Microsoft

MICROSOFT SECURITY INTELLIGENCE-RAPPORT

DEEL 24
JANUARI–DECEMBER 2018

Inhoudsopgave

Auteurs en bijdragers

Abhishek Agrawal
Information Protection

David Fantham
Information Protection

Debraj Ghosh
Microsoft Security Marketing

Diana Kelley
Cybersecurity Solutions Group

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender Research Team

Eric Douglas
Windows Defender Research Team

Francis Tan Seng
Windows Defender Research Team

Jonathan Trull
Cybersecurity Solutions Group

Joram Borenstein
Cybersecurity Solutions Group

Karthik Selvaraj
Windows Defender Research Team

Kasia Kaplinska
Microsoft Security Marketing

Kristina Laidler
Security Incident Response

Matt Duncan
Windows Active Defense Data Engineering and Analytics

Mark Simos
Cybersecurity Solutions Group

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft Security Marketing

Ram Pliskin
Azure Security

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Cybersecurity Solutions Group

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender Research Team

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Voorwoord

Welkom bij de 24e editie van het Microsoft Security Intelligence-rapport (SIR). Als beveiligingsarchitect lees ik rapporten zoals deze in de hoop het vakgebied wat beter te leren begrijpen en om praktische tips te weten te komen over hoe die kennis gebruikt kan worden om organisaties effectiever te beschermen en verdedigen.

Het SIR-team biedt met dit rapport leerzame informatie over een betere digitale veiligheid en heeft een jaar aan data geanalyseerd om er de belangrijkste lessen uit te kunnen trekken.

Dit rapport bevat de inzichten die gedurende een jaar zijn verzameld uit de analyses van beveiligingsdata en de praktische lessen die daaruit kunnen worden getrokken. Geanalyseerde data omvatten de 6,5 biljoen dreigingssignalen die zich iedere dag door de Microsoft-cloud voortbewegen en het onderzoek en de werkelijke, praktische ervaringen van onze duizenden veiligheidsonderzoekers en -ondersteuners van over de hele wereld. In 2018 maakten aanvallers gebruik van een verscheidenheid aan smerige trucs, zowel nieuwe (coin-mining) als oude (phishing), in hun voortdurende zoektocht om data en middelen te stelen van klanten en organisaties. Hybride aanvallen, zoals de Ursnif-campagne, combineerden sociale en technische benaderingen. Naarmate verdedigers beter werden in het tegengaan van ransomware, een opvallend en ontwrichtend aanvalstype, schakelden criminelen over naar de meer geniepige, maar nog steeds winstgevende, coin-miners.

Een dergelijke omschakeling kan frustrerend aanvoelen, alsof aanvallers altijd een stap verder zijn. Maar door er op een andere manier naar te kijken, kan er wel een positieve draai aan worden gegeven. Verdedigers en cyberbeveiligingsprofessionals zoals jij hebben defensieve technieken geïmplementeerd waardoor aanvallers gedwongen zijn om hun favoriete payloads aan te passen en af te stappen van ransomware.

Een ander gebied waar de activiteit van cybercriminelen is toegenomen, is in de supply chain. Een van de meest opvallende aanvallen, de uitbraak van de Dofoil-coin-miner van 6 maart 2018, werd gestart via een vergiftigde peer-to-peer-app. De aanvallen op supply chains gingen verder dan apps en richtten zich op de cloud, en omvatten kwaadaardige browserextensies, gecompromitteerde Linux-opslagplaatsen en meerdere gevallen van modules met trojans. Om deze dreiging aan te pakken bewegen organisaties zich naar een transparant en betrouwbaar supply chain-model.

De hoeveelheid data is groot, maar soms helpt het om erachter te komen wat er werkelijk bij een organisatie heeft plaatsgevonden. Daarom hebben we in dit rapport geleerde lessen uit de praktijk van ons Detection and Response Team (DART) opgenomen. Deze lessen omvatten ook de manier waarop een groot productiebedrijf het voor elkaar kreeg om controles te implementeren om een meerfasige phishingcampagne te blokkeren die hen al maanden teisterde en hoe een financiële dienstverlener uiteindelijk in staat was om een aanval op hun systemen uit te bannen dankzij geavanceerde onderzoekstools en eindpuntcontroles.

Ten slotte is ook het aantal phishingklikken blijven stijgen, maar machine learning-modellen worden steeds beter in het tegenhouden van phishingaanvallen voordat gebruikers geraakt worden en in het voorkomen van schade nadat er is geklikt. Het overige goede nieuws? Een toenemend aantal bedrijven implementeert meervoudige oplossingen om het succes in te perken van phishing-e-mails die zijn gericht op inlogdata.

Aanvallers zoeken naar mogelijkheden, dus hoe meer we weten over hun technieken en handelswijzen, hoe beter we voorbereid zijn om verdediging op te zetten en om snel te reageren. Kleine, belangrijke stappen kunnen een enorm verschil maken in de algehele cyberveiligheid van een organisatie. Daarom vind je in dit rapport naast diepgaande inzichten over het verschuivende malware- en aanvalslandschap ook advies in de vorm van aanbevolen stappen en andere best practices. Toen ik zelf actief was in de praktijk, was dat precies wat ik nodig had in mijn strijd tegen aanvallers. We hopen dat dat ook is wat jij nodig hebt.

Diana Kelley
Microsoft Cybersecurity Field CTO

P.s. We zijn altijd bezig de SIR te verbeteren. Als je feedback hebt, neem dan contact met ons op en laat ons weten hoe je vindt dat we het doen.

DEEL I

Ransomware, cryptovaluta-mining en geld

De grote verhalen van 2017 over digitale veiligheid gingen meestal over ransomware. De zeer grootschalige, wereldwijde uitbraken van WannaCrypt en Petya maakten ransomware (een type malware dat computers encrypt en vergrendelt en vervolgens geld eist om de toegang te herstellen) bekend bij het grote publiek en er werd veelvuldig voorspeld dat het probleem in de toekomst alleen maar zou toenemen. In plaats daarvan daalde het aantal ransomware-aanvallen aanzienlijk in 2018.

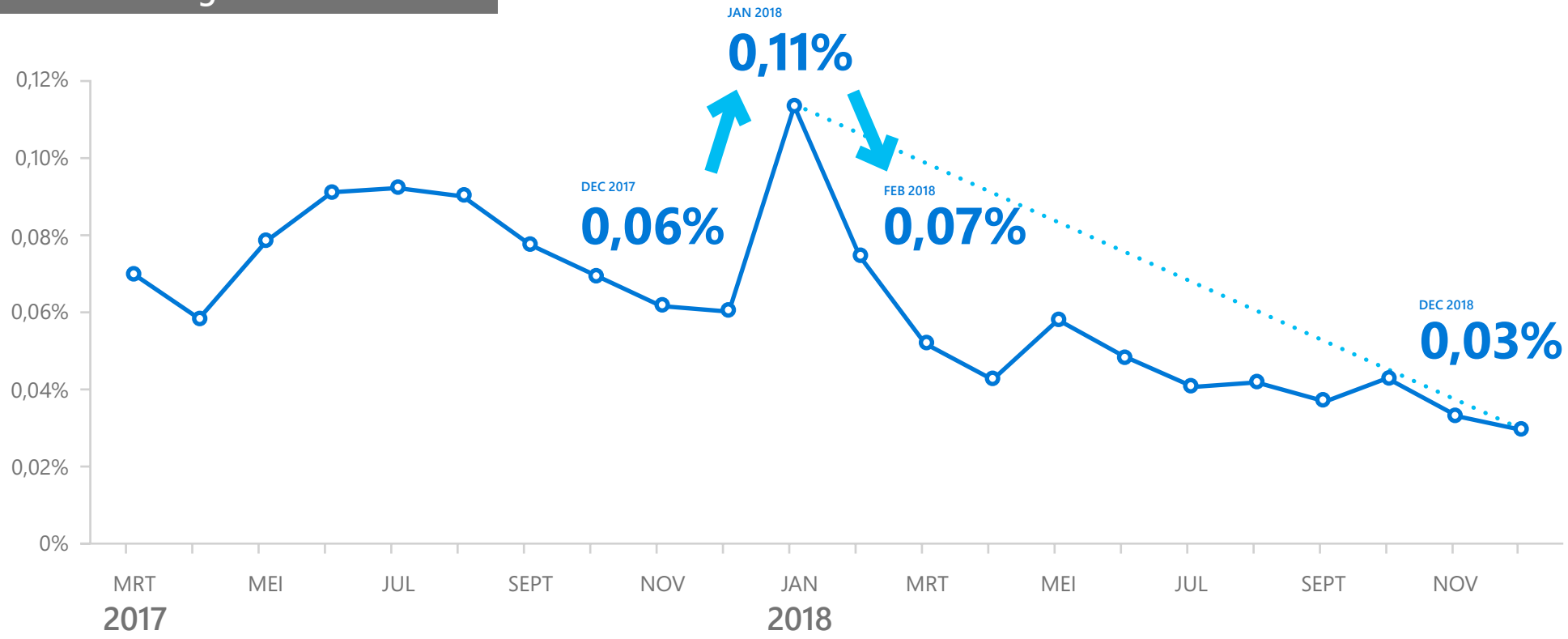
De daling van de ransomware-aanvallen was deels te wijten aan verbeterde herkenning en betere voorlichting waardoor het voor aanvallers moeilijker werd om hier gebruik van te maken. Hierdoor verplaatsten aanvallers hun ransomwarepogingen naar cryptovaluta-mining, waarmee de computermiddelen van slachtoffers worden gebruikt om digitaal geld voor de aanvallers te maken. Deze verschuiving toont het fundamenteel opportunistische karakter van de meeste winstgerichte cybercriminelen: ze hebben de neiging om zich te richten op de makkelijkste route naar geld en wanneer de economie van cybercriminaliteit verandert, gaan ze hier snel in mee.

RANSOMWARE-AANVALLEN DALEN

Meer dan een decennium geleden werden de hackers en grappenmakers die de vroege malwarebeweging domineerden, verdrongen door georganiseerde criminelen en andere winstgerichte personen. Waar vroege uitbraken van malware vaak opvallend en duidelijk waren, is winstgerichte malware vaker veel stiller en trekt zo weinig mogelijk aandacht, zodat het doel (versturen van spam, stelen van gevoelige informatie, uitvoeren van denial-of-service-aanvallen en andere kwaadaardige activiteiten) zolang mogelijk kan worden bereikt.

Ransomware doorbrak deze trend. In plaats van te proberen onopgemerkt te blijven, ontkent ransomware slachtoffers openlijk de toegang tot hun computers en belangrijke bestanden, totdat het slachtoffer het losgeld betaalt (en vaak zelfs daarna gaven de aanvallers hun controle over computers niet vrij, zelfs niet nadat het losgeld was betaald). Aangezien ransomware een hoogtepunt bereikte in 2017, leek het alsof deze stijl van open aanvallen een nieuwe fase in de aanvalstechnieken vertegenwoordigde. Maar meer recente data suggereert dat ransomware verder zal dalen en dat aanvallers steeds meer teruggrijpen op de meer geniepige activiteiten die ze in het verleden toepasten, met als doel onder de radar te blijven om effectiever aanvallen uit te kunnen voeren, zoals cryptovaluta-mining. Hoewel er sprake is van een daling van het aantal ransomware-aanvallen, betekent dit niet noodzakelijkerwijs dat de ernst van de aanvallen is gedaald.

Confrontatiegraad ransomware

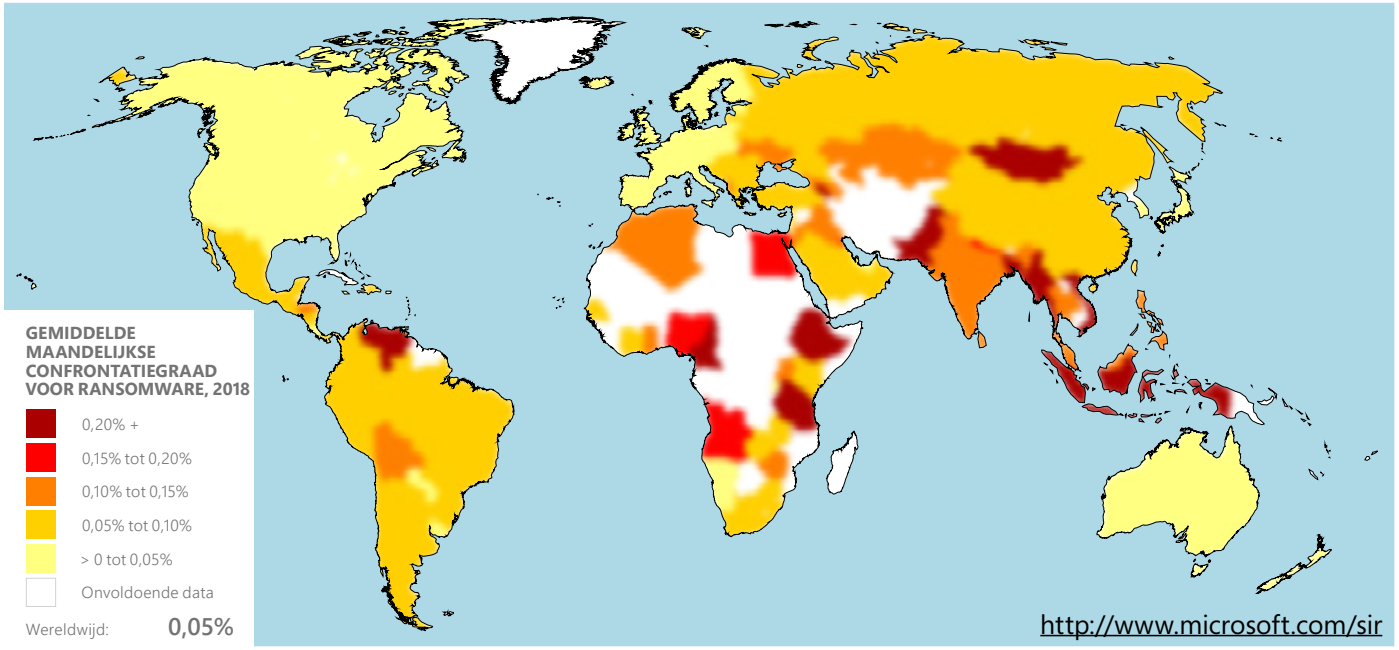


Confrontatiegraad voor ransomware daalde ongeveer met 60 procent tussen maart 2017 en december 2018, met periodieke stijgingen in die periode.

AFBEELDING 1.

Aantal ransomware-aanvallen van maart 2017 tot december 2018

Er zijn waarschijnlijk veel oorzaken voor deze algehele daling, maar beveiligingsonderzoekers van Microsoft vermoeden dat een primaire factor is dat zowel eindgebruikers als organisaties zich steeds meer bewust worden van en intelligenter omgaan met ransomware-bedreigingen. Daarnaast zijn ze ook voorzichtiger maken vaker back-ups van belangrijke bestanden, zodat deze kunnen worden hersteld als ze worden versleuteld door ransomware. Daarnaast, zijn cybercriminelen ook opportunistisch, zoals eerder beschreven.



AFBEELDING 2.

Gemiddelde maandelijkse confrontatiegraad voor ransomware, wereldwijd per land/regio in 2018

LAND DAT HET MEEST WERD GERAAKT DOOR RANSOMWARE: ETHIOPIË

Gemiddelde maandelijkse confrontatiegraad: **0,77%**

De vijf gebieden met de hoogste gemiddelde maandelijkse confrontatiegraad voor ransomware in 2018 waren Ethiopië (0,77%), Mongolië (0,46%), Kameroen (0,41%), Myanmar (0,33%) en Venezuela (0,31%), die in die periode elk een gemiddelde maandelijkse confrontatiegraad voor ransomware van 0,31% of hoger hadden.[1] Een paar jaar geleden kwamen ransomware-aanvallen vooral voor in rijke landen en regio's in Europa en Noord-Amerika, maar sinds ransomware uit de gratie raakte bij aanvallers, lijkt het patroon meer overeen te komen met dat van malware als geheel.

De locaties met het laagste confrontatiegraad voor ransomware in 2018 waren Ierland (0,01%), Japan (0,01%), Verenigde Staten (0,02%), Verenigd Koninkrijk (0,02%) en Zweden (0,02%), die in die periode elk een gemiddelde maandelijkse confrontatiegraad voor ransomware van 0,02% of lager hadden. Locaties met een lage confrontatiegraad hebben in de regel een ontwikkelde infrastructuur voor cyberbeveiliging en gerenommeerde programma's ter bescherming van kritieke infrastructuur en voor communicatie met hun burgers over elementaire veiligheid.

VOETNOTEN

[1] De confrontatiegraad is het percentage van computers met realtime beveiligingsproducten van Microsoft die een malware-aanval melden. De ontdekking van een bedreiging betekent niet dat de computer is besmet. Alleen computers waarvan gebruikers zich hebben aangemeld om data te delen met Microsoft, worden meegenomen bij het berekenen van de confrontatiegraden.

CRYPTOVALUTA-MINING IN OPKOMST

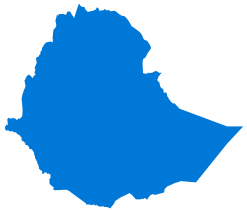
Cryptovaluta is virtueel geld dat gebruikt kan worden om anoniem goederen en services te kopen en verkopen, zowel online als in de fysieke wereld. Er bestaan vele verschillende soorten cryptovaluta, maar ze zijn allemaal gebaseerd op blockchain-technologie, waarin elke transactie wordt opgeslagen in een gedistribueerd grootboek dat door duizenden of miljoenen computers over de wereld wordt beheerd. Nieuwe munten (coins) worden gemaakt, of 'gemined', door computers die complexe berekeningen uitvoeren en die ook het verifiëren van blockchain-transacties als functie hebben.

Het minen van coins kan zeer lucratief zijn (in 2018 was één Bitcoin, de oudste en meest populaire cryptovaluta, enkele duizenden dollars waard), maar het uitvoeren van de noodzakelijke berekeningen kan zeer resource-intensief zijn en dat neemt toe bij elke nieuwe munt die wordt gemined. Voor populaire valuta zoals Bitcoin is het winstgevend minen van coins bijna onmogelijk zonder toegang tot enorme rekenkracht, die vaak buiten het bereik is van de meeste individuen en kleine groepen. Vanwege deze reden zijn aanvallers die op zoek zijn naar ongeoorloofde winsten steeds meer gericht op malware die hen in staat stelt de computers van slachtoffers te gebruiken om cryptovaluta te minen. Door deze aanpak kunnen ze de verwerkingskracht van honderdduizenden, in plaats van een of twee, computers gebruiken. Zelfs wanneer een kleine inbraak wordt ontdekt, maakt de anonieme aard van cryptovaluta het lastig om de verantwoordelijke partijen op te sporen.

In 2018 was de gemiddelde wereldwijde maandelijkse confrontatiegraad voor cryptovaluta-mining 0,12% ten opzichte van slechts 0,05% voor ransomware. Veel factoren dragen bij aan de toegenomen populariteit van mining als de payload van malware. In tegenstelling tot ransomware vereist cryptovaluta-mining geen input van de gebruiker, het proces is namelijk actief op de achtergrond terwijl de gebruiker andere taken uitvoert of niet eens bij de computer aanwezig is. Het is ook mogelijk dat het proces niet eens wordt opgemerkt, tenzij de prestaties van de computer merkbaar achteruitgaan. Hierdoor zullen gebruikers minder waarschijnlijk actie ondernemen om de dreiging te verwijderen en de computer kan doorgaan met het minen van coins voor de aanvaller gedurende een lange periode.

De beschikbaarheid van snel bruikbare producten om in het geheim vele cryptovaluta te minen, is een andere reden waarom deze tendens doorzet. De drempel om ermee te starten is laag vanwege de grote beschikbaarheid van mining-software voor coins, die cybercriminelen opnieuw vormgeven als malware om deze te plaatsen op de computer van nietsvermoedende gebruikers. De geïnfecteerde miners worden vervolgens aangebracht op systemen van slachtoffers via veelgebruikte technieken om andere malware aan te brengen, zoals social engineering, exploits en drive-by-downloads. Nadat de mining-software is geïnstalleerd, wordt deze op de achtergrond actief op computers van slachtoffers om blockchain-berekeningen uit te voeren, waarbij de aanvaller profiteert van het resultaat.

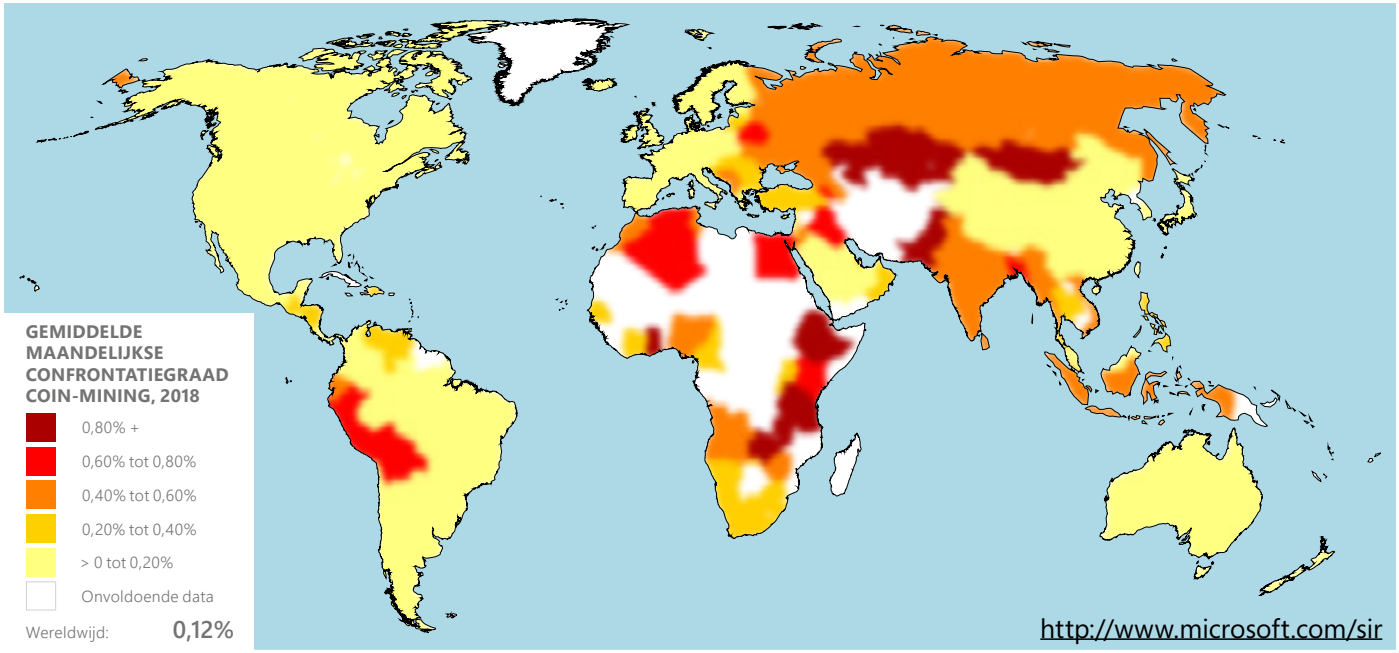
GEMIDDELDE MAANDELIJKSE CONFRONTATIEGRAAD VAN LANDEN DIE HET MEEST GERAAKT WORDEN DOOR CRYPTOVALUTA-MINING



Ethiopië: **5,58%**

Tanzania: **1,83%**

Pakistan: **1,47%**



AFBEELDING 3.

Gemiddelde maandelijkse confrontatiegraad voor coin-mining, wereldwijd per land/regio in 2018

GEMIDDELDE MAANDELIJKSE CONFRONTATIEGRAAD VAN LANDEN DIE HET MINST GERAAKT WORDEN DOOR CRYPTOVALUTA-MINING

Ierland: 0,02%

Japan: 0,02%

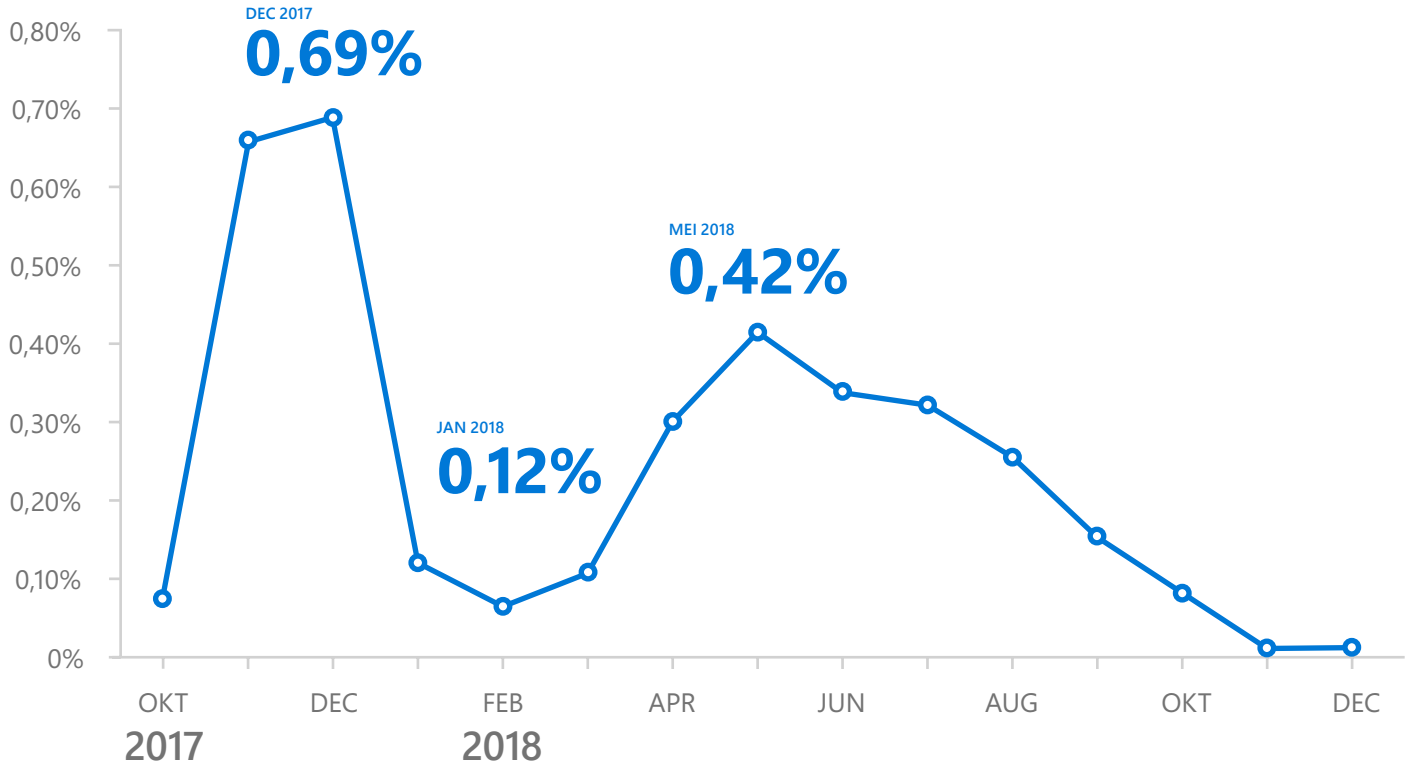
Verenigde Staten: 0,02%

De vijf locaties met de hoogste confrontatiegraad voor cryptovaluta-mining in 2018 waren Ethiopië (5,58%), Tanzania (1,83%), Pakistan (1,47%), Kazachstan (1,24%) en Zambia (1,13%), die in die periode elk een gemiddelde maandelijkse confrontatiegraad voor cryptovaluta-mining hadden van ongeveer 1,13% of hoger. De locaties met de laagste confrontatiegraad voor cryptovaluta-mining in 2018 waren Ierland, Japan, de Verenigde Staten en China, die in die periode elk een gemiddelde maandelijkse confrontatiegraad voor cryptovaluta-mining hadden van ongeveer 0,02%.

OP BROWSER GEBASEERDE CRYPTOVALUTA-MINERS: EEN NIEUWE BEDREIGING

De statistieken die in deze sectie worden getoond betreffen kwaadaardige cryptovaluta-miners die ontworpen zijn om als malware te worden geïnstalleerd op de computers van slachtoffers. Maar sommige van de meest significante cryptovaluta-miners zijn bedreigingen die volledig plaatsvinden binnen webbrowsers en die nooit hoeven te worden geïnstalleerd. Een aantal services adverteren op browser gebaseerde cryptovaluta-miners als een manier voor eigenaren van websites om verkeer op hun sites te gelde te maken zonder gebruik te maken van reclame. Eigenaren van websites moeten dan JavaScript-code toevoegen aan hun pagina's waarmee cryptovaluta op de achtergrond worden gemined terwijl een gebruiker de website bezoekt, waarbij de opbrengst wordt gesplitst tussen de eigenaar van de website en

Confrontatiegraad brocoiner



de service. Helaas hebben aanvallers snel geprofiteerd van deze services door zonder toestemming van eindgebruikers cryptovaluta te minen, vaak ook door legitieme websites te compromitteren en kwaadwillig de mining-code in de broncode te integreren. Voor deze op browser gebaseerde miners is het helemaal niet nodig om de computer van de eindgebruiker te compromitteren en het kan worden uitgevoerd op elk platform met een JavaScript-compatibele webbrowser. Net als trojans voor cryptovaluta-mining, kunnen op browser gebaseerde miners aanzienlijk de computerprestaties verslechteren en stroom verbruiken terwijl een gebruiker een getroffen webpagina bezoekt.

AFBEELDING 4.

Confrontatiegraad voor Brocoiner, de meest voorkomende op browser gebaseerde cryptovaluta-miner

DE IMPACT VAN ONGEVRAAGDE CRYPTOVALUTA-MINING

De meest voor de hand liggende bedreiging voor slachtoffers van kwaadaardige cryptovaluta-mining is het verbruik van computerkracht, waarmee veel stroom wordt verbruikt en de computerprestaties aanzienlijk verslechteren. Gebruikers en organisaties kunnen ook worden geconfronteerd met andere risico's van coin-mining, waaronder:

- **Aanvallers hebben een toegangspunt om meer schade te veroorzaken in de toekomst.**
  Net als andere vormen van malware biedt cryptovaluta-mining aanvallers een toegangspunt. Terwijl de computer op de achtergrond cryptovaluta aan het minen is, kunnen cybercriminelen meer te weten komen over de achterliggende infrastructuur en eventuele zwakke plekken in de beveiliging blootleggen die ze uit kunnen buiten voor andere doeleinden.

- **Op internet aangesloten apparaten kunnen worden aangevallen en ook worden ingesteld als bots voor cryptovaluta-mining.**
  Veel van dergelijke apparaten hebben geen ingebouwde beveiliging, zoals malwaredreigingsdetectie, waardoor ze interessante doelwitten zijn voor aanvallers.

- **Beschadigingen aan systemen.**
  Door software voor cryptovaluta-mining die maandenlang, of nog langer, continu wordt uitgevoerd, kunnen de prestaties verslechteren, en de warmte die wordt gegenereerd door overmatig stroomverbruik en CPU-gebruik kan schade toebrengen aan systemen.

DEEL II

Software-supply chains in gevaar

Al jaren volgt Microsoft aanvallers die supply chains compromitteren als toegangspunt voor aanvallen. Bij de aanval op een supply chain richten aanvallers hun aandacht op het compromitteren van een ontwikkelings- of updateproces van een legitieme softwareleverancier.

Als dit lukt, kan de aanvaller een gecompromitteerde module integreren in een legitieme applicatie of updatepackage, dat vervolgens wordt gedistribueerd naar de gebruikers van de software. De kwaadaardige code wordt vervolgens uitgevoerd met hetzelfde vertrouwen en dezelfde machtigingen als de software. Het toegenomen aantal aanvallen op de software-supply chain van de afgelopen jaren is een belangrijk onderwerp geworden in veel gesprekken over cyberveiligheid en is een primaire bron van zorg voor vele IT-afdelingen.

AFBEELDING 5.

Aanvallen op software-supply chain in 2017 en 2018

GROTE AANVALLEN OP SOFTWARE-SUPPLY CHAIN IN 2017 EN 2018

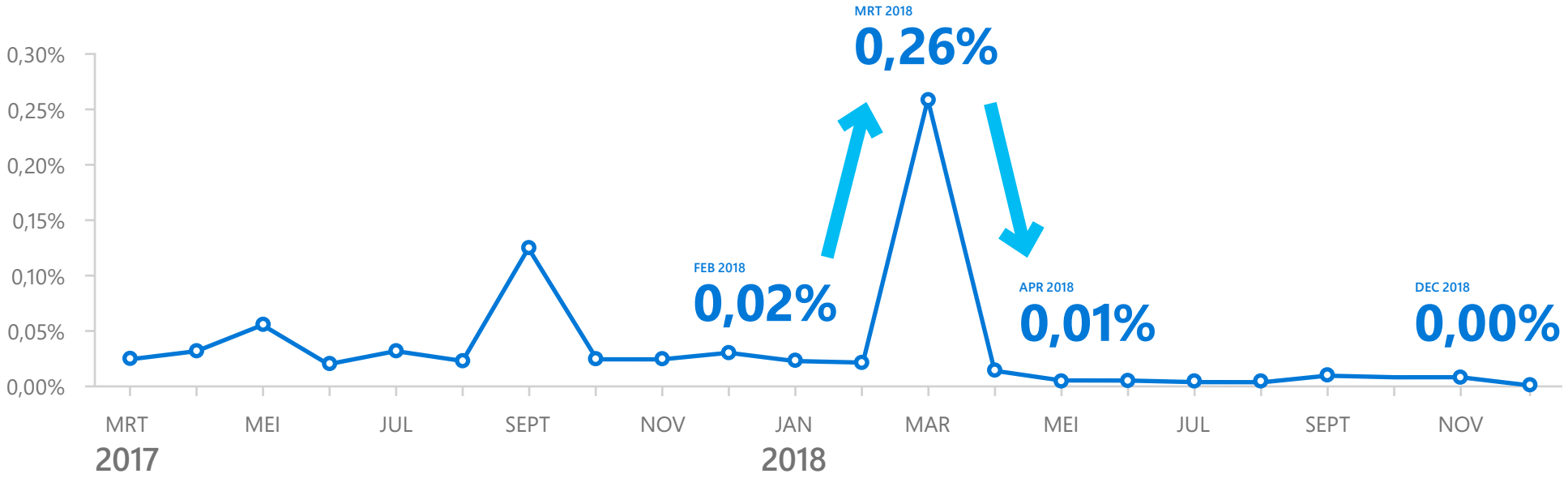
In 2017 waren aanvallen op software-supply chains verantwoordelijk voor een aantal grootschalige incidenten, waarvan de meest opvallende de Petya ransomware-uitbraak in juni was, die herleid werd naar aanvankelijke besmettingen van een gecompromitteerd updateproces voor een populair fiscale boekhoudapplicatie in Oekraïne. In mei compromitteerde de operatie WilySupply de software-updateprogramma van een teksteditor om een trojan te installeren op systemen van gerichte organisaties in de financiële en IT-branche. In juli werd een achterdeur genaamd ShadowPad verborgen in een softwarepackage voor servermanagement, waardoor aanvallers extra malwarepayloads konden installeren voor het verkrijgen van data en het uitvoeren van andere kwaadaardige activiteiten. In september werd de infrastructuur van de populaire freeware-tool CCleaner gecompromitteerd en werd er een versie met een achterdeur geleverd aan gebruikers.

AANVALLEN OP SOFTWARE-SUPPLY CHAINS IN 2018: HOOFDOORZAKEN EN IMPACT

Het eerste grote aanvalsincident op een software-supply chain in 2018 vond plaats op 6 maart, toen Windows Defender ATP een massale campagne blokkeerde om de Dofoil-trojan (ook bekend als Smoke loader) te lanceren. De massale malware-campagne werd veroorzaakt door een geïnfecteerde peer-to-peer-applicatie. De updatepackage van de applicatie werd vervangen door een geïnfecteerde package die gecompromitteerde code downloadde waarmee later de Dofoil-malware werd geïnstalleerd. De geavanceerde trojan bevatte een coin-mining-payload en gaf blijk van geavanceerde procesoverschrijdende injectietechnieken, persistente mechanismen en omzeilende methoden.

AFBEELDING 6.

De trend van confrontaties met Dofoil (Smoke Loader) in 2018 vertoont een piek van geblokkeerde exemplaren in maart



Gedurende de eerste 12 uur van de campagne blokkeerde Windows Defender meer dan 400.000 infectiepogingen wereldwijd. In Rusland bevond zich 73% van de wereldwijde confrontaties en in Turkije en Oekraïne respectievelijk 18% en 4%.

Er werden in 2018 meerdere aanvallen ontdekt die gebruikmaakten van gecompromitteerde software-supply chains als leveringsmechanisme, met inbegrip van de aanvallen in de volgende lijst:

AFBEELDING 7.

Andere aanvallen op software-supply chain in 2018

Periode	Aanval	Beschrijving	Gecompromitteerde software
Maart 2018	Dofoil coin-mining-campagne (gerapporteerd door Microsoft).	Aanvallers infecteerden het updateproces van een peer-to-peer-app om Dofoil te installeren, die vervolgens coin-mining-malware installeerde.	Peer-to-peer-app.
Juli 2018	Gecompromitteerde toeleveringsketen binnen een toeleveringsketen (gerapporteerd door Microsoft).	Aanvallers compromitteerden de gedeelde infrastructuur tussen de leverancier van een PDF-editorapp en een van hun softwareleveranciers.	PDF-editorapp en externe softwareleverancier.
Augustus 2018	Gecompromitteerd programma voor ondersteuning op afstand (Operation Red Signature, gerapporteerd door Trend Micro en IssueMakersLab).	De updateserver van een leverancier voor ondersteuningsoplossingen op afstand werd gecompromitteerd om een Remote Access Tool, genaamd 9002 RAT, af te leveren.	Programma voor ondersteuning op afstand.
Oktober 2018	Gecompromitteerde oplossing voor hostingbeheeromgeving (gerapporteerd door ESET).	Het installatiescript voor een oplossing voor een hostingbeheeromgeving werd veranderd om inlogdata te stelen.	Oplossing voor hostingbeheeromgeving.

VERTROUWEN IN GEVAAR

Aanvallen op de supply chain zijn verraderlijk, omdat ze gebruikmaken van het vertrouwen dat gebruikers en IT-afdelingen hebben in de software die ze gebruiken. De gecompromitteerde software wordt vaak ondertekend en gecertificeerd door de leverancier en kan mogelijk geen enkele indicatie geven dat er iets mis is, waardoor het aanzienlijk moeilijker is om de infectie op te sporen. Ze kunnen schade toebrengen aan de relatie tussen de supply chains en hun klanten, los van of klanten nou bedrijven of particulieren zijn. Door software te infecteren en infrastructuren voor levering en updates te ondermijnen, kunnen aanvallen op de supply chain invloed hebben op de integriteit en veiligheid van goederen en services die organisaties leveren.

Aanvallen op de supply chain hebben een breed scala aan software en organisaties in verschillende sectoren en geografische locaties geraakt. De dreiging van aanvallen op de supply chain is een sectorbreed probleem dat de aandacht van meerdere belanghebbenden vereist, met inbegrip van de softwareontwikkelaars en leveranciers die de code schrijven, de systeembeheerders die softwaresystemen beheren en de professionals in informatiebeveiliging die deze aanvallen detecteren en oplossingen ontwikkelen om mensen en software tegen dergelijke aanvallen te beschermen.

MEER DAN SOFTWARE: SUPPLY CHAIN GECOMPROMITTEERD VIA CLOUDOBJECTEN

Het vermogen van aanvallen op de supply chain om het vertrouwen te ondermijnen, wordt nog eens versterkt en complexer gemaakt in de cloud. Verschillende incidenten betreffende gecompromitteerde cloudobjecten, services en infrastructuren in 2018 benadrukken deze complexiteit:

- Geïnfecteerde Chrome-uitbreidingen die klik-fraude-malware installeerden (gerapporteerd door ICEBRG)
- Diverse gecompromitteerde Linux-opslagplaatsen (gerapporteerd op een aantal online forums)
- Kwaadaardige WordPress plug-ins gebruikt voor verschillende kwaadwillige activiteiten, waaronder de mogelijkheid voor aanvallers om content te publiceren op Wordpress-websites (gerapporteerd door WordPress)
- Kwaadaardige Docker-afbeeldingen die een script bevatten om cryptovaluta-mining-malware te downloaden, geüpload naar Docker Hub-account (gerapporteerd door Fortinet en Kromtech)
- Een schadelijke package in de officiële Python-opslagplaats via typo-squatting. De package bevatte een schadelijk script dat malware downloadde die werd gebruikt om coin-mining-adressen op het klembord over te nemen (gerapporteerd op Medium)
- Gecompromitteerd script in StatCounter die aanvallers in staat stelde om een kwaadwillig script te injecteren in websites die StatCounter gebruikten (gerapporteerd door ESET)
- Meerdere exemplaren van npm-modules met een achterdeur (de NPM-blog, Medium) die, indien uitgebuit, konden leiden tot situaties waar een aanvaller willekeurige code kon invoeren in een actieve server en deze kon uitvoeren

Deze incidenten laten zien hoe het compromitteren van supply chains re reikwijdte van een aanval kan verbreden. Indien niet beveiligd kunnen cloudobjecten onverwachte aanvalsvectoren zijn. Het Docker Hub-incident omvatte bijvoorbeeld een kwaadaardig account dat Docker-afbeeldingen uploadde die een verborgen coin-mining-achterdeur bevatte. De Docker-afbeeldingen werden al bijna een jaar gehost op Docker Hub en waren miljoenen keren gedownload en gebruikt door nietsvermoedende beheerders en gebruikers.

Risico's voor supply chains strekken zich uit tot code in de cloud, open source, weblibrary's, containers en andere objecten in de cloud. Deze risico's, in combinatie met de hoge mate van variatie tussen de compromitteringsincidenten in de software- en hardware-supply chains die aan het licht zijn gekomen, zorgen ervoor dat aanvallen op de software-supply chain een brede bedreigingscategorie zijn. Hoewel er geen enkele oplossing is voor het hele spectrum van deze aanvallen, moeten organisaties wel preventieve bescherming en post-inbraakdetectie aanbrengen tegen aanvallen op de software-supply chain van gecompromitteerde hardware- en softwareleveranciers, aanbieders en overnames, opensourcesoftwareleveranciers en cloudservice- en infrastructuurleveranciers.

Cyberincidenten onderzoeken met DART

Het Microsoft Detection and Response Team (DART) is een wereldwijd team van cyberveiligheidsexperts en incidenthulpverleners die organisaties helpen bij het opsporen, onderzoeken en reageren op cyberbeveiligingsincidenten. Dit deel belicht een aantal van de incidenten die DART heeft behandeld in het afgelopen jaar. Het illustreert gemeenschappelijke aanvalstrends en hoe Microsoft en klanten in staat waren om ze te verijdelen.

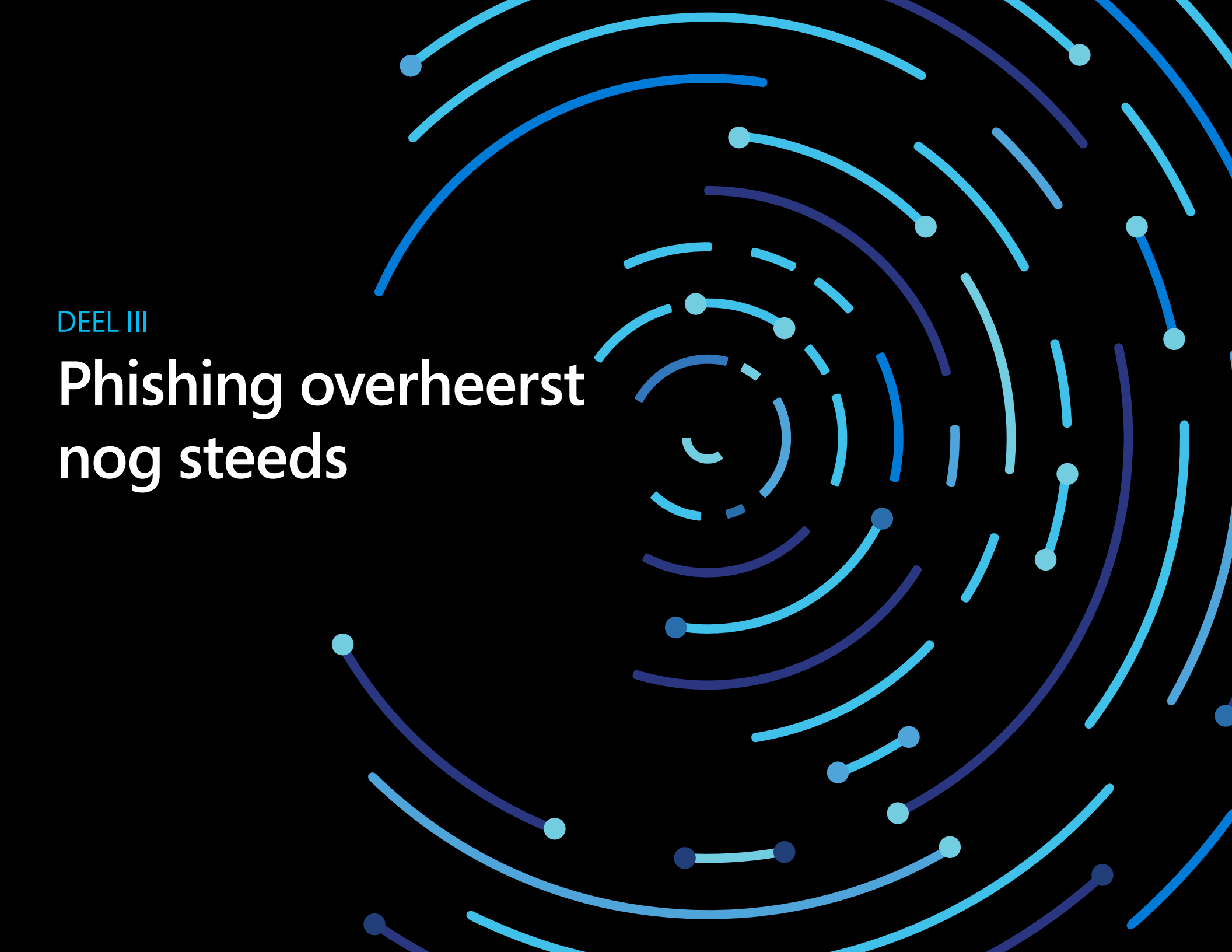
PROFESSIONELE DIENSTVERLENER WERD GECONFRONTEERD MET EEN AANVAL VAN EEN BUITENLANDSE STAAT DIE DATA EXFILTREERDE

Een professionele dienstverlener werd geraakt door een geavanceerde, door een staat ondersteunde Advanced Persistent Threat (APT) waarmee toegang werd verkregen tot inlogdata van de organisatie op hoog niveau. De aanvallers kregen toegang tot het netwerk via een wachtwoordbestuivingsaanval, waarbij gebruik werd gemaakt van een klein aantal zwakke of veelgebruikte wachtwoorden (zoals "p@ssword" of "123456") met een groot aantal gebruikersaccounts als doelwit en om toegang te verkrijgen tot administratieve inlogdata voor Office 365. (Wachtwoordbestuivingsaanvallen worden gebruikt om detectie te voorkomen doordat het aantal aanmeldingspogingen voor elk account wordt beperkt.) Na infiltratie van het netwerk voerde de APT een uitgebreide, geautomatiseerde exfiltratie uit van de data in de e-mailboxen van de medewerkers. Ondanks meerdere interne pogingen om de aanvallers uit te bannen, bleven de aanvallers meer dan 200 dagen in het netwerk aanwezig. Als onderdeel van de aanval maakte de aanvaller gebruik van de supply chain-software van de organisatie en van automatische exfiltratie van data.

Omdat ze vermoedden dat hun klantdata werden aangevallen, benaderde de organisatie het DART-team voor hulp bij het onderzoek en om verdere schade te helpen voorkomen. DART identificeerde gerichte Office 365-mailboxzoekopdrachten, gecompromitteerde accounts en kanalen voor opdrachten en beheersing van de aanvaller. De belangrijkste lessen van dit incident waren het implementeren van controles om cloudservices te beschermen tegen aanvallers en op identiteit gebaseerde aanvallen. De organisatie heeft meervoudige authenticatie (MFA), conditional access voor bepaalde cloudapps en Office 365-logging geïmplementeerd. Om zichzelf nog verder te beschermen tegen vergelijkbare aanvallen in de toekomst, kan de organisatie ook een oplossing voor eindpuntbedreigingsdetectie en -respons (EDR) implementeren om aanvallers te detecteren die het netwerk proberen aan te vallen. Bovendien hebben we deze organisatie een methode voor cloudbeheer en een mondiaal identiteitsteam aanbevolen dat een adequaat gebruikersverificatiebeleid kan beheren en afdwingen, zodat de organisatie toezicht heeft op de beveiliging en effectiever risico's kan inperken.

DEEL III

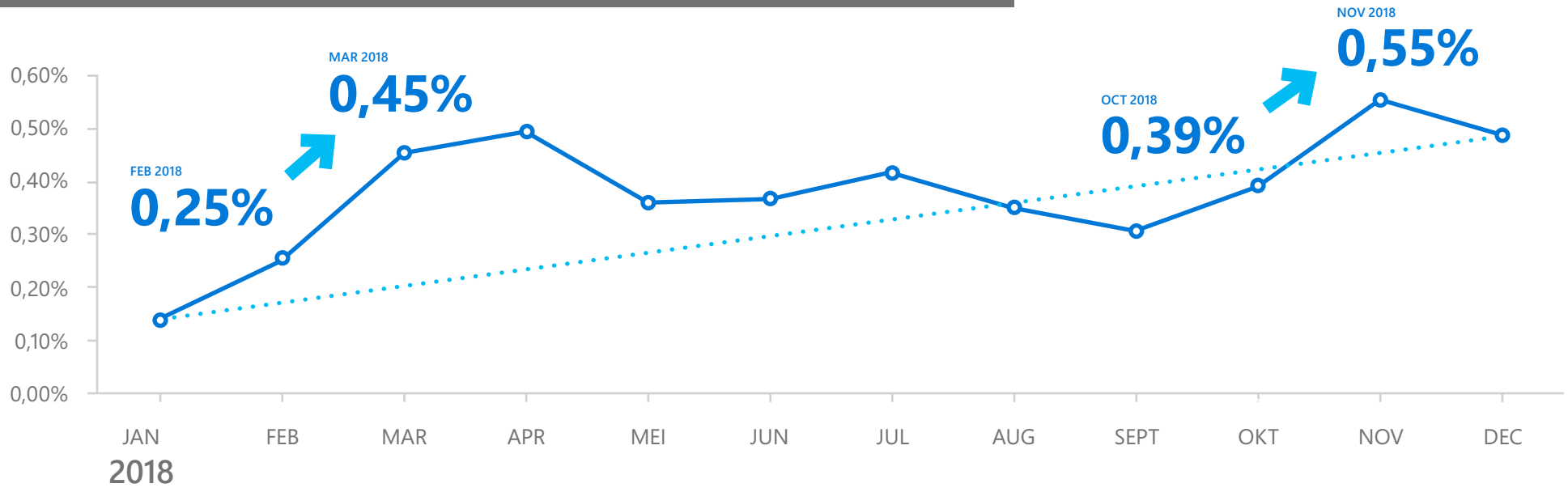
Phishing overheerst nog steeds



In 2018 hebben dreigingsanalisten van Microsoft voldoende bewijs gezien dat aanvallers nog steeds de voorkeur geven aan phishing als favoriete aanvalsmethode. Phishing lijkt een probleem te blijven in de nabije toekomst, omdat het gaat om menselijke beslissingen en oordelen en omdat cybercriminelen zich blijven inspannen om slachtoffers erin te laten trappen.

Phishingcijfers stijgen nog steeds

Percentage phishing-e-mails van het totale aantal inkomende e-mails



PHISHING BLIJFT DE FAVORIETE AANVALSMETHODE VAN AANVALLERS IN 2018.

Microsoft analyseert en scant in Office 365 meer dan 470 biljoen e-mailberichten per maand op phishing en malware, wat analisten een niet gering inzicht biedt in de trends en technieken van aanvallers. Het aantal inkomende e-mails die phishing-e-mails waren is gestegen met 250% tussen januari en december 2018. Phishing blijft een van de meest populaire aanvalsmethodes die worden gebruikt om schadelijke zero-day-payloads uit te kunnen voeren op computers van gebruikers. Microsoft wapent zich verder tegen deze aanvallen met extra bescherming, detectie, onderzoek en reactiemogelijkheden tegen phishing om gebruikers te beveiligen.

▲ **AFBEELDING 8.**

Phishing-e-mails in 2018

Evolutie van phishingaanvalsmethoden

Naarmate de tools en technieken die worden gebruikt om mensen te beschermen tegen phishing geavanceerder worden, worden aanvallers gedwongen zich aan te passen. Phishingaanvallen zijn steeds meer polymorf geworden, wat betekent dat aanvallers niet meer gebruik maken van één URL, domein of IP-adres om e-mail te verzenden, maar dat ze gebruikmaken van een gevarieerde infrastructuur met meerdere aanvalspunten. De aard van de aanvallen zelf is ook verder ontwikkeld, met moderne phishingcampagnes die variëren van korte aanvallen van een paar minuten tot veel langere campagnes met een hoog volume. Andere aanvallen zijn variabele serieaanvallen, waarbij aanvallers een klein aantal e-mails versturen op meerdere opeenvolgende dagen.

Daarnaast heeft Microsoft een trend waargenomen waarbij aanvallers gebruikmaken van gehoste cloudinfrastructuren en andere public cloudinfrastructuren, die het gemakkelijker maken om detectie te voorkomen doordat ze zich kunnen verbergen tussen legitieme sites en middelen. Aanvallers gebruiken bijvoorbeeld steeds meer populaire sites en services voor samenwerking en het delen van documenten om schadelijke payloads en valse aanmeldingsformulieren te verspreiden, die vervolgens worden gebruikt om inlogdata te stelen. Er is ook een toename van het gebruik van gecompromitteerde accounts om kwaadwillige e-mails verder binnen en buiten een organisatie te verspreiden.

Phishingcampagnes variëren van gerichte tot brede aanvallen

Net als bij de verspreiding van malware in het algemeen, variëren phishingcampagnes van gerichte tot brede, algemene aanvallen. Hoewel zeer verfijnde aanvallen grotere geldelijke winsten opleveren per succesvolle phishingaanval, brengen meer algemene aanvallen minder geld op per gecompromitteerd account, maar hiermee kunnen wel meer gebruikers worden aangevallen.

Een voorbeeld van een geavanceerde, gerichte campagne is Ursnif, waarbij aanvallers de naam van een document passend maken voor een bekende organisatie of branche van het doelwit. Dergelijke aanvallen zijn heel anders dan brede campagnes en lijken voor slachtoffers legitiemer en betrouwbaarder.

Sommige van de breed gerichte campagnes in 2018 waren gerelateerd aan bedrijfs-e-mailaanvallen (BEC) en omvatten de imitatie van bekende merken, domeinen, of gebruikers binnen de organisatie die het doelwit was, en geavanceerde spoofingcampagnes. Domeinimitatie is een bekende aanvalstactiek die gebruikt wordt om organisaties te laten geloven dat de e-mail betrouwbaar is en moet worden geopend.

Phishinglokmiddelen zijn er in vele vormen

Onderzoekers van Microsoft hebben geconstateerd dat er vele verschillende soorten phishinglokmiddelen en payloads worden gebruikt in campagnes, waaronder:

- **Domein-spoofing** (het domein waarvan het e-mailbericht afkomstig is, komt exacte overeen met de oorspronkelijke domeinnaam)
- **Domeinimitatie** (het domein waarvan het e-mailbericht afkomstig is, lijkt op de originele domeinnaam)[2]
- **Gebruikersimitatie** (het e-mailbericht lijkt afkomstig te zijn van een vertrouwd persoon)
- **Lokmiddel via tekst** (het tekstbericht lijkt afkomstig van een legitieme bron, zoals een bank, overheidsinstantie of een ander bedrijf, en meestal wordt het slachtoffer gevraagd om gevoelige informatie, zoals gebruikersnamen, wachtwoorden of gevoelige financiële data, te verstrekken)
- **Links voor phishing van inlogdata** (het e-mailbericht bevat een link naar een pagina die lijkt op een inlogpagina voor een legitieme site, zodat gebruikers hun inlogdata invoeren)
- **Phishingbijlagen** (het e-mailbericht bevat een schadelijke bestandsbijlage en de afzender verleidt het slachtoffer deze te openen)
- **Links naar valse cloudopslaglocaties** (het e-mailbericht lijkt afkomstig van een legitieme bron en verleidt de gebruiker om toestemming te geven en/of om persoonlijke informatie in te voeren, zoals inlogdata, in ruil voor toegang tot een valse cloudopslaglocatie)

Deze verscheidenheid aan lokmiddelen die kunnen worden ingezet door aanvallers, verhogen de complexiteit van phishingaanvallen waar organisaties rekening mee moeten houden.

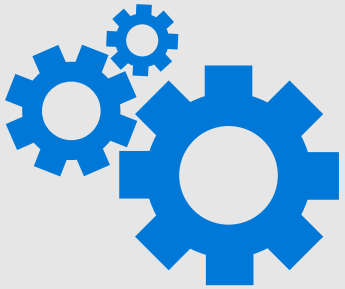
VOETNOTEN

[2] domeinimitatie kan lijken op domein-spoofing (een exacte overeenkomst met de oorspronkelijke domeinnaam) in het uitzonderlijke geval waarbij het domein wordt weergegeven in de weergavenaam van de e-mail.

Cyberincidenten onderzoeken met DART

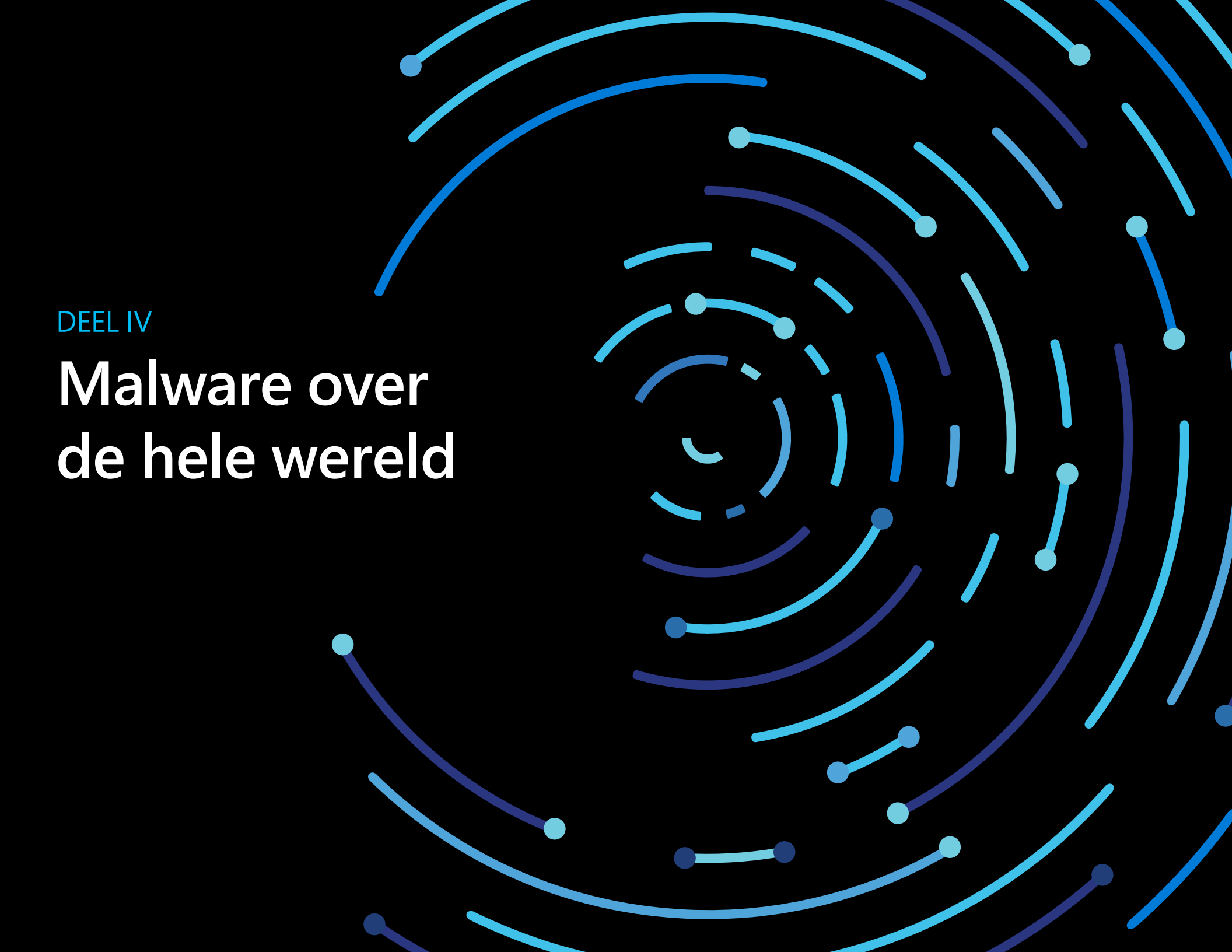
GROTE PRODUCTIEORGANISATIE GETROFFEN DOOR GERICHTE PHISHINGAANVAL

Een productieorganisatie werd gedurende enkele maanden geconfronteerd met een meerfasige phishingcampagne. Deze methode is niet ongebruikelijk. Tijdens de eerste fase gaat de aanvaller op verkenning uit en in de tweede fase worden de pijlen gericht op activa van hoge waarde. De eerste fase van deze campagne maakte gebruik van een bekende phishingaanval die is gebaseerd op een URL in een e-mail, die gericht wordt verstuurd naar een kleine groep in de organisatie. In de e-mail werd beweerd dat voor het doelwit een belangrijk elektronisch document klaar stond ter inzage en de ontvanger hoefde zich alleen met zijn of haar domeininlogdata te verifiëren om toegang te krijgen. Deze vervalste landingspagina die was opgezet voor het doelwit om het zogenaamde 'belangrijke document' in te zien, zorgde er in de praktijk voor dat de aanvaller inlogdata verkreeg voor toegang tot Office 365-accounts van overal ter wereld. De tweede fase van de phishingcampagne was bedoeld om gericht soortgelijke phishing-e-mails te sturen naar belangrijke medewerkers binnen de productieorganisatie in de hoop toegang te krijgen tot nog waardevollere data. Microsoft werkte samen met deze klant tijdens de tweede fase van de phishingcampagne. De belangrijkste lessen uit dit incident waren: phishing blijft een van de meest effectieve aanvalsmethoden en gebruikers zijn nog steeds de zwakste schakel in de beveiligingsketen.



Gebruikers trainen om op hun hoede te zijn voor phishing, tools inzetten om aanvallers te identificeren en aan te pakken, en regelmatig systemen patchen, zijn allemaal even belangrijk. Als de organisatie zelfs maar een van deze middelen negeert, kan dat leiden tot kwetsbaarheden.

In dit geval was het belangrijkste aandachtspunt van de klant de onmiddellijke noodzaak om de toegang tot de gecompromitteerde accounts te blokkeren. DART stelde, in samenwerking met Azure Identity en Office 365-teams, een plan op om de aanvaller uit het netwerk te bannen en om alle verkeer van en naar het besturings- en controlekanaal te volgen met behulp van de nieuwe geïmplementeerde oplossing voor Microsoft Azure Log Analytics. Het team was in staat om in slechts drie uur de situatie op te lossen. De toegang van de aanvaller werd geblokkeerd en de organisatie kon zich richten op schadebeoordeling en herstel. DART gebruikte de tools van Azure Log Analytics om het gedrag van de aanvaller te identificeren, wat hielp bij het ontdekken van veel configuratiekwesties voor de organisatie. DART identificeerde bijvoorbeeld hiaten in patches op kritieke servers, ontdekte computers op het netwerk die communiceerden met onbetrouwbare hosts op internet en vond ook een aantal belangrijke servers zonder malwarebescherming.

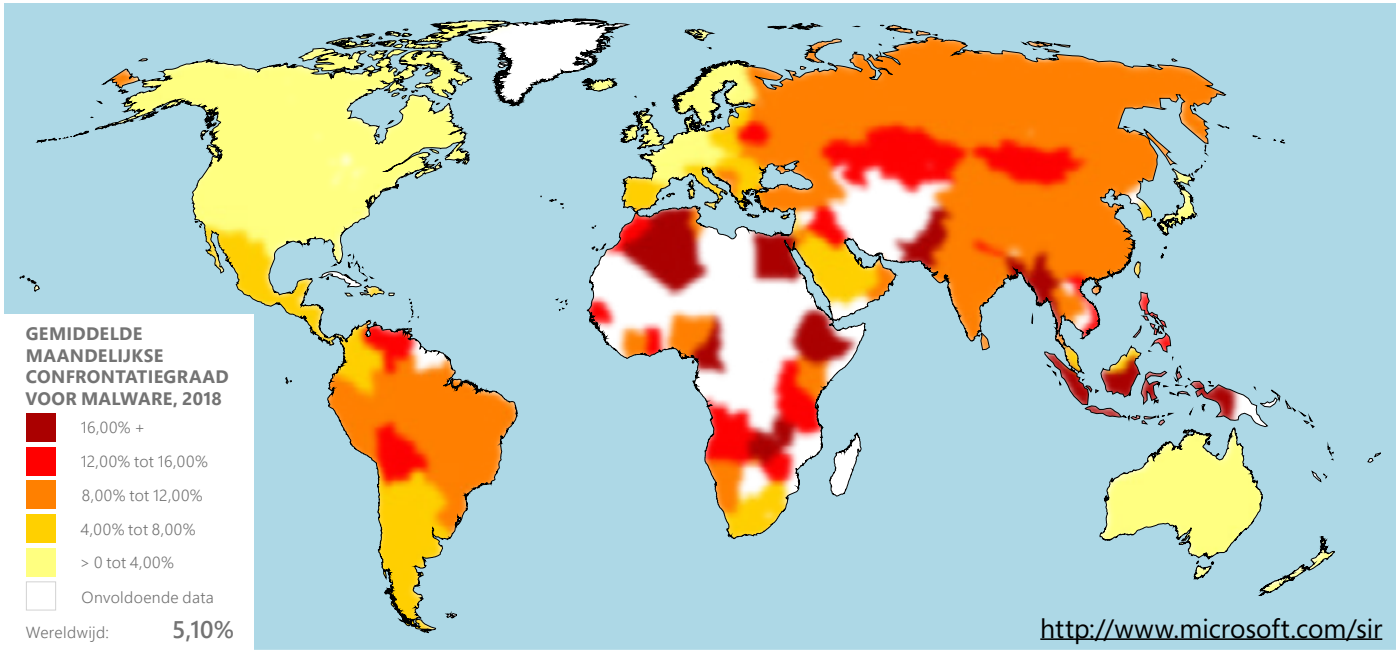


DEEL IV

Malware over de hele wereld

Malware zorgt voor risico's voor organisaties en particulieren in de vorm van verminderde bruikbaarheid, dataverlies, diefstal van intellectuele eigendommen, financiële verliezen, emotioneel leed en kan zelfs menselijke levens in gevaar brengen. Microsoft maakt gebruik van een uitgebreide set tools en technieken om malware-infecties te identificeren, blokkeren en uit te bannen, waar ze ook worden gevonden.

In 2017 varieerde de confrontatiegraad voor malware van ongeveer 5% tot meer dan 7%. In het begin van 2018 was er een piek waarna er gedurende het grootste deel van het jaar een afname plaatsvond tot net boven de 4%. Enkele mogelijke oorzaken voor de algehele daling van de confrontatiegraad voor malware in 2018 zijn het groeiende gebruik van Windows 10 en een verhoogd gebruik van Windows Defender ter bescherming. De confrontatiegraad is het percentage van computers met Windows Defender Antivirus die gedurende de maand malware gemeld hebben, met inbegrip van infectiepogingen die Defender heeft geblokkeerd.



AFBEELDING 9.

Gemiddelde maandelijkse confrontatiegraad voor malware, wereldwijd per land/regio in 2018

De vijf locaties met de hoogste confrontatiegraad voor malware tijdens de periode januari-december 2018 waren Ethiopië (26,33%), Pakistan (18,94%), de Palestijnse gebieden (17,50%), Bangladesh (16,95%) en Indonesië (16,59%), die in die periode een gemiddelde maandelijkse confrontatiegraad hadden van ongeveer 16,59% of hoger. De infectiepercentages lijken sterk samen te hangen met menselijke ontwikkelingsfactoren en technologische ontwikkeling in een maatschappij. Alle locaties met de hoogste confrontatiegraad in 2018 vielen in de onderste 40 procent van landen en regio's in de 2017 Information and Communications Technologies (ICT) Index, die is gepubliceerd door de United Nations International Telecommunication Union (ICT).

De vijf locaties met de laagste confrontatiegraad voor malware in diezelfde periode waren Ierland (1,26%), Japan (1,51%), Finland (1,74%), Noorwegen (1,79%) en Nederland (1,82%), die tijdens die periode allemaal een gemiddelde maandelijkse confrontatiegraad van 1,82% of lager hadden. Deze locaties hebben in de regel een ontwikkelde infrastructuur voor cyberbeveiliging en gerenommeerde programma's ter bescherming van kritieke infrastructuur en voor communicatie met hun burgers over elementaire veiligheid.

GEMIDDELDE MAANDELIJKSE CONFRONTATIEGRAAD VAN LANDEN DIE HET MEEST GERAAKT WORDEN DOOR MALWARE

Ethiopië: 26,33%

Pakistan: 18,94%

Palestijnse gebieden: 17,50%

Cyberincidenten onderzoeken met DART

MEERDERE FINANCIËLE DIENSTVERLENERS HEBBEN AANVALLEN MEEGEMAAKT VAN ANDERE NATIES DIE DE ACTIVITEITEN VERSTOORDEN

In een van de meest destructieve incidenten die DART heeft gezien, werden verschillende financiële dienstverleners gericht aangevallen door een door de staat gesteunde APT (een andere groep dan de groep die de professionele dienstverlener aanviel waarnaar eerder werd verwezen), met hetzelfde effect.

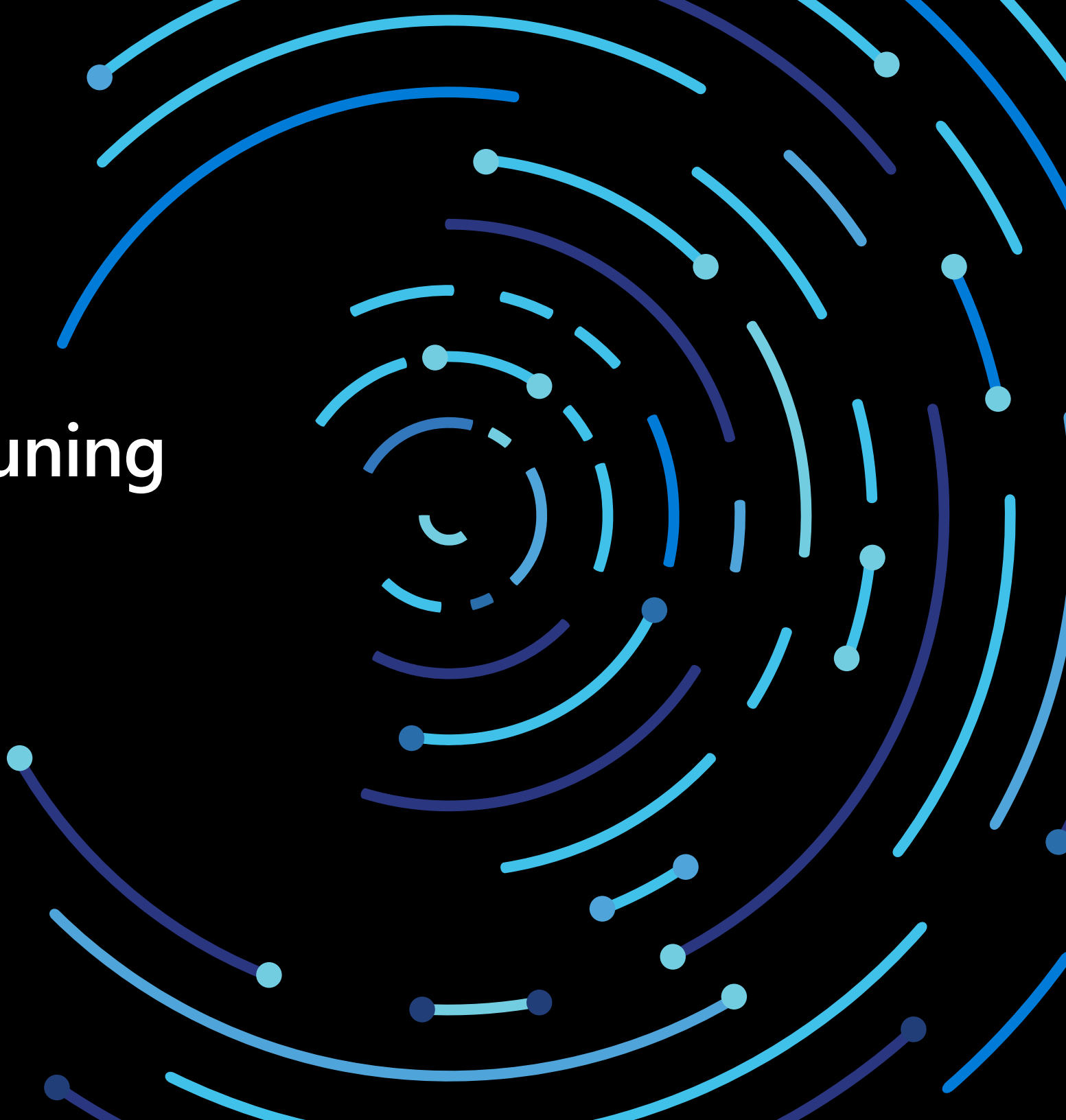
Deze APT kreeg beheertoegang na het infecteren van een initiële machine met een zeer gerichte, gemaskeerde achterdeur, mogelijk aangebracht via een spearphishing-e-mail. Vervolgens voerde de APT meerdere frauduleuze transacties uit en werden grote sommen geld overgeboekt naar buitenlandse bankrekeningen. In sommige gevallen bleef de aanvaller meer dan 100 dagen onopgemerkt. Nadat de aanvaller besefte dat de aanval was gedetecteerd, voerde de aanvaller snel een vooraf ingestelde aanval uit, waarbij destructieve malware werd aangebracht op meer dan de helft van de systemen in de infrastructuur. De klantactiviteiten werden meerdere dagen stilgelegd.

Er konden een paar belangrijke klantlessen worden getrokken uit deze incidenten. De eerste is dat softwarelevenscyclusbeheer zeer belangrijk is, wat het regelmatig updaten (besturingssystemen en beveiliging), patchen en auditen van systemen omvat.

In één geval had de Linux-systeemomgeving van een organisatie een uitzonderlijk hoog aantal workloads dat volledig onbeheerd werd uitgevoerd, wat leidde tot een opmerkelijk hoog risico op aanvallen. De tweede les was dat het belangrijk is om back-ups van systeemdata te bewaren op offline locaties in het geval dat de primaire data verloren gaan. Een andere les was dat traditionele antivirusoplossingen niet volstaan als er meer informatie nodig is over de activiteit van aanvallers.

Terugkeren naar de normale operationele modus had de hoogste prioriteit voor deze organisaties. DART hielp bij het herstellen van deze services door de impact te onderzoeken en om vervolgens de noodzakelijke maatregelen te ondernemen, zoals het verwijderen van malware van de getroffen systemen en om deze weer bij te werken naar een veilige staat. Het team heeft ook klanten getraind in het gebruik van Microsoft-tools voor dreigingsonderzoek, waaronder EDR, zodat ze zelf kunnen zoeken naar afwijkend gedrag en aanvallers in hun netwerk. DART benadrukte dat eindpuntbewaking van cruciaal belang is in de strijd tegen geavanceerde, gerichte aanvallen die onopgemerkt kunnen blijven voor traditionele antivirusoplossingen.

Ondersteuning



Ondersteuning

Het opbouwen van organisatorische veerkracht en zinvolle risicoreductie vereist een beveiligingsaanpak die preventie, detectie en reactie omvat. Wij hebben de volgende aanbevolen best practices en controlemaatregelen in die categorieën onderverdeeld.

PREVENTIE:

Preventieve controlemaatregelen spelen een belangrijke rol in een algehele verdedigingsstrategie, omdat de juiste investeringen de kosten van aanvallen voor cybercriminelen kunnen verhogen en deze verhoogde aanvalskosten in de loop van de tijd kunnen behouden (zonder dat een deskundige analist de uitvoer hoeft te controleren en interpreteren). Investeringen voor preventieve controlemaatregelen moeten zijn gericht op de laagste kostentechnieken om voortdurend goedkope en effectieve aanvalstechnieken uit te bannen.

Vier zaken om voor preventie te overwegen zijn:

1. **Gezonde beveiliging is essentieel. Zoals je hebt gezien in enkele van de cyberincidenten in dit rapport, kunnen algemene beveiligingsproblemen zorgen voor geavanceerde beveiligingsdreigingen, dus het volgen van deze tips kan helpen bij het inperken van risico's:**

- Vermijd het gebruik van onbekende gratis en/of illegale software. Gebruik alleen software van betrouwbare bronnen.
- Beperk het risico op diefstal van inlogdata en beveilig beheerdersaccounts. Voor meer informatie lees je dit blog met een overzicht van enkele principes en tools die Microsoft heeft gebruikt om onze eigen houding ten opzichte van veiligheid te verbeteren en met enkele beschrijvende roadmaps die je helpen om je eigen initiatieven te plannen.
- Pas de basisprincipes voor veilige configuratie toe die door softwareleveranciers worden verstrekt.
- Houd machines up-to-date door snel de meest recente updates toe te passen op besturingssystemen en applicaties, en implementeer onmiddellijk essentiële beveiligingsupdates voor besturingssystemen, browsers en e-mail. Isoleer (of verwijder) systemen die niet bijgewerkt of gepatcht kunnen worden.
- Implementeer geavanceerde e-mail- en browserbeveiligingen. Implementeer een beveiligde e-mailgateway met geavanceerde mogelijkheden voor bedreigingsbescherming tegen moderne phishingvarianten.
- Schakel hostantimalware- en netwerkverdediging in voor bijna realtime blokkerende reacties van de cloud (indien beschikbaar voor de oplossing).

2. **Implementeer toegangscontroles. Overweeg het volgende:**

   - Pas het principe van minimale bevoegdheid toe, inclusief de implementatie van netwerksegmentatie, waarbij je lokale beheerdersbevoegdheden afneemt van eindgebruikers, en wees behoedzaam bij het verlenen van bevoegdheden voor applicaties die op de computer worden uitgevoerd.
   - Download applicaties alleen van betrouwbare bronnen (een officiële appstore).
   - Implementeer sterke beleidsregels voor code-integriteit, waaronder het inperken van applicaties die gebruikers kunnen uitvoeren. Kies indien mogelijk voor een beveiligingsoplossing waarmee de uitgevoerde code in de systeemkern (kernel) wordt beperkt en waarmee niet-ondertekende scripts en andere vormen van niet-vertrouwde code kunnen worden geblokkeerd. Pas het whitelisten van applicaties toe.
   - Voor meer informatie over aanvallen op supply chains lees je dit blog van Microsoft-onderzoekers.

3. **Zorg voor back-ups.**

   - Maak vernietigingsbestendige back-ups van essentiële systemen en data.
   - Gebruik cloudopslagservices voor automatische online back-ups van data. Maak van on-premises data regelmatig back-ups van belangrijke data met behulp van de 3-2-1-regel. Bewaar drie back-ups van data, op twee verschillende opslagtypen, en ten minste één back-up op een andere locatie.

4. **Let op en onderneem actie als je iets vermoedt.**

   - Instrueer medewerkers om op hun hoede te zijn voor verdachte communicatie waarin om gevoelige informatie wordt gevraagd, instrueer hen hoe ze moeten reageren en laat hen onmiddellijk rapporteren aan het beveiligingsteam van de organisatie. Training kan ook helpen om social engineering en spearphishing-aanvallen tegen te gaan.
   - Wees voorzichtig bij het klikken op URL's. Veilige gewoontes bij het browsen op internet en het gebruiken van oplossingen die waarschuwingen geven over het opvragen van onveilige sites, of deze zelfs blokkeren, kan helpen de kans te verminderen op confrontatie met websites die zijn gekoppeld aan cryptovaluta-mining.
   - Als een computer uitzonderlijk traag is, zoek dan naar verdachte bestanden die worden uitgevoerd en laat daarvan gerust een voorbeeld zien aan de leverancier van het besturingssysteem. Je kunt bestanden voor malware-analyse bij Microsoft indienen op https://www.microsoft.com/wdsi/filesubmission.

DETECTIE EN REACTIE:

Detectie en reactie dragen bij aan de veerkracht door de tijd te beperken die een aanvaller toegang heeft tot bronnen. Dit vermindert de ROI van de aanvaller door zowel de kosten voor de aanvallers te verhogen (ze moeten hun activiteiten opnieuw uitvoeren of aanpassen) als het rendement te verlagen (de kans beperken om hun doelstelling te bereiken).

Dezelfde cloudtechnologie die bedrijven in staat stelt om beter te voldoen aan marktbehoeften kan ook bij beveiligingsoperaties helpen om beter terug te vechten tegen aanvallers.

AFBEELDING 10.

Ontwikkelingstraject van SOC´s

Als we kijken naar het ontwikkelingsverloop van Security Operations Centers (SOC's), zien we dat technologie voortdurend de snelheid en kwaliteit van beslissingen en acties van SOC's verbetert. Veel van deze innovaties kunnen worden gekoppeld aan elke fase van de Observe Orient Decide Act (OODA)-lus, die werd gedocumenteerd door USAF Kolonel John Boyd.[3]

OBSERVEER: SOC's kunnen de grote hoeveelheid beveiligingsdata (van Microsoft en andere bronnen) toepassen om hun inzicht in de organisatie en de externe omgeving flink te vergroten.

ORIËNTEER: terwijl deze nieuwe databronnen beschikbaar komen voor reeds overbelaste SOC's, wordt machine learning (een subset van kunstmatige intelligentie) als essentiële tool voor enorme datasets en om afwijkingen te identificeren het onderzoeken waard. Beveiligingsleveranciers (waaronder Microsoft) gebruiken technologie voor machine learning om gebeurtenissen snel te prioriteren (en machine learning helpt ook om afzonderlijke gebeurtenissen samen te voegen om de grote lijn te begrijpen).

BESLIS: omdat het volume en de complexiteit van een aanval een SOC snel kan overbelasten, moeten analisten en incidenthulpverleners snel beslissingen maken en handelen in reactie op waarschuwingen en detecties. Microsoft en andere leveranciers hebben geautomatiseerde onderzoeksmogelijkheden geïntegreerd, maar ook begeleiding om analisten te helpen snel de juiste beslissingen te nemen (om bijvoorbeeld potentieel geïnfecteerde of gecompromitteerde apparaten te isoleren). Op dit moment is de automatisering gericht op het snel oplossen van incidenten met een lage prioriteit, zodat gespecialiseerde vaardigheden kunnen worden toegepast op meer complexe problemen.

HANDEL: voor een reactie is een snelle en accurate uitvoering over vele technologieën en platforms vereist en dat is precies wat technologieën voor beveiliging en reactieautomatisering mogelijk maken. Microsoft en vele andere organisaties blijven investeren in deze technologieën, waaronder in detectie van moderne dreigingen en geautomatiseerde reactieoplossingen.

VOETNOTEN:

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Enkele andere trends die van toepassing zijn op een moderne SOC:

- **Kwaliteit boven kwantiteit van waarschuwingsfeeds:** terwijl organisaties zich verplaatsen van het beheren van 'niet genoeg informatie' naar het beheren van 'te veel informatie', wordt de tijd en aandacht van zeer gespecialiseerde SOC-analisten steeds waardevoller. Dit leidt tot een verhoogde behoefte van kwaliteit in de signaleringen die de aandacht van analisten uit laag 1 en 2 vereisen. Terwijl extra datafeeds altijd nuttig zijn voor onderzoekers en proactief jagen, meet Corporate IT SOC van Microsoft het daadwerkelijke percentage waarschuwingsfeeds waarop analisten moeten reageren (en vereist het momenteel een daadwerkelijk percentage van 90% of hoger).

- **Datazwaarte:** analytics over grote datasets (inclusief beveiligingsdata) is moeilijk te analyseren zonder toegang tot de onderliggende ruwe data. Naarmate meer beveiligingsdata beschikbaar komt, wordt het economischer en praktischer om de beveiligingsanalyses in de cloud uit te voeren in plaats van op een on-premises systeem. Dit zal waarschijnlijk leiden tot een evolutie van SIEM- en SOC-architecturen die mogelijk kunnen bestaan uit hybride SIEM-benaderingen of de aanname van cloud-SIEM as a service.

- **Hoge context:** dit soort detecties zijn veel nuttiger vanwege het vermogen om datasets effectiever aan elkaar te koppelen. Hoewel traditionele op netwerkverkeer gebaseerde detecties nog wel enige beveiligingswaarde heeft, ontbreekt bij dergelijke ruwe data vaak de context om onderscheid te maken tussen legitieme en abnormale activiteiten. We zien dat SOC's veel meer waarde verkrijgen uit contextrijke detecties, zoals:

  - **Oplossingen voor eindpuntdetectie en -respons (EDR)** oplossingen met diepe context voor hostactiviteit
  - **Op identiteit** gebaseerde detecties die inzicht geven in normale patronen voor gebruikersverificatie (locaties, tijden, gebruikte services, enz.) en die gedragsanalyse toepassen

Deze contextrijke detecties zijn moeilijker te ontwijken door tegenstanders omdat ze veel complexere activiteiten moeten nabootsen (ten opzichte van enkele technische attributen van IP-verkeer).

Een andere les die we hebben geleerd van grote inbraken bij klanten was de moeilijkheid om snel te reageren op incidenten wanneer de IT-functies gedeeltelijk of volledig zijn uitbesteed. Wij raden aan contracten voor IT-outsourcing en Service Level Agreements (SLA's) te herzien, evenals supply chain-leveranciers, om er zeker van te zijn dat ze raad weten met snelle beveiligingsreacties. Voor meer informatie over onze incidentonderzoeken bij klanten, bekijk je de Incident Response Reference Guide (IRRG) op https://aka.ms/IRRG.

Databronnen

Databronnen

Microsoft heeft de data in het Microsoft Security Intelligence-rapport verzameld tijdens het aanbieden van een breed scala aan Microsoft-producten en -services, zoals besproken in de privacyverklaring van Microsoft. Deze data bieden ons waardevolle informatie over de veiligheid en activiteiten van onze producten en services, evenals inzicht in het cyberbeveiligingslandschap in het algemeen. Deze data bevatten analyses uit de volgende bronnen:[4]

- **Azure Security Center** is een service die organisaties helpt bij het voorkomen, detecteren en reageren op bedreigingen door meer inzicht te bieden in de beveiliging van workloads in de cloud en het gebruiken van advanced analytics en bedreigingsinformatie om aanvallen te detecteren.

- **Bing** is de zoek- en beslissingsengine die miljarden scans van webpagina's per jaar uitvoert om te zoeken naar schadelijke content. Nadat dergelijke content is gedetecteerd, geeft Bing waarschuwingen weer aan gebruikers om infectie te voorkomen.

- **Exchange Online** is de door Microsoft gehoste e-mail- en productiviteitsservice. Antimalware- en antispamservices van Exchange Online scannen jaarlijks miljarden berichten om spam en malware te identificeren en blokkeren.

- **Malicious Software Removal Tool** (MSRT) is een gratis tool die Microsoft heeft ontworpen om specifieke veelvoorkomende malware op computers van klanten te helpen identificeren en verwijderen. MSRT wordt hoofdzakelijk uitgebracht als een belangrijke update via Windows Update, Microsoft Update en Automatic Updates. Een versie van de tool is ook beschikbaar via het Microsoft Download Center. MSRT is geen vervanging voor een up-to-date realtime antivirusoplossing.

- **Microsoft Safety Scanner** is een gratis downloadbare beveiligingstool die on-demand kan scannen en die helpt bij het verwijderen van malware en andere schadelijke software. Microsoft Safety Scanner is geen vervanging voor een up-to-date antivirusoplossing, omdat deze geen realtime bescherming biedt en niet kan voorkomen dat een computer geïnfecteerd raakt.

VOETNOTEN:

[4] Het is belangrijk om te weten dat deze data altijd strenge privacy- en compliancescheidslijnen doorloopt voordat deze worden gebruikt voor beveiligingsdoeleinden.

- **Microsoft Security Essentials** is een gratis en eenvoudig te downloaden realtime beveiligingsproduct die fundamentele, effectieve antivirus- en antispywarebescherming biedt voor Windows Vista en Windows 7.

- **Microsoft System Center Endpoint Protection** (voorheen Forefront Client Security en Forefront Endpoint Protection) is een uniform product dat bescherming biedt tegen malware en ongewenste software voor zakelijke desktops, laptops en serverbesturingssystemen. De applicatie maakt gebruik van de Microsoft Malware Protection Engine en Microsoft Antivirus Signature Database om realtime, geplande en on-demand beschikbare bescherming te bieden.

- **Office 365** is de Microsoft Office-abonnementsservice voor organisaties en thuisgebruikers. Geselecteerde abonnementsplannen omvatten toegang tot Office 365 Advanced Threat Protection.

- **Windows Security** in Windows 10 biedt realtime scannen en verwijderen van malware en ongewenste software. Daarnaast maakt de nieuwste versie van Windows gebruik van rijke contextuele data, zoals machineconfiguratie, apparaatprestaties en -status en andere soortgelijke informatie om de beveiliging van klanten te verbeteren. Tegelijkertijd zorgen we ervoor dat klanten beter geïnformeerd zijn over hun privacy in Windows 10. Lees dit blog voor meer informatie over een aantal manieren waarop Microsoft dit doet.

- **Windows Defender Advanced Threat Protection** is een service die is ingebouwd in de Windows 10 Anniversary Update en latere versies, waarmee zakelijke klanten geavanceerde persistente bedreigingen en datalekken op hun netwerken kunnen detecteren, onderzoeken en verhelpen.

- **Windows Defender Offline** is een downloadbare tool die kan worden gebruikt om een opstartbare cd, dvd of USB-flashstation te maken om een computer te scannen op malware en andere bedreigingen. Het biedt geen realtime bescherming en is geen vervanging voor een up-to-date antimalwareoplossing.

- **Windows Defender SmartScreen**, een functie in Microsoft Edge en Internet Explorer die gebruikers bescherming biedt tegen phishingsites en sites die malware hosten. Microsoft onderhoudt een database met phishing- en malwaresites die worden gerapporteerd door gebruikers van Microsoft Edge, Internet Explorer en andere producten en services van Microsoft. Wanneer een gebruiker een site in de database probeert te bezoeken terwijl het filter is ingeschakeld, wordt er een waarschuwing weergegeven en wordt de navigatie naar de pagina geblokkeerd.