Microsoft

Microsoft Digital Defense Report 2022

Licht werpen op het bedreigingslandschap en een digitale verdediging mogelijk maken.

Inhoudsopgave

De data, inzichten en gebeurtenissen in dit rapport zijn van juli 2021 tot en met juni 2022 (fiscaal jaar 2022 van Microsoft), tenzij anders vermeld.

Voor de beste ervaring bij het bekijken en navigeren in dit rapport raden we aan om Adobe Reader te gebruiken, dat gratis kan worden gedownload van de Adobe-website.

Inleiding door Tom Burt

Corporate Vice President, Customer Security & Trust

"De biljoenen signalen die we analyseren uit ons wereldwijde ecosysteem van producten en diensten onthullen de heftigheid, de reikwijdte en de omvang van digitale bedreigingen over de hele wereld "

Een momentopname van ons landschap...

Reikwijdte en omvang van het dreigingsland-schap

Het aantal wachtwoord-aanvallen is gestegen tot naar schatting 921 aanvallen per seconde, een toename van 74% vergeleken met slechts een jaar geleden.

Ontmanteling van cybercriminaliteit

Tot op heden heeft Microsoft meer dan 10.000 domeinen verwijderd die door cybercriminelen worden gebruikt en 600 die door actoren van vreemde mogendheden worden gebruikt.

Aanpak van kwetsbaarheden

Bij 93% van onze incidentrespons na ransomware-incidenten bleek dat er onvoldoende controle was over toegangsrechten en zijdelingse verplaatsing.

Op 23 februari 2022 betrad de wereld van de cyberbeveiliging een nieuw tijdperk, namelijk het tijdperk van de hybride oorlog. Op die dag, uren voordat raketten werden gelanceerd en tanks de grenzen overstaken, lanceerden Russische actoren een massale verwoestende cyberaanval tegen doelen van de regering, de technologie en de financiële sector in Oekraïne. Je kunt meer lezen over deze aanvallen en de lessen die je daaruit kunt trekken in het hoofdstuk Bedreigingen door vreemde mogendheden van deze derde jaarlijkse editie van het Microsoft Digital Defense Report (MDDR). Een van de belangrijkste lessen is dat de cloud de beste fysieke en logische beveiliging biedt tegen cyberaanvallen en vooruitgang mogelijk maakt op het gebied van bedreigingsinformatie en endpointbescherming die zijn waarde heeft bewezen in Oekraïne.

Hoewel elk onderzoek naar de ontwikkelingen in cyberbeveiliging dit jaar daar moet beginnen, biedt het rapport van dit jaar een diepe duik in nog veel meer onderwerpen. In het eerste hoofdstuk van het rapport richten we ons op de activiteiten van cybercriminelen, gevolgd door bedreigingen door vreemde mogendheden in hoofdstuk twee. Beide groepen hebben hun aanvallen veel geavanceerder gemaakt, waardoor de impact van hun acties drastisch is toegenomen. Terwijl Rusland in het nieuws kwam, voerden Iraanse actoren hun aanvallen op na een presidentiële machtsovername, waarbij ze vernietigende aanvallen op Israël lanceerden, en ransomware- en hack-en-lekaanvallen op essentiële infrastructuur in de Verenigde Staten. Ook China heeft zijn spionage-inspanningen in Zuidoost-Azië en elders in het zuidelijke deel van de wereld opgevoerd om de Amerikaanse invloed tegen te gaan en essentiële data en informatie te stelen.

Buitenlandse actoren gebruiken ook zeer effectieve technieken om door de propaganda beïnvloede activiteiten in regio's over de hele wereld mogelijk te maken, zoals behandeld in het derde hoofdstuk. Rusland heeft bijvoorbeeld hard gewerkt om zijn burgers, en de burgers van veel andere landen, ervan te overtuigen dat de invasie in Oekraïne gerechtvaardigd was, terwijl er ook propaganda werd verspreid die COVID-vaccins in het Westen in diskrediet bracht en tegelijkertijd hun effectiviteit in eigen land promootte. Daarnaast richten actoren zich steeds meer op IoT-apparaten (Internet of Things) of besturingsapparaten voor operationele technologie (OT) als toegangspunten tot netwerken en essentiële infrastructuur. Dit wordt besproken in hoofdstuk vier. Tot slot bespreken we in het laatste hoofdstuk de inzichten en lessen die we het afgelopen jaar hebben geleerd bij de verdediging tegen aanvallen op Microsoft en onze klanten, terwijl we de ontwikkelingen van het jaar op het gebied van cyberveerkracht evalueren.

Elk hoofdstuk bevat de belangrijkste lessen en inzichten op basis van het unieke gezichtspunt van Microsoft. De biljoenen signalen die we analyseren uit ons wereldwijde ecosysteem van producten en diensten onthullen de heftigheid, de reikwijdte en de omvang van digitale bedreigingen over de hele wereld. Microsoft neemt maatregelen om onze klanten en het digitale ecosysteem tegen deze bedreigingen te beschermen. Je kunt ook lezen over onze technologie die miljarden pogingen tot phishing, identiteitsdiefstal en andere bedreigingen voor onze klanten identificeert en blokkeert.

Inleiding door Tom Burt

Vervolg

We gebruiken ook juridische en technische middelen voor het in beslag nemen en afsluiten van de infrastructuur die wordt gebruikt door cybercriminelen en actoren van vreemde mogendheden en om klanten te informeren wanneer ze worden bedreigd of aangevallen door een actor van een vreemde mogendheid. We werken aan het ontwikkelen van steeds effectievere functies en services die gebruikmaken van AI/ML-technologie om cyberdreigingen te identificeren en blokkeren en van beveiligingsprofessionals die zich sneller en effectiever kunnen verdedigen tegen cyberinbreuken.

Misschien wel het allerbelangrijkste: in de hele MDDR bieden we ons beste advies over de stappen die individuen, organisaties en ondernemingen kunnen nemen om zich te verdedigen tegen deze toenemende digitale bedreigingen. Het toepassen van goede praktijken voor cyberhygiëne is de beste verdediging en kan het risico op cyberaanvallen aanzienlijk verminderen.

De staat van cybercriminaliteit

Cybercriminelen blijven optreden als geavanceerde bedrijven met winstoogmerken. Aanvallers passen zich aan en vinden nieuwe manieren om hun technieken te implementeren, waardoor de complexiteit toeneemt van hoe en waar ze de infrastructuur voor campagneactiviteiten hosten. Tegelijkertijd worden cybercriminelen zuiniger. Om hun overhead te verlagen en de schijn van legitimiteit te wekken, maken aanvallers gebruik van zakelijke netwerken en apparaten om phishingcampagnes of malware te hosten of zelfs hun rekenkracht te gebruiken om cryptovaluta te minen.

Ga voor meer informatie naar p6

"De opkomst van de inzet van cyberwapens in de hybride oorlog in Oekraïne is het begin van een nieuw tijdperk van conflicten."

Bedreigingen door vreemde mogendheden

Actoren van vreemde mogendheden lanceren steeds geavanceerdere cyberaanvallen die zijn ontworpen om detectie te omzeilen en hun strategische prioriteiten te bevorderen. De opkomst van de inzet van cyberwapens in de hybride oorlog in Oekraïne is het begin van een nieuw tijdperk van conflicten. Rusland heeft zijn oorlog ook ondersteund met informatiebeïnvloedingsactiviteiten, met behulp van propaganda om meningen in Rusland, Oekraïne en wereldwijd te beïnvloeden. Buiten Oekraïne zijn actoren van vreemde mogendheden steeds meer actief en gebruiken ze nieuwe ontwikkelingen in automatisering, cloudinfrastructuur en technologieën voor externe toegang om een breder scala aan doelen aan te vallen. Vaak werden IT-supply chains van bedrijven die toegang tot de uiteindelijke doelen mogelijk maken, aangevallen. Cyberbeveiliging werd nog belangrijker omdat actoren snel gebruikmaakten van niet-gepatchte kwetsbaarheden, zowel geavanceerde als brute force-technieken gebruikten om aanmeldingsreferenties te stelen en hun activiteiten verhulden met open-source- of legitieme software. Daarnaast sluit Iran zich aan bij Rusland bij het gebruik van destructieve cyberwapens, waaronder ransomware, als onderdeel van hun aanvallen.

Deze ontwikkelingen vereisen een dringende invoering van een consistent, wereldwijd kader dat prioriteit geeft aan mensenrechten en mensen beschermt tegen roekeloos online gedrag van de staat. Alle landen moeten samenwerken om normen en regels voor verantwoord gedrag van de staat te implementeren.

Ga voor meer informatie naar p30

Apparaten en infrastructuur

De pandemie, in combinatie met de snelle invoering van allerlei internetapparaten als onderdeel van de versnelling van de digitale transformatie, heeft het aanvalsoppervlak van onze digitale wereld sterk vergroot. Het gevolg is dat cybercriminelen en vreemde mogendheden snel profiteren. Hoewel de beveiliging van IT-hardware en -software de afgelopen jaren is verbeterd, heeft de beveiliging van IoT- en OT-apparaten geen gelijke tred gehouden. Bedreigingsactoren benutten deze apparaten om toegang tot netwerken te krijgen en laterale verplaatsing mogelijk te maken, een voet aan de grond te krijgen in een supply chain of de OT-activiteiten van de doelorganisatie te verstoren.

Ga voor meer informatie naar p56

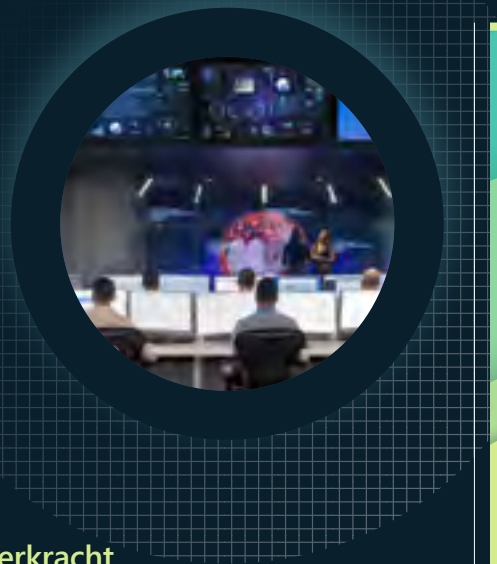
Inleiding door Tom Burt

Vervolg

Cyberbeïnvloedingsactiviteiten

Vreemde mogendheden maken steeds vaker gebruik van geavanceerde beïnvloedingsactiviteiten om propaganda te verspreiden en invloed uit te oefenen op de publieke opinie, zowel nationaal als internationaal. Deze campagnes tasten het vertrouwen aan, vergroten de polarisatie en bedreigen democratische processen. Deskundige geschoolde hardnekkige manipulators gebruiken traditionele media samen met internet en sociale media om de reikwijdte, schaal en efficiëntie van hun campagnes en de grote impact die deze hebben op het wereldwijde informatie-ecosysteem enorm te vergroten. In het afgelopen jaar hebben we gezien dat deze activiteiten werden gebruikt als onderdeel van de hybride oorlog in Rusland in Oekraïne, maar we zagen ook dat Rusland en andere landen, waaronder China en Iran, in toenemende mate propagandamaatregelen inzetten die worden aangestuurd door sociale media om hun wereldwijde invloed op een scala van problemen uit te breiden.

Ga voor meer informatie naar p71



Cyberveerkracht

Beveiliging is een belangrijke drijvende factor voor technologisch succes. Innovatie en verhoogde productiviteit kunnen alleen worden bereikt door beveiligingsmaatregelen te nemen die organisaties zo veerkrachtig mogelijk maken tegen moderne aanvallen. De pandemie heeft ons bij Microsoft uitgedaagd om onze beveiligingspraktijken en -technologieën om te zetten in bescherming van onze werknemers, waar deze ook werken. Het afgelopen jaar bleven bedreigingsactoren profiteren van kwetsbaarheden die werden blootgelegd tijdens de pandemie en de verschuiving naar een hybride werkomgeving. Sindsdien is onze belangrijkste uitdaging het beheren van de prevalentie en complexiteit van verschillende aanvalsmethoden en de toegenomen activiteit van vreemde mogendheden. In dit hoofdstuk beschrijven we de uitdagingen waarmee we te maken hebben gehad en de verdedigingsmechanismen die we samen onze meer dan 15.000 partners hebben ingezet als reactie hierop.

Ga voor meer informatie naar p86

Ons unieke gezichtspunt

37 miljard
e-maildreigingen geblokkeerd

34,7 miljard
identiteitsdreigingen geblokkeerd

43 biljoen
signalen per dag gesynthetiseerd, met behulp van geavanceerde data-analytics en AI-algoritmen om digitale bedreigingen en criminele cyberactiviteit te begrijpen en hier bescherming tegen te bieden.

2,5 miljard
endpointsignalen per dag geanalyseerd

Meer dan 8500
technici, onderzoekers, datawetenschappers, cyberveiligheidsexperts, bedreigingsjagers, geopolitieke analisten, onderzoekers en eerstelijnsrespondenten in 77 landen.

Meer dan 15.000
partners in ons beveiligingsecosysteem die de cyberveerkracht van onze klanten vergroten.

Van 1 juli 2021 tot en met 30 juni 2022

Inleiding door Tom Burt

Vervolg

Wij zijn van mening dat Microsoft, onafhankelijk en via nauwe partnerschappen met anderen in de particuliere industrie, bij de overheid en in de burgermaatschappij, een verantwoordelijkheid heeft om de digitale systemen te beschermen die de sociale structuur van onze samenleving ondersteunen en veilige, veilige computeromgevingen te bevorderen voor elke persoon, waar deze zich ook bevindt. Deze verantwoordelijkheid is de reden dat we de MDDR elk jaar sinds 2020 hebben gepubliceerd. Het rapport is het resultaat van de enorme hoeveelheid data en het uitgebreide onderzoek van Microsoft. Het rapport deelt onze unieke inzichten over hoe het digitale dreigingslandschap evolueert en welke cruciale acties vandaag kunnen worden ondernomen om de beveiliging van het ecosysteem te verbeteren.

We hopen een gevoel van urgentie op te wekken, zodat lezers onmiddellijk actie ondernemen op basis van de data en inzichten die we hier en in onze vele cyberbeveiligingspublicaties het hele jaar door presenteren. Als we kijken naar de ernst van de bedreiging voor het digitale landschap, en de vertaling hiervan naar de fysieke wereld, is het belangrijk om te onthouden dat we allemaal in staat zijn om actie te ondernemen om onszelf, onze organisaties en ondernemingen te beschermen tegen digitale bedreigingen.

Bedankt dat je de tijd hebt genomen om het Microsoft Digital Defense Report voor dit jaar te bekijken. We hopen dat je vindt dat het waardevolle inzichten en aanbevelingen biedt om ons te helpen het digitale ecosysteem collectief te verdedigen.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Ons doel met dit rapport is tweeledig:

1. Om het veranderende digitale bedreigingslandschap voor onze klanten, partners en stakeholders in het bredere ecosysteem te belichten, een licht te werpen op zowel nieuwe cyberaanvallen als evoluerende trends in historisch hardnekkige bedreigingen.
2. Om onze klanten en partners in staat te stellen hun cyberveerkracht te verbeteren en te reageren op deze bedreigingen.

De staat van cybercriminaliteit

Terwijl cyberverdedigingen verbeteren en steeds meer organisaties een proactieve aanpak van preventie hanteren, passen aanvallers hun technieken aan.

Een overzicht van

de staat van cybercriminaliteit

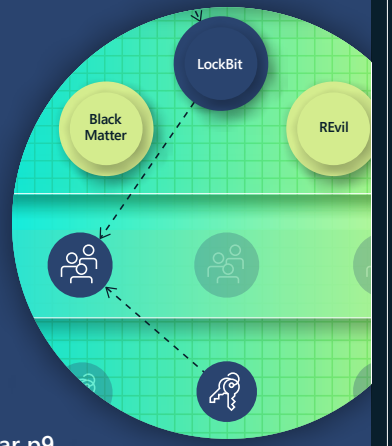
Terwijl cyberverdedigingen verbeteren en steeds meer organisaties een proactieve aanpak van preventie hanteren, passen aanvallers hun technieken aan.

Cybercriminelen blijven optreden als geavanceerde bedrijven met winstoogmerken. Aanvallers passen zich aan en vinden nieuwe manieren om hun technieken te implementeren, waardoor de complexiteit toeneemt van hoe en waar ze de infrastructuur voor campagneactiviteiten hosten. Tegelijkertijd worden cybercriminelen zuiniger. Om hun overhead te verlagen en de schijn van legitimiteit te wekken, maken aanvallers gebruik van zakelijke netwerken en apparaten om phishingcampagnes of malware te hosten of zelfs hun rekenkracht te gebruiken om cryptovaluta te minen.

Terwijl de industrialisering van de cybercriminaliteit de toegangsbarrière voor vaardigheden verlaagt door een betere toegang tot tools en infrastructuur te bieden, blijft cybercriminaliteit toenemen.

Ga voor meer informatie naar p18

De dreiging van ransomware en afpersing wordt steeds zwaarder met aanvallen op overheden, bedrijven en essentiële infrastructuur.

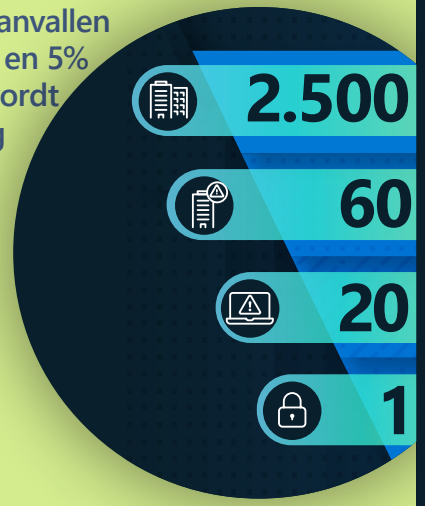


Ga voor meer informatie naar p9

Aanvallers dreigen steeds vaker gevoelige data bekend te maken om organisaties over te halen tot het betalen van losgeld.

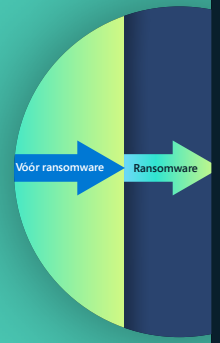
Ga voor meer informatie naar p10

Door mensen uitgevoerde ransomwareaanvallen komen het meest voor, aangezien een derde van de doelwitten met succes wordt gecompromitteerd door criminelen die deze aanvallen gebruiken en 5% daarvan wordt in gijzeling genomen.



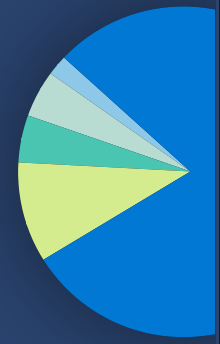
Ga voor meer informatie naar p9

De meest effectieve verdediging tegen ransomware omvat meervoudige verificatie, frequente beveiligings-patches en Zero Trust-principes in de netwerkarchitectuur.



Ga voor meer informatie naar p13

Phishingprogramma's voor referenties die zonder onderscheid alle postvakken als doelwit hebben, zijn in opkomst en zakelijke e-mailinbreuken, waaronder factuurfraude, vormen een aanzienlijk risico op cybercriminaliteit voor ondernemingen.

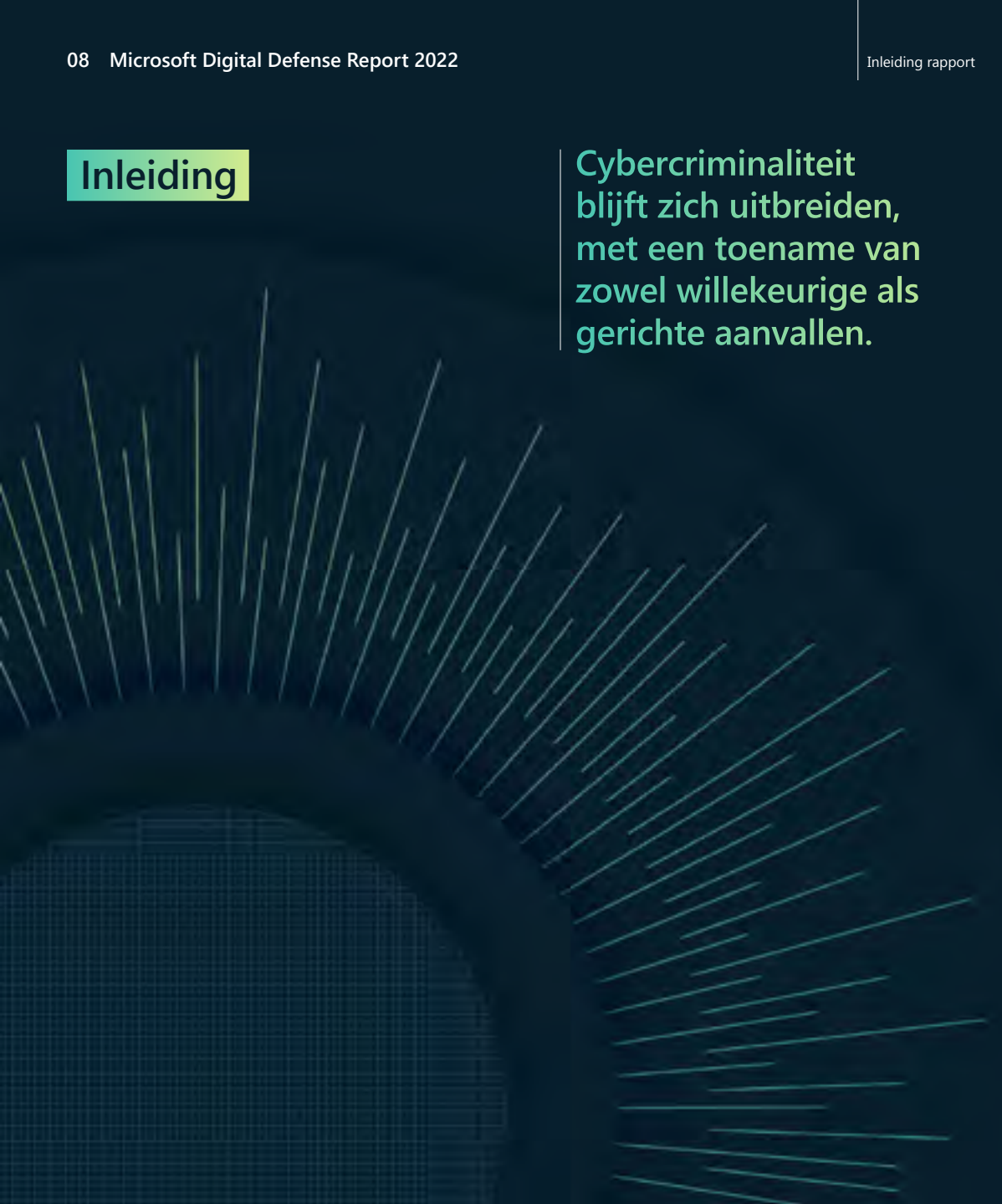


Ga voor meer informatie naar p21

Microsoft wil de schadelijke infrastructuren van cybercriminelen en actoren van vreemde mogendheden verstoren door te vertrouwen op innovatieve juridische benaderingen en onze publieke en private partnerschappen.

Ga voor meer informatie naar p25

Inleiding



Cybercriminaliteit blijft zich uitbreiden, met een toename van zowel willekeurige als gerichte aanvallen.

Naarmate cyberverdedigingen verbeteren en steeds meer overheden en bedrijven een proactieve aanpak van preventie hanteren, zien we dat aanvallers twee strategieën gebruiken om toegang te krijgen die nodig is om cybercriminaliteit te faciliteren. Eén aanpak is een campagne met brede doelwitten die afhankelijk is van volume. De andere maakt gebruik van bewaking en selectievere targeting om het rendement te verhogen. Zelfs wanneer het genereren van inkomsten niet het doel is, zoals activiteiten van een vreemde mogendheid voor geopolitieke doeleinden, worden zowel willekeurige als gerichte aanvallen gebruikt. Het afgelopen jaar bleven cybercriminelen afhankelijk van social engineering en de benutting van actuele kwesties om het succes van campagnes te maximaliseren. Bijvoorbeeld, terwijl phishing-lokmiddelen met een COVID-thema minder vaak werden gebruikt, zagen we dat het aantal lokmiddelen waarin om donaties ter ondersteuning van de burgers van Oekraïne werd gevraagd, toenam.

Aanvallers passen zich aan en vinden nieuwe manieren om hun technieken te implementeren, waardoor de complexiteit toeneemt van hoe en waar ze de infrastructuur voor campagneactiviteiten hosten. We hebben vastgesteld dat cybercriminelen zuiniger worden en dat aanvallers niet langer betalen voor technologie. Om hun overhead te verlagen en de schijn van legitimiteit te wekken, proberen sommige aanvallers in toenemende mate misbruik te maken van bedrijven om phishingcampagnes of malware te hosten of zelfs hun rekenkracht te gebruiken om cryptovaluta te minen. In dit hoofdstuk onderzoeken we ook de opkomst van hacktivisme, een verstoring die wordt veroorzaakt doordat privéburgers cyberaanvallen uitvoeren op sociale of politieke doelen. Duizenden mensen over de hele wereld, zowel experts als beginners, zijn sinds februari 2022 gemobiliseerd om aanvallen uit te voeren, zoals het uitschakelen van websites en het lekken van gestolen data als onderdeel van de oorlog tussen Rusland en Oekraïne. Het is te vroeg om te voorspellen of deze trend zal doorzetten na beëindiging van de actieve vijandelijkheden.

Organisaties moeten regelmatig toegangscontroles herzien en versterken en beveiligingsstrategieën implementeren om zich te verdedigen tegen cyberaanvallen. Dat is echter niet alles wat ze kunnen doen. We leggen uit hoe onze Digital Crimes Unit (DCU) civiele zaken heeft gebruikt om schadelijke infrastructuur in beslag te nemen die wordt gebruikt door cybercriminelen en actoren van vreemde mogendheden. We moeten deze bedreiging samen bestrijden via zowel openbare als particuliere partnerschappen. We hopen dat we anderen kunnen helpen bij het begrijpen en overwegen van de proactieve maatregelen die ze kunnen nemen om zichzelf en het bredere ecosysteem te beschermen tegen de steeds toenemende dreiging van cybercriminaliteit door te delen wat we de afgelopen 10 jaar hebben geleerd.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

Ransomware en afpersing: een bedreiging op nationaal niveau

Ransomwareaanvallen vormen een verhoogd gevaar voor alle individuen, omdat essentiële infrastructuur, bedrijven van elke omvang en staats- en lokale overheden het doelwit worden van criminelen die gebruikmaken van een groeiend cybercrimineel ecosysteem.

In de afgelopen twee jaar hebben spraakmakende ransomware-incidenten, zoals incidenten met essentiële infrastructuur, gezondheidszorg en IT-serviceproviders, aanzienlijke publieke aandacht getrokken. Naarmate ransomwareaanvallen steeds breder werden, zijn ook de effecten ervan toegenomen. Hier volgen enkele voorbeelden van aanvallen die we al in 2022 hebben gezien:

- In februari trof een aanval op twee bedrijven de betalingsverwerkingssystemen van honderden tankstations in Noord-Duitsland.[1]
- In maart werd de postbezorging tijdelijk verstoord door een aanval op de Griekse posterijen, wat van invloed was op de verwerking van financiële transacties.[2]
- Eind mei dwong een ransomwareaanval overheidsinstanties in Costa Rica om een nationale noodsituatie uit te roepen nadat ziekenhuizen waren gesloten en de douane- en belastinginning werd verstoord.[3]
- Ook in mei veroorzaakte een aanval vertragingen en annuleringen van een van de grootste luchtvaartmaatschappijen in India, waardoor honderden passagiers gestrand raakten.[4]

Het succes van deze aanvallen en de omvang van hun impact in de praktijk zijn het resultaat van een industrialisatie van de cybercriminaliteitseconomie, die toegang tot tools en infrastructuur mogelijk maakt en cybercriminaliteit uitbreidt door hun vaardigheidsbarrière te verlagen.

In de afgelopen jaren is ransomware overgestapt van een model waarbij een enkele 'bende' een ransomware-payload ontwikkelden en distribueerden naar het model van ransomware-as-a-service (RaaS). RaaS stelt één groep in staat om de ontwikkeling van de ransomware-payload te beheren en services voor betaling en afpersing via datalekken te leveren aan andere cybercriminelen die daadwerkelijk de ransomwareaanvallen uitvoeren, de zogenaamde 'partners', in ruil voor een deel van de buit. Deze franchising van de cybercriminaliteit heeft tot een uitbreiding van het aantal aanvallers geleid. De industrialisatie van tools voor cybercriminaliteit heeft het voor aanvallers gemakkelijker gemaakt om inbreuken te plegen, data te stelen en ransomware te implementeren.

Door mensen uitgevoerde ransomwareaanvallen[5], een term die is bedacht door Microsoft-onderzoekers om bedreigingen te beschrijven die worden uitgevoerd door mensen die in elke fase van de aanval beslissingen nemen op basis van wat ze ontdekken in het netwerk van hun doelwit en de dreiging afbakenen van standaard ransomwareaanvallen, blijft een belangrijke bedreiging voor organisaties.

Model gebaseerd op Microsoft Defender voor Eindpunt-data (EDR) (januari-juni 2022).

Ransomware en afpersing: Een bedreiging op nationaal niveau

Vervolg

Ransomwareaanvallen zijn nog effectiever geworden omdat de invoering van een dubbele afpersingsstrategie een standaardpraktijk is geworden. Dit omvat het stelen van data van gecompromitteerde apparaten, het versleutelen van de data op de apparaten en het vervolgens publiceren of dreigen te publiceren van de gestolen data om slachtoffers te dwingen tot het betalen van losgeld.

Hoewel de meeste ransomwareaanvallers ransomware op opportunistische wijze implementeren op het netwerk waartoe zij toegang krijgen, kopen sommigen toegang bij andere cybercriminelen, waarbij ze gebruikmaken van connecties tussen toegangsmakelaars en ransomwareoperators.

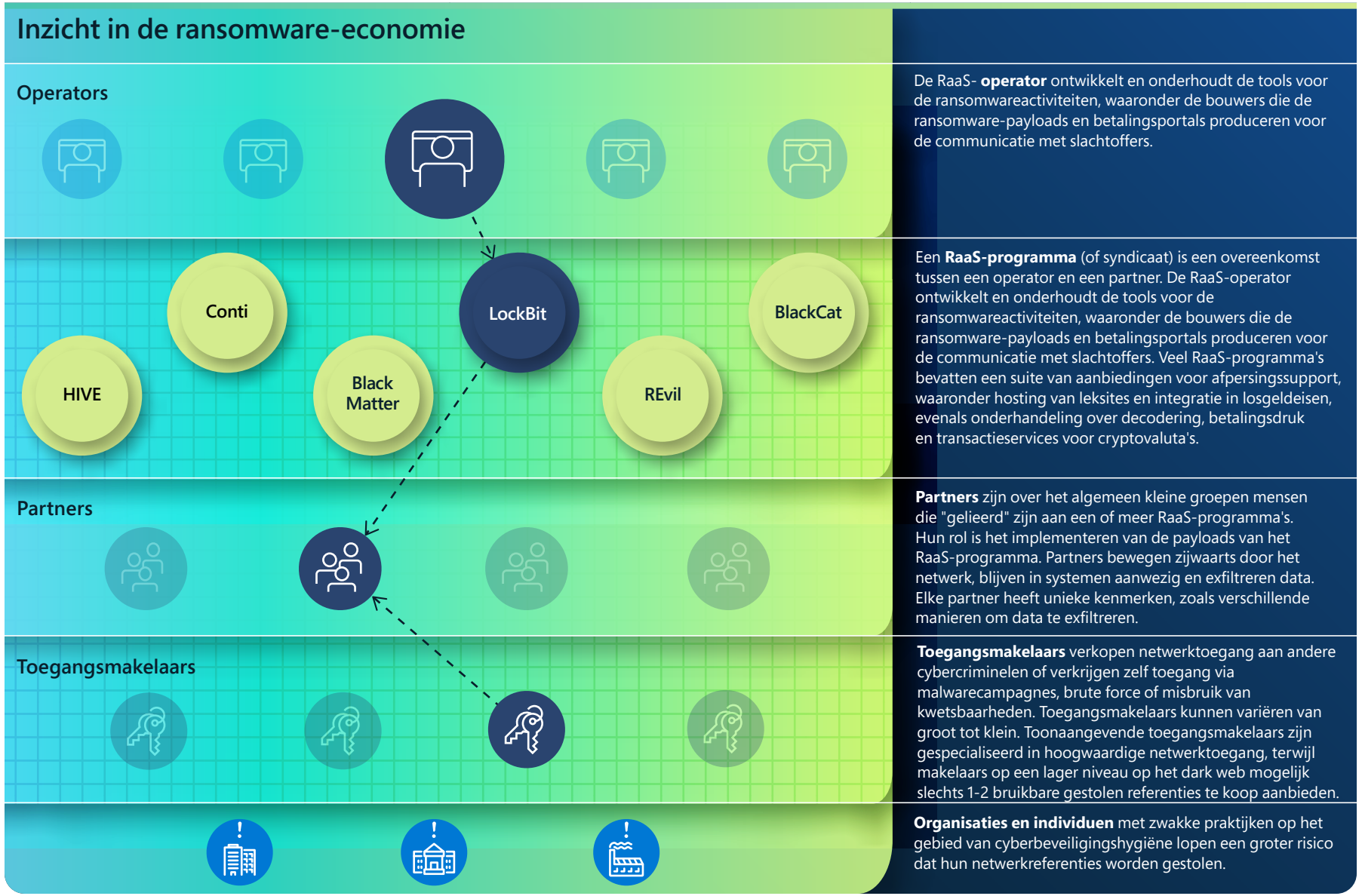
Onze unieke verscheidenheid aan signaalintelligentie wordt verzameld uit meerdere bronnen (identiteit, e-mail, endpoints en cloud) en biedt inzicht in de groeiende ransomware-economie, compleet met een verbonden systeem dat tools bevat die zijn ontworpen voor aanvallers met minder technische vaardigheden.

De uitbreiding van de relaties tussen gespecialiseerde cybercriminelen heeft het tempo, de verfijning en het succes van ransomwareaanvallen verhoogd. Dit heeft geleid tot de evolutie van het cybercriminele ecosysteem tot verbonden spelers met verschillende technieken, doelen en vaardigheden die elkaar ondersteunen bij de eerste toegang tot doelen, betalingsdiensten en decryptie- of publicatietools of -sites.

Ransomwareoperators kunnen nu online toegang tot organisaties of overheidsnetwerken kopen of referenties en toegang verkrijgen via interpersoonlijke relaties met makelaars die als hoofddoel hebben de verkregen toegang te gelde te maken.

De operators gebruiken vervolgens de gekochte toegang om een ransomware-payload te implementeren die is gekocht via marktplaatsen of forums op het dark web. In veel gevallen worden de onderhandelingen met slachtoffers gevoerd door het RaaS-team, niet door de operators zelf. Deze criminele transacties verlopen naadloos en de deelnemers lopen weinig kans om te worden gearresteerd en in staat van beschuldiging gesteld vanwege de anonimiteit van het dark web en de moeilijkheid om wetten overlandsgrenzen heen te handhaven.

Een duurzame en succesvolle aanpak van deze dreiging vereist een strategie van de gehele overheid in nauwe samenwerking met de particuliere sector.



In tegenstelling tot hoe ransomware soms wordt weergegeven in de media, komt het zelden voor dat een enkele ransomware-variant wordt beheerd door één end-to-end 'ransomware-bende'. In plaats daarvan zijn er afzonderlijke entiteiten die malware bouwen, toegang krijgen tot slachtoffers, ransomware implementeren en afpersingsonderhandelingen voeren. De industrialisatie van het criminele ecosysteem heeft geleid tot:

- Toegangsmakelaars die inbreken en toegang verlenen (Access as a Service).
- Malware-developers die tooling verkopen.
- Criminelen en hun partners die inbreuken plegen.
- Encryptie- en afpersingsserviceproviders die het genereren van inkomsten overnemen van partners (RaaS).

Alle door mensen beheerde ransomware-campagnes delen gemeenschappelijke afhankelijkheden van zwakke punten in de beveiliging. In het bijzonder profiteren aanvallers meestal van de slechte cyberhygiëne van een organisatie, die vaak gepaard gaat met onregelmatige patches en het niet implementeren van meervoudige verificatie (MFA).

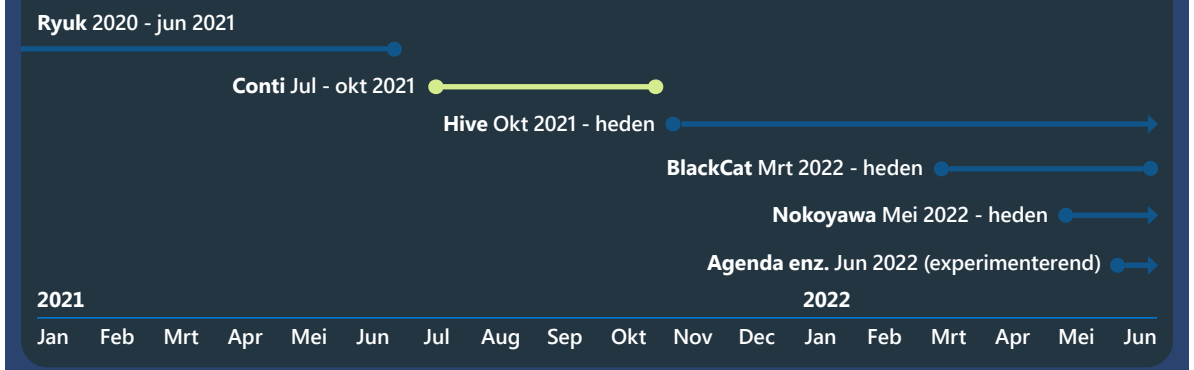
Casestudie: De ontbinding van Conti

Conti, een van de belangrijkste ransomware-varianten in de afgelopen twee jaar, begon zijn activiteiten halverwege 2022 te staken, waarbij het Microsoft Threat Intelligence Center (MSTIC) eind maart en begin april een aanzienlijke daling van de activiteiten constateerde. We zagen de laatste Conti-ransomware-implementaties half april. De ontbinding van Conti had echter, net als de sluitingen van andere ransomwareactiviteiten, geen significante invloed op ransomware-implementaties, omdat MSTIC constateerde dat Conti-partners op andere ransomware-payloads overstapten, waaronder Blackbasta, Lockbit 2.0, LockbitBlack en HIVE. Dit is in overeenstemming met data van voorgaande jaren en suggereert dat wanneer ransomware-bendes offline gaan, ze maanden later opnieuw verschijnen of hun technische mogelijkheden en middelen aan nieuwe groepen ter beschikking stellen.

Onze Microsoft-teams voor bedreigingsinformatie houden bedreigingen van ransomware bij als individuele groepen (aangeduid als DEV's) op basis van hun specifieke tools, in plaats van ze te volgen op basis van de malware die ze gebruiken. Dit betekende dat toen de partners van Conti verspreid gingen werken, we in staat waren om deze DEV's te blijven volgen door hun gebruik van andere tools of RaaS-kits. Een voorbeeld:

- DEV-0230, dat samenwerkt met Trickbot, was een productieve gebruiker van Conti. Eind april merkte MSTIC op dat er gebruik werd gemaakt van QuantumLocker.
- DEV-0237 stapte over van de ransomware-kit van Conti naar HIVE en Nokoyawa, inclusief het gebruik van HIVE bij de aanval op 31 mei tegen overheidsinstanties in Costa Rica.
- DEV-0506, een andere productieve gebruiker van de Conti-ransomware-kit, ging gebruikmaken van BlackBasta.

Voorbeeld van een partner (DEV-0237) die snel wisselt tussen RaaS-programma's



Nadat een RaaS-programma zoals Conti uit de lucht is gehaald, schakelt de ransomware-partner vrijwel onmiddellijk over naar een ander (Hive).

RaaS ontwikkelt het ransomware-ecosysteem en belemmert de toeschrijving

Omdat door mensen beheerde ransomware wordt aangedreven door individuele operators, variëren aanvalspatronen afhankelijk van het doelwit en worden deze afgewisseld tijdens een aanval. In het verleden zagen we een nauwe relatie tussen de aanvankelijke invoervector, tools en keuzes voor ransomware-payload in elke campagne van een enkele ransomware-variant. Dit maakte toeschrijving gemakkelijker. Het RaaS-partnermodel zorgt echter voor een ontkoppeling van deze relatie. Als gevolg hiervan houdt Microsoft aan ransomware gelieerde partners bij die bij specifieke aanvallen payloads implementeren, in plaats van de developers van de ransomware-payload als operators te volgen.

Met andere woorden, we gaan er niet langer van uit dat de HIVE-developer de operator is achter een HIVE-ransomwareaanval. Het is waarschijnlijker dat dit het werk van een partner is.

De cyberbeveiligingssector heeft moeite om deze afbakening tussen developers en operators adequaat vast te leggen. De branche meldt nog steeds vaak een incident met ransomware aan de hand van de naam van de payload, waardoor de valse indruk wordt gewekt dat een enkele entiteit, of ransomware-bende, achter alle aanvallen zit met behulp van die specifieke ransomware-payload, en alle incidenten die daarmee verband houden, en dat alle hierbij betrokken incidenten gemeenschappelijke technieken en infrastructuur delen. Om netwerkverdedigers te ondersteunen, is het belangrijk om meer te weten te komen over de fasen die voorafgaan aan de aanvallen van verschillende partners, zoals data-exfiltratie en extra persistentiemechanismen, en de detectie- en beveiligingsmogelijkheden die mogelijk bestaan.

Meer nog dan malware, hebben aanvallers referenties nodig om hun activiteiten te doen slagen. De succesvolle door mensen uitgevoerde ransomware-infectie van een hele organisatie is afhankelijk van toegang tot een account met een uitgebreide machtigingen.

Spotlight op door mensen uitgevoerde ransomwareaanvallen

In het afgelopen jaar hebben de ransomware-experts van Microsoft diepgaand onderzoek gedaan naar meer dan 100 incidenten met ransomware die door mensen worden uitgevoerd om de technieken van aanvallers te volgen en te begrijpen hoe we onze klanten beter kunnen beschermen.

Het is belangrijk op te merken dat de analyse die we hier delen alleen mogelijk is voor onboarded, beheerde apparaten. Niet-onboarded, niet-beheerde apparaten vormen het minst veilige deel van de hardwaremiddelen van een organisatie.

Meest voorkomende ransomware-fasetechnieken:

75%
Gebruikt beheertools.

75%
Gebruikt verworven gehackte gebruikersaccount met uitgebreide bevoegdheden om schadelijke payloads te verspreiden via het SMB-protocol.

99%
Probeert ontdekte beveiligings- en back-upproducten te manipuleren met tools die voor het besturingssysteem zijn gebouwd.

De typische door mensen uitgevoerde aanval

Door mensen uitgevoerde ransomwareaanvallen kunnen worden onderverdeeld in de pre-ransomware-fase en de implementatiefase van ransomware. Tijdens de pre-ransomware-fase bereiden aanvallers zich voor om het netwerk te infiltreren door meer te weten te komen over de typologie en de beveiligingsinfrastructuur van de organisatie.

Stop de aanvallers voordat ze de implementatiefase van ransomware bereiken	**Implementatie!**
Vóór ransomware	**Ransomware**
Deze fase kan variëren van enkele dagen tot enkele weken of maanden, hoewel deze de afgelopen twee jaar is ingekort.	Deze fase kan slechts enkele minuten duren
Aanvallers bereiden zich voor op het infiltreren in het netwerk door zo veel mogelijk te weten te komen over de topologie en beveiligingsinfrastructuur. Aanvallers kunnen ook data exfiltreren in deze fase.	Aanvallers willen zo veel mogelijk data versleutelen.

Uit ons onderzoek bleek dat de meeste actoren achter door de mens uitgevoerde ransomwareaanvallen gebruikmaken van vergelijkbare zwakke punten in de beveiliging en gemeenschappelijke aanvalspatronen en -technieken delen.

Een duurzame beveiligingsstrategie

Het bestrijden en voorkomen van dit soort aanvallen vereist een verandering in de mentaliteit van een organisatie om zich te richten op de uitgebreide bescherming die nodig is om aanvallers te vertragen en af te stoppen voordat ze kunnen overstappen van de pre-ransomware-fase naar de ransomware-implementatiefase.

Ondernemingen moeten best practices op het gebied van beveiliging op consistente en strikte wijze toepassen op hun netwerken, met het beperken van aanvallen als doel. Als gevolg van de menselijke besluitvorming kunnen deze ransomwareaanvallen meerdere, schijnbaar uiteenlopende beveiligingsproductwaarschuwingen genereren die gemakkelijk verloren kunnen gaan of waarop niet tijdig wordt gereageerd. Waarschuwingsmoeheid is reëel, en Security Operations Centers (SOC's) kunnen hun leven gemakkelijker maken door te kijken naar trends in hun waarschuwingen of door waarschuwingen te groeperen in incidenten, zodat ze een totaaloverzicht krijgen. SOC's kunnen vervolgens waarschuwingen beperken met behulp van versterkingsmogelijkheden, zoals regels voor het verkleinen van het aanvalsoppervlak. Versterking tegen gemeenschappelijke bedreigingen kan niet alleen het waarschuwingsvolume terugbrengen, maar ook veel aanvallers stoppen voordat ze toegang krijgen tot netwerken.

Organisaties moeten voortdurend hoge normen van beveiliging en netwerkhygiëne handhaven om zichzelf te beschermen tegen door mensen uitgevoerde ransomwareaanvallen.

Direct bruikbare inzichten

Ransomwareaanvallers gaan voor gemakkelijke winsten, dus vormt verhoging van hun kosten via versterking van de beveiliging de sleutel tot het verstoren van de economie van cybercriminaliteit.

1. Zorg voor referentiehygiëne. Meer nog dan malware, hebben aanvallers referenties nodig om hun activiteiten te doen slagen. De succesvolle door mensen uitgevoerde ransomware-infectie van een hele organisatie is afhankelijk van toegang tot een account met uitgebreide machtigingen, zoals een domeinbeheerder, of mogelijkheden om een groepsbeleid te bewerken.
2. Controleer blootstelling van referenties.
3. Geef prioriteit aan de implementatie van Active Directory-updates.
4. Geef prioriteit aan cloudversterking.
5. Verklein het aanvalsoppervlak.
6. Versterk internetgerichte middelen en begrijp je grenzen.
7. Verminder de vermoeidheid van SOC-waarschuwingen door je netwerk te versterken om het volume te beperken en bandbreedte te bewaren voor incidenten met hoge prioriteit.

Links naar verdere informatie

- RaaS: inzicht in de gig-economie van cybercriminaliteit en hoe je jezelf kunt beschermen | Microsoft Security Blog
- Door mensen uitgevoerde ransomwareaanvallen: een vermijdbare ramp | Microsoft Security Blog

Ransomware-inzichten van eerstelijns hulpdiensten

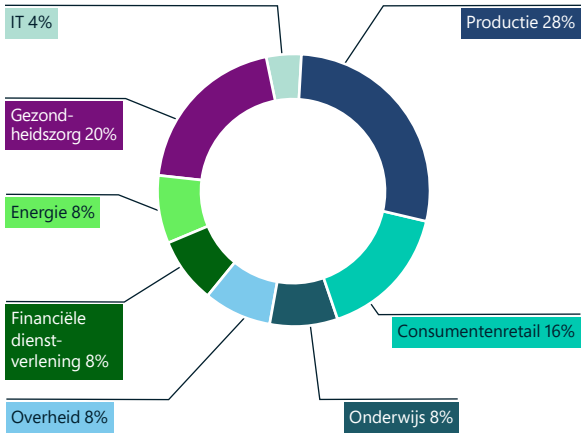
Organisaties wereldwijd zagen vanaf 2019 een gestage groei in door mensen uitgevoerde ransomwareaanvallen. Wetshandhavingsoperaties en geopolitieke gebeurtenissen in het afgelopen jaar hadden echter een aanzienlijke impact op organisaties van cybercriminelen.

De Security Service Line van Microsoft ondersteunt klanten bij een volledige cyberaanval, van onderzoek tot succesvolle beheersing en herstel. De respons- en herstelservices worden aangeboden via twee sterk geïntegreerde teams, waarvan het ene zich richt op het onderzoek en de basis voor herstel en het tweede op beheersing en herstel. In dit gedeelte wordt een samenvatting gegeven van de bevindingen op basis van ransomwareacties in het afgelopen jaar.

93%

van de Microsoft-onderzoeken tijdens herstelbewerkingen met ransomware heeft onvoldoende toegangsrechten en controles op zijdelingse verplaatsing aan het licht gebracht.

Ransomeware-incidenten en herstel van ransomware-incidenten per bedrijfstak

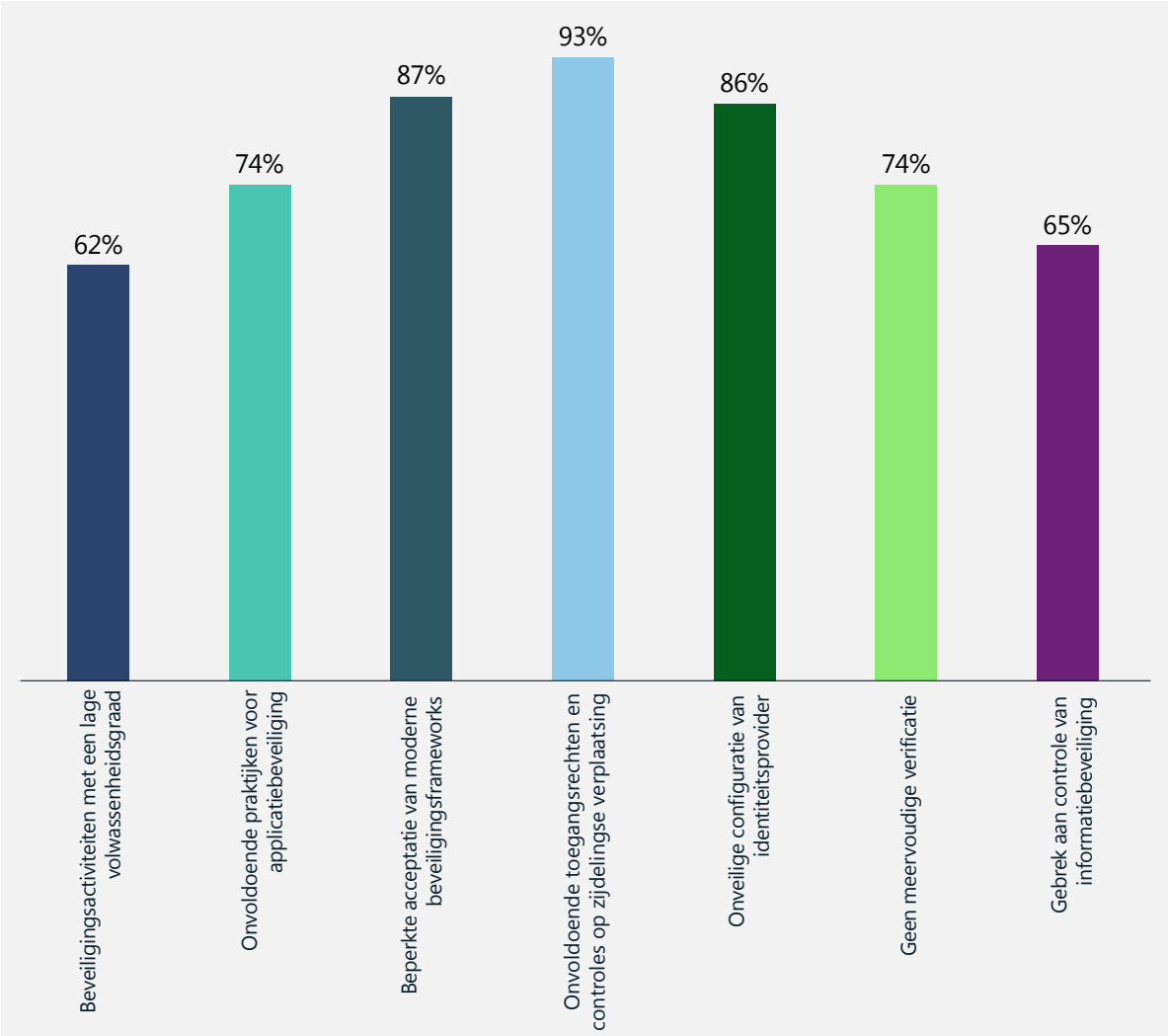


Naarmate er nieuwe kleine groepen en bedreigingen opduiken, moeten verdedigende teams zich bewust zijn van evoluerende ransomware-bedreigingen en tegelijkertijd bescherming bieden tegen voorheen onbekende malwarefamilies van ransomware.
De snelle ontwikkeling van criminele groepen leidde tot de ontwikkeling van intelligente ransomware, verpakt in gebruiksvriendelijke kits. Dit maakt grotere flexibiliteit mogelijk bij de lancering van grootschalige aanvallen op een groter aantal doelen.

Op de volgende pagina's wordt dieper ingegaan op de meest waargenomen factoren die bijdragen aan zwakke bescherming tegen ransomware, gegroepeerd in drie categorieën bevindingen:

1. Zwakke identiteitscontroles
2. Ineffectieve beveiligingsactiviteiten
3. Beperkte databescherming

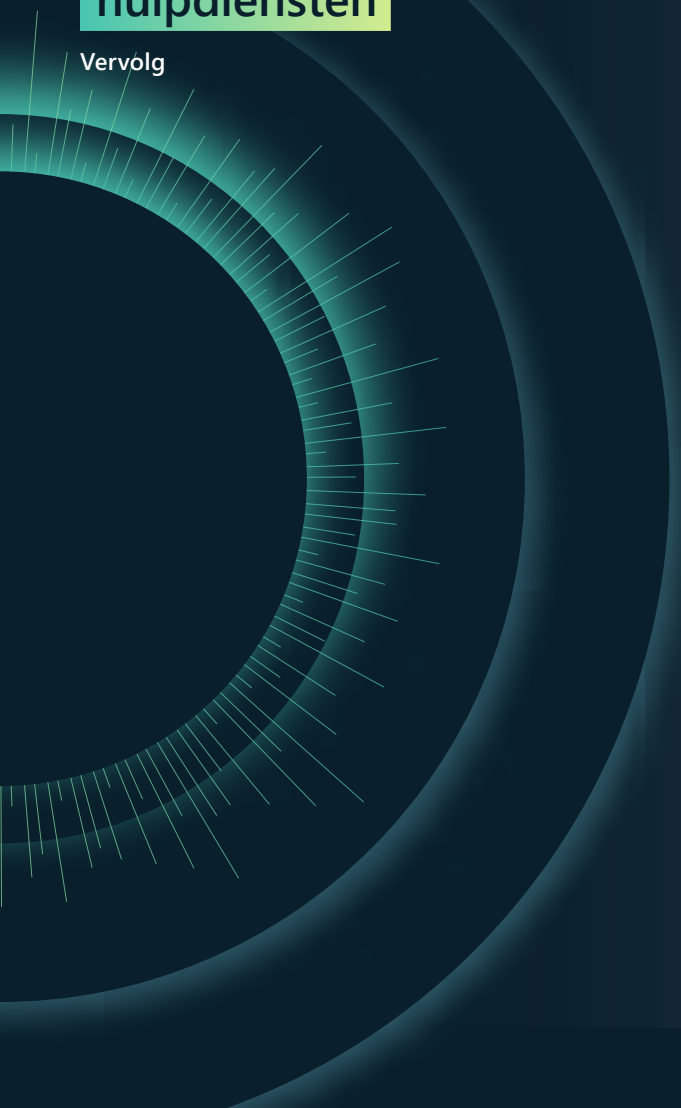
Samenvatting van de meest voorkomende bevindingen bij ransomware-responsen



De meest voorkomende bevinding bij ransomware-incidentrespons was onvoldoende toegang tot bevoegdheden en controles op zijdelingse verplaatsing.

Ransomware-inzichten van eerstelijns hulpdiensten

Vervolg



De drie belangrijkste factoren die bijdragen aan onze respons op locatie:

① Zwakke identiteitscontroles: Diefstal van referenties blijft een van de belangrijkste factoren

② Ineffectieve beveiligingsactiviteiten bieden niet alleen kansen voor aanvallers, maar hebben ook een aanzienlijke invloed op de hersteltijd

③ Uiteindelijk komt het neer op data: organisaties worstelen met het implementeren van een effectieve databeschermingsstrategie die is afgestemd op hun zakelijke behoeften

① Zwakke identiteitscontroles

Door mensen uitgevoerde ransomware blijft zich ontwikkelen en gebruikt diefstal van aanmeldingsreferenties en methoden voor zijdelingse verplaatsing die traditioneel in verband worden gebracht met gerichte aanvallen. Succesvolle aanvallen zijn vaak het resultaat van langlopende campagnes waarbij identiteitssystemen zijn aangetast, zoals Active Directory (AD), waarmee menselijke operators aanmeldingsreferenties kunnen stelen, toegang kunnen krijgen tot systemen en permanent aanwezig kunnen blijven in het netwerk.

Active Directory (AD) en Azure AD-beveiliging

88%

van de getroffen klanten maakte geen gebruik van best practices op het gebied van AD en Azure AD-beveiliging. Dit is een veelvoorkomende aanvalsvector geworden, omdat aanvallers misbruik maken van onjuiste configuraties en zwakkere beveiliging in essentiële identiteitssystemen om bredere toegang tot bedrijven te verkrijgen en hun impact te versterken.

Toegang tot en gebruik van Privileged Access Workstations (PAW) op basis van minimale bevoegdheden

Geen van de betrokken organisaties implementeerde de juiste principes voor scheiding van beheerdersreferenties en toegang op basis van minimale bevoegdheden via toegewezen werkstations tijdens het beheer van hun essentiële identiteit en waardevolle bedrijfsmiddelen, zoals bedrijfseigen systemen en bedrijfskritische applicaties.

Beveiliging van accounts met bevoegdheden

88%

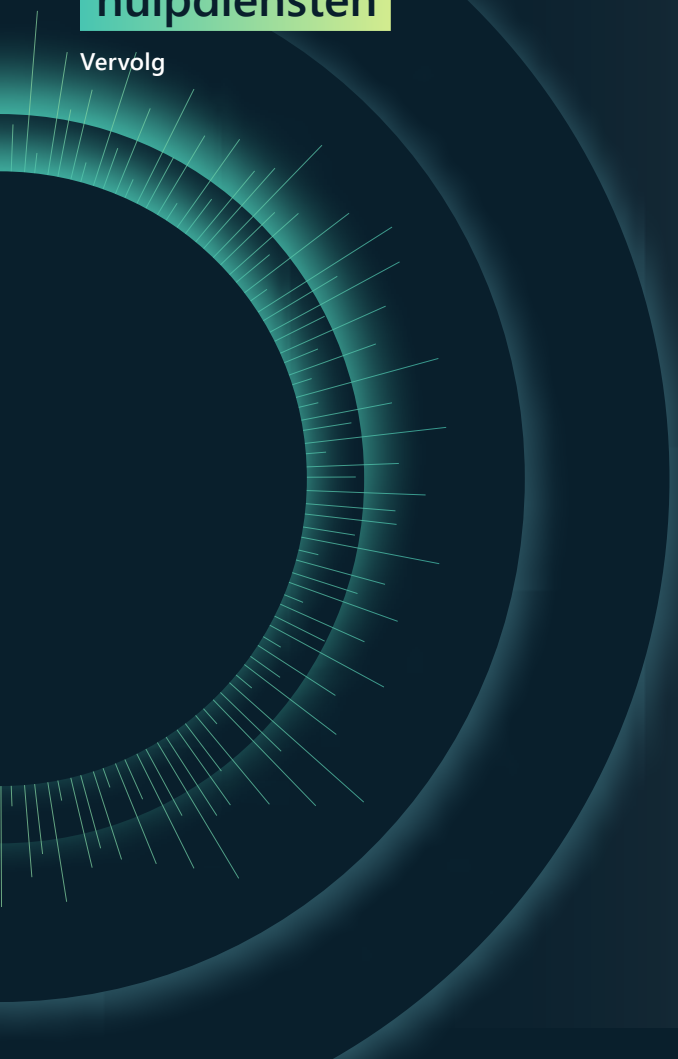
van de contacten implementeerde geen MFA voor gevoelige accounts met hoge bevoegdheden, waardoor aanvallers een beveiligingskloof konden achterlaten om referenties in gevaar te brengen en verdere aanvallen uit te voeren met behulp van legitieme referenties.

84%

Beheerders in 84 procent van de organisaties maakten geen gebruik van identiteitscontroles voor bevoegdheden zoals just-in-time-toegang om verder schadelijk gebruik van gecompromitteerde referenties met machtigingen te voorkomen.

Ransomware-inzichten van eerstelijns hulpdiensten

Vervolg



② Ineffectieve beveiligingsactiviteiten

Onze data laten zien dat organisaties die te maken hebben gehad met ransomwareaanvallen aanzienlijke lacunes hebben in hun beveiligingsactiviteiten, tools en het beheer van de levenscyclus voor IT-bedrijfsmiddelen. Op basis van de beschikbare data werden de volgende hiaten het meest waargenomen:

Patching:

68%

van de getroffen organisaties beschikte niet over een effectief kwetsbaarheids- en patchbeheerproces en een grote afhankelijkheid van handmatige processen versus geautomatiseerde patching leidde tot kritieke openingen. Productie en essentiële infrastructuur blijven worstelen met onderhoud en patching van verouderde OT-systemen (operationele technologie).

Gebrek aan tools voor beveiligingsactiviteiten:

De meeste organisaties meldden een gebrek aan end-to-end zichtbaarheid van de beveiliging als gevolg van een gebrek aan of onjuiste configuratie van beveiligingstools, wat leidde tot een afname van de effectiviteit van detectie en respons.

60%

van de organisaties meldde geen gebruik van een EDR[6]-tool, een fundamentele technologie voor detectie en respons.

60%

heeft niet geïnvesteerd in SIEM-technologie (Security Information and Event Management), wat heeft geleid tot bewakingssilo's, beperkte mogelijkheden om end-to-end-bedreigingen te detecteren en inefficiënte beveiligingsactiviteiten. Automatisering blijft een belangrijke kloof in SOC-tools en -processen, waardoor SOC-personeel gedwongen wordt om talloze uren te besteden aan het verkrijgen van inzicht in beveiligingstelemetrie.

84%

van de getroffen organisaties heeft niet de integratie van hun multicloudomgevingen in hun beveiligingstools mogelijk gemaakt.

Respons- en herstelprocessen:

76%

Het ontbreken van een effectief responsplan was een kritiek gebied dat werd waargenomen bij 76 procent van de getroffen organisaties, waardoor de juiste crisisbestendigheid van de organisatie werd voorkomen en de tijd om te reageren en te herstellen negatief werd beïnvloed.

③ Beperkte databescherming

Veel gehackte organisaties beschikten niet over de juiste databeschermingsprocessen die een grote impact hadden op hersteltijden en de mogelijkheid om terug te keren naar bedrijfsactiviteiten. De meest voorkomende hiaten zijn:

Onveranderlijke back-ups:

44%

van de organisaties beschikten niet over onveranderlijke back-ups voor de getroffen systemen. Uit data blijkt ook dat beheerders geen back-ups en herstelplannen hadden voor essentiële bedrijfsmiddelen zoals AD.

Preventie van dataverlies:

Aanvallers vinden meestal hun weg om systemen te compromitteren door gebruik te maken van kwetsbaarheden in de organisatie, essentiële data te exfiltreren voor afpersing, diefstal van intellectueel eigendom of het genereren van inkomsten.

92%

van de getroffen organisaties heeft geen effectieve preventie van dataverlies geïmplementeerd om deze risico's te beperken, wat leidt tot kritiek dataverlies.

Ransomware nam in sommige regio's af en in andere toe

Dit jaar zagen we een daling van het totale aantal gevallen van ransomware dat aan onze responsteams in Noord-Amerika en Europa werd gemeld ten opzichte van het voorgaande jaar. Tegelijkertijd nam het aantal gemelde gevallen in Latijns-Amerika toe.

Een van de interpretaties van deze observatie is dat cybercriminelen zich afzijdig houden van gebieden die een hoger risico lopen op wetshandhaving en kiezen voor minder lastige doelen. Aangezien Microsoft geen waarneembare verbetering in de wereldwijde netwerkbeveiliging zag om de daling van het aantal ransomware-gerelateerde supportgesprekken te verklaren, is de meest waarschijnlijke oorzaak een combinatie van wetshandhavingsactiviteiten in 2021 en 2022 die de kosten van criminele activiteiten verhoogden en enkele geopolitieke gebeurtenissen in 2022.

Een van de meest actieve RaaS-operaties vormt onderdeel van een Russischtalige criminele groep die bekendstaat als REvil (ook bekend als Sodinokibi) en sinds 2019 actief is. In oktober 2021 werden de servers van REvil offline gehaald als onderdeel van de internationale wetshandhavingsactie Operation GoldDust.[7] In januari 2022 arresteerde Rusland 14 vermeende leden van REvil en werden er op 25 locaties invallen gedaan in verband hiermee.[8] Dit was de eerste keer dat Rusland actie ondernam tegen ransomwareoperators op eigen bodem.

Hoewel wetshandhavingsactiviteiten waarschijnlijk het aantal aanvallen in 2022 hebben vertraagd, is het heel goed mogelijk dat dreigingsactoren nieuwe strategieën ontwikkelen om te voorkomen dat ze in de toekomst worden betrapt. Bovendien lijkt de spanning tussen Rusland en de Verenigde Staten over de invasie van Rusland in Oekraïne een einde te hebben gemaakt aan de opkomende samenwerking van Rusland in de wereldwijde strijd tegen ransomware. Na een korte periode van onzekerheid na de arrestaties van REvil, stopten de Verenigde Staten en Rusland met de samenwerking bij het vervolgen van ransomwareactoren, wat betekent dat cybercriminelen Rusland opnieuw als een veilige haven zouden kunnen beschouwen.

Voor de toekomst voorspellen we dat het tempo van ransomwareactiviteiten zal afhangen van de uitkomst van enkele belangrijke vragen:

1. Zullen overheden actie ondernemen om te voorkomen dat ransomware-criminelen binnen hun grenzen opereren of zullen ze proberen actoren te verstoren die vanuit het buitenland opereren?
2. Zullen ransomware-groepen van tactiek veranderen om de noodzaak van ransomware weg te nemen en hun toevlucht te nemen tot aanvallen in afpersingsstijl?
3. Zullen organisaties in staat zijn hun IT-activiteiten sneller te moderniseren en transformeren dan criminelen kwetsbaarheden kunnen misbruiken?
4. Zullen ontwikkelingen in het volgen en traceren van losgeldbetalingen ertoe leiden dat ontvangers van losgeld gedwongen worden om van tactieken en onderhandelingspraktijken te veranderen?

Hoewel wetshandhavings-activiteiten waarschijnlijk het aantal aanvallen in 2022 hebben vertraagd, is het heel goed mogelijk dat dreigingsactoren nieuwe strategieën ontwikkelen om te voorkomen dat ze in de toekomst worden betrapt.

2X

Ransomwareaanvallen namen in sommige regio's af, maar de losgeldeisen lieten meer dan een verdubbeling zien.

Direct bruikbare inzichten

1. Focus op holistische beveiligingsstrategieën, aangezien alle ransomware-families profiteren van dezelfde zwakke punten in de beveiliging om een netwerk te beïnvloeden.
2. Update en onderhoud de basisbeginselen van beveiliging om het basisniveau van beveiliging te verhogen en de beveiligingsactiviteiten te moderniseren. Door over te stappen naar de cloud kun je bedreigingen sneller detecteren en sneller reageren.

Links naar verdere informatie

- Je organisatie beschermen tegen ransomware | Microsoft Security
- Zeven manieren om je omgeving beter te beschermen tegen schendingen | Microsoft Security Blog
- Verbetering van de op AI gebaseerde bescherming om door mensen uitgevoerde ransomware te verstoren | Microsoft 365 Defender Research Team
- Security Insider: ontdek de nieuwste inzichten en updates op het gebied van cyberbeveiliging | Microsoft Security

Cybercrime as a Service

Cybercrime als een service (CaaS) vormt een groeiende en zich ontwikkelende bedreiging voor klanten wereldwijd. De Microsoft Digital Crimes Unit (DCU) constateerde een voortdurende groei van het CaaS-ecosysteem met een toenemend aantal online services dat verschillende cybercriminelen faciliteert, waaronder BEC en door mensen uitgevoerde ransomware. Phishing blijft een geprefereerde aanvalsmethode, omdat cybercriminelen aanzienlijke waarde kunnen behalen uit het stelen en verkopen van toegang tot gestolen accounts.

Als reactie op de groeiende CaaS-markt heeft DCU zijn luistersystemen verbeterd om CaaS-producten te detecteren en te identificeren in het hele ecosysteem van internet, deep web, doorgelichte forums,[9] gespecialiseerde websites, online discussieforums en berichtenplatforms.

Cybercriminelen werken nu samen in verschillende tijdzones en talen om specifieke resultaten te leveren. Eén CaaS-website die in Azië wordt beheerd door een persoon, onderhoudt bijvoorbeeld activiteiten in Europa en maakt schadelijke accounts aan in Afrika. Het feit dat deze activiteiten plaatsvinden in meerdere rechtsgebieden zorgt voor complexe uitdagingen op het gebied van recht en rechtshandhaving. In reactie hierop richt DCU haar inspanningen op het uitschakelen van schadelijke criminele infrastructuur die wordt gebruikt om CaaS-aanvallen te faciliteren en het samenwerken met wetshandhavingsinstanties over de hele wereld om criminelen verantwoordelijk te houden.

Cybercriminelen gebruiken steeds meer analytics om hun bereik, reikwijdte en winst te maximaliseren. Net als legitieme bedrijven moeten CaaS-websites de geldigheid van producten en services waarborgen om een solide reputatie te behouden. CaaS-websites automatiseren bijvoorbeeld routinematig de toegang tot gehackte accounts om de geldigheid van gehackte referenties te waarborgen. Cybercriminelen stoppen met de verkoop van specifieke accounts wanneer wachtwoorden opnieuw worden ingesteld of kwetsbaarheden worden gepatcht. In toenemende mate hebben we CaaS-websites geïdentificeerd die kopers van on-demand verificatie voorzien als kwaliteitscontroleproces. Als gevolg hiervan kunnen kopers er zeker van zijn dat de CaaS-website actieve accounts en wachtwoorden verkoopt, terwijl de potentiële kosten voor de CaaS-handelaar worden verminderd als de gestolen referenties worden hersteld voordat ze worden verkocht.

DCU heeft ook geconstateerd dat CaaS-websites kopers de mogelijkheid bieden om gehackte accounts te kopen die afkomstig zijn van specifieke geografische locaties, aangewezen online serviceproviders en specifieke individuen, beroepen en sectoren. Vaak bestelde accounts zijn gericht op professionals of afdelingen die facturen verwerken, zoals CFO's of medewerkers van de debiteurenafdeling. Ook sectoren die deelnemen aan openbare aanbestedingen zijn vaak het doelwit vanwege de hoeveelheid informatie die beschikbaar wordt gesteld via het openbare biedingsproces.

DCU-onderzoek naar CaaS bracht een aantal belangrijke trends aan het licht:

Het aantal en de verfijning van services neemt toe.

Een voorbeeld is de evolutie van webshells die meestal bestaan uit gehackte webservers die worden gebruikt om phishing-aanvallen te automatiseren. DCU heeft waargenomen dat CaaS-resellers het uploaden van phishingkits of malware via gespecialiseerde webdashboards hebben vereenvoudigd. CaaS-verkopers proberen vervolgens vaak extra services aan de bedreigingsactor te verkopen via het dashboard, zoals services voor spamberichten en gespecialiseerde lijsten met geadresseerden van spam op basis van gedefinieerde kenmerken, waaronder geografische locatie of beroep. In sommige gevallen zagen we dat één webshell werd gebruikt in meerdere aanvalscampagnes, wat suggereert dat bedreigingsactoren permanente toegang tot de gehackte server kunnen hebben. We zagen bovendien een toename van de anonimiseringsservices die beschikbaar zijn als onderdeel van het CaaS-ecosysteem, evenals aanbiedingen voor VPN-accounts (Virtual Private Networks) en VPS-accounts (Virtual Private Server). In de meeste gevallen werden de aangeboden VPN/VPS-accounts in eerste instantie verkregen via gestolen creditcards. CaaS-websites boden ook een groter aantal Remote Desktop Protocol (RDP), Secure Shell (SSH) en cPanels voor gebruik als platform voor het uitvoeren van cybercriminaliteitsaanvallen. CaaS-verkopers configureren de RDP, SSH en cPanels met de juiste tools en scripts om verschillende typen cyberaanvallen mogelijk te maken.

Services voor het maken van homogliefdomeinen vereisen in toenemende mate betaling in cryptovaluta's.

Homogliefdomeinen imiteren legitieme domeinnamen door tekens te gebruiken die identiek of bijna identiek zijn aan een ander teken. Het doel is om de kijker zodanig te misleiden dat deze denkt dat het homogliefdomein het echte domein is. Deze domeinen vormen een alomtegenwoordige bedreiging en zijn een gateway voor een aanzienlijke hoeveelheid cybercriminaliteit. CaaS-sites verkopen nu aangepaste homogliefdomeinnamen, waardoor kopers specifieke bedrijfs- en domeinnamen kunnen aanvragen voor imitatiedoeleinden. Nadat de betaling is ontvangen, gebruiken de CaaS-verkopers een tool voor het genereren van homogliefen om de domeinnaam te selecteren en vervolgens de schadelijke homoglief te registreren. De betaling voor deze service gebeurt bijna uitsluitend in cryptovaluta.

2.750.000

siteregistraties zijn dit jaar met succes geblokkeerd door de DCU om criminele actoren voor te zijn die van plan waren ze te gebruiken voor wereldwijde cybercriminaliteit.

Cybercrime as a Service

Vervolg

CaaS-verkopers bieden in toenemende mate gehackte referenties te koop aan.

Gehackte referenties maken ongeautoriseerde toegang tot gebruikersaccounts mogelijk, waaronder de service voor e-mailberichten, resources voor het delen van bedrijfsbestanden en OneDrive voor Bedrijven. Als beheerdersreferenties worden gehackt, kunnen onbevoegde gebruikers toegang krijgen tot vertrouwelijke bestanden, Azure-resources en gebruikersaccounts van het bedrijf. In veel gevallen werd bij DCU-onderzoek vastgesteld dat ongeautoriseerd gebruik van dezelfde referenties op meerdere servers was bedoeld om de verificatie van referenties te automatiseren. Dit patroon suggereert dat de gehackte gebruiker mogelijk het slachtoffer is van meerdere phishing-aanvallen of apparaat-malware heeft waardoor botnet-keyloggers referenties kunnen verzamelen.

CaaS-services en -producten met verbeterde functies zijn in opkomst om detectie te voorkomen.

Eén CaaS-verkoper biedt phishingkits met verhoogde complexiteits- en anonimiseringsfuncties die zijn ontworpen om detectie- en preventiesystemen te omzeilen voor slechts $ 6 per dag. De service biedt een reeks omleidingen die controles uitvoeren voordat verkeer naar de volgende laag of site wordt toegestaan. Bij een van deze runs worden meer dan 90 controles uitgevoerd op het apparaat, zoals of het om een virtuele machine gaat, waarbij details over de browser en de gebruikte hardware en meer worden verzameld. Als alle controles zijn geslaagd, wordt het verkeer doorgestuurd naar een landingspagina die wordt gebruikt voor phishing.

End-to-end cybercriminaliteitsservices verkopen abonnementen op beheerde services.

Doorgaans kan elke stap in het plegen van een online misdaad bedreigingsactoren blootleggen als de operationele beveiliging slecht is. Het risico van blootstelling en identificatie neemt toe als services worden gekocht van meerdere CaaS-sites. DCU zag een zorgwekkende trend op het dark web waarbij er een toename is in het aanbod van services om softwarecode te anonimiseren en websitetekst te genereren om de blootstelling te verminderen. End-to-end providers van abonnementsservices voor cybercriminaliteit beheren alle services en garanderen resultaten die de blootstellingsrisico's voor het abonnerende OCN verder verminderen. Het verminderde risico heeft tot een toename van de populariteit van deze end-to-end services geleid.

Phishing as a service (PhaaS) is één voorbeeld van een end-to-end cybercriminaliteitsservice. PhaaS is een evolutie van eerdere services die bekendstaan als FUD (Full Undetectable Services - volledig ondetecteerbare services) en wordt aangeboden op basis van een abonnement. Typische PhaaS-voorwaarden omvatten bijvoorbeeld het een maand lang actief houden van phishing-websites.

DCU heeft ook een CaaS-leverancier geïdentificeerd die DDoS (Distributed Denial of Service) biedt op basis van een abonnementsmodel. Bij dit model wordt het maken en onderhouden van het botnet dat nodig is voor het uitvoeren van aanvallen uitbesteed aan de CaaS-leverancier. Elke klant van een DDoS-abonnement ontvangt een versleutelde service om de operationele veiligheid te verbeteren en 24/7-support gedurende één jaar. De DDoS-abonnementsservice biedt verschillende architecturen en aanvalsmethoden, dus selecteert een koper simpelweg een resource om aan te vallen en biedt de verkoper toegang tot een scala aan gehackte apparaten op hun botnet om de aanval uit te voeren. De kosten voor het DDoS-abonnement bedragen slechts $ 500.

Het werk dat DCU besteedt aan het ontwikkelen van tools en technieken om CaaS-cybercriminelen te identificeren en te verstoren is in volle gang. De evolutie van CaaS-services biedt aanzienlijke uitdagingen, met name bij het verstoren van betalingen in cryptovaluta's.

PhaaS, cybercriminelen bieden meerdere services binnen een enkel abonnement. In het algemeen hoeft een koper slechts drie acties uit te voeren:

Zodra deze stappen zijn voltooid, maakt de PhaaS-leverancier services met drie of vier lagen omleidings- en hostingresources om specifieke gebruikers aan te vallen. De campagne wordt vervolgens gestart en de referenties van slachtoffers worden verzameld, geverifieerd en naar het e-mailadres verzonden dat door de koper is opgegeven. Als extraatje bieden veel PhaaS-verkopers aan phishing-sites op de openbare blockchain te hosten, zodat ze door elke browser kunnen worden benaderd en omleidingen gebruikers naar een resource in het gedistribueerde grootboek kunnen verwijzen.

Crimineel gebruik van cryptovaluta's

Naarmate de invoering van cryptovaluta's gangbaar wordt, gebruiken criminelen het in toenemende mate om wetshandhaving en anti-witwaspraktijken (AML) te omzeilen. Dit vergroot de uitdaging voor wetshandhavers om betalingen in cryptovaluta's aan cybercriminelen te volgen en te traceren.

De wereldwijde uitgaven aan blockchain-oplossingen zijn de afgelopen vier jaar met ongeveer 340 procent gegroeid, terwijl nieuwe cryptovalutaportemonnees met ongeveer 270 procent groeiden. Er zijn wereldwijd meer dan 83 miljoen unieke portemonnees en de totale marktkapitalisatie van alle cryptovaluta's bedroeg op 28 juli 2022 ongeveer $ 1,1 biljoen.[10]

Bron: Twitter.com—@PeckShieldAlert (PeckShield is een in China gevestigd blockchain-beveiligingsbedrijf).

Ransomware-betalingen bijhouden

Ransomware is een van de grootste bronnen van illegaal verworven cryptovaluta's. In een poging om schadelijke technische infrastructuur die wordt gebruikt bij ransomwareaanvallen te verstoren, bijvoorbeeld de verstoring van Zloader in april 2022[11] - De DCU van Microsoft houdt criminele portemonnees bij om tracerings- en herstelfuncties voor cryptovaluta's mogelijk te maken.

DCU-onderzoekers hebben gezien dat ransomwareactoren hun communicatietactieken met slachtoffers ontwikkelen om het geldspoor te verbergen. Oorspronkelijk namen cybercriminelen Bitcoin-adressen op in hun losgeldbriefjes. Dit maakte het echter gemakkelijk om betalingstransacties op de blockchain te volgen, dus namen ransomwareactoren geen portemonneeadressen meer op en voegden in plaats daarvan e-mailadressen of links naar chatwebsites toe om adressen voor de betaling van losgeld aan slachtoffers te communiceren. Sommige actoren hebben zelfs unieke webpagina's en aanmeldingen voor elk slachtoffer gemaakt om te voorkomen dat veiligheidsonderzoekers en wetshandhavers de portemonneeadressen van de criminelen in handen krijgen door zich voor te doen als slachtoffers. Ondanks de inspanningen van criminelen om hun sporen te verbergen, kunnen sommige losgeldbetalingen toch worden teruggevorderd door samen te werken met wetshandhavings- en crypto-analysebedrijven die bewegingen op de blockchain kunnen volgen.

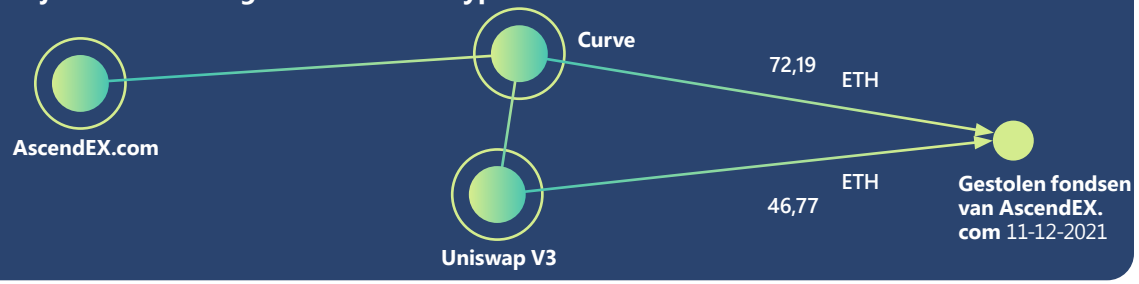
Trending: DEX-witwaspraktijken voor illegale opbrengsten

Een belangrijk probleem voor cybercriminelen is de conversie van cryptovaluta naar fiatvaluta. Cybercriminelen hebben verschillende mogelijke conversiepunten, die elk een verschillende mate van risico met zich meebrengen. Eén methode die wordt gebruikt om het risico te verminderen, is het witwassen van de opbrengsten via een gedecentraliseerde centrale (DEX) voordat deze worden uitbetaald via beschikbare uitbetalingsopties, zoals CEX- (gecentraliseerde), P2P- (peer-to-peer) en OTC-uitwisselingen (over-the-counter). DEX's zijn een aantrekkelijke witwaslocatie omdat ze vaak geen AML-maatregelen hanteren.

In december 2021 vielen hackers het wereldwijde handelsplatform voor cryptovaluta's AscendEx aan en stalen ongeveer $ 77,7 miljoen aan cryptovaluta van zijn klanten.[12] AscendEx huurde bedrijven voor blockchain-analytics in en nam contact op met andere CEX's, zodat de portemonnees die gestolen geld ontvingen op de zwarte lijst konden worden geplaatst. Daarnaast werden adressen waar de munten naartoe werden gestuurd als zodanig gelabeld op de Ethereum blockchain-verkenner Etherscan.[13] Om de waarschuwingen en zwarte lijsten te omzeilen, stuurden de hackers op 18 februari 2022 $ 1,5 miljoen in Ethereum naar Uniswap, een van's werelds grootste DEX's.[14]

De invoering van sterkere AML-maatregelen door DEX's kan het witwassen van activiteiten op hun platforms afzwakken en cybercriminelen dwingen om andere verdoezelingsmethoden te gebruiken, zoals coin tumbling of ongelicentieerde uitwisselingen. Als voorbeeld heeft Uniswap onlangs aangekondigd dat het gebruik gaat maken van zwarte lijsten om portemonnees waarvan bekend is dat ze betrokken zijn bij illegale activiteiten, te verhinderen transacties op de beurs uit te voeren.[15]

Het bijhouden van illegaal verworven cryptovaluta's



Met behulp van de cryptovaluta-onderzoekstool Chainalysis ontdekte de Digital Crimes Unit van Microsoft dat de AcendEX-hackers hun gestolen geld omwisselden op een kleinere DEX, genaamd Curve, naast Uniswap. Dit diagram illustreert de witwasroutes die het team heeft ontdekt. Elke cirkel vertegenwoordigt een cluster van portemonnees en de getallen op elke regel vertegenwoordigen de totale hoeveelheid Ethereum die wordt verzonden voor het witwassen van geld.

Direct bruikbare inzichten

1. Als je het slachtoffer bent van cybercriminaliteit die de crimineel heeft betaald met behulp van cryptovaluta, neem dan contact op met de lokale wetshandhavingsinstanties. Zij kunnen je mogelijk helpen bij het volgen en terughalen van verloren fondsen.
2. Raak vertrouwd met de aanwezige ALM-maatregelen bij het selecteren van een DEX.

Links naar verdere informatie

- Op hardware gebaseerde verdediging tegen bedreigingen tegen steeds complexere crypto-jackers | Microsoft 365 Defender Research Team

Het zich ontwikkelende landschap van phishing-bedreigingen

Phishing-programma's voor het ontfutselen van referenties worden steeds populairder en vormen een aanzienlijke bedreiging voor gebruikers overal, omdat ze zonder onderscheid tegen alle postvakken gericht zijn. Onder de bedreigingen die onze onderzoekers volgen en waartegen ze bescherming bieden, is het aantal phishing-aanvallen een orde van grootte hoger dan alle andere bedreigingen.

Met behulp van data van Defender for Office zien we schadelijke e-mail en activiteiten van gehackte identiteiten. Azure Active Directory Identity Protection biedt nog meer informatie via waarschuwingen voor gebeurtenissen met gehackte identiteiten. Met Defender for Cloud Apps zien we gebeurtenissen voor datatoegang door gehackte identiteiten en Microsoft 365 Defender (M365D) biedt correlatie tussen producten. De meetwaarde voor zijdelingse verplaatsing is afkomstig van Defender for Endpoint (waarschuwingen en gebeurtenissen bij aanvalsgedrag), Defender for Office (schadelijke e-mail) en opnieuw M365D voor correlatie tussen producten).

710 miljoen
phishing-e-mails per week geblokkeerd.

1 uur 12 m
De gemiddelde tijd die een aanvaller nodig heeft om toegang te krijgen tot je privédata als je het slachtoffer wordt van een phishing-e-mail.[16]

1 uur 42 m
De gemiddelde tijd die een aanvaller nodig heeft om zich zijdelings binnen je bedrijfsnetwerk te verplaatsen zodra een apparaat is gehackt.[17]

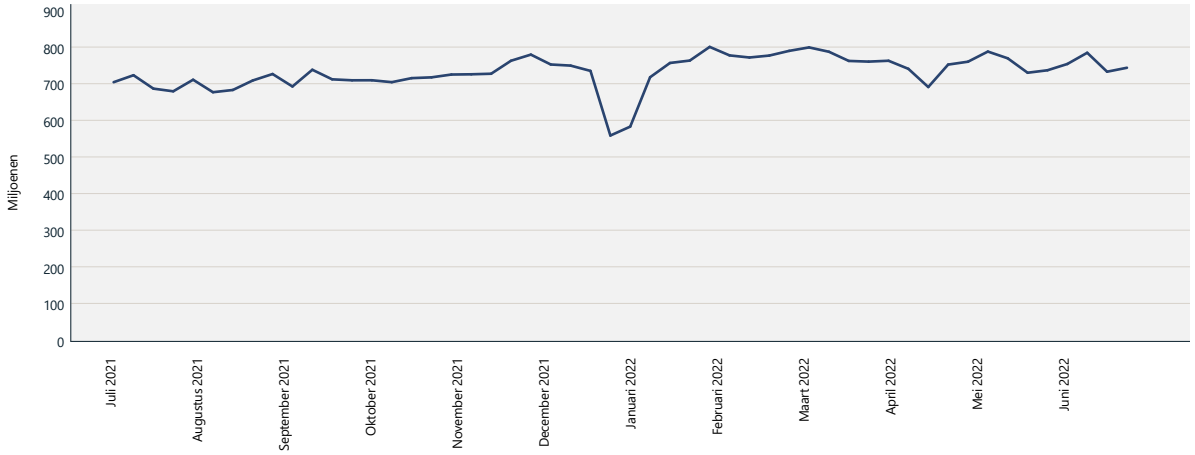
Microsoft 365-referenties blijven een van de meest gewilde accounttypen voor aanvallers. Zodra de aanmeldingsreferenties zijn gehackt, kunnen aanvallers zich aanmelden bij computersystemen die aan het bedrijf zijn gekoppeld om infectie met malware en ransomware te vergemakkelijken, vertrouwelijke bedrijfsdata en -informatie stelen door toegang te krijgen tot SharePoint-bestanden en phishing verspreiden door extra schadelijke e-mails te sturen via Outlook, om maar een aantal acties te noemen.

Naast campagnes met bredere doelen, phishing naar referenties, donaties en persoonlijke informatie, nemen aanvallers specifieke bedrijven op de korrel voor grotere uitbetalingen. Phishing-aanvallen per e-mail op bedrijven voor financieel gewin worden gezamenlijk BEC-aanvallen genoemd. Microsoft detecteert elke maand miljoenen BEC-e-mails, wat overeenkomt met 0,6 procent van alle waargenomen phishing-e-mails. Een rapport van IC3[18] dat in mei 2022 werd gepubliceerd duidt op een stijgende trend in geleden verliezen als gevolg van BEC-aanvallen.

De technieken die worden gebruikt bij phishing-aanvallen worden steeds complexer. Als reactie op tegenmaatregelen passen aanvallers zich aan en vinden nieuwe manieren om hun technieken te implementeren, waardoor de complexiteit van hoe en waar ze de infrastructuur voor campagneactiviteiten hosten toeneemt. Dit betekent dat organisaties hun strategie voor het implementeren van beveiligingsoplossingen om schadelijke e-mails te blokkeren en de toegangscontrole voor individuele gebruikersaccounts te versterken, regelmatig moeten herzien.

531.000
Naast de URL's die werden geblokkeerd door Defender for Office, regelde onze Digital Crimes Unit de verwijdering van 531.000 unieke phishing-URL's die buiten Microsoft werden gehost.

Gedetecteerde phishing-e-mails



Het aantal phishing-detecties per week blijft toenemen. De daling in december-januari is een verwachte seizoensgebonden daling, zoals ook gerapporteerd in het rapport van vorig jaar. Bron: Exchange Online Protection-signalen.

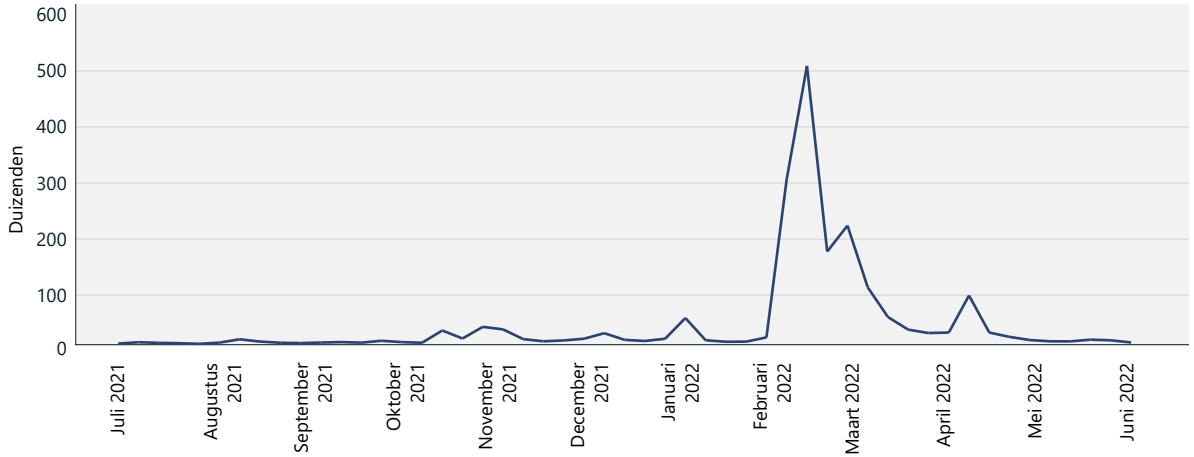
Het zich ontwikkelende landschap van phishing-bedreigingen

Vervolg

We blijven een gestage toename van phishing-e-mails zien op jaarbasis. De verschuiving naar extern werken in 2020 en 2021 zorgde voor een aanzienlijke toename van phishing-aanvallen om misbruik te maken van de veranderende werkomgeving. Phishing-operators zijn er snel bij om nieuwe e-mailsjablonen te gebruiken met lokmiddelen die zijn afgestemd op grote wereldgebeurtenissen zoals de COVID-19-pandemie en thema's die zijn gekoppeld aan samenwerking en productiviteitstools zoals Google Drive of OneDrive-bestandsdeling. Hoewel de COVID-19-thema's zijn afgenomen, werd de oorlog in Oekraïne begin maart 2022 een nieuw lokmiddel. Onze onderzoekers zagen een verbazingwekkende toename van e-mails waarin legitieme organisaties werden geïmiteerd die om cryptovalutadonaties vroegen in Bitcoin en Ethereum, onder het voorwendsel support te willen bieden aan de burgers van Oekraïne.

Slechts een paar dagen na het begin van de oorlog in Oekraïne, eind februari 2022, nam het aantal gedetecteerde phishing-e-mails met Ethereum-adressen voor zakelijke klanten drastisch toe. Het totaal aantal ontmoetingen piekte in de eerste week van maart, toen een half miljoen phishing-e-mails een Ethereum-portemonneeadres bevatten. Vóór het begin van de oorlog lag het aantal adressen van Ethereum-portemonnees in andere e-mails dat als phishing werd gedetecteerd, aanzienlijk lager, met gemiddeld een paar duizend e-mails per dag.

Phishing-e-mails met Ethereum-portemonneeadressen



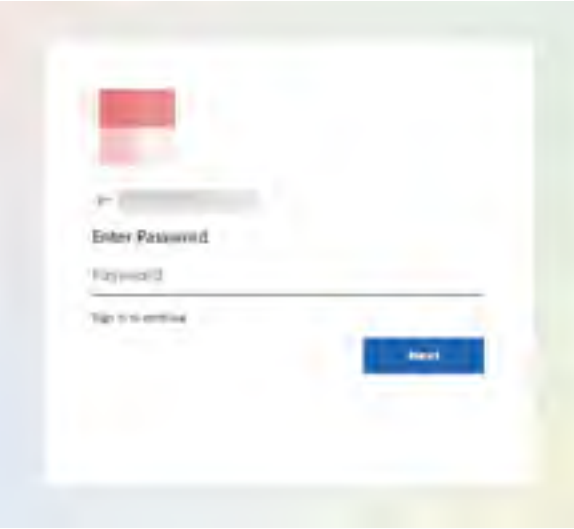
Het totale aantal e-mails dat werd gedetecteerd als phishing met Ethereum-portemonneeadressen nam toe aan het begin van het conflict tussen Oekraïne en Rusland en zwakte af na de eerste push.

Meer dan ooit vertrouwen phishers op een legitieme infrastructuur om te kunnen opereren, waardoor phishing-campagnes worden gestimuleerd die zijn gericht op het aantasten van verschillende aspecten van een operatie, zodat ze hun eigen activiteiten niet hoeven te kopen, hosten of exploiteren. Schadelijke e-mails kunnen bijvoorbeeld afkomstig zijn van gehackte afzenderaccounts. Aanvallers profiteren van het gebruik van deze e-mailadressen, die een hogere reputatiescore hebben en worden gezien als betrouwbaarder dan nieuw aangemaakte accounts en domeinen. In sommige meer geavanceerde phishing-campagnes hebben we gezien dat aanvallers liever verzenden en spoofen vanuit domeinen waar DMARC[19] op onjuiste wijze is ingesteld met een 'geen actie'-beleid, waardoor de deur opengaat voor spoofing van e-mails.

Grote phishing-operaties gebruiken meestal cloudservices en virtuele cloudmachines (VM's) om grootschalige aanvallen uit te voeren. Aanvallers kunnen het proces van het implementeren en bezorgen van e-mails vanaf VM's volledig automatiseren met behulp van SMTP-e-mailrelais of e-mailinfrastructuur in de cloud om te profiteren van de hoge bezorgingspercentages en de positieve reputatie van deze legitieme services. Als schadelijke e-mails kunnen worden verzonden via deze cloudservices, moeten verdedigers vertrouwen op krachtige e-mailfiltermogelijkheden om te voorkomen dat e-mails hun omgeving binnenkomen.

Microsoft-accounts blijven een belangrijk doelwit voor phishing-operators, zoals blijkt uit de talloze phishing-landingspagina's die de Microsoft 365-aanmeldingspagina nabootsen. Phishers proberen bijvoorbeeld de aanmeldingservaring van Microsoft te evenaren in hun phishingkits door een unieke URL te genereren die is aangepast aan de ontvanger. Deze URL verwijst naar een schadelijke webpagina die is ontwikkeld om referenties te verzamelen, maar een parameter in de URL bevat het e-mailadres van de specifieke ontvanger. Zodra het doel naar de pagina is genavigeerd, vult de phishingkit de aanmeldingsdata van gebruikers en een bedrijfslogo in dat is aangepast aan de e-mailontvanger. Dit weerspiegelt het uiterlijk van de aangepaste Microsoft 365-aanmeldingspagina van het bedrijf.

Phishing-pagina waarop een Microsoft-aanmelding met dynamische content wordt nagebootst

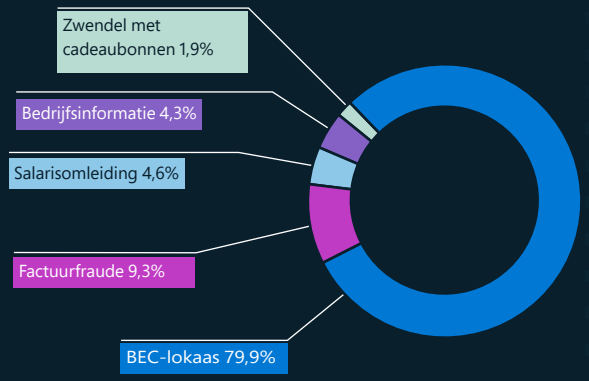


Spotlight op het infiltreren van zakelijke e-mail

Cybercriminelen ontwikkelen steeds complexere schema's en technieken om beveiligingsinstellingen te verslaan en zich te richten op individuen, bedrijven en organisaties. Als respons hierop investeren wij aanzienlijke middelen om ons handhavingsprogramma voor BEC verder te verbeteren.

BEC is de duurste vorm van financiële cybercriminaliteit, met een geschatte $ 2,4 miljard aan gecorrigeerde verliezen in 2021, wat neerkomt op meer dan 59 procent van de top vijf van internetcriminaliteit wereldwijd.[20] Om inzicht te krijgen in de omvang van het probleem en hoe je gebruikers het beste kunt beschermen tegen BEC, hebben beveiligingsonderzoekers van Microsoft de meest voorkomende thema's bij aanvallen gevolgd.

BEC-thema's (januari-juni 2022)



BEC-thema's per percentage van voorkomen

BEC-trends

Als uitgangspunt proberen BEC-aanvallers normaal gesproken een gesprek te beginnen met potentiële slachtoffers om een relatie op te bouwen. De aanvaller, die zich voordoet als collega of zakelijke kennis, leidt het gesprek geleidelijk in de richting van een financiële transactie. De introductie-e-mail, die we volgen als BEC-lokmiddel, vertegenwoordigt bijna 80 procent van de gedetecteerde BEC-e-mails. Andere trends die beveiligingsonderzoekers van Microsoft in het afgelopen jaar hebben geïdentificeerd, zijn onder andere:

- De meest gebruikte technieken bij BEC-aanvallen die in 2022 werden waargenomen, waren spoofing[21] en imitatie.[22]
- Het BEC-subtype dat de meeste financiële schade berokkende aan slachtoffers was factuurfraude (op basis van het volume en de gevraagde dollarbedragen die we hebben gezien in onze onderzoeken naar BEC-campagnes).
- Diefstal van bedrijfsinformatie zoals debiteurenrapporten en klantcontacten stelt aanvallers in staat om overtuigende factuurfraude te creëren.
- De meeste verzoeken om omleiding van salarisbetalingen werden verzonden via gratis e-mailservices en zelden via gehackte accounts. Het e-mailvolume van deze bronnen piekte rond de eerste en vijftiende van elke maand, de meest voorkomende betaaldatums.
- Hoewel het om bekende fraudepraktijken gaat, vormde zwendel met cadeaubonnen slechts 1,9 procent van de gedetecteerde BEC-aanvallen.

Direct bruikbare inzichten

Bescherming bieden tegen phishing

Om de blootstelling van je organisatie aan phishing te verminderen, worden IT-beheerders aangemoedigd om de volgende beleidsregels en functies te implementeren:

1. Vereis het gebruik van MFA voor alle accounts om ongeautoriseerde toegang te beperken.
2. Schakel functies voor voorwaardelijke toegang in voor accounts met hoge bevoegdheden om de toegang te blokkeren voor landen, regio's en IP-adressen die meestal geen verkeer binnen je organisatie genereren.
3. Overweeg het gebruik van fysieke beveiligingssleutels voor leidinggevenden, werknemers die betrokken zijn bij betalings- of aankoopactiviteiten en andere accounts met bevoegdheden.
4. Dwing het gebruik af van browsers die services ondersteunen zoals Microsoft SmartScreen om URL's te analyseren op verdacht gedrag en de toegang tot bekende schadelijke websites te blokkeren.[23]
5. Gebruik een op machine learning gebaseerde beveiligingsoplossing die phishing met een hoge waarschijnlijkheid in quarantaine plaatst en URL's en bijlagen in een sandbox laat ontploffen voordat e-mail het postvak bereikt, zoals Microsoft Defender for Office 365.[24]
6. Schakel functies voor beveiliging tegen imitatie en spoofing in binnen je organisatie.
7. Configureer actiebeleid voor DomainKeys Identified Mail (DKIM) en Domain-based Message Authentication Reporting & Conformance (DMARC) om bezorging te voorkomen van niet-geverifieerde e-mails die betrouwbare afzenders kunnen spoofen.
8. Met de audittenant en -gebruiker kunnen regels worden toegestaan en brede, op domein en IP-adressen gebaseerde uitzonderingen worden verwijderd. Deze regels hebben vaak voorrang en kunnen bekende schadelijke e-mails toestaan via e-mailfiltering.
9. Voer regelmatig phishing-simulators uit om het potentiële risico in je organisatie te meten en kwetsbare gebruikers te identificeren en te informeren.

Links naar verdere informatie

- Van cookiediefstal tot BEC: aanvallers gebruiken AiTM-phishing-sites als toegangspoort tot verdere financiële fraude | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Homogliefmisleiding

BEC en phishing zijn gangbare tactieken voor social engineering. Social engineering speelt een belangrijke rol bij criminaliteit en haalt een doelwit over om interacties met de crimineel aan te gaan door vertrouwen te winnen.

In de fysieke handel worden handelsmerken gebruikt om het vertrouwen in de oorsprong van een product of service te waarborgen, terwijl namaakproducten misbruik van het handelsmerk vormen. Op dezelfde manier doen cybercriminelen het voorkomen alsof zij een vertrouwde contactpersoon van het doelwit zijn tijdens een phishing-aanval, waarbij ze homogliefen gebruiken om potentiële slachtoffers te misleiden.

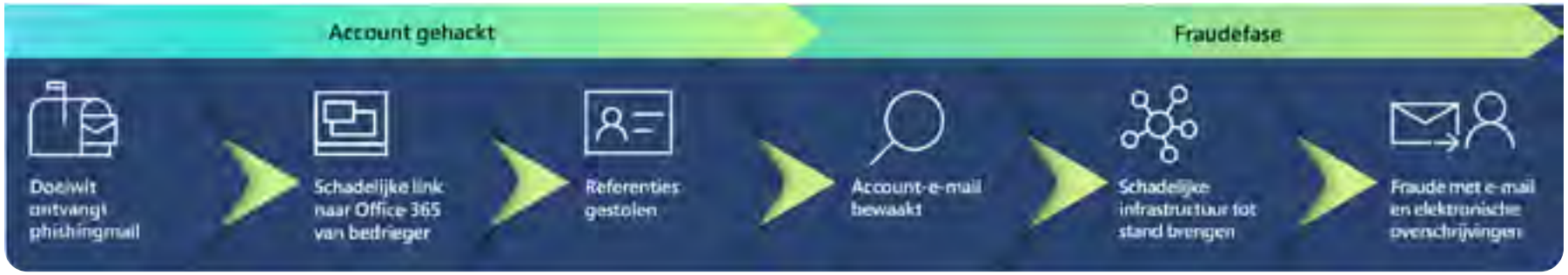
Een homoglief is een domeinnaam die wordt gebruikt voor e-mailcommunicatie in BEC, waarbij een teken wordt vervangen door een teken dat er identiek of bijna identiek uitziet, om het doelwit te misleiden.

Homoglieftechnieken die worden gebruikt bij BEC-pogingen

BEC kent in het algemeen twee fasen, waarvan de eerste betrekking heeft op het hacken van referenties. Deze typen lekken van referenties kunnen het gevolg zijn van phishing-aanvallen of grote datalekken. De referenties worden vervolgens verkocht of verhandeld op het dark web.

De tweede fase is de fraudefase, waarbij aanvallers gehackte referenties gebruiken om geavanceerde social engineering uit te voeren met behulp van homoglief-e-maildomeinen.

Progressie van een BEC-aanval



Techniek	% van domeinen met homoglieftechniek
vervang l door I	25%
vervang i door l	12%
vervang q door g	7%
vervang rn door m	6%
vervang .cam door .com	6%
vervang 0 door o	5%
vervang ll door l	3%
vervang ii door i	2%
vervang vv door w	2%
vervang l door ll	2%
vervang e door a	2%
vervang nn door m	1%
vervang ll door I, vervang l door i	1%
vervang o door u	1%

Analyse van meer dan 1700 homogliefdomeinen tussen januari en juli 2022. Hoewel 170 homoglieftechnieken werden toegepast, gebruikte 75% van de domeinen slechts 14 technieken.

Een homoglief in actie

Een homogliefdomein dat er identiek uitziet als een e-maildomein dat het slachtoffer herkent, wordt met een identieke gebruikersnaam geregistreerd bij een e-mailprovider. Vervolgens wordt een gehackte e-mail verzonden vanuit het gehackte domein met nieuwe betalingsinstructies.

Aan de hand van open-source-informatie en toegang tot e-mailthreads, identificeert de crimineel personen die verantwoordelijk zijn voor facturering en betalingen. Vervolgens maken ze een imitatie van een e-mailadres van de persoon die facturen verzendt. Deze imitatie bestaat uit een identieke gebruikersnaam en een e-maildomein dat een homoglief is van de echte afzender.

De aanvaller kopieert een e-mailketen met een legitieme factuur en wijzigt vervolgens de factuur zodat deze zijn eigen bankdata bevat. Deze nieuwe, gewijzigde factuur wordt vervolgens opnieuw verzonden vanuit de e-mail met de homogliefidentiteit naar het doel. Omdat de context logisch is en de e-mail er echt uitziet, volgt het doelwit vaak de frauduleuze instructies.

Direct bruikbare inzichten

1. Dwing het gebruik af van browsers die services ondersteunen om URL's te analyseren op verdacht gedrag en de toegang tot bekende schadelijke websites te blokkeren, zoals Safe Links en SmartScreen.[25]
2. Gebruik een op machine learning gebaseerde beveiligingsoplossing die phishing met een hoge waarschijnlijkheid in quarantaine plaatst en URL's en bijlagen in een sandbox activeert voordat e-mail het postvak bereikt.

Links naar verdere informatie

- Internet Crime Complaint Center (IC3) | Aanvallen op zakelijke e-mails: De oplichtingszaak van $ 43 miljard
- Informatie-inzichten spoofen - Office 365 | Microsoft Docs
- Inzicht in imitaties - Office 365 | Microsoft Docs

Een tijdlijn van botnet-verstoringen uit de begintijd van de samenwerking met Microsoft

Al meer dan tien jaar probeert DCU cybercriminaliteit proactief te stoppen, met 26 malware-verstoringen en verstoringen door vreemde mogendheden als resultaat. Naarmate het DCU-team geavanceerdere tactieken en tools gebruikt om deze illegale activiteiten te stoppen, zien we dat de cybercriminelen ook hun aanpak veranderen in een poging om een stap voor te blijven. Hier is een tijdlijn met een voorbeeld van de botnets die zijn verstoord door DCU en de strategieën die Microsoft heeft gebruikt om ze uit te schakelen.

2008

Conficker-botnet

Beschrijving: Een zich snel verspreidende worm die zich richtte op het Windows-besturingssysteem en die miljoenen computers en apparaten in een gemeenschappelijk netwerk infecteerde; zorgde voor netwerkstoringen wereldwijd.

Samenwerking: Oprichting van de Conficker-werkgroep, het eerste consortium in zijn soort. Microsoft werkte samen met 16 organisaties over de hele wereld om de bot te verslaan.

Microsoft-respons: De groep werkte samen in vele internationale rechtsgebieden en was succesvol bij het uitschakelen van Conficker.

2009

Waledac-botnet

Beschrijving: Een complex spambotnet met Amerikaanse domeinen dat e-mailadressen verzamelde en spam verspreidde en tot 90.000 computers over de hele wereld heeft besmet.[26]

Samenwerking: Oprichting van een ander consortium, het Microsoft Malware Protection Center (MMPC) met een focus op nauwe samenwerking met academici.[27]

Microsoft-respons: Microsoft gebruikte gelaagde verstoring van C2 en verraste kwaadwillenden door zonder kennisgeving domeinen in de VS over te nemen..[28] Het eigendom van bijna 280 domeinen die door de servers van Waledac worden gebruikt is tijdelijk toegekend aan Microsoft.

2011

Microsoft Digital Crimes Unit opgericht

Samenwerking: Ontworpen om cybercriminaliteit die het Microsoft-ecosysteem beïnvloedt te dwarsbomen door nauwe integratie tussen een team van onderzoekers, advocaten en technici.

Microsoft-aanpak: Het doel is.om de technische aspecten van uiteenlopende malware beter te begrijpen en deze inzichten te bieden aan het juridische team van Microsoft om een effectieve verstoringsstrategie te ontwikkelen.

2013

Rustock-botnet

Beschrijving: Een backdoor trojaanse e-mailbot voor spam die internetproviders als primaire C2 gebruikt; ontworpen voor de verkoop van farmaceutische producten.

Samenwerking: Microsoft is een samenwerking aangegaan met Pfizer Pharmaceuticals om inzicht te krijgen in de medicijnen die door Rustock worden verkocht en werkt nauw samen met Nederlandse wetshandhavers.[29]

Microsoft-respons: Microsoft werkte samen met de US Marshalls en rechtshandhaving in Nederland om de C2-servers in dat land uit te schakelen. Alle toekomstige domeingeneratoralgoritmen (DGA's) geregistreerd en geblokkeerd.

Sirefef/Zero Access-botnet

Beschrijving: Een advertentiebotnet dat is ontworpen om mensen naar gevaarlijke websites te leiden die malware zouden installeren of persoonlijke informatie zouden stelen; besmette meer dan twee miljoen computers en kostte adverteerders meer dan $ 2,7 miljoen per maand; voornamelijk in de VS en West-Europa.

Samenwerking: De peer-to-peer-infrastructuur werd buiten werking gesteld in nauwe samenwerking met de FBI en het Cybercrime Center van Europol.

Microsoft-respons: Heeft zich aangesloten bij het Zero Access-netwerk, heeft de criminele C2-servers vervangen en downloadserverdomeinen met succes in beslag genomen.

2019

Trickbot-botnet

Beschrijving: Een geavanceerd botnet met gefragmenteerde infrastructuur over de hele wereld dat gericht was op de financiële dienstensector; tastte IoT-apparaten aan.

Samenwerking: Microsoft ging samenwerken met het Financial Services Information Sharing and Analysis Center (FS-ISAC) om Trickbot uit te schakelen.[30]

Microsoft-respons: DCU bouwde een systeem voor het identificeren en volgen van de botinfrastructuur en genereerde meldingen voor actieve internetproviders, rekening houdend met specifieke wetten in verschillende landen.

Blijvende focus op verstoring

Beschrijving: Microsoft verstoorde de infrastructuur van zeven bedreigingsactoren in het afgelopen jaar, waardoor ze niet langer extra malware konden verspreiden, de computers van slachtoffers konden beheersen en extra slachtoffers konden belagen.

Samenwerking: In samenwerking met internetproviders, overheden, wetshandhavingsinstanties en de particuliere sector, heeft Microsoft informatie gedeeld om meer dan 17 miljoen slachtoffers van malware wereldwijd herstel te bieden.

2022

Vooruitblik

DCU blijft innoveren en wil zijn ervaring met botnetverstoringen gebruiken om gecoördineerde activiteiten uit te voeren die verder gaan dan malware. Ons voortdurende succes vereist creatieve engineering, het delen van informatie, innovatieve juridische theorieën en publieke en particuliere partnerschappen.

Misbruik van infrastructuur door cybercriminelen

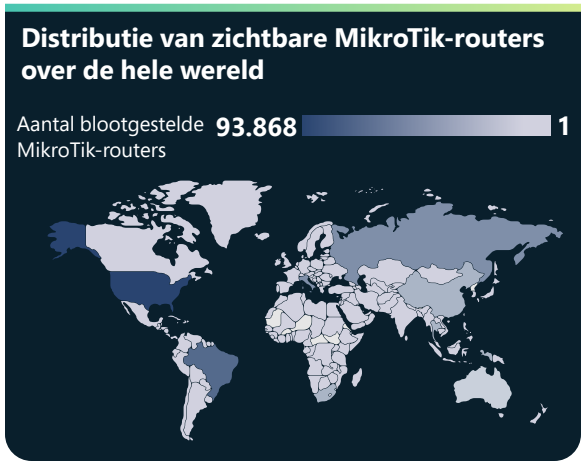
Internetgateways als criminele commando- en controle-infrastructuur

IoT-apparaten worden een steeds populairder doelwit voor cybercriminelen die wijdverbreide botnets gebruiken. Wanneer routers niet worden gepatcht en rechtstreeks aan internet worden blootgesteld, kunnen bedreigingsactoren deze misbruiken om toegang te krijgen tot netwerken, schadelijke aanvallen uit te voeren en zelfs hun activiteiten te ondersteunen.

Het team van Microsoft Defender voor IoT doet onderzoek naar apparatuur, variërend van verouderde industriële controlesystemen tot geavanceerde IoT-sensoren. Het team onderzoekt IoT- en OT-specifieke malware om bij te dragen aan de gedeelde lijst van aanwijzingen voor inbreuken.

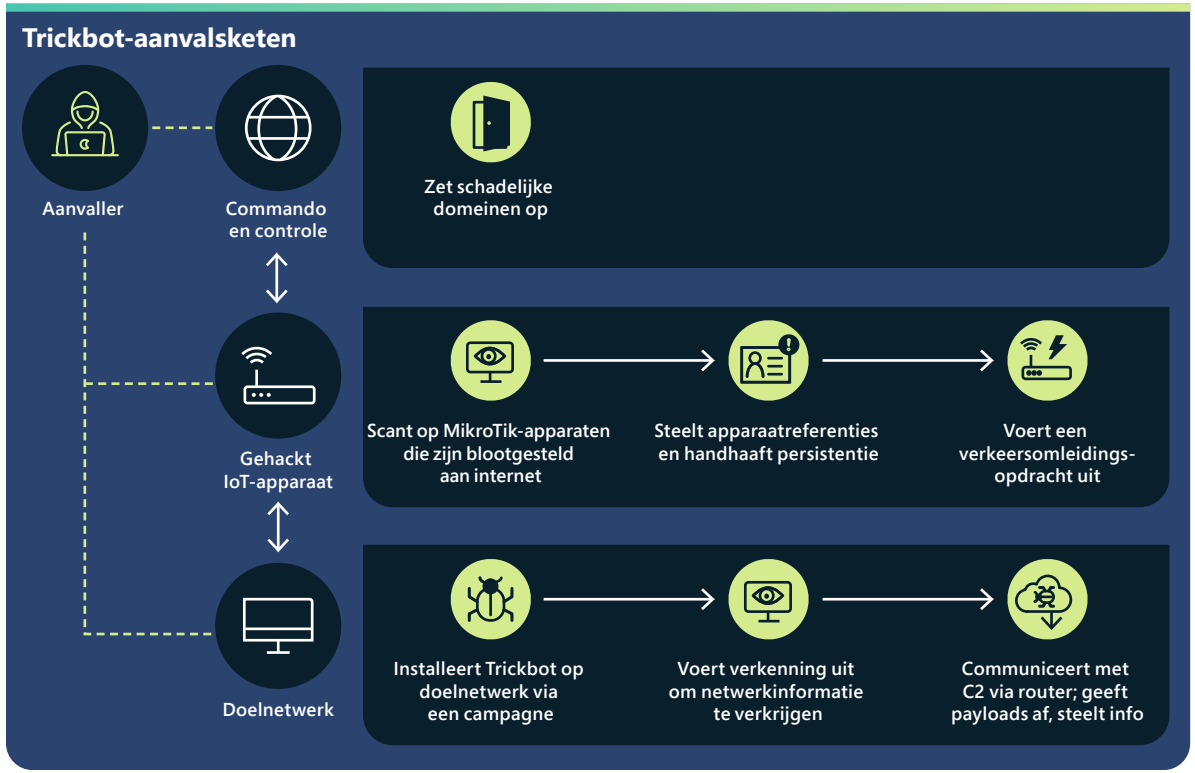
Routers zijn bijzonder kwetsbare aanvalsvectoren, omdat ze op grote schaal aanwezig zijn in huizen en organisaties met een internetverbinding. We hebben de activiteit van MikroTik-routers, een populaire router over de hele wereld, in particulier en commercieel verband gevolgd, waarbij we hebben vastgesteld hoe deze worden gebruikt voor command and control (C2), DNS-aanvallen (Domain Name System) en kaping voor crypto-mining.

Meer specifiek hebben we vastgesteld hoe Trickbot-operators gehackte MikroTik-routers gebruiken en deze opnieuw configureren als onderdeel van hun C2-infrastructuur. De populariteit van deze apparaten maakt misbruik door Trickbot nog erger en hun unieke hardware en software stellen bedreigingsactoren in staat om traditionele beveiligingsmaatregelen te omzeilen, hun infrastructuur uit te breiden en meer apparaten en netwerken in gevaar te brengen.



Blootgestelde routers lopen het risico dat potentiële kwetsbaarheden worden misbruikt.

Door verkeer met SSH-opdrachten (Secure Shell) bij te houden en te analyseren, zagen we dat aanvallers MikroTik-routers gebruikten om te communiceren met de Trickbot-infrastructuur nadat ze legitieme referenties naar apparaten hadden verkregen. Deze referenties kunnen worden verkregen via brute force-aanvallen, waarbij misbruik wordt gemaakt van bekende kwetsbaarheden met kant-en-klaar beschikbare patches en standaardwachtwoorden. Zodra toegang tot een apparaat is verkregen, verstrekt de aanvaller een unieke opdracht die verkeer omleidt tussen twee poorten in de router, waardoor de



Trickbot-aanvalsketen met het gebruik van MikroTik IoT-apparaten als proxyservers voor C2.

communicatielijn tot stand wordt gebracht tussen door Trickbot getroffen apparaten en de C2.

We hebben onze kennis van de verschillende methoden voor het aanvallen van MikroTik-apparaten, naast Trickbot, evenals bekende veelvoorkomende kwetsbaarheden en blootstellingen (CVE's) samengevoegd tot een open-source tool voor MikroTik-apparaten, die de forensische artefacten met betrekking tot aanvallen op deze apparaten kan extraheren.[31]

Apparaten die fungeren als reverse proxy's voor malware C2 zijn niet alleen uniek voor Trickbot- en MikroTik-routers. In samenwerking met het RiskIQ-team van Microsoft hebben we de betrokken C2 herleid en via SSL-certificaten de Ubiquiti- en LigoWave-apparaten geïdentificeerd die eveneens zijn getroffen.[32] Dit is een sterke aanwijzing dat IoT-apparaten actieve onderdelen worden van gecoördineerde aanvallen van vreemde mogendheden en een populair doelwit voor cybercriminelen die wijdverspreide botnets gebruiken.

Crypto-criminelen die IoT-apparaten misbruiken

Gatewayapparaten worden een steeds waardevoller doelwit voor bedreigingsactoren, omdat het aantal bekende kwetsbaarheden van jaar tot jaar toeneemt. Ze worden gebruikt voor crypto-mining en andere typen schadelijke activiteiten.

Naarmate cryptovaluta's populairder worden, hebben veel individuen en organisaties rekenkracht en netwerkresources geïnvesteerd vanaf apparaten zoals routers om valuta te delven op de blockchain. Het delven van cryptovaluta's is echter een tijdrovend en resource-intensief proces met een lage kans op succes. Mijnwerkers proberen de waarschijnlijkheid van het delven van een valuta te vergroten door samen te werken in gedistribueerde, coöperatieve netwerken, waarbij ze hashes ontvangen met betrekking tot het percentage van de valuta die ze hebben weten te delven met hun verbonden resources.

In het afgelopen jaar constateerde Microsoft een groeiend aantal aanvallen waarbij misbruik werd gemaakt van routers voor het omleiden van activiteiten met betrekking tot het delven van cryptovaluta's. Cybercriminelen hacken routers die zijn verbonden met mining-pools en leiden mining-verkeer om naar hun bijbehorende IP-adressen met DNS-vergiftigingsaanvallen, waardoor de DNS-instellingen van aangevallen apparaten worden gewijzigd. Getroffen routers registreren het verkeerde IP-adres voor een bepaalde domeinnaam en sturen hun mining-resources (of hashes) naar pools die door bedreigingsactoren worden gebruikt. Deze pools kunnen anonieme valuta's delven die verband houden met criminele activiteiten of legitieme hashes gebruiken die zijn gegenereerd door mijnwerkers om een percentage te verkrijgen van de valuta die ze hebben gedolven en zo te profiteren van hun activiteiten.

Bij meer dan de helft van de bekende kwetsbaarheden in 2021 ontbreekt een patch en blijft het updaten en beveiligen van routers op bedrijfs- en particuliere netwerken een grote uitdaging voor eigenaren en beheerders van apparaten.

Aantasting van apparaten voor illegale crypto-mining.

Een deel van de hashes uit de oorspronkelijke pool wordt gestolen door bedreigingsactoren, resources worden overgebracht naar hun pool of routers bevatten malware die resources stelen voor mining.

DNS-vergiftiging van gatewayapparaten brengt legitieme miningactiviteiten in gevaar en leidt resources om naar criminele miningactiviteiten.

Virtuele machines als criminele infrastructuur

De wijdverbreide overstap naar de cloud omvat cybercriminelen die gebruikmaken van privémiddelen van onwetende slachtoffers die zijn verkregen via phishing of het verspreiden van malafide referentie-stealers. Veel cybercriminelen kiezen ervoor om hun schadelijke infrastructuur in te stellen op cloudgebaseerde virtuele machines (VM's), containers en microservices.

Zodra de cybercrimineel toegang heeft, kan er een reeks gebeurtenissen plaatsvinden om de infrastructuur in te stellen, zoals een reeks virtuele machines, via scripting en geautomatiseerde processen. Deze gescripte, geautomatiseerde processen worden gebruikt om schadelijke activiteiten te starten, waaronder grootschalige spamaanvallen op e-mails, phishing-aanvallen en webpagina's die schadelijke content hosten. Het kan zelfs het opzetten van een geschaalde virtuele omgeving omvatten voor het uitvoeren van cryptovaluta-mining, waardoor het slachtoffer uiteindelijk een rekening van honderdduizenden dollars krijgt aan het einde van de maand.

Cybercriminelen begrijpen dat hun schadelijke activiteit een beperkte levensduur heeft voordat deze wordt gedetecteerd en uitgeschakeld. Als gevolg hiervan hebben ze opgeschaald en houden zij bij hun activiteiten op proactieve wijze rekening met onvoorziene gebeurtenissen. Ze zijn geobserveerd bij het vooraf voorbereiden van aangetaste accounts en het bewaken van hun omgevingen. Zodra een account (ingesteld met behulp van honderdduizenden virtuele machines) wordt gedetecteerd, stappen ze over op het volgende account, dat al is voorbereid via scripts voor onmiddellijke activering, en wordt hun schadelijke activiteit met weinig of geen onderbreking voortgezet.

Net als cloudinfrastructuur kan on-premises infrastructuur worden gebruikt in aanvallen met virtuele lokale omgevingen die onbekend zijn voor de on-premises gebruiker. Hiervoor moet het aanvankelijke toegangspunt open en toegankelijk blijven. On-premises privémiddelen zijn ook misbruikt door cybercriminelen om een verdere keten van cloudinfrastructuur te starten, die is ingesteld om hun oorsprong te verdoezelen en detectie van verdachte infrastructuur te voorkomen.

Direct bruikbare inzichten

1. Implementeer goede cyberhygiëne en geef cyberbeveiligingstraining voor werknemers met richtlijnen om te voorkomen dat ze het slachtoffer worden van social engineering.
2. Voer regelmatig geautomatiseerde controles van activiteitsanomalieën uit door middel van detecties op schaal om dit type aanvallen te helpen verminderen.
3. Update en beveilig routers op zakelijke en particuliere netwerken.

Is hacktivisme een blijvertje?

Hoewel hacktivisme geen nieuw fenomeen is, gaf de oorlog in Oekraïne een golf van vrijwillige hackers, waaronder enkele onder leiding van vreemde mogendheden, te zien die gebruikmaakten van cybertools om de reputatie of bezittingen van politieke tegenstanders, organisaties en zelfs vreemde mogendheden te beschadigen.

In februari 2022 riep de regering van Oekraïne particuliere burgers over de hele wereld op om cyberaanvallen uit te voeren op Rusland als onderdeel van het 300.000 man sterke 'IT-leger' van het land.[33] Tegelijkertijd begonnen gevestigde hacktivistische groepen zoals Anonymous, Ghostsec, Against The West, Belarusian Cyber Partisans en RaidForum2 aanvallen uit te voeren ter ondersteuning van Oekraïne. Andere groepen, waaronder een deel van de Conti-ransomware-bende, kozen de kant van Rusland.[34]

In de maanden die volgden waren de activiteiten van Anonymous goed zichtbaar. Hackers die handelden in naam van de groep, of in naam van een van haar partners, hebben tijdelijk duizenden Russische en Wit-Russische websites uitgeschakeld, honderden gigabytes aan gestolen data gelekt, Russische tv-kanalen gehackt om pro-Oekraïense content af te spelen en zelfs aangeboden om Bitcoin te betalen voor overgegeven Russische tanks.

De opkomst van burgerhackers

Sociale-mediaplatforms maakten de snelle organisatie en mobilisatie mogelijk van duizenden zogenaamde burgerhackers, die instructies kregen voor het uitvoeren van gemakkelijk uitvoerbare aanvallen zoals DDoS-aanvallen. Organisatoren maakten gebruik van Twitter, Telegram en privéforums om hackers te verzamelen, activiteiten te organiseren en handleidingen voor hacking te verspreiden.

De meeste van deze hackers beschikken echter waarschijnlijk over beperkte vaardigheden, zelfs met instructie. Dit suggereert twee mogelijke toekomsten: een toekomst waarin honderden of duizenden individuen met rudimentaire technische mogelijkheden gebruikmaken van aanvalsjablonen om gecoördineerde of individuele hacktivistische aanvallen uit te voeren op doelen, of een tweede toekomst waarbij het uiteindelijke einde van de vijandelijkheden in Oekraïne leidt tot de beëindiging van hun hacktivisme, althans tot de volgende politieke of sociale kwestie hen tot actie inspireert.

Politisering van hackers

Het grotere risico dat deze politieke mobilisatie met zich meebrengt, is de inzet van technisch onderlegde hackers die mogelijk cyberaanvallen kunnen blijven uitvoeren tegen doelen van buitenlandse overheden om hun eigen nationale prioriteiten te ondersteunen, op eigen initiatief of op initiatief van hun overheid.

Iran, China en Rusland maken al gebruik van hacktivisme als wervingskanaal voor hun groepen van staatshackers. In april 2022 lanceerde de pro-Russische hackgroep Killnet bijvoorbeeld DDoS-aanvallen op de spoorwegmaatschappijen, regionale vliegvelden en servers van de overheid in Tsjechië, ook al is Tsjechië niet direct betrokken bij de oorlog.[35] Tegelijkertijd kunnen sommige overheden hacktivisme gebruiken als dekmantel voor traditionele cyberspionage of sabotageacties, bijvoorbeeld Iraanse activiteiten tegen Israël.

In een omgeving van toenemende DDoS-aanvallen in verband met hacktivisme wordt de technologie-industrie uitgedaagd om snel het verschil tussen normale en abnormale verkeersstromen naar een website te ontcijferen. Microsoft en zijn partners hebben een verzameling tools ontwikkeld die schadelijk DDoS-verkeer identificeren en herleiden tot de oorsprong. Daarnaast kan het Azure-platform van Microsoft machines op het platform identificeren die buitengewoon veel uitgaand verkeer genereren en deze afsluiten.

Opkomst van protestware

Protestware is ontstaan als een direct gevolg van emotionele reacties op de oorlog tussen Rusland en Oekraïne. Sommige developers van open-sourcesoftware gebruikten de populariteit van hun software als middel om hun stem te laten horen of actie te ondernemen tegen een zich ontwikkelende geopolitieke situatie. Dit omvatte onschadelijke tekstbestanden die op een bureaublad of browser werden geopend om berichten van vrede te verspreiden, maar ook gerichte aanvallen op basis van geolocatie van IP-adressen en destructieve acties, zoals het wissen van een harde schijf. Naar verwachting zal bij andere wereldwijde gebeurtenissen die zich in de toekomst zullen voordoen opnieuw protestware worden ingezet. Aangezien dit over het algemeen gevallen zijn waarin gerespecteerde open-sourcebeheerders besluiten om persoonlijke verklaringen af te leggen met behulp van hun eigen open-sourceonderdelen, is er momenteel geen bescherming aanwezig om dit soort wijzigingen in de bronbestandspakketten te voorkomen en moeten gebruikers rekening houden met de mogelijke impact.

Sociale-mediaplatforms maakten de organisatie en mobilisatie mogelijk van duizenden zogenaamde burgerhackers, die instructies kregen voor het uitvoeren van gemakkelijk uitvoerbare aanvallen zoals DDoS-aanvallen.

Direct bruikbare inzichten

1. De technologische industrie moet de handen ineenslaan om een uitgebreid antwoord op deze nieuwe bedreiging te ontwerpen.
2. Toonaangevende technologiebedrijven, waaronder Microsoft, hebben tools om schadelijk verkeer in verband met DDoS-aanvallen te identificeren en de verantwoordelijke machines uit te schakelen.
3. Open-sourcegebruikers moeten extra goed opletten in tijden van geopolitieke conflicten.

Eindnoten

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. Endpoint detection and response. 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. Een Vetted Forum is een online discussieforum waarbij een bestaand lid garant moet staan bij toevoeging van een nieuw lid.
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. Databron: Defender for Office (schadelijke e-mail/activiteiten van gehackte identiteiten), Azure Active Directory Identity Protection (gebeurtenissen/waarschuwingen voor gehackte identiteiten), Defender for Cloud Apps (gebeurtenissen voor datatoegang door gehackte identiteiten) en M365D (correlatie tussen producten).
17. Databron: Defender for Endpoint (waarschuwingen/gebeurtenissen over aanvalsgedrag), Defender for Office (schadelijke e-mail) en M365D (correlatie tussen producten).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Op domein gebaseerde berichtverificatie, rapportage en conformiteit: een e-mailverificatie-, beleids- en rapportageprotocol dat is ontworpen om eigenaren van e-maildomeinen de mogelijkheid te bieden hun domein te beschermen tegen onbevoegd gebruik.
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 feb 2010).
27. Zie Bowden, Mark. Worm: The First Digital World War. Grove / Atlantic, Inc., 27 sep 2011.
28. In het bijzonder staat Regel 65 van de federale regels voor burgerlijke rechtsvordering een partij toe om een dergelijke voorziening te zoeken als: 1) de partij directe en onherstelbare schade zal lijden als de vrijstelling niet wordt verleend, en 2) de partij probeert de andere partij tijdig in kennis te stellen. Bovendien vereist de wet dat er een afwegingstoets wordt toegepast, waarbij het recht van de gedaagde om kennis te nemen wordt afgezet tegen de omvang van de schade voor het publiek.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9 feb 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 aug 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Bedreigingen door vreemde mogendheden

Actoren van vreemde mogendheden lanceren steeds geavanceerdere cyberaanvallen om detectie te omzeilen en hun strategische prioriteiten te bevorderen.

Een overzicht van

bedreigingen door vreemde mogendheden

Actoren van vreemde mogendheden lanceren steeds geavanceerdere cyberaanvallen om detectie te omzeilen en hun strategische prioriteiten te bevorderen. De opkomst van de inzet van cyberwapens in de hybride oorlog in Oekraïne is het begin van een nieuw tijdperk van conflicten.

Rusland heeft zijn oorlog ook ondersteund met informatiebeïnvloedingsactiviteiten, met behulp van propaganda om meningen in Rusland, in Oekraïne en wereldwijd te beïnvloeden. Dit eerste grootschalige hybride conflict heeft ons andere belangrijke lessen geleerd. Ten eerste kan de beveiliging van digitale activiteiten en data het best worden beschermd, zowel in cyberspace als in de fysieke ruimte, door de overstap te maken naar de cloud. Aanvankelijke Russische aanvallen waren gericht op on-premises services met vernietigingsmalware en op fysieke datacenters met een van de eerste gelanceerde projectielen.

Oekraïne reageerde hierop door workloads en data snel naar hyperscale clouds te verplaatsen die in datacenters buiten Oekraïne worden gehost. Ten tweede hielpen ontwikkelingen op het gebied van informatie over cyberbedreigingen en endpointbeveiliging die mogelijk werden gemaakt door de data en geavanceerde AI- en ML-services in de cloud Oekraïne zich te verdedigen tegen Russische cyberaanvallen.

Elders zijn actoren van vreemde mogendheden steeds meer actief en gebruiken ze nieuwe ontwikkelingen in automatisering, cloudinfrastructuur en technologieën voor externe toegang om een breder scala aan doelen aan te vallen. Vaak werden IT-supply chains van bedrijven die toegang tot de uiteindelijke doelen mogelijk maken, aangevallen. Cyberbeveiliging werd nog belangrijker omdat actoren snel gebruikmaakten van niet-gepatchte kwetsbaarheden, zowel geavanceerde als brute force-technieken gebruikten om aanmeldingsreferenties te stelen en hun activiteiten verhulden met open-source- of legitieme software. En Iran sluit zich aan bij Rusland bij het gebruik van destructieve cyberwapens, waaronder ransomware, als onderdeel van hun aanvallen.

Deze ontwikkelingen vereisen een dringende invoering van een consistent, wereldwijd kader dat prioriteit geeft aan mensenrechten en mensen beschermt tegen roekeloos online gedrag van de staat. Alle landen moeten samenwerken om overeengekomen normen en regels voor verantwoord gedrag van de staat te implementeren.

De bescherming van Oekraïne: eerste lessen uit de cyberoorlog - Microsoft On the Issues

Essentiële infrastructuur is in toenemende mate het doelwit, met name in de IT-sector, financiële dienstverlening, transportsystemen en communicatie-infrastructuur.

Ga voor meer informatie naar p35

IT-supply chain die wordt gebruikt als gateway voor toegang tot doelen.

NOBELIUM

Ga voor meer informatie naar p36

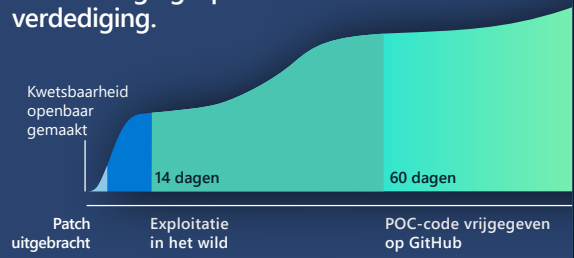
China breidt zijn wereldwijde doelgroep uit, met name naar kleinere landen in Zuidoost-Azië, om informatie en concurrentievoordeel te verkrijgen.

Ga voor meer informatie naar p44

Iran werd steeds agressiever na de machtsoverdracht, breidde ransomwareaan-vallen uit die verder reikten dan regionale tegenstanders en slachtoffers maakten in de VS en de EU, en richtte zich op prominente en essentiële infrastructuur in de VS.

Ga voor meer informatie naar p46

Identificatie en snelle exploitatie van niet-gepatchte kwetsbaarheden is een belangrijke tactiek geworden. Snelle implementatie van beveiligingsupdates is de sleutel tot verdediging.



Ga voor meer informatie naar p39

Noord-Korea richtte zijn pijlen op defensie- en luchtvaartbedrijven, cryptovaluta's, persdiensten, overlopers en hulporganisaties om de doelstellingen van het regime te bereiken: de defensie opbouwen, de economie versterken en binnenlandse stabiliteit waarborgen.

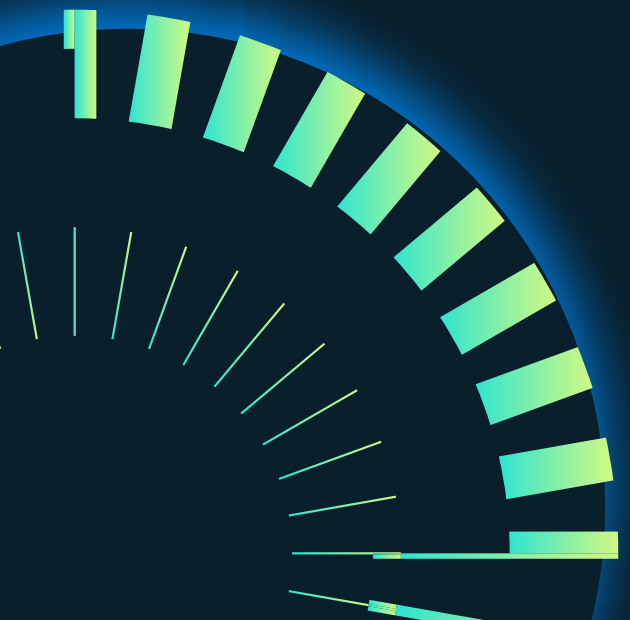
Ga voor meer informatie naar p49

Cyberhuurlingen bedreigen de stabiliteit van cyberspace omdat deze groeiende industrie van particuliere bedrijven geavanceerde tools, technieken en services ontwikkelt en verkoopt om hun klanten (vaak overheden) in staat te stellen in te breken in netwerken en apparaten.

Ga voor meer informatie naar p52

Inleiding

Na spraakmakende aanvallen in 2020 en 2021 besteedden bedreigingsactoren van vreemde mogendheden aanzienlijke middelen aan de aanpassing aan nieuwe beveiligingsmaatregelen die door organisaties werden geïmplementeerd om zich te verdedigen tegen geavanceerde bedreigingen.



Net als bij bedrijfsorganisaties, gebruikten tegenstanders verbeteringen in automatisering, cloudinfrastructuur en technologieën voor externe toegang om hun aanvallen op een breder scala aan doelen uit te breiden. Deze tactische aanpassingen resulteerden in nieuwe benaderingen en grootschalige aanvallen op supply chains van bedrijven. IT-hygiëne op het gebied van IT-beveiliging werd nog belangrijker toen actoren nieuwe manieren ontwikkelden om snel niet-gepatchte kwetsbaarheden te benutten, technieken voor het binnendringen van bedrijfsnetwerken uitbreidden en hun activiteiten verdoezelden met open-source- of legitieme software. Nieuwe aanvalstechnieken boden nieuwe en moeilijker te detecteren vectoren om toegang te krijgen tot het netwerk van een doelwit. Tot slot zagen we, toen fysieke aanvallen in oorlogstijd escaleerden, dat cyberaanvallen een prominente rol speelden bij militaire activiteiten.

Het conflict in Oekraïne heeft voor een bijzonder aangrijpend voorbeeld gezorgd van de manier waarop cyberaanvallen zich ontwikkelen en parallel aan de militaire conflicten op de grond een impact op de wereld hebben. Stroomsystemen, telecommunicatiesystemen, media en andere essentiële infrastructuur werden allemaal het doelwit van zowel fysieke aanvallen als cyberaanvallen. Pogingen tot netwerkinbreuken die vaak werden waargenomen als onderdeel van spionage- en informatie-exfiltratiecampagnes gingen zich in de hybride oorlog richten op destructieve aanvallen met vernietigingsmalware op essentiële infrastructuursystemen. Het verbinden van de beveiliging van deze systemen met de cloud resulteerde in een vroegtijdige detectie en verstoring van potentieel verwoestende aanvallen.[1]

Voor het eerst tijdens een grote cybergebeurtenis gebruikten gedragsdetecties waarbij gebruik werd gemaakt van machine learning bekende aanvalspatronen om met succes nieuwe aanvallen te identificeren en te stoppen zonder voorafgaande kennis van de onderliggende malware, zelfs nog voordat mensen zich bewust waren van de bedreigingen. We hebben ook de waarde bevestigd van het in realtime delen van bedreigingsinformatie met verdedigers die deze systemen beschermen, waardoor ze essentiële informatie krijgen om te anticiperen op en zich te verdedigen tegen actieve aanvallen.

Bedreigingsactoren die wereldwijd actief zijn namens vreemde mogendheden blijven hun activiteiten op nieuwe en oude manieren uitbreiden. China, Noord-Korea, Iran en Rusland voerden allemaal aanvallen uit op klanten van Microsoft. De supply chain voor IT-services werd een gemeenschappelijk doelwit omdat actoren de focus verlegden naar upstream-services die toegangspunten kunnen zijn tot meerdere organisaties. We verwachten dat actoren vertrouwde relaties in de supply chains van ondernemingen blijven benutten, waarbij de nadruk ligt op het belang van uitgebreide handhaving van verificatieregels, zorgvuldige patching en accountconfiguratie voor externe toegangsinfrastructuur en frequente audits van partnerrelaties om de authenticiteit te verifiëren.

Staatshackers hebben, net als ransomware- en criminele exploitanten, gereageerd op de toegenomen blootstelling door zich te richten op slecht geconfigureerde of niet-gepatchte bedrijfssystemen (VPN/VPS-infrastructuur, on-premises servers, software van derden) voor het uitvoeren van aanvallen met middelen die al op het netwerk beschikbaar zijn ('living-off-the-land'). Velen hebben het gebruik van standaardmalware en open-source red-teamtools om hun schadelijke activiteiten te verhullen, verhoogd.

Het resultaat is dat het handhaven van een sterke basishygiëne op het gebied van IT-beveiliging via patching met prioriteit, het inschakelen van anti-manipulatiefuncties, het gebruiken van beheertools voor aanvalsoppervlakken zoals RiskIQ om een extern beeld van een aanvalsoppervlak te krijgen en het inzetten van meervoudige verificatie in de hele onderneming zijn uitgegroeid tot basisprincipes voor proactieve bescherming tegen veel geavanceerde actoren.

Staatshackers maken ook op grotere schaal gebruik ransomware als tactiek bij hun aanvallen, vaak met hergebruik van malware voor het afpersen van losgeld die door dat criminele ecosysteem is gecreëerd. We hebben gezien dat zowel in Iran als in Noord-Korea gevestigde actoren ransomware-tools gebruiken om systemen van regionale concurrenten, vaak met inbegrip van essentiële infrastructuur, te beschadigen. Tot slot hebben we de groeiende dreiging gezien van cyberhuurlingen die tools, technieken en services ontwikkelen en verkopen om exploits in te zetten tegen kwetsbare oplossingen van derden. De verfijning en wendbaarheid van aanvallen door actoren van vreemde mogendheden zullen zich elk jaar blijven ontwikkelen. Organisaties moeten reageren door op de hoogte te blijven van deze actorwijzigingen en parallel hieraan beschermingsmaatregelen te ontwikkelen.

John Lambert
Corporate Vice President and Distinguished Engineer, Microsoft Threat Intelligence Center

Achtergrond van data van vreemde mogendheden

Bedreigingen door vreemde mogendheden zijn cyberbedreigingsactiviteiten die hun oorsprong vinden in een bepaald land met de klaarblijkelijke bedoeling om de nationale belangen te behartigen. Staatshackers vormen enkele van de meest geavanceerde en hardnekkige bedreigingen waarmee onze klanten worden geconfronteerd, waaronder diefstal van intellectueel eigendom, spionage, bewaking, diefstal van aanmeldingsreferenties, destructieve aanvallen en meer.

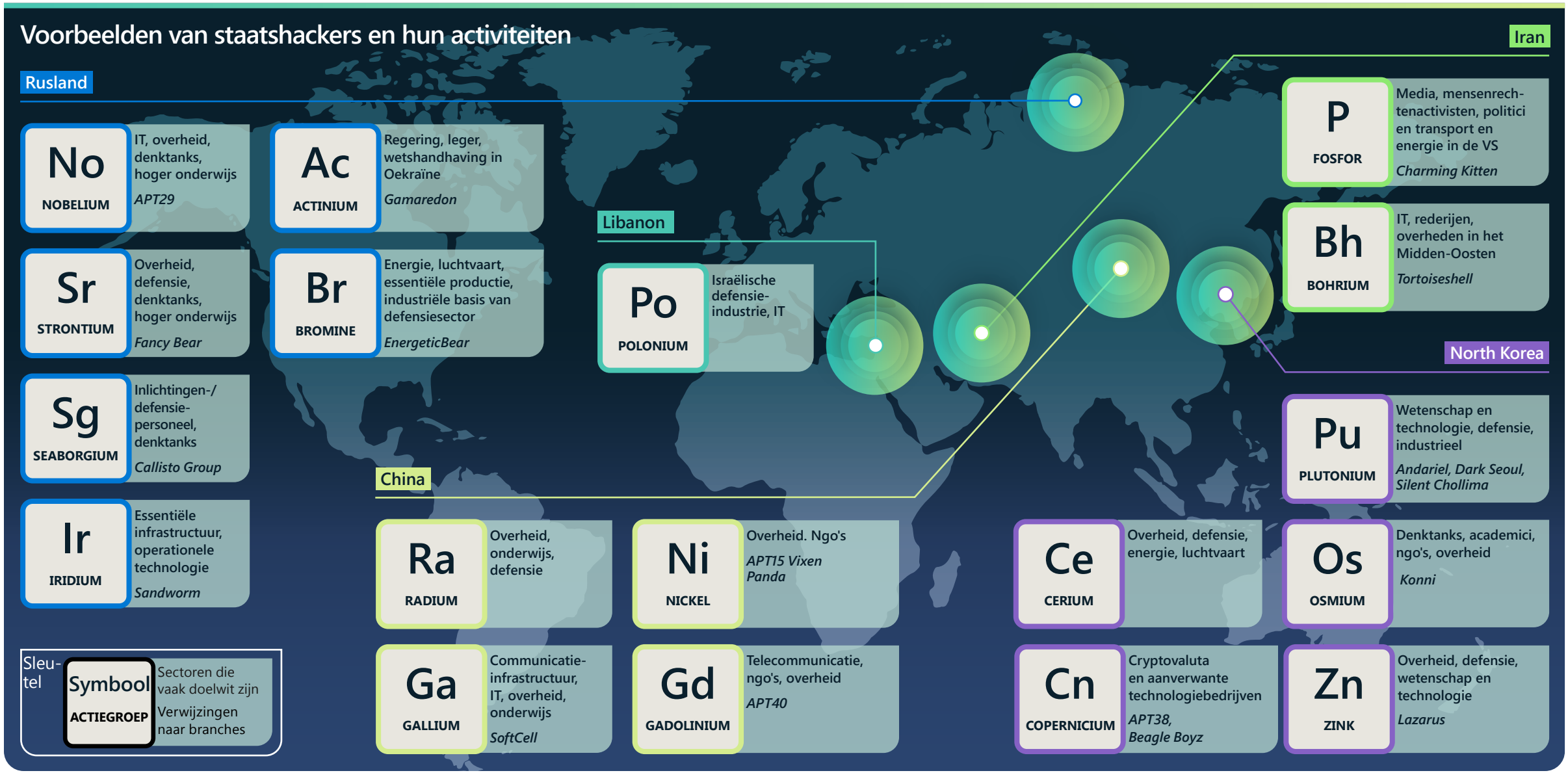
We investeren aanzienlijke middelen in het ontdekken, begrijpen en bestrijden van deze bedreigingen. Wanneer een organisatie of individuele accounthouder wordt aangevallen of gehackt door waargenomen activiteiten van een staatshacker, stuurt Microsoft een waarschuwing in de vorm van een NSN (Nations State Notification of melding over een vreemde mogendheid) rechtstreeks naar de klant, inclusief de informatie die ze nodig hebben om de activiteit te onderzoeken. Tot juni 2022 hebben we meer dan 67.000 NSN's afgegeven nadat we in 2018 zijn begonnen.

Microsoft NSN-waarschuwingsdata worden in dit hoofdstuk gepresenteerd om een overzicht te bieden van meetbare activiteit. Het niveau van de activiteit van een vreemde mogendheid in de grafieken is gebaseerd op het aantal NSN's dat Microsoft aan klanten heeft uitgegeven als reactie op de detectie van actoren van vreemde mogendheden die ten minste één account in de klantorganisatie als doelwit hebben of hebben gehackt.

De vier primaire vreemde mogendheden waarvan we de bedreigingsgroepen in dit rapport opnemen zijn Rusland, China, Iran en Noord-Korea. Deze vertegenwoordigen de landen van herkomst voor de meest waargenomen actoren die zich het afgelopen jaar op klanten van Microsoft hebben gericht. Het rapport bevat ook onze observaties over bedreigingsgroepen uit Libanon en van cyberhuurlingen of schadelijke actoren uit de particuliere sector.

Microsoft identificeert groepen die optreden namens vreemde mogendheden aan de hand van namen van chemische elementen (zoals NOBELIUM), waarvan er enkele op de volgende pagina worden weergegeven. We gebruiken DEV-####-aanduidingen als tijdelijke naam voor een onbekend, opkomend of zich ontwikkelend cluster van bedreigingsactiviteiten, waardoor we dit kunnen volgen als een unieke set informatie totdat we een hoge mate van zekerheid hebben over de oorsprong of identiteit van de actor achter de activiteit.

Zodra een DEV aan de criteria voldoet, wordt deze omgezet in een benoemde actor of samengevoegd met bestaande actoren. In dit hoofdstuk geven we voorbeelden van groepen die optreden namens vreemde mogendheden en DEV-groepen om een dieper inzicht te krijgen in aanvalsdoelen, technieken en analyse van motivaties. Hoewel veel van deze groepen dezelfde tools gebruiken als cybercriminelen, vormen ze unieke bedreigingen in de vorm van op maat gemaakte malware, de mogelijkheid om zero-day-kwetsbaarheden te ontdekken en te verzilveren en juridische straffeloosheid.


Voorbeelden van staatshackers en hun activiteiten
Rusland
No
NOBELIUM
IT, overheid, denktanks, hoger onderwijs
APT29
Ac
ACTINIUM
Regering, leger, wetshandhaving in Oekraïne
Gamaredon
Sr
STRONTIUM
Overheid, defensie, denktanks, hoger onderwijs
Fancy Bear
Br
BROMINE
Energie, luchtvaart, essentiële productie, industriële basis van defensiesector
EnergeticBear
Sg
SEABORGIUM
Inlichtingen-/ defensie-personeel, denktanks
Callisto Group
Ir
IRIDIUM
Essentiële infrastructuur, operationele technologie
Sandworm
Libanon
Po
POLONIUM
Israëlische defensie-industrie, IT
China
Ra
RADIUM
Overheid, onderwijs, defensie
Ni
NICKEL
Overheid. Ngo's
APT15 Vixen Panda
Ga
GALLIUM
Communicatie-infrastructuur, IT, overheid, onderwijs
SoftCell
Gd
GADOLINIUM
Telecommunicatie, ngo's, overheid
APT40
Iran
P
FOSFOR
Media, mensenrecht-tenactivisten, politici en transport en energie in de VS
Charming Kitten
Bh
BOHRIUM
IT, rederijen, overheden in het Midden-Oosten
Tortoiseshell
North Korea
Pu
PLUTONIUM
Wetenschap en technologie, defensie, industrieel
Andariel, Dark Seoul, Silent Chollima
Ce
CERIUM
Overheid, defensie, energie, luchtvaart
Os
OSMIUM
Denktanks, academici, ngo's, overheid
Konni
Cn
COPERNICIUM
Cryptovaluta en aanverwante technologiebedrijven
APT38, Beagle Boyz
Zn
ZINK
Overheid, defensie, wetenschap en technologie
Lazarus
Sleu-tel
Symbool
ACTIEGROEP
Sectoren die vaak doelwit zijn
Verwijzingen naar branches

Het zich ontwikkelende dreigingslandschap

De missie van Microsoft om actoren van vreemde mogendheden te volgen en klanten te informeren wanneer we zien dat ze het doelwit of gecompromitteerd zijn, is geworteld in onze missie om onze klanten tegen aanvallen te beschermen.

Deze melding is een cruciaal onderdeel van ons streven om klanten te informeren of waargenomen aanvallen met succes worden voorkomen door onze beveiligingsproducten, of dat de aanvallen effectief zijn vanwege onbekende zwakke punten in de beveiliging. Het bijhouden van meldingen in de loop van de tijd helpt Microsoft om trends in bedreigingen te identificeren door actoren en productbescherming te richten op het op proactieve wijze beperken van bedreigingen voor klanten in onze cloudservices.

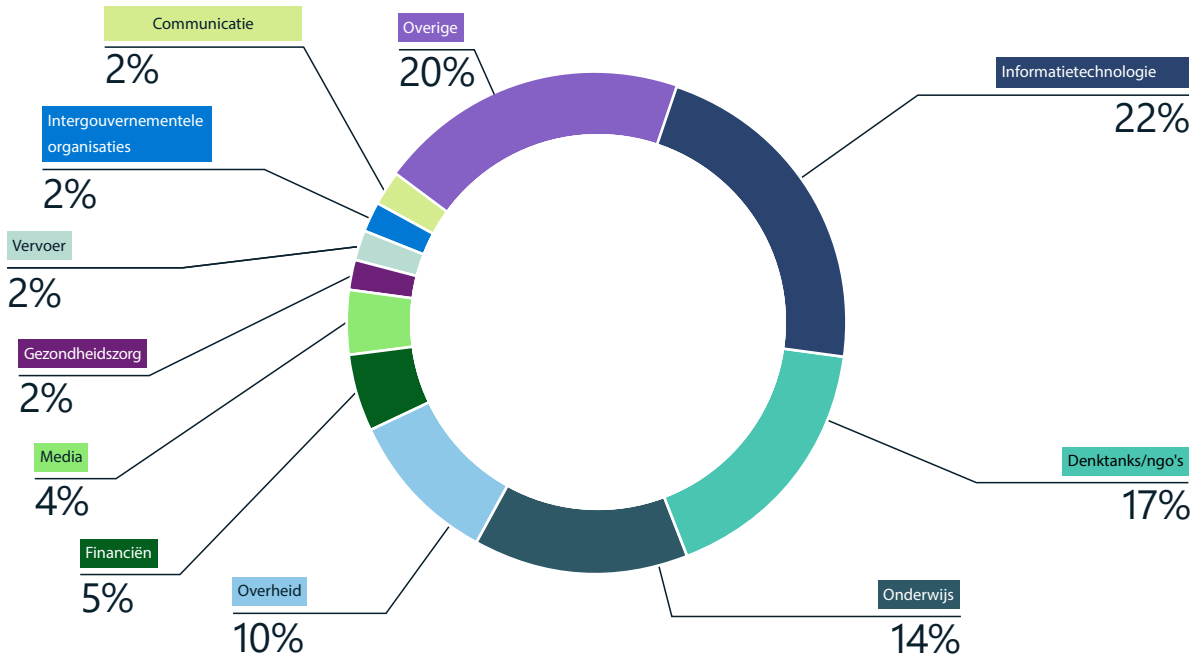
Met deze tracking kunnen we ook data en inzichten delen over wat we zien. De analisten die deze actoren volgen en hun aanvallen in de gaten houden, vertrouwen op een combinatie van technische indicatoren en geopolitieke expertise om de motivaties van de actoren te begrijpen, waarbij technische en wereldwijde context worden gecombineerd met nieuwe inzichten. Deze curatie biedt een uniek beeld van de prioriteiten van cyberactoren van vreemde mogendheden en hoe hun motivaties de politieke, militaire en economische prioriteiten van de vreemde mogendheden waarvoor zij werken zouden kunnen weerspiegelen.

Politieke ontwikkelingen in het afgelopen jaar hebben de prioriteiten en risicotolerantie van door de staat gesponsorde bedreigingsgroepen wereldwijd bepaald. Nu de geopolitieke relaties zijn verstoord en haviken in sommige landen meer controle hebben gekregen, zijn cyberactoren brutaler en agressiever geworden. Een voorbeeld:

- Rusland viel op meedogenloze wijze de regering van Oekraïne en de essentiële infrastructuur van het land aan als aanvulling op zijn militaire actie ter plaatse.[2]
- Iran voerde agressieve aanvallen uit op essentiële Amerikaanse infrastructuur zoals havenautoriteiten.
- Noord-Korea zette zijn campagne voort om cryptovaluta te stelen van financiële en technologiebedrijven.
- China breidde zijn wereldwijde cyberspionageactiviteiten uit.

Hoewel actoren van een vreemde mogendheid technisch geavanceerd kunnen zijn en een breed scala aan tactieken kunnen gebruiken, kunnen hun aanvallen vaak worden beperkt door een goede cyberhygiëne te hanteren. Veel van deze actoren vertrouwen op relatief low-tech middelen, zoals e-mails voor spear-phishing, om geavanceerde malware te leveren in plaats van te investeren in het ontwikkelen van aangepaste exploits of gebruik te maken van gerichte social engineering om hun doelstellingen te bereiken.

Industrietakken die het doelwit zijn van actoren van vreemde mogendheden



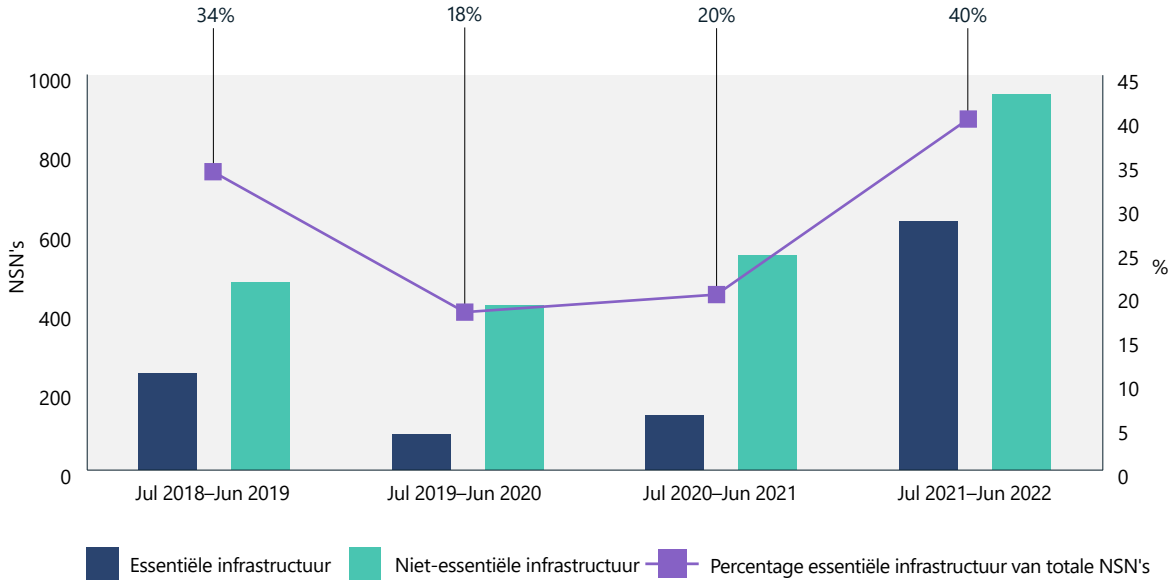
Staatshackersgroepen richtten zich op een reeks sectoren. Russische en Iraanse staatshackers richtten zich op de IT-industrie als middel om toegang te krijgen tot klanten van IT-bedrijven. Denktanks, niet-gouvernementele organisaties (ngo's), universiteiten en overheidsinstellingen bleven andere gemeenschappelijke doelwitten van actoren van vreemde mogendheden.

Staatshackers hebben een verscheidenheid aan doelstellingen die kunnen leiden tot een aanval op specifieke groepen organisaties of individuen. In het afgelopen jaar is het aantal aanvallen op supply chains toegenomen, met een speciale focus op IT-bedrijven. Door IT-serviceproviders in gevaar te brengen, zijn bedreigingsactoren vaak in staat om hun oorspronkelijke doelwit te bereiken via een vertrouwde relatie met het bedrijf dat verbonden systemen beheert, of mogelijk aanvallen op een veel grotere schaal uit te voeren door honderden downstreamklanten in één aanval te compromitteren. Na de IT-sector waren de meest beoogde entiteiten denktanks, academici die aan universiteiten zijn verbonden en ambtenaren. Dit zijn aantrekkelijke 'zachte doelen' voor spionage om informatie te verzamelen over geopolitieke kwesties.

Het zich ontwikkelende dreigingslandschap

Vervolg

Trends in essentiële infrastructuur

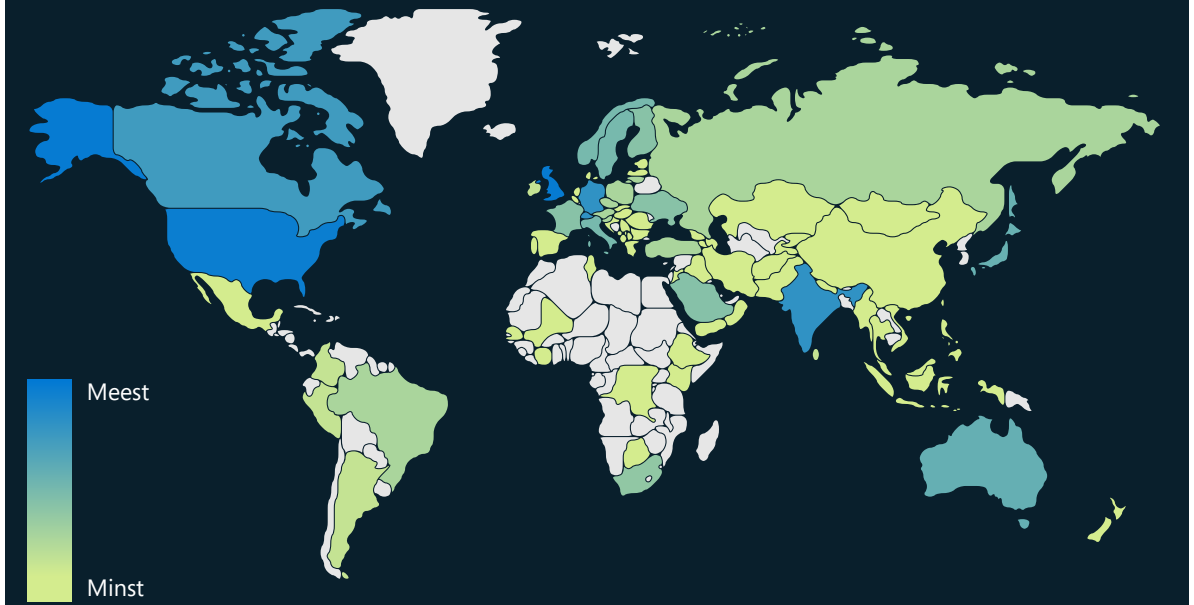


Staatshackersgroepen hebben zich het afgelopen jaar in toenemende mate op essentiële infrastructuur[3] gericht, waarbij actoren zich concentreren op bedrijven in de IT-sector, financiële dienstverlening, transportsystemen en communicatie-infrastructuur.

"Vóór de invasie in Oekraïne dachten overheden dat data in een land moesten blijven om veilig te zijn. Na de invasie maakt het migreren van data naar de cloud en het verplaatsen buiten de territoriale grenzen nu deel uit van de planning voor veerkracht en goed bestuur."

Cristin Flynn Goodwin,
Associate General Counsel, Customer Security & Trust

Geografische targeting van actoren van vreemde mogendheden



De cybertargeting van staatshackersgroepen omvatte het afgelopen jaar de hele wereld, met een bijzonder zware focus op Amerikaanse en Britse ondernemingen. Organisaties in Israël, de Verenigde Arabische Emiraten, Canada, Duitsland, India, Zwitserland en Japan behoorden eveneens tot de meest populaire doelwitten, volgens onze NSN-data.

Direct bruikbare inzichten

1. Identificeer en bescherm je potentiële hoogwaardige datadoelen, risicotechnologieën, informatie en bedrijfsactiviteiten die mogelijk aansluiten bij de strategische prioriteiten van staatshackersgroepen.
2. Schakel cloudbeveiliging in om bekende en nieuwe bedreigingen voor je netwerk op schaal te identificeren en te beperken.

De supply chain voor IT als gateway naar het digitale ecosysteem

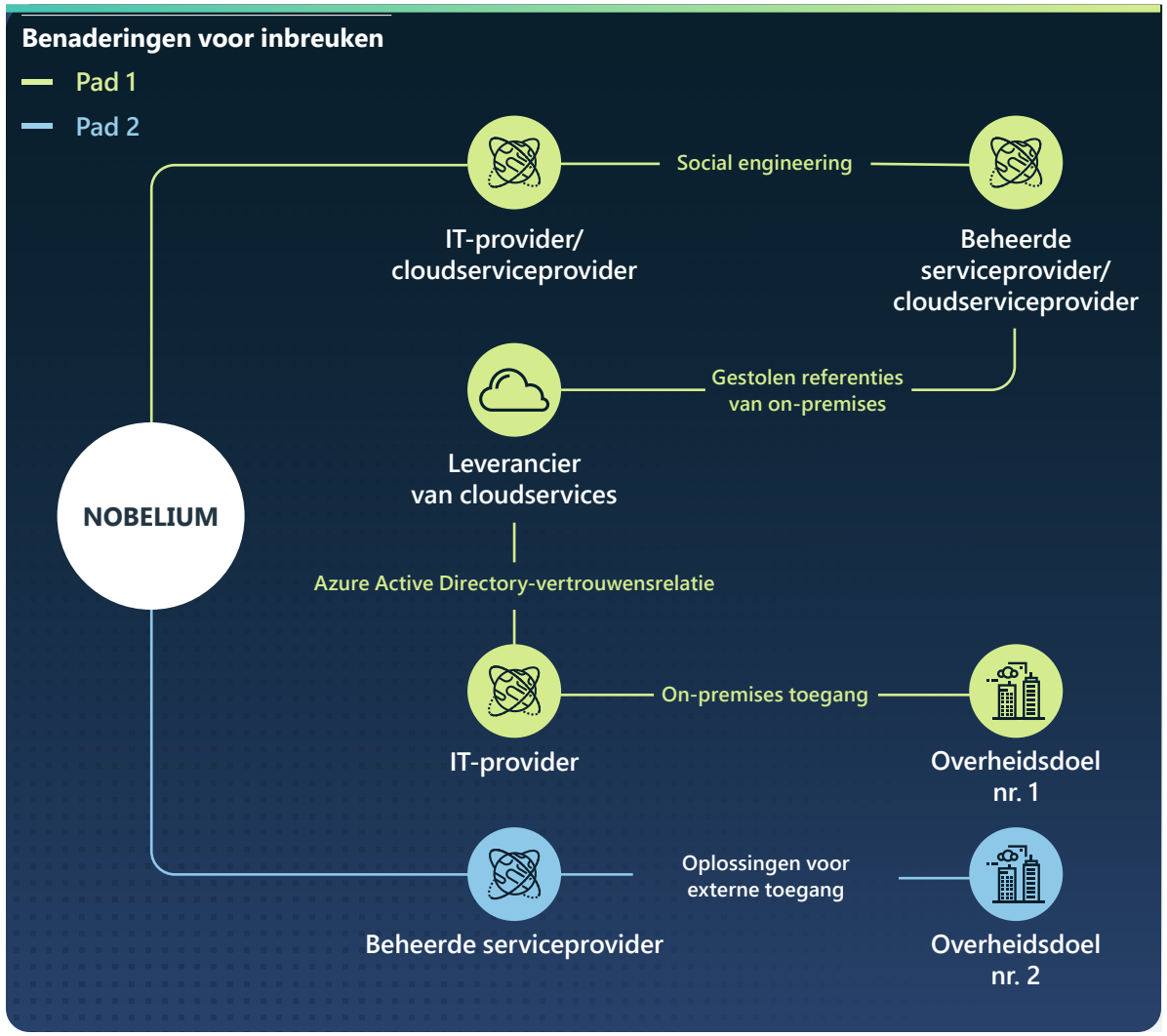
Door hun pijlen te richten op IT-serviceproviders kunnen de bedreigingsactoren misbruik maken van andere interessante organisaties door te profiteren van het vertrouwen en de toegang die wordt verleend aan deze leveranciers in de supply chain. In het afgelopen jaar richtten cyberbedreigingsgroepen van vreemde mogendheden hun pijlen op IT-serviceverleners om externe doelen aan te vallen en toegang te krijgen tot downstreamclients in de sectoren overheid, beleid en essentiële infrastructuur.

IT-serviceproviders zijn aantrekkelijke tussenliggende doelwitten omdat ze honderden directe en duizenden indirecte klanten bedienen die van belang zijn voor buitenlandse inlichtingendiensten. Bij misbruik hiervan, kunnen de routinematige bedrijfspraktijken en de gedelegeerde beheerdersbevoegdheden die deze bedrijven genieten, kwaadwillende actoren in staat stellen om toegang te krijgen tot clientnetwerken van IT-serviceproviders en deze te manipuleren zonder dat dit onmiddellijk tot waarschuwingen leidt.

In het afgelopen jaar heeft NOBELIUM geprobeerd om toegang te verkrijgen tot bevoegde accounts bij cloudoplossingen en andere beheerde serviceproviders om gerichte downstreamtoegang te verkrijgen tot voornamelijk Amerikaanse en Europese overheids- en beleidsklanten.

NOBELIUM liet zien hoe een aanpak van "één schending uitvoeren om vele te laten volgen" kan worden gericht tegen een vermeende geopolitieke tegenstander. Het afgelopen jaar probeerde de bedreigingsactor zowel externe als directe inbreuken uit te voeren bij gevoelige organisaties in de lidstaten van de Noord-Atlantische Verdragsorganisatie (NAVO), die door de Russische overheid als een existentiële bedreiging worden gezien. Tussen juli 2021 en begin juni 2022 ging 48 procent van de klantmeldingen van Microsoft over bedreigingen door Rusland tegen klanten van online services naar IT-bedrijven in de NAVO-landen, waarschijnlijk als tussenliggende toegangspunten. Over het geheel genomen ging 90 procent van de meldingen over Russische bedreigingsactiviteiten in dezelfde periode naar klanten in de NAVO-lidstaten, voornamelijk in de sectoren IT, denktanks en niet-gouvernementele organisaties (ngo's) en overheid, hetgeen een strategie suggereert om via meerdere middelen initiële toegang tot deze doelen te verkrijgen.

Er is een verschuiving gaande van het exploiteren van de supply chain voor software naar het exploiteren van de supply chain voor IT-services, waarbij de focus ligt op cloudoplossingen en beheerde serviceproviders om downstreamklanten te bereiken.



Dit diagram toont de aanpak met meerdere vectoren van NOBELIUM voor het uitvoeren van inbreuken op de uiteindelijke doelwitten en de bijkomende schade aan andere slachtoffers onderweg. Naast de hierboven getoonde acties lanceerde NOBELIUM wachtwoordspray- en phishing-aanvallen op de betrokken entiteiten, waarbij zelfs het persoonlijke account van ten minste één overheidsmedewerker als een potentiële route voor schending werd beschouwd.

De supply chain voor IT als gateway naar het digitale ecosysteem

Vervolg

Het hele jaar door ontdekte Microsoft Threat Intelligence Center (MSTIC) een toenemend aantal Iraanse staatshackers en aan Iran gelieerde actoren die IT-bedrijven in gevaar brachten. In veel gevallen werden actoren gedetecteerd bij het stelen van aanmeldingsreferenties om toegang te krijgen tot downstreamclients voor een reeks doelstellingen, van het verzamelen van inlichtingen tot het uitvoeren van destructieve aanvallen als vergeldingsmaatregelen.

- In juli en augustus 2021 heeft DEV-0228 een Israëlische zakelijke softwareleverancier gecompromitteerd om later te kunnen inbreken bij downstreamklanten in de Israëlische defensie-, energie- en juridische sector.[4]
- Van augustus tot september 2021 ontdekte Microsoft een piek in Iraanse staatsactoren die zich richtten op IT-bedrijven die waren gevestigd in India. Het ontbreken van dringende geopolitieke problemen die tot een dergelijke verschuiving zouden hebben geleid, suggereert dat deze aanval erop is gericht om indirecte toegang te verkrijgen tot dochterondernemingen en klanten buiten India.
- In januari 2022, voerde DEV-0198, een groep die naar ons oordeel is gelieerd aan de Iraanse overheid, een inbreuk uit bij een Israëlische leverancier van cloudoplossingen. Microsoft gaat ervan uit dat de actor waarschijnlijk gehackte referenties van de provider heeft gebruikt voor verificatie bij een Israëlisch logistiek bedrijf. MSTIC observeerde hoe dezelfde actor later die maand probeerde een destructieve cyberaanval uit te voeren op het logistieke bedrijf.
- In april 2022 brak POLONIUM, een in Libanon gevestigde groep die naar onze mening met Iraanse overheidsgroepen samenwerkten aan IT-supply chain-technieken, in bij een ander Israëlisch IT-bedrijf om toegang te krijgen tot Israëlische defensie- en juridische organisaties.[5]

Het afgelopen jaar aan activiteiten laat zien dat bedreigingsactoren zoals NOBELIUM en DEV-0228 het landschap van de vertrouwde relaties van een organisatie beter leren kennen dan de organisaties zelf. Deze toegenomen bedreiging benadrukt de noodzaak voor organisaties om de grenzen en toegangspunten van hun digitale domeinen te begrijpen en te versterken. Het onderstreept ook het belang voor IT-serviceproviders om hun eigen cyberbeveiligingsstatus nauwgezet te bewaken. Organisaties moeten bijvoorbeeld beleid voor meervoudige verificatie en voorwaardelijke toegang implementeren dat het voor kwaadwillenden moeilijker maakt om bevoegde accounts te schenden of zich over een netwerk te verspreiden.

Het uitvoeren van een grondige beoordeling en audit van partnerrelaties helpt onnodige machtigingen tussen je organisatie en upstreamproviders zoveel mogelijk te vermijden en de toegang voor relaties die er niet vertrouwd uitzien onmiddellijk te verwijderen. Door de bekendheid met activiteitenlogboeken te vergroten en beschikbare activiteiten te bekijken, kun je gemakkelijker afwijkingen detecteren die tot verder onderzoek zouden kunnen leiden.

> Door hun pijlen op derden te richten, kunnen actoren van vreemde mogelijkheden gevoelige organisaties aantasten door gebruik te maken van vertrouwen en toegang in een supply chain.

Direct bruikbare inzichten

1. Beoordeel en controleer de relaties van upstream- en downstreamserviceproviders en de toegangsrechten met gedelegeerde bevoegdheden om onnodige machtigingen tot een minimum te beperken. Verwijder de toegang voor partnerrelaties die er niet vertrouwd uitzien of die nog niet zijn gecontroleerd.[6]
2. Schakel logboekregistratie in en bekijk alle verificatieactiviteiten voor RAS-infrastructuur en virtuele particuliere netwerken (VPN's), met een focus op accounts die zijn geconfigureerd met enkelvoudige verificatie (single-factor authentication), om de verificatie te bevestigen en afwijkende activiteiten te onderzoeken.
3. Schakel MFA in voor alle accounts (met inbegrip van serviceaccounts) en zorg ervoor dat MFA wordt afgedwongen voor alle externe verbindingen.
4. Gebruik wachtwoordloze oplossingen om accounts te beveiligen.[7]

Links naar verdere informatie

- NOBELIUM viel gedelegeerde beheerdersbevoegdheden aan om bredere aanvallen mogelijk te maken | Microsoft Threat Intelligence Center (MSTIC)
- Iraanse aanvallen op IT-sector in opkomst | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Blootlegging van activiteiten en infrastructuur van POLONIUM die waren gericht tegen Israëlische organisaties | Microsoft Threat Intelligence Center (MSTIC)

Snelle exploitatie van kwetsbaarheden

Naarmate organisaties hun cyberbeveiliging versterken, reageren actoren van vreemde mogelijkheden door nieuwe en unieke tactieken te volgen om aanvallen uit te voeren en detectie te ontwijken. Het identificeren en misbruiken van voorheen onbekende kwetsbaarheden, ook wel zero-day kwetsbaarheden genoemd, vormt een belangrijke tactiek bij dit streven.

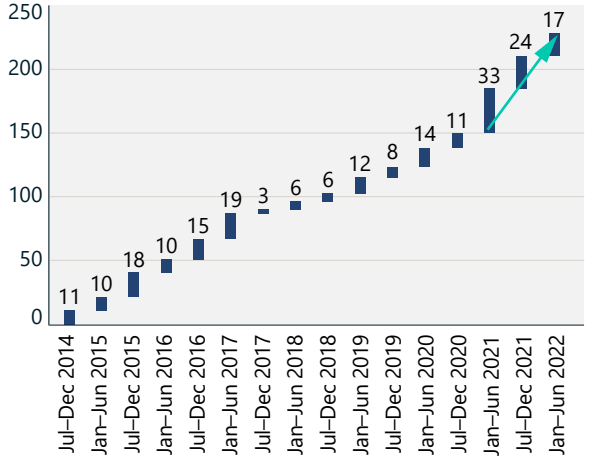
Zero-day kwetsbaarheden zijn een bijzonder effectief middel voor eerste misbruik en kunnen, wanneer ze eenmaal openbaar zijn gemaakt, snel worden hergebruikt door andere actoren van vreemde mogendheden en criminelen. Het aantal openbaar gemaakte zero-day kwetsbaarheden in het afgelopen jaar ligt op hetzelfde niveau als in het voorgaande jaar, het hoogste aantal ooit.

Naarmate cyberbedreigingsactoren, zowel actoren van vreemde mogendheden als criminelen, steeds bedrevener worden in het benutten van deze kwetsbaarheden, zien we een afname in de tijd tussen de aankondiging van een kwetsbaarheid en de commoditisering van die kwetsbaarheid. Daarom is het essentieel dat organisaties exploits onmiddellijk patchen. Evenzo is het van cruciaal belang dat organisaties of personen die nieuwe kwetsbaarheden blootleggen, deze op verantwoorde wijze zo snel mogelijk openbaar maken of rapporteren aan getroffen leveranciers, in overeenstemming met gecoördineerde openbaarmakingsprocedures voor kwetsbaarheden.

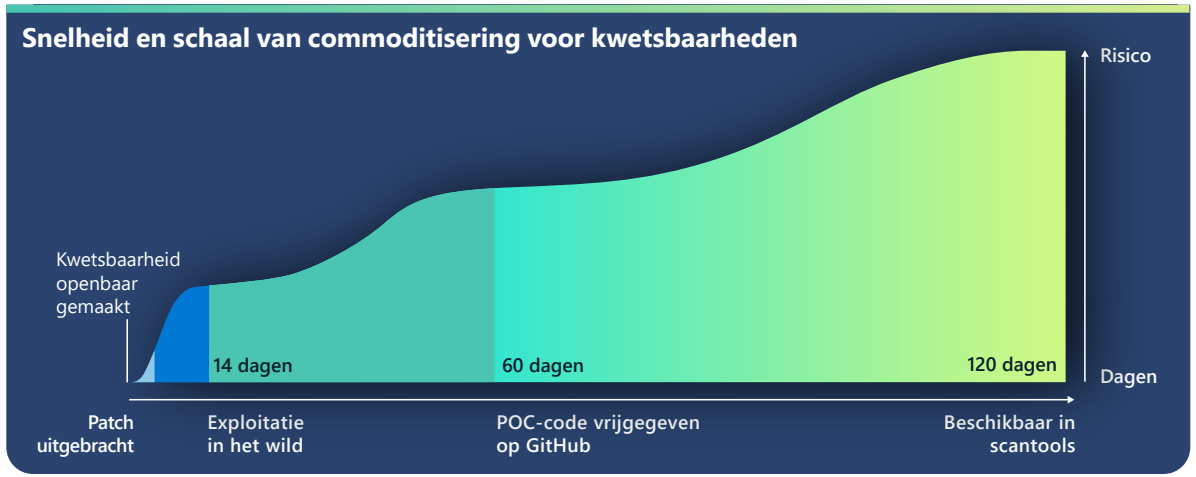
Dit zorgt ervoor dat kwetsbaarheden tijdig worden geïdentificeerd en dat patches worden ontwikkeld om klanten te beschermen tegen voorheen onbekende bedreigingen.

Veel organisaties gaan ervan uit dat ze minder vaak slachtoffer zullen zijn van zero-day aanvallen als kwetsbaarheidsbeheer een integraal onderdeel van hun netwerkbeveiliging vormt. De commoditisering van exploits leidt er echter toe dat deze in een veel hoger tempo plaatsvinden. Zero-day exploits worden vaak ontdekt door andere actoren en worden in een korte periode op grote schaal hergebruikt, waardoor niet-gepatchte systemen gevaar lopen. Hoewel zero-day exploitatie moeilijk kan worden gedetecteerd, zijn acties na de exploitatie van actoren vaak gemakkelijker te detecteren en kunnen ze, als ze afkomstig zijn van volledig gepatchte software, fungeren als een waarschuwing voor een inbreuk.

Patches vrijgegeven voor zero-day kwetsbaarheden



Aantallen openbaar gemaakte zero-day exploits uit de lijst met veelvoorkomende beveiligingslekken en openbaarmakingen (CVE's).



Gemiddeld duurt het slechts 14 dagen dat een exploit in het wild beschikbaar is nadat een kwetsbaarheid openbaar is gemaakt. Deze weergave biedt een analyse van de tijdlijnen voor exploitatie van zero-day kwetsbaarheden, samen met het aantal systemen dat kwetsbaar is voor de betreffende exploit en actief is op internet vanaf het moment van de eerste openbaarmaking.

Hoewel aanvallen via zero-day kwetsbaarheden in eerste instantie gericht zijn tegen een beperkt aantal organisaties, worden ze snel opgenomen in het grotere ecosysteem van bedreigingsactoren. Dit is de start van een race voor bedreigingsactoren om de kwetsbaarheid op zo groot mogelijke schaal te misbruiken voordat hun potentiële doelwitten patches installeren.

Hoewel we zien dat veel actoren van vreemde mogendheden exploits ontwikkelen op basis van onbekende kwetsbaarheden, zijn de bedreigingsactoren in China bijzonder bedreven in het ontdekken en ontwikkelen van zero-day exploits. De Chinese regelgeving voor het melden van kwetsbaarheden werd in september 2021 van kracht, waarmee een overheid als eerste ter wereld verplicht werd om kwetsbaarheden te melden bij een overheidsinstantie voordat de kwetsbaarheid werd gedeeld met de eigenaar van het product of de service. Deze nieuwe verordening kan elementen in de Chinese overheid in staat stellen om gemelde kwetsbaarheden op te slaan om ze als wapen te gebruiken. Het toegenomen gebruik van zero-days in het afgelopen jaar door in China gevestigde actoren weerspiegelt waarschijnlijk het eerste volledige jaar van de openbaarmakingsvereisten voor kwetsbaarheid in China voor de Chinese veiligheidsgemeenschap en vormt een belangrijke stap in het gebruik van zero-day exploits als staatsprioriteit. De hieronder beschreven kwetsbaarheden zijn voor het eerst ontwikkeld en geïmplementeerd door in China gevestigde nationale actoren bij aanvallen, voordat ze werden ontdekt door en verspreid onder andere actoren in het grotere bedreigingsecosysteem.

Snelle exploitatie van kwetsbaarheden

Vervolg

Zelfs organisaties die geen doelwit zijn van aanvallen door staatshackers hebben een beperkte periode om zero-day kwetsbaarheden in getroffen systemen te repareren voordat ze worden misbruikt door het bredere ecosysteem van actoren.

Deze voorbeelden van nieuw geïdentificeerde kwetsbaarheden tonen aan dat organisaties gemiddeld 60 dagen de tijd hebben vanaf het moment dat een kwetsbaarheid wordt gepatcht en POC-code (Proof Of Concept) online beschikbaar wordt gesteld, en vaak door andere actoren wordt opgepikt voor hergebruik. Op dezelfde manier hebben organisaties gemiddeld 120 dagen voordat een kwetsbaarheid beschikbaar is in geautomatiseerde kwetsbaarheidsscans en -exploitatietools zoals Metasploit, die vaak resulteren in het op grote schaal gebruiken van de exploit. Dit onderstreept dat zelfs organisaties die geen doelwit zijn van staatshackers een beperkte periode hebben om zero-day kwetsbaarheden in getroffen systemen te repareren voordat de kwetsbaarheden worden misbruikt door het bredere ecosysteem van actoren.

CVE-2021-35211 SolarWinds Serv-U

In juli 2021 publiceerde SolarWinds een beveiligingsadvies voor CVE-2021-35211, waarin de melding aan Microsoft werd toegeschreven.[8] Destijds ontdekten we dat staatshacker DEV-0322 op actieve wijze gebruikmaakte van de SolarWinds Serv-U-kwetsbaarheid. Ons RiskIQ-team nam tussen 15 juni en 9 juli 12.646 IP-adressen waar die met internet verbonden versies van de getroffen apparaten hosten.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

In september 2021 zagen onze onderzoekers aan China gelieerde actoren die Zoho ManageEngine misbruikten bij verschillende in de VS gevestigde entiteiten. Het beveiligingslek werd op 6 september openbaar gemaakt als CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, dat organisaties meestal gebruiken om wachtwoordresets uit te voeren.[9] DEV-0322 misbruikte het beveiligingslek later in september en gebruikte het als een aanvankelijke vector om voet aan de grond te krijgen in netwerken en aanvullende acties uit te voeren, zoals het dumpen van referenties, het installeren van aangepaste binaire bestanden en het verwijderen van malware om de aanwezigheid te handhaven. Op het moment van publicatie heeft RiskIQ 4.011 exemplaren van deze systemen waargenomen die actief zijn en zich op internet bevinden.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Eind oktober 2021 zagen we dat DEV-0322 gebruikmaakte van een kwetsbaarheid (CVE-2021-44077) in een tweede Zoho ManageEngine-product, ServiceDesk Plus. Dit is IT-helpdesksoftware met asset management. DEV-0322 gebruikte deze kwetsbaarheid om entiteiten in de sector voor gezondheidszorg, informatietechnologie, hoger onderwijs en essentiële productie aan te vallen. Op 2 december hebben de Federal Bureau of Investigation (FBI) en de Cyber Security and Infrastructure Security Agency (CISA) een gezamenlijke waarschuwing aan het publiek verstrekt over bedreigingen door actoren van vreemde mogendheden die gebruikmaken van deze kwetsbaarheid. Op het moment van publicatie heeft RiskIQ 7.956 exemplaren van deze systemen waargenomen die actief zijn en zich op internet bevinden.

CVE-2021-42321 Microsoft Exchange

Een zero-day exploit voor een Exchange-kwetsbaarheid CVE-2021-42321 werd onthuld tijdens de Tianfu Cup, een internationale cyberbeveiligingsconferentie en hackingcompetitie die op 16 en 17 oktober 2021 werd gehouden in het Chinese Chengdu. Beveiligingsonderzoekers van Microsoft zagen dat de exploit voor de Exchange-kwetsbaarheid in het wild werd gebruikt op 21 oktober, slechts drie dagen nadat de kwetsbaarheid was bekendgemaakt. Op het moment van publicatie heeft RiskIQ 61.559 exemplaren van deze systemen waargenomen die actief zijn en zich op internet bevinden. We bleven tot in november 2021 misbruikactiviteiten waarnemen.

CVE-2022-26134 Confluence

Een aan China gelieerde actor beschikte waarschijnlijk over de zero-day exploit-code voor de Confluence-kwetsbaarheid (CVE-2022-26134) vier dagen voordat de kwetsbaarheid op 2 juni openbaar werd gemaakt en heeft deze waarschijnlijk ingezet tegen een in de VS gevestigde entiteit. Op het moment van publicatie heeft RiskIQ 53.621 exemplaren van kwetsbare Confluence-systemen waargenomen op internet.

Kwetsbaarheden worden op grote schaal en in steeds kortere tijdsbestekken opgepakt en benut.

Direct bruikbare inzichten

1. Geef prioriteit aan patching van zero-day kwetsbaarheden zodra deze worden vrijgegeven; wacht niet op implementatie van de patchbeheercyclus.
2. Documenteer en inventariseer alle ondernemingshardware en -software om risico's te bepalen en snel na te gaan wanneer op patches moet worden gereageerd.

De cybertactieken in oorlogstijd van Russische overheidsactoren bedreigen Oekraïne en andere landen

Dit jaar lanceerden Russische staatshackers cyberactiviteiten als aanvulling op militaire acties tijdens de invasie van Rusland in Oekraïne, vaak met behulp van dezelfde tactieken en technieken die worden ingezet tegen doelen buiten Oekraïne. Het is van cruciaal belang dat organisaties over de hele wereld maatregelen nemen om de cyberbeveiliging te versterken tegen digitale dreigingen die afkomstig zijn van aan Rusland gelieerde bedreigingsactoren.

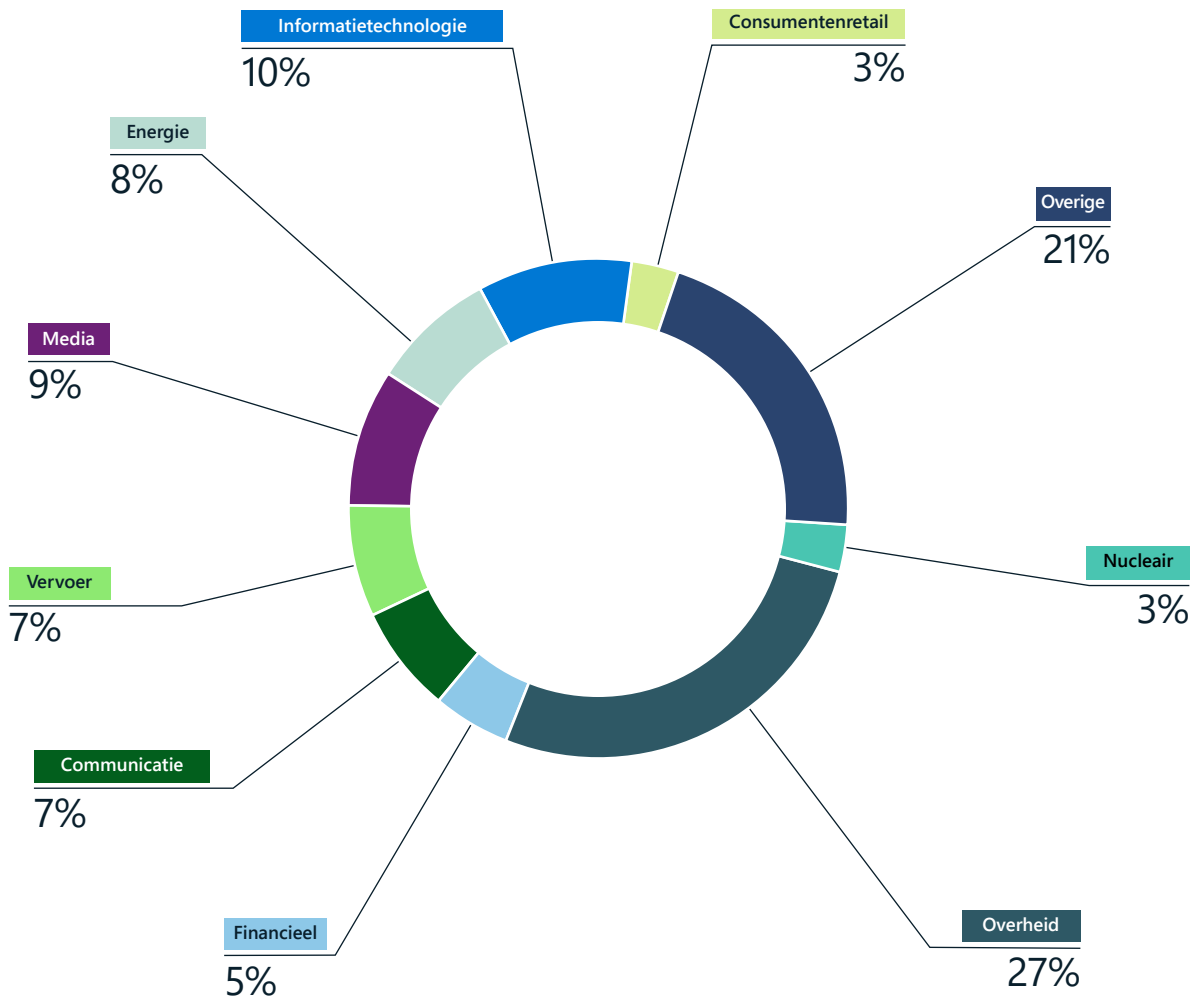
De situatie in het veld blijft fluctueren naarmate het militaire conflict voortduurt, en Oekraïne en zijn bondgenoten moeten bereid zijn zich te verdedigen als de aan de Russische staat gelieerde hackers de frequentie of intensiteit van inbreuken opvoeren in overeenstemming met militaire doelstellingen. Tijdens de eerste vier maanden van de oorlog merkte Microsoft dat bedreigingsactoren die aan het Russische leger waren gelieerd meerdere golven van destructieve cyberaanvallen lanceerden tegen bijna 50 verschillende instanties en ondernemingen in Oekraïne en op spionage gerichte inbreuken uitvoerden tegen vele anderen. Als de activiteiten tegen klanten van online services niet worden meegeteld, was tussen eind februari en juni 64 procent van de Russische bedreigingsactiviteiten gericht tegen bekende doelen bij in Oekraïne gevestigde organisaties.

Bij elke operatie gebruikten Russische bedreigingsactoren veel van de tactieken, technieken en procedures (TTP's) die we vóór de invasie zagen tegen doelen binnen en buiten Oekraïne. Deze actoren waren van plan om data te vernietigen en de overheidsinstellingen van Oekraïne in de beginperiode van het conflict uit evenwicht te brengen. Ze hebben sindsdien geprobeerd het transport van militaire en humanitaire hulp naar Oekraïne te doen ontsporen, de openbare toegang tot services en media te verstoren en inlichtingen op de langere termijn of informatie die van economische waarde is voor Rusland te stelen.

De aanval op het transport bedreigt een gebied dat van cruciaal belang is voor de burgers van Oekraïne die proberen het conflict te overleven. Volgens een door UNICEF gesponsord onderzoek in mei waren respondenten in door conflicten getroffen stedelijke gebieden het meest bezorgd over transport en brandstof, onderbrekingen van leveringen, veiligheid en beperkte toegang tot voedsel, medische diensten en financiële diensten.[10] In juni zei de VN-crisiscoördinator voor Oekraïne dat ten minste 15,7 miljoen mensen in Oekraïne dringend humanitaire hulp nodig hadden en dat dit aantal zou toenemen naarmate de oorlog voortduurt.[11]

Buiten Oekraïne ontdekte Microsoft tussen eind februari en juni Russische pogingen tot netwerkinbreuken bij 128 netwerken in 42 landen. De Verenigde Staten vormden het belangrijkste doelwit van Rusland. Ook Polen, dat als doorvoerland voor een groot deel van de internationale militaire en humanitaire hulp aan Oekraïne geldt, vormde een belangrijk doelwit tijdens deze periode. Bedreigingsactoren die zijn gelieerd aan de Russische staat hebben in april en mei ook organisaties in de Baltische landen en computernetwerken in Denemarken, Noorwegen, Finland en Zweden aangevallen.

Meest aangevallen industrietakken in Oekraïne sinds de invasie



Federale, provinciale en lokale overheidsorganisaties in Oekraïne zijn gedurende het hele conflict prioriteitsdoelen gebleven voor Russische staatshackers en aan Rusland gelieerde bedreigingsgroepen. De focus op organisaties in de transportsector, de energiesector, de financiële sector en de mediasector benadrukt het risico dat deze cyberactiviteiten vormen voor diensten waarvan de burgers van Oekraïne afhankelijk zijn.

De cybertactieken in oorlogstijd van Russische overheidsactoren bedreigen Oekraïne en andere landen

Vervolg

We hebben een toename gezien in soortgelijke activiteiten die waren gericht tegen de ministeries van Buitenlandse Zaken van NAVO-landen.

Russische staatshackersgroepen bleven het afgelopen jaar geïnteresseerd in het compromitteren van essentiële infrastructuur binnen en buiten Oekraïne. IRIDIUM implementeerde de Industroyer2-malware in een mislukte poging om miljoenen mensen in Oekraïne zonder stroom achter te laten. Buiten Oekraïne voerde BROMINE begin 2022 inbreuken uit tegen organisaties die betrokken zijn bij productie en industriële controlesystemen.

Russische staathackers en aan de staat gelieerde actoren hebben dit jaar veel cyberactiviteiten uitgevoerd tegen Oekraïne, zijn bondgenoten en andere inlichtingendoelwitten, waarbij veel van de volgende TTP's werden gebruikt:

Spearphishing met schadelijke bijlagen of links

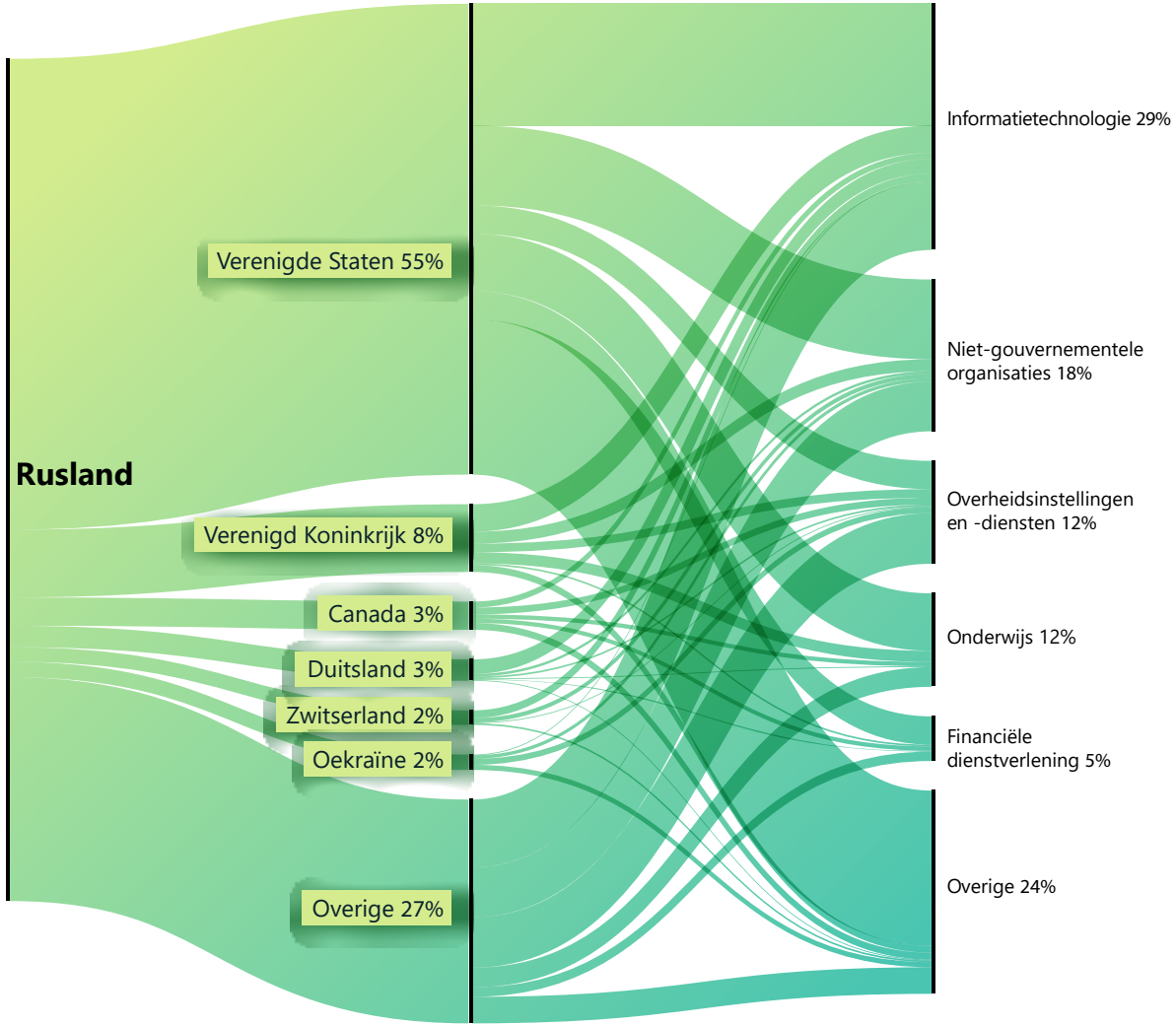
Russische staatshackers en aan Rusland gelieerde groepen zoals ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM en IRIDIUM gebruikten allemaal phishingcampagnes om in eerste instantie toegang te krijgen tot de gewenste accounts en netwerken in organisaties binnen en buiten Oekraïne. Veel campagnes maakten gebruik van gehackte of vervalste accounts bij aangevallen organisaties of binnen dezelfde bedrijfstak en van aansprekende thema's om slachtoffers te lokken. NOBELIUM gebruikte gehackte diplomatieke accounts om phishing-berichten te verzenden, vermomd als diplomatieke communicatie naar medewerkers van ministeries van Buitenlandse Zaken over de hele wereld. STRONTIUM maakte vervalste accounts op basis van openbaar beschikbare namen van accounthouders bij denktanks in de Verenigde Staten en verstuurde phishing-berichten om toegang te krijgen tot accounts bij deze denktanks. SEABORGIUM gebruikte phishing met behulp van lokmiddelen in verband met rapportage over het conflict in Oekraïne om in eerste instantie toegang te krijgen tot accounts bij denktanks voor internationale zaken in de Scandinavische landen.

Misbruik van de supply chain van IT-services om downstreamklanten te beïnvloeden

Eind 2021 maakten Russische staatshackers gebruik van IT-serviceproviders en gebruikten ze de toegang om verstoringen van websites en de implementatie van Whispergate-destructieve malware door DEV-0586 in januari te vergemakkelijken.[12] DEV-0586 tastte ook het netwerk van een IT-bedrijf aan dat resourcebeheersystemen heeft gebouwd voor het ministerie van Defensie van Oekraïne en andere organisaties in de communicatie- en transportsector, wat aangeeft dat de groep ook in die sectoren opties voor aanvallen op derden onderzocht.

Wereldwijd, maar vooral in de Verenigde Staten en West-Europa, richtte NOBELIUM zijn pijlen op IT-serviceproviders om toegang te verkrijgen tot overheids- en andere gevoelige netwerken in de hele periode 2021-2022 (zie de bespreking van kwetsbaarheden in de supply chain eerder in dit hoofdstuk).

Rusland: belangrijkste aangevallen landen en industriesectoren



Ondanks een versterkte focus op organisaties in Oekraïne sinds het begin van 2022, golden ondernemingen in Noord-Amerika en West-Europa nog steeds als meestgekozen doelwit voor Russische actoren. Vanwege de campagne van NOBELIUM tegen de IT-sector was dit het afgelopen jaar de sector die het vaakst als doelwit werd gekozen.

De cybertactieken in oorlogstijd van Russische overheidsactoren bedreigen Oekraïne en andere landen

Vervolg

Misbruik van openbare applicaties om initiële toegang tot netwerken te krijgen

Sinds minstens eind 2021 heeft STRONTIUM gewerkt aan het ontwikkelen en verfijnen van de mogelijkheden om openbare services te misbruiken, zoals Microsoft Exchange-servers, voor het stelen van informatie. STRONTIUM maakte gebruik van niet-gepatchte Exchange-servers om toegang te krijgen tot overheidsaccounts van de Oekraïense overheid, evenals militaire instanties en aan de defensie-industrie gelieerde organisaties in de Verenigde Staten, Libanon, Peru en Roemenië en andere overheidsinstellingen in Armenië, Bosnië, Kosovo en Maleisië. DEV-0586, dat eveneens aan het Russische leger is gelieerd, misbruikte Confluence-serverkwetsbaarheden om in eerste instantie toegang te krijgen tot overheids- en IT-sectororganisaties in Oekraïne en andere Oost-Europese landen.

Russische staatshackers en aan Rusland gelieerde hackers veel van dezelfde TTP's om organisaties waarin zij zijn geïnteresseerd te schenden in tijden van oorlog en vrede.

Gebruik van beheerdersaccounts en -protocollen en native hulpprogramma's voor netwerkdetectie en laterale verplaatsing

Microsoft merkte op dat, nadat Russische staatshackers voor het eerst toegang tot een netwerk hadden verkregen, zij gebruikmaakten van legitieme accounts en softwarehulpprogramma's voor het uitvoeren van elementaire onderhoudstaken om detectie zo lang mogelijk te vermijden. Zij vertrouwden op gehackte identiteiten met beheermogelijkheden en geldige beheerprotocollen, tools en methoden om zich zijdelings binnen netwerken te verplaatsen zonder onmiddellijk de aandacht van geautomatiseerde monitoren en netwerkverdedigers te trekken.

Elementaire cyberhygiëne en inzet van tools voor endpointdetectie en -respons kunnen helpen de negatieve impact van dit type activiteiten in vredestijd en in tijden van oorlog te beperken.

De onvoorspelbaarheid van het voortdurende conflict vereist dat organisaties over de hele wereld maatregelen treffen om de cyberbeveiliging te versterken tegen digitale bedreigingen die afkomstig zijn van Russische staatshackers en aan Rusland gelieerde bedreigingsactoren.

Direct bruikbare inzichten

1. Beperk diefstal van referenties en accountmisbruik door de identiteiten van je gebruikers te beschermen door MFA-tools voor identiteitsbescherming te implementeren en toegangsrechten met de minst mogelijke bevoegdheden af te dwingen om de meest gevoelige en bevoegde accounts en systemen te beveiligen.
2. Pas updates toe om ervoor te zorgen dat al je systemen zo snel mogelijk het hoogste beveiligingsniveau krijgen en up-to-date worden gehouden.
3. Implementeer oplossingen voor antimalware, endpointdetectie en identiteitsbescherming in je hele organisatie. Een combinatie van diepgaande beveiligingsoplossingen, in combinatie met getraind en bekwaam personeel, kan je organisatie in staat stellen om inbraken die tegen je bedrijf zijn gericht te identificeren, te detecteren en te voorkomen.
4. Maak onderzoeken en herstelactiviteiten mogelijk voor het geval je een bedreiging voor je omgeving detecteert of ontvangt door een back-up te maken van essentiële systemen en logboekregistratie in te schakelen. Het opstellen van een incidentresponsplan wordt sterk aangemoedigd.

Links naar verdere informatie

- De bescherming van Oekraïne: eerste lessen uit de cyberoorlog | Microsoft On the Issues
- De hybride oorlog in Oekraïne | Microsoft On the Issues
- Cyberbedreigingsactiviteit in Oekraïne: analyse en informatiebronnen | Microsoft Security Response Center (MSRC)
- Verstorende cyberaanvallen gericht op Oekraïne | Microsoft On the Issues
- Malware-aanvallen gericht op de overheid van Oekraïne | Microsoft On the Issues
- MagicWeb: de truc van NOBELIUM na het hacken voor verificatie als willekeurige gebruiker | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

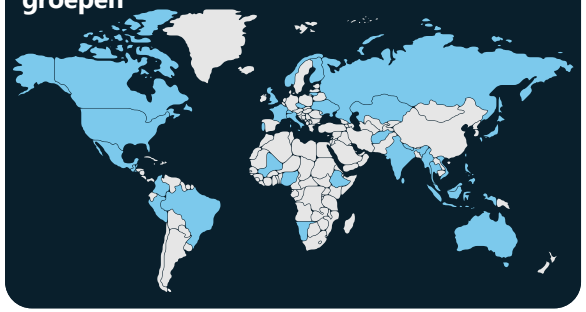
China breidt wereldwijde targeting uit voor concurrentievoordeel

In het huidige complexe geopolitieke klimaat proberen Chinese staatshackers en aan China gelieerde bedreigingsactoren cyberactiviteiten uit te voeren die vaak zijn bedoeld om de strategische militaire, economische en aan buitenlandse relaties gerelateerde doelen van het land te bevorderen als onderdeel van de doelstelling van China om een concurrentievoordeel te verwerven. In het afgelopen jaar heeft Microsoft een groot aantal Chinese bedreigingsactiviteiten gezien die gericht zijn op landen over de hele wereld.

Sinds medio 2021 probeert China de economische en financiële stabiliteit te waarborgen te midden van de ergste COVID-19-piek in twee jaar.[13] China bleef pogingen ondernemen om zijn standpunt met betrekking tot geopolitieke gebeurtenissen, zoals de strijd om hun "onbeperkte" partnerschap met Rusland in evenwicht te houden,[14] en de eigen positie op het wereldtoneel te handhaven.[15] Daarnaast bleef het standpunt van China ten opzichte van de Verenigde Staten en zijn bondgenoten ten aanzien van Taiwan[16] en de Zuid-Chinese Zee de buitenlandse betrekkingen met veel landen onder druk zetten.[17]

Chinese staatshackers en aan China gelieerde bedreigingsgroepen versterkten hun aanvallen op kleinere landen over de hele wereld met een focus op Zuidoost-Azië om op alle fronten concurrentievoordeel te behalen.

Landen die het doelwit zijn van Chinese staatshackers en aan de staat gelieerde groepen

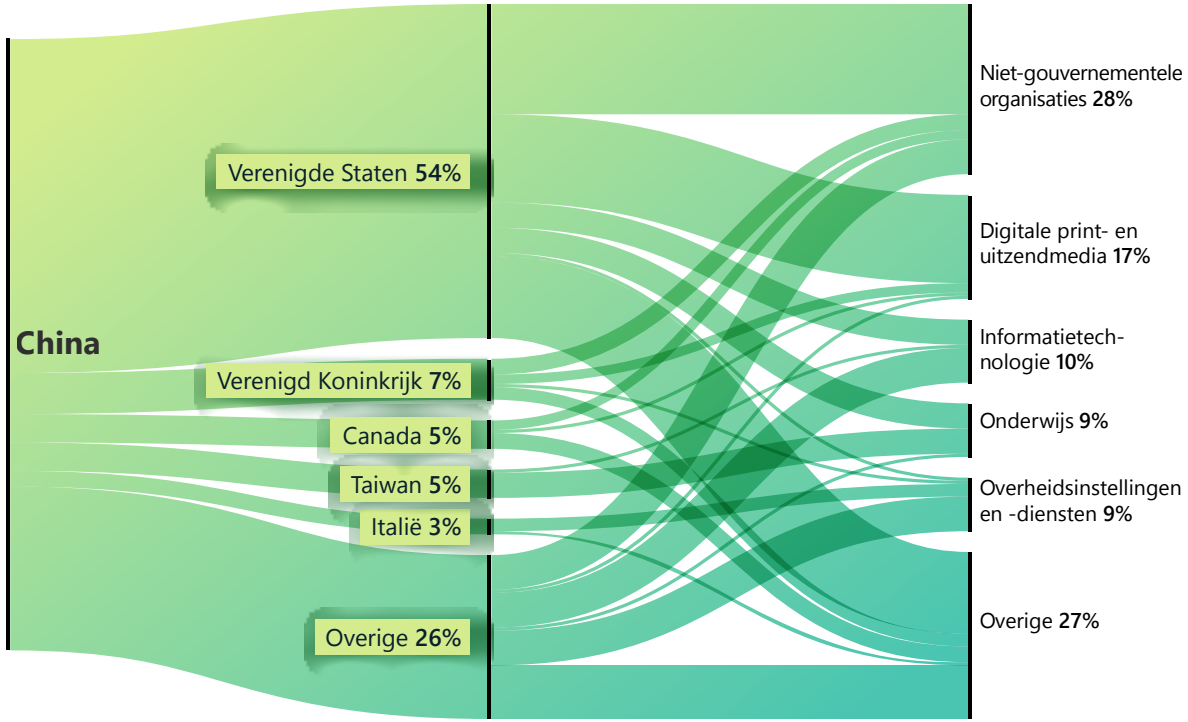


China is ook doorgegaan met het uitbreiden van zijn economische invloed wereldwijd via eerder opgerichte Belt and Road-initiatieven (BRI), in een poging om een uitgebreid investeringskader met de EU nieuw leven in te blazen,[18] en het onderhandelen over een nieuwe regionale handelsovereenkomst met 15 landen in Azië-Pacific, ook wel bekend als het Regional Comprehensive Economic Partnership.[19] Microsoft is van mening dat China cyberverzameling zal blijven gebruiken als instrument om zijn strategische politieke, militaire en economische doelen te helpen verbeteren vanwege de waargenomen cyberactiviteiten en de veelheid aan aangevallen entiteiten.

Cybertargeting die waarschijnlijk economische en militaire belangen zal bevorderen.

Microsoft constateerde wijdverbreide aanvallen op kleinere landen over de hele wereld door Chinese staatshackers en aan China gelieerde bedreigingsactoren, wat suggereert dat China waarschijnlijk cyberspionage gebruikt als onderdeel van zijn wereldwijde economische en militaire invloed.

China: belangrijkste aangevallen landen en industriesectoren



Denktanks/ngo's, media, IT, overheid en onderwijssector behoorden tot de meest gerichte sectoren voor in China gevestigde bedreigingsgroepen, waarschijnlijk voor het permanent verzamelen van inlichtingen en het uitvoeren van verkenningen.

De doelwitten omvatten onder andere, maar niet uitsluitend, landen in Afrika, het Caribisch gebied, het Midden-Oosten, Oceanië en Zuid-Azië, met een specifieke focus op de landen in Zuidoost-Azië en de Pacifische eilanden.

In lijn met de BRI-strategie van China richtten in China gevestigde dreigingsgroepen zich op entiteiten in Afghanistan, Kazachstan, Mauritius, Namibië en Trinidad en Tobago.[20] Trinidad en Tobago was bijvoorbeeld het eerste Caribische land dat de BRI-strategie van China in 2018 onderschreef en China beschouwt het als een belangrijke partner in de regio. NICKEL heeft sinds 2021 persistente netwerkactiviteiten gericht op Trinidad en Tobago. Zo heeft NICKEL in maart 2022 verkenningsactiviteiten uitgevoerd bij een overheidsinstelling, waarschijnlijk voor het verzamelen van inlichtingen.

China breidt wereldwijde targeting uit voor concurrentievoordeel

Vervolg

Ondertussen constateerde Microsoft dat Chinese staatshackers en aan de staat gelieerde bedreigingsgroepen hun netwerkactiviteiten richtten op entiteiten in Zuidoost-Azië en zich uitbreidden naar landen in de Stille Zuidzee terwijl China zijn militaire en economische prioriteiten verlegde om de uitdagingen van de hernieuwde belangstelling van de Verenigde Staten voor de regio het hoofd te bieden. In januari 2022 merkte Microsoft op dat RADIUM een energiebedrijf en een aan energie gerelateerde overheidsinstelling in Vietnam aanviel, evenals een Indonesische overheidsinstelling. De activiteiten van RADIUM kwamen waarschijnlijk overeen met de strategische doelen van China in de Zuid-Chinese Zee.[21] Eind februari en begin maart heeft GALLIUM meer dan 100 accounts gehackt die zijn gelieerd aan een prominente intergouvernementele organisatie (IGO) in de regio Zuidoost-Azië. De timing van de aanval van GALLIUM op de IGO in de regio viel samen met de aankondiging van een geplande vergadering tussen de Amerikaanse en regionale leiders. GALLIUM-actoren werden waarschijnlijk belast met het bewaken van de communicatie en het verzamelen van informatie vóór het evenement.

Naarmate China zijn invloed op eilanden in de Stille Zuidzee verder uitbreidde, namen ook de activiteiten van Chinese bedreigingsgroepen toe. In april ondertekenden China en de Salomonseilanden een veiligheidsovereenkomst die was bedoeld om "vrede en veiligheid te bevorderen". Dankzij de overeenkomst kan China gewapende politie en militairen inzetten op de Salomonseilanden.[22] In mei organiseerde China de tweede bijeenkomst van ministers van Buitenlandse Zaken tussen China en de Stille Zuidzee-eilanden (FIC) en stelde voor om een "alomvattend strategisch partnerschap" in te richten om politieke, culturele, sociale, veiligheids- en klimaatbelangen te bevorderen en ook om de pandemie te bestrijden.[23] Rond dezelfde tijd in mei identificeerde Microsoft de malware van GADOLINIUM op de overheidssystemen van de Salomonseilanden. RADIUM heeft ook schadelijke code uitgevoerd op systemen van een telecommunicatiebedrijf in Papoea-Nieuw-Guinea. Wij beoordelen dat deze activiteiten waarschijnlijk werden gebruikt voor het verzamelen van inlichtingen ter ondersteuning van de algemene regionale strategie van China.

Microsoft verstoort de activiteiten van NICKEL, maar de bedreigingsgroep toont zich hardnekkig.

In december 2021 diende de Microsoft Digital Crimes Unit (DCU) verzoekschriften in bij de Amerikaanse rechtbank voor het Oostelijk District van Virginia, op zoek naar bevoegdheid voor het in beslag nemen van 42 CS-domeinen (command and control) die onder controle van NICKEL stonden. Deze C2-domeinen werden sinds september 2019 gebruikt in activiteiten tegen overheden, diplomatieke entiteiten en ngo's in Midden- en Zuid-Amerika, het Caribisch gebied, Europa en Noord-Amerika.[24] Door deze activiteiten heeft NICKEL langdurige toegang verkregen tot verschillende entiteiten en sinds eind 2019 op consistente wijze data van sommige slachtoffers geëxfiltreerd.

Naarmate China met steeds meer landen economische relaties aangaat, vaak in overeenkomsten die verband houden met BRI, zal de wereldwijde invloed van China blijven groeien. Naar onze mening zullen Chinese staatshackers en aan de staat gelieerde bedreigingsactoren doelen nastreven in hun overheids-, diplomatieke en ngo-sectoren om nieuwe inzichten te verkrijgen, waarschijnlijk om economische spionage uit te voeren of traditionele doelstellingen voor het verzamelen van inlichtingen te realiseren. Sinds de verstoring door Microsoft heeft NICKEL zich op verschillende overheidsinstanties gericht, waarschijnlijk om de verloren toegang terug te krijgen. Tussen eind maart en mei 2022 heeft NICKEL opnieuw toegang verkregen tot ten minste vijf overheidsinstanties over de hele wereld. Dit suggereert dat de groep extra toegangspunten tot die entiteiten had of opnieuw toegang kreeg via nieuwe C2-domeinen. De volharding van NICKEL bij het uitvoeren van inbraken bij dezelfde overheidsinstanties wereldwijd wijst op het belang van de taak op een hoog niveau.

China hanteert een assertievere houding met betrekking tot het buitenlandse beleid. We schatten dat economische cyberspionage en het verzamelen van inlichtingenwaarschijnlijk zal doorgaan.

Direct bruikbare inzichten

1. Geef cyberverdediging een boost om cyberdreigingen proactief te beperken. De voortdurende aanwezigheid van Chinese bedreigingsactoren vereist dat organisaties op tijdige wijze mogelijke inbraken identificeren, beschermen, detecteren en hierop reageren.
2. Bedreigingsactoren misbruiken geplande taken[25] als een veelgebruikte methode voor persistentie en om verdedigingen te omzeilen. Zorg ervoor dat je omgeving aanvullende beveiligingsrichtlijnen gebruikt om je tegen deze veelgebruikte techniek te beschermen.[26]
3. We blijven het gebruik van webshells als een eerste vector in aangevallen netwerken observeren.[27] Organisaties zouden hun systemen moeten beschermen tegen aanvallen via webshells, waarmee aanvallers toegang kunnen krijgen om externe opdrachten uit te voeren.[28]

Links naar verdere informatie

- NICKEL richt zich op overheidsorganisaties in Latijns-Amerika en Europa | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Mensen beschermen tegen recente cyberaanvallen | Microsoft On the Issues

Iran wordt steeds agressiever na machtsoverdracht

Microsoft heeft geconstateerd dat Iraanse staatshackers en gelieerde actoren het tempo en de reikwijdte van cyberaanvallen op Israël verhogen, ransomwareaanvallen uitbreiden tot buiten de regionale tegenstanders naar slachtoffers in de VS en EU, en zich richten op prominente Amerikaanse essentiële infrastructuur om ten minste een beginpositie te verwerven voor potentiële destructieve cyberaanvallen.

De groeiende cyberagressie van Iraanse staatshackers heeft geleid tot een overdracht van de presidentiële macht. In de zomer van 2021 verving hardline-president Ibrahim Raisi de gematigde president Hassan Rouhani. In schril contrast met Raisi, die een beschermeling is van de Opperste Leider en een nauwe bondgenoot van de IRGC (Islamitisch Revolutionaire Garde), stond voormalig president Rouhani vaak op gespannen voet met de Opperste Leider en hogere leiders van de IRGC vanwege zijn voorliefde voor diplomatie.[29] De oorlogszuchtige opvattingen van de Raisi-regering lijken de bereidheid van de Iraanse actoren te hebben vergroot om krachtigere acties te ondernemen tegen Israël en het Westen, met name de Verenigde Staten, ondanks de hervatting van de diplomatieke contacten om de atoomovereenkomst met Iran nieuw leven in te blazen.

Toegenomen tempo en omvang van Iraanse cyberaanvallen tegen Israël

Binnen enkele weken nadat Raisi de formatie van zijn team voor buitenlands beleid had voltooid,[30] hervatten Iraanse staatshackers de verwoestende cyberaanvallen tegen Israël in een sneller tempo dan het jaar ervoor. Deze ransomware- en hack-en-lekaanvallen werden vanaf september om de paar weken uitgevoerd door ten minste drie aan Iran gelieerde actoren, wat suggereert dat de aanvallen mogelijk deel uitmaakten van een landelijke vergeldingscampagne tegen Israël. In ten minste één geval beoordeelde Microsoft dat een ransomwareaanval eind 2021 op een Israëlische organisatie bedoeld was om een onderliggende aanval voor het verwijderen van data te verbergen. Tijdens de malwareanalyse van Microsoft werd vastgesteld dat de ransomware die aan het slachtoffer werd geleverd, was geprogrammeerd om na versleuteling vernietigingsmalware uit te voeren.

Tegen 2022 escaleerden de Iraanse cyberaanvallen wat de selectie van doelen en de vorm van aanvallen betrof. In februari probeerde DEV-0198 een destructieve aanval uit te voeren op essentiële Israëlische infrastructuur. Microsoft beoordeelde tevens dat een aan Iran gelieerde actor hoogstwaarschijnlijk verantwoordelijk was voor een geavanceerde cyberaanval die in juni noodraketsirenes in Israël deed afgaan, waarschijnlijk met behulp van software die audio regelt via IP-netwerken.

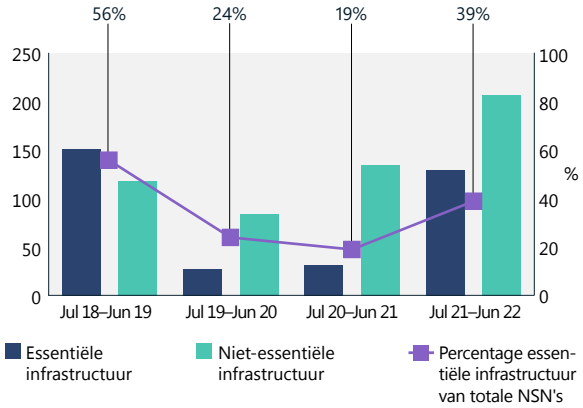
Iraanse bedreiging van essentiële infrastructuur in de VS en Israël nam het hele jaar door toe

Naar mening van Microsoft voerden aan de IRGC (PHOSPHORUS en DEV-0198) gelieerde actoren van eind 2021 tot medio 2022 aanvallen uit op prominente Amerikaanse en Israëlische essentiële infrastructuur. Het waarschijnlijke doel was om Teheran opties te bieden voor vergeldingsmaatregelen tegen dezelfde sectoren die volgens hoge IRGC-ambtenaren door de Verenigde Staten en Israël werden ontwricht in Iran.[31] Naar onze mening is deze activiteit gekoppeld aan uitspraken van eind oktober 2021 door IRGC-generaal Gholamreza Jalali, hoofd van de Iraanse Passive Defense Organisation, die beweringen van andere invloedrijke personen binnen het regime herhaalde dat de Verenigde Staten en Israël cyberaanvallen hadden uitgevoerd op havens, spoorwegen en tankstations van Iran.[32] Jalali uitte deze beschuldiging een tweede keer in voorbereide opmerkingen tijdens een geënsceneerde gebedsrede op een podium met een afbeelding van een inslaand projectiel op de tekst "VS", wat suggereert dat zijn superieuren dezelfde opvatting deelden.[33]

PHOSPHORUS begon in oktober 2021 met het scannen van Amerikaanse organisaties op niet-gepatchte Fortinet- en ProxyShell-kwetsbaarheden. Na te zijn aangetast, werden deze ongepatchte systemen gebruikt om ransomwareaanvallen uit te voeren, in verschillende gevallen op essentiële infrastructuur in de Verenigde Staten en andere westerse landen. Deze markeerden de eerste bevestigde gevallen van door Iraanse staatshackers uitgevoerde ransomwareaanvallen buiten het Midden-Oosten. Na de cyberaanval tegen de tankstations in Iran eind oktober, zag Microsoft een piek in Iraanse ransomwareaanvallen op Amerikaanse bedrijven, wat een mogelijke correlatie suggereerde.

Tegelijkertijd richtte PHOSPHORUS zich op gerichte targeting, vaak via spearphishing, van prominente Amerikaanse essentiële infrastructuurbedrijven, waaronder grote zee- en luchthavens, transportsystemen, nutsbedrijven en olie- en gasmaatschappijen. Deze targeting, die vaak werd uitgevoerd via spearphishing, duurde tot medio 2022. De doelen zijn direct in lijn met de sectoren in Iran die volgens Teheran door de Verenigde Staten en Israël werden aangevallen en boden Iran waarschijnlijk opties voor vergelding. Het schenden van bijna identieke doelen zou een afschrikkende werking kunnen hebben voor mogelijke toekomstige aanvallen, terwijl werd geprobeerd om escalatie te voorkomen door de oorzaak van aanvallen aan te geven zonder schuld te bekennen.

Heropleving van Iraanse infrastructuurtargeting



De Iraanse targeting van essentiële infrastructuur is toegenomen tot het hoogste niveau sinds de periode van eind 2018 tot begin 2019. We hebben de Amerikaanse presidentiële beleidsrichtlijn 21 (PPD-21) gebruikt om te bepalen of een bedrijf voldoet aan de criteria voor essentiële infrastructuur. (Juli 2021 - juni 2022).

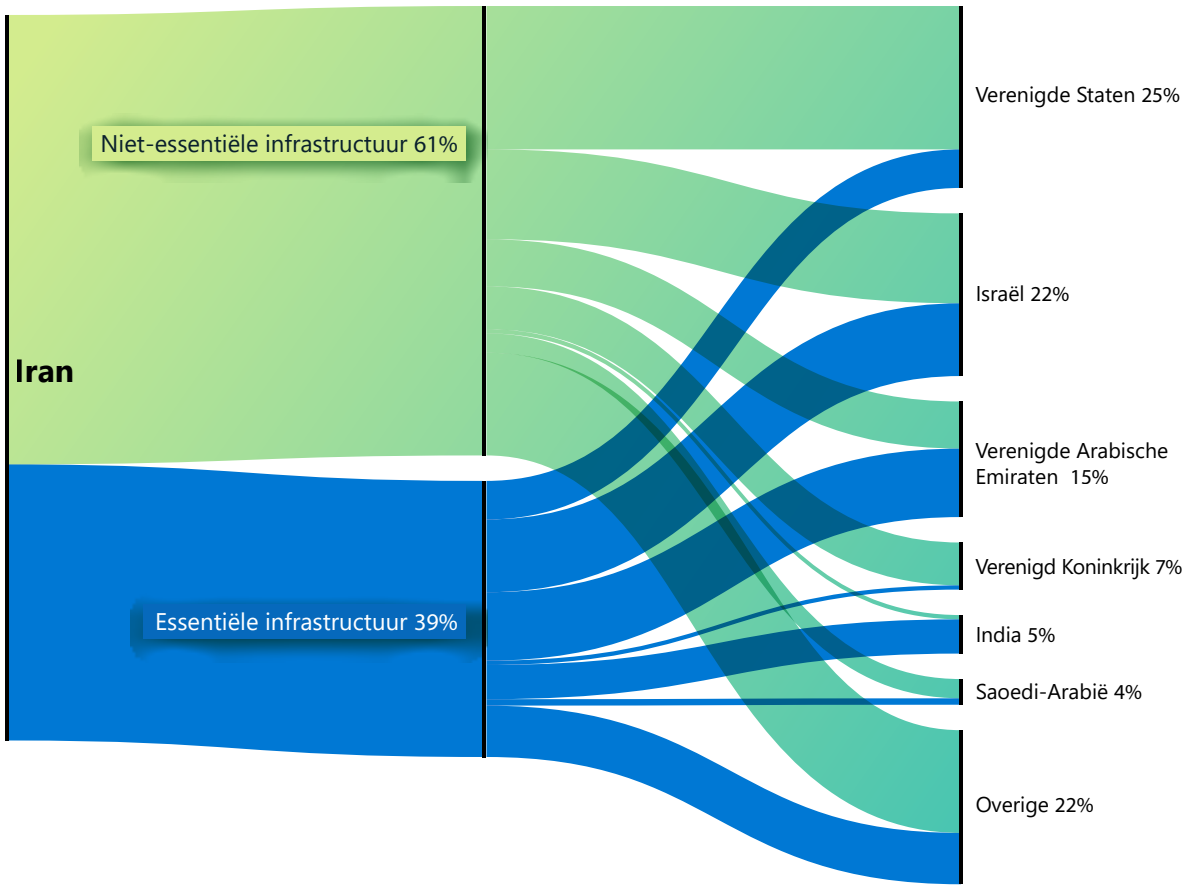
Iran wordt steeds agressiever na machtsoverdracht

Vervolg

In Israël richtte DEV-0198 zijn pijlen op Israëlische spoorwegen, logistieke bedrijven, softwareleveranciers van logistieke bedrijven en brandstofbedrijven met een focus op tankstations. In het begin van 2022 voerde de groep een ontwrichtende aanval uit op het netwerk van een groot Israëlisch logistiek bedrijf, waardoor het bedrijf zijn computers en een deel van zijn activiteiten moest afsluiten om de aanval in te dammen. In een ander geval zagen we een poging van de groep om toegang te krijgen tot het netwerk van een grote Israëlische transportprovider via gestolen of hergebruikte referenties. Ondertussen schond een andere Iraanse actor, DEV-0343, die bedrijven op het gebied van defensie, maritiem transport en satellietbeelden als doelwit heeft en gelieerd lijkt te zijn aan de IRGC, accounts bij Israëlische transport- en havengerelateerde entiteiten in het begin van 2021.

Iraanse bedreigingsgroepen zullen waarschijnlijk een bedreiging blijven vormen voor Amerikaanse en Israëlische transport- en energiebedrijven, vooral nu diplomatieke inspanningen om de Iraanse kernovereenkomst te doen herleven vast beginnen te lopen en Washington, Tel Aviv en Teheran op zoek zijn naar alternatieve dwangmiddelen om concessies te verkrijgen.

Iraanse aanvallen op essentiële infrastructuur per land



Iraanse aanvallen op essentiële infrastructuur vonden het meest plaats tegen organisaties in Israël, de Emiraten en de Verenigde Staten.

Iraanse actoren zullen het komende jaar waarschijnlijk een bedreiging blijven vormen voor Amerikaanse transport- en energiebedrijven.

Iraanse groepen hebben hun ransomwareaanvallen uitgebreid tot voorbij de regionale tegenstanders en richten zich op prominente doelen voor essentiële infrastructuur in de VS en Israël.

Direct bruikbare inzichten

1. Verbeter de algehele cyberhygiëne van je organisatie door wachtwoordloze oplossingen zoals MFA in te schakelen en het gebruik ervan af te dwingen voor alle externe verbindingen om mogelijk gehackte referenties te voorkomen.
2. Evalueer de authenticiteit van alle binnenkomende e-mailverkeer om er zeker van te zijn dat het afzenderadres legitiem is.
3. Patch vroeg en vaak.[34]
4. Beoordeel en controleer elk van je partnerrelaties met serviceproviders om onnodige machtigingen tussen je organisatie en upstream providers te minimaliseren. Microsoft adviseert onmiddellijk de toegang te verwijderen voor partnerrelaties die er niet vertrouwd uitzien of die nog niet zijn gecontroleerd.[35]

Links naar verdere informatie

- Iraanse aanvallen op IT-sector in opkomst | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Aan Iran gelieerde DEV-0343 richt zich op sectoren defensie, GIS en zeevaart | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

In Libanon gevestigde groep met links naar Iran die aanvallen uitvoert op Israël

Microsoft bewaakt cyberbedreigingsactiviteiten, ongeacht het platform, beoogde slachtoffer of geografische regio. We zorgen wereldwijd voor zichtbaarheid en zoeken actief naar bedreigingen om betere detecties voor onze klanten te kunnen schrijven.

Hoewel bedreigingen vanuit Rusland, China, Iran en Noord-Korea de meerderheid van onze waargenomen actoren vertegenwoordigen, volgen en communiceren we ook over bedreigingen vanuit NAVO-lidstaten en democratische landen. Vorig jaar bespraken we activiteiten van een in Turkije gevestigde actor (SILICON) en een in Vietnam gevestigde actor (BISMUTH). Dit jaar gaan we dieper in op de details van een groep uit Libanon die we eerder openbaar hebben gemaakt.[36]

Microsoft ontdekte een voorheen nog niet gedocumenteerde groep in Libanon waarvoor we met gematigd vertrouwen hebben vastgesteld dat zij samenwerkten met actoren die zijn gelieerd aan het Iraanse ministerie van Inlichtingen en Veiligheid (MOIS). Een dergelijke samenwerking of aanwijzing vanuit Teheran zou in lijn zijn met onthullingen sinds eind 2020 dat de regering van Iran derden gebruikt om cyberoperaties uit te voeren, waarschijnlijk om de plausibele ontkenbaarheid van Iran te vergroten.

In de geobserveerde activiteit viel POLONIUM tussen februari en mei 2022 twee dozijn in Israël gevestigde organisaties en één IGO die actief was in Libanon aan, voordat Microsoft de activiteiten onderbrak en openbaar maakte. Bijna de helft van de Israëlische organisaties maakte deel uit van de Israëlische defensie-industrie of had banden met Israëlische defensiebedrijven, wat aangeeft dat de groep een vergelijkbare reeks belangen heeft als Iran bij het verzamelen van inlichtingen over en/of het direct bestrijden van Israël.[37]

De vastgestelde links van POLONIUM met MOIS-groepen zijn gebaseerd op waargenomen overlappingen van slachtoffers en het gemeenschappelijk gebruik van tools en technieken.

- Overlapping van slachtoffers: een Iraanse staatgroep die is gelieerd aan het MOIS in Iran, en die Microsoft volgt onder de naam MERCURY, compromitteerde eerder meerdere slachtoffers van POLONIUM, wat duidt op een convergentie van de missievereisten of een mogelijke "overdracht" van slachtoffers tussen groepen.
- Gemeenschappelijke tools en technieken: net als bij POLONIUM, nam MSTIC waar dat DEV-0588 (ook bekend als CopyKittens) vaak gebruikmaakt van AirVPN voor activiteiten en dat DEV-0133 (ook bekend als Lyceum[38]) OneDrive gebruikt voor C2 en exfiltratie. Net als de Iraanse overheidsactoren gebruikte POLONIUM een cloudserviceprovider om een aanval uit te voeren op een Israëlisch luchtvaartbedrijf en een advocatenkantoor.[39]

POLONIUM implementeerde een reeks aangepaste geïmplanteerde systemen met behulp van cloudservices voor C2 en data-exfiltratie, met name OneDrive en DropBox. POLONIUM maakte vaak unieke OneDrive-applicaties voor doelen, waarschijnlijk om detectie te omzeilen.

In juni 2022 heeft Microsoft meer dan 20 door POLONIUM gemaakte OneDrive-applicaties uit de lucht gehaald, de getroffen organisaties op de hoogte gesteld en een reeks beveiligingsinformatie-updates geïmplementeerd om door POLONIUM ontwikkelde tools in quarantaine te plaatsen.

Microsoft heeft met succes het misbruik van OneDrive als C2 door POLONIUM gedetecteerd en uitgeschakeld.

Direct bruikbare inzichten

1. Update antivirussoftware[40] en zorg ervoor dat cloudbescherming[41] is ingeschakeld om de bijbehorende indicatoren te detecteren.
2. Voor klanten met serviceproviderrelaties moet je ervoor zorgen dat alle partnerrelaties worden beoordeeld en gecontroleerd om onnodige machtigingen tussen je organisatie en upstream providers tot een minimum te beperken.[42] Verwijder onmiddellijk de toegang voor partnerrelaties die niet vertrouwd lijken of niet zijn gecontroleerd.

Links naar verdere informatie

- Blootlegging van activiteiten en infrastructuur van POLONIUM die waren gericht tegen Israëlische organisaties | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY maakt gebruik van Log4j 2-kwetsbaarheden in niet-gepatchte systemen om Israëlische organisaties aan te vallen | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Noord-Koreaanse cyber-capaciteiten ingezet om de drie hoofddoelen van het regime te realiseren

De cyberprioriteiten van Noord-Korea in het afgelopen jaar weerspiegelden de aangegeven wereldwijde prioriteiten van de overheid. Kim Jong Un benadrukte de drie prioriteiten van het opbouwen van defensiecapaciteit, het versterken van de worstelende economie van het land en het waarborgen van binnenlandse stabiliteit tijdens verschillende belangrijke toespraken.[43] Uit de acties van Noord-Koreaanse staatsactoren blijkt duidelijk dat cyber wordt gebruikt om deze drie doelen te bereiken.

Noord-Koreaanse staatshackers maakt gebruik van verschillende tactieken om binnen te dringen bij luchtvaartbedrijven over de hele wereld.

Noord-Koreaanse staatshackersgroepen, voornamelijk CERIUM en ZINC, gebruikten een verscheidenheid aan tactieken om door te dringen tot netwerken van defensie- en luchtvaartbedrijven over de hele wereld. Toen Noord-Korea in de eerste helft van 2022 aan zijn meest agressieve testperiode begon, werd gebruikgemaakt van cyberspionage om Noord-Koreaanse onderzoekers te helpen een voorsprong te krijgen bij het ontwikkelen van binnenlandse verdedigingssystemen en tegenmaatregelen voor de vorderingen die zijn tegenstanders maakten.

We zagen dat COPERNICIUM aanvallen uitvoerde op een aantal aan cryptovaluta's gerelateerde bedrijven over de hele wereld, vaak met succes, om de worstelende economie van Noord-Korea te helpen ondersteunen. Hoewel we niet kunnen bevestigen of de groep in staat was om geld te exfiltreren na een schending, zagen we dat COPERNICIUM tientallen machines infecteerde door schadelijke documenten te verzenden die ogenschijnlijk voorstellen van andere cryptovalutabedrijven bevatten.

Tot slot zet een groep die Microsoft volgt onder de naam DEV-0215 zich in om de stabiliteit en loyaliteit in Noord-Korea te handhaven door aanvallen uit te voeren op nieuwsorganisaties die rapporteren over Noord-Koreaanse kwesties. Deze persdiensten hebben bronnen in zowel Noord-Korea als binnen gemeenschappen van overlopers, die Pyongyang als een existentiële bedreiging beschouwt. Bovendien ondernam de groep acties om toegang te krijgen tot netwerken van Koreaans sprekende christelijke groepen, die de neiging hebben zich uit te spreken tegen Noord-Korea en actief samen te werken met Noord-Koreaanse overlopers.

Targeting van defensie- en luchtvaartbedrijven

Noord-Koreaanse staatsactoren onder leiding van CERIUM en ZINC hebben aanzienlijke inspanningen verricht om tactieken te ontwikkelen die gericht zijn op het binnendringen van defensie- en luchtvaartbedrijven. CERIUM heeft herhaaldelijk Zuid-Koreaanse virtuele particuliere netwerken (VPN's) getest door clients te downloaden en naar zwakke punten te zoeken. Het downloadde ook veelvoorkomende applicaties die worden gebruikt door militaire en overheidsklanten in Zuid-Korea, waarschijnlijk op zoek naar kwetsbaarheden. De groep volgde de actuele gebeurtenissen op de voet en schreef nieuwe lokdocumenten waarin belangrijke onderwerpen als lokaas werden gebruikt om doelen aan te moedigen op hun uitvoerbare malware-bestanden en links te klikken.

Zowel ZINC als CERIUM maakten gebruik van sociale media en social engineering in campagnes. ZINC was bijzonder bedreven in het creëren van nepprofielen op LinkedIn en andere professionele sociale-mediasites, waar de operators zich voordeden als recruiters voor grote defensie- en luchtvaartbedrijven. Met behulp van deze profielen stuurden ze links of schadelijke bestandsbijlagen naar potentiële slachtoffers via directe berichten op sociale media of e-mail.

Behalve op medewerkers van bedrijven, richtte CERIUM zijn pijlen ook op leden van het Zuid-Koreaanse leger, met speciale belangstelling voor zowel Zuid-Koreaanse militaire academies als militaire leden die werkzaam waren in de academische wereld.

Cryptovaluta gebruiken om verliezen in evenwicht te brengen

Sinds VN-sancties werden opgelegd in 2016, is de economie van Noord-Korea blijven krimpen, verergerd door natuurrampen zoals overstromingen[44] en droogte[45] evenals een vrijwel volledige sluiting van de grenzen voor imports sinds het begin van de COVID-19-pandemie begin 2020.[46] Hoewel Noord-Korea begin 2022 de grenzen voor de handel met China opende, werden deze al snel weer gesloten.[47] Half mei meldde Noord-Korea zijn eerste binnenlandse geval van COVID-19.[48] Het heeft sindsdien een 'zero COVID'-strategie in China-stijl toegepast om het virus te bestrijden, wat een negatieve invloed heeft op de toch al fragiele economie van Noord-Korea.

De Noord-Koreaanse staatshackersgroep COPERNICIUM probeerde een deel van de verloren inkomsten te compenseren door geld, meestal in de vorm van cryptovaluta's, te stelen van elk bedrijf waarvan het de netwerken kon binnendringen. We zagen dat tientallen machines werden aangetast die eigendom waren van cryptovalutabedrijven in de Verenigde Staten, Canada, Europa en Azië. COPERNICIUM heeft zelfs machines aangetast van cryptovalutabedrijven binnen de sterkste bondgenoot van Noord-Korea, China, zowel op het vasteland als in Hongkong. De groep vertrouwde sterk op sociale media voor de vroege verkenning en benadering van doelwitten. Actoren bouwden profielen waarin zij zich voordeden als developers of senior functionarissen bij cryptovalutabedrijven. Vervolgens gingen ze relaties aan met medewerkers in de industrie en verzonden schadelijke links of bestanden zodra ze een band hadden opgebouwd.

Noord-Koreaanse cybercapaciteiten ingezet om de drie hoofddoelen van het regime te realiseren

Vervolg

Een groep gerelateerd aan PLUTONIUM ontwikkelt en implementeert ransomware

Een groep actoren uit Noord-Korea die Microsoft volgt als DEV-0530 begon met het ontwikkelen en gebruiken van ransomware bij aanvallen in juni 2021. Deze groep, die zichzelf H0lyGh0st noemde, gebruikte een ransomware-payload met dezelfde naam voor zijn campagnes en viel in september 2021 met succes kleine bedrijven in meerdere landen aan.

Naar oordeel van Microsoft had DEV-0530 connecties met een andere in Noord-Korea gevestigde groep met de naam PLUTONIUM (ook bekend als DarkSeoul of Andariel). Hoewel het gebruik van H0lyGh0st-ransomware in campagnes uniek is voor DEV-0530, heeft MSTIC communicatie tussen de twee groepen waargenomen, terwijl DEV-0530 gebruikmaakte van tools die exclusief door PLUTONIUM waren gemaakt.

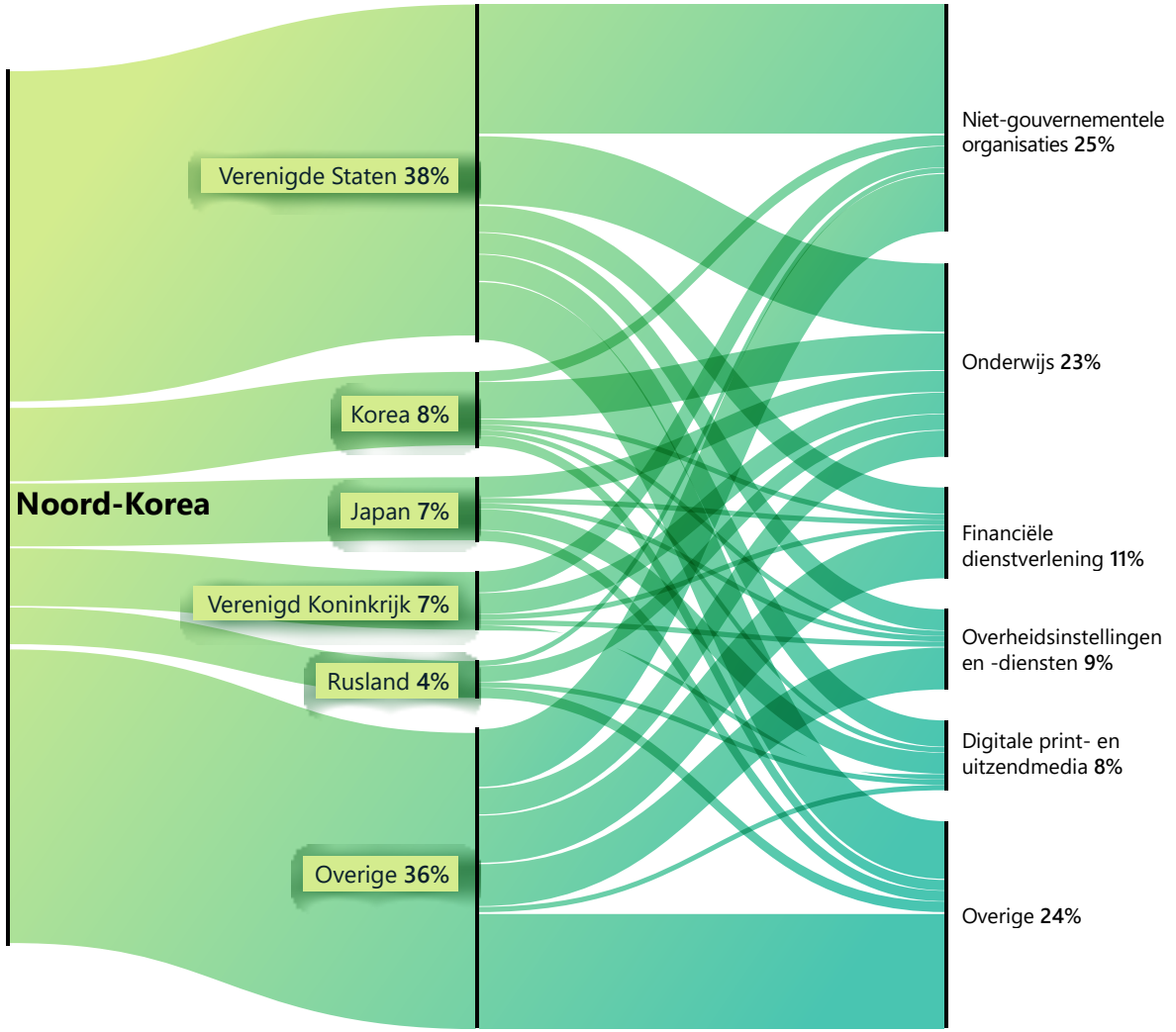
Het is niet zeker of de activiteiten van DEV-0530 door de overheid werden gesponsord. Hoewel het mogelijk is dat ransomwareaanvallen door de staat zijn besteld om dezelfde reden als waarom deze diefstal bij cryptovalutabedrijven sponsort, is het ook mogelijk dat de actoren achter DEV-0530 zelfstandig optreden om geld voor zichzelf in de wacht te slepen. Als Noord-Koreaanse hackers onafhankelijk zouden opereren, zou dat verklaren waarom de activiteit niet wijdverspreid was in vergelijking met door de overheid gesponsorde diefstallen bij cryptovalutabedrijven.

Aanvallen op Noord-Koreaanse persdiensten, overlopers, religieuze groeperingen en hulporganisaties

In het afgelopen jaar richtte opperleider Kim Jong Un zich publiekelijk meer op interne veiligheid en loyaliteit dan op projectielen en kernwapens. Als gevolg van deze bezorgdheid over binnenlandse kwesties, legden ten minste twee Noord-Koreaanse staatsgroepen de nadruk op aspecten die het regime als binnenlandse bedreigingen zou beschouwen.

De eerste was een groep die door Microsoft wordt gevolgd als DEV-0215 en die mediaorganisaties die het Noord-Koreaanse nieuws nauwlettend volgen als doelwit heeft. Een mogelijke reden voor deze aanvallen is dat deze media hun nieuws ontvangen van Noord-Koreaanse overlopers, Chinese burgers die nauw samenwerken met Noord-Korea en zelfs sommige Noord-Koreaanse burgers in het land, die via een verscheidenheid aan methoden met de buitenwereld communiceren. De Noord-Koreaanse overheid beschouwt deze groepen als een existentiële bedreiging voor het voortbestaan, met name burgers in Noord-Korea die als verraders en spionnen worden beschouwd. DEV-0215 heeft waarschijnlijk geprobeerd de bronnen van deze persdiensten te identificeren, zodat ze potentiële informatielekken konden neutraliseren.

Noord-Korea: de meest aangevallen landen en industriesectoren



Noord-Korea beschouwt de Verenigde Staten, Zuid-Korea en Japan als hun primaire vijand. Hoewel Rusland een oude bondgenoot is, richten Noord-Koreaanse bedreigingsactoren zich op Russische denktanks, academici en diplomatieke ambtenaren om inlichtingen te verkrijgen over de Russische opvattingen over mondiale aangelegenheden.

Noord-Koreaanse cybercapaciteiten ingezet om de drie hoofddoelen van het regime te realiseren

Vervolg

Microsoft heeft ook bewijs gezien dat DEV-0215 aanvallen uitvoerde op Koreaans sprekende christelijke gemeenschappen. Evangelisch-christelijke Koreaanse kerken zijn geneigd kritisch te zijn op zowel Noord-Korea als Zuid-Koreaanse regeringen die voorstander zijn van betrokkenheid bij Noord-Korea. Deze kerken zullen waarschijnlijk overlopers de helpende hand reiken, terwijl sommige zich bezighouden met humanitair werk met Noord-Korea. Noord-Korea beschouwt ze als een bedreiging omdat, hoewel de stroom van overlopers uit Noord-Korea bijna opdroogde tijdens de pandemie,[49] deze christelijke groepen vaak een cruciale rol spelen bij het helpen ontsnappen van overlopers. DEV-0215 heeft valse documenten over christelijke conferenties gegenereerd voor Koreaanse sprekers als lokmiddel om de groep aan te vallen en erachter te komen wie hulp biedt bij het organiseren van ontsnappingspogingen.

Tot slot gaf de staatsgroep OSMIUM het hele jaar door blijk van een constante belangstelling voor internationale hulporganisaties, waaronder organisaties die Noord-Korea in het verleden hebben geholpen. Hoewel Noord-Korea in het algemeen aanbiedingen van hulp van buiten het land heeft afgewezen, met name sinds het uitbreken van COVID-19,[50] is het mogelijk dat Noord-Korea overweegt om hulp aan te nemen, maar is het wellicht huiverig voor de veiligheidsaspecten van het toestaan van buitenlandse hulpverleners in het land. Noord-Korea dringt mogelijk door in de netwerken van hulporganisaties wereldwijd om te bepalen of dergelijke hulp in hun eigen land kan worden toegestaan.

Direct bruikbare inzichten

1. Noord-Koreaanse staatsactoren zijn bekwaam, meedogenloos en creatief, maar organisaties kunnen zich hiertegen beschermen.
2. De meeste succesvolle aanvallen kunnen worden gestopt met elementaire cyberhygiëne, zoals tweeledige verificatie of het niet openen van bijlagen van onbekende personen in een virtuele omgeving.

Links naar verdere informatie

- Noord-Koreaanse bedreigingsactor richt zijn pijlen op kleine en middelgrote bedrijven met H0lyGh0st-ransomware | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Onder kenners van Noord-Korea wordt sinds lange tijd gediscussieerd over de vraag of de Noord-Koreaanse regering serieus is met haar openbare verklaringen of dat deze puur effectbejag vormen. De afstemming van cyberaanvallen op de aangekondigde prioriteiten van Noord-Korea bevestigt de overtuiging dat Noord-Korea meent wat het zegt wanneer het in het openbaar over zijn doelen spreekt.

Cyberhuurlingen bedreigen de stabiliteit van de cyberspace

Er is een groeiende sector van particuliere bedrijven die tools, technieken en diensten ontwikkelen en verkopen waarmee hun klanten – vaak overheden – kunnen inbreken in netwerken, computers, telefoons en apparaten met internetverbinding. Deze entiteiten vormen een aanwinst voor actoren van vreemde mogendheden en brengen vaak dissidenten, mensenrechtenbeschermers, journalisten, maatschappelijke pleitbezorgers en andere particulieren in gevaar. We noemen dit cyberhuurlingen of offensieve actoren uit de particuliere sector.

Een wereld waarin bedrijven uit de particuliere sector cyberwapens maken en verkopen, is gevaarlijker voor consumenten, bedrijven van elke omvang en overheden. Deze offensieve tools kunnen worden ingezet op manieren die niet stroken met de normen en waarden van goed bestuur en democratie. Microsoft gelooft dat de bescherming van mensenrechten een fundamentele verplichting is, die we serieus nemen door 'surveillance as a service' over de hele wereld in te perken.

Microsoft heeft vastgesteld dat bepaalde staatsactoren in democratische en autoritaire regimes de ontwikkeling of het gebruik van 'surveillance as a service'-technologie uitbesteden. Op deze manier vermijden ze verantwoordelijkheid en toezicht, en verwerven ze capaciteiten die moeilijk zelf te ontwikkelen zouden zijn.

> Deze cyberwapens bieden vreemde mogendheden bewakingsmogelijkheden die ze niet op eigen houtje hadden kunnen ontwikkelen.

De markt waarin cyberhuurlingen opereren is ondoorzichtig. Toch blijven we deze groepen observeren die gebruikmaken van zero-day exploits en zelfs zero-click exploits die helemaal geen interactie met het slachtoffer vereisen, waardoor surveillance als een service mogelijk wordt.

Microsoft heeft onlangs de naam bekendgemaakt van een offensieve actor in de Europese particuliere sector die we KNOTWEED noemen. Dit is een in Oostenrijk gevestigde PSOA genaamd DSIRF. Meerdere nieuwsberichten hebben het bedrijf in verband gebracht met de ontwikkeling en poging tot verkoop van een malware-toolset genaamd Subzero.[51] Tot de slachtoffers behoren onder meer advocatenkantoren, banken en strategische adviesbureaus in landen als Oostenrijk, het Verenigd Koninkrijk en Panama.[52]

Omdat deze offensieve bewakingscapaciteiten niet langer zeer vertrouwelijke capaciteiten zijn die zijn gecreëerd door defensie- en inlichtingendiensten, maar veeleer commerciële producten die nu aan bedrijven en individuen worden aangeboden, moet elk regelgevend regime voor cyberwapens verder gaan dan exportcontrole. De impact van deze cyberwapens kan verwoestend zijn.

Wanneer cyberhuurlingen misbruik maken van een kwetsbaarheid in een product of dienst, brengen zij het hele computerecosysteem in gevaar. Wanneer kwetsbaarheden publiekelijk worden geïdentificeerd, bevinden bedrijven zich in een race tegen de klok om beveiligingen vrij te geven voordat op grote schaal aanvallen plaatsvinden (zie onze eerdere bespreking van kwetsbaarheidsexploits). Dit is een gevaarlijke en moeilijke cyclus voor zowel softwareleveranciers (die op doelmatige wijze patches moeten ontwikkelen) als consumenten van producten (die de patches onmiddellijk moeten implementeren).

Als een van de oprichters van het Cybersecurity Tech Accord[53], een toonaangevende alliantie waarin meer dan 150 technologiebedrijven zijn verenigd, heeft Microsoft een toezegging gedaan om zich niet in te laten met offensieve operaties online. Wij doen die toezegging gestand en staat pal achter onze verantwoordelijkheden op het gebied van mensenrechten op dit gebied. We hebben technische verstoringen uitgevoerd en zijn juridische uitdagingen aangegaan om de negatieve gevolgen te benadrukken die worden veroorzaakt door de diensten die worden geleverd door cyberhuurlingen en zullen onze klanten blijven beschermen wanneer we misbruik zien.

> Cyberhuurlingen creëren en bieden 'surveillance as a service'-mogelijkheden die technologisch geavanceerd en algemeen beschikbaar zijn, inclusief geavanceerde malware en een reeks van technieken.

Direct bruikbare inzichten voor overheden

1. Implementeer transparantie- en toezichtvereisten voor surveillance als een service, met name bij aanbestedingen, inclusief het uitbannen van deze offensieve actoren, zoals de VS hebben gedaan met de opname van bedrijven op de entiteitenlijst van het ministerie van Handel.
2. Stel tewerkstellingsbeperkingen achteraf in voor voormalige werknemers in deze sector.
3. Streef ernaar "ken uw klant"-verplichtingen te implementeren en moedig bedrijven aan om hun mensenrechtenverplichtingen na te komen.

Links naar verdere informatie

- Het ontwarren van KNOTWEED: offensieve actor in de Europese particuliere sector die gebruikmaakt van 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Voortzetting van de strijd tegen cyberwapens uit de particuliere sector | Microsoft On the Issues

Operationele normen voor cyberbeveiliging voor vrede en veiligheid in cyberspace

We hebben dringend een consistent, wereldwijd kader nodig dat prioriteit geeft aan mensenrechten en mensen beschermt tegen roekeloos online gedrag van de staat. Nergens wordt dit duidelijker aangetoond dan in de voortdurende oorlog in Oekraïne. Overheden kunnen nu een wereldwijde strategische inspanning verrichten en bovendien ingrijpen om een onmiddellijke positieve impact te hebben.

Vijf jaar geleden riep Microsoft op tot een 'Digitale Conventie van Genève' om verantwoordelijkheden en verplichtingen in alle sectoren te bevorderen ter bescherming van vrede en veiligheid online. De cyberspace kwam op als een duidelijk en vluchtig domein van conflicten en concurrentie tussen staten, waarbij aanvallen steeds vaker voorkwamen, zelfs in tijden van vrede.

Vandaag de dag is er nog steeds een duidelijke behoefte aan een dergelijk kader, zoals blijkt uit de Russische cyberaanvallen op Oekraïne als onderdeel van de Russische invasie. Deze oorlog heeft een nieuwe frontlinie gecreëerd die dramatisch afwijkt van we tot nu toe hebben gekend.

Als we voor stabiliteit in cyberspace willen zorgen, moeten instellingen voor mondiaal bestuur worden versterkt en opnieuw ontworpen om ze geschikt te maken voor hun doel. Cyberspace is fundamenteel anders dan andere domeinen: het is grenzeloos, synthetisch en wordt grotendeels onderhouden door de particuliere industrie. Dit betekent dat de technologie-industrie wordt gevraagd om meer verantwoordelijkheid te nemen voor zowel de beveiliging van producten en diensten als het bredere digitale ecosysteem. Hoewel er op alle fronten opmerkelijke vooruitgang is geboekt, zijn de uitdagingen enorm toegenomen.

We moeten de collectieve inspanningen verdubbelen om de veiligheid van cyberspace te verdedigen. We kunnen de rechten en vrijheden die we online gewend zijn, niet als vanzelfsprekend beschouwen. Terwijl we worstelen om de uitdagingen het hoofd te bieden, plannen kwaadwillende actoren hoe en waar ze vervolgens zullen toeslaan met behulp van AI, waarbij ze gebruikmaken van desinformatie en manieren zoeken om de jonge metaverse te ondermijnen. Mensenrechtenbeschermers, de technologie-industrie en overheden die rechten respecteren, moeten samenwerken aan een bevestigende visie voor een veilige en beveiligde online wereld. De weg die voor ons ligt is lang, maar er zijn dingen die overheden nu kunnen doen om het cybersecurity-ecosysteem onmiddellijk te verbeteren:

- Noem normen, wetten en consequenties in toeschrijvingen. Een belangrijke verbetering in de afgelopen vijf jaar is de snelheid en coördinatie van de toeschrijvingen van cyberaanvallen door de overheid. Deze verklaringen moeten verder gaan dan simpelweg 'naming and shaming', maar moeten ook duidelijk maken welke internationale wetten of normen worden geschonden en welke consequenties deze zullen hebben om de erkenning van internationale verwachtingen te versterken.
- Verduidelijk de interpretatie van internationaal recht online. Hoewel regeringen het erover eens zijn dat internationaal recht online van toepassing is, blijven er vragen over hoe het in specifieke gevallen van toepassing is. Dit is met name relevant in de nasleep van de invasie in Oekraïne. Overheden kunnen een grote bijdrage leveren aan het scheppen van verwachtingen, het vermijden van misverstanden en het opbouwen van vertrouwen door aan te geven hoe zij hun verplichtingen onder internationaal recht verstaan.
- Voer overleg met andere stakeholders. Terwijl internationale forums de beste manieren blijven ontdekken om robuuste inclusie van meerdere stakeholders mogelijk te maken, kunnen overheden een geïnformeerde dialoog ondersteunen door te overleggen met gemeenschappen met meerdere stakeholders, met name de technologie-industrie, om de voordelen te bieden van een dialoog met degenen die over onmisbare expertise beschikken.
- Vorm een permanent orgaan om verantwoord staatsgedrag in cyberspace te ondersteunen. Het werk van internationale diplomatieke forums om verantwoord overheidsgedrag online te bevorderen, is nog nooit zo belangrijk geweest. Er is duidelijk behoefte aan een permanent VN-mechanisme om cyberspace als conflictgebied aan te pakken.
- Definieer nieuwe normen voor zich ontwikkelende bedreigingen. Cyberspace-bedreigingen evolueren voortdurend samen met technologische innovaties. Hoewel internationale normen technologieneutraal moeten zijn, moeten ze worden bijgewerkt en afgezwakt op basis van veranderingen in het dreigingslandschap en de wijze waarop we technologie gebruiken. Ook nu nog zien we dat hiaten in het bestaande internationale kader worden misbruikt. Staten moeten zich ertoe verbinden de kernprocessen die ten grondslag liggen aan het digitale ecosysteem en die momenteel niet worden beschermd, zoals het software-updateproces, uitdrukkelijk te beschermen. Bovendien verdienen specifieke gebieden extra bescherming. Zoals we bijvoorbeeld tijdens de pandemie hebben geleerd, zijn normen voor de bescherming van de gezondheidszorg essentieel.

Actoren van vreemde mogendheden en aanvallen nemen toe in volume en verfijning, waardoor een onhoudbare situatie ontstaat.

Onmiddellijke actie is absoluut noodzakelijk - er zijn dingen die overheden nu kunnen doen om het cyberbeveiligingsecosysteem onmiddellijk te verbeteren, inclusief het implementeren van overeengekomen normen en regels voor het gedrag van staten in cyberspace en het samenwerken met de bredere community van stakeholders om opkomende lacunes aan te pakken.

Multilaterale instellingen moeten een nieuwe invulling krijgen om de dringende uitdaging van cyberaanvallen door vreemde mogendheden het hoofd te bieden.

Links naar verdere informatie

- Een cruciaal moment: de noodzaak van een krachtige en wereldwijde cyberbeveiligingsrespons | Microsoft On the Issues
- Cyberaanvallen op de gezondheidszorg moeten stoppen | Microsoft On the Issues
- Het volgende hoofdstuk van cyberdiplomatie bij de Verenigde Naties lonkt | Microsoft On the Issues

Eindnoten

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

Eindnoten vervolg

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. Patch met name Exchange-servers voor ProxyShell-kwetsbaarheden (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 en CVE-2021-27065, CVE-2021-34473). Zorg er ook voor dat je Fortinet FortiOS SSL VPN-apparaten patcht op kwetsbaarheden.
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. Zoals opgemerkt in onze technische blog, betekent de identificatie van doelen in een land niet noodzakelijkerwijs dat een DSIRF-klant in hetzelfde land woont, aangezien internationale targeting gebruikelijk is.
53. Home | Cybersecurity Tech Accord (cybertechaccord.org)

Apparaten en infrastructuur

Met de versnelling van de digitale transformatie is de beveiliging van de digitale infrastructuur belangrijker dan ooit.

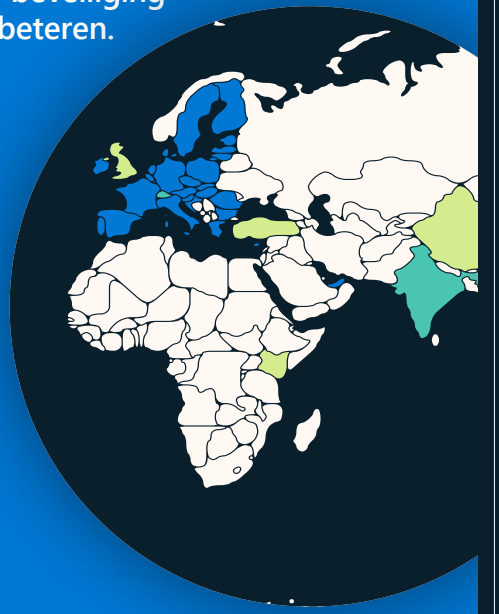
Een overzicht van

apparaten en infrastructuur

De pandemie, in combinatie met de snelle invoering van allerlei internetapparaten als onderdeel van de versnelling van de digitale transformatie, heeft het aanvalsoppervlak van de digitale wereld sterk vergroot.

Cybercriminelen en vreemde mogendheden profiteren snel. Hoewel de beveiliging van IT-hardware en -software de afgelopen jaren is verbeterd, heeft de beveiliging van IoT- (Internet of Things) en OT-apparaten (Operational Technology) geen gelijke tred gehouden. Bedreigingsactoren benutten deze apparaten om toegang tot netwerken te krijgen en laterale verplaatsing mogelijk te maken, een voet aan de grond te krijgen in een supply chain of de OT-activiteiten van de doelorganisatie te verstoren.

Overheden over de hele wereld zijn in beweging om kritieke infrastructuur te beschermen door IoT- en OT-beveiliging te verbeteren.

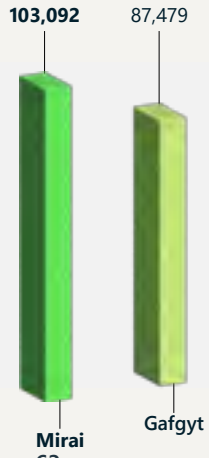


Ga voor meer informatie naar p59

Er is wereldwijd consistent en interoperabel beveiligingsbeleid nodig om brede acceptatie te garanderen.

Ga voor meer informatie naar p59

Malware as a service is uitgegroeid tot grootschalige operaties tegen blootgestelde IoT en OT in infrastructuur en hulpprogramma's, evenals in bedrijfsnetwerken.



Ga voor meer informatie naar p63

Aanvallen op apparaten voor beheer op afstand nemen toe, met meer dan 100 miljoen aanvallen waargenomen in mei 2022, oftewel een vervijfvoudiging in het afgelopen jaar.

Ga voor meer informatie naar p62

Aanvallers maken in toenemende mate gebruik van kwetsbaarheden in de firmware van IoT-apparaten om bedrijfsnetwerken te infiltreren en verwoestende aanvallen uit te voeren.

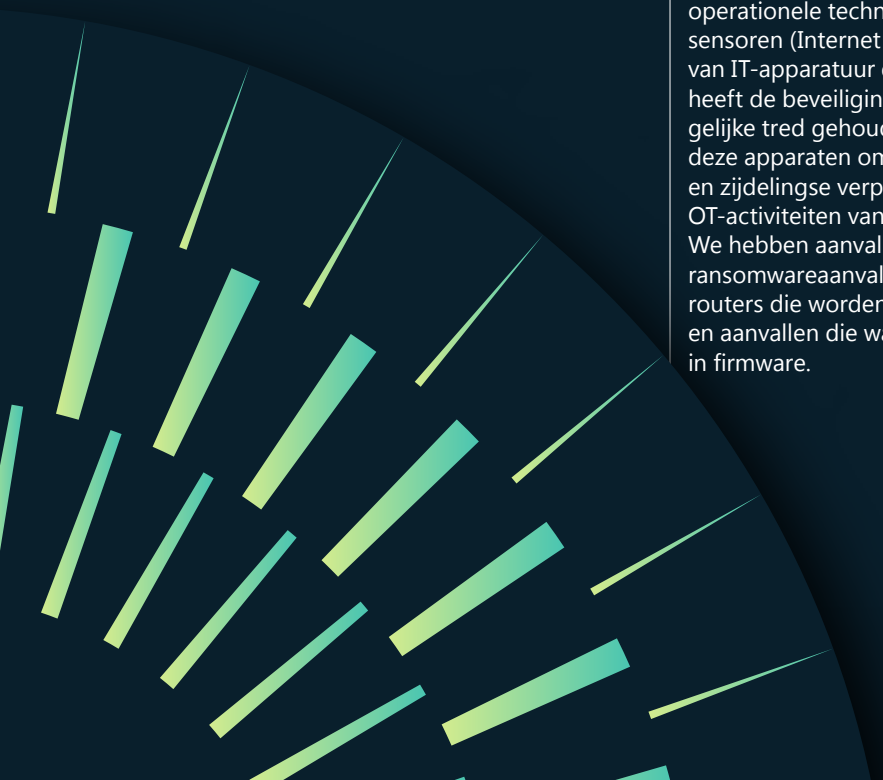
Ga voor meer informatie naar p65

32% van de geanalyseerde firmware-images bevatte ten minste 10 bekende kritieke kwetsbaarheden.

Ga voor meer informatie naar p66

Inleiding

Het versnellen van de digitale transformatie heeft het cyberbeveiligingsrisico voor essentiële infrastructuur en cyberfysieke systemen vergroot.



De afgelopen jaren hebben ongekende veranderingen plaatsgevonden in de digitale wereld. Organisaties evolueren om gebruik te maken van de vooruitgang in computercapaciteiten van zowel de intelligente cloud als intelligente randapparatuur. Als gevolg van de pandemie die entiteiten dwong tot digitaliseren om te overleven en de snelheid waarmee industrieën over de hele wereld overstappen op internetapparaten, neemt het aanvalsoppervlak van de digitale wereld exponentieel toe.

Deze snelle migratie heeft het vermogen van de beveiligingsgemeenschap om bij te blijven overtroffen. Het afgelopen jaar hebben we bedreigingen waargenomen die gebruikmaken van apparaten in elk deel van de organisatie, van traditionele IT-apparatuur tot controllers voor operationele technologie (OT) of eenvoudige IoT-sensoren (Internet of Things). Hoewel de beveiliging van IT-apparatuur de afgelopen jaren is verbeterd, heeft de beveiliging van IoT- en OT-apparaten geen gelijke tred gehouden. Bedreigingsactoren misbruiken deze apparaten om toegang tot netwerken te krijgen en zijdelingse verplaatsing mogelijk te maken of de OT-activiteiten van de doelorganisatie te verstoren. We hebben aanvallen op elektriciteitsnetten gezien, ransomwareaanvallen die OT-operaties verstoren, IoT-routers die worden gebruikt voor meer persistentie en aanvallen die waren gericht op kwetsbaarheden in firmware.

Hoewel de prevalentie van IoT- en OT-kwetsbaarheden een uitdaging is voor alle organisaties, loopt essentiële infrastructuur een verhoogd risico omdat bedreigingsactoren hebben geleerd dat het uitschakelen van essentiële services een krachtige hefboom is. De ransomwareaanval van 2021 op de Colonial Pipeline Company toonde aan hoe criminelen een essentiële service kunnen verstoren om de kans op betaling van losgeld te vergroten. En de Russische cyberaanvallen op Oekraïne tonen aan dat sommige vreemde mogendheden cyberaanvallen op essentiële infrastructuur als acceptabele sabotage beschouwen om de eigen militaire doelen te bereiken.

Er gloort echter hoop aan de horizon. Beleidsmakers en netwerkverdedigers treden op om de cyberbeveiliging van essentiële infrastructuur te verbeteren, inclusief de IoT- en OT-apparaten waarop ze vertrouwen. Beleidsmakers versnellen de ontwikkeling van wet- en regelgeving om het vertrouwen van het publiek in de cyberbeveiliging van essentiële infrastructuur en apparaten op te bouwen.

Microsoft werkt samen met overheden over de hele wereld om deze kans te grijpen om de cyberbeveiliging te verbeteren en we verwelkomen extra betrokkenheid. We zijn echter bezorgd dat inconsistente, op maat gemaakte of complexe vereisten onbedoelde effecten kunnen hebben, waaronder in sommige gevallen een afnemende beveiliging door schaarse beveiligingsresources in te zetten voor naleving van meerdere dubbele certificeringen.

Vanuit het oogpunt van beveiligingsoperaties hanteren netwerkverdedigers meerdere benaderingen om de IoT/OT-beveiligingsstatus van hun organisatie te verbeteren. Een benadering is het implementeren van continue bewaking van IoT- en OT-apparaten. Een andere manier is om "naar links te schuiven", wat betekent dat we betere cyberbeveiligingspraktijken eisen en implementeren voor de IoT- en OT-apparaten zelf. Een derde benadering is het implementeren van een oplossing voor beveiligingsbewaking die zowel IT- als OT-netwerken omvat. Deze holistische benadering heeft als belangrijk bijkomend voordeel dat het bijdraagt aan kritieke organisatorische processen, zoals het "doorbreken van de silo's" tussen OT en IT, wat de organisatie op zijn beurt in staat stelt een verbeterde beveiligingsstatus te bereiken en tegelijkertijd zakelijke doelstellingen te behalen.

Michal Braverman-Blumenstyk
Corporate Vice President, Chief Technology Officer, Cloud and AI Security

Overheden die optreden om de beveiliging en veerkracht van essentiële infrastructuur te verbeteren

Overheden over de hele wereld ontwerpen en ontwikkelen beleid om de cyberbeveiligingsrisico's van essentiële infrastructuur te beheren. Velen voeren ook beleid uit om de beveiliging van IoT- en OT-apparaten te verbeteren. De groeiende wereldwijde golf van beleidsinitiatieven creëert enorme kansen om de cyberbeveiliging te verbeteren, maar stelt ook stakeholders in het hele ecosysteem voor uitdagingen.

Het ontwikkelen van een holistische visie voor het beheer van het cyberrisico van essentiële infrastructuur is van cruciaal belang, maar complex, vooral gezien de mate van onderlinge verbinding tussen technologieën en wereldwijde leveranciers, het scala aan technologiegebruik en bijbehorende risico's, en de noodzaak om te investeren in strategieën voor zowel de korte als de lange termijn. Beleid met een effectief bereik dat iteratief leren en verbeteringen stimuleert en wereldwijde, sectoroverschrijdende interoperabiliteit ondersteunt, kan helpen de complexiteit te beheersen en een meer op veiligheid gerichte digitale transformatie mogelijk te maken. Een gefragmenteerde benadering van wetgeving kan echter leiden tot overlappende en inconsistente regelgevingsvereisten. Dit kan gevolgen hebben voor resources en uiteindelijk de beveiligingsdoelstellingen ondermijnen. Organisaties zouden bijvoorbeeld resources die zich bezighouden met innovatie en beveiliging kunnen gaan inzetten voor formalistische nalevingsoefeningen.

Microsoft wil samenwerken met regeringen over de hele wereld bij het nastreven van een effectief cyberbeveiligingsbeleid voor essentiële infrastructuur, het vergroten van het begrip van uitdagingen en kansen en het ondersteunen van inspanningen om de collectieve risicosituatie te verbeteren.

Beleidsontwikkelingen op het gebied van cyberbeveiligingsrisicobeheer van essentiële infrastructuur

Het afgelopen jaar hebben meerdere jurisdicties, waaronder Australië, Chili, de Europese Unie (EU), Japan, Singapore, het Verenigd Koninkrijk (VK) en de Verenigde Staten, sectoroverschrijdende of sectorspecifieke vereisten voor cyberbeveiliging ontwikkeld, bijgewerkt of geïmplementeerd.[1] Veel van deze regeringen, en anderen zoals India[2] en Zwitserland[3], hebben al vereisten voor de rapportage van cyberbeveiligingsincidenten uitgevaardigd of hebben deze in ontwikkeling voor essentiële infrastructuur en aanbieders van essentiële diensten.[4]

Het afgelopen jaar hebben zich enkele opmerkelijke beleidsontwikkelingen voorgedaan in Australië, de EU, Indonesië en de Verenigde Staten. Australië heeft twee wetten aangenomen om het te helpen de sectoroverschrijdende cyberbeveiligingsrisico's van essentiële infrastructuur te beheren. De wetten wijzen onder meer nieuwe essentiële infrastructuursectoren aan, vereisen de ontwikkeling van risicobeheerplannen, stellen cyberbeveiligingsincidentrapportage verplicht en machtigen de overheid om in te grijpen als zij vaststelt dat een exploitant van essentiële infrastructuur niet bereid of in staat is adequaat te reageren op een incident.

De EU heeft aan de actualisering van haar NIS-richtlijn van 2016 gewerkt, die een kader biedt voor EU-lidstaten om technologische diensten en producten te reguleren die van cruciaal belang worden geacht voor hun economie en het functioneren van de samenleving. De voorgestelde NIS 2 omvat herzieningen die een nieuwe categorie essentiële digitale infrastructuur zouden creëren, de vereisten voor het melden van cyberincidenten zouden verhogen en aanvullende vereisten op het gebied van cyberbeveiligingsrisicobeheer zouden opleggen. De EU heeft ook een voorgestelde update van haar Digital Operational Resilience Act (DORA) ontwikkeld, waardoor nieuwe vereisten ontstaan voor informatiecommunicatietechnologieën die in de financiële dienstensector worden gebruikt.

In mei heeft Indonesië een presidentiële verordening uitgevaardigd over de bescherming van vitale informatie-infrastructuur ("IIV"), die in mei 2024 van kracht wordt en betrekking heeft op sectoren zoals energie, transport, financiën en gezondheidszorg. Het doel van Indonesië met de verordening is om de continuïteit van de uitvoering van IIV te beschermen, cyberaanvallen te voorkomen en de paraatheid bij het omgaan met cyberincidenten te vergroten. IIV-aanbieders zijn verantwoordelijk voor het uitvoeren van veilige en betrouwbare bescherming, het implementeren van effectief cyberrisicobeheer en het rapporteren van cyberrisicoresultaten aan de overeenkomstige overheidsinstanties. In de verordening is een verplichting opgenomen om cyberincidenten binnen 24 uur te melden.

Overheden die optreden om de beveiliging en veerkracht van essentiële infrastructuur te verbeteren

Vervolg

Het Amerikaanse Congres heeft een wet aangenomen die het Cybersecurity and Infrastructure Security Agency (CISA) machtigt om voorschriften uit te vaardigen om de rapportage van cyberincidenten door exploitanten van essentiële infrastructuur verplicht te stellen, terwijl de Amerikaanse Transportation Security Administration (TSA) nieuwe sectorspecifieke cyberbeveiligingsvereisten in de transportsector heeft uitgevaardigd. In 2021 vaardigde TSA twee veiligheidsrichtlijnen uit voor exploitanten van gevaarlijke vloeistof- en aardgaspijpleidingen als reactie op de ransomwareaanval op de Colonial Pipeline Company:

- De eerste richtlijn vereiste dat operators een cyberbeveiligingscoördinator aanwijzen, cyberincidenten binnen 12 uur melden en een kwetsbaarheidsbeoordeling van hun systemen uitvoeren.
- De tweede richtlijn, die de TSA in 2022 heeft herzien, verplichtte hen om specifieke risicobeperkende maatregelen te nemen om bescherming te bieden tegen ransomwareaanvallen en andere bekende bedreigingen voor IT- en OT-systemen, om binnen 30 dagen een nood- en responsplan voor cyberbeveiliging te ontwikkelen en te implementeren, en om een jaarlijkse beoordeling van het ontwerp van de cyberbeveiligingsarchitectuur te ondergaan.

Voortbouwend op zijn regelgeving voor pijpleidingen, heeft TSA later in 2021 twee aanvullende beveiligingsrichtlijnen uitgevaardigd die cyberbeveiligingsvereisten afkondigden voor goederenvervoer per spoor, passagiersvervoer per spoor of spoorwegvervoersystemen. De richtlijnen verplichtten de betrokken operators om een cyberbeveiligingscoördinator aan te wijzen, cyberbeveiligingsincidenten binnen 24 uur te melden, een responsplan voor cyberbeveiligingsincidenten te ontwikkelen en uit te voeren en een kwetsbaarheidsbeoordeling op het gebied van cyberbeveiliging uit te voeren. TSA kondigde tegelijkertijd aan dat het ook zijn luchtvaartbeveiligingsprogramma's heeft bijgewerkt om luchthavenautoriteiten en luchtvaartmaatschappijen te verplichten de eerste twee bepalingen uit te voeren, een coördinator aan te wijzen en incidenten binnen 24 uur te melden.

Beleidsontwikkelingen in IoT- en OT-apparaatbeveiliging

In tientallen landen zijn overheden actief bezig met het ontwikkelen van vereisten om de cyberbeveiliging van producten en diensten op het gebied van informatie- en communicatietechnologie (ICT), waaronder IoT- en OT-apparaten, te verbeteren. In de context van ICT-producten en -diensten zijn de grootste zorgen de beveiliging van de supply chain van software en IoT-beveiliging.

- De Europese Commissie heeft de Cyber Resilience Act voorgesteld, die cyberbeveiligingsvereisten zou vaststellen voor stand-alone software en aangesloten apparaten en ondersteunende diensten.[5] Relevante praktijken voor softwareleveranciers zijn onder meer het hanteren van een veilige levenscyclus voor softwareontwikkeling[6] en het verstrekken van een softwarestuklijst.[7] Er zouden nieuwe beveiligingsvereisten van toepassing zijn op aangesloten apparaten en alle fabrikanten zouden de taak krijgen om gecoördineerde openbaarmakingsprocessen van kwetsbaarheden[8] voor vrijgegeven producten te beheren.

Beleidsmakers hebben ook hun aandacht gericht op de aanhoudende verspreiding van IoT-apparaten en in netwerken opgenomen OT-apparaten.

- In het Verenigd Koninkrijk zal de ontwerpwet voor productbeveiliging en telecommunicatie-infrastructuur fabrikanten van consumentenproducten, zoals smart-tv's, verplichten om te stoppen met het gebruik van standaardwachtwoorden die een gemakkelijk doelwit zijn voor cybercriminelen, om een beleid inzake openbaarmaking van kwetsbaarheden op te stellen (zoals een manier om op de hoogte te worden gesteld van beveiligingsfouten) en om transparantie te bieden over de minimale tijdsduur waarin ze beveiligingsupdates zullen leveren.[9]
- In de EU worden nieuwe beveiligingsnormen of -vereisten geïmplementeerd via meerdere wetgevingsinstrumenten, waaronder een gedelegeerde wet voor de richtlijn voor radioapparatuur die van toepassing is op draadloze apparaten en die beoogt de veerkracht van het netwerk te verbeteren, de privacy van consumenten te beschermen en het risico op monetaire fraude te verminderen.[10] Daarnaast zou het gebruik van een cloudcertificeringsschema,[11] dat momenteel in ontwikkeling is als gevolg van de EU-cyberbeveiligingswet van 2019,[12] nodig kunnen zijn.

De behoefte aan consistentie

In veel gevallen wordt het scala aan activiteiten in regio's, sectoren, technologieën en operationele risicobeheergebieden tegelijkertijd nagestreefd, wat resulteert in mogelijke overlapping of inconsistentie in reikwijdte, vereisten en complexiteit voor organisaties die begeleiding willen gebruiken of naleving willen aantonen. Zonder een universeel aanvaarde definitie van IoT is de reikwijdte vooral een uitdaging voor de regelgeving voor IoT- en OT-apparaten. De bovenstaande voorbeelden zijn mogelijk van toepassing op 'verbonden producten en ondersteunende diensten', 'producten die door consumenten kunnen worden aangesloten' en 'draadloze apparaten'. Tegelijkertijd streven veel overheden ernaar om robuustere beoordelingsregimes te implementeren om beter te begrijpen of en hoe organisaties en producten voldoen aan de huidige, opkomende en evoluerende vereisten. Naarmate deze trends samensmelten, zal de complexiteit toenemen. Het is bemoedigend dat tijdens de raadpleging voor de Cyber Resilience Act van de EU werd onderzocht hoe nieuwe regelgeving zou kunnen interageren met bestaande regelgeving op het gebied van cyberbeveiliging, wat duidt op de intentie om tegenstrijdige cyberbeveiligingsvereisten te vermijden.

Iteratieve benaderingen die op risico's zijn gebaseerd en resultaat- of procesgericht zijn (versus implementatiespecifiek) kunnen verbeterde cyberbeveiliging en continue verbetering bevorderen. Evenzo zou een focus op het mogelijk maken van interoperabiliteit tussen sectoren, regio's en beleidsgebieden de cyberbeveiliging in onderling verbonden wereldwijde supply chains consequent kunnen verhogen.

Overheden die optreden om de beveiliging en veerkracht van essentiële infrastructuur te verbeteren

Vervolg

Er is een steeds complexer cyberbeveiligingsbeleid voor essentiële infrastructuur in ontwikkeling in regio's, sectoren en onderwerpgebieden. Deze activiteit brengt grote kansen en aanzienlijke uitdagingen met zich mee. Hoe overheden te werk gaan, zal cruciaal zijn voor de toekomst van digitale transformatie en ecosysteembrede beveiliging.

Het versnellen van ecosysteembrede investeringen in de beveiliging van de supply chain voor software en Zero Trust-architectuur

US Executive Order (EO) 14028 ter verbetering van cyberbeveiliging is een katalysator geweest voor het versnellen van de lopende initiatieven van Microsoft om te investeren in onze eigen en ecosysteembrede beveiliging van de supply chain en om onze klanten in staat te stellen de Zero Trust-doelstellingen te halen.

We geloven al heel lang dat het verbeteren van de supply chain voor software het delen van lessen en best practices vereist, te beginnen met onze openbare release van de Security Development Lifecycle van Microsoft ongeveer 15 jaar geleden.

Daarnaast werken we nauw samen met het National Cybersecurity Center of Excellence om benaderingen van Zero Trust Architecture te demonstreren die worden toegepast op zowel on-premises als cloudtechnologie en om nieuwe productmogelijkheden tot stand te brengen, waaronder de mogelijkheid om phishing-resistente verificatie af te dwingen voor hybride en multicloudomgevingen.

Tegenwoordig gaan we verder dan de vereisten van de EO om conformiteit met de beveiligingsvereisten van de supply chain voor software aan te tonen en verstrekken op twee manieren SBOM-informatie (Software Bill of Materials):

1. Ten eerste delen we een open-sourceversie van onze SBOM-generatortool, die we hebben gebouwd voor eenvoudige integratie met CI/CD-pijplijnen die builds ondersteunen op Windows-, Linux-, Mac-, iOS- en Android-platforms.[13]
2. Ten tweede dragen we bij aan de ontwikkeling van industriestandaarden voor Integriteit, transparantie en vertrouwen van de supply chain (Supply Chain Integrity, Transparency, and Trust - SCITT). Dit zal de geautomatiseerde uitwisseling van verifieerbare supply chain-informatie mogelijk maken, inclusief artefacten die conformiteit aantonen met vereisten zoals die voortvloeien uit de supply chain-richtlijnen voor software van de EO.

Direct bruikbare inzichten

1. Multilaterale instellingen moeten een nieuwe invulling krijgen om de dringende uitdaging van cyberaanvallen door vreemde mogendheden het hoofd te bieden.
2. Ontwikkel een cyberbeveiligingsbeleid dat consistent en interoperabel is in alle regio's, sectoren en thema's.

Links naar verdere informatie

- Voortgezette investeringen in supply chain-beveiliging ter ondersteuning van de Cybersecurity Executive Order | Microsoft Tech Community
- Amerikaanse overheid zet strategie en vereisten voor Zero Trust-architectuur uiteen | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Integriteit, transparantie en vertrouwen van de supply chain | github.com
- Een Zero Trust-architectuur implementeren | NCCoE (nist.gov)

IoT en OT blootgesteld: trends en aanvallen

De steeds meer verbonden digitale wereld betekent dat apparaten snel online komen, communiceren met grotere systemen, data verzamelen en zichtbaarheid creëren in voorheen aan het oog onttrokken ruimten. Dit biedt kansen voor zowel organisaties als bedreigingsactoren, waarbij cybercriminaliteit zowel een miljardenindustrie als een risico wordt.

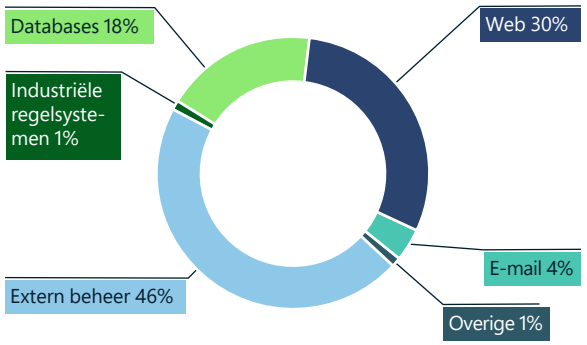
IoT-apparaten, waaronder alles van printers tot webcamera's, apparaten voor klimaatbeheersing en toegangscontroles voor gebouwen, vormen unieke beveiligingsrisico's voor individuen, organisaties en netwerken. Hoewel ze van cruciaal belang zijn voor de activiteiten van veel organisaties, kunnen ze snel een belasting en beveiligingsrisico worden. De snelle acceptatie van IoT-oplossingen in bijna elke branche heeft het aantal aanvalsvectoren en het blootstellingsrisico van organisaties vergroot.

Malware as a service is uitgegroeid tot grootschalige operaties tegen civiele infrastructuur en nutsbedrijven (waaronder ziekenhuizen, olie en gas, elektriciteitsnetten, transportdiensten en andere essentiële infrastructuur) en bedrijfsnetwerken. Aanvallers moeten aanzienlijke onderzoeksinspanningen verrichten om de configuratie van besturingsomgevingen en embedded IoT- en OT-apparaten te ontdekken en te exploiteren.

IoT-apparaten vormen unieke beveiligingsrisico's als toegangs- en draaipunten in het netwerk. Miljoenen IoT-apparaten zijn ongepatcht of blootgesteld.

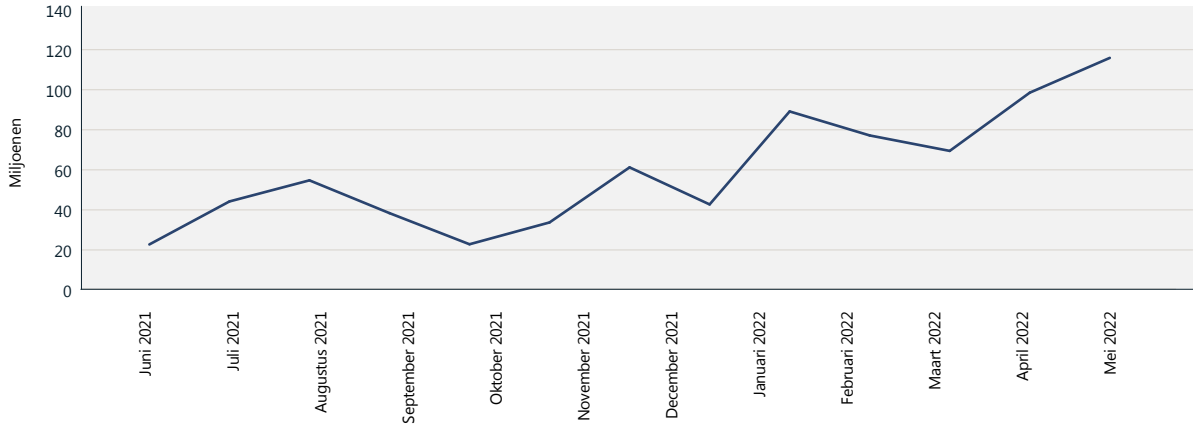
Blootgestelde apparaten kunnen worden gedetecteerd via zoektools op internet door services te identificeren die luisteren op open netwerkpoorten. Deze poorten worden gewoonlijk gebruikt voor extern beheer van apparaten. Als het niet correct is beveiligd, kan een blootgesteld IoT-apparaat worden gebruikt als draaipunt naar een andere laag van het bedrijfsnetwerk, aangezien onbevoegde gebruikers op afstand toegang kunnen krijgen tot de poorten. We hebben verschillende bedreigingsactoren waargenomen die proberen kwetsbaarheden te misbruiken in via internet blootgestelde apparaten, variërend van camera's tot routers en thermostaten. Ondanks het risico blijven miljoenen apparaten echter ongepatcht of blootgesteld.

Samenvatting van aanvalstypen op IoT/OT



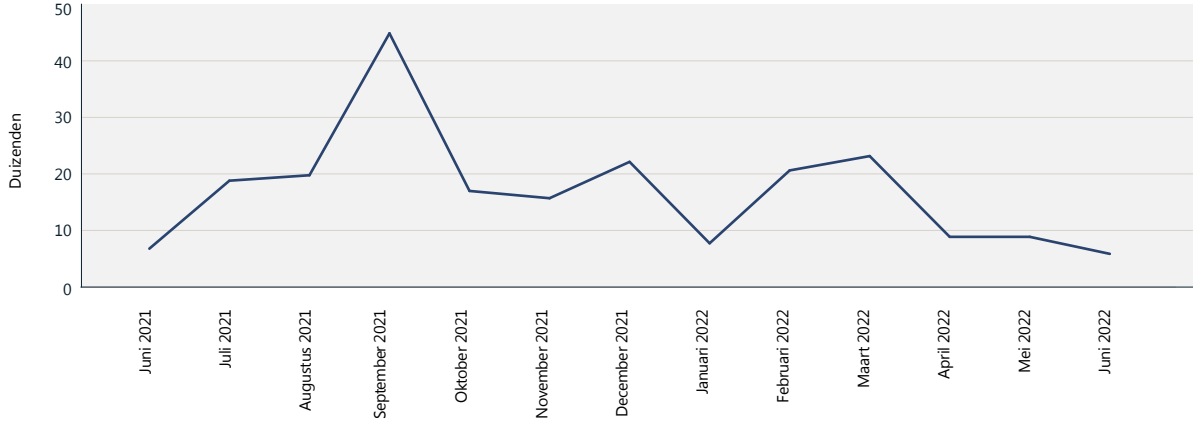
Aanvalstypen waargenomen via MSTIC-sensornetwerk. De meest voorkomende aanvallen waren aanvallen op apparaten voor beheer op afstand, aanvallen via internet en aanvallen op databases (brute force-aanvallen of exploits).

Aanvallen op apparaten voor beheer op afstand



Toenemende aanvallen op externe beheerpoorten in de loop van de tijd, zoals te zien is via het MSTIC-sensornetwerk.

Webaanvallen tegen IoT en OT



Volume van webaanvallen in de loop van de tijd, zoals te zien is via het MSTIC-sensornetwerk. Aangezien het aantal apparaten dat rechtstreeks met internet is verbonden blijft dalen, is het mogelijk dat aanvallers er uiteindelijk minder snel naar zullen zoeken.

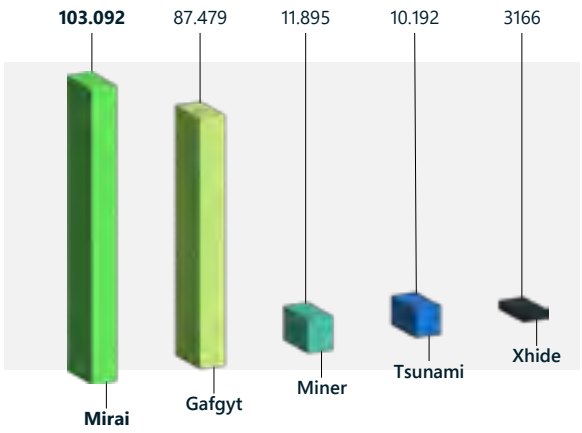
IoT en OT blootgesteld: trends en aanvallen

Vervolg

Vernieuwd malwarehulpprogramma

Naarmate cybercriminaliteitsgroepen zijn geëvolueerd, heeft ook hun inzet van malware en de keuze van doelwitten een ontwikkeling doorgemaakt. In het afgelopen jaar zagen we dat aanvallen op veelgebruikte IoT-protocollen, zoals Telnet, aanzienlijk daalden, in sommige gevallen wel 60 procent. Tegelijkertijd werden botnets hergebruikt door cybercriminaliteitsgroepen en actoren van vreemde mogendheden. De persistentie van malware, zoals Mirai, benadrukt de modulariteit van deze aanvallen en het aanpassingsvermogen van bestaande bedreigingen.

Meest in het wild gedetecteerde malware



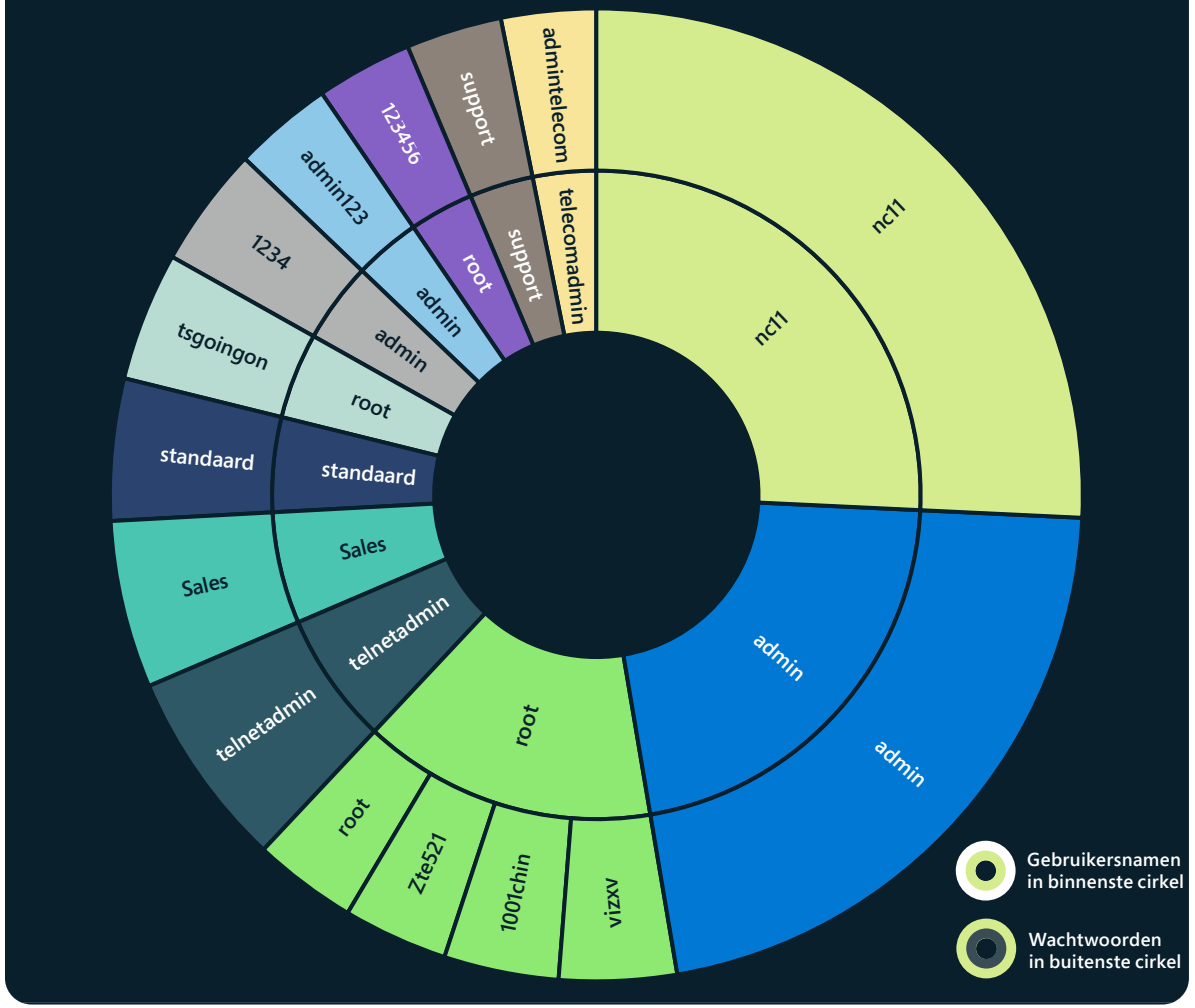
Mirai is zodanig geëvolueerd dat het een breed scala aan IoT-apparaten kan infecteren, waaronder internetprotocolcamera's, digitale videorecorders met beveiligingscamera's en routers. De aanvalsvector omzeilde verouderde beveiligingscontroles en vormt een risico voor endpoints binnen het netwerk door extra kwetsbaarheden te misbruiken en zich zijdelings te verplaatsen. Mirai is meerdere keren opnieuw ontworpen, met varianten die zijn aangepast aan verschillende architecturen en die gebruikmaken van zowel bekende kwetsbaarheiden als zero-day kwetsbaarheden om nieuwe aanvalsvectoren te bieden.

Het gebruik van Mirai groeide het afgelopen jaar onder zowel 32- als 64-bits x86 CPU-architecturen en de malware kreeg nieuwe mogelijkheden die snel werden overgenomen door actoren van vreemde mogendheden en criminele groepen. Aanvallen door actoren van vreemde mogendheden maken nu gebruik van nieuwe varianten van bestaande botnets in DDoS-aanvallen (Distributed Denial of Service) op buitenlandse tegenstanders.

Toen de inkomsten uit aanvallen op IoT-apparaten in 2022 daalden, zagen we dat verschillende groepen bedreigingsactoren misbruik maakten van kwetsbaarheden, zoals Log4j en Spring4Shell, om een schadelijke payload te leveren aan apparaten zoals servers, deze te infecteren en ze te rekruteren voor grote botnets die DDoS-aanvallen uitvoeren. Het vernieuwde gebruik van malware die is ontworpen om kwetsbare IoT-apparaten aan te vallen, heeft ernstige gevolgen voor zowel organisaties als landen, aangezien zijdelingse verplaatsing kan leiden tot blootstelling van achterdeuren aan extra payloads en andere apparaten op netwerken.

Veel protocollen voor industriële regelsystemen worden niet bewaakt en zijn daarom kwetsbaar voor OT-specifieke aanvallen. Dit kan leiden tot een verhoogd risico voor essentiële infrastructuur.

Relatieve prevalentie van gebruikersnaam- en wachtwoordparen waargenomen onder IoT/OT-apparaten in 45 dagen aan sensorsignalen



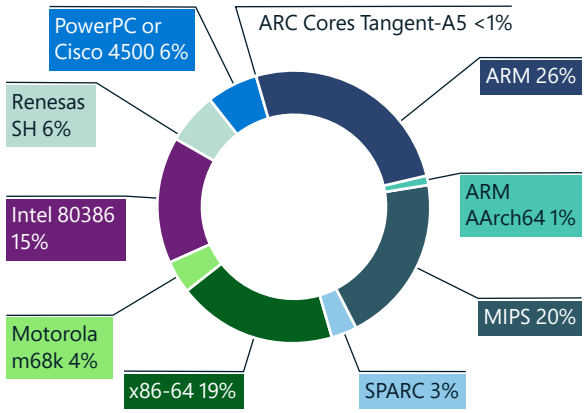
Het gebruik van veelvoorkomende gebruikersnaam- en wachtwoordparen verhoogt het risico op schending. Bij een steekproef onder meer dan 39 miljoen IoT- en OT-apparaten bleek dat ongeveer 20 procent gebruikmaakte van identieke gebruikersnamen en wachtwoorden.

IoT en OT blootgesteld: trends en aanvallen

Vervolg

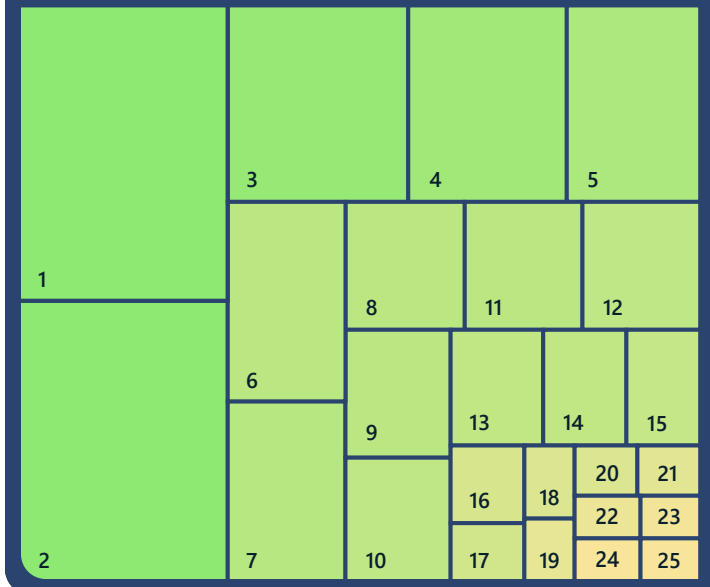
Hoewel zwakke configuraties en standaardreferenties nog steeds een risico vormen voor netwerken, heeft Microsoft veel webgebaseerde exploits waargenomen die HTTP gebruiken. We zagen deze toename van aanvallen op webgebaseerde services met behulp van legacy botnets. Ondertussen nam het aantal open telnet-poorten op internet af, een positief teken voor netwerkbeveiliging, aangezien botnets die een historisch risico vormden voor apparaten aan relevantie inboeten. Ondanks deze afname van open telnet-poorten, zagen we nog steeds hardnekkige botnets in sensornetwerken.

Distributie van IoT-malware per CPU-architectuur



Microsoft merkte op dat IoT-apparaten die op ARM worden uitgevoerd het vaakst het doelwit vormen van malware, gevolgd door MIPS, X86-64 en Intel 80386 CPU.

Prevalentie van protocollen voor industriële regelsystemen



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

Kwetsbaarheden van protocollen voor industriële regelsystemen

We hebben naar OT-data van onze met de cloud verbonden sensoren gekeken, waarbij de meest voorkomende protocollen voor industriële regelsystemen (ICS) werden onthuld. Deze protocollen bieden inzicht in de aard van deze apparaten en hun aanvalsoppervlak. Dit is vooral relevant voor de beveiliging van essentiële infrastructuur. Enkele belangrijke lessen zijn:

1. De meeste van de weergegeven protocollen zijn bedrijfseigen, zodat standaard IT-bewakingstools niet voldoende zicht hebben op de beveiliging van deze apparaten en protocollen. Als gevolg hiervan worden netwerken niet gecontroleerd en zijn ze daardoor kwetsbaarder voor OT-specifieke aanvallen.
2. Er is sprake van een grote verscheidenheid aan leverancierssspecifieke protocollen. Dit betekent dat leverancierspecifieke beveiligingsoplossingen niet in staat zullen zijn om op adequate wijze het hele netwerk af te dekken. Microsoft geeft prioriteit aan een leverancieronafhankelijke benadering om beveiligingsdekking te bieden voor de grote verscheidenheid aan verschillende apparaten.
3. Organisaties moeten ervoor zorgen dat deze protocollen niet rechtstreeks vanuit hun netwerken worden blootgesteld aan internet. Deze blootstelling kan een groot beveiligingsrisico vormen vanwege kwetsbaarheden en het onveilige karakter van deze protocollen.

Malware zoals Mirai blijft bestaan doordat er nieuwe mogelijkheden worden ontwikkeld en de malware wordt overgenomen door cybercriminaliteitsgroepen en actoren van vreemde mogendheden, waarbij gebruik wordt gemaakt van nieuwe varianten van bestaande botnets bij DDoS-aanvallen op buitenlandse tegenstanders.

Direct bruikbare inzichten

1. Zorg ervoor dat apparaten robuust zijn door patches toe te passen en standaardwachtwoorden en standaard SSH-poorten te wijzigen.
2. Verklein het aanvalsoppervlak door onnodige internetverbindingen en open poorten te elimineren, externe toegang te beperken door poorten te blokkeren, externe toegang te weigeren en VPN-services te gebruiken.
3. Gebruik een IoT/OT-aware NDR-oplossing (netwerkdetectie en -respons) en een SIEM- (Security Information and Event Management) of SOAR-oplossing (Security Orchestration and Response) om apparaten te controleren op afwijkend of onbevoegd gedrag, zoals communicatie met onbekende hosts.
4. Segmenteer netwerken om het vermogen van een aanvaller om zich zijdelings te verplaatsen en assets in gevaar te brengen na de eerste inbraak te beperken. IoT-apparaten en OT-netwerken moeten via firewalls van bedrijfs-IT-netwerken worden geïsoleerd.
5. Zorg ervoor dat ICS-protocollen niet rechtstreeks aan internet worden blootgesteld.

Supply chain en het hacken van firmware

Bijna elk apparaat met een internetverbinding heeft firmware. Dit is software die is ingebed in de hardware of printplaat van het apparaat. In de afgelopen paar jaar hebben we gezien dat firmware steeds meer wordt gericht op het lanceren van verwoestende aanvallen. Aangezien firmware waarschijnlijk een waardevol doelwit zal blijven voor bedreigingsactoren, moeten organisaties zich beschermen tegen het hacken van firmware.

Firmware is verantwoordelijk voor de primaire functies van een apparaat, zoals het maken van verbinding met een netwerk of het opslaan van data. Firmware is te vinden in routers, camera's, televisietoestellen en andere apparaten die worden gebruikt in ondernemingen (IoT), samen met industriële regelapparatuur (OT) die wordt gebruikt in essentiële infrastructuur. In het verleden werd firmware geschreven met onbeveiligde code, waardoor aanzienlijke kwetsbaarheden ontstonden die konden worden misbruikt om het apparaat over te nemen of schadelijke code in de firmware te injecteren.

Dit risico wordt nog vergroot als het gaat om de supply chain. De meeste apparaten zijn gebouwd met behulp van software- en hardwareonderdelen van verschillende fabrikanten en met open source-library's. In veel gevallen hebben apparaatoperators geen inzicht in de hardware- en softwarematerialiaallijst (H/SBOM) om het supply chain-risico van apparaten in hun netwerk te evalueren. In juni 2020 werden kwetsbaarheden onthuld in een netwerkstack die door veel verschillende fabrikanten wordt gebruikt en die honderden miljoenen IoT-apparaten in de consumenten- en industriële apparatuurruimte treft.[14] In sommige gevallen werd de netwerkstack omgedoopt door andere leveranciers en was er geen indicatie dat een apparaat kwetsbaar was. We zien een groeiende dreiging van kwaadwillende actoren die zich richten op deze software- en hardware-supply chain van IoT/OT-apparaten om organisaties binnen te dringen.

Het firmware-updateproces varieert sterk tussen apparaten, en de complexiteit en logistieke uitdaging om het uit te voeren, is van invloed op de updatefrequentie. Het is niet altijd mogelijk om te bepalen of een apparaat de nieuwste firmware gebruikt, waardoor het voor beveiligingsprofessionals moeilijk is om de beveiligingsstatus van hun IoT- en OT-apparaten te bewaken en te waarborgen. Bovendien hebben sommige apparaten firmware die niet cryptografisch is ondertekend, waardoor ze kunnen worden bijgewerkt zonder verificatie door de gebruiker. Deze zwakke punten stellen de apparaten verder bloot voor aanvallen op de supply chain in de hele productie- en distributieketen.

Om deze bedreigingen aan te pakken, investeert Microsoft aanzienlijk in het waarborgen van de veiligheid en integriteit van de firmware terwijl deze verschillende stadia van de supply chain doorloopt, en in het op elk moment bevestigen dat er niet mee is geknoeid tijdens inname of onderweg. Dit stelt ons in staat om het vertrouwen tussen elk pijplijnsegment te valideren en een gecertificeerde en aantoonbare end-to-end beheerketen (chain of custody) te bieden voor elk onderdeel dat we naar klanten verzenden. We werken samen met onze partners om deze chip-to-cloud-beveiliging naar alle apparaten in het ondernemings- en OT-netwerk te brengen.

"ICT-infrastructuurleveranciers zijn in toenemende mate doelwit omdat ze wijdverbreide replicatie van een enkele aanval mogelijk maken. Tegelijkertijd nemen de wereldwijde wet- en regelgeving en de vraag van klanten naar beveiliging en veerkracht van de supply chain toe, waarbij de vereisten vaak uiteenlopen.

De oplossing is partnerschap. Samen met leveranciers en wereldwijde overheden zet Microsoft zich in om de veiligheid in ons hele supply chain-ecosysteem aan te pakken en de vraag van zowel klanten als regelgevers te overtreffen. Om dit te doen, stimuleren we een alomvattende benadering van beveiliging en operationele veerkracht die flexibel wordt ingezet in de hele supply chain.

Het stimuleren van firmware-integriteit van ontwerp tot apparaatgebruik is de sleutel tot onze collectieve aanpak. Het waarborgen van de SDL-processen van leveranciers en het inzetten van hardwarematige root of trust-innovatie zijn voorbeelden van hoe we de integriteit van de supply chain kunnen 'inbouwen'.

Onze community maakt gebruik van collectief onderzoek en ontwikkeling met betrekking tot nieuwe anti-manipulatietechnieken en cryptografische mechanismen, gecombineerd met voortdurende bewaking en detectie van afwijkingen. Samen boeken we vooruitgang bij het tot een minimum beperken van de aantrekkingskracht van de supply chain als aanvalsoppervlak."

Edna Conway,
Vice President, Security & Risk Officer,
Cloud Infrastructure

Kwetsbaarheden in firmware in de schijnwerpers

Aanvallers maken in toenemende mate gebruik van kwetsbaarheden in de firmware van IoT-apparaten om bedrijfsnetwerken te infiltreren. In tegenstelling tot traditionele IT-endpoints die XDR-agents gebruiken om zwakke punten te identificeren, is identificatie van kwetsbaarheden binnen IoT/OT-apparaten veel ongrijpbaarder.

In een recent onderzoek dat werd uitgevoerd door Microsoft en het Ponemon Institute werden zowel de kansen als de beveiligingsuitdaging van IoT/OT-apparaten in een onderneming benadrukt.[15] Terwijl 68 procent van de respondenten gelooft dat de adoptie van IoT/OT cruciaal is voor hun strategische digitale transformatie, erkent 60 procent dat IoT/OT-beveiliging een van de minst beveiligde aspecten van de IT/OT-infrastructuur is.

Een voorbeeld van aanvallers die kwetsbaarheden in de firmware van IoT-apparaten gebruiken om een netwerk te infiltreren, is de Trickbot-trojan die gebruikmaakte van standaardwachtwoorden en kwetsbaarheden in Mikrotik-routers[16] om verdedigingssystemen van bedrijven te omzeilen. De fundamentele uitdaging met firmware voor IoT-apparaten is het gebrek aan inzicht in de beveiligingsstatus en kwetsbaarheden van apparaten.

Hoewel er oplossingen beschikbaar zijn om veilige apparaten te bouwen, zijn er al miljarden apparaten op de markt en in gebruik bij ondernemingen. Deze staan bekend als brownfield-apparaten. In 2021 nam Microsoft het bedrijf ReFirm Labs over om een licht te werpen op de beveiliging van brownfield-apparaten en apparaatbouwers in staat te stellen de beveiliging van hun producten te verbeteren. ReFirm Labs analyseert het binaire firmware-image van een apparaat en produceert een gedetailleerd rapport over mogelijke zwakke punten in de beveiliging.[17] Deze technologie wordt opgenomen in een toekomstige release van Microsoft Defender voor IoT.

In het afgelopen jaar hebben we de samengevoegde resultaten onderzocht van de unieke firmware die door onze klanten is gescand. Hoewel mogelijk niet elke ontdekte zwakte kan worden misbruikt, onderstrepen ze de fundamentele uitdaging van de beveiliging van apparaatfirmware.

Houd er rekening mee dat de typen zwakke punten die bestaan in IoT/OT-apparaten nooit acceptabel zouden zijn op traditionele Windows- of Linux-endpoints.

- Zwakke wachtwoorden: 27 procent van de gescande firmware-images bevatte accounts met wachtwoorden die waren gecodeerd met zwakke algoritmen (MD5/DES), die gemakkelijk door aanvallers kunnen worden gekraakt.

Beveiligingszwakheden in firmware-images geanalyseerd

- Bekende kwetsbaarheden: net als andere systemen werd in IoT/OT-apparaatfirmware uitgebreid gebruikgemaakt van open-sourcelibrary's. Apparaten worden echter vaak geleverd met verouderde versies van deze onderdelen. In onze analyse bevatte 32 procent van de images ten minste 10 bekende kwetsbaarheden (CVE's) die als kritiek werden beoordeeld (9,0 of hoger). Vier procent bevatte ten minste 10 kritieke kwetsbaarheden die meer dan zes jaar oud waren.
- Verlopen certificaten: certificaten worden gebruikt om verbindingen en identiteiten te verifiëren en om gevoelige data te beschermen, maar 13 procent van de geanalyseerde images bevatte ten minste 10 certificaten die meer dan drie jaar geleden waren verlopen.
- Softwareonderdelen: zesendertig procent van de images bevat softwareonderdelen. Microsoft raadt aan om deze uit te sluiten in IoT-apparaten zoals tools voor package-opname (tcpdump, libpcap), die kunnen worden gebruikt voor netwerkverkenning als onderdeel van een aanvalsketen.

Firmwareaanvallen in het wild

Viasat: een firmwarekwetsbaarheid gebruiken om satellietcommunicatie te targeten

In februari 2022 zorgde een incident met een satellietnetwerk ervoor dat een strategisch communicatienetwerk werd ontkoppeld met gevolgen voor heel Europa. Het KA-SAT-systeem van Viasat ontving een grote hoeveelheid verkeer waarbij veel modems werden losgekoppeld en er een denial-of-service-aanval op het netwerk werd gestart. Aangezien vast breedband werd verstoord, werden duizenden windturbines op afstand ontoegankelijk voor operators en werd schadelijke vernietigingsmalware ingezet tegen getroffen modems. De storing trof meer dan 30.000 satellietterminals die door bedrijven en organisaties worden gebruikt voor communicatie.

Cyclops Blink: een aanval op firmware in de supply chain om firewall-gateways aan te vallen

Voor bedreigingsactoren is de ontwikkeling en uitbreiding van command and control (C2) en aanvalsinfrastructuur een cruciaal onderdeel van succes. Naarmate de behoefte aan een stabiele C2-infrastructuur is gegroeid, zijn routers een populaire aanvalsvector geworden vanwege hun onregelmatige patching en het ontbreken van uitgebreide beveiligingsoplossingen.

Microsoft werkt samen met de overheid en de industrie op het gebied van firmware-analysetechnologie om meer inzicht te krijgen in apparaatbeveiliging en volledige levenscyclusbeveiliging te bieden voor apparaatbouwers en exploitanten.

Sinds juni 2019 gebruikte een aan de staat gelieerde APT-groep (Advanced Persistent Threat) de modulaire malware Cyclops Blink om kwetsbare WatchGuard-firewallapparaten en ASUS-routers aan te vallen door schadelijke firmware-updates uit te voeren en ze te werven voor een groot botnet. De malware infecteert apparaten met succes door gebruik te maken van een bekende kwetsbaarheid die een escalatie van bevoegdheden mogelijk maakt, waardoor de bedreigingsactoren het apparaat kunnen beheren. Eenmaal geïnfecteerd, maakt de malware het mogelijk om verdere modules te installeren en firmware-updates te omzeilen. Er zijn aangetaste apparaten waargenomen die verbinding maken met C2-servers die worden gehost op andere WatchGuard-apparaten. Door veel SSL-certificaten uit te geven voor hun C2 op verschillende TCP-poorten, kregen Cyclops Blink-operators externe toegang met bevoegdheden tot netwerken door schadelijke firmware-updates uit te voeren en traditionele beveiligingsmethoden zoals scannen te omzeilen.

Hoe Microsoft de beveiliging van de supply chain verbetert

Microsoft werkt samen met de overheid en de industrie om deze uitdagingen op het gebied van IoT- en OT-apparaatbeveiliging aan te pakken (zie de discussie op pagina 66). Onze bijdrage omvat het gebruik van firmware-analysetechnologie om apparaatexploitanten inzicht te bieden in de beveiligingsstatus van de apparaten op hun netwerk. Hierdoor kunnen klanten apparaten identificeren en prioriteren die extra bescherming, upgrades of vervanging nodig hebben, terwijl bovendien de vraag naar apparaatbouwers om te investeren in apparaatbeveiliging wordt gestimuleerd. Tegelijkertijd ondersteunen we bouwers met uitgebreide oplossingen om veilige apparaten te ontwerpen en veilige ontwikkelingslevenscycli aan te nemen.

Een ander belangrijk onderdeel is het bieden van een robuuste infrastructuur voor bouwers en exploitanten waarmee apparaatfirmware kan worden bijgewerkt wanneer beveiligingsproblemen worden ontdekt en opgelost. Microsoft combineert firmware-analyse en Defender voor IoT met Device Update for IoT Hub om een oplossing te bieden voor de volledige levenscyclus van IoT- en OT-apparaatbeveiliging. Dit zijn belangrijke stappen bij het realiseren van onze visie voor klanten om de infrastructuur te beveiligen door apparaten te gebruiken die een Zero Trust-benadering van hun IoT- en OT-oplossingen ondersteunen.[18]

Aanvallers richten zich in toenemende mate op kwetsbaarheden in de firmware van IoT-apparaten om bedrijfsnetwerken te infiltreren.

Direct bruikbare inzichten

1. Krijg meer inzicht in IoT/OT-apparaten in je netwerk en geef prioriteit aan risico's voor de onderneming als ze worden gecompromitteerd.
2. Gebruik tools voor het scannen van firmware om potentiële beveiligingszwakheden te begrijpen en werk samen met leveranciers om te bepalen hoe de risico's voor apparaten met een hoog risico kunnen worden beperkt.
3. Beïnvloed de beveiliging van IoT/OT-apparaten op positieve wijze door te eisen dat je leveranciers best practices van de levenscyclus voor veilige ontwikkeling invoeren.

Links naar verdere informatie

- Evaluatie van de essentiële supply chains die de Amerikaanse informatie- en communicatietechnologie-industrie ondersteunen

Op verkenning gebaseerde OT-aanvallen

Complexe supply chains gebruiken specifieke ontwerpinformatie om het eigenlijke systeem te plannen. Van de talloze assets waaruit deze ontwerpinformatie is samengesteld, is de meest gevoelige het projectbestand, dat de omgeving en zijn assets definieert. Dit bestand is een cruciaal strategisch doelwit voor bedreigingsactoren die toegang willen krijgen tot en een succesvolle aanval willen uitvoeren die volledig is afgestemd op de omgeving.

Het aanvallen van industriële systemen om operationele processen te verstoren, omvat twee stappen.

1. Eerst moet de aanvaller toegang krijgen tot het OT-netwerk. Dit kan worden gedaan door via IoT-apparaten aan de bedrijfskant van het netwerk (Purdue Model Level 4) binnen te dringen en de IT-OT-grens te overschrijden, die traditioneel wordt gescheiden door firewalls en netwerkapparatuur, naar de bedienings- en controleniveaus.
2. Ten tweede moeten de netwerkapparaten worden geïdentificeerd. Industriële systemen gebruiken standaard apparaten en onderdelen in aangepaste architecturen die specifiek zijn ontworpen voor hun omgeving. Een van deze standaardapparaten is de programmeerbare logische controller (PLC). Elke fabrikant ontwikkelt unieke interfaces en functies voor hun PLC's, die een essentieel onderdeel vormen van industriële systemen, en deze apparaten worden verder geconfigureerd met aangepaste schema's die specifiek zijn ontworpen voor de omgevingen van de klant.

De unieke configuratie van elke PLC wordt beschreven in het projectbestand, dat de definitie van de omgeving en zijn assets, de ladderlogica en meer bevat.

In de meeste omgevingen die tekenen van een aanval vertonen, blijkt uit analyse dat de voorbereidingen voor de aanval ver vóór de aanval zelf beginnen. Bedreigingsactoren investeren vaak maanden in het op afstand simuleren van de omgeving en haar assets, waarbij ze vele pogingen doen om een model te bouwen en hun gerichte aanval voor te bereiden. Omdat omgevingen voortdurend veranderen en nieuwe apparaten integreren, ontstaan er kwetsbaarheden specifiek rond de data in de project- en configuratiebestanden. De diefstal van een projectbestand kan een aanval weken of maanden vervroegen en aanvallers in staat stellen de doelomgeving snel en nauwkeurig te modelleren, waardoor het moeilijker wordt om schadelijke activiteiten te detecteren.

Industroyer en Incontroller

We hebben een toenemend aantal aanvallen met modulaire malware en aanvalsframeworks waargenomen op organisaties, essentiële infrastructuur en overheidsdoelen door actoren die door vreemde mogendheden worden gesponsord. Nieuwe pogingen om essentiële activiteiten in Oekraïne te verstoren, onderstrepen de groeiende dreiging van op verkenning gebaseerde OT-aanvallen die sterk zijn afgestemd op hun doelomgevingen. De uitgebreide verkennings- en onderzoeksfasen die worden uitgevoerd door cyberactoren van vreemde mogendheden wijzen op een strategie om cyberoorlogvoering te gebruiken om de infrastructuur op afstand te verlammen om specifieke strategische of operationele doelen te bereiken in een combinatie van Cyber- kinetische activiteiten en politieke strategie.

We hebben een groeiende dreiging waargenomen van op verkenning gebaseerde OT-aanvallen die sterk zijn afgestemd op hun doelomgevingen.

Op verkenning gebaseerde OT-aanvallen

Vervolg

Begin 2022 werden twee aanpasbare kritieke OT-aanvallen geïdentificeerd. Een cyberfysieke aanval op elektrische substations en beveiligingsrelais in Oekraïne werd uitgevoerd met aangepaste malware, waaronder een variant van Industroyer, een malware waarvan bekend is dat deze na de implementatie in 2016 stroomuitval in Oekraïne heeft veroorzaakt.

Industroyer2 is de eerste bekende herimplementatie van schadelijke OT-aanvalmalware op een nieuw doelwit. Hierbij werd gebruikgemaakt van het IEC104-protocol (standaardprotocol voor bewaking en besturing van elektriciteitssystemen) dat is ontwikkeld voor Industroyer en was gericht op voornamelijk PLC-achtige externe terminalunits met modelnummer ABB RTU540/560. De schrijver van deze malware gebruikte kennis van de omgeving van het slachtoffer om herhaaldelijk opdrachten te geven aan vooraf bepaalde uitgangen, zodat ze niet handmatig konden worden ingeschakeld. Dit zorgde voor langdurige stroomuitval en grotere schade.

Incontroller, een modulair aanvalsframework dat in dezelfde periode werd geïdentificeerd, is een modulaire toolkit die de doorlooptijd voor het penetreren en aanvallen van OT-apparaten aanzienlijk verkort, waarbij legacy-beveiligingsoplossingen worden omzeild. De toolkit voor algemene doeleinden beschikt over mogelijkheden voor dataverzameling, verkenning en aanval die in hoge mate kunnen worden aangepast aan verschillende omgevingen en die een grote invloed kunnen hebben op de onderzoeksfase voor een OT-aanval. Hierdoor wordt de tijd die nodig is om verkenningen uit te voeren, verminderd en wordt de simulatie van omgevingen ondersteund door informatie te extraheren over apparaten en hun configuraties.

Het Incontroller-framework ondersteunt protocollen voor PLC's van Schneider Electric en Omron en verzamelt informatie, zoals firmwareversie, modeltype en aangesloten apparaten. De toolkit kan opdrachten geven om configuraties te wijzigen en uitgangen in en uit te schakelen. Zodra een omgeving is geopend, ondersteunt het framework het implanteren van backdoors in apparaten voor de levering van meer payloads, het uitgeven van kwetsbaarheden om toegangspunten te vergroten, het uploaden van ladderlogica en de mogelijkheid om DoS-aanvallen te initiëren. Het generieke karakter van de toolkit stelt een bedreigingsactor in staat om snel een omgeving aan te vallen zonder voor elke PLC of locatie nieuwe aanvallen te hoeven schrijven. Hierdoor kan de actor gemakkelijk communiceren met verschillende typen machines die in potentie zijn verspreid over vele verschillende industrieën.

Direct bruikbare inzichten

1. Vermijd het overbrengen van bestanden die systeemdefinities bevatten via onbeveiligde kanalen of naar niet-essentieel personeel.
2. Als het overzetten van dergelijke bestanden onvermijdelijk is, moet je de activiteit op het netwerk in de gaten houden en ervoor zorgen dat de assets veilig zijn.
3. Bescherm technische stations door bewaking met EDR-oplossingen.
4. Voer op proactieve wijze incidentrespons uit voor OT-netwerken.
5. Implementeer continue bewaking, zoals Defender for IoT.

Eindnoten

1. Zie bijv. Herziene richtlijn betreffende de beveiliging van netwerk- en informatiesystemen (NIS2) | De digitale toekomst van Europa vormgeven (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Wijziging veiligheidswetgeving (bescherming van essentiële infrastructuur) Act 2022 (homeaffairs.gov.au); Chili: wetsvoorstel voor cyberbeveiliging en kritieke informatie-infrastructuur geïntroduceerd in Senaat | Nieuwsbericht | Databegeleiding; Japan neemt economische veiligheidswet aan om gevoelige technologie te bewaken | The Japan Times; Herziening van de Cybersecurity Act en update van de Cybersecurity Code of Practice voor CII's (csa.gov.sg); Voorstel voor wetgeving om de cyberverkracht van het VK te verbeteren - GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updaten van het NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In—Startpagina
3. Start van overleg over invoering van meldplicht voor cyberaanvallen (admin.ch)
4. Zie bijv. zonder titel (house.gov)
5. Cyber Resilience Act | De digitale toekomst van Europa vormgeven (europa.eu)
6. Zie bijv. Microsoft Security Development Lifecycle
7. Zie bijvoorbeeld Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft; zie ook bijvoorbeeld The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Zie bijv. https://www.microsoft.com/en-us/msrc/cvd
9. De Product Security and Telecommunications Infrastructure (PSTI) Bill—factsheet over productbeveiliging—GOV.UK (www.gov.uk)
10. Commissie versterkt cyberbeveiliging van draadloze apparaten en producten (europa.eu)
11. Cloudcertificeringssysteem: bouwen van vertrouwde cloudservices in heel Europa — ENISA (europa.eu)
12. Certificering — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool"GitHub - microsoft/sbom-tool: De SBOM-tool is een zeer schaalbare en bedrijfsklare tool om SPDX 2.2-compatibele SBOM's te maken voor een verscheidenheid aan artefacten.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. IoT/OT Innovation Critical but Comes with Significant Risks (december 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. Uncovering Trickbot's use of IoT devices in C2 Infrastructure (maart 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. Aflevering van IoT Show op Channel 9 over het scannen van IoT-firmware (mei 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. How to apply a Zero Trust approach to your IoT solutions (mei 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Cyberbeïnvloedings-activiteiten

De activiteiten voor buitenlandse beïnvloeding van vandaag maken gebruik van nieuwe methoden en technologieën, waardoor hun campagnes die zijn ontworpen om het vertrouwen te ondermijnen, efficiënter en effectiever worden.

Een overzicht van

cyberbeïnvloedings-activiteiten

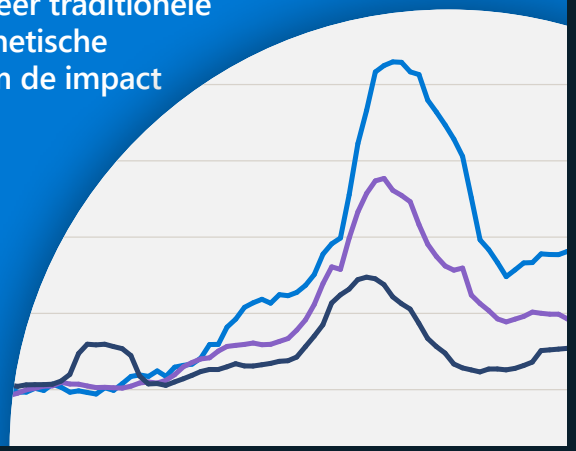
De activiteiten voor buitenlandse beïnvloeding van vandaag maken gebruik van nieuwe methoden en technologieën, waardoor hun campagnes die zijn ontworpen om het vertrouwen te ondermijnen, efficiënter en effectiever worden.

Vreemde mogendheden maken steeds vaker gebruik van geavanceerde beïnvloedingsactiviteiten om propaganda te verspreiden en invloed uit te oefenen op de publieke opinie, zowel nationaal als internationaal. Deze campagnes tasten het vertrouwen aan, vergroten de polarisatie en bedreigen democratische processen. Deskundige geschoolde hardnekkige manipulators gebruiken traditionele media samen met internet en sociale media om de reikwijdte, schaal en efficiëntie van hun campagnes en de grote impact die deze hebben op het wereldwijde informatie-ecosysteem enorm te vergroten. In het afgelopen jaar hebben we gezien dat deze activiteiten werden gebruikt als onderdeel van de hybride oorlog in Rusland in Oekraïne, maar we zagen ook dat Rusland en andere landen, waaronder China en Iran, in toenemende mate propagandamaatregelen via sociale media inzetten om hun wereldwijde invloed uit te breiden.

Cyberbeïnvloedingsactiviteiten worden steeds geavanceerder naarmate meer regeringen en vreemde mogendheden deze activiteiten gebruiken om meningen te vormen, tegenstanders in diskrediet te brengen en onenigheid te bevorderen.

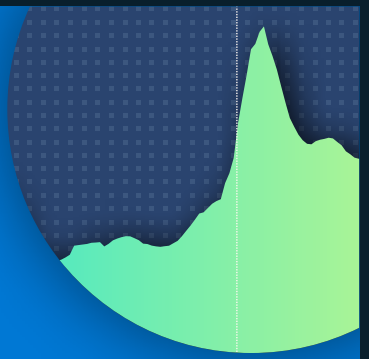
Ga voor meer informatie naar p74

Tijdens de Russische invasie van Oekraïne vonden cyberbeïnvloedingsactiviteiten plaats in combinatie met meer traditionele cyberaanvallen en kinetische militaire operaties om de impact te maximaliseren.



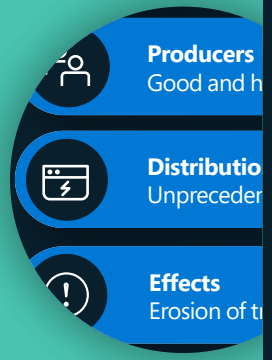
Ga voor meer informatie naar p76

Rusland, Iran en China gebruikten tijdens de COVID-19-pandemie vaak propaganda- en beïnvloedingscampagnes als een strategisch middel om bredere politieke doelstellingen te bereiken.



Ga voor meer informatie naar p76

Synthetische media komen steeds vaker voor vanwege de toename van tools waarmee gemakkelijk zeer realistische kunstmatige afbeeldingen, video's en audio kunnen worden gemaakt en verspreid. Digitale herkomsttechnologie die de oorsprong van media-assets certificeert, belooft misbruik te bestrijden.



Ga voor meer informatie naar p80

Een holistische aanpak voor bescherming tegen cyberbeïnvloedingsactiviteiten

Microsoft bouwt voort op zijn reeds volwassen infrastructuur voor cyberbedreigingsinformatie om cyberbeïnvloedingsactiviteiten te bestrijden. Onze strategie is om propagandacampagnes van buitenlandse agressors op te sporen en te verstoren, hier bescherming tegen te bieden en ze te ontmoedigen.

Ga voor meer informatie naar p83

Inleiding

Democratie heeft betrouwbare informatie nodig om te floreren. Een cruciaal aandachtsgebied voor Microsoft zijn de beïnvloedingsactiviteiten die worden ontwikkeld en bestendigd door vreemde mogendheden. Deze campagnes tasten het vertrouwen aan, vergroten de polarisatie en bedreigen democratische processen.

Buitenlandse beïnvloedingsactiviteiten zijn altijd een bedreiging geweest voor het informatie-ecosysteem. Wat echter verschilt in het tijdperk van internet en sociale media, is de enorm toegenomen reikwijdte, schaal en efficiëntie van campagnes en de buitensporige impact die deze kunnen hebben op de gezondheid van het wereldwijde informatie-ecosysteem.

Het eeuwenoude gezegde dat "een leugen de halve wereld bereikt voordat de waarheid de kans krijgt om haar schoenen aan te trekken", wordt nu bevestigd met data. Een onderzoek van het Massachusetts Institute of Technology (MIT)[1] stelde vast dat onwaarheden 70 procent meer kans hebben om te worden geretweet dan de waarheid en dat ze de eerste 1500 mensen zes keer sneller bereiken. Het informatie-ecosysteem is steeds troebeler geworden doordat propagandacampagnes op internet en sociale media floreren en het vertrouwen in traditioneel nieuws ondermijnen. In een studie uit 2021[2] gaf slechts zeven procent van de volwassenen in de VS aan "veel" vertrouwen te hebben in kranten, televisie- en radioverslaggeving, terwijl 34 procent zei "helemaal geen" vertrouwen te hebben.

Microsoft heeft gewerkt aan het identificeren van de belangrijkste actoren, bedreigingen en tactieken in de buitenlandse cyberbeïnvloedingsruimte en om geleerde lessen te delen. In juni van dit jaar hebben we een uitgebreid rapport gepubliceerd over de lessen die we uit Oekraïne hebben getrokken, met een gedetailleerd overzicht van de Russische cyberbeïnvloedingsactiviteiten.[3]

We onderzoeken ook hoe geavanceerde technologieën, zoals deep fakes (diepe vervalsingen), als wapen kunnen worden gebruikt en de geloofwaardigheid van journalisten kunnen ondermijnen. En we werken samen met de industrie, de overheid en de academische wereld om betere manieren te ontwikkelen om synthetische media te detecteren en het vertrouwen te herstellen, zoals systemen voor kunstmatige intelligentie (AI) die vervalsingen kunnen herkennen.

De snel veranderende aard van het informatie-ecosysteem en de online propaganda van vreemde mogendheden, inclusief de versmelting van traditionele cyberaanvallen met beïnvloedingsactiviteiten en de inmenging in democratische verkiezingen, vereist een benadering van de hele samenleving om zowel online als offline bedreigingen voor de democratie te verminderen.

Microsoft zet zich in voor het ondersteunen van een gezond informatie-ecosysteem waarin vertrouwd nieuws en informatie gedijen. We ontwikkelen tools en mogelijkheden voor het detecteren van bedreigingen om het zich ontwikkelende en groeiende risico van door vreemde mogendheden aangestuurde beïnvloedingsactiviteiten tegen te gaan. Om dit werk mogelijk te maken, hebben we onlangs Miburo Solutions overgenomen, werken we samen met externe validators zoals de Global Disinformation Index en NewsGuard, en nemen we deel aan en leiden we soms partnerschappen met meerdere stakeholders, waaronder de Coalition for Content Provenance and Authenticity (C2PA). Alleen door samen te werken kunnen we erin slagen om diegenen aan te pakken die democratische processen en instellingen willen ondermijnen.

Teresa Hutson

Vice President, Technology
and Corporate Responsibility

Trends in cyberbeïnvloedings-activiteiten

Cyberbeïnvloedingsactiviteiten worden steeds geavanceerder naarmate de technologie zich in hoog tempo ontwikkelt. Bij cyberbeïnvloedingsactiviteiten zien een overlapping met en uitbreiding van de tools die worden ingezet bij traditionele cyberaanvallen. Daarnaast zien we een toegenomen coördinatie en versterking onder vreemde mogendheden.

Microsoft heeft dit jaar geïnvesteerd in het bestrijden van buitenlandse beïnvloedingsactiviteiten door de overname van Miburo Solutions, een bedrijf dat is gespecialiseerd in de analyse van buitenlandse beïnvloedingsoperaties. Microsoft heeft deze analisten gecombineerd met de bedreigingscontextanalisten van Microsoft en daarbij het Digital Threat Analysis Center (DTAC) opgericht. DTAC analyseert en rapporteert over bedreigingen van vreemde mogendheden, waaronder zowel cyberaanvallen als beïnvloedingsactiviteiten, waarbij informatie en bedreigingsintelligentie worden gecombineerd met geopolitieke analyse om inzichten te verschaffen en effectieve respons en bescherming te bieden.

Meer dan driekwart van de mensen over de hele wereld zei zich zorgen te maken over het tot wapen maken van informatie,[4] en onze data ondersteunt deze zorgen. Microsoft en haar partners hebben bijgehouden hoe actoren van vreemde mogendheden beïnvloedingsactiviteiten gebruiken om hun strategische en politieke doelen te realiseren. Naast destructieve cyberaanvallen en cyberspionage-inspanningen, gebruiken autoritaire regimes steeds vaker cyberbeïnvloedingsactiviteiten om meningen te vormen, tegenstanders in diskrediet te brengen, angst aan te wakkeren, onenigheid te bevorderen en de realiteit te vervormen.

Deze buitenlandse cyberbeïnvloedings-activiteiten hebben doorgaans drie fasen:

Positionering vooraf

Net als bij het vooraf positioneren van malware binnen het computernetwerk van een organisatie, worden bij buitenlandse cyberbeïnvloedingsactiviteiten valse verhalen in het publieke domein op internet geplaatst. De tactiek van vooraf positioneren heeft lang geholpen bij meer traditionele cyberactiviteiten, vooral als IT-beheerders hun meest recente netwerkactiviteit scannen. Malware die gedurende een langere tijd op een netwerk sluimert, kan het latere gebruik ervan effectiever maken. Valse verhalen die onopgemerkt blijven op internet, kunnen latere verwijzingen geloofwaardiger maken.

Lancering

Vaak wordt, op het moment dat het meest gunstig is om de doelen van de actor te bereiken, een gecoördineerde campagne gelanceerd om verhalen te verspreiden via door de overheid gesteunde en beïnvloede media en kanalen in de sociale media.

Versterking

Tot slot versterken door de staat gecontroleerde media en gevolmachtigden de verhalen binnen beoogde doelgroepen. Vaak vergroten onwetende tech-enablers het bereik van de verhalen. Online adverteren kan bijvoorbeeld helpen bij het financieren van activiteiten, terwijl gecoördineerde systemen voor het leveren van content zoekmachines kunnen overspoelen.

Deze benadering in drie stappen werd eind 2021 toegepast om het Russische valse verhaal rond vermeende biowapens en biolabs in Oekraïne te ondersteunen. Dit verhaal werd op 29 november 2021 voor het eerst geüpload naar YouTube als onderdeel van een regulier Engelstalig programma door een in Moskou gevestigde Amerikaanse expat die beweerde dat door de VS gefinancierde biolabs in Oekraïne verbonden waren met biowapens. Het verhaal bleef maandenlang grotendeels onopgemerkt. Op 24 februari 2022, net toen Russische tanks de grens overstaken, werd het verhaal het strijdperk ingestuurd. Een data-analyseteam van Microsoft identificeerde 10 door Rusland gecontroleerde of beïnvloede nieuwssites die op 24 februari gelijktijdig rapporten publiceerden die terugverwezen naar "het rapport van vorig jaar" en probeerden het geloofwaardig te maken. Bovendien hielden functionarissen van het Russische ministerie van Buitenlandse Zaken persconferenties waarop de valse beweringen over Amerikaanse biolabs verder werden verspreid in de informatieomgeving. Door Rusland gesponsorde teams verrichtten vervolgens inspanningen om het verhaal breder te versterken op sociale media en internetsites.

We zien autoritaire regimes over de hele wereld samenwerken om het informatie-ecosysteem in hun wederzijds voordeel te vervuilen. Bijvoorbeeld, tijdens de COVID-19-pandemie gebruikten Rusland, Iran en China propaganda en beïnvloedingsactiviteiten met behulp van een mix van openlijke, semi-geheime en geheime verspreidingsmethoden om democratieën aan te vallen en verdere geopolitieke doelen te realiseren (verder besproken op pagina 76). De drie regimes borduurden voort op elkaars berichten- en informatie-ecosystemen om voorkeursverhalen te promoten. Veel van deze berichtgeving bestond uit kritiek of samenzweringstheorieën over de Verenigde Staten en hun bondgenoten die door regeringsfiguren in officiële verklaringen naar buiten werden gebracht, terwijl ze hun eigen vaccins en reacties op COVID-19 promootten als superieur aan die van de Verenigde Staten en andere democratieën. Door elkaar te versterken, creëerden door de staat beheerde mediakanalen een ecosysteem waarin negatieve berichtgeving over democratieën, of positieve berichtgeving over Rusland, Iran en China, die door het ene staatsmediakanaal was geproduceerd door anderen werd versterkt.

Illustratie van hoe verhalen over Amerikaanse biolabs en biologische wapens zich verspreidden via de drie brede fasen van veel buitenlandse beïnvloedingsactiviteiten: positionering vooraf, lancering en versterking.

Trends in cyberbeïnvloedingsactiviteiten

Vervolg

Om de uitdaging nog groter te maken, is het denkbaar dat deze campagnes onbewust mogelijk worden gemaakt door technologie-entiteiten uit de particuliere sector. Enablers kunnen bedrijven zijn die internetdomeinen registreren, websites hosten, materiaal promoten op sociale media en zoeksites, verkeer kanaliseren en deze oefeningen helpen betalen via digitale advertenties. Organisaties moeten op de hoogte zijn van de tools en methoden die door autoritaire regimes worden gebruikt voor cyberbeïnvloedingsactiviteiten, zodat ze de verspreiding van campagnes kunnen detecteren en vervolgens kunnen voorkomen. Er is ook een groeiende behoefte om consumenten te helpen een geavanceerder vermogen te ontwikkelen om buitenlandse beïnvloedingsactiviteiten te identificeren en de betrokkenheid bij hun verhalen of content te beperken.

Cyberbeïnvloedingsactiviteiten, inclusief autoritaire propaganda, vormen een bedreiging voor democratieën over de hele wereld omdat ze het vertrouwen aantasten, de polarisatie vergroten en democratische processen bedreigen.

Meer coördinatie en informatie-uitwisseling tussen de overheid, de particuliere sector en maatschappelijke organisaties is nodig om de transparantie te vergroten en deze beïnvloedingscampagnes aan het licht te brengen en te verstoren.

Wereldwijd maakt meer dan driekwart van de mensen zich zorgen over de manier waarop informatie als wapen wordt ingezet.

Aandacht voor beïnvloedingsactiviteiten tijdens COVID-19 en de invasie van Rusland in Oekraïne

Vreemde mogendheden die de informatieomgeving tijdens de pandemie en tijdens de Russische invasie van Oekraïne willen beheersen, bieden grimmige voorbeelden van hoe autoritaire regimes Cyber- en informatieactiviteiten combineren.

COVID-19-propaganda

Rusland, Iran en China hebben gedurende de COVID-19-pandemie propaganda- en beïnvloedingscampagnes gevoerd. Op twee centrale manieren was COVID-19 prominent aanwezig in deze campagnes:

1. Beweringen over de pandemie zelf.
2. Campagnes die COVID-19 gebruikten als strategisch middel om bredere politieke doelstellingen te verwezenlijken.

Het algemene doel van dit soort campagnes is tweeledig. Ten eerste proberen zij democratieën, democratische instellingen en het imago van de Verenigde Staten en hun bondgenoten op het wereldtoneel te ondermijnen en ten tweede ondernemen zij pogingen om hun eigen positie in binnen- en buitenland te versterken.

Een voorbeeld hiervan is te zien in de berichten van bekende Russische accounts en mediaorganisaties die zich richten op Engelstalige lezers, versus hoe de Russische regering met haar eigen mensen communiceerde over het vaccin en de ernst van COVID-19.

Onderwerpen die aan bod kwamen in de 10 meest bekeken coronavirusverhalen op RT.com
(oktober 2021–april 2022)

Antivaccinatiepropaganda richt zich op niet-Russische lezers

Russisch (Hieronder vertaald naar het Engels)	Engels
'Lockdowns en boosters voorkomen overdracht'	'Vaccinaties remmen de overdracht niet af en zijn niet effectief tegen nieuwe varianten'
'Russische publieke figuren testen positief'	'Pfizer-vaccin heeft gevaarlijke bijwerkingen'
'Besmettingen en sterfgevallen nemen toe in Rusland'	'Massavaccinatie is politiek gemotiveerd'
'Het Spoetnik V-vaccin is zeer effectief'	'Pfizer en Moderna voeren ongereguleerde proeven uit'
'Vaccinbewijs nodig in openbaar vervoer'	

Russische COVID-19-berichten verschillen per taal.

Campagnes die de oorsprong van het COVID-19-virus probeerden te verdoezelen, vormen een ander voorbeeld. Sinds het begin van de pandemie heeft de Russische, Iraanse en Chinese COVID-19-propaganda de berichtgeving van de anderen gebruikt om deze centrale thema's te versterken. Veel van deze berichtgeving bestond uit het promoten van kritiek of complottheorieën over de Verenigde Staten. Door elkaar regelmatig te versterken, ontwikkelden door de staat beheerde mediakanalen een ecosysteem waarin negatieve berichtgeving over democratieën of positieve berichtgeving over Rusland, Iran en China die door het ene staatsmediakanaal was geproduceerd steeds opnieuw door de anderen werd versterkt.

Een voorbeeld hiervan is de vroege suggestie van Russische en Iraanse staatsmedia dat COVID-19 een door de Verenigde Staten vervaardigd biowapen zou kunnen zijn. Deze bewering circuleerde vroeg in de pandemie op marginale samenzweringswebsites na een interview met een professor in de rechten die beweerde dat hij geloofde dat COVID-19 als wapen was gemaakt.[6] Nadat het interview op enkele websites met een beperkt bereik was gepubliceerd, werd het verhaal opgepikt door staatsmedia. PressTV, een Engels- en Franstalig Iraans mediakanaal dat wordt gesponsord door de Iraanse regering,[7] publiceerde in februari 2020 een Engelstalig verhaal met de titel "Is coronavirus a US biowarfare weapon as Francis Boyle believes?" (Is coronavirus een Amerikaans wapen voor biologische oorlogsvoering zoals Francis Boyle gelooft?) In het artikel, waarin werd gesuggereerd dat de Verenigde Staten achter de COVID-19-uitbraak zaten, werd gezegd: "in alle Amerikaanse oorlogen worden radiologische, chemische, biologische en andere verboden wapens ingezet, wat een verwoestende tol eist van mensen in getroffen gebieden."[8] Dit werd beaamd door Russische staatsmedia en Chinese regeringsaccounts. Russia Today (RT), een staatsbedrijf dat bekend staat om zijn rol bij de verspreiding van propaganda voor het Kremlin,[9] publiceerde ten minste één verhaal waarin verklaringen van Iraanse functionarissen werden gepromoot die beweerden dat COVID-19 een "product zou kunnen zijn van een Amerikaanse 'biologische aanval' die was gericht op Iran en China"[10] en brachten berichten op sociale media naar buiten waarin hetzelfde werd gesuggereerd. Een RT-tweet van 27 februari 2020 luidde bijvoorbeeld: "Steek je hand op als je niet verbaasd zou zijn als ooit wordt onthuld dat #coronavirus een biowapen is?"[11]

De oorlog in Oekraïne: propaganda als oorlogswapen

De Russische invasie van Oekraïne is een duidelijk voorbeeld van hoe cyberbeïnvloedingsactiviteiten kunnen worden versmolten met meer traditionele cyberaanvallen en militaire operaties op de grond om hun impact te maximaliseren.

In de aanloop naar de invasie van Oekraïne zagen Microsoft-analisten van bedreigingsinformatie dat ten minste zes afzonderlijke, aan Rusland gelieerde actoren meer dan 237 cyberaanvallen tegen Oekraïne lanceerden. Deze campagnes waren bedoeld om diensten en instellingen aan te tasten, de toegang van Oekraïners tot betrouwbare informatie te verstoren en twijfel te zaaien over het leiderschap van het land.

Aandacht voor beïnvloedingsactiviteiten tijdens COVID-19 en de invasie van Rusland in Oekraïne

Vervolg

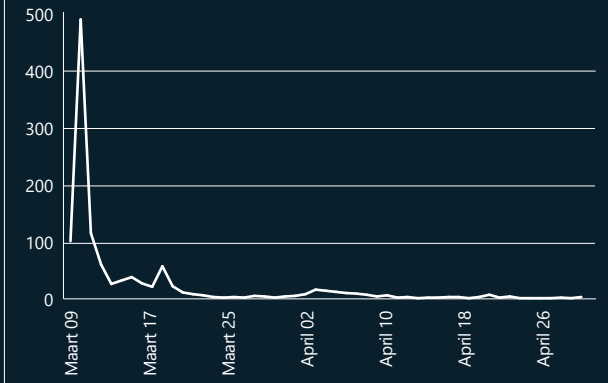
In een Microsoft-rapport dat in april 2022 werd uitgebracht, lieten we zien hoe Rusland, in een klaarblijkelijke poging om de informatieomgeving in Kiev te controleren, een raketaanval lanceerde op een tv-toren in Kiev op dezelfde dag dat het een vernietigende malware-aanval lanceerde tegen een groot Oekraïens mediabedrijf.[12]

In een ander voorbeeld van hoe cyberaanvallen en beïnvloedingsactiviteiten samenkomen, stuurde een Russische dreigingsactor Oekraïense burgers e-mails die zogenaamd afkomstig waren van inwoners van Mariupol, waarbij hij de Oekraïense regering de schuld gaf van de escalatie van de oorlog en hun landgenoten opriep om tegengas te geven aan de regering. Deze e-mails waren specifiek geadresseerd (op naam) aan degenen die de e-mail ontvingen, wat aangeeft dat hun informatie mogelijk is gestolen tijdens een eerdere spionagegerelateerde cyberaanval. Er waren geen schadelijke links opgenomen, wat suggereert dat het puur de bedoeling was om de opinie van de geadresseerden te beïnvloeden.

Het tonen van zogenaamd gehackt, gelekt of anderszins gevoelig materiaal is een veelvoorkomende tactiek die wordt gebruikt door Russische actoren bij beïnvloedingsactiviteiten. Gedurende de oorlog in Oekraïne hebben pro-Russische sociale mediakanalen gepromoot wat volgens hen gelekt of anderszins gevoelig materiaal uit Oekraïense bronnen was. Gelekt of gevoelig materiaal wordt gebruikt door pro-Russische sociale mediakanalen en -outlets als onderdeel van een bredere beïnvloedingsstrategie om het vertrouwen in instellingen aan te tasten en mainstream verhalen in twijfel te trekken. Deze informatie kan worden gemanipuleerd om op Oekraïne en het Westen gerichte propaganda te creëren, het vertrouwen in digitale veiligheid te ondermijnen en de steun voor westerse hulp aan Oekraïne uit te hollen.

Rusland gebruikte andere informatie-aanvallen om de publieke opinie vorm te geven na gebeurtenissen ter plaatse om feiten te verdoezelen of te ondermijnen. Op 7 maart heeft Rusland bijvoorbeeld een verhaal vooraf gepositioneerd door middel van een melding aan de Verenigde Naties (VN) dat een kraamkliniek in Mariupol, Oekraïne, was ontruimd en werd gebruikt als militair terrein. Op 9 maart bombardeerde Rusland het ziekenhuis. Nadat het nieuws over de bomaanslag bekend werd, tweette de Russische VN-vertegenwoordiger Dmitry Polyanskiy dat de berichtgeving over de bomaanslag "nepnieuws" was en haalde hij eerdere beweringen van Rusland aan over het vermeende gebruik ervan als militair terrein. Rusland verspreidde dit verhaal vervolgens gedurende twee weken na de aanval op het ziekenhuis op grote schaal via door Rusland gecontroleerde websites.

Domeinen met verkeer
(9 maart 2022 – 30 april 2022)



Propagandawebsites publiceerden ongeveer twee weken lang verhalen over de kraamkliniek met een korte opleving die begon op 1 april 2022. Bron: Microsoft AI for Good Lab.

Satellietbeelden van een perinataal ziekenhuis in Mariupol in februari en maart 2022

De eigen satellietbeeldanalyse van Microsoft toonde aan dat het perinatale ziekenhuis was gebombardeerd. De eerste foto is van 24 februari 2022 en de tweede van 24 maart 2022. Bron foto: Planet Labs.

Het witwassen van Russische wreedheden ging door naarmate de oorlog vorderde. Eind juni 2022 schilderden Russische media en influencers bijvoorbeeld de bombardementen op een winkelcentrum af als gerechtvaardigd en noodzakelijk, waarbij ze ten onrechte beweerden dat het niet in gebruik was als winkelcentrum, maar eerder in gebruik was als arsenaal voor Oekraïense territoriale strijdkrachten.[13] Verschillende pro-Kremlin-bloggers op Telegram plaatsten en versterkten content die het 'valse vlag'-verhaal verder bevestigde, waarbij bloggers wezen op vermeende indicatoren van fabricage, zoals de aanwezigheid van mensen in militair uniform in beelden ter plekke[14] en de afwezigheid van vrouwen in de beelden.[15] Rusland lanceerde campagnes door te vertrouwen op een ingebouwd systeem van propagandaboodschappers en -media. De versterking van deze verhalen online biedt Rusland de mogelijkheid om de schuld op het internationale toneel af te schuiven en aansprakelijkheid te vermijden.

Vreemde mogendheden zoals Rusland begrijpen de waarde van het gebruik van informatie uit gesloten bronnen om de publieke perceptie te beïnvloeden, het gebruik van "hack-en-lek"-campagnes om tegenargumenten te verspreiden en wantrouwen te zaaien.

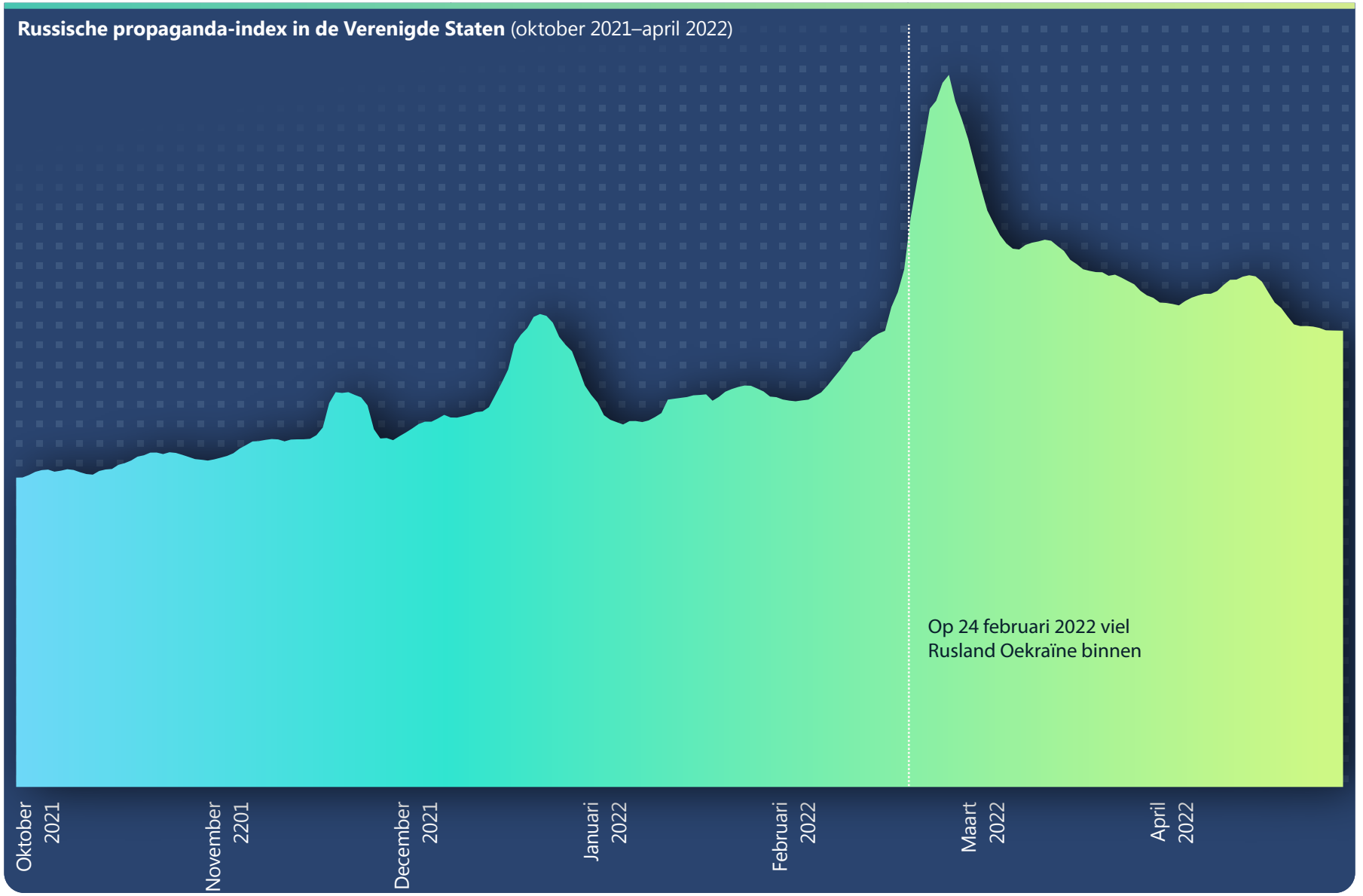
Links naar verdere informatie

- De bescherming van Oekraïne: eerste lessen uit de cyberoorlog | Microsoft On the Issues
- Een overzicht van de Russische cyberaanvalactiviteiten in Oekraïne | Speciaal verslag van Microsoft
- Verstorende cyberaanvallen gericht op Oekraïne | Microsoft On the Issues

De Russische propaganda-index volgen

In januari 2022 verwezen bijna duizend Amerikaanse websites verkeer door naar Russische propagandawebsites. De meest voorkomende onderwerpen voor Russische propagandawebsites die gericht waren op een Amerikaans publiek waren de oorlog in Oekraïne, de Amerikaanse binnenlandse politiek (pro-Trump of pro-Biden) en verhalen die waren gerelateerd aan COVID-19 en vaccins.

De Russian Propaganda Index (RPI) volgt de nieuwsstroom van door de Russische staat gecontroleerde en gesponsorde nieuwsuitzendingen en -versterkers als percentage van het totale nieuwsverkeer op internet. De RPI kan worden gebruikt om de consumptie van Russische propaganda via internet en in verschillende geografische gebieden op een precieze tijdlijn in kaart te brengen. Microsoft merkt echter op dat we alleen de Russische propaganda kunnen zien die op eerder geïdentificeerde websites is gepubliceerd. We hebben geen inzicht in propaganda op andere typen websites, waaronder gezaghebbende nieuwswebsites, niet-geïdentificeerde websites en sociale netwerkgroepen.



De Russische propaganda-index volgen

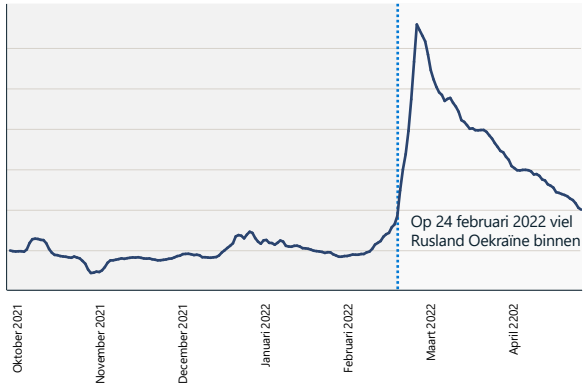
Vervolg

Russische propaganda-index: Oekraïne

Toen de oorlog in Oekraïne begon, zagen we een toename van 216 procent in de Russische propaganda, met een piek op 2 maart. De onderstaande grafiek laat zien hoe deze plotselinge toename samenviel met de invasie. De twee grafieken laten zien hoe de Russische propaganda snel toenam na het begin van de invasie.

RPI, Oekraïne

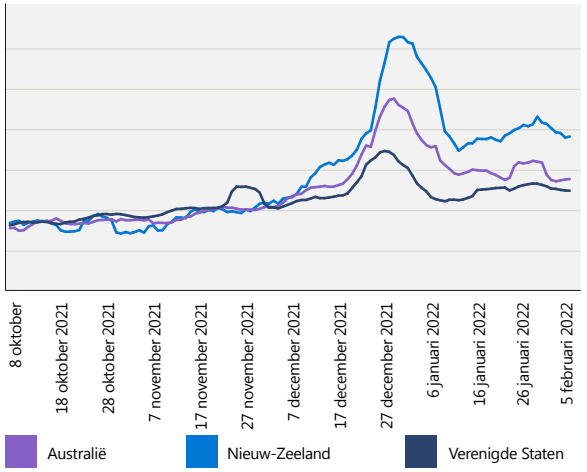
(7 oktober 2021 – 30 april 2022)



Russische propaganda-index: Nieuw-Zeeland versus Australië en de Verenigde Staten

Een evaluatie van de RPI in Nieuw-Zeeland toonde eind 2021 een piek die verband hield met COVID-19-propaganda. Deze piek in de consumptie van Russische propaganda in Nieuw-Zeeland ging vooraf aan een toename van openbare protesten begin 2022 in Wellington. Een tweede piek was duidelijk gerelateerd aan de Russische invasie van Oekraïne en overtrof de RPI's van Australië en de Verenigde Staten.

RPI, Nieuw-Zeeland versus Australië en de Verenigde Staten



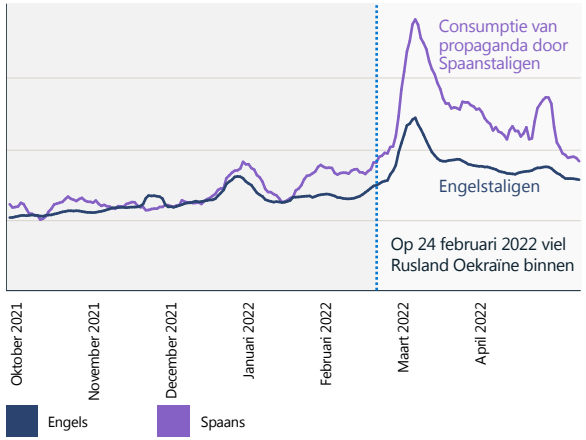
De Russische propagandaconsumptie in Nieuw-Zeeland is vergelijkbaar met die in Australië tot de eerste week van december 2021. Na december steeg de Russische propagandaconsumptie in Nieuw-Zeeland met ruim 30 procent ten opzichte van de consumptie in Australië en de Verenigde Staten.

Russische propaganda-index in de Verenigde Staten: Engels en Spaans

De RPI volgt ook propaganda in verschillende talen. Meerdere mediakanalen, waaronder RT en Sputnik News, zijn beschikbaar in meer dan 20 talen. Deze omvatten Engels, Spaans, Duits, Frans, Grieks, Italiaans, Tsjechisch, Pools, Servisch, Lets, Litouws, Moldavisch, Wit-Russisch, Armeens, Ossetisch, Georgisch, Azerbeidzjaans, Arabisch, Turks, Perzisch en Dari.

De volgende grafiek laat zien dat de RPI voor Spaanstalig nieuws in de Verenigde Staten veel hoger is dan voor Engelstalig nieuws.

Russische propagandaconsumptie is 2x hoger onder Spaanstaligen



De consumptie van Russische propaganda in de Verenigde Staten is twee keer zo hoog onder Spaanstaligen.

De consumptie van Russische propaganda is hoog in Latijns-Amerika

RT in het Spaans is de internationale nieuwszender met het hoogste aantal paginaweergaven en Facebook-volgers.

Bron: Microsoft AI for Good Research Lab

Synthetische media

We gaan een gouden tijdperk in voor het maken en manipuleren van media met behulp van AI. Microsoft-analisten merken op dat dit wordt aangedreven door twee belangrijke trends: de verspreiding van gebruiksvriendelijke tools en services voor het kunstmatig creëren van uiterst realistische synthetische afbeeldingen, video's, audio en tekst, en de mogelijkheid om snel content te verspreiden die is geoptimaliseerd voor specifieke doelgroepen.

Geen van beide ontwikkelingen is op zichzelf inherent problematisch. Op AI gebaseerde technologie kan worden gebruikt om leuke en opwindende digitale inhoud te creëren, of het nu puur synthetisch is of bestaand materiaal verbetert. Deze tools worden op grote schaal gebruikt door bedrijven voor reclame en communicatie en door individuen om boeiende content voor hun volgers te creëren. Wanneer synthetische media echter worden gemaakt en verspreid met de bedoeling schade te berokkenen, kunnen deze ernstige schade toebrengen aan personen, bedrijven, instellingen en de samenleving. Microsoft is een drijvende kracht geweest bij het ontwikkelen van technologieën en praktijken, zowel intern als in het bredere media-ecosysteem, om deze schade te beperken.

In deze sectie worden inzichten onderzocht uit de Microsoft-analyse van de huidige stand van de techniek voor het maken van schadelijke synthetische content, de schade die kan ontstaan als deze content wijdverbreid wordt en technische oplossingen die bescherming kunnen bieden tegen op synthetische media gebaseerde cyberbedreigingen.

Synthetische media maken

Het gebied van synthetische tekst en media ontwikkelt zich ongelooflijk snel, omdat technieken die ooit alleen mogelijk waren met de enorme computerresources van grote filmstudio's nu zijn geïntegreerd in telefoon-apps. Tegelijkertijd worden tools gebruiksvriendelijker en kunnen ze content genereren met een realisme dat zelfs forensische mediaspecialisten voor de gek kan houden. We hebben bijna het punt bereikt waarop iedereen een synthetische video kan maken van iedereen die iets zegt of doet. Het is niet onredelijk om te geloven dat we een tijdperk betreden waarin een aanzienlijk deel van de content die we online zien geheel of gedeeltelijk synthetisch is met behulp van AI-technieken.

> Met de beschikbaarheid van meer geavanceerde, gebruiksvriendelijke en algemeen beschikbare tools, is het maken van synthetische content in opkomst en zal deze binnenkort niet meer van de werkelijkheid te onderscheiden zijn.

Er zijn veel gratis en commerciële beeld-, video- en audiobewerkingstools van hoge kwaliteit. Deze tools kunnen worden gebruikt om eenvoudige maar potentieel schadelijke wijzigingen aan te brengen in digitale content, zoals het toevoegen van misleidende tekst, het verwisselen van gezichten en het verwijderen of wijzigen van context. Dergelijke "goedkope vervalsingen" worden veel gebruikt om snode content te verspreiden, politieke ideologieën te promoten en reputaties te schaden. Een bekend voorbeeld is de video uit 2019[16] van de Amerikaanse voorzitter van het Huis, Nancy Pelosi, die onduidelijk spreekt en dronken lijkt. Hoewel snel werd vastgesteld dat de video vertraagd was om het effect te creëren, verspreidde de "goedkope vervalsing" zich wijd en zijd voordat de originele video en context opdook.

Meer geavanceerde benaderingen voor het wijzigen van mediacontent omvatten de toepassing van geavanceerde AI-technieken om (a) puur synthetische media te creëren en (b) meer geavanceerde bewerkingen van bestaande media uit te voeren. De term deepfake wordt vaak gebruikt voor synthetische media die zijn gemaakt met behulp van geavanceerde AI-technieken (de naam is afkomstig van de diepe neurale netwerken die soms worden gebruikt). Deze technologieën worden ontwikkeld als op zichzelf staande apps, tools en services en geïntegreerd in gevestigde commerciële en open source bewerkingstools.

Dergelijke technologieën worden als wapen ingezet door kwaadwillende actoren in de hoop individuen en instellingen te schaden. Voorbeelden van deepfake-technieken zijn:

- **Face swap (Gezichtswissel) (video, afbeeldingen)**, waarbij een gezicht in een video wordt vervangen door een ander gezicht. Deze techniek kan worden gebruikt om een persoon, bedrijf of instelling te chanteren, of om personen op gênante locaties of in pijnlijke situaties te plaatsen.
- **Puppeteering (Poppenspel) (video, afbeeldingen)**, waarbij een video wordt gebruikt om een stilstaand beeld of tweede video van animatie te voorzien. Hierdoor kan het lijken alsof iemand iets gênants of misleidends heeft gezegd.
- **Generatieve vijandige netwerken (video, afbeeldingen)**, waarbij een reeks technieken wordt gebruikt voor het genereren van fotorealistische beelden.
- **Transformatormodellen (video, afbeeldingen, tekst)**, waarbij rijke beelden worden gecreëerd op basis van tekstbeschrijvingen.

Dergelijke geavanceerde op AI gebaseerde technieken worden tegenwoordig nog niet veel gebruikt in cyberbeïnvloedingscampagnes, maar we verwachten dat het probleem zal toenemen naarmate de tools gebruiksvriendelijker worden en breder beschikbaar komen.

De impact van manipulatie van synthetische media

Het gebruik van informatieactiviteiten om schade toe te brengen of invloed uit te breiden is niet nieuw. De snelheid waarmee informatie zich kan verspreiden en ons onvermogen om snel feiten en fictie te scheiden, betekent echter dat de impact en schade veroorzaakt door vervalsingen en andere synthetisch gegenereerde schadelijke media veel groter kan zijn, zoals aangetoond met het Pelosi-voorbeeld.

Er zijn verschillende categorieën van schade die we in overweging nemen: marktmanipulatie, betalingsfraude, vishing, imitaties, merkschade, reputatieschade en botnets. Veel van deze categorieën hebben wijdverbreide voorbeelden uit de echte wereld gerapporteerd, die ons vermogen om feiten van fictie te scheiden zouden kunnen ondermijnen.

Een meer verraderlijke bedreiging voor de langere termijn is ons begrip van wat waar is als we niet langer kunnen vertrouwen op wat we zien en horen. Hierdoor kan elke compromitterende afbeelding, audio of video van een publieke of private figuur worden afgedaan als nep - een uitkomst die bekend staat als The Liar's Dividend.[17] Recent onderzoek[18] toont aan dat dit misbruik van technologie al wordt gebruikt om financiële systemen aan te vallen, hoewel veel andere misbruikscenario's aannemelijk zijn.

Synthetische media

Vervolg

Synthetische media detecteren

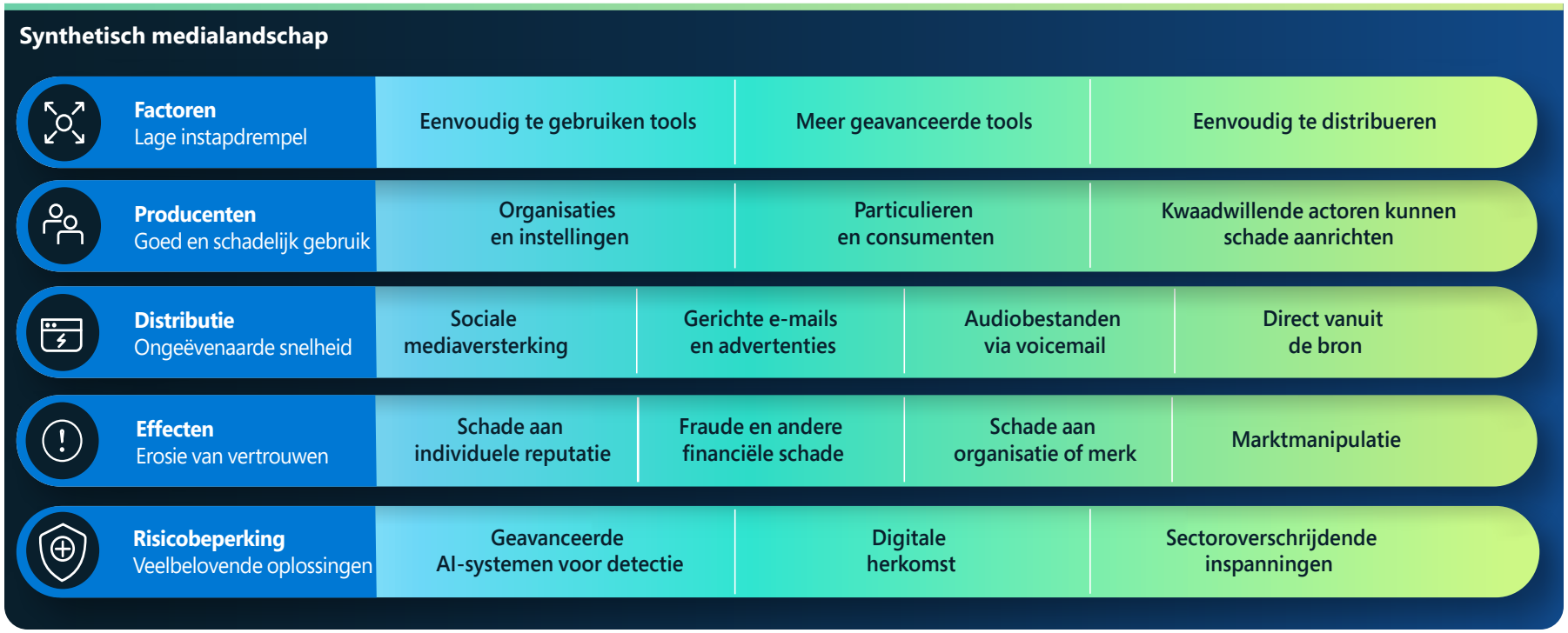
Er worden inspanningen geleverd in de industrie, bij de overheid en in de academische wereld om betere manieren te ontwikkelen om synthetische media op te sporen, het effect hiervan te verminderen en het vertrouwen te herstellen. Er zijn verschillende veelbelovende paden voorwaarts, evenals barrières die het overwegen waard zijn.

Eén benadering is het bouwen van op AI gebaseerde systemen die vervalsingen kunnen herkennen. Dit zijn in wezen "defensieve" AI-systemen die als tegenhanger van de offensieve AI-systemen fungeren. Dit is een gebied van actief onderzoek waar de huidige systemen voor het maken van synthetische audio en video veelbetekenende artefacten achterlaten die kunnen worden opgemerkt door getrainde forensische media-analisten en geautomatiseerde tools.

Helaas geldt dat, hoewel de huidige vervalsingen onthullende gebreken hebben, de precieze artefacten meestal specifiek zijn voor een bepaalde tool of een bepaald algoritme. Dit betekent dat training met bekende vervalsingen meestal niet algemeen kan worden toegepast voor andere algoritmen, zoals aangetoond in een open wedstrijd in 2020 voor het bouwen van deepfake-beelddetectoren.[19] Het is verleidelijk om meer te investeren in de ontwikkeling van geavanceerdere detectoren, maar Microsoft is om twee redenen zeer sceptisch over de vraag of dit tot zinvolle verbeteringen zal leiden:

Ten eerste hebben we uitstekende fysieke modellen die de echte wereld weerspiegelen. Huidige nepmakers gaan voor gemakkelijke oplossingen, wat resulteert in detecteerbare artefacten, maar nieuwere modellen zullen steeds realistischer worden. Er is niets bijzonders aan een scène uit de echte wereld die is vastgelegd met een camera die niet door een computer kan worden gemodelleerd.

Ten tweede gebruiken geavanceerde algoritmen voor nepcreatie een techniek genaamd Generative Adversarial Networks (GAN's) als onderdeel van het creatieproces. Een GAN speelt twee AI-systemen tegen elkaar uit met behulp van een generator om de nep te maken en een discriminator om nepbeelden te detecteren en de generator te trainen. Elke investering in het ontwikkelen van een betere detector zal de generator in staat stellen de kwaliteit van de vervalsingen te verbeteren.



Synthetische media

Vervolg

Herkomst van digitale assets

Als het detecteren van vervalsingen onbetrouwbaar is, wat kan er dan worden gedaan om bescherming te bieden tegen het schadelijke gebruik van synthetische media? Eén belangrijke opkomende technologie is digitale herkomst: een mechanisme dat makers van digitale media in staat stelt een asset te certificeren en dat consumenten helpt te identificeren of er al dan niet met de digitale asset is geknoeid. Digitale herkomst is met name belangrijk in de context van de huidige sociale-medianetwerken, gezien de snelheid waarmee content over het internet kan reizen en de mogelijkheid voor kwaadwillenden om content gemakkelijk te manipuleren.

900%

toename op jaarbasis bij de verspreiding van deepfakes sinds 2019.[20]

Digital Provenance Technology is een moderne versie van cryptografische documentondertekening, ontworpen om de bron, bewerkingsgeschiedenis en metadata van objecten vast te leggen terwijl ze door het huidige web stromen. De visie en technische methoden om dit type end-to-end fraudebestendige certificering van media mogelijk te maken, zijn ontwikkeld door een team van onderzoekers en wetenschappers van Microsoft. We leiden samen een sectoroverschrijdend partnerschap dat is gericht op het tot leven brengen van technologie voor de herkomst van media in Project Origin (opgericht door Microsoft, BBC, CBC/Radio-Canada en de New York Times) en nemen deel aan het Content Authenticity Initiative (opgericht door Adobe). Microsoft werkte ook samen met partners in technologie en mediadiensten om de Coalition for Content Provenance and Authenticity (C2PA) op te richten. C2PA is een standaardiseringsorganisatie die onlangs de meest geavanceerde digitale herkomstspecificatie heeft gepubliceerd voor gebruik met media-items, waaronder afbeeldingen, video's, audio en tekst.

Een object met C2PA-functionaliteit bevat een manifest dat het object en de metadata beschermt tegen manipulatie, terwijl het bijbehorende certificaat de uitgever identificeert.

Synthetische media zijn oorspronkelijk niet ontworpen om schade aan te richten, maar worden door kwaadwillenden als wapen gebruikt om het vertrouwen in individuen en instellingen te ondermijnen.

Digitale herkomst is een veelbelovende opkomende technologie die het potentieel heeft om het vertrouwen van mensen in online mediacontent te herstellen door de oorsprong van een media-item te certificeren.

Openbaar beschikbare oplossingen op basis van de C2PA-specificatie duiken op als een nieuwe functie in bestaande producten of als nieuwe zelfstandige apps en diensten. We verwachten dat de meeste van de veelgebruikte tools voor vastleggen, bewerken en schrijven over een paar jaar C2PA-compatibel zullen zijn. Dit biedt ondernemingen de mogelijkheid om hun behoeften en gebruik van digitale herkomst van vandaag te bepalen en om deze extra beschermingslaag te eisen in de tools die ze in bestaande workflows gebruiken.

Direct bruikbare inzichten

1. Neem proactieve stappen om je organisatie te beschermen tegen desinformatiebedreigingen door proactief rekening te houden met je PR- en communicatiereacties.
2. Gebruik herkomsttechnologie om officiële communicatie te beschermen.

Links naar verdere informatie

- A promising step forward on disinformation | Microsoft On the Issues
- A Milestone Reached, 31 januari 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Explore technical details about the system Project Origin uses for media authentication | Microsoft ALT Innovation

Een holistische aanpak voor bescherming tegen cyberbeïnvloe-dingsactiviteiten

Microsoft bouwt voort op zijn reeds volwassen infrastructuur voor cyberbedreigingsinformatie om een bredere, meer omvattende kijk op cyberbeïnvloedingsactiviteiten te ontwikkelen.

We gebruiken een framework voor voorgestelde respons- en mitigatiestrategieën om de dreiging van activiteiten te bestrijden, dat kan worden onderverdeeld in vier belangrijke pijlers: detecteren, verstoren, verdedigen en afschrikken.

Daarnaast heeft Microsoft vier principes aangenomen om ons werk in deze ruimte te verankeren. Ten eerste zeggen we toe de vrijheid van meningsuiting te respecteren en het vermogen van onze klanten om informatie te creëren, te publiceren en te zoeken via onze platforms, producten en diensten te handhaven. Ten tweede spannen we ons op proactieve wijze in om te voorkomen dat onze platforms en producten worden gebruikt om sites en content met buitenlandse cyberbeïnvloeding te versterken. Ten derde zullen we niet opzettelijk profiteren van content of actoren van buitenlandse cyberbeïnvloeding. Tot slot geven we prioriteit aan het naar boven brengen van content om buitenlandse cyberbeïnvloedingsactiviteiten tegen te gaan door gebruik te maken van interne en vertrouwde data van derden op onze producten.

Detecteren

Net als bij cyberdefensie, omvat de eerste stap bij het tegengaan van buitenlandse cyberbeïnvloedingsactiviteiten het ontwikkelen van het vermogen om deze te detecteren. Geen enkel bedrijf of organisatie kan hopen op eigen houtje de vooruitgang te boeken die nodig is. Nieuwe, bredere samenwerking in de technische sector zal cruciaal zijn, waarbij de vooruitgang bij het analyseren en rapporteren van cyberbeïnvloedingsactiviteiten sterk afhankelijk is van de rol van samenleving, ook in academische instellingen en non-profitorganisaties.

De onderzoekers Jake Shapiro en Alicia Wanless van respectievelijk de Princeton University en de Carnegie Endowment for International Peace erkennen deze rol en hebben plannen uitgestippeld om het nieuwe "Institute for Research on the Information Environment" (IRIE) te lanceren. Met steun van Microsoft, de Knight Foundation en Craig Newmark Philanthropies, zal de IRIE een inclusieve onderzoeksinstelling voor meerdere stakeholders creëren, gemodelleerd naar de Europese Organisatie voor Nucleair Onderzoek (CERN). Het zal expertise op het gebied van dataverwerking en -analyse combineren om nieuwe ontdekkingen op dit gebied te versnellen en op te schalen. Bevindingen zullen worden gedeeld om beleidsmakers, technologiebedrijven en consumenten breder te informeren.

Verdedigen

De tweede strategische pijler is het versterken van de democratische verdediging, een al lang bestaande prioriteit die investeringen en innovatie vereist. Er moet rekening worden gehouden met de uitdagingen die technologie heeft gecreëerd voor de democratie, en met de kansen die technologie heeft gecreëerd om democratische samenlevingen effectiever te beschermen.

Het strategieframework van Microsoft is bedoeld om sectoroverschrijdende stakeholders te helpen bij het opsporen, verstoren, verdedigen en afschrikken van propaganda, met name campagnes van buitenlandse agressors.

Het is gepast om te beginnen met een van de grote technologische uitdagingen van onze tijd: de impact van internet en digitale reclame op de traditionele journalistiek. Sinds de 18e eeuw heeft een vrije en onafhankelijke pers een speciale rol gespeeld bij het ondersteunen van elke democratie op de planeet: het blootleggen van corruptie, het documenteren van oorlogen en het belichten van de grootste maatschappelijke uitdagingen van deze en andere tijden. Het internet heeft het lokale nieuws echter uitgekleed door advertentie-inkomsten op te slokken en betalende abonnees weg te lokken. Veel lokale kranten hebben het loodje gelegd. Een van de vele inzichten uit ons recente werk is dat steden die geen krant hebben, onbewust en onvermijdelijk worden blootgesteld aan een meer dan gemiddelde hoeveelheid buitenlandse propaganda. Om deze redenen moet een van de kritische verdedigingspunten van de democratie de traditionele journalistiek en een vrije pers versterken, vooral op lokaal niveau. Dit vereist voortdurende investeringen en innovatie die de lokale behoeften van verschillende landen en continenten moeten weerspiegelen. Deze problemen zijn niet eenvoudig en vereisen benaderingen met meerdere stakeholders, die Microsoft en andere technologiebedrijven steeds meer ondersteunen.

We hebben ook nieuwe innovaties nodig in het overheidsbeleid, dat een publieke prioriteit moet zijn. Dit kan wetten omvatten die uitgevers in staat stellen om gezamenlijk te onderhandelen over advertentie-inkomsten met technologiebedrijven, en wetgeving die belastingverminderingen biedt om lokale redacties te ontlasten van een deel van hun loonbelasting voor journalisten die ze in dienst hebben. Journalisten hebben veel andere hulpmiddelen nodig voor hun vak, waaronder de mogelijkheid om content te scheiden van legitieme en frauduleuze bronnen.

Er is ook een snel evoluerende behoefte om consumenten te helpen een meer geavanceerd vermogen te ontwikkelen om door de staat aangestuurde informatieactiviteiten te identificeren. Hoewel dit misschien ontmoedigend lijkt, vertoont het overeenkomsten met het werk dat de technologiesector al lang doet om andere cyberbedreigingen te bestrijden. Overweeg het voorlichten van consumenten zodat zij zorgvuldiger naar een e-mailadres gaan kijken om spam of andere frauduleuze communicatie te helpen herkennen. Initiatieven in de Verenigde Staten, zoals het News Literacy Project en het Trusted Journalism

Een meer verraderlijke bedreiging voor de langere termijn is ons begrip van wat waar is als we niet langer kunnen vertrouwen op wat we zien en horen.

Een holistische aanpak voor bescherming tegen cyberbeïnvloedings-activiteiten

Vervolg

Program helpen om beter geïnformeerde consumenten van nieuws en informatie te ontwikkelen. Wereldwijd kan nieuwe technologie, zoals de browserplug-in van NewsGuard, deze inspanning veel sneller vooruit helpen.

Dit zou ons er ook aan moeten herinneren dat een deel van de basis voor democratie een opleiding in burgerschap is. Zoals altijd, moet deze inspanning op scholen worden gestart. Maar we leven in een wereld die vereist dat we gedurende ons hele leven voortdurend burgerschapsonderwijs ondergaan. De nieuwe belofte van Civics at Work, dat wordt geleid door het Center for Strategic and International Studies en waarvan Microsoft een inaugurele ondertekenaar en partner was, is bedoeld om de burgerzin in het bedrijfsleven nieuw leven in te blazen. Het is een goed voorbeeld van de vele mogelijkheden om onze democratische verdediging te versterken.

Verstoren

De afgelopen jaren heeft de Digital Crimes Unit (DCU) van Microsoft tactieken verfijnd en tools ontwikkeld om cyberbedreigingen te verstoren, variërend van ransomware tot botnets en aanvallen van vreemde mogendheden. We hebben veel cruciale lessen geleerd, te beginnen met de rol van actieve verstoring bij het tegengaan van een breed scala aan cyberaanvallen.

Terwijl we nadenken over het tegengaan van cyberbeïnvloedingsactiviteiten, speelt verstoring misschien een nog grotere rol en wordt de beste aanpak van verstoring steeds duidelijker. Het meest effectieve tegengif tegen grootschalige misleiding is transparantie. Dat is de reden waarom Microsoft zijn capaciteit heeft vergroot om beïnvloedingsactiviteiten van vreemde mogendheden te detecteren en te verstoren door Miburo Solutions over te nemen. Dit is een toonaangevend analyse- en onderzoeksbedrijf voor cyberbedreigingen dat is gespecialiseerd in de detectie van en reactie op buitenlandse cyberbeïnvloedingsactiviteiten.

Onze ervaring heeft geleerd dat overheden, technologiebedrijven en NGO's cyberaanvallen zorgvuldig en met voldoende bewijs moeten toeschrijven. Inzicht in de impact van een dergelijke verstoring is van vitaal belang en kan zelfs nog nuttiger zijn bij het verstoren van cyberinvloed. Wees getuige van het delen van informatie door de Amerikaanse regering in de aanloop naar de Russische invasie van Oekraïne, die transparantie in effectieve actie bracht, zoals het blootleggen van Russische plannen, waaronder specifieke campagnes zoals een complot om een nepvideo te gebruiken.

Zoals blijkt uit de publicatie van afgelopen zomer van het CyberPeace Institute in Genève over aanhoudende cyberaanvallen binnen en buiten Oekraïne, is er een kans voor een breed scala aan maatschappelijke organisaties en organisaties uit de particuliere sector om de transparantie met betrekking tot cyberbeïnvloedingsactiviteiten te bevorderen. Betrouwbare rapporten over nieuw ontdekte en goed gedocumenteerde activiteiten kunnen het publiek helpen beter te evalueren wat het leest, ziet en hoort, vooral op internet. Daartoe zal Microsoft voortbouwen op zijn bestaande cyberrapporten en deze uitbreiden en nieuwe rapporten, data en updates vrijgeven met betrekking tot wat we ontdekken over cyberbeïnvloedingsactiviteiten, met inbegrip van toeschrijvingsverklaringen indien van toepassing. We zullen een jaarverslag publiceren dat een datagestuurde benadering gebruikt om in het hele bedrijf te kijken naar de prevalentie van buitenlandse informatieactiviteiten en de volgende stappen om te zorgen voor incrementele verbetering. We zullen ook aanvullende stappen overwegen die voortbouwen op dit soort transparantie.

Zo is bijvoorbeeld vooral de rol van digitale reclame belangrijk, omdat reclame kan helpen bij het financieren van buitenlandse activiteiten en tegelijkertijd een schijn van legitimiteit kan wekken voor door het buitenland gesponsorde propagandasites. Er zullen nieuwe inspanningen nodig zijn om deze geldstromen te verstoren.

Afschrikken

Tot slot kunnen we niet verwachten dat landen hun gedrag veranderen als er geen verantwoordelijkheid is voor het overtreden van internationale regels. Het afdwingen van een dergelijke aansprakelijkheid is uitsluitend een verantwoordelijkheid van de overheid. Maar in toenemende mate spelen acties door meerdere stakeholders een belangrijke rol bij het versterken en uitbreiden van internationale normen. Meer dan 30 online platforms, adverteerders en uitgevers, waaronder Microsoft, hebben zich aangesloten bij de recent bijgewerkte praktijkcode van de Europese Commissie inzake desinformatie, waarmee ze instemmen met versterkte toezeggingen om deze groeiende uitdaging aan te gaan. Net als de recente oproep van Parijs, de oproep van Christchurch en de verklaring over de toekomst van het internet, kunnen multilaterale acties en acties van meerdere stakeholders de overheden en het publiek onder democratische naties samenbrengen. Overheden kunnen dan voortbouwen op deze normen en wetten om de verantwoordingsplicht te bevorderen die de democratieën van de wereld nodig hebben en verdienen.

Door snelle radicale transparantie kunnen democratische regeringen en samenlevingen invloedscampagnes effectief afzwakken door de bron van aanvallen door vreemde mogendheden aan te wijzen, het publiek te informeren en vertrouwen in instellingen op te bouwen.

We hebben de technische capaciteit vergroot om buitenlandse beïnvloedingsactiviteiten op te sporen en te verstoren en zetten ons in om transparant te rapporteren over deze activiteiten, zoals onze rapportage over cyberaanvallen.

Direct bruikbare inzichten

1. Implementeer sterke digitale hygiënepraktijken in je hele organisatie.
2. Overweeg manieren om onbedoeld inschakelen van cyberbeïnvloedingscampagnes door je werknemers of je bedrijfspraktijken te verminderen. Dit omvat het verminderen van het aanbod aan bekende buitenlandse propagandasites.
3. Ondersteun campagnes voor informatie-geletterdheid en burgerbetrokkenheid als een belangrijk onderdeel om samenlevingen te helpen zich te verdedigen tegen propaganda en buitenlandse invloeden.
4. Ga rechtstreeks in contact met groepen die relevant zijn voor je branche om samen beïnvloedingsactiviteiten aan te pakken.

Eindnoten

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. Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Woordvoerster van het Russische ministerie van Buitenlandse Zaken Maria Zakharova: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Russia's Kremenchuk Claims Versus the Evidence—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas, and Kristjan Peterson, October 2020

Cyberveerkracht

Inzicht in de risico's en voordelen van modernisering wordt cruciaal voor een holistische benadering van veerkracht.

Een overzicht van

cyberveerkracht

Cyberbeveiliging is een belangrijke drijvende factor voor technologisch succes. Innovatie en verhoogde productiviteit kunnen alleen worden bereikt door beveiligingsmaatregelen te nemen die organisaties zo veerkrachtig mogelijk maken tegen moderne aanvallen.

De pandemie heeft ons uitgedaagd om de beveiligingspraktijken en -technologieën van Microsoft te richten op bescherming van onze werknemers, waar deze ook werken. Het afgelopen jaar bleven bedreigingsactoren profiteren van kwetsbaarheden die werden blootgelegd tijdens de pandemie en de verschuiving naar een hybride werkomgeving. Sindsdien is onze belangrijkste uitdaging het beheren van de prevalentie en complexiteit van verschillende aanvalsmethoden en de toegenomen activiteit van vreemde mogendheden.

Effectieve cyberveerkracht vereist een holistische, adaptieve aanpak om de veranderende bedreigingen voor kernservices en infrastructuur het hoofd te bieden.

Ga voor meer informatie naar p89

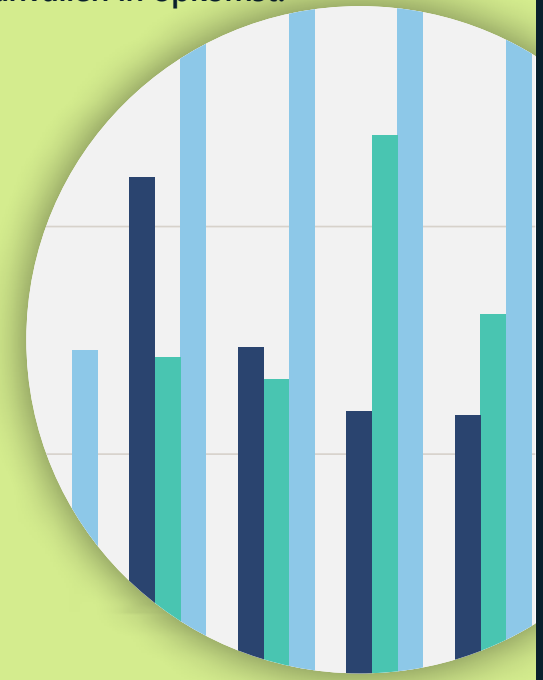
Gemoderniseerde systemen en architectuur zijn belangrijk voor het beheer van bedreigingen in een hyperverbonden wereld.

Ga voor meer informatie naar p90

De basishouding voor beveiliging is bepalend voor de effectiviteit van geavanceerde oplossingen.

Ga voor meer informatie naar p92

Hoewel op wachtwoorden gebaseerde aanvallen de belangrijkste bron van identiteitsschendingen blijven, zijn ook andere typen aanvallen in opkomst.



Ga voor meer informatie naar p93

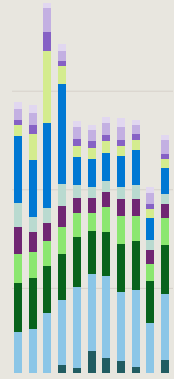
De menselijke dimensie van veerkracht tegen cyberbeïnvloedings-activiteiten is ons vermogen om samen te werken.

Ga voor meer informatie naar p102

De overgrote meerderheid van succesvolle cyberaanvallen zou kunnen worden voorkomen door gebruik te maken van elementaire beveiligingshygiëne.

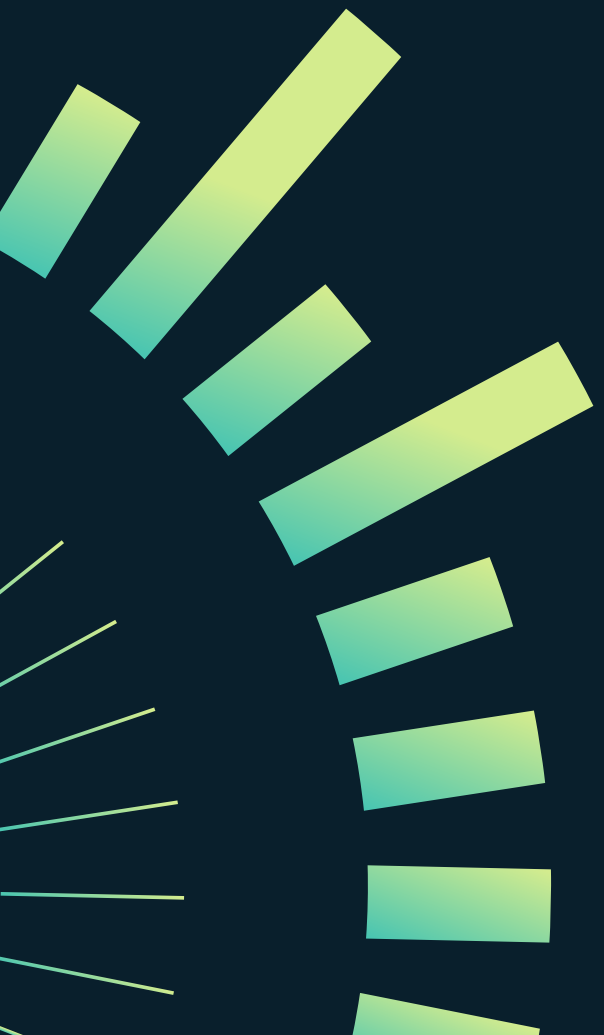
Ga voor meer informatie naar p108

In het afgelopen jaar heeft de wereld te maken gehad met DDoS-activiteiten die ongekend waren in volume, complexiteit en frequentie.



Ga voor meer informatie naar p98

Inleiding



De pandemie heeft ons uitgedaagd om de beveiligingspraktijken en -technologieën van Microsoft te richten op bescherming van onze werknemers, waar deze ook werken. Het afgelopen jaar bleven bedreigingsactoren profiteren van kwetsbaarheden die werden blootgelegd tijdens de pandemie en de verschuiving naar een hybride werkomgeving. Sindsdien is onze belangrijkste uitdaging het beheren van de prevalentie en complexiteit van verschillende aanvalsmethoden en de toegenomen activiteit van vreemde mogendheden.

De digitale bedreigingsactiviteit en het niveau van verfijning van cyberaanvallen neemt elke dag toe. Veel van de complexe aanvallen van tegenwoordig zijn gericht op het compromitteren van identiteitsarchitecturen, supply chains en derde partijen met beveiligingscontroles in wisselende gradaties. We hebben met name gezien dat phishing-aanvallen voor identiteitsdiefstal een duidelijke en actuele bedreiging vormen. Dit type aanvallen is echter over het algemeen niet succesvol bij goed identiteitsbeheer, phishing-controle en praktijken voor endpointbeheer. Daarom moeten we de basisprincipes onthouden: achtennegentig procent van de aanvallen kan worden gestopt met elementaire hygiënemaatregelen. Bij Microsoft beheren we identiteiten en apparaten als onderdeel van onze Zero Trust-aanpak, die toegang met de minst mogelijke bevoegdheden en phish-resistente referenties omvat om bedreigingsactoren effectief te stoppen en onze data te beschermen.

Vandaag de dag kunnen zelfs bedreigingsactoren die niet over geavanceerde technische vaardigheden beschikken, ongelooflijk destructieve aanvallen lanceren, aangezien toegang tot geavanceerde tactieken, technieken en procedures algemeen beschikbaar wordt in de cybercriminaliteitseconomie. De oorlog in Oekraïne heeft aangetoond hoe actoren van vreemde mogendheden hun offensieve cyberactiviteiten hebben opgevoerd door in toenemende mate gebruik te maken van ransomware. Ransomware is nu een geavanceerde industrie met bedreigingsactoren die dubbele of driedubbele afpersingstactieken gebruiken om een uitbetaling te verkrijgen en developers die ransomware as a service (RaaS) aanbieden. Met RaaS gebruiken bedreigingsactoren een aangesloten netwerk om aanvallen uit te voeren, waardoor de toegangsdrempel voor minder bekwame cybercriminelen wordt verlaagd en uiteindelijk de aanvallerspool wordt vergroot.

Daarom heeft Microsoft een programma voor eliminatie van ransomware ontworpen. Het doel van het programma is om hiaten in de controle en dekking te verhelpen, bij te dragen aan functieverbeteringen voor services en herstel-playbooks te ontwikkelen voor ons beveiligingscentrum en onze technische teams in het geval van een ransomwareaanval.

Recente aanvallen op supply chain en externe leveranciers wijzen op een belangrijk omslagpunt in de branche. De verstoring die deze aanvallen veroorzaken voor onze klanten, partners, overheden en Microsoft blijft toenemen, wat het belang illustreert van gerichte aandacht voor cyberveerkracht en samenwerking tussen stakeholders op het gebied van beveiliging. Aanvallers richten zich ook op on-premises systemen, wat de noodzaak voor organisaties versterkt om kwetsbaarheden van legacy-systemen te beheren door de infrastructuur te moderniseren en naar de cloud te verplaatsen, waar de beveiliging robuuster is.

We leven in een tijdperk waarin beveiliging een belangrijke factor voor technologisch succes vormt. Innovatie en verhoogde productiviteit kunnen alleen worden bereikt door beveiligingsmaatregelen te nemen die organisaties zo veerkrachtig mogelijk maken tegen moderne aanvallen. Naarmate digitale dreigingen toenemen en evolueren, is het van cruciaal belang om cyberveerkracht in te bouwen in de structuur van elke organisatie.

Bret Arsenault
Chief Information Security Officer

Cyberveerkracht: een cruciaal fundament van een verbonden samenleving

Door de revolutie in digitale technologie hebben organisaties transformaties ondergaan om steeds meer verbonden te raken, zowel in de manier waarop ze werken als in de services die ze aanbieden. Naarmate de bedreigingen in het cyberlandschap toenemen, is het inbouwen van cyberveerkracht in de structuur van de organisatie net zo cruciaal als financiële en operationele veerkracht.

Digitale transformatie heeft de manier waarop organisaties omgaan met klanten, partners, werknemers en andere stakeholders voorgoed veranderd. Nieuwe technologieën bieden enorme mogelijkheden om contacten te onderhouden met mensen, producten te transformeren en activiteiten te optimaliseren. De pandemie heeft de digitale transformatie versneld door als drijvende factor te fungeren voor innovatieve technologieën waarmee mensen op nieuwe manieren en vanaf elke locatie kunnen samenwerken.

Terwijl cyberbedreigingen endemisch worden, wordt het moeilijker om te voorkomen dat ze een organisatie in gevaar brengen in onze 'altijd verbonden' wereld. Cyberveerkracht vertegenwoordigt het vermogen van een organisatie om haar activiteiten voort te zetten en de groei te versnellen ondanks het spervuur van aanvallen. Preventie moet worden afgewogen tegen overlevings- en herstelmogelijkheden en overheden en ondernemingen ontwikkelen uitgebreide modellen die verder gaan dan beveiliging en privacy om assets, data en andere resources te beschermen als onderdeel van cyberveerkracht.

Een holistische benadering van cyberveerkracht ontwikkelen

Cyberveerkracht vereist een holistische, adaptieve en wereldwijde aanpak die in staat is de veranderende bedreigingen voor kernservices en infrastructuur het hoofd te bieden, met inbegrip van:

- Basiscyberhygiëne zoals beschreven in onze klokkromme van cyberveerkracht.
- Inzicht in en beheer van de afweging tussen risico en beloning van digitale transformatie.
- Realtime responsmogelijkheden die proactieve detectie van bedreigingen en kwetsbaarheden mogelijk maken.
- Bescherming tegen bekende aanvallen en preventieve activiteiten tegen nieuwe en verwachte aanvalsvectoren, met inbegrip van de mogelijkheid om automatisch herstel uit te voeren.
- Verminderde impact van aanvallen en rampen via foutisolatie en segmentering.
- Geautomatiseerd herstel en redundantie bij verstoringen.
- Prioriteitstelling voor operationele testactiviteiten om hiaten te vinden en inzicht te krijgen in gedeelde verantwoordelijkheden en afhankelijkheden van externe resources, zoals cloudgebaseerde beveiligingsoplossingen.

Een effectief programma voor cyberveerkracht begint met de basisprincipes van resources, zoals inzicht in de beschikbare services en het hebben van een betrouwbare catalogus van resources waarop een beroep kan worden gedaan in het geval van een verstoring. Voortbouwend op die basis moet het programma in staat zijn om zijn eigen effectiviteit te beoordelen, de prestaties van essentiële services en hun afhankelijkheden te meten, capaciteiten te testen en valideren voor on-premises en cloudservices, en voor continue verbetering te zorgen in de digitale levenscyclus van de organisatie.

Om een holistische benadering te bieden, werken we samen met organisaties om hun meest essentiële on-premises en online services, bedrijfsprocessen, afhankelijkheden, personeel, verkopers en leveranciers te identificeren. We zoeken ook naar assets en resources die verband houden met klant- en marktverwachtingen, wettelijke en contractuele verplichtingen en interne activiteiten. Na identificatie van deze kritieke resources moeten parallelle inspanningen dreigingen, verstoringen, potentiële aanvalsvectoren en systeem- en proceskwetsbaarheden detecteren en bewaken. De mogelijkheid om dit te doen onder het huidige tekort aan vaardigheden vereist een strikte prioriteitstelling op basis van het algehele risico voor de organisatie.

Dit type holistische benadering moet adaptief zijn tegen de achtergrond van een voortdurend evoluerend bedreigingslandschap, met als doel meetbare prestatieverbetering, kortere detectie-, reactie- en hersteltijden, en een geringere impact in het geval van verstoringen. De aanpak moet tevens de toenemende verbondenheid van bedreigingen herkennen. Een beveiligingsincident kan bijvoorbeeld resulteren in een datalek met gevolgen voor de privacy, waardoor veel interne en externe teams moeten samenwerken om snel te reageren en de impact tot een minimum te beperken.

> Cyberveerkracht is het vermogen van een onderneming om de eigen activiteiten voort te zetten en de groei te versnellen ondanks verstoringen, waaronder cyberaanvallen.

Direct bruikbare inzichten

1. Bouw en beheer technologische systemen die de impact van een inbreuk beperken en hen in staat stellen veilig en effectief te blijven werken, zelfs bij een succesvolle inbreuk. Focus op gemeenschappelijke kritieke assets, ondersteun veerkracht en ontwerp voor aanpassingsvermogen (bijvoorbeeld hybride en multi-cloud, multi-platform), verminder aanvalsoppervlakken (verwijder bijvoorbeeld ongebruikte applicaties en te ruime ingerichte toegangsrechten), ga uit van gecompromitteerde resources en verwacht dat tegenstanders zich verder ontwikkelen.
2. Houd bij het plannen van digitale projecten rekening met potentiële bedreigingen naast kansen en gedeelde verantwoordelijkheden voor veerkracht in de hele digitale supply chain op technologiegebied, met inbegrip van cloudgebaseerde beveiligingsoplossingen.
3. Bouw systemen om security by design in te bedden en onderneem stappen om te anticiperen op toekomstige zich ontwikkelende bedreigingen en deze te detecteren, het hoofd te bieden en aan te pakken.
4. Zorg ervoor dat bedrijfsleiders zo nodig overleggen met beveiligingsteams om de risico's van nieuwe ontwikkelingen te begrijpen. Evenzo moeten beveiligingsteams zakelijke doelen in overweging nemen en leiders adviseren over hoe ze deze veilig kunnen nastreven.
5. Zorg voor duidelijke operationele praktijken en procedures voor de veerkracht van organisaties bij cyberincidenten.

Het belang van modernisering van systemen en architectuur

Terwijl we nieuwe mogelijkheden ontwikkelen voor een hyperverbonden wereld, moeten we de bedreigingen van legacy-systemen en -software beheren.

Verouderde systemen, die zijn ontwikkeld voordat moderne connectiviteitstools zoals smartphones, tablets en cloudservices de norm werden, vormen een risico voor een organisatie die ze nog steeds gebruikt. Deze blootstelling aan risico's wordt versterkt door de bevindingen van het Microsoft Security Services for Incident Response-team, een groep beveiligingsprofessionals die klanten helpt bij het reageren op en herstellen van aanvallen.

In het afgelopen jaar waren problemen die werden aangetroffen bij klanten die herstellend waren van aanvallen, gerelateerd aan zes categorieën, zoals weergegeven in de grafiek op deze pagina. Op de volgende pagina worden bruikbare stappen beschreven die je kunt ondernemen om de veerkracht te verbeteren.

Meer dan 80 procent van de beveiligingsincidenten is te herleiden tot een paar ontbrekende elementen die kunnen worden verholpen door middel van moderne beveiligingsbenaderingen.

Belangrijke kwesties die van invloed zijn op cyberveerkracht

Deze grafiek toont het percentage getroffen klanten waarbij elementaire beveiligingscontroles ontbreken die essentieel zijn voor het vergroten van de cyberveerkracht van de organisatie. De bevindingen zijn gebaseerd op Microsoft-contacten in het afgelopen jaar.

"Leiders moeten cyberveerkracht als een essentieel facet van zakelijke veerkracht beschouwen. Ze moeten cyberverstoringen op dezelfde manier plannen als natuurrampen of andere onvoorziene gebeurtenissen en interne stakeholders zoals operaties, communicatie, juridische zaken en meer samenbrengen om strategieën te ontwikkelen. Door dit te doen, kunnen organisaties ervoor zorgen dat hun essentiële bedrijfssystemen zo snel mogelijk weer online worden gebracht om de normale bedrijfsactiviteiten te hervatten.

Maar het gaat verder dan dat. Aangezien veel organisaties afhankelijk zijn van externe leveranciers en serviceproviders, moeten leiders de planning van cyberveerkracht uitbreiden naar hun end-to-end waardeketen om de bedrijfscontinuïteit en veerkracht verder te waarborgen."

Ann Johnson,
Corporate Vice President of Security, Compliance, Identity, and Management Business Development

Het belang van modernisering van systemen en architectuur

Vervolg

Er zijn duidelijke gebieden waarop organisaties zich kunnen richten bij de modernisering van hun aanpak en de bescherming tegen bedreigingen:

Probleem	Direct bruikbare stappen
Onveilige configuratie van identiteitsprovider Onjuiste configuratie en blootstelling van identiteitsplatforms en de onderdelen hiervan vormen een veelvoorkomende vector voor het verkrijgen van ongeautoriseerde toegang met hoge bevoegdheden.	Volg de basislijnen en best practices voor beveiligingsconfiguratie bij het implementeren en onderhouden van identiteitssystemen zoals AD en Azure AD-infrastructuur. Implementeer toegangsbeperkingen door scheiding van bevoegdheden, het afdwingen van toegang met de minst mogelijke bevoegdheden en het gebruiken van werkstations met uitgebreide toegang (PAW's) voor het beheer van identiteitssystemen.
Onvoldoende toegangsrechten en controles op zijdelingse verplaatsing Beheerders hebben overmatige machtigingen in de digitale omgeving en stellen vaak beheerdersreferenties bloot op werkstations die onderhevig zijn aan internet- en productiviteitsrisico's.	Beveilig en beperk beheerderstoegang om de omgeving veerkrachtiger te maken en de omvang van een aanval te beperken. Gebruik controles voor Privileged Access Management, zoals just-in-time-toegang en Just Enough Administration.
Geen meervoudige verificatie (MFA) De aanvallers van vandaag breken niet in, maar melden zich aan.	MFA is een essentiële en fundamentele controle voor gebruikerstoegang die alle organisaties zouden moeten inschakelen. In combinatie met voorwaardelijke toegang kan MFA van onschatbare waarde zijn bij het bestrijden van cyberbedreigingen.
Beveiligingsactiviteiten met een lage volwassenheidsgraad De meeste getroffen organisaties gebruikten traditionele tools voor het detecteren van bedreigingen en beschikten niet over relevante inzichten voor tijdige respons en herstel.	Een uitgebreide strategie voor het detecteren van bedreigingen vereist investeringen in uitgebreide detectie en respons (XDR) en moderne cloud-native tools die gebruikmaken van machine learning om ruis van signalen te scheiden. Moderniseer tools voor beveiligingsbewerkingen door XDR op te nemen voor diepgaande beveiligingsinzichten in het digitale landschap.
Gebrek aan controle van informatiebeveiliging Organisaties blijven worstelen met het samenstellen van holistische informatiebeveiligingscontroles die volledige dekking bieden over datalocaties, effectief blijven gedurende de informatielevenscyclus en zijn afgestemd op de zakelijke relevantie van data.	Identificeer je essentiële bedrijfsdata en waar deze zich bevindt. Beoordeel de levenscyclusprocessen van informatie en dwing databescherming af met waarborging van de bedrijfscontinuïteit.
Beperkte acceptatie van moderne beveiligingsframeworks Identiteit is de nieuwe beveiligingsperimeter die toegang verleent tot ongelijksoortige digitale services en computeromgevingen. De integratie van Zero Trust-principes, applicatiebeveiliging en andere moderne cyberframeworks stelt organisaties in staat om op proactieve wijze risico's te beheren waar organisaties anders mogelijk moeilijk kijk op zouden krijgen.	Zero Trust-frameworks dwingen concepten af van minste bevoegdheden, expliciete verificatie van alle toegang en altijd uitgaan van schendingen. Ook moeten organisaties beveiligingscontroles en -praktijken implementeren in DevOps- en applicatielevenscyclusprocessen voor hogere betrouwbaarheidsniveaus in hun bedrijfssystemen.

De basishouding voor beveiliging is bepalend voor de effectiviteit van geavanceerde oplossingen

Door onze analyse ontdekten we een prevalentie van veelvoorkomende blinde vlekken in de verdediging van organisaties die aanvallers in staat stellen om de eerste toegang te krijgen, een steunpunt te vormen en een aanval uit te voeren, zelfs in aanwezigheid van geavanceerde beveiligingsoplossingen.

In veel gevallen wordt de uitkomst van een cyberaanval bepaald lang voordat de aanval van start gaat. Aanvallers maken gebruik van kwetsbare omgevingen om de eerste toegang te krijgen, op verkenning te gaan en schade aan te richten via zijdelingse verplaatsing en versleuteling of exfiltratie. Door een aanvaller in een vroeg stadium te stoppen, wordt de kans om de totale impact te verminderen enorm vergroot.

Microsoft bestudeerde specifieke configuraties in beveiligingsstatussen om de meest voorkomende tekortkomingen in de praktijk in deze omgevingen te identificeren. Dit stelde ons in staat om de meest voorkomende kwetsbaarheden te zien die werden uitgebuit tijdens door mensen uitgevoerde ransomwareaanvallen, waardoor de bedreigingsactoren toegang konden krijgen en ongemerkt een netwerk konden doorkruisen.

Basisbeveiligingsconfiguraties moeten zijn ingeschakeld

De apparaten van een organisatie die niet onboarded of verouderd zijn (zowel met betrekking tot kwetsbaarheden als de status van beveiligingsagenten) dienen als potentiële toegangspunten en toegangswegen voor aanvallers. We hebben geconstateerd dat onboarding van een bijgewerkte EDR- (endpointdetectie en -respons[1]) en EPP-oplossing (platform voor endpointbeveiliging[2]) weliswaar is een belangrijke stap vormt, maar geen garantie biedt dat ransomware wordt gestopt.

Geavanceerde oplossingen zoals EDR en EPP zijn van cruciaal belang om een aanvaller vroeg in de aanvalsstroom te detecteren en automatisch herstel en bescherming mogelijk te maken. Aangezien deze geavanceerde oplossingen echter afhankelijk zijn van een fundamenteel vermogen om een aanval te detecteren, moeten basisbeveiligingsconfiguraties worden ingeschakeld. We hebben zelfs een prevalentie waargenomen van scenario's met geavanceerde oplossingen die werden ondermijnd door de afwezigheid van basisbeveiligingsconfiguraties.

Best practices in beveiligingsconfiguraties zijn een grotere indicator van veerkracht dan de responstijd van SOC-analisten (Security Operations Center)

We zagen dat de tijd die een SOC-analist nodig heeft om een relevante waarschuwing te bekijken en erop te reageren met 70 procent verminderde gedurende een periode van zes maanden binnen onze klanten- en partnerpopulatie. Dit toegenomen bewustzijn is een goed teken. Hoewel de zichtbaarheid van de beveiligingsconfiguratie tot een verbetering van de prestaties van SOC-analisten leidde, vormde het mogelijk maken van productzichtbaarheid door het onboarden en updaten van de apparaten van de organisatie een betere voorspellende factor voor succesvolle preventie.

Risico van onbekende apparaten

In tegenstelling tot cloudnetwerken, waar klanten weten welke assets op welke besturingssystemen draaien, kunnen on-premises netwerken een breed scala aan apparaten bevatten, zoals IoT, desktops, servers en netwerkapparaten die niet door de organisatie worden gecontroleerd of beheerd.

Het gemiddelde bedrijfsnetwerk heeft meer dan 3500 aangesloten apparaten die niet worden beschermd door een EDR-agent en die mogelijk toegang hebben tot bedrijfsresources of zelfs tot waardevolle assets. Microsoft Defender voor Eindpunt (MDE) gebruikt netwerkinspectie om apparaten te detecteren en informatie te verstrekken over apparaatclassificaties voor degenen die op het netwerk zijn aangesloten, zoals apparaatnaam, besturingssysteemdistributie en apparaattype.

3500

gemiddeld aantal verbonden apparaten in een onderneming die niet worden beschermd door een endpointdetectie- en responsagent.

Voor apparaten die niet door een EDR-agent worden ondersteund, moet je je op zijn minst bewust zijn van hun bestaan en ze beschermen door kwetsbaarheden te beoordelen en de netwerktoegang te beperken.

Direct bruikbare inzichten

1. Zelfs geavanceerde oplossingen kunnen worden ondermijnd door het ontbreken van elementaire beveiligingsconfiguraties.
2. Investeer in best practices bij de configuratie van de beveiligingsstatus om je te beschermen tegen toekomstige aanvallen. Deze basisinstellingen leveren een enorm investeringsrendement op in termen van het vermogen van een organisatie om zich tegen aanvallen te verdedigen.
3. Onboard alle toepasselijke apparaten naar een EDR-oplossing.
4. Zorg ervoor dat je beveiligingsagenten bijwerkt en bescherming biedt tegen manipulatie om grotere zichtbaarheid en volledigere beschermingsvoordelen van producten mogelijk te maken.

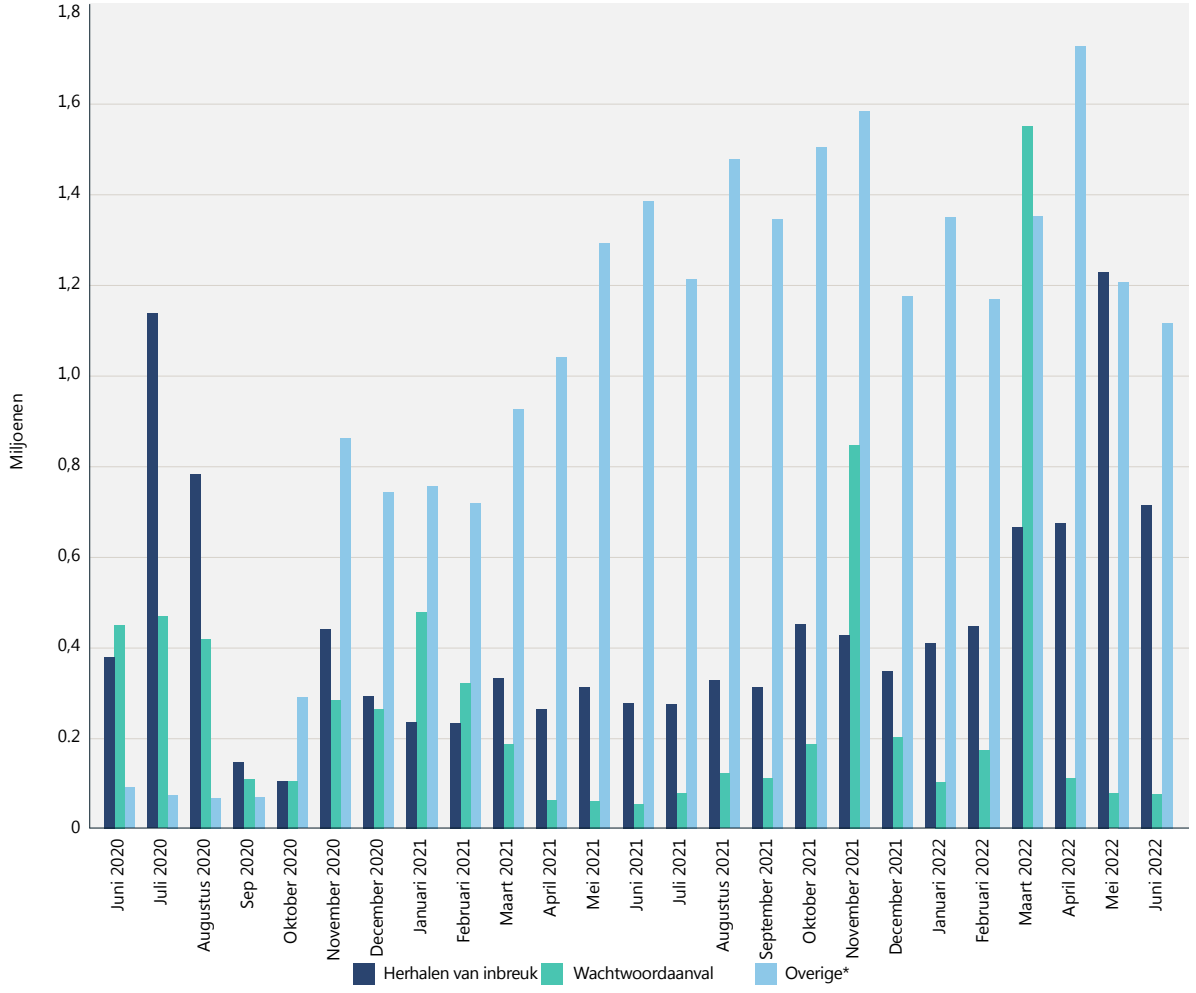
Handhaving van de gezondheid van identiteiten is van fundamenteel belang voor het welzijn van de organisatie

Bescherming van de identiteit is belangrijker dan ooit. Hoewel op wachtwoorden gebaseerde aanvallen de belangrijkste bron van identiteitsschendingen blijven, zijn ook andere typen aanvallen in opkomst. Het aantal geavanceerde aanvallen blijft toenemen ten opzichte van de vorige norm van wachtwoordspray-aanvallen en herhaling van inbreuken.

Op wachtwoorden gebaseerde aanvallen komen nog steeds veel voor en meer dan 90 procent van de accounts die via deze methoden zijn gehackt, zijn niet beveiligd met sterke verificatie. Bij sterke verificatie wordt meer dan één verificatiefactor gebruikt, bijvoorbeeld wachtwoord + sms en FIDO2-beveiligingssleutels.

We hebben een toename gezien van gerichte wachtwoordspray-aanvallen, met zeer sterke pieken in het volume van aanvallersverkeer verspreid over duizenden IP-adressen.

Gebruikers gehackt per aanvalscategorie



Gebruikers gehackt per maand per aanvalscategorie. De volumes van wachtwoordspray-aanvallen waren buitengewoon grillig, zoals te zien is aan de pieken in november 2021 en maart 2022. Deze pieken vertegenwoordigen duizenden gebruikers en duizenden aangetaste IP-adressen. *"Overig" geeft andere aanvallen aan dan wachtwoordspray en het herhalen van inbreuken, waaronder phishing, malware, man-in-the-middle, on-premises schending van tokenverstrekkers en andere. Bron: Azure AD Identity Protection.

4500

In de tijd die nodig is om deze verklaring te lezen, hebben we ons verdedigd tegen 4500 wachtwoordaanvallen.

Handhaving van de gezondheid van identiteiten is van fundamenteel belang voor het welzijn van de organisatie

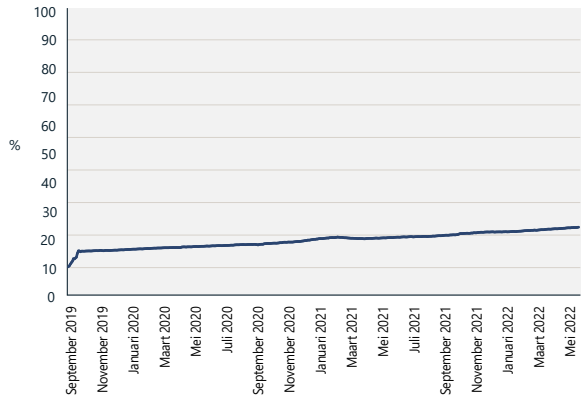
Vervolg

Sterke verificatie invoeren

Positief is dat we een gestage groei zien in de acceptatie van sterke verificatie bij de zakelijke klanten van Azure Active Directory (Azure AD). Voor Azure AD groeide het maandelijkse aantal actieve gebruikers met sterke verificatie (MAU) van 19 procent naar 26 procent in het afgelopen jaar, terwijl de MAU voor sterke verificatie voor beheerdersaccounts groeide van 30 naar ongeveer 33 procent.

Deze trend is positief, maar er is nog een aanzienlijke groei nodig om een meerderheidsdekking van sterke verificatie te bereiken. Klanten die in hun omgeving nog geen sterke verificatie gebruiken, moeten beginnen met het plannen en implementeren van sterke verificatie om hun gebruikers te beschermen.[3] Bij het ontwerpen van de implementatie van sterke verificatie moet wachtwoordloze verificatie worden overwogen, omdat dit de meest veilige bruikbare ervaring biedt en het risico van wachtwoordaanvallen wordt geëlimineerd.

Gebruik van sterke verificatie
(september 2019 – mei 2022)

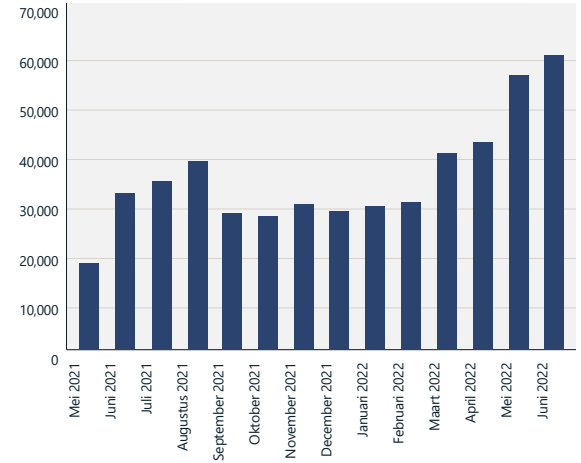


Hoewel het gebruik van sterke verificatie sinds 2019 is verdubbeld, gebruikt slechts 26 procent van de gebruikers en 33 procent van de beheerders sterke verificatie. Bron: Azure Active Directory.

Gestage toename van aanvallen via token replay

Het aandeel van andere aanvalsvormen nam in 2022 toe. We zagen een toename van gerichte aanvallen die met name wachtwoordgebaseerde verificatie ontwijken om de kans op detectie te verkleinen. Deze aanvallen maken gebruik van SSO-cookies (Single Sign-On) in de browser of vernieuwingstokens die zijn verkregen via malware, phishing en andere methoden. In sommige gevallen kiezen aanvallers voor infrastructuur op locaties in de buurt van de geografische locatie van de beoogde gebruiker om de kans op detectie verder te verkleinen. We hebben een gestage toename gezien van aanvallen via token replay, met meer dan 40.000 detecties per maand in Azure AD Identity Protection. Token replay is het gebruik van tokens die zijn uitgegeven aan een legitieme gebruiker door een aanvaller die in het bezit is van genoemde tokens. Tokens worden gewoonlijk verkregen via malware, bijvoorbeeld door de cookies uit de browser van de gebruiker te exfiltreren of via geavanceerde phishing-methoden.

Volume van gedetecteerde token replay-aanvallen



Gedetecteerde token replay-aanvallen per maand. Bron: Azure AD Identity Protection, unieke sessies die zijn gemarkeerd door de afwijkende tokendetectie.

Handhaving van de gezondheid van identiteiten is van fundamenteel belang voor het welzijn van de organisatie

Vervolg

Tokens extraheren

Meer nog dan malware hebben aanvallers referenties nodig om hun doelen te bereiken. In feite omvat 100 procent van alle door mensen uitgevoerde ransomwareaanvallen gestolen aanmeldingsreferenties. Veel geavanceerde inbreuken omvatten aanmeldingsreferenties die zijn gekocht op het dark web en aanvankelijk zijn gestolen via ongecompliceerde en wijdverbreide malware voor diefstal van aanmeldingsreferenties. Deze klasse van malware is geëvolueerd om tokens te stelen, met inbegrip van sessie-informatie en MFA-claims. Dit betekent dat infecties op thuissystemen, waarbij gebruikers zich aanmelden bij bedrijfsmiddelen, kunnen leiden tot ernstige incidenten op bedrijfsnetwerken.

Aanvallers kunnen ook tokens van de apparaten van slachtoffers halen via 'man-in-the-middle'-aanvallen, waarbij het slachtoffer op een schadelijke link in een phishing-e-mail of expresbericht klikt en wordt doorgestuurd naar een website die eruitziet als de legitieme aanmeldingspagina van de identiteitsleverancier. In werkelijkheid is het een webservice die is opgezet door de aanvaller en die al het verkeer tussen de gebruiker en de identiteitsprovider doorstuurt en onderschept. De aanvaller kan de gebruikersnaam en het wachtwoord onderscheppen en ook MFA-uitdagingen doorgeven, terwijl resulterende tokens die zijn uitgegeven door de identiteitsprovider en onderschept door de aanvaller, MFA-claims kunnen bevatten die door de aanvaller kunnen worden gebruikt om aan MFA-vereisten te voldoen.

Microsoft Defender for Cloud Apps heeft sinds begin 2022 gemiddeld 895 van dergelijke aanvallen per maand gedetecteerd. Deze vorm van aanval kan worden voorkomen door gebruik te maken van phish-resistente factoren van MFA, zoals Certificate Based Authentication, Windows Hello for Business of FIDO2-beveiligingssleutels.

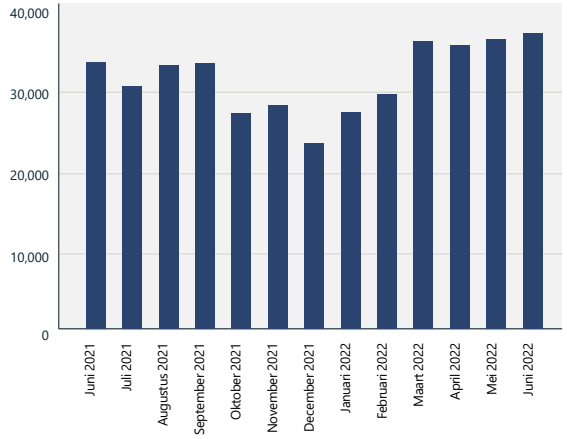
> Op wachtwoorden gebaseerde aanvallen vormen de primaire methode voor het hacken van accounts.

MFA-vermoeidheid

Met behulp van het concept van 'MFA-vermoeidheid' genereren aanvallers meerdere aanvragen voor MFA naar het apparaat van het slachtoffer, in de hoop dat het slachtoffer de aanvraag zal accepteren, hetzij per ongeluk, hetzij ten gevolge van vermoeidheid. Deze aanval kan worden voorkomen door gebruik te maken van moderne verificatieapps zoals Microsoft Authenticator in combinatie met functies zoals getalafstemming (number matching)[4] en inschakeling van extra context.[5] Azure AD Identity Protection schat dat er 30.000 MFA-vermoeidheidsaanvallen per maand plaatsvinden.

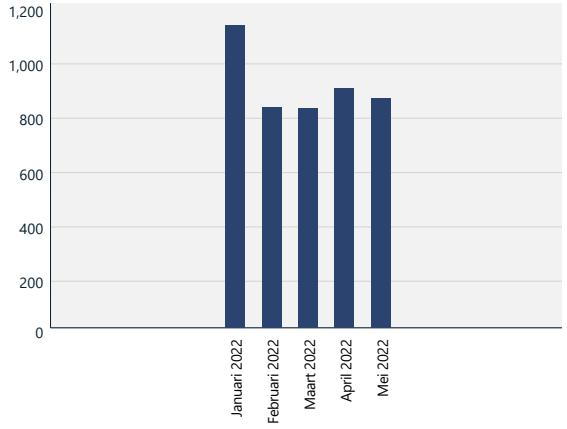
> Het aandeel van geavanceerde aanvallen blijft stijgen, wat de behoefte aan phish-resistente factoren van meervoudige verificatie onderstreept.

Geschatte aantal gevallen van MFA-vermoeidheidsaanvallen



Bron: Azure AD Identity Protection.

Gedetecteerde gevallen van phishing gevolgd door man-in-the-middle-aanvallen



Bron: Microsoft Defender for Cloud Apps.

Direct bruikbare inzichten

1. Zorg ervoor dat alle accounts in je organisatie worden beschermd door sterke verificatiemaatregelen.
2. Wachtwoordloze verificatie biedt de meest veilige en gebruiksvriendelijke ervaring, doordat het risico op wachtwoordaanvallen wordt geëlimineerd.
3. Schakel verouderde verificatie uit voor je hele organisatie.
4. Bescherm hoogwaardige en administratieve accounts met phish-resistente vormen van sterke verificatie.
5. Moderniseer van een on-premises identiteitsprovider naar een cloudidentiteitsprovider en verbind al je apps met de cloudgebaseerde identiteitsprovider voor een consistente gebruikerservaring en beveiliging.

Links naar verdere informatie

- Overweeg vanaf deze Wereldwachtwoorddag helemaal geen wachtwoorden meer te gebruiken | Microsoft Security

Standaardbeveiligings-instellingen van het besturingssysteem

Met het voortdurend evoluerende landschap van beveiligingsbedreigingen, zien we een toenemende behoefte aan computerbeveiliging die standaard is geconfigureerd om de cyberveerkracht te verbeteren. Hoewel de beveiliging van besturingssystemen urgenter, complexer en bedrijfskritischer is dan ooit tevoren, kan het een uitdaging zijn om dit goed te doen en te beheren.

In het verleden omvatte computer- en apparaatbeveiliging ingebouwde beveiligingsfuncties die de klant of IT-professional op het eigen gewenste niveau moest configureren. Deze aanpak is niet langer adequaat, omdat aanvallers meer geavanceerde tools gebruiken op het gebied van automatisering, cloudinfrastructuur en technologieën voor externe toegang om hun doelen te bereiken. Het is van cruciaal belang geworden dat alle beveiligingslagen, van de chip tot de cloud, standaard worden geconfigureerd. Microsoft is geëvolueerd om standaard de beveiliging van het Windows-besturingssysteem te configureren.[6]

Klanten die defensie volledig omarmen, inclusief een gelaagde beveiligingsstatus, nieuwe beveiligingsfuncties, regelmatige en consistente patches en updates, evenals beveiligingstraining en bewustzijn om phishing en andere vormen van oplichting te melden, kunnen minder malware verwachten.

Om diepgaande verdediging te vereenvoudigen, heeft Windows 11 strak geïntegreerde hardware- en softwarebeveiliging die standaard is ingeschakeld, met inbegrip van geheugenintegriteit, Secure Boot en een Trusted Platform Module 2.0. Windows 10-gebruikers op geschikte hardware kunnen deze functies ook inschakelen in de app Windows-instellingen of in het BIOS-menu.

Oudere apparaten hebben over het algemeen vaak niet zo'n sterke afstemming tussen hardwarebeveiliging en softwarebeveiligingstechnieken. Voor apparaten waarop beveiliging niet standaard is ingeschakeld, moet deze waar mogelijk handmatig worden geconfigureerd in de instellingen.[7]

Voor apparaten waarop beveiliging niet standaard is ingeschakeld, adviseert Microsoft deze waar mogelijk handmatig te configureren.

Wees proactief bij het toepassen van continue updates van het besturingssysteem en beveiligingspatches die bescherming bieden gedurende de hele hardware- en softwarelevenscyclus.

Direct bruikbare inzichten

1. Gebruik een wachtwoordloze oplossing die aanmeldingsreferenties in de Trusted Platform Module bindt. Zoek daarbij specifiek naar een wachtwoordloze oplossing die voldoet aan de industrienorm van de Faster Identity Online (FIDO) Alliance[8].
2. Voer tijdig een opschoonactie uit van alle ongebruikte en verouderde uitvoerbare bestanden die op de apparaten van organisaties staan.
3. Bied bescherming tegen geavanceerde firmwareaanvallen door geheugenintegriteit, Secure Boot en Trusted Platform Module 2.0 in te schakelen, indien niet standaard ingeschakeld. Dit versterkt de opstartprocedure met behulp van mogelijkheden die zijn ingebouwd in moderne CPU's.
4. Schakel dataversleuteling en bescherming van aanmeldingsreferenties in.
5. Schakel applicatie- en browserbesturingselementen in voor verbeterde bescherming tegen niet-vertrouwde applicaties en andere ingebouwde beveiligingen tegen exploits.
6. Schakel geheugentoegangsbeveiliging in om bescherming te helpen bieden tegen toevallige fysieke aanvallen, zoals iemand die een schadelijk apparaat aansluit op extern toegankelijke poorten.

Links naar verdere informatie

- Windows Security Book | Commercial
- Nieuwe beveiligingsfuncties voor Windows 11 helpen hybride werk te beschermen | Microsoft Security Blo

Supply chain-centraliteit voor software

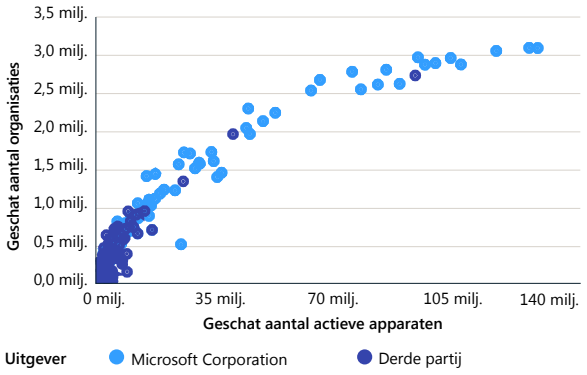
Aanvallen op apps, plug-ins en extensies van derden kunnen het vertrouwen van de klant aantasten in leveranciers die een centrale rol spelen in het leveringsecosysteem. Via het gebruik van netwerktheorie om te kijken naar de centraliteit van software, wordt het belang van patching duidelijk, vooral voor centrale apps.

Het Windows App Network van 18 miljoen uitvoerbare programma's wordt geïnstalleerd en gebruikt door vijf miljoen organisaties en biedt een overzicht op het hoogste niveau van ons software-ecosysteem. Van de 100.000 meest gebruikte applicaties wordt 97 procent geproduceerd door externe organisaties waarvan de updates en beveiligingspatches door hen worden onderhouden. Dit illustreert twee belangrijke kenmerken van ons commerciële applicatie-ecosysteem.

Ten eerste is er een centrale plaats in het ecosysteem van commerciële Windows-applicaties. Alleen de top 100.000 (van de 18 miljoen) applicaties worden gebruikt op 1000 of meer apparaten. Met andere woorden: slechts iets meer dan de helft van één procent van deze applicaties heeft een dergelijk verstrekkend effect op het ecosysteem van het apparaat.

Ten tweede is er diversiteit in de beheerbaarheid van die applicaties, waarbij de top 10.000 applicatieleveranciers de updates en beveiligingspatches van deze meest gebruikte commerciële applicaties beheren. Dit toont aan hoe afhankelijk een bedrijf is van een diverse reeks beveiligings-, compliance- en managementcontroles van softwareleveranciers.

Commerciële penetratie van de meest gebruikte applicaties



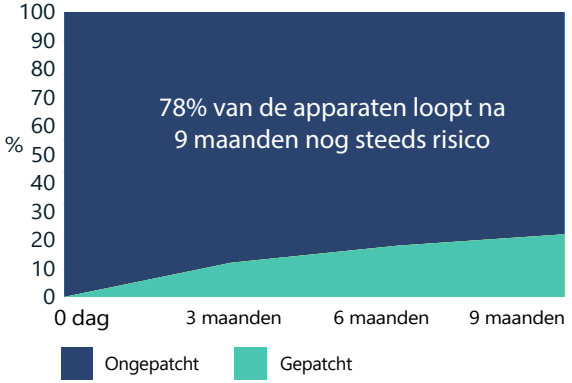
De topapplicaties worden gebruikt door miljoenen organisaties en tientallen miljoenen apparaten. Omdat ze bijna alomtegenwoordig zijn, zijn tegenstanders constant op zoek naar kwetsbaarheden in deze topapplicaties die miljoenen apparaten in het gebruikersbestand kunnen treffen.

We zien dat miljoenen commerciële apparaten nog steeds kwetsbare applicatieversies gebruiken, vele maanden na het uitbrengen van de patch of zelfs jaren na het einde van de productsupport. Er zijn bijvoorbeeld meer dan een miljoen actieve commerciële Windows-apparaten met een versie van een PDF-lezer die sinds 2017 niet meer wordt ondersteund.

Oude versies van applicaties die niet worden ondersteund, blijven actief in gebruik op miljoenen commerciële apparaten. Als gevolg hiervan lopen organisaties het risico kwetsbaarheden met zich mee te dragen die niet worden gepatcht.

Voor applicatieversies met actieve support zien we een afvlakking van de snelheid van invoering van essentiële patches, wat het tegenovergestelde is van de trend waarbij de veerkracht wordt gestimuleerd. In plaats daarvan zou de curve maandelijks een exponentiële opwaartse acceptatie van patches moeten laten zien, om de vereiste veerkracht te bereiken.

Snelheid van implementatie van essentiële patches



Na onderzoek van een kritieke kwetsbaarheid die 134 versies van een reeks browsers trof, ontdekten we dat 78 procent, of miljoenen apparaten, negen maanden nadat de patch was uitgebracht, nog steeds een van de getroffen versies gebruikte.

We gebruikten de InterpretML[9]-toolkit om kenmerken te identificeren die verband houden met organisaties die vaker over apparaten met oudere app-versies beschikken. De belangrijkste van deze voorspellende factoren waren: weinig uren betrokkenheid op apparaten; geografische gebieden zoals Azië-Pacific en Latijns-Amerika; en bedrijfstakken zoals auto's, chemicaliën, telecommunicatie, transport en logistiek, zorgverzekeraars (claimbehandelaars) en verzekeringswezen.

Onderhoud van de softwareveerkracht moet het regelmatig uitschakelen of verwijderen van ongebruikte applicaties omvatten.

De beveiliging en compliance van een organisatie hangt af van de eigen inspanningen en van de inspanningen van haar softwareleveranciers.

Direct bruikbare inzichten

1. Voer tijdig updates uit voor alle applicaties en endpoints via je organisatie.
2. Voer tijdig een opschoonactie uit van alle ongebruikte en verouderde uitvoerbare bestanden die op de apparaten van organisaties staan.

Links naar verdere informatie

- Microsoft Intune-documentatie | Microsoft Docs
- Apps beheren | Microsoft Docs
- Microsoft Defender voor Eindpunt | Microsoft Security
- OSS Secure Supply Chain Framework | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

Veerkracht opbouwen tegen nieuwe DDoS-, webapplicatie- en netwerkaanvallen

Versnelde digitale transformatie heeft een einde gemaakt aan het traditionele netwerk- en beveiligingsperimetermodel. De overstap naar de cloud betekent dat bedrijven cloud-native netwerkbeveiliging moeten toepassen ter bescherming van digitale assets.

De complexiteit, de frequentie en het volume van aanvallen blijven groeien en zijn niet langer beperkt tot vakantieseizoenen, wat wijst op een verschuiving naar aanvallen het hele jaar door. Dit benadrukt het belang van doorlopende bescherming na de traditionele seizoenen met druk verkeer.

Distributed Denial of Service-aanvallen (DDoS)

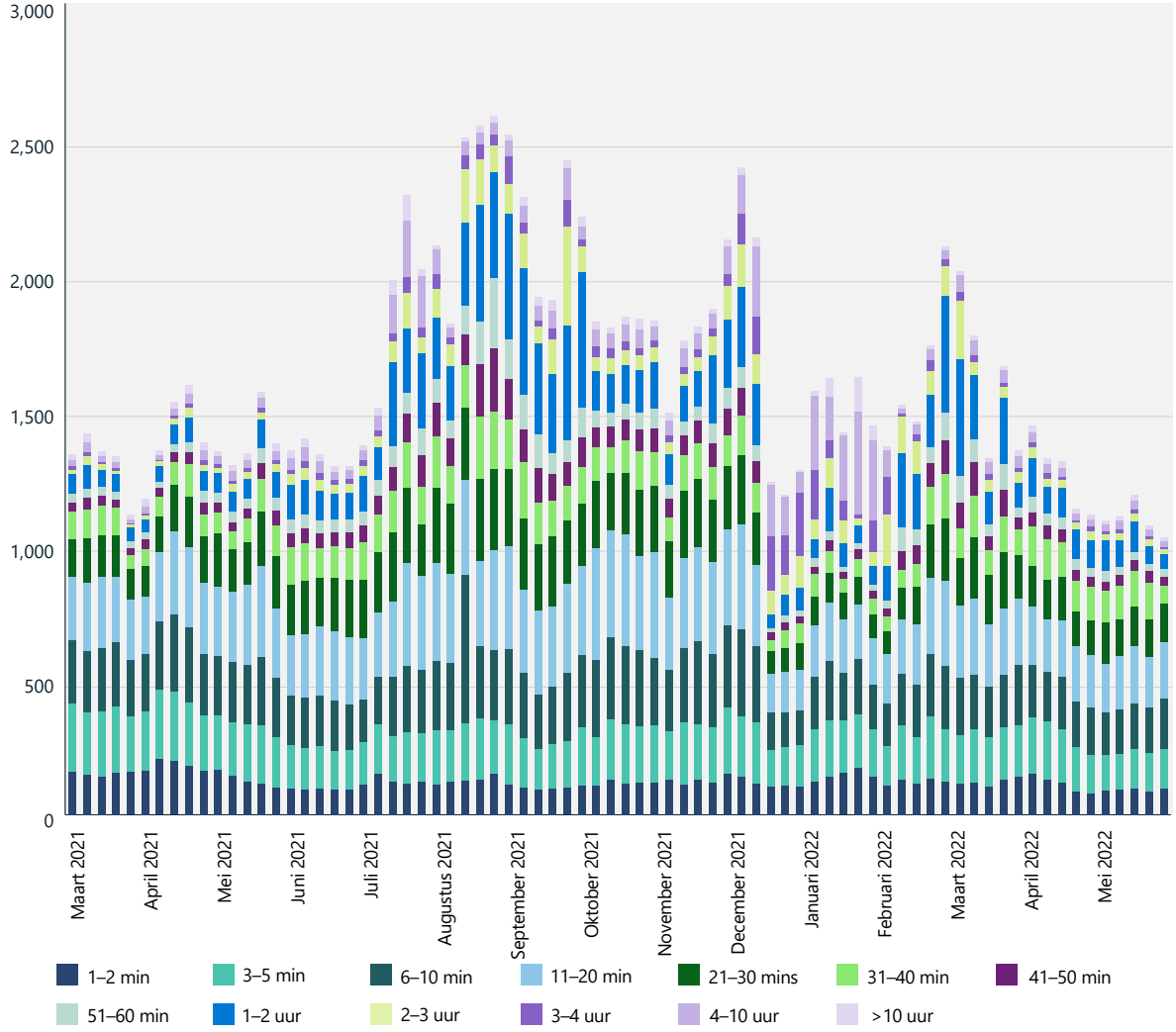
In het afgelopen jaar heeft de wereld te maken gehad met DDoS-activiteiten die ongekend waren in volume, complexiteit en frequentie. Deze DDoS-explosie werd veroorzaakt door een substantiële toename van aanvallen door vreemde mogendheden en een aanhoudende verspreiding van goedkope DDoS-for-hire-services. Microsoft loste gemiddeld 1955 aanvallen per dag op, een stijging van 40 procent ten opzichte van het voorgaande jaar. Voorheen vond het piekaantal aanvallen normaal gesproken plaats tijdens de eindejaarsperiode. Dit jaar werden echter de meeste aanvallen op een dag geregistreerd op 10 augustus 2021. Dit kan wijzen op een verschuiving naar aanvallen het hele jaar door en benadrukt het belang van voortdurende bescherming buiten de traditionele piekseizoenen.

In november 2021 verijdelde Microsoft een volumetrische DDoS-aanval met een doorvoer van 3,4 terabit per seconde (Tbps) uit ongeveer 10.000 bronnen verspreid over meerdere landen. In 2022 werden vergelijkbare aanvallen met een hoog volume van meer dan 2 Tbps verijdeld, wat erop wijst dat niet alleen de complexiteit en frequentie van aanvallen toeneemt, maar ook het aanvalsvolume (bandbreedte).

Duur van aanvallen

De meeste aanvallen die het afgelopen jaar zijn waargenomen, waren van korte duur. Ongeveer 28 procent van de aanvallen duurde minder dan 10 minuten, 26 procent duurde 10-30 minuten en 14 procent duurde 31-60 minuten. Tweeëndertig procent van de aanvallen duurde meer dan een uur.

Aantal DDoS-aanvallen en duurverdeling
(maart 2021–mei 2022)



De meeste aanslagen in het afgelopen jaar waren van korte duur. Ongeveer 28 procent van de aanvallen duurde minder dan 10 minuten.

Veerkracht opbouwen tegen nieuwe DDoS-, webapplicatie- en netwerkaanvallen

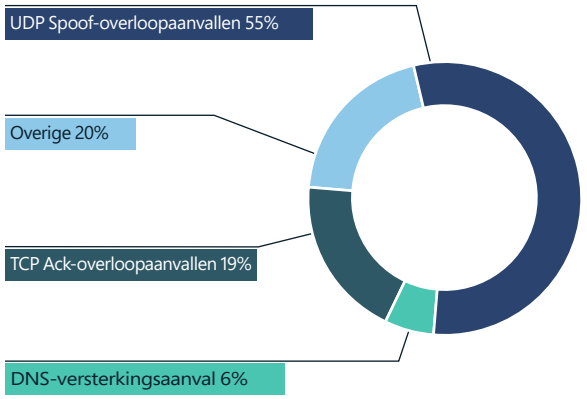
Vervolg

DDoS-aanvalsvectoren

In het afgelopen jaar bestonden de meest gebruikte aanvalsvectoren uit UDP-reflectie (User Datagram Protocol) op poort 80 met behulp van het Simple Service Discovery Protocol (SSDP), Connectionless Lightweight Directory Access protocol (CLDAP), Domain Name System (DNS) en Network Time Protocol (NTP) met een enkele piek. We zagen ook een toename van DDoS-aanvallen op de applicatielaag die waren gericht tegen websites, met 16,3 miljoen piek-RPS (aanvragen per seconde) en piekverkeer van 9,89 Tbps.

In 2022 handelde Microsoft bijna 2000 DDoS-aanvallen per dag af en verijdelde het de grootste DDoS-aanval die ooit werd gerapporteerd in de geschiedenis.

DDoS-aanvalsvectoren



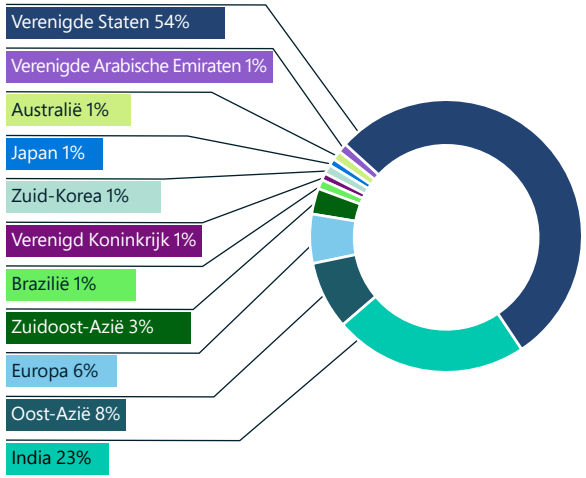
De UDP Spoof-overloopaanval groeide uit tot topvector in de eerste helft van 2022, van 16 procent naar 55 procent. De TCP Ack-overloopaanval nam af van 54 procent naar 19 procent.

De game-industrie blijft het belangrijkste doelwit van DDoS-aanvallen, voornamelijk door mutaties van het Mirai-botnet en laag-volume UDP-protocolaanvallen. Aangezien UDP vaak wordt gebruikt in gaming- en streamingapplicaties, bestond een overweldigende meerderheid van de aanvalsvectoren uit UDP-spoof-floods, terwijl een klein deel UDP-reflectie- en versterkingsaanvallen waren.

Geografische doelregio's

Van de DDoS-aanvallen die het afgelopen jaar zijn gedetecteerd, werd 54 procent uitgevoerd tegen doelen in de Verenigde Staten, een trend die gedeeltelijk kan worden verklaard door het feit dat de meeste Azure- en Microsoft-klanten zich in de Verenigde Staten bevinden. We zagen ook een sterke stijging van de aanvallen op India, van slechts 2 procent van alle aanvallen in de tweede helft van 2021 tot 23 procent in de eerste helft van 2022. Oost-Azië, met name Hongkong, blijft met 8 procent een populair doelwit. Voor Europa zagen we concentraties van aanslagen op de regio's Amsterdam, Wenen, Parijs en Frankfurt.

Bestemming van DDoS-aanvallen

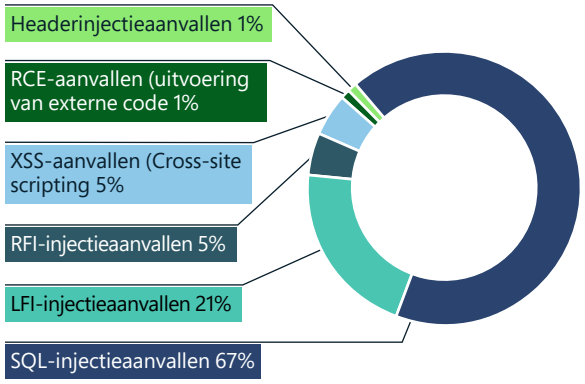


We schrijven het grote aantal aanvallen in Azië toe aan de enorme gamingvoetafdruk van de regio, vooral in China, Japan, Zuid-Korea en India. Deze voetafdruk zal blijven groeien naarmate de toenemende penetratie van smartphones de populariteit van mobiel gamen stimuleert, wat suggereert dat dit geografische doelwit alleen maar zal blijven groeien.

Exploits in webapplicaties

Web Application Firewall (WAF), in combinatie met DDoS-bescherming, vormt een integraal onderdeel van een diepgaande verdedigingsstrategie voor het beschermen van web- en API-assets (Application Programming Interface). Microsoft heeft meer dan 300 miljard WAF-regels waargenomen die per maand worden geactiveerd via Azure WAF's.

Verspreiding van meest voorkomende aanvalstypen



Azure WAF detecteert dagelijks miljarden Open Web Application Security Project (OWASP) Top 10^{10}-aanvallen. Volgens onze signalen probeerden aanvallers het vaakst SQL-injectieaanvallen, gevolgd door aanvallen via lokale bestandsinjectie en externe bestandsinjectie. Dit is in lijn met de OWASP Top Tien-lijst die injectieaanvallen als het op twee na meest voorkomende type webaanvallen laat zien.

Er is ook een toename van botaanvallen op Azure-webapplicaties te zien, met gemiddeld 1,7 miljard botaanvragen per maand, waarbij 4,6 procent van dat verkeer uit schadelijke bots bestaat.

Veerkracht opbouwen tegen nieuwe DDoS-, webapplicatie- en netwerkaanvallen

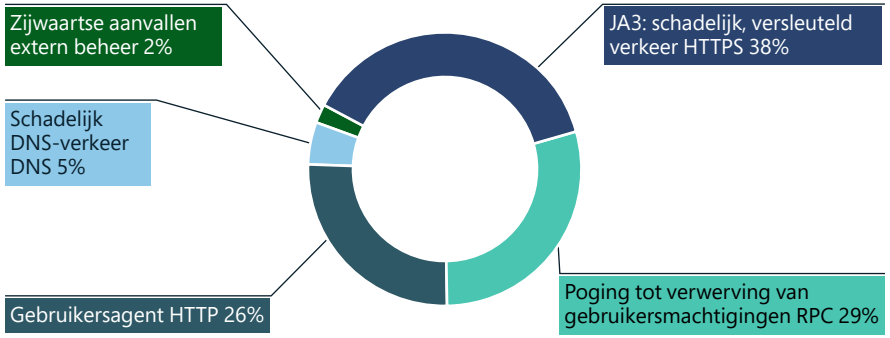
Vervolg

Vanwege een toenemend aantal bots dat aanvallen uitvoert met gestolen referenties, creditcardfraude, cyberbeïnvloedingscampagnes en supply chain-aanvallen, verwachten we een gestage toename van botaanvallen op webapplicaties.

Netwerkinbreuken: detectie en preventie

We hebben in 2022 een significante toename waargenomen in exploits van netwerklagen, met name malware. Het Azure Firewall-systeem voor inbreukdetectie en preventie (IDPS) blokkeerde alleen al in de maand juni meer dan 150 miljoen verbindingen.

IDPS-reden voor weigering van verkeer



Redenen voor IDPS-verkeerswaarschuwingen

Analyse van IDPS-waarschuwings- en weigeringsverkeer toont de volgende benaderingen die door aanvallers worden gebruikt. Bij het weigeringsverkeer zien we dat aanvallers SSL gebruiken om hun activiteiten te verbergen, terwijl aanvallen op afstand steeds vaker voorkomen. Bij het waarschuwingsverkeer zien we SMB/SMB2-protocollen die worden gebruikt om aanvallen op afstand uit te voeren.

Direct bruikbare inzichten

1. Inspecteer al het verkeer tussen systemen binnen een datacenter of cloudservice en het verkeer dat toegang zoekt.
2. Ontwikkel een robuuste responsstrategie voor netwerkbeveiliging, het hele jaar door.
3. Gebruik cloudeigen beveiligingsservices om een robuuste, Zero Trust-netwerkbeveiliging te implementeren.

Links naar verdere informatie

- Verbeter je beveiliging tegen ransomwareaanvallen met Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Anatomie van een DDoS-versterkingsaanval | Microsoft Security Blog
- Intelligente applicatiebescherming van edge tot cloud met Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Een evenwichtige aanpak voor databeveiliging en cyberveerkracht ontwikkelen

De digitale transformatie heeft geleid tot een enorme uitbreiding van data-assets en een toename van beveiligings-, compliance- en privacyrisico's. Organisaties met cyberveerkracht moeten investeringen in databescherming, compliance en herstelmogelijkheden in evenwicht brengen en deze integreren met gespecialiseerde responsprocessen van regelgevende instanties om verschillende soorten inbreuken aan te pakken.

Datalekken zijn niet een kwestie van of, maar wanneer. De studie "Cost of a Data Breach, 2021" van IBM en het Ponemon Institute meldt een wereldwijde gemiddelde kostenpost voor datalekken van $ 4,24 miljoen (een stijging van 10 procent ten opzichte van het voorgaande jaar) en $ 9,05 miljoen in de Verenigde Staten. Compliancefouten bleken de belangrijkste kostenverhogende factor te zijn. Omgekeerd waren kostenbesparingen bij inbreuken geassocieerd met best practices zoals planning voor incidentrespons (IR), volwassenheid van Zero Trust-implementatie, AI en automatisering van beveiliging en het gebruik van encryptie.

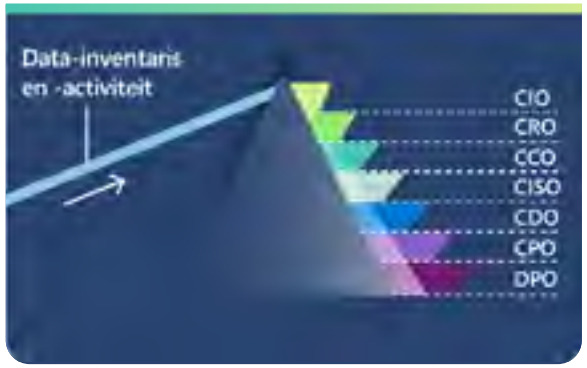
Datalekken zijn onvermijdelijk. Organisaties die een evenwichtige veerkrachtbenadering hanteren, zullen de frequentie, impact en kosten van inbreuken zien afnemen.

Databeheer, beveiliging, compliance en privacy zijn onderling afhankelijk

We hebben de afgelopen jaren gezien dat data aan belang winnen als essentiële motor voor waardecreatie voor organisaties. Tegelijkertijd heeft de opkomst van privacyregelgeving die zowel databeheer als beveiliging vereist, de grenzen tussen risicorollen vervaagd. Hoewel nieuwere functies op C-niveau, zoals de Chief Data Officer (CDO) of de Chief Privacy Officers (CPO), een gevestigd belang hebben bij beveiliging en compliance, is de implementatie en operationalisering van databescherming vaak afhankelijk van teams onder leiding van de Chief Information Officer (CIO) en/of Chief Information Security Officer (CISO). Het is geen eenrichtingsverkeer, aangezien initiatieven op het gebied van datagovernance onder leiding van CDO's ook beveiligingsvoordelen hebben. Als gevolg van deze onderlinge verbondenheid moeten IT-, datagovernance-, beveiligings-, compliance- en privacyteams steeds nauwer samenwerken om efficiëntie te bereiken en risico's te beheersen.

Uniforme platforms voor datarisicobeheer voor het datadomein van de hele organisatie hebben de toekomst

Het op elkaar afstemmen van het IT-, datagovernance-, beveiligings-, compliance- en privacybeheerproces is moeilijk in een omgeving van op maat gemaakte applicaties voor elke discipline en inconsistente dekking over de typische wildgroei van hybride, multicloud data binnen de organisatie. Wij zijn van mening dat organisaties een enkel toegangspunt nodig hebben om hun data te lokaliseren en kennen, hun data te beschermen, de toegang te regelen, het gebruik en de levenscyclus van data te beheren en dataverlies in het hele datadomein te voorkomen. Werken vanuit dezelfde data-inventaris en activiteitsinformatie faciliteert teamoverschrijdende processen, levert een uitgebreider risicobeeld op en stelt organisaties in staat om hun respons op een inbreuk beter voor te bereiden en te stroomlijnen.



De 'enkele glasplaat' moet als prisma fungeren. Teams die belang hebben bij databeveiliging, compliance en privacy hebben verschillende maar consistente weergaven van dezelfde data-inventaris en -activiteit nodig om op één lijn te komen en samen te werken. Data-activiteit omvat datatoegang, wijziging en verplaatsingsgebeurtenissen, die een waardevol onderdeel vormen van de vergelijking voor databeveiliging.

Effectief databeheer, beveiliging, compliance en privacy zijn onderling afhankelijk en vereisen samenwerking tussen teams.

Direct bruikbare inzichten

1. Breng de verdediging in evenwicht met herstel en minimaliseer de impact van datalekken door te investeren in compliance, databescherming en responsmogelijkheden.
2. Ontwikkel en adopteer processen en tools die datarisicosilo's doorbreken en het volledige datadomein omvatten.

Links naar verdere informatie

- Microsoft Purview—Oplossingen voor databescherming | Microsoft Security
- De toekomst van compliance en datagovernance is hier: Introductie van Microsoft Purview | Microsoft Security Blog

Veerkracht van cyber-beïnvloedingsactiviteiten: de menselijke dimensie

In de afgelopen vijf jaar hebben de ontwikkelingen op het gebied van graphics en machine learning gebruiksvriendelijke tools geïntroduceerd waarmee snel hoogwaardige, realistische content kan worden gegenereerd die zich binnen enkele seconden over het internet kan verspreiden.

Als het gaat om gebeurtenissen die worden gerapporteerd via tekst, audio en visuele content, hebben we een punt bereikt waarop noch mensen noch algoritmen onderscheid kunnen maken tussen feit en fictie. De wildgroei van deze tools en de resultaten daarvan doen twijfels rijzen over de betrouwbaarheid van alle digitale media en verstoren onze inzichten in lokale en wereldwijde gebeurtenissen. Nieuwe vormen van beïnvloedingsactiviteiten die mogelijk worden gemaakt door technologische vooruitgang, hebben ernstige gevolgen voor democratische processen.[11]

Er ontstaan vragen over wat we kunnen doen om ons voor te bereiden op een veerkrachtiger toekomst tegen deze cyberbeïnvloedingsactiviteiten. Technologie is slechts één deel van de puzzel. Het gaat meerdere inspanningen vergen, waaronder onderwijs gericht op mediageletterdheid, bewustwording en waakzaamheid, investeringen in kwaliteitsjournalistiek met vertrouwde verslaggevers ter plekke, lokaal, nationaal en internationaal, netwerken voor het delen van informatie en waarschuwingen over beïnvloedingsactiviteiten, en nieuwe typen regelgeving voor het bestraffen van kwaadwillende actoren die digitale media genereren of manipuleren met misleiding als doel.

We erkennen ook dat het herstellen van vertrouwen in digitale content een ambitieus doel is dat verschillende perspectieven en participatie vereist. Er is niet één bedrijf, instelling of overheid die deze bedreigingen alleen kan oplossen. Onze superkracht als mens is ons vermogen om samen te werken. Dit is nu vooral belangrijk omdat iedereen, van wereldwijde overheden, industrieën, de academische wereld en vooral nieuws-, sociale en mediaorganisaties, moet samenwerken om onze samenleving beter en gezonder te maken.

Links naar verdere informatie

- Applications for artificial intelligence in Department of Defense cyber missions | 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 mei 2022; getuigenis van Eric Horvitz)

De menselijke factor versterken met vaardigheden

Het aanpakken van de menselijke factor is een belangrijk onderdeel van elke strategie voor vaardigheden op het gebied van cyberbeveiliging. Volgens een onderzoek van Kaspersky Human Factor in IT Security[12] gaat het bij 46 procent van de cyberbeveiligingsincidenten om onzorgvuldig of ongeïnformeerd personeel dat onbedoeld de aanval vergemakkelijkt.

Het Education and Awareness-team in de Digital Security and Resilience-organisatie van Microsoft is verantwoordelijk voor het versterken van de menselijke factor van cyberbeveiliging door werknemers in staat te stellen onze eigen systemen en data en die van onze klanten te beveiligen. Onze doelen zijn:

- Het verminderen van het risico voor Microsoft en onze klanten door een centrale beveiligingsbrede vaardighedenset voor de hele werknemerspopulatie op ondernemingsniveau op te bouwen.
- Versterk de beveiligingskennis van werknemers door middel van een meerfasenaanpak voor trainingsversterking ter ondersteuning van het gewenste gedrag.
- Bevorder cultuurverandering door een beveiligingsmentaliteit tot intrinsiek onderdeel van de cultuur van Microsoft te maken door middel van jaarlijks vereiste beveiligingstrainingen en -evenementen.
- Bevorder een centrale webresource voor best practices, informatie over bedrijfsbeleid en incidentrapportage voor alles wat met cyberbeveiliging te maken heeft.

Een gericht, gecentraliseerd vaardigheidsprogramma voor cyberbeveiliging bereikt elke werknemer van Microsoft ten minste eenmaal per jaar. Het trainingsaanbod is geoptimaliseerd om huidige cyberbeveiligingsinitiatieven te ondersteunen en meetbare gedragsresultaten te leveren. De Information Risk Management Council (IRMC) van Microsoft speelt een belangrijke rol bij het identificeren van belangrijke resultaten van gedragsverandering in cyberbeveiliging die door training moeten worden aangepakt.

Met al onze vaardigheidsprogramma's voor cyberbeveiliging meten we waar mogelijk de efficiëntie, effectiviteit en resultaten van de oplossing. Ons aanbod van vaardigheden voor bedreigingen door insiders wordt bijvoorbeeld gekenmerkt door 95 procent trainingsnaleving, uitzonderlijke tevredenheid onder studenten en leerlingen en een aanzienlijke toename van managers die mogelijke bedreigingen van binnenuit melden via de Report It Now-tool van het bedrijf. Het programma omvat:

Security Foundations: gecentraliseerde, ondernemingsbrede training voor cyberbewustzijn en naleving waarin de belangrijkste beveiligings- en privacypraktijken aan bod komen. Deze langverwachte trainingsreeks maakt gebruik van een edutainment-model om het leren over cyberbeveiliging boeiend en interessant te maken.

STRIKE: de verplichte technische training van Microsoft voor technici die brancheoplossingen bouwen en onderhouden. Deze training is alleen toegankelijk op uitnodiging en heeft tijdige en kritieke best practices op het gebied van cyberbeveiligingshygiëne als onderwerp. Hierbij wordt gebruikgemaakt van een live hybride leveringsmodel dat is afgestemd op de behoeften van de doelgroep.

Programmaspecifiek: gerichte trainingsprogramma's ondersteunen specifieke cyberbeveiligingsinitiatieven, waaronder Shadow IT, Insider Threat en Microsoft Federal. Deze aanbiedingen zijn nauw geïntegreerd in de algehele betrokkenheidsstrategie voor hun respectievelijke cyberbeveiligingsinitiatieven via executive sponsoring en scorecardrapportage om een trainingsaanpak te voorkomen waarbij alleen vakjes hoeven te worden aangevinkt.

MSProtect: een centrale webresource van Microsoft die best practices, informatie over bedrijfsbeleid en incidentrapportage omvat voor alles wat met cyberbeveiliging te maken heeft. Deze on-demand resource is de beste keuze voor werknemers buiten het formele trainingsaanbod.

> Beveiligingsvaardigheden mogen niet worden gezien als een nalevingsactiviteit waarbij alleen vakjes hoeven te worden aangevinkt. Richt je in plaats daarvan op gedragsverandering om de resultaten van geïdentificeerd doelgedrag te kunnen monitoren en luister naar systemen om de impact van het aanbod te bepalen.

Direct bruikbare inzichten

1. Bied beveiligingstrainingen en -resources aan werknemers wanneer en waar ze die nodig hebben.
2. Ontwikkel een gecentraliseerde vaardigheidsstrategie op basis van informatie van stakeholders uit de hele onderneming.
3. Zorg ervoor dat de impact van training wordt bijgehouden en geanalyseerd op efficiëntie (kwantiteit), effectiviteit (kwaliteit) en resultaten (zakelijke impact).

Links naar verdere informatie

- Microsoft launches next stage of skills initiative after helping 30 million people

Inzichten uit ons eliminatieprogramma voor ransomware

Microsoft heeft de afgelopen vijf jaar een eigen Zero Trust-traject[13] doorlopen om ervoor te zorgen dat identiteiten en apparaten op robuuste wijze worden beheerd en gezond zijn. Naarmate het risico op ransomware toeneemt, hebben we een diepere visie ontwikkeld ter ondersteuning van onze aanpak om onszelf en onze klanten te beschermen.

Na een diepgaande interne evaluatie, hebben we een eliminatieprogramma voor ransomware ontwikkeld om hiaten in controles en dekking te verhelpen, bij te dragen aan functieverbeteringen voor services zoals Defender for Endpoint, Azure en M365, en om playbooks te ontwikkelen voor onze SOC- en engineeringteams met herstelprocedures in het geval van een ransomwareaanval.

De eerste stap was het begrijpen van de omvang van onze bescherming tegen een ransomwareaanval die was gericht op Microsoft. Er werden al inspanningen geleverd om Defender for Endpoint te implementeren en om ervoor te zorgen dat alle apparaten worden beheerd en voldoen aan ons Zero Trust-beleid, maar we moesten een manier vinden om inzicht te krijgen in alle facetten van de grotere vraag of een effectief herstel van een aanval mogelijk was. Om inzicht te verwerven hebben we NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile[14] geëvalueerd, dat in overeenstemming is met ons algemene beleid voor ondernemingen ten opzichte van onze bekende lijst met controles. Bij deze analyse werden snel hiaten in de dekking geïdentificeerd.

Vervolgens hebben we de prioriteit bepaald van hiaten in de functies Identificeren, Detecteren, Beschermen, Reageren en Herstellen van de CSF. We hebben strategische afstemming gevonden met Zero Trust en andere programma's en ontdekten bovendien hiaten waar bestaande workstreams ontbraken. Nadat we de hoeveelheid werk en inspanning hadden beoordeeld die nodig was om deze hiaten te verhelpen, hebben we ze in twee pijlers onderverdeeld:

- **Protect the enterprise (Bescherm de onderneming, PtE):** definieer werkitems die we als onderneming moeten uitvoeren om onszelf te beschermen en te kunnen herstellen van een eventuele geslaagde aanval.
- **Protect the customer (Bescherm de klant, PtC):** bouw mogelijkheden in ons aanbod in om zowel onze klanten als ons bedrijf te beschermen.

Inbedding van bevindingen in onze eigen onderneming

Om de belangrijkste risico's te verhelpen en onze essentiële services te beschermen tegen een ransomwareaanval, zijn we van plan om de komende zes tot twaalf maanden te focussen op het realiseren van de vijf onderstaande scenario's als onderdeel van een speciaal ransomware-programma. Zodra we in elk van de scenario's zijn geslaagd, breiden we de reikwijdte van het programma geleidelijk uit naar alle delen van de onderneming.

Scenario 1: leden van het beveiligingsteam begrijpen het algehele risico dat gepaard gaat met een ransomwareaanval en hebben een proces opgesteld om de leidinggevenden bewust te maken van lacunes in de controle en risicostatus.

Scenario 2: leden van het beveiligingsteam hebben toegang tot playbooks die zijn ontworpen om hen en andere teams binnen Microsoft te helpen reageren op essentiële services en deze te herstellen van een ransomwareaanval.

Scenario 3: leden van het Enterprise Resilience-team hebben een te volgen norm voor de back-up van essentiële systemen. Er bestaan playbooks en er worden regelmatig back-ups en herstelbewerkingen uitgevoerd om ervoor te zorgen dat data kunnen worden hersteld in het geval van een ransomwareaanval.

Scenario 4: service-eigenaren begrijpen en implementeren de vereiste beveiligings- en operationele controles en beleidsregels om hun service, klantdata, endpoints en netwerkassets te beschermen tegen ransomwareaanvallen met speciale focus op services die prioriteit krijgen als essentiële services van Microsoft.

Scenario 5: alle medewerkers hebben toegang tot educatieve en trainingsresources waarin wordt beschreven hoe een ransomwareaanval wordt herkend en hoe het beveiligingsteam op de hoogte wordt gesteld en de reactie wordt geïnitieerd.

Direct bruikbare inzichten

1. Documenteer en valideer end-to-end correctie- en herstelactiviteiten met betrekking tot ransomwareaanvallen op essentiële services.
2. Betrek stakeholders bij het bijwerken van je Enterprise Crisis Management-playbooks met ransomware-specifieke activiteiten en een beslissingsproces en richtlijnen om te bepalen of/wanneer je moet betalen voor ransomware.
3. Verbeter de detectie- en beschermingsdekking door mogelijkheden beschikbaar te maken in je geïmplementeerde beveiligingsproducten (bijvoorbeeld Attack Surface Reduction-regels in Defender for Endpoint).
4. Werk samen met het team voor beveiligingsstandaarden om een basislijn te definiëren voor bescherming tegen een ransomwareaanval en verzorg training en documentatie voor technische teams over bescherming tegen een ransomwareaanval.
5. Zet automatisering in om de implementatie van beveiligings- en operationele beleid voor de DevOps-teams te vergemakkelijken en ervoor te zorgen dat een systeem dat niet langer aan de wet- en regelgeving voldoet snel wordt gemarkeerd en hersteld.

Links naar verdere informatie

- Sharing how Microsoft protects against ransomware | Microsoft Inside Track

Kom nu in actie tegen de gevolgen voor quantumbeveiliging

Er staat druk op de ketel om de bedreiging te beheren die quantumcomputing vormt voor de hedendaagse cryptografie en alles wat hiermee wordt beschermd. Het onlangs uitgebrachte Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] bouwt voort op US Executive Order 10428[16] for Improving the Nation's Cybersecurity en benoemt de beveiliging van supply chain voor softwares als cruciale factor voor het aanpakken van toekomstige aanvallen door vreemde mogendheden.

Wat zijn quantumcomputers?

Quantumcomputers zijn machines die de eigenschappen van de quantumfysica gebruiken om data op te slaan en berekeningen uit te voeren. Dit kan zeer voordelig zijn voor bepaalde taken, waarbij zij zelfs veel beter kunnen presteren dan onze beste supercomputers. Quantumcomputing opent nu al nieuwe perspectieven voor dataencryptie en -verwerking. Studies voorspellen dat quantumcomputing al in 2030 zal zijn uitgegroeid tot een quantumindustrie van meerdere miljarden dollars (USD).[17] Sterker nog, quantumcomputing en quantumcommunicatie zullen waarschijnlijk een transformatief effect hebben in een groot aantal sectoren, variërend van gezondheidszorg en energie tot financiën en beveiliging.

Quantumcomputing vormt een bedreiging voor de hedendaagse cryptografie en alles wat hiermee wordt beschermd.

De bedreiging voor de hedendaagse cryptografie

Met het algoritme van Shor uit 1994 en een quantumcomputer op industriële schaal van meer dan een paar miljoen fysieke qubits, konden al onze huidige, wijdverbreide cryptografische algoritmen met openbare sleutels op efficiënte wijze worden gekraakt. Het is van cruciaal belang om 'quantumveilige' cryptosystemen te overwegen, evalueren en standaardiseren die efficiënt, agile en veilig zijn tegen een op quantumcomputing gebaseerde aanval. Softwaremigratie naar 'post-quantumcryptografie', namelijk bestaande klassieke algoritmen en protocollen die robuust zijn voor quantumaanvallen, zal jaren, zo niet een decennium of meer, in beslag nemen.[18]

Dit betekent dat er druk op de ketel staat om de bedreiging te beheren voor de hedendaagse cryptografie en alles wat hiermee wordt beschermd. Aanvallers kunnen nu versleutelde data vastleggen en deze later misbruiken zodra een quantumcomputer beschikbaar is. Het zal te laat zijn om te wachten met het aanpakken van de cryptografische implicaties totdat quantumcomputing beschikbaar is.

Aangezien cryptografie wordt gebruikt in het hele cyberecosysteem, betekent dit dat onze op cryptografie gebaseerde beveiligingsservices in gevaar kunnen komen. Dit omvat bijvoorbeeld services voor communicatie (TLS, IPSec), berichten (e-mail, webconferencing), identiteits- en toegangsbeheer, webbrowsen, ondertekening van code, betalingstransacties en andere services die afhankelijk zijn van cryptografie voor beveiliging.

Wanneer quantumcomputers werkelijkheid worden, zal ook extra onderzoek vereist zijn voor softwareonderdelen van derden die implementaties van cryptografische algoritmen en mogelijkheden bevatten. Dit vereist dat alle organisaties in de waardeketen hun steentje bijdragen om ervoor te zorgen dat de keten veilig blijft. Organisaties in de industrie en overheden zijn steeds meer bezig met het definiëren van beveiligingsvereisten voor de supply chain voor software en, in sommige gevallen, met het invoeren van nieuwe mandaten voor het beveiligen van de keten. Nationale veiligheidsnota NSM-8[19] stelt vereisten en tijdlijnen vast voor de implementatie van post-quantumcryptografie in National Security Systems (NSS). Hierbij wordt gevraagd om timingverwachtingen binnen 180 dagen voor 'modernisering van de planning, gebruik van niet-ondersteunde encryptie, goedgekeurde unieke missiesprotocollen, quantumbestendige protocollen en planning voor het gebruik van quantumbestendige cryptografie waar dat nodig is.'

Standaardisatie is een activiteit met lange doorlooptijd bij de overgang naar quantumveilige cryptografie. Normalisatie-instituten die werken aan normen met behulp van openbare-sleutelcryptografie, moeten nu beginnen met experimenteren met en zich aanpassen aan post-quantumalgoritmen.

Nieuwe PQC-algoritmen (post-quantumcryptografie), klassieke algoritmen waarvan wordt gedacht dat ze bestand zijn tegen quantumaanvallen, worden nu beoordeeld via het Post-Quantum Standardization Project van NIST.[20] Dit werk zal van invloed zijn op de wereldwijde inspanningen binnen normalisatie-instituten. Hoewel er een aantal overlappingen zullen zijn met de algoritmeselecties van de Amerikaanse overheid, kunnen verschillende nationale/regelgevende keuzes voor compatibele algoritmen internationale uitdagingen opleveren. Deze fragmentatie maakt de product- en servicetechniek gecompliceerder.

Nieuwe algoritmen voor post-quantumcryptografie worden momenteel onderzocht via het Post-Quantum Cryptography Standardization-programma van NIST. Dit werk zal van invloed zijn op de wereldwijde inspanningen binnen normalisatie-instituten.

Direct bruikbare inzichten

Naast SAFECode en partnerleden, moeten bedrijven op de korte termijn activiteiten ondernemen om zich voor te bereiden op de PQC-overgang.[21] Deze omvatten:

1. Een inventaris opstellen van je producten/codes die gebruikmaken van cryptografie.
2. Een strategie voor crypto agility implementeren in je hele organisatie die het minimaliseren van de vereiste codeverandering bij cryptografische wijzigingen omvat.
3. Een pilot uitvoeren met het gebruik van quantumveilige algoritmen in je producten of services die gebruikmaken van cryptografie.
4. Voorbereid zijn op het gebruik van verschillende openbare sleutelalgoritmen voor encryptie, sleuteluitwisseling en handtekeningen.
5. Je applicaties testen op de impact van zeer grote sleutelgrootten, sleutels en handtekeningen.

Links naar verdere informatie

- Microsoft has demonstrated the underlying physics required to create a new kind of qubit | Microsoft Research

Integratie van bedrijfsvoering, beveiliging en IT voor vergroting van de veerkracht

Robuuste cyberveerkracht is alleen mogelijk als leidinggevenden samenwerken met beveiligingsteams bij het implementeren van beveiliging. De ervaring van Microsoft is dat beveiligingsleiderschap een uitdagende discipline vormt die support van organisatieleiders vereist om de organisatie zo effectief mogelijk te beschermen.

Beveiligingsleiders moeten hun weg zien te vinden door een spectrum van dynamische uitdagingen rond onderwerpen met betrekking tot risico, technologie, economie, organisatieproces, bedrijfsmodellen, cultuurtransformatie, geopolitieke belangen, spionage en naleving van internationale sancties. Elk van deze bevat nuances die moeten worden begrepen en nauwkeurig beheerd.

Beveiligingsleiders moeten ook zowel intelligente, goed gefinancierde en zeer gemotiveerde menselijke aanvallers als laagopgeleide, maar effectieve, cybercriminelen dwarsbomen. Hun teams moeten complexe technische gebieden verdedigen die vaak stapsgewijs zijn opgebouwd in de loop van meer dan 30 jaar waarin beveiliging een lage of niet-bestaande prioriteit vormde. Beslissingen die jaren geleden zijn genomen, kunnen tegenwoordig tot risico's leiden totdat we de technische schuld hebben afgelost en de hiaten in de beveiliging hebben opgelost.

Leiders van organisaties en beleidsmakers kunnen een aanzienlijke positieve impact hebben op beveiliging door beveiligingsleiders actief te ondersteunen en een brug te slaan tussen geïntegreerde beveiliging en de rest van de organisatie. Wanneer Microsoft werkt met klanten die deze afstemming hebben, zien we dat ze een veerkrachtigere organisatie opbouwen en ook hun vermogen om zich aan te passen en te innoveren vergroten.

De leiding van organisaties kan beveiligingsleiders ondersteunen door zich op drie belangrijke gebieden te richten:

1. Bouw beveiliging door ontwerp

Beveiliging wordt soms gezien als een obstakel of een bijzaak in bedrijfsprocessen, die vaak pas in beslissingen wordt meegenomen wanneer het te laat is om een risico te vermijden of dit goedkoop en gemakkelijk te repareren.

De leiders van organisaties en beleidsmakers moeten ervoor zorgen dat zij:

Vroegtijdig beveiliging opnemen bij nieuwe initiatieven. Bij nieuwe digitale initiatieven en de overstap naar de cloud moet prioriteit worden gegeven aan beveiliging om ervoor te zorgen dat de risico's voor de organisatie niet toenemen bij elke nieuwe applicatie of digitale mogelijkheid. Zodra de beveiliging op een betrouwbare manier is opgenomen, kun je deze processen gebruiken om verouderde systemen te moderniseren en tegelijkertijd voordelen op het gebied van beveiliging en productiviteit te realiseren.

Normaliseer preventief onderhoud voor beveiliging. Zorg voor basisonderhoud voor beveiliging, zoals het toepassen van beveiligingsupdates en -patches en veilige configuraties, met volledige support vanuit de organisatie (waaronder budgetten, geplande downtime, acquisitievereisten voor productsupport door leveranciers).

Helaas zijn er veel organisaties die deze algemene procedures vertraagd uitvoeren, uitstellen of slechts gedeeltelijk toepassen. Dit biedt aanvallers uitgebreide mogelijkheden om misbruik te maken. De noodzaak van normalisatie van de beveiliging is vastgelegd in US NIST 800-40.[22]

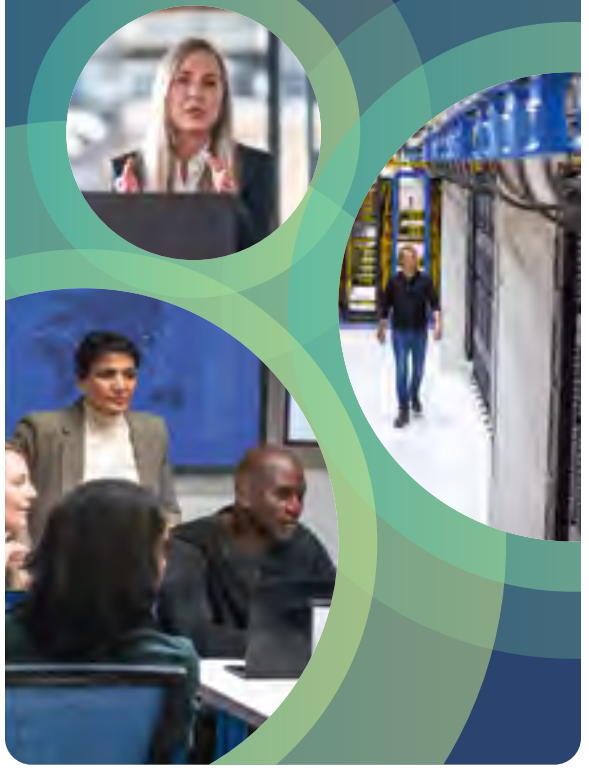
2. Raak betrokken bij beveiliging

Leiders van organisaties moeten actief deelnemen aan en support bieden bij belangrijke beveiligingsprocessen om ervoor te zorgen dat prioriteiten worden vastgesteld voor resources en dat organisaties voorbereid zijn op beveiligingsrampen. Dit omvat het volgende:

Identificeren van essentiële bedrijfsmiddelen. Beveiligingsmanagers en -teams moeten weten welke assets essentieel zijn voor de bedrijfsvoering om beveiligingsresources gericht te kunnen inzetten bij wat het belangrijkst is. Dit is vaak een nieuwe activiteit die het stellen en beantwoorden van nieuwe vragen omvat die nog niet eerder aan bod zijn gekomen.

UItvoeren van activiteiten voor bedrijfscontinuïteit en noodherstel op het gebied van cyberbeveiliging. Cyberaanvallen kunnen ingrijpende gebeurtenissen worden die de meeste of alle bedrijfsactiviteiten verstoren of tot stilstand brengen. Als je ervoor zorgt dat teams in de hele organisatie voorbereid zijn op het aanpakken van deze situaties, zal er minder tijd nodig zijn om de bedrijfsvoering te herstellen, blijft de schade voor de organisatie beperkt en wordt het vertrouwen van klanten, burgers en betrokkenen behouden. Dit moet worden geïntegreerd in een bestaand proces voor bedrijfscontinuïteit en noodherstel.

Beslissingen over beveiligingsrisico's kunnen het beste worden genomen door bedrijfs- of missie-eigenaren die volledig inzicht hebben in alle risico's en kansen.



Integratie van bedrijfs-voering, beveiliging en IT voor vergroting van de veerkracht

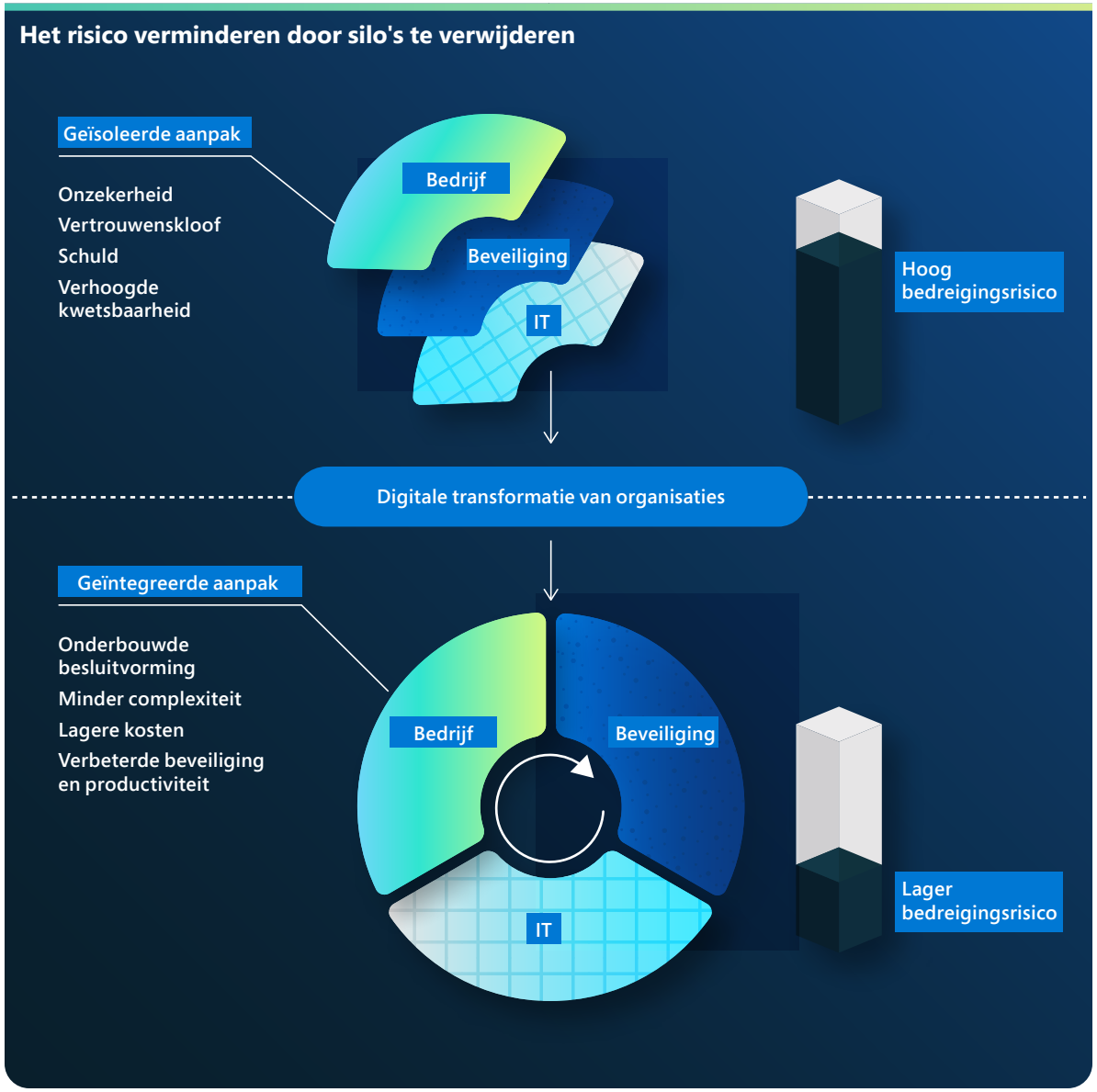
Vervolg

3. Positioneer beveiliging op correcte wijze

De manier waarop organisaties de aansprakelijkheid voor beveiligingsrisico's structureren, leidt vaak tot slechte besluitvorming over beveiligingsrisico's. Risicobeslissingen kunnen het beste worden genomen door bedrijfs- of missie-eigenaren die volledig inzicht hebben in alle risico's en kansen, maar organisaties wijzen in plaats daarvan vaak (impliciet of expliciet) de verantwoordelijkheid voor beveiligingsrisico's toe aan materiedeskundigen in het beveiligingsteam. Dit zorgt voor ongezonde druk op de beveiligingsteams en ontneemt bedrijfseigenaren het zicht op en de controle over een belangrijk risico voor hun bedrijf. Organisaties kunnen dit corrigeren door het volgende te doen:

Bedrijfseigenaren voorbereiden: licht bedrijfseigenaren voor over beveiligingsrisico's in het algemeen en hoe deze bedreigingen hun bedrijf kunnen en zullen beïnvloeden. Door beveiligingsteams rechtstreeks bij deze inspanning te betrekken, wordt ook de samenwerkingsrelatie met beveiliging en de algehele zakelijke wendbaarheid versterkt.

Beveiligingsrisico toewijzen aan bedrijfseigenaren: wanneer bedrijfseigenaren voldoende geïnformeerd raken om beveiligingsrisico's te begrijpen en te accepteren, moet de organisatie expliciet de verantwoordelijkheid voor beveiligingsrisico's naar hen verschuiven, terwijl de beveiligingsteams verantwoordelijk blijven voor het beheer van dat risico en het verstrekken van geïnformeerde expertise en begeleiding aan de eigenaar.



"Cyberveerkracht maakt deel uit van een glijdende schaal van klassieke bedrijfscontinuïteit en noodherstel, beginnend met goede databack-up; evoluerend naar herstelmogelijkheden voor processen, technologie en hun afhankelijkheden (met inbegrip van mensen en derde partijen); en evoluerend naar altijd actieve, zelfherstellende services, veerkracht voor kritieke rollen en failovers voor essentiële derde partijen. De meest veerkrachtige organisaties bevorderen de integratie tussen IT, bedrijfsmanagers en beveiligingsprofessionals. Grote veerkracht omvat ontwerpen voor veerkracht vanaf het begin, veilig wijzigingsbeheer en gedetailleerde foutisolatie. Cyberveerkracht is slechts één scenario in een goed planningsprogramma waarbij rekening wordt gehouden met alle gevaren. Naarmate cyberrisico's toenemen en het snijvlak tussen cyberbeveiliging en veerkracht belangrijker wordt, wordt de band van de Chief Information Security Officer (CISO) met het veerkrachtprogramma van de onderneming sterker. Elk jaar nemen meer CISO's verantwoordelijkheid voor bedrijfsbrede veerkracht."

Lisa Reshaur
General Manager, Risk Management, Microsoft

Links naar verdere informatie

- From resilience to digital perseverance: How organizations are using digital technology to turn the corner in unprecedented times | Officiële Microsoft-blog
- How IT and security teams can work together to improve endpoint security | Microsoft Security

De klokkromme van cyberveerkracht

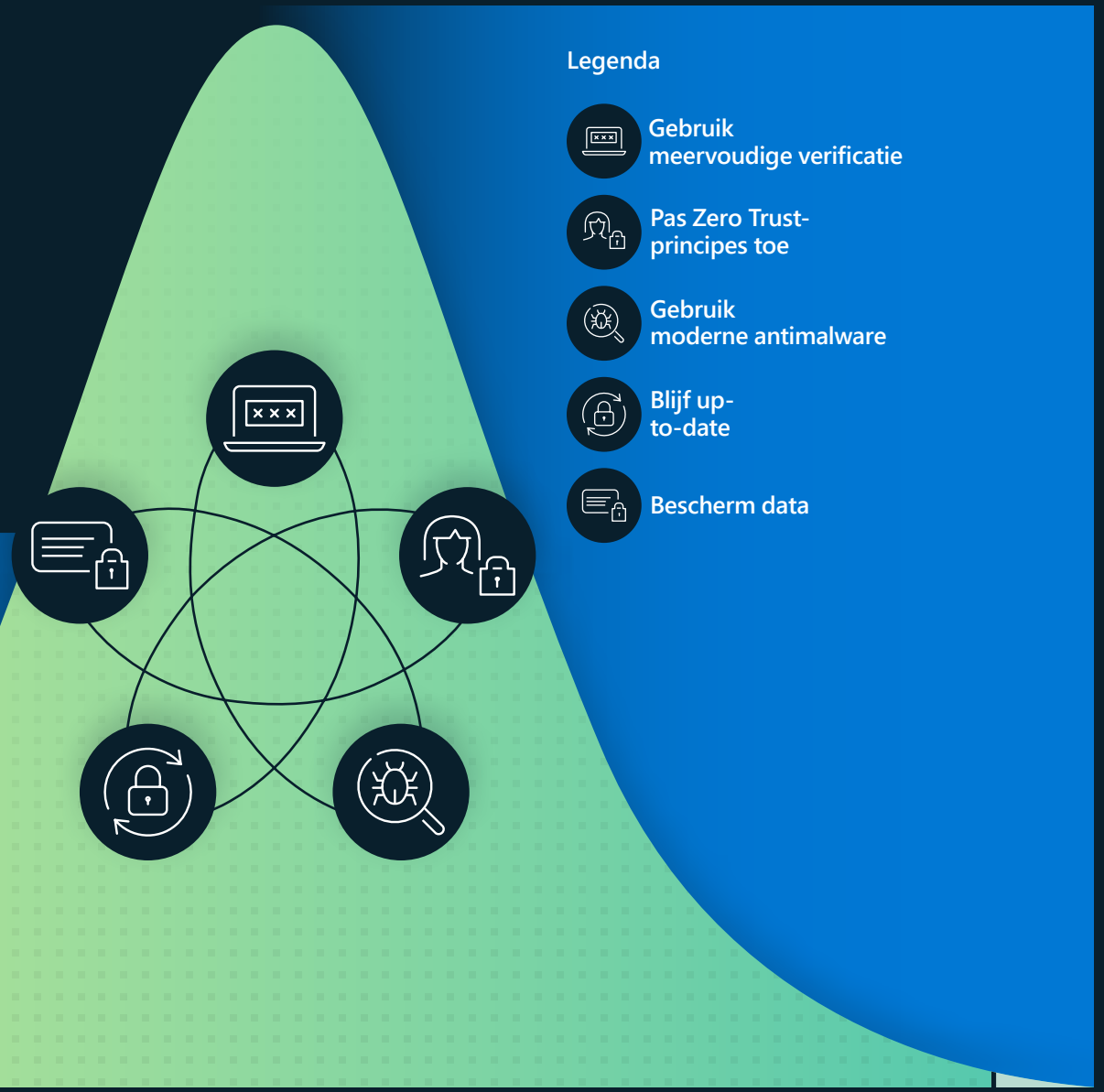
Succesfactoren voor veerkracht waarvoor elke organisatie zou moeten kiezen

Zoals we hebben gezien, slagen veel cyberaanvallen omdat de basisveiligheidshygiëne niet is gevolgd. Elke organisatie zou de volgende minimumnormen moeten hanteren:

- **Gebruik meervoudige verificatie:** zorgt voor bescherming tegen gehackte gebruikerswachtwoorden en helpt bij het bieden van extra veerkracht voor identiteiten.
- **Pas Zero Trust-principes toe:** de hoeksteen van elk veerkrachtplan dat de impact op een organisatie beperkt. Deze principes zijn:
  1. – Voer expliciete verificaties uit: zorg ervoor dat gebruikers en apparaten in goede staat verkeren voordat ze toegang tot resources krijgen.
  2. – Gebruik toegang met de minste bevoegdheden: sta alleen de bevoegdheden toe die nodig zijn voor toegang tot een resource en niet meer.
  3. – Ga uit van een inbreuk: neem aan dat de systeemverdediging is geschonden en dat systemen mogelijk zijn gehackt. Dit betekent dat de omgeving voortdurend moet worden gecontroleerd op mogelijke aanvallen.
- **Gebruik uitgebreide antimalware voor detectie en respons:** implementeer software om aanvallen te detecteren en automatisch te blokkeren en bied inzicht in de beveiligingsactiviteiten. Het monitoren van inzichten uit bedreigingsdetectiesystemen is van essentieel belang om tijdig op bedreigingen te kunnen reageren.
- **Blijf up-to-date:** niet-gepatchte en verouderde systemen zijn een belangrijke reden waarom veel organisaties het slachtoffer worden van een aanval. Zorg ervoor dat alle systemen up-to-date worden gehouden, met inbegrip van firmware, het besturingssysteem en applicaties.
- **Bescherm data:** weten wat je belangrijke data zijn, waar deze zich bevindt en of de juiste systemen zijn geïmplementeerd, is cruciaal voor het implementeren van de juiste bescherming.

98%

Elementaire beveiligings-hygiëne beschermt nog steeds tegen 98% van de aanvallen.



Eindnoten

1. Endpoint Detection and Response (EDR) is een beveiligingsplatform voor endpoints op ondernemingsniveau dat is ontworpen om bedrijfsnetwerken bij te staan bij het voorkomen, detecteren en onderzoeken van en reageren op geavanceerde bedreigingen. Mogelijkheden voor endpointdetectie en -respons bieden geavanceerde aanvalsdetectie die bijna realtime en uitvoerbaar is. Beveiligingsanalisten kunnen op effectieve wijze prioriteiten toewijzen aan waarschuwingen, inzicht verwerven in de volledige reikwijdte van een inbreuk en responsacties ondernemen om bedreigingen te verhelpen.
2. Een Endpoint Protection Platform (EPP) is een oplossing die wordt ingezet op endpointapparaten om op bestanden gebaseerde malware te voorkomen, om schadelijke activiteiten van vertrouwde en niet-vertrouwde applicaties te detecteren en te blokkeren, en om de onderzoeks- en herstelmogelijkheden te bieden die nodig zijn om dynamisch te kunnen reageren op beveiligingsincidenten en -waarschuwingen.
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. Windows Security Book: Commercial
7. Nieuwe beveiligingsfuncties voor Windows 11 helpen hybride werk te beschermen | Microsoft Security Blo
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. 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

Bijdragende teams

Bijdragende teams

De data en inzichten in dit rapport zijn geleverd door een diverse groep op beveiliging gerichte professionals, die in veel verschillende Microsoft-teams werken. Samen willen ze Microsoft, de klanten van Microsoft en de rest van de wereld beschermen tegen computeraanvallen. We zijn graag bereid om deze inzichten te delen in de geest van transparantie en met het gemeenschappelijke doel om van de wereld een veiligere plek voor iedereen te maken.

AI for Good Research Lab: gebruikmaken van de kracht van data en AI benutten om veel van de uitdagingen van de wereld aan te pakken. Het lab werkt samen met organisaties buiten Microsoft en past AI toe om levens en omgevingen te verbeteren. Aandachtsgebieden zijn onder meer online veiligheid (desinformatie, cyberbeveiliging, veiligheid van kinderen), rampenbestrijding, duurzaamheid en AI voor de gezondheidszorg.

Azure Edge & Platform, Enterprise & OS Security: verantwoordelijk voor de belangrijkste besturingssysteem- en platformbeveiliging binnen Windows, Azure en andere Microsoft-producten. Het team bouwt toonaangevende beveiligings- en hardwareoplossingen in Microsoft-platforms om misbruik, identiteitsdiefstal en schendingen via malware terug te dringen van chip tot cloud. Makers van Microsoft's Secured-core platform voor pc, Edge en Server, de Microsoft Pluton Security Processor en meer.

Azure Networking, Core: een cloudnetwerkteam dat is gericht op het Microsoft-WAN, datacenternetwerken en de softwaregedefinieerde netwerkinfrastructuur van Azure, inclusief het DDoS-platform, het netwerkrandplatform en netwerkbeveiligingsproducten zoals Azure WAF, Azure Firewall en Azure DDoS Protection Standard.

Cloud Security Research-team: door de Microsoft-cloud te beveiligen, innovatieve beveiligingsfuncties en -producten te bouwen en onderzoek te doen, beschermt dit team Microsoft-klanten en stelt ze in staat hun organisaties veilig te transformeren.

Customer Security and Trust (CST): een team dat voortdurende verbetering van de klantbeveiliging in Microsoft-producten en online services nastreeft. CST werkt samen met de technische en beveiligingsteams in het hele bedrijf om compliance te waarborgen, de beveiliging te verbeteren en meer transparantie te bieden, zodat klanten worden beschermd en wereldwijd het vertrouwen in Microsoft toeneemt.

Customer Success: beveiligingsteams in Customer Success werken rechtstreeks met klanten om best practices, geleerde lessen en begeleiding te delen om de transformatie en modernisering van beveiliging te versnellen. Dit team verzamelt en organiseert best practices en lessen die zijn geleerd tijdens de reis van Microsoft, evenals die van onze klanten, en zet deze om in referentiestrategieën, referentiearchitecturen, referentieplannen en meer.

Cyber Defense Operations Center (CDOC): dit is het centrum voor computerbeveiliging en verdediging van Microsoft waarin beveiligers uit het hele bedrijf worden samengebracht om onze bedrijfsinfrastructuur en de cloudinfrastructuur waartoe klanten toegang hebben te beschermen. Eerstehulpverleners zijn 24 uur per dag, zeven dagen per week aanwezig, naast datawetenschappers en beveiligingstechnici die werkzaam zijn bij de teams voor de services, producten en apparaten van Microsoft om bedreigingen vast te stellen en hierop te reageren en 24x7 bescherming te bieden.

Democracy Forward Initiative: een Microsoft-team dat werkt aan het behouden, beschermen en bevorderen van de fundamenten van democratie door een gezond informatie-ecosysteem te bevorderen, open en veilige democratische processen te waarborgen en te pleiten voor maatschappelijk verantwoord ondernemen.

Digital Crimes Unit (DCU): een team van advocaten, onderzoekers, datawetenschappers, technici, analisten en zakelijke professionals dat zich inzet voor de bestrijding van cybercriminaliteit op wereldwijde schaal met behulp van technologie, forensisch onderzoek, civiele procedures, strafrechtelijke verwijzingen en zowel publieke als private partnerschappen.

Digital Diplomacy: een internationaal team van voormalige diplomaten, beleidsmakers en juridische experts die werken aan het bevorderen van een vreedzame, stabiele en veilige cyberspace in het licht van toenemende conflicten met vreemde mogendheden.

Digital Security & Resilience (DSR): een organisatie die zich inzet om Microsoft in staat te stellen de meest vertrouwde apparaten en services te bouwen, terwijl we ons bedrijf veilig houden en zowel onze bedrijfs- als klantdata worden beschermd.

Digital Security Unit (DSU): een team van cyberbeveiligingsadvocaten en analisten die juridische, geopolitieke en technische expertise bieden om Microsoft en haar klanten te beschermen. DSU bouwt vertrouwen op in de ondernemingsbrede beveiligingsmogelijkheden van Microsoft tegen geavanceerde cybercriminelen wereldwijd.

Digital Threat Analysis Center (DTAC): een team van experts die bedreigingen van vreemde mogendheden analyseren en rapporteren, met inbegrip van cyberaanvallen en beïnvloedingsactiviteiten. Het team combineert informatie en intelligentie over cyberbedreigingen met geopolitieke analyses om inzichten te verschaffen aan onze klanten en aan Microsoft ten behoeve van effectieve respons en bescherming.

Enterprise and Security: een team dat zich richt op het leveren van een modern, veilig en beheersbaar platform voor de intelligente cloud en intelligente randapparatuur.

Enterprise Mobility: een team dat helpt bij het leveren van de moderne werkplek en modern beheer om data veilig te houden, zowel in de cloud als on-premises. Endpoint Manager omvat de services en tools die Microsoft en klanten gebruiken voor het beheren en bewaken van mobiele apparaten, desktopcomputers, virtuele machines, embedded apparaten en servers.

Bijdragende teams

Vervolg

Enterprise Risk Management: een team dat in verschillende business units werkt om prioriteit te geven aan risicodiscussies met het senior leiderschap van Microsoft. ERM verbindt meerdere operationele risicoteams, beheert het bedrijfsrisicoframework van Microsoft en faciliteert de interne veiligheidsbeoordeling van het bedrijf met behulp van het NIST Cybersecurity Framework.

Global Cybersecurity Policy: een team dat samenwerkt met overheden, ngo's en industriepartners om het openbare beleid voor computerbeveiliging te promoten. Hiermee kunnen klanten hun beveiliging versterken en veerkracht vergroten als ze gebruik gaan maken van Microsoft-technologie.

Identity and Network Access (IDNA) Security: een team dat werkt om alle Microsoft-klanten te beschermen tegen ongeoorloofde toegang en fraude. IDNA Security is een multidisciplinair team van technici, productmanagers, datawetenschappers en beveiligingsonderzoekers.

M365 Security: organisatie die beveiligingsoplossingen ontwikkelt, waaronder Microsoft Defender voor Eindpunt (MDE), Microsoft Defender for Identity (MDI) en andere, om zakelijke klanten te beveiligen.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): een adviesraad bij Microsoft die als missie heeft ervoor te zorgen dat nieuwe technologieën op een verantwoorde manier worden ontwikkeld en toegepast.

Microsoft Bing Search and Distribution: een team dat zich toelegt op het leveren van een zoekmachine van wereldklasse op internet, waarmee gebruikers over de hele wereld snel betrouwbare zoekresultaten en informatie kunnen vinden, inclusief het volgen van onderwerpen en trending verhalen die voor hen belangrijk zijn, terwijl gebruikers controle krijgen over hun privacy.

Microsoft Customer and Partner Solutions: de uniforme commerciële marktorganisatie van Microsoft die verantwoordelijk is voor functies op locatie, zoals beveiligings- en technische salesspecialisten en adviseurs.

Microsoft Defender Experts: de grootste wereldwijde organisatie van Microsoft met productgerichte beveiligingsonderzoekers, beoefenaars van toegepaste wetenschap en analisten van bedreigingsinformatie. Defender Experts levert innovatieve detectie- en responsmogelijkheden in Microsoft 365-beveiligingsproducten en beheerde Microsoft Defender Experts-services.

Microsoft Defender for IoT: een team bestaande uit deskundige domeinonderzoekers die zijn gespecialiseerd in reverse-engineering van IoT/OT-malware, protocollen en firmware. Het team jaagt op IoT/OT-bedreigingen om schadelijke trends en campagnes te ontdekken.

Microsoft Defender Threat Intelligence (RiskIQ): een team dat tactische intelligentie produceert door analyse van de uitgebreide externe telemetrieverzameling van Microsoft, het bedreigingslandschap in kaart brengt terwijl het zich ontwikkelt om voorheen onbekende bedreigingsinfrastructuur te ontdekken en context toevoegt aan bedreigingsactoren en campagnes. Het team publiceert regelmatig actueel en onderscheidend onderzoek om cruciale tactische informatie aan verdedigers te bieden.

Microsoft Security Business Development Team: een team dat de groeistrategie, partnerschappen en strategische investeringen van Microsoft leidt.

Microsoft Security Response Center (MSRC): een team dat contacten onderhoudt met beveiligingsonderzoekers die werken aan de bescherming van de klanten en het partnerecosysteem van Microsoft. MSRC vormt een integraal onderdeel van het CDOC (Cyber Defense Operations Center) van Microsoft en brengt beveiligingsresponsexperts uit het hele bedrijf samen om bedreigingen in realtime te detecteren, erop te reageren en hiertegen te beschermen.

Microsoft Security Services for Incident Response: een team van cyberbeveiligingsexperts dat klanten helpt bij de gehele cyberaanval, van onderzoek tot succesvolle inperkings- en herstelgerelateerde activiteiten. Services worden aangeboden via twee sterk geïntegreerde teams, het Detection and Response Team (DART) met een focus op het onderzoek en de basis voor herstel, en de Compromise Recovery Security Practice (CRSP), die zich richt op de inperkings- en herstelaspecten.

Microsoft Threat Intelligence Center (MSTIC): een team dat zich richt op het identificeren, volgen en verzamelen van informatie met betrekking tot de meest geavanceerde bedreigingen die Microsoft-klanten treffen, waaronder bedreigingen door vreemde mogendheden, malware en phishing.

One Engineering System (1ES): een team met de missie om tools van wereldklasse te leveren om Microsoft-developers te helpen zo productief en veilig mogelijk te zijn. Het team leidt de centrale strategie voor het beveiligen van de end-to-end supply chain voor software van Microsoft.

Operational Threat Intelligence Center (OpTIC): het team dat verantwoordelijk is voor het beheren en verspreiden van informatie over cyberbedreigingen en dat de missie van het Microsoft Cyber Defense Operation Center (CDOC) ondersteunt om Microsoft en onze klanten te beschermen.

Microsoft

Het dreigingslandschap verlichten en een digitale verdediging bieden.

- Meer informatie: **https://microsoft.com/mddr**
- Nader bekeken: **https://blogs.microsoft.com/on-the-issues/**
- Blijf verbonden: **@msftissues en @msftsecurity**