaram a tirar partido das vulnerabilidades expostas durante a pandemia e da mudança para um ambiente de trabalho híbrido. Desde então que o nosso principal desafio tem sido gerir a prevalência e a complexidade de vários métodos de ataque e aumentar a atividade do estadonação.

A resiliência cibernética eficaz exige uma abordagem holística e adaptável para enfrentar as ameaças em mudança aos principais serviços e infraestruturas.

Saiba mais na pág. 89

Os sistemas e a arquitetura modernizados são importantes para gerir as ameaças num mundo hiperligado.

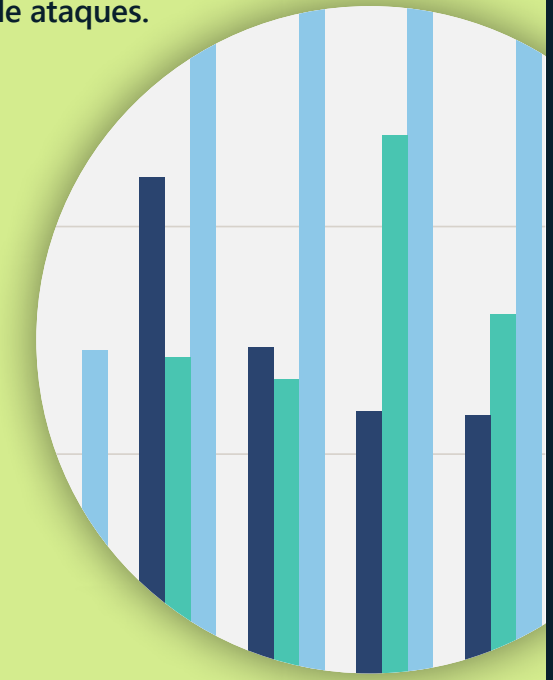


Saiba mais na pág. 90

A postura de segurança básica é um fator determinante na eficácia de soluções avançadas.

Saiba mais na pág. 92

Apesar de os ataques baseados nas palavras-passe continuarem a ser a principal fonte de violação de identidade, estão a surgir outros tipos de ataques.



Saiba mais na pág. 93

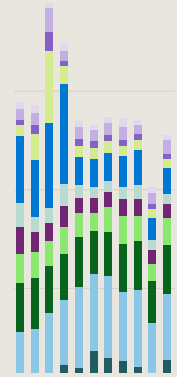
A dimensão humana de resiliência nas operações de ciberinfluência é a nossa capacidade de colaborar e cooperar.

Saiba mais na pág. 102

A grande maioria dos ciberataques bem-sucedidos pode ser evitada graças da higiene de segurança básica.

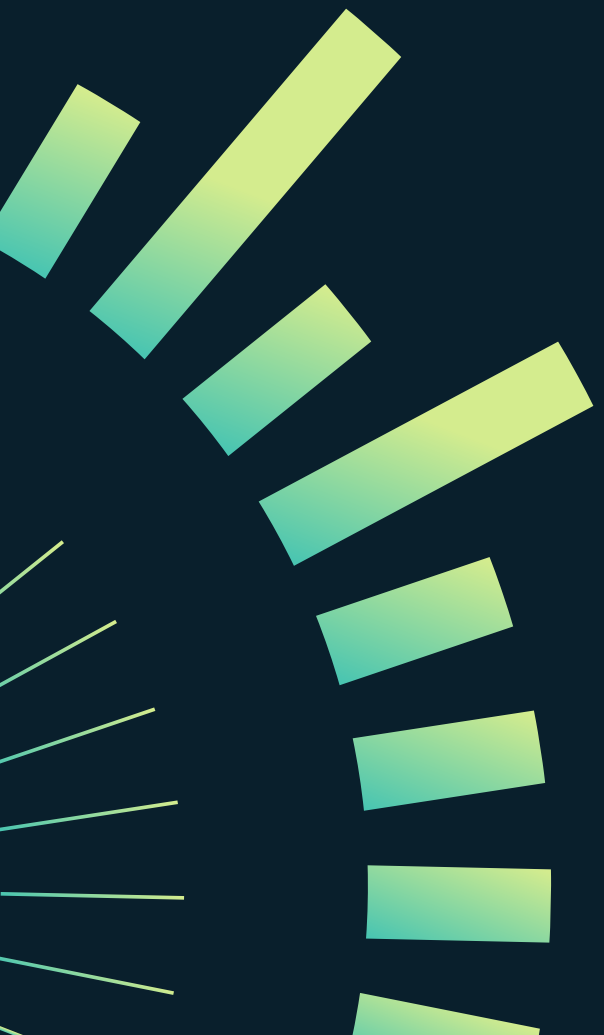
Saiba mais na pág. 108

No ano passado, o mundo viu um volume, complexidade e frequência de ataques DDoS sem precedentes.



Saiba mais na pág. 98

Introdução



A pandemia desafiou-nos a mudar as nossas práticas e tecnologias de segurança para proteger os colaboradores da Microsoft onde quer que estivessem a trabalhar. No ano passado, os atores de ameaças continuaram a tirar partido das vulnerabilidades expostas durante a pandemia e da mudança para um ambiente de trabalho híbrido. Desde então que o nosso principal desafio tem sido gerir a prevalência e a complexidade de vários métodos de ataque e aumentar a atividade do Estado-nação.

A atividade de ameaças digitais e o nível de sofisticação dos ciberataques aumenta a cada dia. Muitos dos ataques complexos dos nossos dias concentram-se em comprometer arquiteturas de identidades, cadeias de fornecimento e terceiros com diferentes níveis de controlos de segurança. Observámos que os ataques de phishing de identidades são, em especial, uma ameaça clara e presente. No entanto, estes tipos de ataques são, geralmente, efetuados sem sucesso graças a uma boa gestão da identidade, controlo de phishing e práticas de gestão de endpoint. Como resultado, temos de nos lembrar das noções básicas: noventa e oito por cento dos ataques podem ser interrompidos com medidas de higiene básica em vigor. Na Microsoft, gerimos as identidades e os dispositivos como parte da nossa abordagem de Confiança Zero, que inclui um acesso mais restrito e credenciais resistentes ao phishing, de forma a impedir eficazmente os perpetradores e manter os nossos dados protegidos.

Hoje em dia, mesmo os atores de ameaças com poucas competências técnicas sofisticadas podem lançar ataques incrivelmente destrutivos, uma vez que o acesso a táticas, técnicas e procedimentos avançados estão amplamente disponíveis na economia do cibercrime. A guerra na Ucrânia demonstrou como os agentes dos estados-nação escalaram as suas operações cibernéticas ofensivas através da crescente utilização do ransomware. O ransomware é, agora, uma indústria sofisticada com atores de ameaças que utilizam táticas de extorsão duplas ou triplas para obterem resgates e programadores que oferecem ransomware como serviço (RaaS). Com o RaaS, os atores de ameaças utilizam uma rede de afiliados para executar ataques, reduzindo as barreiras para a entrada de cibercriminosos menos qualificados e, em último caso, para expandir o conjunto de atacantes.

Em consequência disso, a Microsoft criou um programa de eliminação de ransomware. O objetivo do programa é preencher as lacunas nos controlos e na proteção, contribuir para as melhorias das funcionalidades nos serviços e desenvolver manuais de procedimento de recuperação para o nosso centro de operações de segurança e equipas de engenharia no caso de um ataque de ransomware.

A recente cadeia de fornecimento e os ataques de fornecedores de terceiros indicam um importante ponto de inflexão no setor. A perturbação que estes ataques causam aos nossos clientes, parceiros, governos e à Microsoft continua a aumentar, ilustrando a importância da atenção focada na ciber-resiliência e na colaboração entre os intervenientes na segurança. Os adversários também estão a visar os sistemas on-premises, reforçando a necessidade de as organizações gerirem as vulnerabilidades existentes nos sistemas legados através da modernização e migração da infraestrutura para a cloud, onde a segurança é mais robusta.

Vivemos numa era em que a segurança é um fator-chave para o sucesso tecnológico. A inovação e a melhoria da produtividade só podem ser alcançadas através da introdução de medidas de segurança que tornem as organizações o mais resilientes possível contra ataques modernos. À medida que as ameaças digitais aumentam e evoluem, é essencial criar uma ciber-resiliência no tecido de cada organização.

Bret Arsenault
Diretor Executivo de Segurança Informática

Resiliência Cibernética: Um alicerce fundamental de uma sociedade interligada

A revolução na tecnologia digital tem visto as organizações a transformarem-se para estarem, cada vez mais, interligadas na forma como operam e nos serviços que oferecem. À medida que as ameaças no panorama cibernético aumentam, a criação de ciber-resiliência no tecido da organização é tão crucial como a resiliência financeira e operacional.

A transformação digital alterou para sempre a forma como as organizações interagem com os clientes, parceiros, colaboradores e outros intervenientes. As novas tecnologias oferecem enormes oportunidades para interagir com as pessoas, transformar produtos e otimizar as operações. A pandemia acelerou a transformação digital ao impulsionar tecnologias inovadoras que permitem às pessoas colaborar através de novas formas e a partir de qualquer local.

À medida que as ciberameaças se tornam endémicas, impedir que estas criem problemas numa organização torna-se mais difícil no nosso mundo "sempre interligado". A ciber-resiliência representa a capacidade de uma organização em continuar as operações e manter a aceleração do crescimento, apesar do conjunto de ataques. A prevenção tem de ser equilibrada com as capacidades de sobrevivência e recuperação, sendo que os governos e as empresas estão a desenvolver modelos abrangentes, que vão além da segurança e da privacidade, para proteger ativos, dados e outras funcionalidades como parte da ciber-resiliência.

Desenvolver uma abordagem holística de resiliência cibernética

A ciber-resiliência exige uma abordagem holística, adaptável e global que possa enfrentar as ameaças em mudança aos principais serviços e infraestruturas, incluindo:

- Higiene cibernética básica, tal como descrito na nossa curva do sino da resiliência cibernética.
- Compreender e gerir o equilíbrio risco/benefício da transformação digital.
- Capacidades de resposta em tempo real que permitam a deteção proativa de ameaças e vulnerabilidades.
- Proteção contra ataques conhecidos e atividade preventiva contra vetores de ataque novos e antecipados, incluindo a capacidade de remediação automática.
- Redução do impacto de ataques e catástrofes através da segmentação e isolamento de falhas.
- Recuperação automatizada e redundância em caso de perturbação.
- Dar prioridade aos testes operacionais para encontrar lacunas e compreender as responsabilidades partilhadas e dependências em recursos externos, como as soluções de segurança baseadas na cloud.

Um programa de ciber-resiliência eficaz começa com as noções básicas dos recursos, como saber quais os serviços que estão disponíveis e ter um catálogo de recursos fiável que possa ser utilizado em caso de perturbação. Com base nesse alicerce, o programa tem de ser capaz de avaliar a sua própria eficácia, medir o desempenho dos serviços críticos e das suas dependências, testar e validar as capacidades nos serviços on-premises e da cloud, para além de impulsionar a melhoria contínua em todo o ciclo de vida digital da organização.

Para oferecer uma abordagem holística, estamos a estabelecer uma parceria com as organizações para identificar os seus serviços on-premises e online mais críticos, processos de negócio, dependências, colaboradores e fornecedores. Também procuramos identificar os ativos e os recursos associados às expectativas dos clientes e do mercado, às obrigações legais e contratuais e às operações internas. À medida que estes recursos críticos são identificados, os esforços paralelos devem detetar e monitorizar ameaças, perturbações, potenciais vetores de ataque e vulnerabilidades do sistema e dos processos. A capacidade de fazer isto com a atual falta de competências exige rigor na definição de prioridades com base no risco global a que a organização está exposta.

Este tipo de abordagem holística tem de ser versátil num panorama de ameaças em constante mudança, cujo objetivo é o de impulsionar o aumento mensurável do desempenho, reduzir o tempo de deteção, resposta e recuperação, bem como a redução do impacto na existência de perturbações. A abordagem também tem de reconhecer a crescente conectividade das ameaças. Por exemplo, um incidente de segurança pode resultar numa violação de dados com implicações para a privacidade, o que exige que muitas equipas internas e externas trabalhem em conjunto para responder rapidamente ao incidente e minimizar o seu impacto.

A resiliência cibernética é a capacidade que uma empresa tem para continuar as operações e manter a aceleração do crescimento apesar das perturbações, como os ciberataques.

Insights acionáveis

1. Crie e faça a gestão de sistemas tecnológicos que limitem o impacto de uma violação e permita que continuem a operar de forma segura e eficaz, mesmo que uma violação seja bem-sucedida. Concentre-se nos ativos críticos comuns, dê apoio para a agilidade e construa uma arquitetura para versatilidade (por exemplo, sistema híbrido e multicloud, multiplataforma), reduza as superfícies de ataque (por exemplo, remova as aplicações não utilizadas e os direitos de acesso sobredimensionados), assuma os recursos comprometidos e espere que os adversários evoluam.
2. Ao planear projetos digitais, considere potenciais ameaças e oportunidades e as responsabilidades partilhadas para a resiliência na cadeia de fornecimento de tecnologia digital, incluindo as soluções de segurança baseadas na cloud.
3. Crie sistemas para segurança integrada por design e tome medidas para antecipar, detetar, suportar, adaptar e responder às futuras ameaças em mudança.
4. Certifique-se de que os líderes empresariais consultam as equipas de segurança, sempre que necessário, para compreenderem os riscos associados aos novos desenvolvimentos. Da mesma forma, as equipas de segurança devem considerar os objetivos do negócio e aconselhar os líderes sobre como os alcançar os mesmos em segurança.
5. Certifique-se de que as práticas e os procedimentos operacionais claros para a resiliência organizacional estão em vigor para ciberincidentes.

A importância da modernização dos sistemas e da arquitetura

À medida que desenvolvemos novas funcionalidades para um mundo hiperligado, temos de gerir as ameaças impostas pelos sistemas e software legados.

Os sistemas legados - todos os sistemas desenvolvidos antes das modernas ferramentas de conectividade, como smartphones, tablets e serviços de cloud, se terem tornado a norma – representam um risco para uma organização que continue a utilizá-los. Esta exposição ao risco é reforçada pelas conclusões da equipa de Serviços de Segurança da Microsoft para Resposta a Incidentes, um grupo de profissionais de segurança que ajuda os clientes a responderem e recuperarem de ataques.

No último ano, os problemas encontrados entre os clientes que recuperaram de ataques estavam relacionados com seis categorias, tal como é mostrado no gráfico desta página. A página seguinte descreve os passos concretos a dar para melhorar a resiliência.

Cerca de 80% dos incidentes de segurança podem ser detetados em alguns elementos em falta que podem ser resolvidos através de abordagens de segurança modernas.

Principais problemas que afetam a ciber-resiliência

Este gráfico mostra a percentagem de clientes afetados em que faltam controlos de segurança básicos fundamentais para aumentar a ciber-resiliência organizacional. Os resultados baseiam-se nas interações da Microsoft durante o ano passado.

"Os líderes devem pensar na resiliência cibernética como uma parte crítica da resiliência da empresa. Devem planear as perturbações cibernéticas da mesma forma que o fazem para as catástrofes naturais ou outros eventos imprevistos e reunir equipas internas, como as do departamento de operações, de comunicações, jurídico entre outros, para criarem estratégias. Isto irá ajudar a assegurar que as organizações voltam a colocar os seus sistemas empresariais críticos online o mais rapidamente possível, de forma a retomar as operações normais da empresa.

Mas não fica por aqui. Como muitas organizações dependem de fornecedores de serviços e externos, os líderes devem expandir o planeamento da resiliência cibernética para a sua cadeia de valor integral, de forma a assegurar, ainda mais, a continuidade e a resiliência do negócio."

Ann Johnson,
Vice-presidente empresarial de segurança, conformidade e identidade e de gestão do desenvolvimento do negócio

A importância da modernização dos sistemas e da arquitetura

Continuação

Existem áreas claras que as organizações podem analisar de forma a modernizarem a sua abordagem e protegerem-se contra ameaças:

Problema	Passos concretos
Configuração insegura do fornecedor de identidade A configuração incorreta e a exposição das plataformas de identidade e dos seus componentes são um vetor comum para obter um acesso não autorizado a privilégios restritos.	Siga as linhas de base de configuração de segurança e as melhores práticas quando implementar e fizer a manutenção de sistemas de identidade, como o AD e a infraestrutura do Azure AD. Implemente as restrições de acesso através da segregação de privilégios, do acesso com privilégios reduzidos e da utilização de estações de trabalho com acesso privilegiado (PAW) para a gestão de sistemas de identidades.
Acesso com privilégios insuficientes e controlos de movimentos laterais Os administradores têm permissões excessivas em todo o ambiente digital e expõem, muitas das vezes, as credenciais administrativas em estações de trabalho sujeitas a riscos de produtividade e da Internet.	Proteja e limite o acesso administrativo para tornar o ambiente mais resiliente e limite a extensão de um ataque. Empregue controlos de gestão de acessos privilegiados, como o acesso just-in-time e a administração just enough.
Nenhuma autenticação multifator (MFA) Os hackers de hoje não forçam a entrada, iniciam sessão.	A MFA é um controlo de acesso de utilizadores vital e crítico que todas as organizações devem ativar. Juntamente com o acesso condicionado, a MFA pode ser inestimável na luta contra as ciberameaças.
Operações de segurança com baixa maturidade A maioria das organizações afetadas utilizou ferramentas tradicionais de deteção de ameaças e não tinham insights relevantes para uma resposta e remediação atempadas.	Uma estratégia de deteção de ameaças abrangente exige investimentos em deteção e resposta alargada (XDR) e ferramentas nativas da cloud modernas que usem machine learning para separar o ruído dos sinais. Modernize as ferramentas de operações de segurança incorporando a XDR, que pode fornecer insights de segurança profundos em todo o ambiente digital.
Falta de controlo da proteção das informações As organizações continuam a lutar por reunir controlos holísticos para a proteção das informações que tenham cobertura total em localizações de dados e que continuem eficazes ao longo do ciclo de vida das informações, bem como estarem alinhados com a importância dos dados da empresa.	Identifique os dados da sua empresa que sejam críticos e onde se encontram localizados. Analise os processos de ciclo de vida das informações e implemente a proteção dos dados, assegurando, ao mesmo tempo, a continuidade do negócio.
Adoção limitada de estruturas de segurança modernas A identidade é o novo perímetro de segurança, que permite o acesso a diferentes ambientes de computação e serviços digitais. Ao serem integrados os princípios de Confiança Zero, a segurança das aplicações e outros sistemas de cibersegurança modernos, isto permite às organizações gerirem proativamente os riscos que, de outra forma, as mesmas poderiam ter dificuldade em imaginar.	As estruturas de Confiança Zero impõem conceitos com privilégios reduzidos, a verificação explícita de todos os acessos e assumem sempre a possibilidade dos sistemas serem corrompidos. As organizações também devem implementar controlos e práticas de segurança nos processos de ciclo de vida das aplicações e DevOps para obterem níveis de fiabilidade mais elevados nos seus sistemas empresariais.

A postura de segurança básica é um fator determinante na eficácia de soluções avançadas

Através da nossa análise, descobrimos uma predominância de ângulos mortos comuns nas defesas organizacionais que permitem aos atacantes obter o acesso inicial, estabelecer um ponto de apoio e lançar um ataque, mesmo na presença de soluções de segurança avançada.

Em muitos dos casos, o resultado de um ciberataque é determinado muito antes do início do ataque. Os hackers aproveitam os ambientes vulneráveis para obterem o acesso inicial, executarem atividades de vigilância e causarem estragos através de movimentos laterais e encriptação ou fugas. Parar um hacker numa fase inicial aumenta consideravelmente a oportunidade de reduzir o impacto global.

Microsoft estudou configurações específicas em posturas de segurança para identificar as lacunas mais comuns na realidade nestes ambientes. Isto permitiu-nos ver as vulnerabilidades mais comuns exploradas durante os ataques de ransomware perpetrados por humanos, em que os atores de ameaças obtiveram acesso e viajaram numa rede sem terem sido detetados.

As configurações de segurança básicas têm de ser ativadas

Os dispositivos de uma organização que não estejam integrados ou que estejam ultrapassados (tanto em relação às vulnerabilidades como ao estado do agente de segurança) servem como potenciais pontos de entrada e rotas de definição do acesso para os hackers. Constatámos que, apesar da garantia de que os dispositivos da organização estão integrados numa solução de resposta e deteção alargada[1] (EDR) e de plataforma de proteção de endpoints[2] (EPP) ser um passo importante, isso não invalida o surgimento ataques de ransomware.

As soluções avançadas, como a EDR e a EPP, são fundamentais para detetar um hacker no início do fluxo de ataque e permitir a remediação e proteção automáticas. No entanto, uma vez que estas soluções avançadas dependem de uma capacidade fundamental para detetar um ataque, elas exigem a ativação de configurações de segurança básicas. De facto, observámos uma predominância de cenários com soluções avançadas implementadas que foram prejudicadas pela ausência de configurações de segurança básicas.

As melhores práticas nas configurações de segurança são um dos maiores indicadores de resiliência do que o tempo de resposta dos analistas do centro de operações de segurança (SOC)

Observámos uma redução de 70% no tempo que leva um analista do SOC a visualizar e a agir num alerta relevante durante um período de seis meses em toda a nossa carteira de clientes e parceiros. Esta maior sensibilização é um bom sinal. No entanto, apesar da visibilidade da configuração de segurança ter melhorado o desempenho do analista do SOC, permitir a visibilidade do produto através da integração e atualização dos dispositivos da organização foi um bom indicador de uma prevenção bem-sucedida.

Riscos representados por dispositivos desconhecidos

Contrariamente às redes de cloud, onde os clientes sabem quais os ativos que estão a ser executados nos sistemas operativos, as redes on-premises podem ter uma grande variedade de dispositivos, como a IoT, ambientes de trabalho, servidores e dispositivos de rede que não são monitorizados ou geridos pela organização.

A rede empresarial média tem mais de 3.500 dispositivos interligados que não estão protegidos por um agente de EDR e podem ter acesso a recursos empresariais ou, até mesmo, a ativos de grande valor. O Microsoft Defender para Endpoint (MDE) utiliza a inspeção da rede para detetar os dispositivos e fornecer informações sobre as classificações do dispositivo às pessoas ligadas à rede, como o nome do dispositivo, a distribuição do sistema operativo e o tipo de dispositivo.

3.500

número médio de dispositivos interligados numa empresa que não estão protegidos por um agente de deteção e resposta de endpoints.

Para os dispositivos não suportados por um agente de EDR, saiba, pelo menos, da sua existência e tome medidas para protegê-los através da avaliação de vulnerabilidades, bem como colocar restrições no acesso à rede.

Insights acionáveis

1. Mesmo as soluções avançadas podem ser prejudicadas pela ausência de configurações de segurança básicas.
2. Invista nas melhores práticas nas configurações da postura de segurança para se proteger de futuros ataques. Estas definições básicas geram um enorme retorno do investimento em termos de capacidade de uma organização em se defender de ataques.
3. Integre todos os dispositivos aplicáveis a uma solução de EDR.
4. Certifique-se de que atualiza os agentes de segurança e assegura a proteção contra a adulteração, de forma a permitir uma maior visibilidade e todos os benefícios de proteção dos produtos.

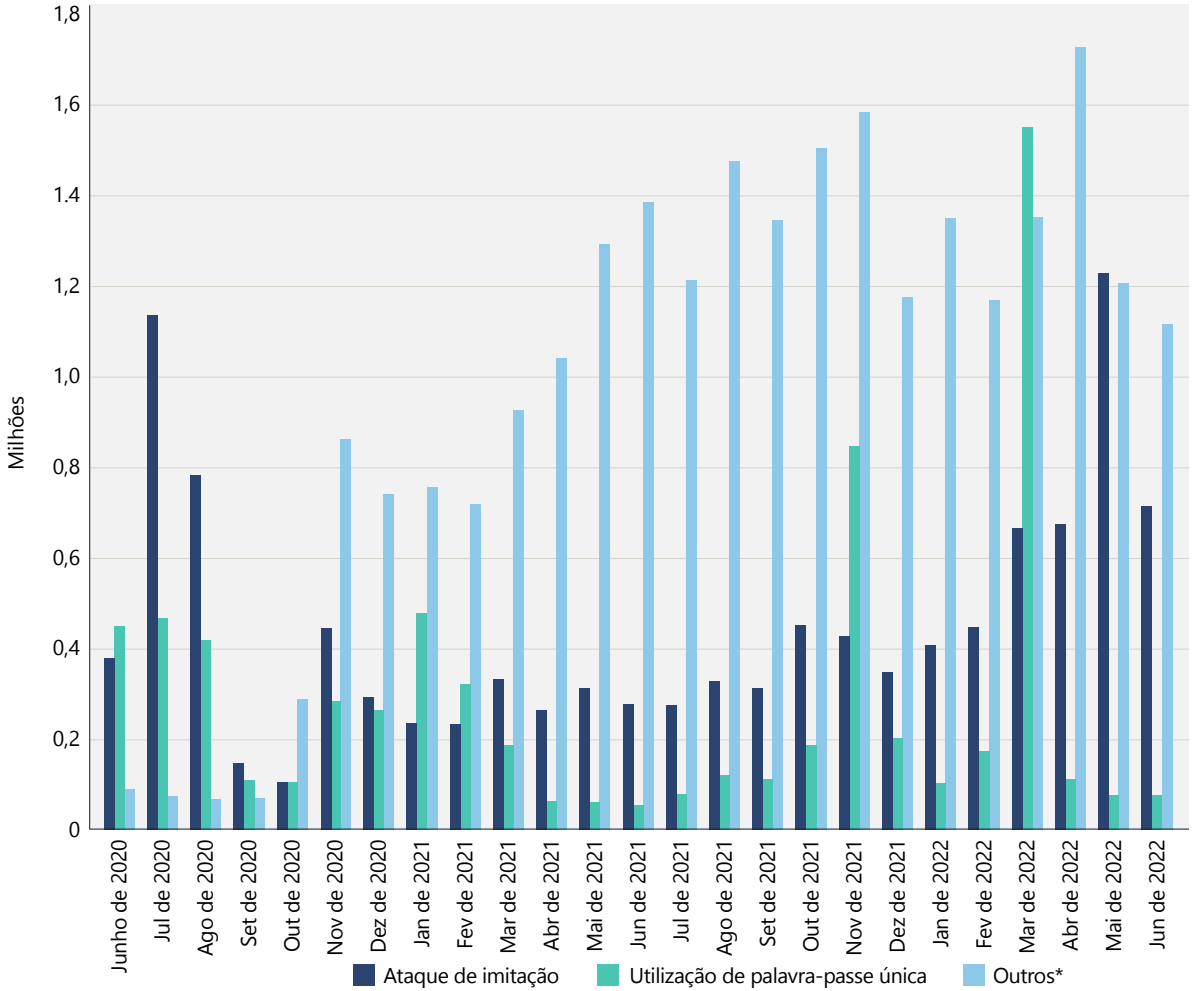
Manter a integridade da identidade é fundamental para o bem-estar organizacional

Salvaguardar a identidade é mais importante do que nunca. Apesar de os ataques baseados nas palavras-passe continuarem a ser a principal fonte de violação de identidade, estão a surgir outros tipos de ataques. O volume de ataques sofisticados continua a aumentar em relação à anterior norma de palavra-passe única e repetição de falhas de segurança.

Os ataques baseados em palavras-passe ainda são comuns e mais de 90% das contas comprometidas através destes métodos não estão protegidas com uma autenticação forte. A autenticação forte utiliza mais do que um fator de autenticação, por exemplo, palavra-passe + SMS e chaves de segurança FIDO2.

Temos visto um aumento nos ataques dirigidos à utilização de palavra-passe única, com grandes picos de volume de tráfego de hackers espalhados por milhares de endereços de IP.

Utilizadores comprometidos por categoria de ataque



Utilizadores comprometidos mensalmente por categoria de ataque. Os volumes de ataques por utilização de palavra-passe única foram altamente voláteis, como visto nos picos em novembro de 2021 de novembro e em março de 2022. Estes picos representam milhares de utilizadores e de endereços de IP atingidos. *"Outro" significa ataques diferentes dos ataques por utilização de palavra-passe e repetição de falhas de segurança, incluindo phishing, malware, man-in-the-middle, comprometimento do emissor de tokens on-premises, entre outros.
Fonte: Azure AD Identity Protection.

4.500

Enquanto está a ler esta afirmação, defendemos 4.500 ataques baseados na palavra-passe.

Manter a integridade da identidade é fundamental para o bem-estar organizacional

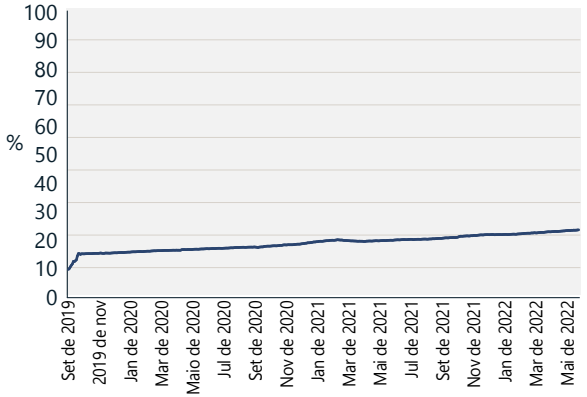
Continuação

Adoção da autenticação forte

Nem tudo são más notícias, pois estamos a ver um crescimento constante na adoção de uma autenticação forte entre a base de clientes empresariais do Azure Active Directory (Azure AD). Para o Azure AD, os utilizadores ativos mensais (MAU) com autenticação forte tiveram um crescimento de 19% para 26% no último ano, enquanto os MAU com autenticação forte para contas administrativas teve um crescimento de 30% para, aproximadamente, 33%.

Esta tendência é positiva, mas continua a ser necessário um crescimento significativo para atingir uma cobertura maior da autenticação forte. Os clientes que ainda não utilizam a autenticação forte nos seus ambientes devem iniciar o planeamento e a implementação de uma autenticação forte para protegerem os seus utilizadores.[3] Ao definir uma implementação de autenticação forte, deve ser considerada a autenticação sem palavras-passe, pois oferece a experiência de utilização mais segura, eliminando o risco de ataques baseados em palavraspasse.

Utilização de autenticação forte
(setembro de 2019 – maio 2022)

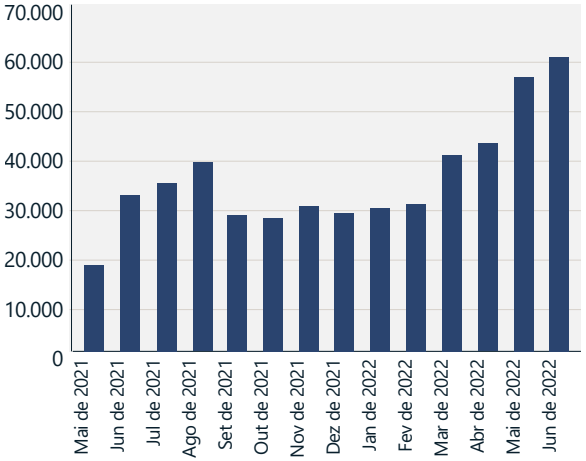


Apesar de a utilização de autenticação forte ter duplicado desde 2019, apenas 26% dos utilizadores e 33% dos administradores estão a utilizar uma autenticação forte. Fonte: Azure Active Directory.

Aumento constante dos ataques por repetição de tokens

A percentagem de outras formas de ataque aumentou em 2022. Vimos um aumento nos ataques direcionados que evitam, especificamente, a autenticação baseada em palavras-passe para reduzir a probabilidade de deteção. Estes ataques aproveitam os cookies de início de sessão único (SSO) do browser e os tokens de atualização obtidos através de malware, phishing e de outros métodos. Em alguns casos, os hackers escolhem infraestruturas em zonas perto da localização geográfica do utilizador escolhido, de forma a reduzir, ainda mais, as probabilidades de deteção. Assistimos a um aumento constante dos ataques por repetição de tokens, atingindo mais de 40.000 deteções por mês no Azure AD Identity Protection. A repetição de tokens é a utilização de tokens, que foram emitidos para um utilizador legítimo, por um hacker que possui os referidos tokens. Os tokens são, normalmente, obtidos através de malware, por exemplo, extraindo os cookies do browser do utilizador ou através de métodos avançados de phishing.

Volume de ataques por repetição de tokens detetados



Ataques por repetição de tokens detetados por mês. Fonte: Azure AD Identity Protection, sessões únicas marcadas pela deteção de tokens anómalos.

Manter a integridade da identidade é fundamental para o bem-estar organizacional

Continuação

Extrair tokens

Mais do que o malware, os hackers precisam de credenciais para atingirem os seus objetivos. De facto, 100% de todos os ataques de ransomware lançados por humanos incluem credenciais roubadas. Muitas intrusões sofisticadas incluem as credenciais adquiridas na dark web, inicialmente roubadas a partir de um malware de roubo de credenciais pouco sofisticado e amplamente distribuído. Esta classe de malware evoluiu para roubar tokens, incluindo as informações da sessão e os pedidos de MFA. Isto significa que as infeções nos sistemas domésticos, onde os utilizadores se ligam a ativos empresariais, podem causar incidentes graves nas redes empresariais.

Os atacantes também podem extrair tokens dos dispositivos das vítimas através de ataques man-in-the-middle, em que a vítima clica numa ligação maliciosa num e-mail ou mensagem instantânea de phishing e é encaminhada para um site semelhante ao da página de início de sessão legítima do fornecedor de identidade. Na realidade, é um serviço web lançado pelo hacker que reencaminha e interceta todo o tráfego entre o utilizador e o fornecedor de identidade. O hacker consegue intercetar o nome de utilizador e a palavra-passe e, também, reencaminhar os desafios da MFA. Os tokens gerados pelo fornecedor de identidade e intercetados pelo hacker podem conter pedidos de MFA passíveis de serem utilizados pelo hacker para satisfazer os requisitos da MFA.

O Microsoft Defender para aplicações na Cloud detetou, em média, 895 ataques por mês desde o início de 2022. Esta forma de ataque pode ser evitada através da utilização de fatores de MFA resistentes ao phishing, como a Autenticação Baseada em Certificados, o Windows Hello para empresas ou as chaves de segurança FIDO2.

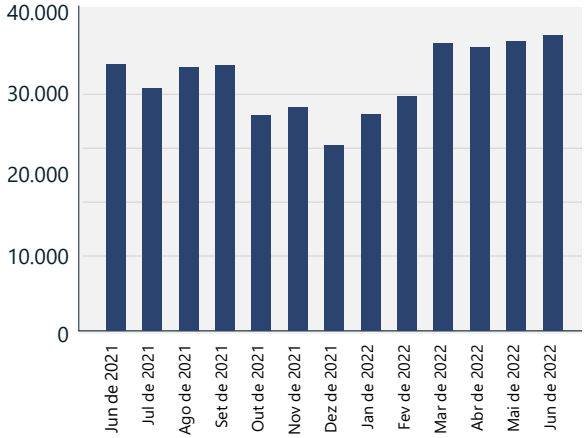
Os ataques baseados em palavras-passe são o método principal usado para corromper contas.

Fadiga de MFA

Utilizando o conceito de "fadiga de MFA", os hackers geram vários pedidos de MFA para o dispositivo da vítima, na esperança de que a vítima aceite o pedido inadvertidamente ou como resultado da fadiga. Este ataque pode ser evitado através da utilização de aplicações de autenticação modernas, como o Microsoft Authenticator, combinadas com funcionalidades como a correspondência de números[4] e a ativação de contexto adicional.[5] O Azure AD Identity Protection estimou que existem 30.000 ataques por fadiga de MFA por mês.

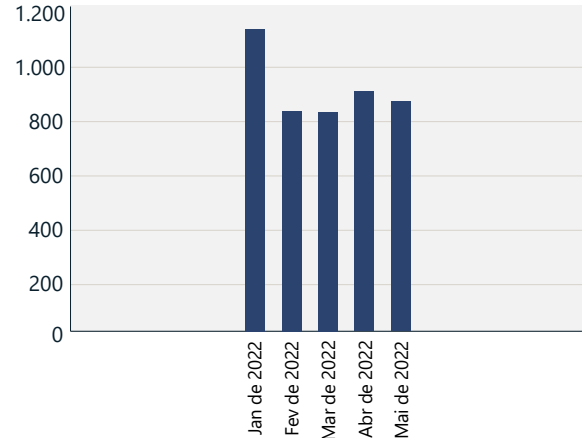
A percentagem de ataques sofisticados continua a aumentar, sublinhando a necessidade de fatores de autenticação multifator resistentes aos phishing.

Instâncias estimadas de ataques por fadiga de MFA



Fonte: Azure AD Identity Protection.

Instâncias de phishing detetadas seguidas por ataques man-in-the-middle



Fonte: Microsoft Defender para Aplicações na Cloud.

Insights acionáveis

1. Certifique-se de que todas as contas na sua organização estão protegidas por fortes medidas de autenticação.
2. A autenticação sem palavra-passe oferece a experiência mais segura e intuitiva, eliminando o risco de ataques a palavras-passe.
3. Desative a autenticação legada em toda a sua organização.
4. Proteja as contas mais valiosas e administrativas com formas de autenticação forte resistentes ao phishing.
5. Passe de um fornecedor de identidades on-premises para um fornecedor de identidades na cloud e ligue todas as suas aplicações ao fornecedor de identidades baseado na cloud para obter uma experiência de utilizador e segurança consistentes.

Ligações para mais informações

- Este Dia Mundial da Palavra-passe considera o abandono total da palavra-passe | Microsoft Security

Definições de segurança predefinidas do sistema operativo

Com o panorama de ameaças de segurança em constante mudança, vemos uma necessidade, cada vez maior, de ter segurança do computador configurada por predefinição para melhorar a ciber-resiliência. Apesar de a segurança do sistema operativo ser mais urgente, complexa e crítica para o negócio do que nunca, pode ser difícil a conseguir e gerir.

No passado, a segurança do computador e do dispositivo incluía funcionalidades de segurança incorporadas que o cliente ou profissional de TI deveria configurar com o nível pretendido. Esta abordagem já não é adequada, pois os hackers estão a utilizar ferramentas mais avançadas em automatização, infraestrutura na cloud e tecnologias de acesso remoto para atingirem os seus objetivos. Por isso, tornou-se fundamental que todas as camadas de segurança, desde o chip à cloud, sejam configuradas por predefinição. A Microsoft passou a configurar a segurança do sistema operativo Windows por predefinição.[6]

Os clientes que adotam a defesa — em profundidade, incluindo uma postura de segurança em camadas, novas funcionalidades de segurança, correções e atualizações regulares e consistentes, bem como formação e sensibilização na área da segurança para denunciar o phishing e outros esquemas fraudulentos – podem esperar menos malware.

Para simplificar a defesa em detalhe, o Windows 11 tem uma proteção de hardware e software totalmente integrada ativada por predefinição, incluindo a integridade da memória, Arranque Seguro e um Trusted Platform Module 2.0. Os utilizadores do Windows 10 com hardware compatível também podem ativar estes recursos na aplicação de Definições do Windows ou no menu da BIOS.

Regra geral, os dispositivos mais antigos não têm um alinhamento tão forte entre a segurança de hardware e as técnicas de segurança de software. Para dispositivos em que a segurança não está ativada por predefinição, configure-os manualmente nas definições, sempre que possível.[7]

Para dispositivos em que a segurança não está ativada por predefinição, a Microsoft recomenda que os configure manualmente nas definições, sempre que possível.

Seja proativo no que diz respeito à aplicação contínua de atualizações e correções de segurança do sistema operativo que ajudam a fornecer proteção ao longo do ciclo de vida do hardware e do software.

Insights acionáveis

1. Utilize uma solução sem palavra-passe que vincule as credenciais de início de sessão no Trusted Platform Module. Procure, em específico, uma solução sem palavra-passe que satisfaça a norma de indústria da Faster Identity Online (FIDO) Alliance[8].
2. Realize atempadamente a limpeza de todos os ficheiros executáveis não utilizados e obsoletos nos dispositivos das organizações.
3. Proteja-se de ataques avançados de firmware, ativando a integridade da memória, o Arranque Seguro e o Trusted Platform Module 2.0, se não estiverem ativados por predefinição. Estas funcionalidades reforçam o arranque utilizando capacidades integradas em CPUs modernos.
4. Ative a encriptação de dados e a proteção de credenciais.
5. Ative os controlos da aplicação e do browser para uma maior proteção contra aplicações não fidedignas e outras proteções de exploração incorporadas.
6. Ative a proteção do acesso à memória para ajudar a proteger contra ataques físicos pontuais, como, por exemplo, se alguém ligar um dispositivo malicioso a portas acessíveis externamente.

Ligações para mais informações

- Livro de Segurança do Windows | Comercial
- As novas funcionalidades de segurança do Windows 11 irão ajudar a proteger o trabalho híbrido | Blogue Microsoft Security

Centralidade da cadeia de fornecimento de software

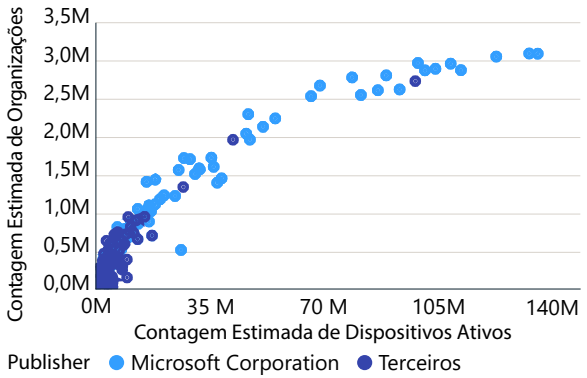
Os ataques a aplicações, plug-ins e extensões de terceiros podem afetar a confiança dos clientes em fornecedores que desempenham um papel central no ecossistema de fornecimento. Utilizar a teoria de rede para analisar a centrali-dade do software ajuda a destacar a criticidade das correções, sobretudo para aplicações centrais.

A Rede de Aplicações do Windows, com 18 milhões de ficheiros executáveis de aplicações, está instalada e é utilizada por 5 milhões de organizações, proporcionando uma visão de alto nível do nosso ecossistema de software. Das 100.000 aplicações mais utilizadas, 97% são produzidas por organizações externas cujas atualizações e correções de segurança são mantidas pelas mesmas. Isto ilustra dois traços importantes do nosso ecossistema de aplicações comerciais.

Primeiro, há centralidade no ecossistema de aplicações comerciais do Windows. Apenas as principais 100.000 aplicações (das 18 milhões) são utilizadas em 1.000 ou mais dispositivos. Por outras palavras, pouco mais de metade de 1% destas aplicações conseguem um grande alcance deste tipo entre o ecossistema do dispositivo.

Em segundo lugar, existe uma diversidade na capacidade de gestão destas aplicações, em que os 10.000 principais fornecedores de aplicações gerem as atualizações e as correções de segurança destas aplicações comerciais mais utilizadas. Isto demonstra a interdependência que uma empresa tem num conjunto diversificado de controlos de gestão, conformidade e de segurança dos fornecedores de software.

Penetração comercial das aplicações mais utilizadas



As principais aplicações são utilizadas por milhões de organizações e dezenas de milhões de dispositivos. Como são quase omnipresentes, os adversários estão constantemente à procura de explorar vulnerabilidades nestas principais aplicações, o que pode afetar milhões de dispositivos na base de utilizadores.

Observamos milhões de dispositivos comerciais ainda a utilizarem versões de aplicações vulneráveis muitos meses após o lançamento da correção ou, até mesmo, vários anos depois do fim do suporte do produto. Por exemplo, existem mais de 1 milhão de dispositivos comerciais do Windows ativos que executam a versão de um leitor de PDF que não é suportado desde 2017.

As versões antigas das aplicações que não têm suporte continuam a ser utilizadas ativamente em milhões de dispositivos comerciais. Como consequência, as organizações estão em risco de terem vulnerabilidades que não serão corrigidas.

Para as versões de aplicações com suporte, observamos uma estabilização da velocidade da adoção de correções críticas, o que é contrário à tendência que irá impulsionar a resiliência. Em vez disso, a curva deve mostrar uma adoção exponencial de correções todos os meses, de forma a obter a resiliência necessária.

Taxa de implementação de correções críticas

Depois de examinar uma vulnerabilidade crítica que afetou 134 versões de um conjunto de browsers, descobrimos que milhões de dispositivos, 78%, ainda usavam uma das versões afetadas nove meses depois de a correção ter sido lançada.

Utilizámos o toolkit InterpretML[9] para identificar as características relacionadas com as organizações com maior probabilidade de terem dispositivos com versões mais antigas das aplicações. O mais importante destes indicadores incluiu: horas de interação reduzidas em dispositivos; áreas geográficas, como a Ásia-Pacífico e a América Latina; e indústrias, como a do automóvel, produtos químicos, telecomunicações, transportes e logística, contribuintes de saúde (gestores de sinistros) e seguros.

A manutenção da resiliência do software deve incluir a desativação regular ou desinstalação de aplicações não utilizadas.

A segurança e a conformidade de uma organização depende dos seus próprios esforços e dos esforços dos seus fornecedores de software.

Insights acionáveis

1. Execute atualizações atempadamente em todas as aplicações e endpoints na sua organização.
2. Realize atempadamente a limpeza de todos os ficheiros executáveis não utilizados e obsoletos nos dispositivos das organizações.

Ligações para mais informações

- Documentação do Microsoft Intune | Microsoft Docs
- Gerir aplicações | Microsoft Docs
- Microsoft Defender para Endpoint | Microsoft Security
- Estrutura da Cadeia de Fornecimento Protegida de OSS | Microsoft Security Engineering
- Estrutura da Cadeia de Fornecimento Protegida de Software Open Source da Microsoft | Github

Criar resiliência a ataques emergentes de DDoS, aplicações Web e redes

A aceleração da transformação digital pôs fim ao modelo tradicional de perímetro de segurança e de rede. A migração para a cloud significa que as empresas têm de adotar a segurança de rede nativa da cloud para proteger os ativos digitais.

A complexidade, frequência e volume dos ataques continuam a crescer e já não se limitam às épocas festivas, o que indica uma mudança para a existência de ataques o ano inteiro. Isto realça a importância da proteção contínua para além das tradicionais épocas com picos de tráfego.

Ataques denial of service (DDoS) distribuídos

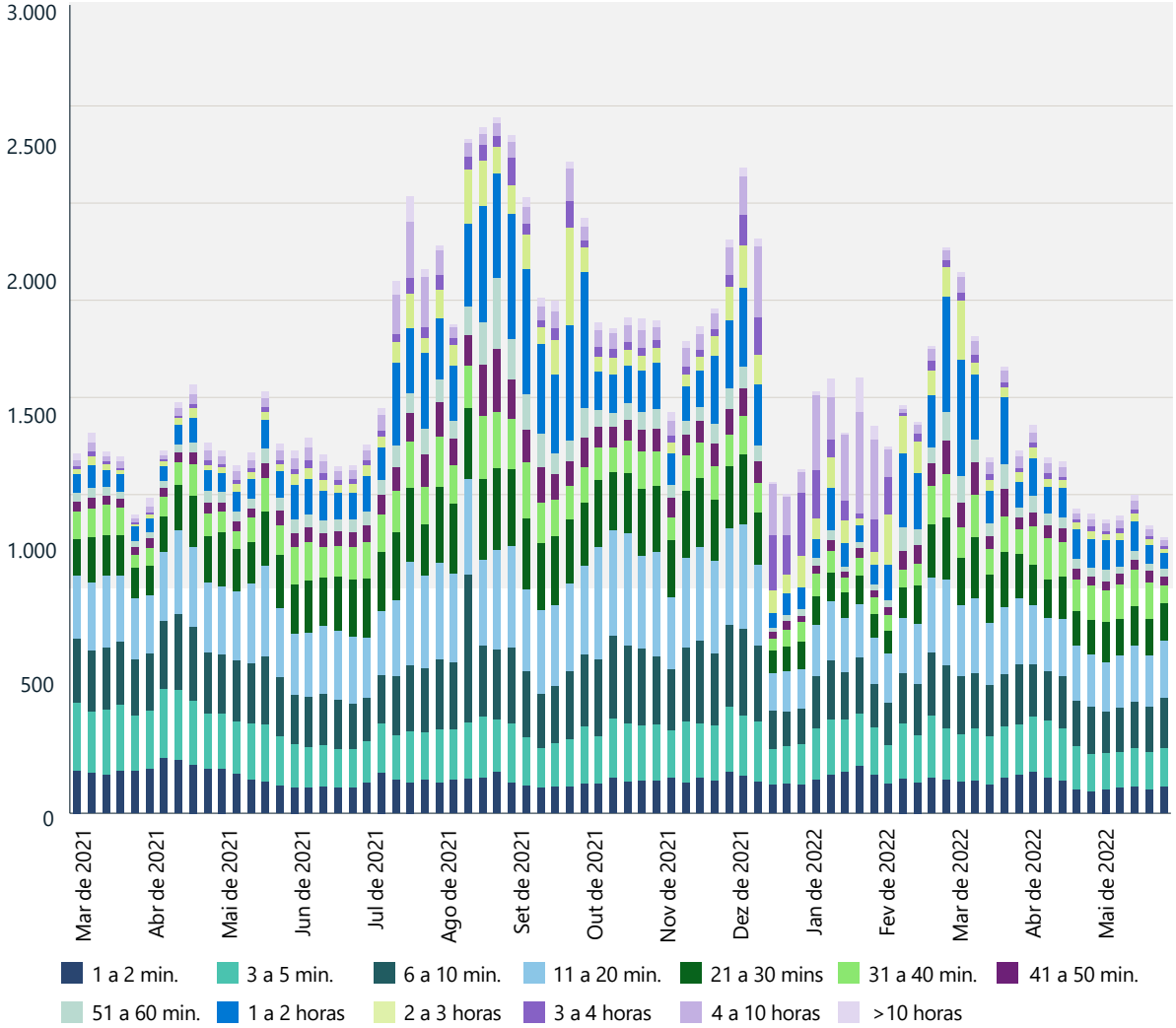
No ano passado, o mundo viu um volume, complexidade e frequência de ataques DDoS sem precedentes. Este boom de ataques DDoS foi impulsionado por um aumento substancial dos ataques de estado-nação e pela contínua proliferação de serviços DDoS de baixo custo. A Microsoft mitigou, em média, 1.955 ataques por dia, um aumento de 40% em relação ao ano anterior. Anteriormente, o número máximo de ataques acontecia, normalmente, durante a época festiva, no final do ano. Este ano, no entanto, o dia com mais registos deu-se a 10 de agosto de 2021. Isto pode indicar uma mudança para o lançamento de ataques durante o ano inteiro e realça a importância da proteção contínua para além das épocas de pico de tráfego tradicionais.

Em novembro de 2021, a Microsoft impediu um ataque DDoS volumétrico com um débito de 3,4 terabits por segundo (Tbps) de, aproximadamente, 10.000 origens em vários países. Foram mitigados ataques semelhantes com elevado volume, acima dos 2 Tbps, em 2022. Isto realça que não é só a complexidade e a frequência dos ataques que está a aumentar, mas também o volume (largura de banda) do ataque.

Duração do ataque

A maioria dos ataques observados no último ano foram de curta duração. Cerca de 28% dos ataques durou menos de 10 minutos, 26% entre 10 e 30 minutos e 14% entre 31 e 60 minutos. 32% dos ataques duraram mais de uma hora.

Número de ataques DDoS e distribuição da duração
(Março de 2021 – Maio de 2022)



A maioria dos ataques no último ano foram de curta duração. Cerca de 28% dos ataques duraram menos de 10 minutos.

Criar resiliência a ataques emergentes de DDoS, aplicações Web e redes

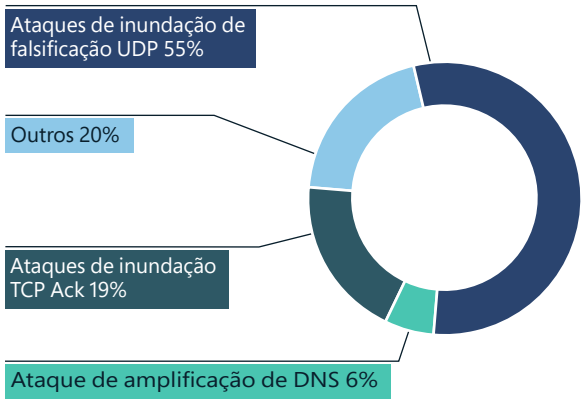
Continuação

Vetores de ataques DDoS

No ano passado, os vetores de ataque habitualmente utilizados foram a reflexão do User Datagram Protocol (UDP) na porta 80 através do Simple Service Discovery Protocol (SSDP), o protocolo de acesso ao diretório leve sem ligação (CLDAP), sistema de nomes de domínio (DNS) e o protocolo de tempo de rede (NTP), composto por um único pico. Também vimos um aumento dos ataques DDoS de camada da aplicação cujos alvos eram sites, com um pico de 16,3 milhões de RPS (pedidos por segundo) e 9,89 Tbps de tráfego de pico.

Em 2022, a Microsoft mitigou quase 2.000 ataques DDoS por dia e impediu o maior ataque DDoS alguma vez visto na história.

Vetores de ataques DDoS



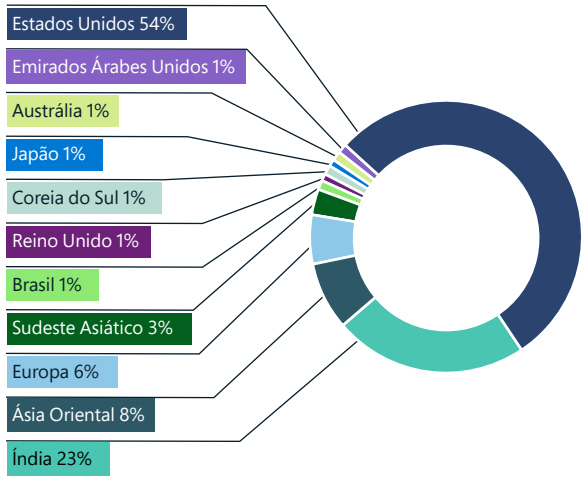
O ataque por entupimento de UDP falsificados tornou-se no vetor principal durante o primeiro semestre de 2022, passando de 16% para 55%. O ataque por entupimento de Ack de TCP baixou de 54% para 19%.

A indústria do gaming continua a ser o principal alvo dos ataques DDoS, a maioria das vezes a partir de mutações do botnet Mirai e de ataques de baixo volume ao protocolo UDP. Uma vez que o UDP é, normalmente, utilizado em aplicações de jogos e de streaming, uma grande maioria dos vetores de ataque foram o entupimento de UDP falsificados, enquanto uma pequena parte eram ataques de reflexão e amplificação de UDP.

Regiões geográficas alvo

Dos ataques DDoS detetados no ano passado, 54% foram conduzidos contra alvos nos EUA, uma tendência que pode ser explicada, parcialmente, pelo facto de a maioria dos clientes do Azure e da Microsoft estarem localizados neste país. Também observámos um aumento acentuado nos ataques contra a Índia, de apenas 2% no segundo semestre de 2021 para 23% no primeiro semestre de 2022. A Ásia Oriental, com Hong Kong em particular, continua a ser um alvo popular, com 8%. Na Europa, vimos concentrações de ataques contra as regiões de Amesterdão, Viena, Paris e Frankfurt.

Destino dos ataque DDoS

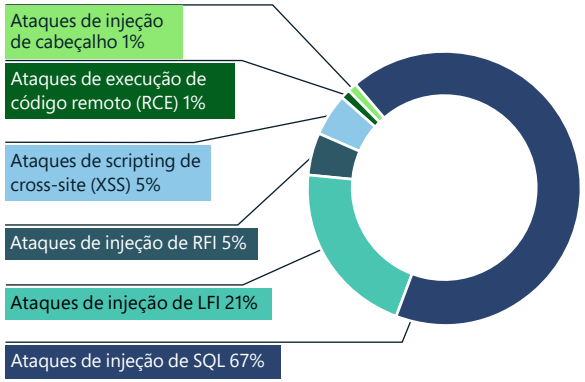


Atribuímos o elevado volume de ataques na Ásia à enorme quantidade de gamers na região, sobretudo na China, Japão, Coreia do Sul e Índia. Este número continuará a expandir-se à medida que o aumento da penetração do smartphone impulsiona a popularidade dos jogos para telemóveis, o que sugere que este alvo geográfico vai continuar a crescer.

Explorações de aplicações web

A firewall de aplicações web (WAF), em combinação com a proteção contra DDoS, faz parte da estratégia de defesa aprofundada que se destina a proteger os ativos da interface de programação de aplicações (API) e da web. A Microsoft observou que mais de 300 biliões de regras de WAF foram acionadas por mês através das WAF do Azure.

Distribuição dos tipos de ataque mais predominantes



A WAF do Azure deteta biliões de ataques diários na lista dos 10 principais Open Web Application Security Project (OWASP)[10]. De acordo com os nossos sinais, a maioria dos ataques lançados pelos hackers eram por injeção de SQL seguidos por injeção de ficheiros locais e ataques por injeção de ficheiros remotos. Isto está em consonância com o Top Ten do OWASP, que mostra que os ataques por injeção como o terceiro tipo mais comum de ataques na internet.

Também houve um aumento dos ataques de bots contra as aplicações Web do Azure, com uma média de 1,7 biliões de pedidos de bot por mês, sendo 4,6% desse tráfego composto por bots nocivos.

Criar resiliência a ataques emergentes de DDoS, aplicações Web e redes

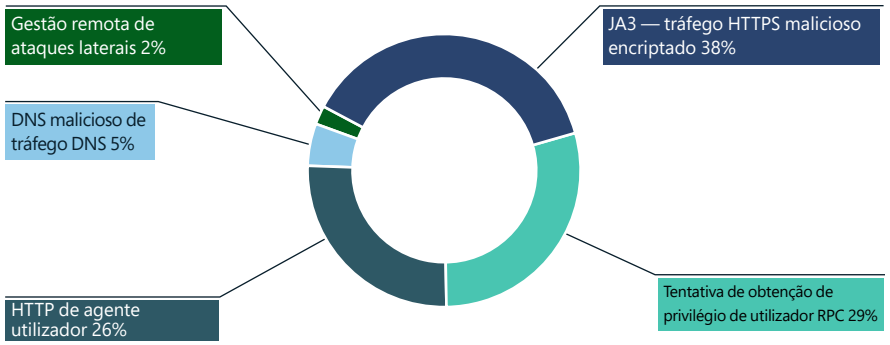
Continuação

Devido a um número cada vez maior de bots a executarem ataques de credenciais roubadas, fraudes com cartões de crédito, campanhas de ciber-influência e ataques à cadeia de fornecimento, esperamos ver um aumento constante dos ataques de bots contra aplicações web.

Intrusões na rede: deteção e prevenção

Observámos um aumento significativo nas explorações de camada de rede, sobretudo de malware, em 2022. O sistema de deteção e prevenção de intrusão (IDPS) do Azure Firewall bloqueou mais de 150 milhões ligações apenas no mês de junho.

Razões para a o IDPS rejeitar o tráfego



Razões de alerta de tráfego do IDPS

A análise de alertas do IDPS e de rejeição do tráfego mostra as seguintes abordagens utilizadas pelos atacantes. No tráfego rejeitado, vemos que os hackers utilizam SSL para ocultar as suas atividades e os ataques executados remotamente estão a tornar-se mais comuns. No tráfego de alerta, estamos a ver protocolos SMB/SMB2 utilizados para executar ataques remotos.

Insights acionáveis

1. Inspecione todo o tráfego entre sistemas num datacenter ou serviço de cloud, bem como o tráfego que procura aceder aos mesmos.
2. Desenvolva uma estratégia de resposta robusta à segurança da rede durante todo o ano.
3. Utilize os serviços de segurança nativos da cloud para implementar uma postura robusta de segurança de rede de confiança zero.

Ligações para mais informações

- Melhore as defesas de segurança nos ataques de ransomware com o Azure Firewall | Blogue Azure e Atualizações | Microsoft Azure
- Anatomia de um ataque de amplificação de DDoS | Blogue Microsoft Security
- Proteção inteligente de aplicações da periferia à cloud com a Firewall de Aplicações Web do Azure | Blogue Azure e Atualizações | Microsoft Azure

Desenvolver uma abordagem equilibrada quanto à segurança dos dados e à resiliência cibernética

A transformação digital impulsionou uma grande expansão dos ativos de dados e um aumento dos riscos para a segurança, conformidade e privacidade. As organizações ciber-resilientes têm de equilibrar os investimentos em proteção de dados, conformidade e capacidades de recuperação e integrá-las em processos especializados de resposta regulamentar para resolver tipos de falhas distintos.

As violações de dados não são uma questão de saber se existe ou não a probabilidade de acontecerem, mas sim quando é que vão acontecer. O estudo da IBM e do Ponemon Institute "Cost of a Data Breach, 2021" divulga um custo global médio das violações de dados de 4,24 milhões de USD (10% em relação ao ano transato) e de 9,05 milhões de USD nos Estados Unidos. As falhas de conformidade foram consideradas como o principal fator da amplificação dos custos. Por outro lado, as reduções de custos das violações foram associadas às melhores práticas, como o planeamento de resposta a incidentes (IR), maturidade da implementação da confiança zero, segurança da IA e automatização, para além da utilização da encriptação.

As violações de dados são inevitáveis. As organizações que têm uma abordagem de resiliência equilibrada vão reduzir a frequência, o impacto e o custo das violações.

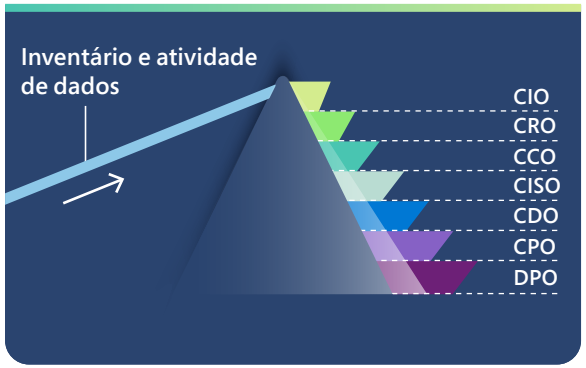
A gestão de dados, a segurança, a conformidade e a privacidade não dependem umas das outras

Vimos os dados ganharem destaque nos últimos anos como um motor de criação de valor crucial para as organizações. Ao mesmo tempo, o surgimento dos regulamentos de privacidade que exigem a gestão e a segurança dos dados têm atenuado as linhas entre funções de risco. Apesar de as funções de nível de direção mais recentes, como o Diretor de Dados (CDO) ou os Diretores de Privacidade (CPO), terem um interesse pessoal na segurança e conformidade, a implementação e a operacionalização da proteção de dados dependem, muitas das vezes, das equipas lideradas pelos Diretores de informação (CIO) e/ou Diretor Executivo de Segurança Informática (CISO). Não é uma via de sentido único, uma vez que as iniciativas de gestão de dados lideradas pelos CDOs também têm vantagens em termos de segurança. Como resultado desta interligação, as equipas de TI, gestão de dados, segurança, conformidade e privacidade precisam de trabalhar, cada vez mais, estreitamente para atingirem a eficiência e gerirem o risco.

As plataformas de gestão de riscos de dados unificados para todo o acervo de dados da organização são o futuro

O alinhamento entre TI, gestão dos dados, segurança, conformidade e gestão da privacidade é difícil num ambiente de aplicações personalizadas para cada disciplina e cobertura inconsistente na expansão de dados híbrida e multicloud da organização típica. Acreditamos que as organizações precisam de um único painel de vidro para localizarem e conhecerem os seus dados, protegerem-nos, controlarem o seu acesso, utilização e ciclo de vida, bem como impedirem a perda de dados em todo o acervo.

Trabalhar a partir do mesmo inventário de dados e informações sobre a atividade facilita os processos entre equipas, produz uma imagem de risco mais abrangente e permite que as organizações se preparem melhor e simplifiquem a sua resposta a uma violação.



O "painel de vidro único" deve agir como um prisma. As equipas que têm uma participação na segurança, conformidade e privacidade dos dados precisam de vistas diferentes, mas consistentes, do mesmo inventário e atividade de dados para poderem estar alinhadas e colaborarem. A atividade de dados inclui o acesso, modificação dos dados e os eventos de movimentação, que são uma parte valiosa da equação da segurança dos dados.

A gestão de dados eficaz, a segurança, conformidade e privacidade são interdependentes e exigem uma colaboração entre equipas.

Insights acionáveis

1. Equilibre a defesa com a recuperação e minimize o impacto da violação de dados ao investir em conformidade, proteção de dados e capacidades de resposta.
2. Desenvolva e adote processos e ferramentas que cortem os silos de riscos de dados e que cobram todo o acervo de dados.

Ligações para mais informações

- Microsoft Purview - Soluções de Proteção de Dados | Microsoft Security
- O futuro da conformidade e da gestão de dados está aqui: Introdução ao Microsoft Purview | Blogue Microsoft Security

Resiliência nas operações de ciberinfluência: a dimensão humana

Nos últimos cinco anos, os avanços nos gráficos e no machine learning introduziram ferramentas intuitivas capazes de gerar, rapidamente, conteúdos realistas e de alta qualidade que podem ser disseminados amplamente pela Internet em poucos segundos.

Quando se trata de eventos transmitidos através de texto, áudio e conteúdos visuais, chegámos a um ponto em que nem os humanos nem os algoritmos conseguem distinguir, de forma fiável, os factos da ficção. A proliferação destas ferramentas e os seus resultados estão a lançar dúvidas sobre a fiabilidade de todos os meios de comunicação digitais, perturbando a nossa compreensão sobre os eventos a nível local e mundial. As novas formas de influência das operações, possibilitadas pelos avanços tecnológicos, têm sérias implicações para os processos democráticos.[11]

Surgem perguntas sobre o que podemos fazer para preparar um futuro mais resiliente contra estas operações de ciberinfluência. A tecnologia é apenas uma peça do puzzle. Vão ser necessários vários esforços, incluindo a educação destinada à literacia mediática, sensibilização e vigilância, investimento em jornalismo de qualidade (com repórteres fiáveis onde a história acontece, quer seja a nível local, nacional e internacional), redes de partilha e de alerta sobre as operações de influência e novos tipos de regulamentos que penalizem os agentes maléficos que gerarem ou manipularem meios de comunicação digitais com o objetivo de enganar.

Também reconhecemos que a restauração da confiança nos conteúdos digitais é um objetivo ambicioso que vai exigir perspetivas e participação diversificadas. Não existe uma empresa, instituição ou um governo que consiga resolver sozinho estas ameaças. A nossa superpotência como humanos é a nossa capacidade de colaborar e cooperar. Isto é especialmente importante agora, porque vai exigir que todos (governos mundiais, indústrias, universidades e, em especial, as agências noticiosas, sociais e multimédia) trabalhem em conjunto para melhorar o estado da nossa sociedade.

Ligações para mais informações

- Aplicações para inteligência artificial nas missões cibernéticas do Departamento de Defesa | 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 maio de 2022; Testimony of Eric Horvitz)

Fortalecer o fator humano com o desenvolvimento de competências

Abordar o fator humano é um componente essencial para qualquer estratégia de desenvolvimento de competências de cibersegurança. De acordo com um estudo Kaspersky Human Factor in IT Security[12], 46% dos incidentes de cibersegurança envolvem funcionários negligentes ou mal informados que, inadvertidamente, facilitam o ataque.

A equipa de Educação e Sensibilização da Microsoft na organização de Segurança Digital e Resiliência é responsável por reforçar o fator humano da cibersegurança, ao capacitar os colaboradores para protegerem os nossos sistemas e dados dos nossos clientes. Os nossos objetivos são:

- Reduzir o risco para a Microsoft e para os nossos clientes através da criação de um conjunto de competências de segurança, ao nível da empresa, para todos os colaboradores.
- Reforçar os conhecimentos de segurança dos colaboradores através de uma abordagem de reciclagem de formação em várias fases para obter os resultados de comportamento desejados.
- Fomentar a mudança de cultura, fazendo com que uma mentalidade de segurança seja parte intrínseca da cultura da Microsoft através da formação e dos eventos de segurança necessários anualmente.
- Promover um recurso web centralizado único para obter as melhores práticas, informações sobre a política da empresa e relatórios de incidentes para todas as questões relacionadas com a cibersegurança.

Um programa de desenvolvimento de competências em cibersegurança direcionado e centralizado chega a cada colaborador da Microsoft, pelo menos, uma vez por ano. As ofertas de formação estão otimizadas para suportar as iniciativas de cibersegurança atuais e proporcionar resultados de comportamento mensuráveis. O Conselho de Gestão de Riscos de Informação da Microsoft (IRMC) desempenha um papel fundamental na identificação de resultados importantes na mudança de comportamentos de cibersegurança a serem abordados pela formação.

Com todos os nossos programas de desenvolvimento de competências de cibersegurança, medimos a eficiência, a eficácia e os resultados da solução, sempre que possível. Por exemplo, a nossa oferta de desenvolvimento de competências em ameaças internas tem uma conformidade de formação de 95%, um nível de satisfação excecional, e resultou num aumento significativo de gestores que reportam potenciais casos de ameaças internas através da ferramenta Report It Now da empresa. O programa inclui:

Fundações de segurança: formação em conformidade e sensibilização para a cibersegurança ao nível da empresa e centralizada que aborda as principais práticas de segurança e de privacidade. Esta série de formações muito aguardada implementa um modelo de educação/entretenimento para tornar a aprendizagem sobre cibersegurança mais envolvente e interessante.

STRIKE: a formação técnica necessária da Microsoft para engenheiros que criam e fazem a manutenção de soluções da linha de negócio. Esta formação funciona só por convite e aborda as áreas oportunas e críticas das melhores práticas de higiene de cibersegurança, para além de utilizar um modelo de oferta híbrido em tempo real adaptado às necessidades do público.

Programa específico: programas de formação vocacionados que suportam iniciativas específicas de cibersegurança, incluindo o Shadow IT, Insider Threat e Microsoft Federal. Estas ofertas estão intimamente integradas na estratégia global de interação para as respetivas iniciativas de cibersegurança, através de patrocínios executivos e relatórios de indicadores para evitar uma abordagem de formação do tipo "assinalar a caixa".

MSProtect: o recurso web centralizado da Microsoft oferece as melhores práticas, informações sobre a política da empresa e relatórios de incidentes para todas as questões relacionadas com a cibersegurança. Este recurso a pedido é o recurso imprescindível para os colaboradores fora das ofertas de formação formais.

O desenvolvimento de competências de segurança não deve ser encarado como uma atividade check-the-box e de conformidade. Em vez disso, concentre-se na mudança de comportamentos para permitir que os resultados sejam monitorizados nos comportamentos desejados identificados e estabeleça sistemas de escuta para determinar o impacto das ofertas.

Insights acionáveis

1. Forneça formação e recursos de segurança aos colaboradores sempre e onde precisarem.
2. Desenvolva uma estratégia de desenvolvimento de competências centralizada informada por intervenientes de toda a empresa.
3. Certifique-se de que o impacto da formação é monitorizado e analisado ao nível da eficiência (quantidade), eficácia (qualidade) e resultados (impacto no negócio).

Ligações para mais informações

› A Microsoft lança a próxima fase da iniciativa de competências depois de ajudar 30 milhões de pessoas

Insights do nosso programa de eliminação de ransomware

A Microsoft tem usado a sua Confiança Zero nos[13] últimos cinco anos para garantir que as identidades e os dispositivos são geridos de forma robusta e saudável. À medida que o risco de ransomware vai crescendo, fomos desenvolvendo uma visão mais profunda para apoiar os nossos esforços de proteção própria e de proteção dos nossos clientes.

Após uma avaliação interna profunda, desenvolvemos um programa de eliminação de ransomware para remediar as lacunas nos controlos e na cobertura, contribuir para as melhorias de funcionalidades para serviços como o Defender for Endpoint, Azure e M365, bem como para desenvolver manuais de procedimentos para as nossas equipas de SOC e de engenheiros sobre como recuperarem no caso de sofrerem um ataque de ransomware.

O primeiro passo foi compreender a extensão da nossa proteção contra um ataque de ransomware direcionado para a Microsoft. Já tínhamos em curso esforços para implementar o Defender for Endpoint e assegurar que todos os dispositivos são geridos e compatíveis com as nossas políticas de Confiança Zero. Contudo, precisávamos de encontrar uma forma de compreender todas as facetas da maior interrogação: se poderíamos recuperar efetivamente de um ataque. Para obtermos insights, avaliámos o perfil NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF),[14] que está alinhado com a nossa política empresarial global relativa à nossa conhecida lista de controlos. Esta análise identificou rapidamente as lacunas na cobertura.

Em seguida, demos prioridade às lacunas nas funções Identificar, Detetar, Proteger, Responder e Recuperar do CSF. Encontrámos o alinhamento estratégico com a Confiança Zero e outros programas, assim como lacunas que não tinham qualquer volume de trabalho existente. Tendo avaliado o volume de trabalho e os esforços necessários para corrigir estas lacunas, separámo-los em dois pilares:

- **Proteger a empresa (PtE):** definir os itens de trabalho que precisamos de fazer como empresa para nos protegermos e conseguirmos recuperar de um ataque bem-sucedido.
- **Proteger o cliente (PtC):** criar capacidades nas nossas ofertas para proteger os nossos clientes, bem como o nosso negócio.

Incorporar as conclusões na nossa própria empresa

Para remediar os principais riscos e proteger os nossos serviços críticos de um ataque de ransomware, planeamos concentrar o investimento nos próximos 6 a 12 meses para alcançarmos os cinco cenários a seguir como parte de um programa de ransomware dedicado. Se conseguirmos ser bem-sucedidos em cada um dos cenários, vamos expandir, gradualmente, o alcance do programa para que chegue a todas as partes da empresa.

Cenário 1: os membros da equipa de segurança sabem qual o risco global associado a um ataque de ransomware e têm um processo definido para sensibilizar os diretores sobre as lacunas do controlo e o estado do risco.

Cenário 2: os membros da equipa de segurança têm acesso aos manuais de procedimentos elaborados para ajudá-los, bem como outras equipas dentro da Microsoft, a responder e recuperar os serviços críticos de um ataque de ransomware.

Cenário 3: os membros da equipa de Resiliência Empresarial têm uma norma a seguir nas cópias de segurança de sistemas críticos. Os manuais de procedimentos existem e são feitos exercícios regulares de cópia de segurança e recuperação para garantir que os dados podem ser recuperados no caso de um ataque de ransomware.

Cenário 4: os proprietários dos serviços compreendem e implementam os controlos e as políticas de segurança e operacionais necessários para protegerem os respetivos serviços, os dados dos clientes, os endpoints e os ativos de rede dos ataques de ransomware, com foco especial nos serviços priorizados como serviços críticos da Microsoft.

Cenário 5: todos os colaboradores podem aceder a recursos educativos e de formação que descrevem como podemos reconhecer um ataque de ransomware e como devemos notificar a equipa de segurança e iniciar a resposta.

Insights acionáveis

1. Documente e valide as atividades integrais de recuperação e remediação relacionadas com ataques de ransomware contra serviços críticos.
2. Envolva os intervenientes na atualização dos seus manuais de procedimentos de Gestão de Crises Empresariais para incluir atividades específicas de ransomware e um processo de decisão e orientação para determinar se/quando deve pagar por um ransomware.
3. Melhore a cobertura de deteção e proteção, ativando funcionalidades disponíveis nos seus produtos de segurança implementados (por ex.: regras para a Redução da Superfície de Ataque do Defender for Endpoint).
4. Trabalhe com a equipa de normas de segurança para definir uma linha de base para proteger-se de um ataque de ransomware e ofereça formação e documentação às equipas de engenheiros sobre como se devem proteger de um ataque de ransomware.
5. Implemente a automatização para facilitar a introdução de políticas de segurança e operações nas equipas de DevOps e assegurar que, se um sistema se desviar da conformidade, é sinalizado e remediado rapidamente.

Ligações para mais informações

› Partilhar a forma como a Microsoft protege contra o ransomware | Microsoft Inside Track

Agir já sobre as implicações da segurança quântica

A pressão existe para gerir a ameaça que a computação quântica representa para a encriptação de hoje e tudo o que protege. O memorando recentemente divulgado sobre Melhorar a Cibersegurança do Departamento de Defesa da Segurança Nacional e os Sistemas Comunitários de Inteligência,[15] baseado na Ordem Executiva dos EUA 10428[16] para Melhorar a Cibersegurança Nacional, realça que a segurança da cadeia de fornecimento de software é crítica para solucionar futuros ataques de estado-nação.

O que são os computadores quânticos?

Os computadores quânticos são máquinas que utilizam as propriedades da física quântica para armazenar dados e efetuar cálculos. Isto pode ser extremamente vantajoso para determinadas tarefas, em que até podem superar, largamente, os nossos melhores supercomputadores. A computação quântica já está a abrir novos horizontes para a encriptação e o processamento de dados. Estudos preveem que a computação quântica se tornará numa indústria quântica de vários biliões de dólares (USD) por volta de 2030.[17] De facto, a computação quântica e a comunicação quântica estão perto de ter um efeito transformador em inúmeros setores, desde a saúde e energia às finanças e segurança.

A computação quântica é uma ameaça para a encriptação de hoje e tudo o que ela protege.

A ameaça à encriptação de hoje

Com o algoritmo 1994 da Shor e um computador quântico à escala industrial com mais do que alguns milhões de qubits físicos, todos os nossos algoritmos de encriptação de chave pública amplamente implementados hoje podem ser quebrados de forma eficiente. É fundamental considerar, avaliar e normalizar criptossistemas "à prova de quântica" que sejam eficientes, ágeis e seguros contra um ataque baseado em quântica. A migração de software para a "encriptação pós-quântica", nomeadamente os algoritmos e protocolos clássicos existentes e resistentes a ataques quânticos, demorará anos – uma década ou mais – a ser conseguida.[18]

Isto significa que a pressão existe para gerir a ameaça que a computação quântica representa para a encriptação de hoje e tudo o que protege. Os adversários podem, agora, registar os dados encriptados e explorá-los mais tarde quando um computador quântico estiver disponível. Esperar que a computação quântica chegue antes de abordar as suas implicações ao nível da encriptação será demasiado tarde.

Como a encriptação é utilizada em todo o ecossistema cibernético, isto significa que os nossos serviços de segurança baseados em encriptação podem estar comprometidos. Por exemplo, isto inclui serviços para comunicações (TLS, IPSec), mensagens (e-mail, conferência web), gestão de identidades e acessos, navegação na web, assinatura de código, transações de pagamentos e outros serviços que dependem da encriptação para estarem protegidos.

À medida que os computadores quânticos se tornam realidade, os componentes de software de terceiros que contenham implementações de algoritmos e funcionalidades de encriptação também vão precisar de uma análise adicional. Isto exige que todas as organizações ao longo da cadeia de valor façam a sua parte para assegurar que a mesma se mantém segura. Os organismos do setor e os governos estão a aumentar os esforços para definir os requisitos de segurança da cadeia de fornecimento de software e, em alguns casos, introduzir novos mandatos para proteger a cadeia. O Memorando de Segurança Nacional NSM-8[19] estabelece os requisitos e os cronogramas para implementar a encriptação pós-quântica nos Sistemas de Segurança Nacional (NSS). Estabelece um período de transição no prazo de 180 dias para "planear a modernização, utilizar a encriptação sem suporte, protocolos exclusivos da missão aprovados, protocolos resistentes à quântica e o planeamento da utilização de encriptação resistente à quântica, sempre que necessário."

A normalização é uma atividade com tempo de execução longo na transição para a encriptação à prova de quântica. Os organismos de normalização que trabalham nas normas com encriptação de chave pública têm de começar a experimentar e a adaptar-se já aos algoritmos pós-quânticos.

Os novos algoritmos de encriptação pós-quântica (PQC), algoritmos clássicos que se pensa serem robustos contra ataques quânticos, estão agora a ser revistos através do Projeto de Normalização Pós-Quântica do NIST.[20] Este trabalho irá influenciar os esforços globais dentro dos organismos de normalização. Apesar de haver alguma sobreposição com as seleções de algoritmos do governo dos EUA, as diferentes escolhas regulamentares/organismos nacionais para algoritmos compatíveis podem apresentar desafios internacionais. Por sua vez, esta fragmentação complica a engenharia de produtos e serviços.

Novos algoritmos de encriptação pós-quântica estão a ser revistos através do programa de Normalização Pós-quântica do NIST. Este trabalho irá influenciar os esforços globais nos organismos de normalização.

Insights acionáveis

Juntamente com a SAFECode e os membros parceiros, devem ser realizadas atividades imediatas de curto prazo pela indústria para se prepararem para a transição da PQC.[21] Estas atividades incluem:

1. Fazer um inventário dos seus produtos/códigos que utilizam encriptação.
2. Implementar uma estratégia de agilidade criptográfica na sua organização que inclua a minimização da rotatividade de códigos necessária quando a encriptação é alterada.
3. Definir a utilização de potenciais algoritmos à prova de quântica nos seus produtos ou serviços que utilizem encriptação.
4. Estar preparado para utilizar diferentes algoritmos de chave pública para encriptação, troca de chaves e assinaturas.
5. Testar as suas aplicações para obter o impacto de tamanhos de chaves, cifras e assinaturas muito grandes.

Ligações para mais informações

- A Microsoft demonstrou a física subjacente necessária para criar um novo tipo de qubit | Microsoft Research

Integrar o negócio, a segurança e as TI para uma maior resiliência

A ciber-resiliência robusta depende dos líderes empresariais que trabalham com as equipas de segurança para implementarem esta última. Na experiência da Microsoft, a liderança em segurança é uma disciplina desafiadora que exige o apoio dos líderes das organizações para proteger a organização de forma mais eficaz.

Os líderes de segurança percorrem vários desafios dinâmicos que abrangem tópicos relacionados com o risco, tecnologia, economia, processos organizacionais, modelos de negócio, transformação da cultura, interesses geopolíticos, espionagem e conformidade das sanções internacionais. Cada um deles tem nuances para serem compreendidos e geridos de perto.

Os líderes de segurança também têm a tarefa de frustrar os hackers humanos inteligentes, bem financiados e altamente motivados, bem como os cibercriminosos pouco qualificados, mas eficazes. As suas equipas têm de defender conjuntos técnicos complexos, muitas das vezes criados incrementalmente ao longo de 30 anos ou mais, numa altura em que a segurança era uma prioridade baixa ou inexistente. As decisões tomadas há vários anos podem implicar riscos hoje em dia até saldarmos a dívida técnica e resolvermos as lacunas na segurança.

Os líderes organizacionais e os decisores políticos podem ter um impacto positivo significativo na segurança, ao apoiarem ativamente os líderes de segurança e ajudarem a construir uma ponte entre a segurança integrada e o resto da organização. Quando a Microsoft trabalha com clientes que pensam desta forma, vemo-los a criar uma organização mais resiliente e, também, a melhorar a sua agilidade para se adaptarem e inovarem.

A liderança organizacional pode dar apoio aos líderes de segurança, ao concentrar-se em três áreas-chave:

1. Criar segurança por design

Por vezes, a segurança é vista como um obstáculo ou uma reflexão posterior nos processos das empresas, sendo, muitas das vezes, considerada nas decisões apenas quando é demasiado tarde para evitar um risco ou implementar correções de forma mais barata e fácil.

Os líderes organizacionais e os políticos devem assegurar que:

Incluem a segurança atempadamente em novas iniciativas. As novas iniciativas digitais e a adoção da cloud devem dar prioridade à segurança para assegurar que o risco organizacional não aumenta em cada nova aplicação ou capacidade digital. Assim que a segurança seja incluída de forma fiável, poderá utilizar esses processos para modernizar os sistemas legados, de forma a obter, ao mesmo tempo, vantagens de segurança e produtividade.

Normalizam a manutenção preventiva para a segurança. Certifique-se de que a manutenção básica da segurança, como aplicar atualizações e correções de segurança e configurações seguras, tem todo o apoio organizacional atribuído (incluindo orçamentos, tempo de paragem agendado, requisitos de aquisição para suporte de produtos de fornecedores).

Infelizmente, muitas organizações atrasam, adiam ou aplicam apenas parcialmente estas práticas comuns. Isto oferece inúmeras oportunidades para os hackers explorarem. A necessidade de normalização da segurança é referida no US NIST 800-40.[22]

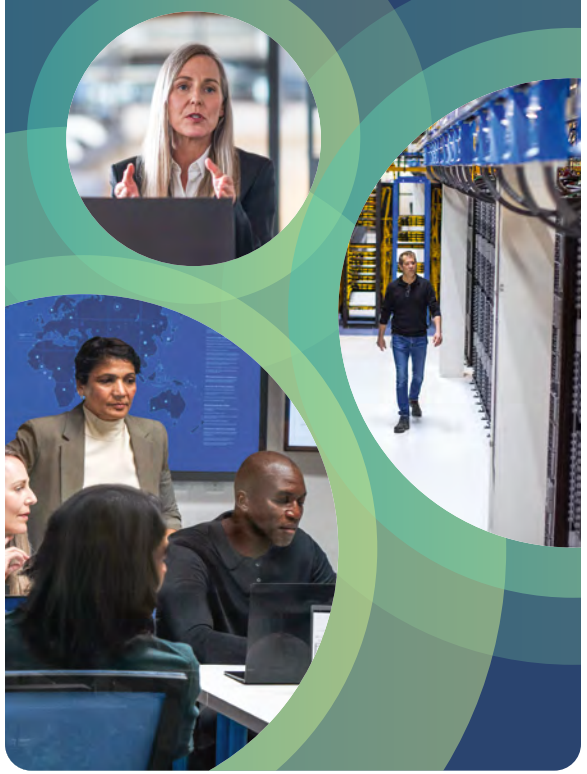
2. Interagir com a segurança

Os líderes das organizações devem participar ativamente e patrocinar os principais processos de segurança para garantir a priorização dos recursos e a preparação para os desastres relacionados com segurança. Isto inclui a interação em:

Identificar os ativos críticos da empresa. Os líderes e as equipas de segurança precisam de saber quais os ativos que são críticos para a empresa para concentrarem os recursos de segurança no que é mais importante. Isto é, muitas das vezes, um novo exercício que inclui pedir e responder a novas questões que não foram abordadas anteriormente.

Exercícios de cibersegurança de continuidade do negócio e recuperação após desastre Os ciberataques podem tornar-se os principais eventos que perturbam ou interrompem a maior parte ou todas as operações da empresa. A garantia de que as equipas de toda a organização estão preparadas para lidar com estas situações reduzirá o tempo para restaurar as operações da empresa, limitar os danos na organização e ajudar a manter a confiança dos clientes, cidadãos e dos constituintes. Isto deve ser integrado num processo de continuidade do negócio e recuperação após desastre existente.

As decisões sobre riscos de segurança são tomadas melhor por proprietários de empresas ou de missões que têm visibilidade total sobre todos os riscos e oportunidades.



Integrar o negócio, a segurança e as TI para uma maior resiliência

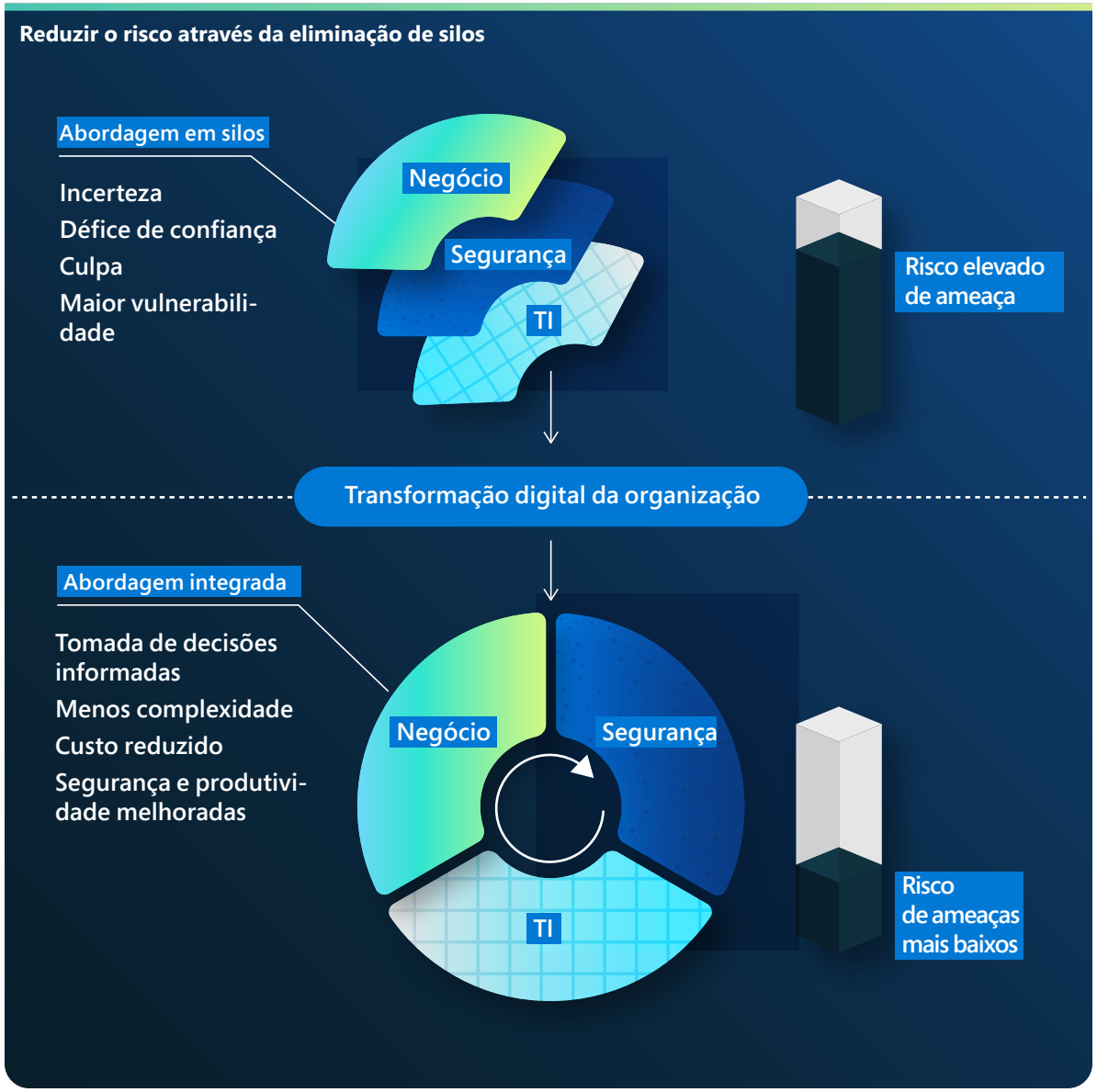
Continuação

3. Posicionar a segurança corretamente

A forma como as organizações estruturam a responsabilização dos riscos de segurança prepara-as, muitas das vezes, para uma tomada de decisões sobre segurança. As decisões de risco são melhor tomadas por proprietários de empresas ou de missões que tenham visibilidade total sobre todos os riscos e oportunidades. Contudo, as organizações atribuem, muitas das vezes (implicita ou explicitamente), a responsabilização dos riscos de segurança aos especialistas no assunto da equipa de segurança. Isto coloca um peso pouco saudável nas equipas de segurança, ao mesmo tempo que priva os empresários de obterem visibilidade e controlo sobre um risco essencial para a sua empresa. As organizações podem corrigir isto:

Preparando os empresários: educar os empresários sobre o risco de segurança no geral e de que forma estas ameaças podem e irão afetar a sua empresa. O envolvimento direto das equipas de segurança neste esforço também aumenta a colaboração com a segurança e a agilidade global da empresa.

Atribuindo riscos de segurança aos empresários: à medida que os empresários ficam suficientemente informados para compreender e aceitar o risco de segurança, a organização deve transferir, explicitamente, a responsabilização pelos riscos de segurança para os mesmos, mantendo as equipas de segurança responsáveis pela gestão desse risco e pelo fornecimento de conhecimentos e orientações detalhados ao proprietário.



"A resiliência cibernética está numa tabela regressiva a partir da continuidade do negócio clássica e recuperação após desastre, começando uma boa cópia de segurança de dados; progredindo para as capacidades de recuperação para processos, tecnologia e suas dependências (incluindo pessoas e terceiros); e mudar para serviços de autorrecuperação e sempre ligados, resiliência para funções críticas e falhas para terceiros igualmente críticos. As organizações mais resilientes promovem a integração entre TI, gestores de empresas e profissionais de segurança. A grande resiliência inclui a criação de resiliência desde o início, ter uma gestão de alterações segura e isolamento de falhas granulares. A ciber-resiliência é apenas um cenário num bom programa de planeamento de todos os perigos. À medida que os riscos cibernéticos aumentam e o cruzamento entre cibersegurança e resiliência se torna mais importante, a ligação do Diretor Executivo de Segurança Informática (CISO) ao programa de resiliência da empresa cresce de forma mais forte. Todos os anos, os CISOs estão a tomar conta da resiliência ao nível da empresa."

Lisa Reshaur
Diretora-Geral, Gestão de Riscos, Microsoft

Ligações para mais informações

- Da resiliência à perseverança digital: de que forma as organizações estão a utilizar a tecnologia digital para avançarem em tempos sem precedentes | Blogue Oficial da Microsoft
- De que forma as equipas de segurança e de TI podem trabalhar em conjunto para melhorar a segurança de endpoints | Microsoft Security

A curva do sino da resiliência cibernética

Fatores de sucesso de resiliência que cada organização deve adotar

Como vimos, muitos dos ciberataques são bem-sucedidos, simplesmente, porque a higiene básica de segurança não foi seguida. Os padrões mínimos que cada organização deve adotar são:

- **Ativar a autenticação multifator (MFA):** para proteger contra palavras-passe de utilizador comprometidas e ajuda a fornecer uma resiliência adicional para as identidades.
- **Aplicar princípios de Confiança Zero:** a pedra basilar de qualquer plano de resiliência que limita o impacto numa organização. Estes princípios são:
  1. – Verificar explicitamente: assegurar que os utilizadores e os dispositivos estão em bom estado antes de permitir o acesso aos recursos.
  2. – Utilizar o acesso menos privilegiado: só permite os privilégios necessários para aceder a um recurso e nada mais.
  3. – Assumir a violação: assuma sempre que as defesas do sistema possam ter sido violadas e os sistemas comprometidos. Isto significa monitorizar constantemente o ambiente para um possível ataque.
- **Utilizar anti-malware de deteção e resposta alargada:** implemente software para detetar e bloquear automaticamente os ataques e fornecer insights para as operações de segurança. A monitorização de insights de sistemas de deteção de ameaças é essencial para poder responder atempadamente às ameaças.
- **Manter tudo atualizado:** a existência de sistemas não corrigidos e desatualizados são um dos principais motivos pelos quais muitas organizações são vítimas de um ataque. Certifique-se de que todos os sistemas estão sempre atualizados, incluindo o firmware, o sistema operativo e as aplicações.
- **Proteger os dados:** saber quais são os dados importantes, onde estão localizados e se os sistemas certos estão devidamente implementados é crucial para implementar a proteção adequada.

98%

A higiene de segurança básica ainda protege contra 98% dos ataques.

Princípios fundamentais

- Ativar a autenticação multifator
- Aplicar os princípios da Confiança Zero
- Utilizar antimalware moderno
- Manter tudo atualizado
- Proteger os dados

Notas finais

1. A Deteção e Resposta de Endpoints (EDR) é uma plataforma de segurança de endpoints da empresa criada para ajudar as redes empresariais a prevenir, detetar, investigar e responder a ameaças avançadas. As capacidades de deteção e resposta de endpoints oferecem deteções de ataque avançadas que são realizadas quase em tempo real e acionáveis. Os analistas de segurança podem priorizar os alertas de forma eficaz, obter visibilidade sobre o âmbito completo de uma violação e executar ações de resposta para remediar as ameaças.
2. Uma Plataforma de Proteção de Endpoints (EPP) é uma solução implementada em dispositivos de endpoint para evitar malware baseado em ficheiros, detetar e bloquear a atividade maliciosa a partir de aplicações fidedignas e não fidedignas, e fornecer as capacidades de investigação e remediação necessárias para responder de forma dinâmica aos alertas e incidentes de segurança.
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. Livro de Segurança do Windows: comercial
7. As novas funcionalidades de segurança do Windows 11 irão ajudar a proteger o trabalho híbrido | Blogue Microsoft Security
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | Fundação OWASP
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. Executive Order 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

Equipas Contribuidoras

Equipas Contribuidoras

Os dados e insights deste relatório foram fornecidos por um grupo diversificado de profissionais focados na segurança, que trabalham em várias equipas diferentes da Microsoft. Têm como objetivo comum proteger a Microsoft, os respetivos clientes e o mundo em geral contra a ameaça dos ciberataques. É com orgulho que partilhamos estes insights num espírito de transparência, com o objetivo comum de tornar o mundo um lugar mais seguro para todos.

AI for Good Research Lab: tirar partido do poder dos dados e da IA para fazer face a muitos dos desafios do mundo. Este laboratório colabora com organizações fora da Microsoft, aplicando a IA para melhorar os meios de subsistência e os ambientes. As áreas de foco incluem: segurança online (desinformação, cibersegurança, segurança infantil), resposta a desastres, sustentabilidade e IA para a área da Saúde.

Azure Edge e Segurança da Plataforma, Empresa e SO: responsável pelo SO central e pela segurança da plataforma no Windows, Azure e outros produtos da Microsoft. A equipa integra soluções de hardware e segurança líderes do setor nas plataformas da Microsoft para reduzir o comprometimento em matéria de exploits, identidade e malware, desde o chip à cloud. Criadores da plataforma Secured-core da Microsoft para PC, Periferia e Servidor, do processador de segurança Microsoft Pluton e muito mais.

Rede Azure, Core: uma equipa de rede na cloud dedicada à WAN da Microsoft, a redes de datacenters e à infraestrutura de ampliação de redes por software do Azure, incluindo a plataforma DDoS, a plataforma de periferia de rede e os produtos de segurança de rede, como o Azure WAF, o Azure Firewall e a norma Azure DDoS Protection.

Equipa de Investigação de Segurança na Cloud: ao proteger a Microsoft Cloud, criar produtos e funcionalidades de segurança inovadores e apostar na investigação, esta equipa protege e proporciona aos clientes da Microsoft os meios necessários para transformarem as suas organizações de forma segura.

Segurança e Confiança dos Clientes (CST): uma equipa que promove a melhoria contínua da segurança dos clientes nos serviços online e produtos da Microsoft. Em colaboração com as equipas de engenharia e segurança de toda a empresa, a equipa da CST assegura a conformidade, melhora a segurança e proporciona maior transparência para proteger os clientes e promover a confiança global na Microsoft.

Sucesso dos Clientes: as equipas de segurança dedicadas ao Sucesso dos Clientes trabalham diretamente com os clientes para partilhar as melhores práticas, lições aprendidas e orientações no sentido de acelerar a transformação e a modernização da segurança. Esta equipa reúne e organiza as melhores práticas e lições aprendidas resultantes do percurso da Microsoft, e dos respetivos clientes, para criar estratégias de referência, arquiteturas de referência, planos de referência e muito mais.

Centro de Operações de Ciberdefesa (CDOC): as instalações da Microsoft dedicadas à cibersegurança e defesa constituem um centro de fusão que reúne profissionais de segurança de toda a empresa para proteger a nossa infraestrutura corporativa e a infraestrutura de cloud a que os clientes têm acesso. Os responsáveis pelas respostas a incidentes trabalham lado a lado com cientistas de dados e engenheiros de segurança de todos os grupos de serviços, produtos e dispositivos da Microsoft para proporcionarem meios de deteção, resposta e proteção contra ameaças 24 horas por dia, 7 dias por semana.

Iniciativa Democracy Forward: uma equipa da Microsoft que desenvolve esforços no sentido de preservar, proteger e promover os princípios fundamentais da democracia ao promover um ecossistema de informações saudável, salvaguardar processos democráticos abertos e seguros e defender a responsabilidade cívica empresarial.

Unidade de Crimes Digitais (DCU): uma equipa de advogados, investigadores, cientistas de dados, engenheiros, analistas e profissionais empresariais dedicados a combater o cibercrime a uma escala global através da aplicação de tecnologia, práticas forenses, ações civis, representações criminais e parcerias público-privadas.

Diplomacia Digital: uma equipa internacional de antigos diplomatas, decisores políticos e juristas que trabalham com o objetivo de promover um ciberespaço pacífico, estável e seguro face ao crescente conflito entre estados-nação.

Segurança e Resiliência Digitais (DSR): uma organização dedicada a proporcionar à Microsoft os meios necessários para a criação de dispositivos e serviços mais fidedignos, ao mesmo tempo que mantém a empresa segura e os dados protegidos, tanto os da empresa como os dos clientes.

Unidade de Segurança Digital (DSU): uma equipa de advogados e analistas de cibersegurança que oferecem conhecimentos jurídicos, geopolíticos e técnicos especializados para proteger a Microsoft e os respetivos clientes. A DSU fomenta a confiança nas defesas de segurança empresarial da Microsoft contra adversários cibernéticos avançados em todo o mundo.

Digital Threat Analysis Center (DTAC): uma equipa de especialistas que analisam e assinalam as ameaças de Estados-nação, incluindo ciberataques e operações de influência. A equipa combina informações e dados sobre ciberameaças com a análise geopolítica para fornecer insights aos nossos clientes e à Microsoft com o objetivo de oferecer insights e propor uma resposta e medidas de proteção eficazes.

Empresa e Segurança: uma equipa que se dedica à disponibilização de uma plataforma moderna, segura e mais fácil de gerir para a cloud inteligente e a periferia inteligente.

Mobilidade Empresarial: uma equipa que ajuda a proporcionar um local de trabalho moderno e uma gestão moderna a fim de manter os dados seguros, na cloud e on-premises. O Endpoint Manager inclui os serviços e as ferramentas utilizados pela Microsoft e pelos clientes para gerir e monitorizar dispositivos móveis, computadores de secretária, máquinas virtuais, dispositivos incorporados e servidores.

Equipas Contribuidoras

Continuação

Gestão de Riscos Empresariais: uma equipa que trabalha com as várias unidades de negócio no sentido de priorizar as discussões sobre riscos com as chefias superiores da Microsoft. A equipa de ERM liga as várias equipas de riscos operacionais, gere a estrutura de riscos empresariais da Microsoft e facilita a avaliação da segurança interna da empresa através da NIST Cybersecurity Framework.

Política de Cibersegurança Global: uma equipa que trabalha com governos, ONGs e parceiros do setor para promover políticas públicas de cibersegurança que capacitam os clientes a fortalecer a sua segurança e resiliência à medida que adotam e utilizam tecnologia da Microsoft.

Segurança de Acesso à Rede e Identidades (IDNA): uma equipa que trabalha para proteger todos os clientes da Microsoft contra o acesso não autorizado e as fraudes. A Segurança de IDNA é uma equipa interdisciplinar de engenheiros, gestores de produtos, cientistas de dados e investigadores de segurança.

M365 Security: uma organização que desenvolve soluções de segurança, incluindo o Microsoft Defender para Endpoint (MDE), o Microsoft Defender para Identidade (MDI), entre outros, para proteger os clientes empresariais.

IA, Ética e Efeitos na Área de Engenharia e Investigação (AETHER) da Microsoft: um conselho consultivo da Microsoft com a missão de assegurar que as novas tecnologias são desenvolvidas e formuladas de forma responsável.

Pesquisa e Distribuição do Microsoft Bing: uma equipa dedicada a fornecer um motor de busca na Internet de classe mundial, permitindo que utilizadores de todo o mundo encontrem rapidamente informações e resultados de pesquisa fidedignos, incluindo o acompanhamento de tópicos e histórias populares que lhes interessam, ao mesmo tempo que possibilita aos utilizadores controlar a respetiva privacidade.

Soluções para Clientes e Parceiros da Microsoft: organização de comercialização unificada da Microsoft responsável por funções no terreno, como especialistas e consultores em segurança e vendas técnicas.

Microsoft Defender Experts: a maior organização global da Microsoft de investigadores em segurança dos produtos, cientistas aplicados e analistas de informações sobre ameaças. A Defender Experts oferece capacidades de deteção e resposta inovadoras em produtos de segurança do Microsoft 365 e serviços geridos da Microsoft Defender Experts.

Microsoft Defender para IoT: uma equipa composta por investigadores da área especializados em engenharia reversa de firmware, protocolos e malware de IoT/OT. Esta equipa busca ameaças de IoT/OT como objetivo de desvendar tendências e campanhas maliciosas.

Informações sobre Ameaças do Microsoft Defender (RiskIQ): uma equipa que produz informações táticas através da análise da extensa coleção de telemetria externa da Microsoft, traçando o panorama das ameaças à medida que este evolui para descobrir a infraestrutura de ameaças anteriormente desconhecida e acrescentando contexto às campanhas e aos atores das ameaças. A equipa publica regularmente pesquisas atempadas e distintas para fornecer informações táticas cruciais aos defensores.

Equipa de Desenvolvimento Empresarial de Segurança da Microsoft: uma equipa que lidera a estratégia de crescimento da cibersegurança, as parcerias e os investimentos estratégicos da Microsoft.

Centro de Resposta de Segurança da Microsoft (MSRC): uma equipa que trabalha com investigadores de segurança e cuja missão é proteger os clientes e o ecossistema de parceiros da Microsoft. Parte integrante do Centro de Operações de Ciberdefesa (CDOC) da Microsoft, o MSRC reúne especialistas em respostas de segurança dedicados à deteção e resposta a ameaças em tempo real.

Serviços de Segurança da Microsoft para Resposta a Incidentes: uma equipa de especialistas em cibersegurança que ajuda os clientes ao longo do ciclo completo do ciberataque, desde a investigação à implementação bem-sucedida das atividades de contenção e recuperação relacionadas. Os serviços são disponibilizados através de duas equipas altamente integradas, a Equipa de Deteção e Resposta (DART), focada na investigação e no estabelecimento de bases para a recuperação, e a equipa de Práticas de Segurança de Recuperação Pós-comprometimento (CRSP), dedicada às vertentes da contenção e recuperação.

Centro de Informações Sobre Ameaças da Microsoft (MSTIC): uma equipa dedicada à identificação, monitorização e recolha de informações relacionadas com os adversários mais sofisticados que afetam os clientes da Microsoft, incluindo ameaças de Estados-nação, malware e phishing.

One Engineering System (1ES): uma equipa cuja missão é disponibilizar ferramentas de classe mundial para ajudar a tornar os programadores da Microsoft o mais produtivos e seguros que for possível. A equipa lidera a estratégia central de proteção da cadeia de fornecimento de software completa da Microsoft.

Centro de Informações sobre Ameaças Operacionais (OpTIC): a equipa responsável pela gestão e disseminação de informações sobre ciberameaças que dá suporte à missão do Centro de Operações de Ciberdefesa da Microsoft (CDOC) de proteger a Microsoft e respetivos clientes.

Microsoft

Ilustração do panorama de ameaças e promoção de uma defesa digital.

- Saiba mais: **https://microsoft.com/mddr**
- Aprofunde os seus pontos: **https://blogs.microsoft.com/on-the-issues/**
- Mantenha-se ligado: **@msftissues e @msftsecurity**