Microsoft

MICROSOFT SECURITY INTELLIGENCE-RAPPORT

UDGAVE 24
JANUAR-DECEMBER 2018

Indholdsfortegnelse

Dette dokument er kun til oplysningsformål. MICROSOFT FRASKRIVER SIG ETHVERT ANSVAR, DET VÆRE SIG UDTRYKKELIGT, STILTIENDE ELLER LOVPLIGTIGT, MED HENSYN TIL OPLYSNINGERNE I DETTE DOKUMENT.

Dette dokument leveres, "som det er og forefindes". De oplysninger og synspunkter, der kommer til udtryk i dette dokument, herunder webadresser og andre referencer til websteder, kan blive ændret uden varsel. Du bærer risikoen for at bruge det.

Navnene på faktiske virksomheder og produkter heri kan være varemærker tilhørende deres respektive ejere.

Forfattere og bidragydere

Abhishek Agrawal
Databeskyttelse

David Fantham
Databeskyttelse

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

Forord

Velkommen til den 24. udgave af Microsoft Security Intelligence-rapporten (SIR). Som bruger og sikkerhedsarkitekt læser jeg rapporter som denne og håber at få en lidt bedre forståelse af landskabet samt praktiske råd til, hvordan jeg kan bruge denne viden til at forsvare og beskytte organisationer på en mere effektiv måde.

SIR-teamet underviser i denne rapport i forbedret cyberbeskyttelse og har gennemgået data for et år for at uddrage de vigtigste konklusioner.

Det, du kan læse dig frem til, er viden, som er hentet på baggrund af sikkerhedsdataanalyser for et helt år, og den praktiske erfaring, man har fået ud af dette. De analyserede data omfatter 6,5 billioner trusselssignaler, der går gennem Microsofts cloud hver eneste dag, og forskning og erfaringer fra den virkelige verden fra vores tusindvis af sikkerhedsforskere og respons-enheder i hele verden. I 2018 brugte hackere en række beskidte tricks, både nye (coin-mining) og gamle (phishing), i deres konstante forsøg på at stjæle data og ressourcer fra kunder og organisationer. Hybride angreb som Ursnif-kampagne, blandede sociale og tekniske tilgange. Efterhånden som forsvarsprogrammer blev klogere i bekæmpelsen af ransomware (en kraftig og ødelæggende form for angreb), vendte de kriminelle sig mod mere "hemmelige", men stadig rentable, coin-miners.

Dette skift kan føles frustrerende – og det kan virke, som om hackerne altid er et skridt foran. Men set fra et andet perspektiv er denne historie positiv. Forsvarere og cybersikkerhedsmedarbejdere som dig har implementeret defensive teknikker, der har tvunget hackerne til at ændre deres foretrukne nyttedata og gå væk fra ransomware.

Et andet område, hvor cyberkriminelle har øget deres aktivitet, er i forsyningskæden. En af de mest bemærkelsesværdige, Dofoil-coin-miner-udbruddet, som slog til den 6. marts 2018, blev sat i gang af en giftig peer-to-peer-app. Bekymringerne for forsyningskæden gik fra apps og videre til cloud-løsningen og omfattede skadelige browserudvidelser, kompromitterede Linux-lagre og flere forekomster af moduler backdoor-moduler. For at imødegå denne trussel går organisationer nu tilbage til en gennemsigtig og pålidelig forsyningskædemodel.

Data er fantastiske, men sommetider hjælper det at finde ud af, hvad der i virkeligheden er sket i en organisation. Derfor har vi medtaget de erfaringer, der er gjort i marken, fra vores DART-team (Detection and Response Team). De omfatter bl.a., hvordan en stor produktionsvirksomhed kunne implementere kontroller, der blokerer en phishing-kampagne med flere faser, som havde plaget dem i månedsvis, og finanstjenesteorganisationer, der langt om længe var i stand til at udradere trusselsaktører fra deres systemer ved hjælp af avancerede undersøgelsesværktøjer og endpoint-overvågning.

Sidst, men ikke mindst, steg antallet af phishing-klik fortsat – men maskinlæringsmodeller bliver bedre og bedre til at fange phishing-angreb, inden de rammer brugerfelter, og til at forhindre skader efter klik, hvis de alligevel når frem. Er der flere gode nyheder? Et stigende antal virksomheder implementerer multifaktorløsninger for at begrænse antallet af gennemførte angreb med phishing-e-mails til tyveri af legitimationsoplysninger.

Hackerne leder efter muligheder, så jo mere vi ved om deres teknikker og aktiviteter, jo bedre kan vi forberede os på at udvikle forsvar og reagere hurtigt. Små vigtige skridt kan gøre en enorm forskel for en organisations generelle cybersikkerhed. Derfor kan du ud over oplysninger om det skiftende malware- og angrebslandskab finde anbefalede skridt og anden vejledning til bedste praksis i denne rapport. Da jeg arbejdede med cybersikkerhed, var det lige præcis det, jeg havde brug for i min kamp mod skurkene. Vi håber, det også er det, du har brug for.

Diana Kelley
Microsoft Cybersecurity Field CTO

P.S. Vi forsøger konstant at forbedre SIR. Hvis du har feedback, er du velkommen til at kontakte os og fortælle os, hvordan du synes, vi klarer os.

AFSNIT I

Ransomware, kryptovaluta-mining og penge

De store sikkerhedshistorier fra 2017 omfattede hovedsageligt ransomware. Højt profilerede verdensomspændende udbrud af WannaCrypt- og Petya betød, at ransomware – en type malware, der låser eller krypterer computere og derefter kræver penge for at genoprette adgangen til dem – blev en del af den generelle bevidsthed, og mange mente, at problemet kun ville blive større i fremtiden. I stedet faldt antallet af ransomwarehændelser markant i 2018.

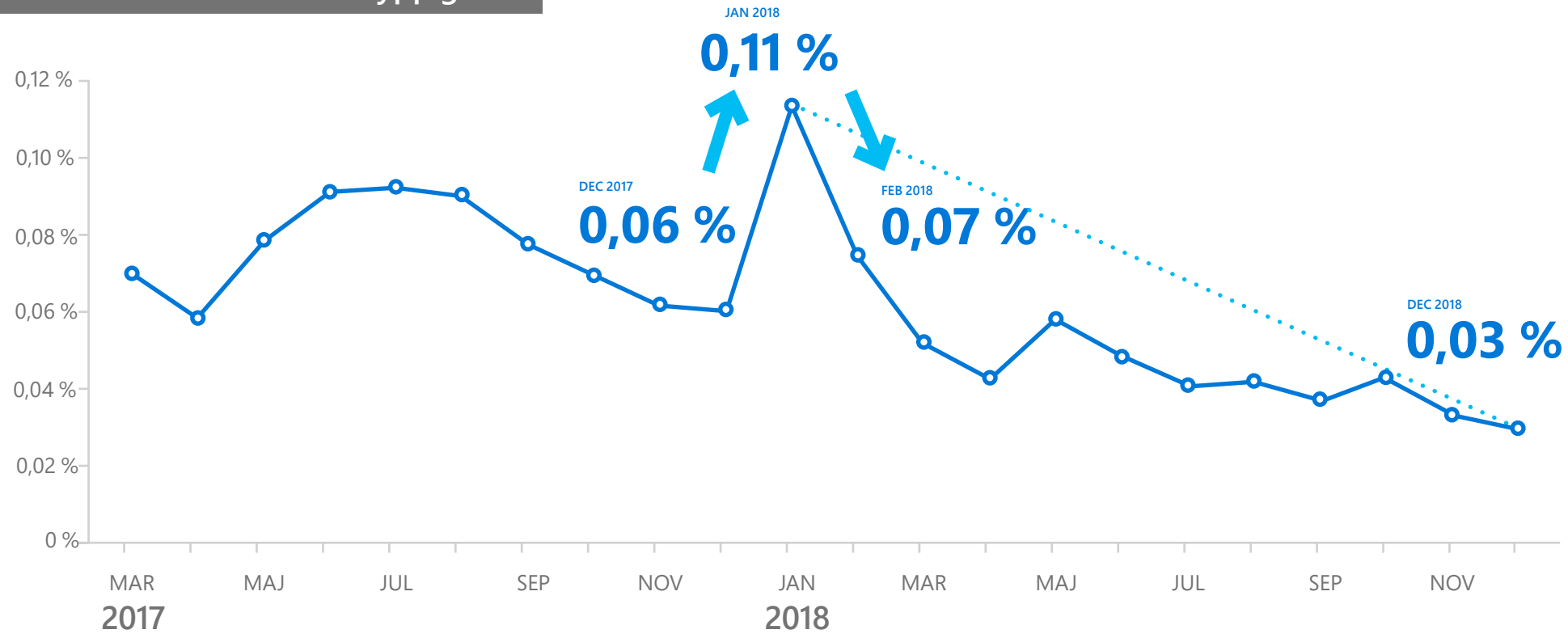
Faldet i antallet af ransomwarehændelser skyldtes til dels forbedret opdagelse og uddannelse, som gjorde det vanskeligere at tjene penge på dem. Det medførte, at hackerne begyndte at rette opmærksomheden væk fra ransomware og i stedet fokusere på kryptovaluta-mining, som bruger ofrenes computerressourcer til at skaffe hackerne digitale penge. Skiftet viser de fleste profitorienterede cyberkriminelles fundamentalt opportunistiske karakter. De har en tendens til at jagte de nemmeste penge, og når økonomien skifter i forbindelse med cyberkriminalitet, er de hurtige til at følge efter.

TILBAGEGANG I ANTALLET AF RANSOMWARE-ANGREB

For mere end et årti siden blev de hackere og svindlere, der dominerede den tidlige malware-undergrund, fortrængt af organiseret kriminalitet og andre profitorienterede interesser. Mens malwareudbrud ofte var iøjnefaldende og tydelige, ville profitorienteret malware højst sandsynligt arbejde meget mere i det skjulte og undlade at tiltrække sig opmærksomhed for at kunne fortsætte med at udføre sin funktion – at sende spam, stjæle følsomme oplysninger, udføre angreb med nægtelse af adgang til tjenester og andre skadelige aktiviteter – så længe som muligt.

Ransomware ændrede denne tendens. I stedet for at forsøge at forblive uopdaget, nægter ransomware åbent ofrenes adgang til deres computere og vigtige filer, indtil ofret betaler løsepengene (og ofte slipper hackerne ikke kontrollen over computerne, selv når løsepengene er betalt). Da ransomware var på sit højeste i 2017, så det ud til, at denne type åbne angreb kunne udgøre en ny fase med hensyn til angrebsteknikker. Men de nyeste data tyder på, at ransomware er på tilbagetog, og at hackerne i stigende grad vender tilbage til den mere skjulte måde at operere på, som de anvendte tidligere, hvor de forsøger at forblive uopdagede, så de mere effektivt kan udføre angreb såsom kryptovaluta-mining. Selvom der har været et fald i antallet af ransomwarehændelser, betyder det ikke nødvendigvis, at angrebenes alvorlighed er aftaget.

Ransomware-hændelseshyppighed

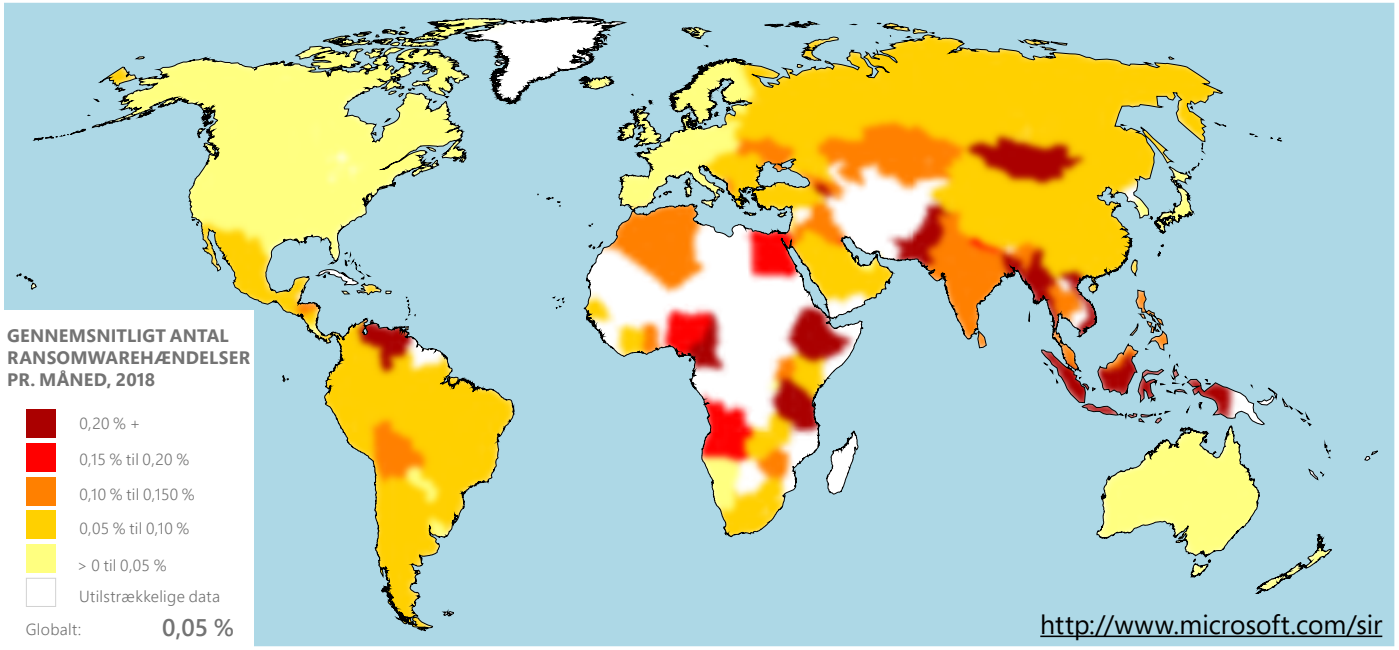


Ransomware-hændelseshyppigheden faldt med ca. 60 procent mellem marts 2017 og december 2018 med midlertidige stigninger i løbet af perioden.

FIGUR 1.

Ransomware-hændelser fra marts 2017 til december 2018

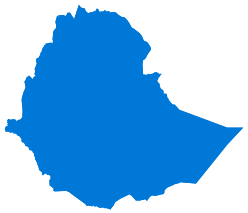
Der er formentlig mange grunde til dette samlede fald, men Microsofts sikkerhedsforskere har en mistanke om, at en primær faktor er, at både slutbrugere og organisationer bliver mere opmærksomme på randomware-trusler og håndterer dem mere intelligent, f.eks. udviser de større forsigtighed og sikkerhedskopierer vigtige filer, så de kan gendannes, hvis de bliver krypteret af ransomware. Desuden er cyberkriminelle som tidligere beskrevet opportunistiske.



FIGUR 2.

Gennemsnitligt antal månedlige ransomwarehændelser på verdensplan efter land/region i 2018

DET LAND, DER ER MEST PÅVIRKET AF RANSOMWARE: ETIOPIEN



Gennemsnitlig antal hændelser pr. måned: 0,77 %

De fem steder med det største antal ransomwarehændelser pr. måned i 2018 var Etiopien (gennemsnitligt 0,77 procent ramsomwarehændelser pr. måned), Mongoliet (0,46), Cameroun (0,41), Myanmar (0,33) og Venezuela (0,31), som hver havde et gennemsnitligt antal ransomwarehændelser pr. måned på 0,31 procent eller derover i perioden.1 For nogle år siden havde ransomware-angreb en tendens til at samle sig i rige lande og områder i Europa og Nordamerika, men efterhånden som ransomware begyndte at blive mindre populære hos hackerne, er hændelsesmønsteret begyndt at ligne mønsteret for malware som helhed mere.

De steder, der havde det laveste antal ransomwarehændelser i 2018, var Irland (0,01), Japan (0,01), USA (0,02), Storbritannien (0,02) og Sverige (0,02 procent), som alle havde et gennemsnitligt antal ransomwarehændelser pr. måned på 0,02 procent eller derunder i den samme periode. Steder med et lavt antal hændelser har en tendens til at have en fuldt udviklet infrastruktur og veletablerede programmer til beskyttelse af kritisk infrastruktur og kommunikation med deres borgere om grundlæggende sikkerhed.

FODNOTER

[1] Antallet af hændelser er den procentdel af computere, der kører Microsoft-sikkerhedsprodukter i realtid, som rapporterer en malwarehændelse. Selvom der registreres en trussel, betyder det ikke, at computeren nødvendigvis er inficeret. Det er kun computere, hvis brugere har valgt at levere data til Microsoft, der medtages i beregningen af antallet af hændelser.

STIGNING I KRYPTOVALUTA-MINING

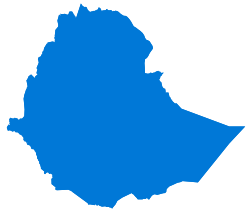
Kryptovalutaer er virtuelle penge, der kan bruges til at købe og sælge varer og tjenester anonymt – både online og i den fysiske verden. Der findes mange forskellige typer kryptovaluta, men de er alle baseret på blockchain-teknologi, hvor hver enkelt transaktion registreres i en distribueret hovedbog, der vedligeholdes af tusindvis eller millionvis af computere rundt om i verden. Der skabes (eller "mines") nye mønter af computere, der udfører komplekse beregner, der også fungerer som bekræftelse af blockchain-transaktioner.

Mønt-mining kan være en indbringende forretning – i 2018 var en enkelt Bitcoin-mønt (Bitcoin er den ældste og mest populære kryptovaluta) flere tusind USD værd – men det kan være ressourcekrævende at udføre de nødvendige beregninger, og den nødvendig indsats øges, efterhånden som hver ny mønt udvindes. I forbindelse med populære valutaer som er også næsten umuligt at "mine" mønter på en rentabel måde uden adgang til omfattende computerressourcer, som er uden for rækkevidde for de fleste enkeltpersoner eller mindre grupper. Derfor er hackere, der er ude efter ulovlige indtægter, i stigende grad gået over til at anvende malware, der giver dem mulighed for at bruge ofrenes computere til at udvinde kryptovalutamønter. Denne fremgangsmåde giver dem mulighed for at udnytte databehandlingskraften fra hundredtusindvis af computere i stedet for en eller to. Selv når der opdages en mindre infektion, gør kryptovalutaers anonyme natur det vanskeligt at spore de ansvarlige bag angrebene.

I 2018 var det gennemsnitlige månedlige antal hændelser med "mining" af kryptovalutamønter på 0,12 procent sammenlignet med blot 0,05 procent for ransomware. Der er mange faktorer, der bidrager til, at mining er blevet mere populær som nyttedata for malware. I modsætning til ransomware kræver kryptovaluta-mining ikke brugerinput. Det fungerer i baggrunden, mens brugeren udfører andre opgaver eller er væk fra computeren, og bemærkes muligvis overhovedet ikke, medmindre det forringer computerens ydeevne i væsentlig grad. Det betyder, at brugerne er mindre tilbøjelige til at fjerne truslen, og den kan fortsætte mining-aktiviteterne til fordel for hackeren i en længere periode.

Tilgængeligheden af "standardprodukter" til skjult mining af mange kryptovalutaer er en anden faktor, der fremmer denne tendens. Det er ikke svært at få adgang på grund af udbredte tilgængelighed af coinmining-software, som cyberkriminelle ompakker som malware, der kan leveres til intetanende brugeres computere. De farlige miners distribueres herefter til ofre ved hjælp af samme teknikker, som hackere brugere til at levere andre trusler, som f.eks. social engineering, udnyttelse og drive-by-downloads. Når mining-softwaren er installeret, kører den i baggrunden på ofrenes computere og udfører blockchain-beregninger, og hackeren høster frugterne af dette.

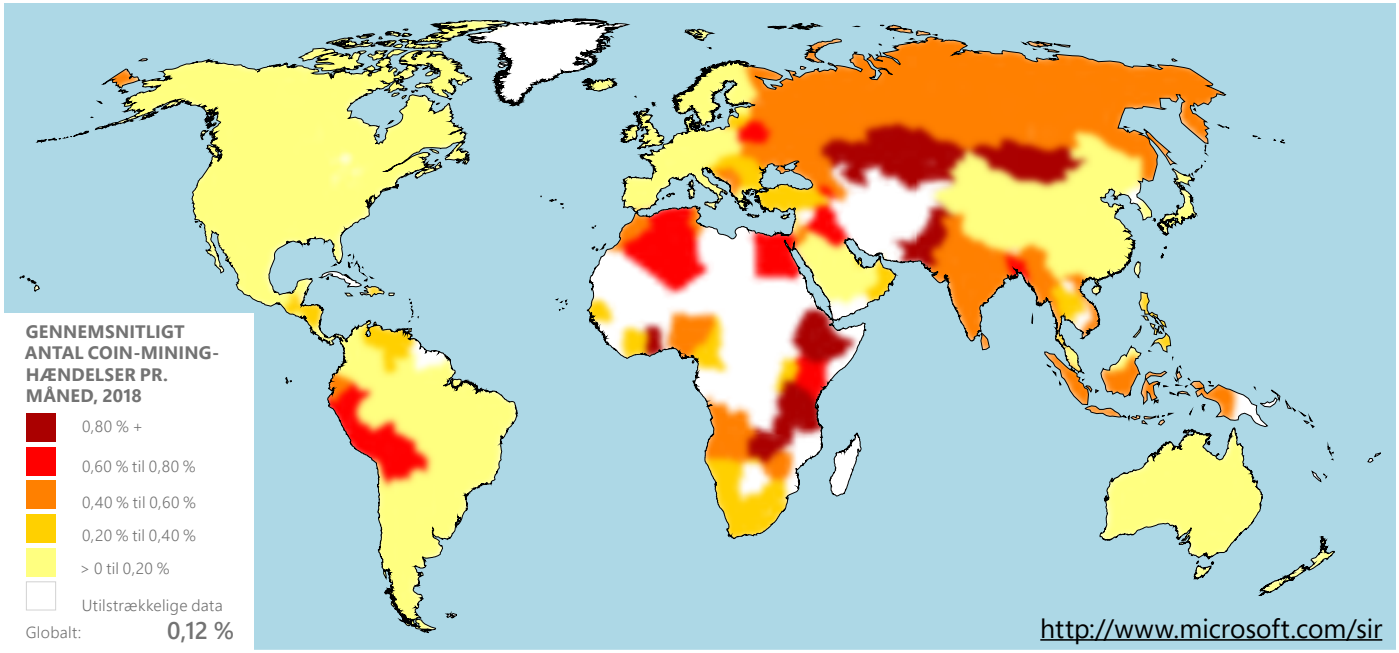
GENNEMSNITLIGT ANTAL HÆNDELSER PR. MÅNED FOR LANDE, DER ER MEST PÅVIRKEDE AF KRYPTOVALUTA-MINING



Etiopien: **5,58 %**

Tanzania: **1,83 %**

Pakistan: **1,47 %**



FIGUR 3.

Gennemsnitligt antal månedlige coin-miner-hændelser på verdensplan efter land/region i 2018

GENNEMSNITLIGT ANTAL HÆNDELSER PR. MÅNED FOR LANDE, DER ER MINDST PÅVIRKEDE AF KRYPTOVALUTA-MINING

Irland: 0,02 %

Japan: 0,02 %

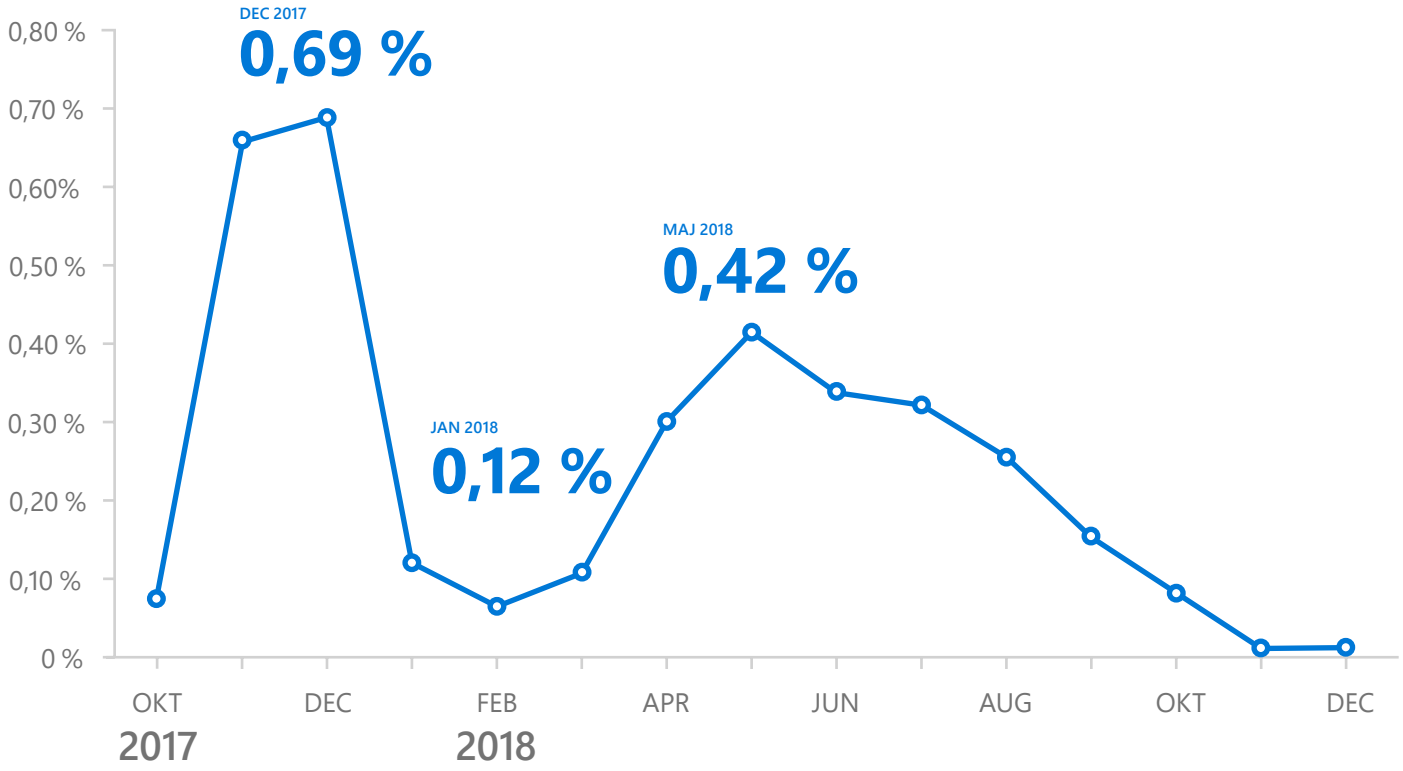
USA: 0,02 %

De fem steder, der havde det højeste antal hændelser med kryptovaluta-mining i 2018, var Etiopien (5,58), Tanzania (1,83), Pakistan (1,47), Kasakhstan (1,24) og Zambia (1,13). Hvert af disse lande havde et gennemsnitligt antal coin-mining-hændelser pr. måned på ca. 1,13 procent eller derover i perioden. Det steder, der havde det laveste antal coin-mining-hændelser i 2018, var Irland, Japan, USA og Kina, og hvert af disse lande havde et gennemsnitligt antal coin-mining-hændelser på ca. 0,02 procent i perioden.

BROWSERBASERET KRYPTOVALUTA-MININGSOFTWARE: EN NY FORM FOR TRUSSEL

De statistikker, der vises i dette afsnit, omfatter skadelig kryptovaluta-miningsoftware, der er beregnet til at blive installeret som malware på ofrenes computere. Nogle af de væsentligste kryptovaluta-miningtrusler befinder sig imidlertid i webbrowsere og skal slet ikke installeres. En række tjenester reklamerer med browserbaseret kryptovaluta-mining som en måde, hvorpå webstedsejere kan tjene penge på trafik på deres websteder uden at behøve at anvende annoncer. Webstedsejere skal tilføje JavaScript-kode på de af deres sider, der udvinder kryptovaluta i baggrunden, når en bruger besøger deres websted. Fortjenesten deles så mellem ejeren og tjenesten. Desværre har hackerne været hurtige til at udnytte disse tjenester til at udvinde kryptovaluta uden at indhente samtykke fra slutbrugerne,

Brocoiner-hændelseshyppighed



FIGUR 4.

Antal hændelser for Brocoiner, som er den mest udbredte browserbaserede kryptovaluta-miningsoftware

og dette sker ofte ved, at de kompromitterer lovlige websteder og indsætter miningkode i deres kildekode. Denne type browserbaserede miningsoftware kræver overhovedet ikke, at slutbrugerens computer kompromitteres, og den kan køre på en hvilken som helst platform med en JavaScript-kompatibel webbrowser. Ligesom trojanske heste, der udvinder kryptovaluta, kan browserbaseret miningsoftware forringe computerens ydeevne væsentligt og spilde elektricitet, når brugeren besøger en berørt webside.

PÅVIRKNINGEN MED UOPFORDRET KRYPTOVALUTA-MINING

Den mest oplagte trussel, som ofrene oplever fra skadelig kryptovaluta-mining, er forbruget af computerressourcer, som kan spilde elektricitet og forringe computerens ydeevne væsentligt. Brugere og organisationer står også over for andre risici i forbindelse med coin-mining, bl.a.:

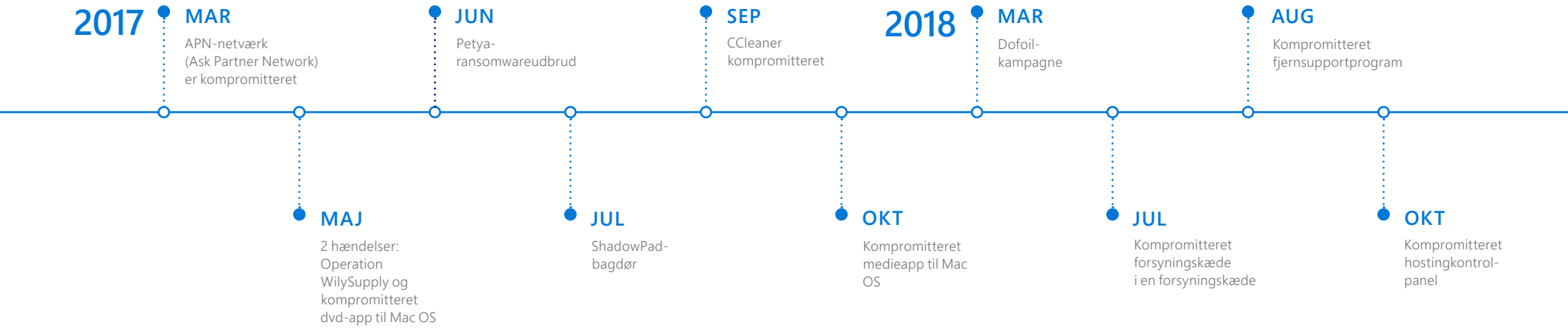
- **At de får foden indenfor så de kan gøre større skade i fremtiden.** Som andre former for malware kan kryptovaluta-mining være et indgangspunkt for hackere. Mens computeren udvinder kryptovaluta i baggrunden, kan cyberkriminelle få større viden om miljøet og muligvis afdække sikkerhedshuller, som de kan udnytte til andre formål.
- **Internetforbundne enheder kan kompromitteres og omdannes til bots til kryptovaluta-mining.** Mange af denne type enheder mangler indbygget sikkerhed som registrering af malwaretrusler, hvilket gør dem til oplagte mål for hackere.
- **Skader maskiner.** Kryptovaluta-miningsoftware, der kører konstant i månedsvis eller længere tid, kan påvirke ydeevnen og den varme, der genereres af overdrevent strømforbrug og CPU-udnyttelse, kan beskadige computere.

AFSNIT II

Software-forsyningskæder er i fare

I årevis har Microsoft overvåget trusselsaktører, der bruger kompromittering af forsyningskæden som et indgangspunkt til angreb. I et forsyningskædeangreb koncentrerer hackeren sig om at kompromittere udviklings- eller opdateringsprocessen for en legitim softwareudgiver.

Hvis det lykkes, kan hackeren inkorporere en kompromitteret komponent i en legitim applikation eller opdateringspakke, som derefter distribueres til brugerne af softwaren. Den skadelige kode kører derefter med den samme tillid og de samme tilladelser som softwaren. Det øgede antal angreb på softwareforsyningskæder i løbet af de seneste år er blevet et vigtigt emne i mange samtaler om cybersikkerhed, og det er den største bekymring i mange it-afdelinger.



FIGUR 5.

Angreb på softwareforsyningskæder i 2017 og 2018

STØRRE ANGREB PÅ SOFTWAREFORSYNINGSKÆDER I 2017

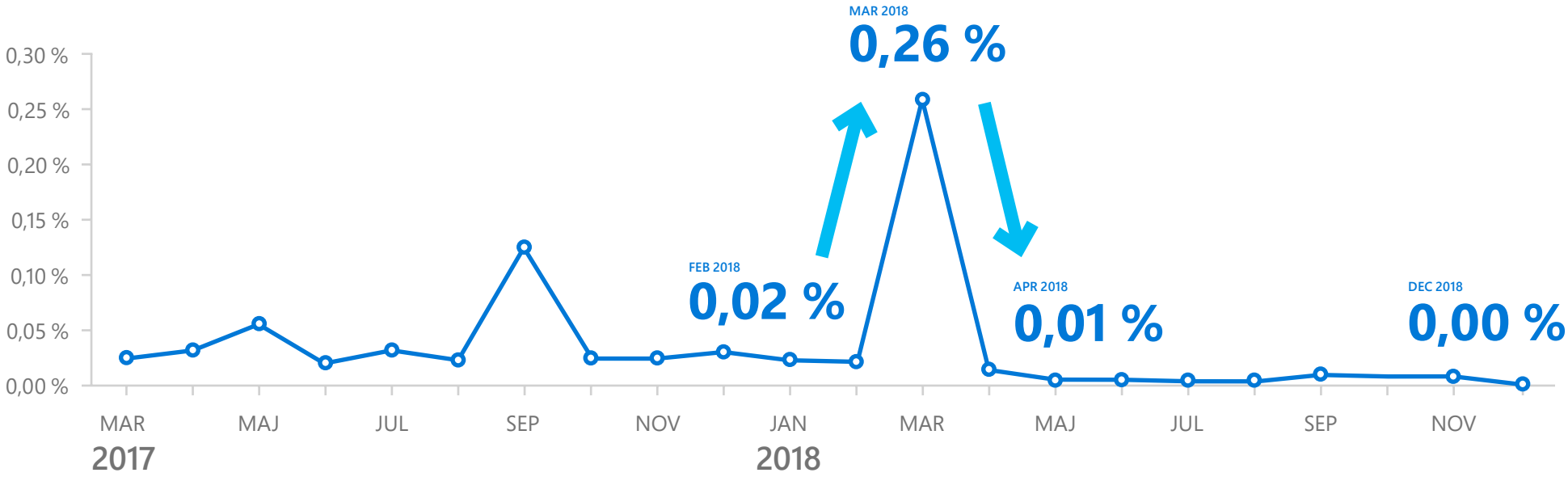
I 2017 var angreb på forsyningskæder ansvarlige for en række højprofilerede hændelser, og heraf var det mest markante Petya-ransomwareudbruddet i juni, som blev sporet til indledende infektioner fra en kompromitteret opdateringsproces for en populær skatteapplikation i Ukraine. I maj kompromitterede Operation WilySupply et tekstredigeringsprograms softwareopdatering, så den installerede en bagdør hos målorganisationer i finans- og it-sektoren. I juli blev en bagdør, der blev kaldt ShadowPad, skjult i en softwarepakke til serverstyring. Den gav hackerne mulighed for at installere yderligere malware-nyttedata til datatyveri og andre skadelige aktiviteter. I september blev infrastrukturen i det populære freewareværktøj CCleaner kompromitteret, og en bagdørsversion blev leveret til dens brugerbase.

Det første store angreb på softwareforsyningskæder i 2018 skete den 6. marts, da Windows Defender ATP blokerede en omfattende kampagne, der havde til formål at levere trojaneren Dofoil (også kaldet Smoke Loader). Den omfattende kampagne blev sporet til en uautoriseret peer-to-peer-applikation. Applikationens opdateringspakke blev erstattet med en skadelig pakke, der downloadede kompromitteret kode, som senere installerede Dofoil-malwaren. Den avancerede trojaner indeholdt coin-mining-nyttedata og udviste avancerede injektionsteknikker, vedholdenhedsmekanismer og undgåelsesmetoder i hele processen.

FIGUR 6.

Tendenserne for Dofoil-hændelser (Smoke Loader) i 2018 viser en stikning for blokerede hændelser i marts

Dofoil-hændelseshyppighed



I kampagnens første 12 timer blokerede Windows Defender Antivirus mere end 400.000 infektionsforsøg på verdensplan. Rusland stod for 73 procent af de globale hændelser, og derefter kom Tyrkiet med 18 procent og Ukraine med 4 procent.

Der blev registreret adskillige flere angreb, hvor kompromitterede softwareforsyningskæder blev anvendt som leveringsmekanismer, i 2018, bl.a. dem, der er beskrevet i følgende tabel:

FIGUR 7.

Andre angreb på softwareforsyningskæder i 2018

Periode	Angreb	Beskrivelse	Berørt software
Marts 2018	Dofoil-coin-mining-kampagne (rapporteret af Microsoft).	Hackere forgiftede opdateringsprocessen for en peer-to-peer-app for at installere Dofoil, som til gengæld installerede coin-mining-malware.	Peer-to-peer-app.
Juli 2018	Kompromitteret forsyningskæde i en forsyningskæde (rapporteret af Microsoft).	Hackere kompromitterede den delte infrastruktur mellem en leverandør af en PDF-redigeringsapp og en af dennes leverandørpartnere.	PDF-redigeringsapp og tredjepartspartnerleverandør.
August 2018	Kompromitteret fjernsupportprogram (Operation Red Signature rapporteret af Trend Micro og IssueMakersLab).	Opdateringen af en server hos en leverandør af fjernsupportløsninger blev kompromitteret til at levere et fjernadgangsværktøj ved navn 9002 RAT.	Fjernsupportprogram.
Oktober 2018	Kompromitteret hostingkontrolpanel-løsning (rapporteret af ESET).	Installationsscriptet til en hostingkontrolpanel-løsning blev ændret med henblik på at stjæle legitimationsoplysninger.	Hostingkontrolpanel-løsning.

TILLIDEN ER I FARE

Angreb på forsyningskæder er lumske, fordi de udnytter den tillid, som brugere og it-afdelinger har til den software, de bruger. Den kompromitterede software er ofte signeret og certificeret af leverandøren og tyder ikke på, at der er noget galt, hvilket gør det en del vanskeligere at opdage en infektion. De kan skade forholdet mellem forsyningskæder og deres kunder, uanset om kunderne er virksomhedsbrugere eller private brugere. Ved at forgifte software og underminere leverings- eller opdateringsinfrastrukturer kan forsyningskædeangreb påvirke integriteten og sikkerheden for de varer og tjenester, som organisationer udbyder.

Forsyningskædeangreb har påvirket en række forskellige organisationer i forskellige brancher og forskellige geografiske områder. Truslen om forsyningskædeangreb er et problem i hele branchen, der kræver mange interessenters opmærksomhed, bl.a. de softwareudviklere og leverandører, der skriver koden, de systemadministratorer, der administrerer softwareinstallationer, og de informationssikkerhedsmedarbejdere, der finder disse angreb og udvikler løsninger, der kan beskytte mennesker og software mod dem.

UD OVER SOFTWARE: ANGREB PÅ FORSYNINGSKÆDER VIA CLOUD-OBJEKTER

Forsyningskædeangrebs evne til at underminere tilliden forstærkes og bliver endnu mere kompleks i en cloud-løsning. Adskillige forekomster af kompromitterede cloud-objekter, -tjenester og -infrastruktur i 2018 understreger denne kompleksitet:

- Uautoriserede Chrome-udvidelser, der installerede kliksvindelmalware (rapporteret af ICEBRG)
- Forskellige kompromitterede Linux-lagre (rapporteret i nogle få onlineforummer)
- Skadelige WordPress-plug-ins anvendt til forskellige skadelige aktiviteter, herunder mulighed for, at hackere kunne udgive indhold på WordPress-websteder (rapporteret af Wordfence)
- Skadelige Docker-billeder, der indeholdt et script til at downloade malware til kryptovaluta-coin-mining og uploade til Docker Hub-konto (rapporteret af Fortinet og Kromtech)
- En skadelig typosquatting-pakke i det officielle Python-lager. Pakken indeholdt et skadeligt script, der downloader malware, der bruges til at overtage coin-mining-adresser i udklipsholderen (rapporteret på Medium)
- Kompromitteret script i StatCounter, der gav hackerne mulighed for at injicere et skadeligt script på websteder, der bruger StatCounter (rapporteret af ESET)
- Flere tilfælde af npm-bagdørsmoduler (npm-bloggen, Medium), som, hvis den blev udnyttet, kunne medføre situationer som f.eks., at en hacker ville kunne indtaste vilkårlig kode på en kørende server og eksekvere den.

Disse hændelser viser, hvordan forsyningskædeangreb kan udvide et angrebs overflade enormt. Hvis cloud-objekter ikke beskyttes, kan de være uventede indgangsvektorer. Docker Hub-hændelsen omfattede f.eks. en skadelig konto, der uploadede Docker-billeder, der indeholdt en skjult coin-mining-bagdør. Docker-billederne blev hostet på Docker Hub i næsten et år og blev downloadet millionvis af gange og brugt af intetanende administratorer og brugere.

Forsyningskæderisici omfatter kode i skyen, open source, webbiblioteker, containere og andre objekter i skyen. Disse risici kombineret med den store variation i de angreb på henholdsvis software- og hardwareforsyningskæder, der er kommet frem i lyset, gør forsyningskædeangreb til en bred kategori af trusler. Selvom der ikke findes en enkelt løsning til hele spektret af denne type angreb, er organisationerne nødt til at opbygge præventiv beskyttelse og registrering efter sikkerhedsbrud for forsyningskædeangreb fra kompromitterede hardware- og softwareudbydere, -leverandører, leverandører af open source-software samt leverandører af cloud-tjenester og -infrastruktur.

Undersøgelse af cyberangreb med DART

Microsoft Detection and Response Team (DART) er et globalt team bestående af cybersikkerhedseksperter og hændelsesrespons-enheder, der hjælper organisationer med at registrere, undersøge og reagere på angreb på cybersikkerheden. Dette afsnit omhandler nogle af de kundesager, som DART har behandlet i det seneste år. Almindelige tendenser hos hackere beskrives, samt hvordan Microsoft og kunderne var i stand til at forhindre angrebene.

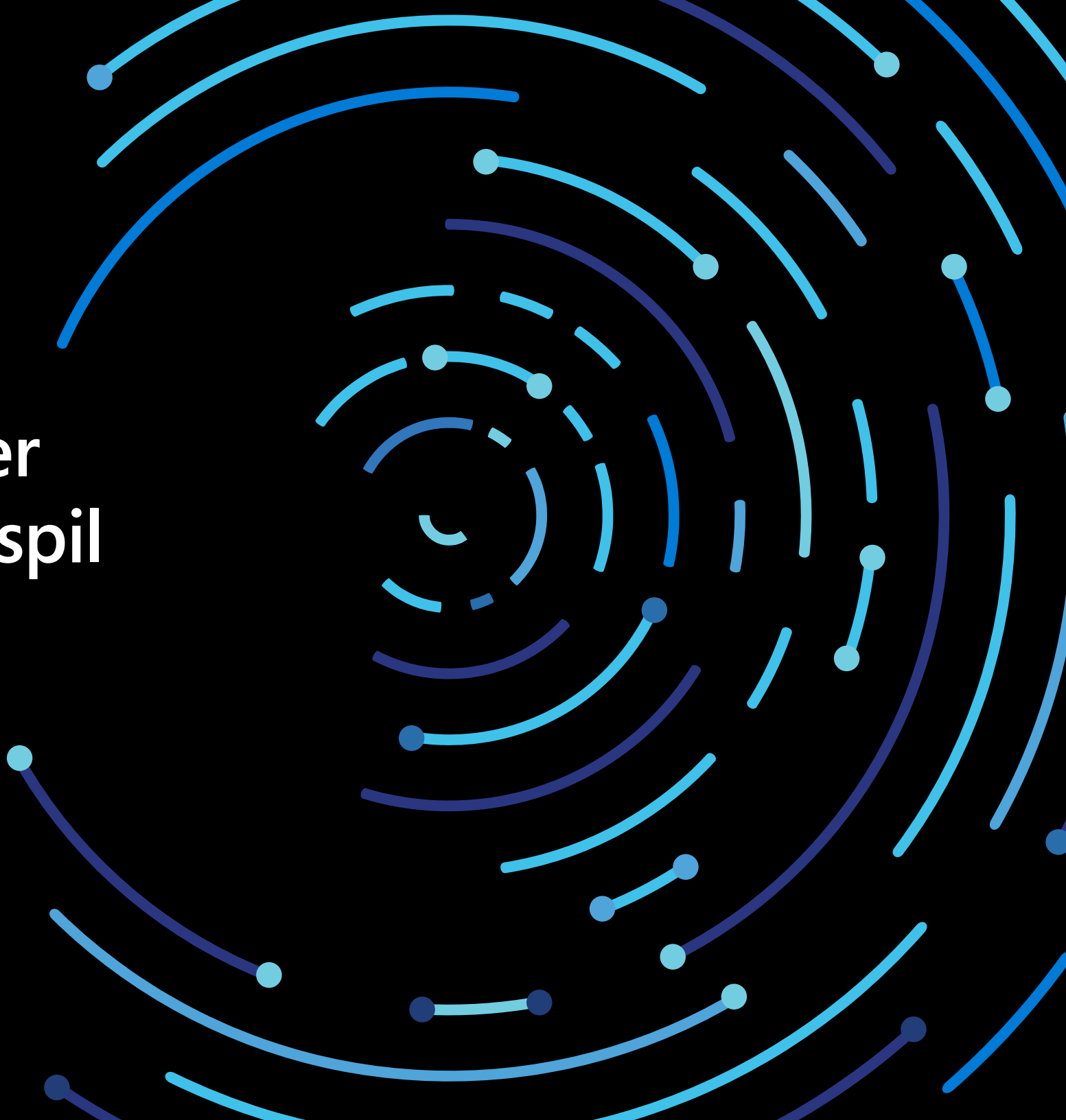
ORGANISATION, DER UDBYDER PROFESSIONELLE TJENESTER, OPLEVEDE NATIONALSTATANGREB, DER EKSFILTREREDE DATA

En organisation, der udbyder professionelle tjenester, blev ramt af en avanceret, statssponsoreret APT-trussel (avanceret vedvarende trussel), der fik adgang til privilegerede legitimationsoplysninger for organisationen. Hackerne fik adgang til netværket ved hjælp af et spredt adgangskodeangreb, hvor de brugte et lille antal svage eller hyppigt brugte adgangskoder (f.eks. "p@ssword" eller "123456") til at målrette mod et stort antal brugerkonti og få adgang til administrative loginoplysninger til Office 365. (Spredte adgangskodeangreb bruges til at undgå opdagelse ved at begrænse antallet af loginforsøg for hver konto). Efter infiltrering af netværket udførte APT'en udførlig, automatiseret eksfiltrering af data fra medarbejderes postkasser. På trods af flere interne forsøg på at komme af med modstanderen, forblev de i netværket i mere end 200 dage. Som en del af angrebet udnyttede hackeren organisationens forsyningskædesoftware og automatiserede eksfiltrering af data.

Organisationen havde en mistanke om, at der havde været et brud på sikkerheden for deres kundedata, og de hyrede DART-teamet til at undersøge det og forhindre yderligere skader. DART identificerede målrettede Office 365-postkassesøgninger, kompromitterede konti og hackerkommando- og kontrolkanaler. En vigtig erfaring, som kunden fik af denne hændelse, var at installere kontroller, der kan beskytte cloud-tjenester mod identitetsbaserede trusler og hackere. Organisationen indførte MFA-godkendelse (multifaktorgodkendelse), politikker med betinget adgang for visse cloud-apps og Office 365-logføring. For yderligere at beskytte sig mod lignende trusler i fremtiden kan organisationen også indføre en EDR-løsning (Endpoint Threat Detection and Response) for at opdage hackere, der forsøger at udnytte organisationens netværk. Desuden har vi anbefalet, at denne organisation udpeger en cloud-styringsinstans eller et globalt enhedsteam, der kan administrere og håndhæve passende politikker for brugergodkendelse, så organisationen har overblik over deres sikkerhedsforhold og mere effektivt kan begrænse risikoen.

AFSNIT III

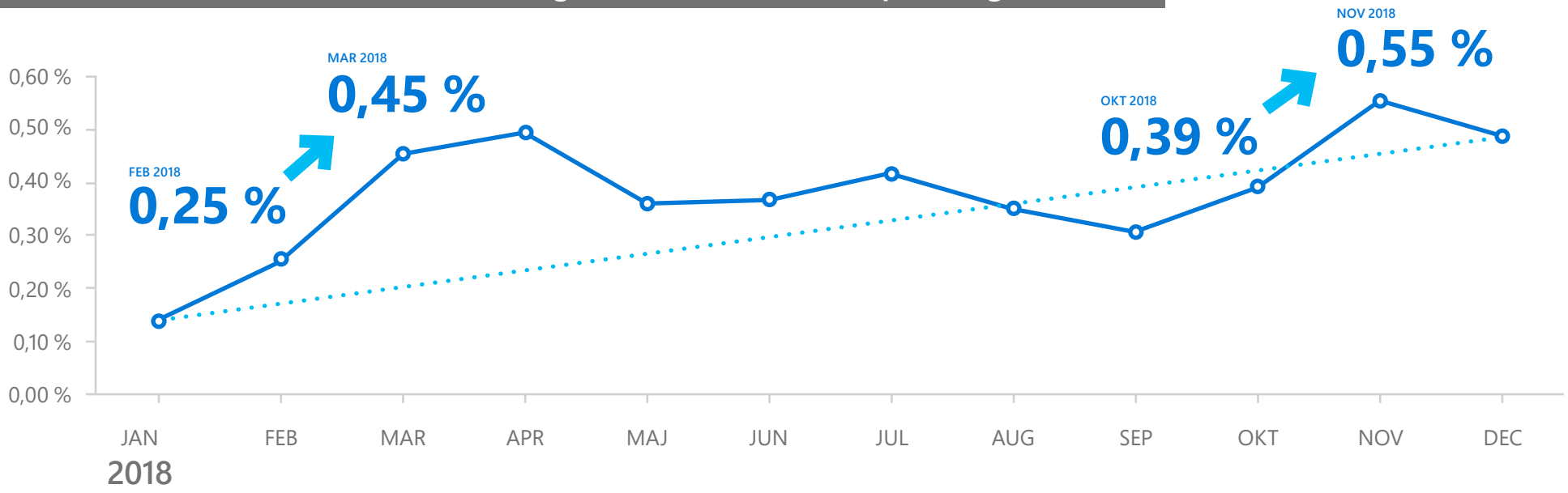
Phishing er stadig på spil



I 2018 har Microsoft-trusselsanalytikere set beviser på, at hackere fortsætter med at bruge phishing som en foretrukken angrebsmetode. Phishing ser ud til at vedblive med at være et problem et godt stykke tid fremover, fordi det omfatter menneskelige beslutninger og vurderinger over for cyberkriminelles vedholdende forsøg på at få ofre til at falde for deres fælder.

Phishing-antallet er stadig stigende

Procentdelen af det samlede antal indgående e-mails, der er phishing-e-mails



FIGUR 8.

Phishing-mails i 2018

PHISHING ER FORTSAT DEN FORETRUKNE ANGREBSBÆRER I 2018

Microsoft analyserer og scanner hver måned mere end 470 milliarder mails i Office 365 for phishing and malware, og det giver analytikerne et omfattende indblik i tendenser og teknikker for hackerne. Andelen af indgående e-mails, der var phishing-meddelelser, steg med 250 procent mellem januar og december 2018. Phishing er stadig en af de hyppigst anvendte angrebsbærere til at levere skadelige zero-day-nyttedata til brugere, og Microsoft har skærpet sikkerheden i forhold til disse angreb med ekstra anti-phishing-beskyttelses, -registrerings, -undersøgelses og -responsfunktioner for at beskytte brugerne.

Udviklingen inden for phishing-angrebsmetoder

Efterhånden som de værktøjer, der bruges til at beskytte brugerne mod phishing, bliver mere avancerede, bliver hackerne tvunget til at tilpasse sig. Phishing-angreb er blevet mere og mere polymorfe, hvilket betyder, at hackerne ikke bruger en enkelt URL, et enkelt domæne eller en enkelt IP-adresse til at sende mail, men anvender en varieret infrastruktur med flere angrebspunkter. Selve angrebene har også ændret karakter, og moderne phishing-kampagner spænder fra kortvarige angreb, der kun er aktive i få minutter, til længerevarende og mere omfattende kampagner. Andre er angreb med serielle varianter, hvor hackerne sender en lille mængde mail flere dage efter hinanden.

Derudover har Microsoft observeret en tendens til, at hackerne bruger hostet infrastruktur og anden public cloud-infrastruktur, hvilket gør det nemmere at undgå at blive opdaget, fordi man skjuler sig mellem legitime websteder og aktiver. Hackerne anvender f.eks. i stigende grad populære dokumentdelings- og samarbejdswebsteder og -tjenester til at distribuere skadelige nyttedata og falske loginformularer, der bruges til at stjæle brugernes legitimationsoplysninger. Der har også været en stigning i brugen af kompromitterede konti for yderligere at distribuere skadelige mails både i og uden for en organisation.

Phishing-kampagner varierer fra at være målrettede til at være bredt baserede

Som det er tilfældet med malwaredistribution generelt, varierer phishing-kampagner fra at være målrettede til at være bredt baserede, generiske angreb. Selvom yderst avancerede angreb giver større økonomisk gevinst pr. konto, der udsættes for phishing-angreb, giver mere generiske angreb færre penge pr. kompromitteret konto, men de er målrettet mod en bredere gruppe af brugere.

Et eksempel på en avanceret, målrettet kampagne er Ursnif, hvor hackerne fandt det dokumentfilnavn, der var specifikt for en velkendt organisation eller den branche, der var målet. Denne type angreb er helt anderledes end bredt baserede kampagner og virker umiddelbart mere legitim og troværdig.

Nogle af de bredt baserede kampagner i 2018 var relateret til BEC (Business Email Compromise) og efterligning af kendte brands, domæner eller brugere i målorganisationerne og avancerede spoofing-kampagner. Efterligning af domæner er en almindelig angrebsteknik, der bruges til at lokke organisationer til at tro, at mailen er troværdig og bør åbnes.

Phishing-fælder kommer i mange former

Microsofts forskere har erfaret, at mange forskellige typer phishing-fælder eller -nyttedata anvendes i kampagner, herunder:

- **Domæne-spoofing** (maildomænet svarer nøjagtigt til det oprindelige domænenavn)
- **Domæneefterligning** (maildomænet ligner det oprindelige domænenavn)[2]
- **Brugerefterligning** (mailen ser ud til at komme fra en person, du har tillid til)
- **Tekstfælder** (tekstmeddelelsen ser ud til at komme fra en legitim kilde, som f.eks. en bank, offentlig instans eller en anden virksomhed for at give deres påstande et legitimt skær og beder typisk ofret om at angive følsomme oplysninger som f.eks. brugernavne, adgangskoder eller følsomme økonomiske data)
- **Phishing-links til legitimationsoplysninger** (mailen indeholder et link til en side, der ligner en loginside til et legitimt websted, så brugerne indtaster deres legitimationsoplysninger)
- **Vedhæftede filer med phishing** (mailen indeholder en skadelig vedhæftet fil, som afsenderen lokker offeret til at åbne)
- **Links til falske cloud storage-placeringer** (mailen ser ud til at komme fra en legitim kilde og lokker brugeren til at give tilladelse og/eller angive personlige oplysninger som f.eks. legitimationsoplysninger for at få adgang til en falsk cloud storage-placering)

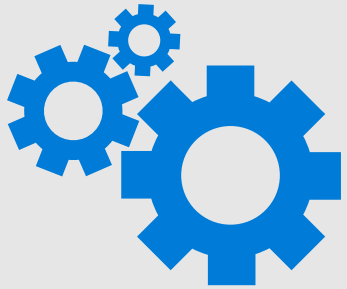
Denne type fælder, som potentielt kan blive installeret af hackere, øger kompleksiteten af de phishing-trusler, som organisationer må slås med.

FODNOTER

[2] Domæneefterligning kan minde om domæne-spoofing (nøjagtigt match med det oprindelige domænenavn) i den usædvanlige situation, hvor domænet vises i mailvisningsnavnet.

Undersøgelse af cyberangreb med DART

STOR PRODUKTIONSORGANISATION RAMT AT MÅLRETTEDE PHISHING-ANGREB



En produktionsorganisation oplevede en phishing-kampagne i flere faser, der foregik over nogle måneder. Denne fremgangsmåde er ikke usædvanlig. I løbet af den første fase vil hackeren udføre rekognoscering, og i den anden fase vil angribe aktiver med høj værdi. Den første fase af denne kampagne udnyttede en velkendt form for phishing-svindel, der var baseret på et websidelink, som var indlejret i en e-mail, der blev sendt til en lille udvalgt gruppe i organisationen. E-mailen påstod, at modtageren havde et vigtigt elektronisk dokument, der skulle gennemgås, og alt, hvad modtageren behøvede at gøre, var at godkende med deres domænelegitimationsoplysninger for at få adgang. Denne falske landingsside, som var oprettet for, at modtageren kunne gennemse det såkaldt "vigtige dokument", høstede faktisk legitimationsoplysningerne og gav hackeren adgang til Office 365-konti fra hele verden. Den anden fase af phishing-kampagnen var beregnet til at sende lignende phishing-mails til aktiver med høj værdi i den produktionsorganisation, der var målet for svindlen, i håbet om at få adgang til flere værdifulde data. Microsoft samarbejdede med denne klient i løbet af den anden fase af phishing-kampagnen. Det vigtigste, kunden lærte af denne hændelse, var følgende: phishing er stadig en af de mest effektive angrebsmetoder, og brugerne er stadig det svageste link. At uddanne brugerne til at være på vagt over for phishing-svindel, at have værktøjer, der kan identificere hackere og reagere på dem samt at udføre programrettelser i systemet regelmæssigt er alle sammen vigtige elementer. Hvis organisationen ikke gør noget af dette, kan den være sårbar.

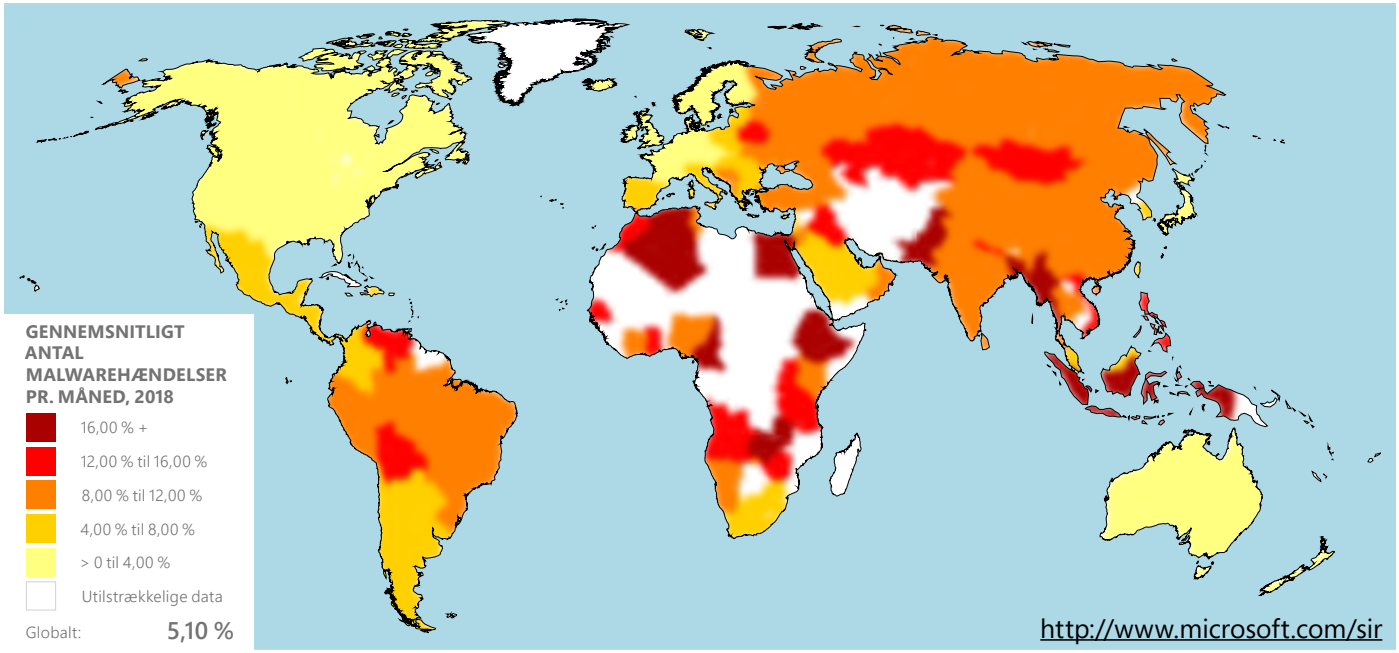
I dette tilfælde var kundens væsentligste bekymring et øjeblikkeligt behov for at blokere adgangen til de kompromitterede konti. I samarbejde med Azure Identity- og Office 365-teams udarbejdede DART en plan for at fjerne hackeren fra netværket og overvåge al trafik til kommando- og kontrolkanalen ved at bruge den nyligt installerede Microsoft Azure Log Analytics-løsning. Teamet var i stand til at hjælpe med at løse problemet på blot tre timer. Hackerens adgang blev blokeret, og organisationen kunne vende opmærksomheden mod vurdering af skaderne og genoprettelse. DART brugte Azure Log Analytics-værktøjerne til at holde øje med hackerens adfærd, og det var en hjælp til afdække mange af organisationens konfigurationsudfordringer. DART identificerede f.eks. huller i programrettelserne på kritiske servere, opdagede computere på netværket, der kommunikerede med kendte dårlige værter på internettet, og de fandt desuden adskillige vigtige servere uden malwarebeskyttelse.

AFSNIT IV

Malware rundt omkring i verden

Malware udgør risici for organisationer og enkeltpersoner i form af forringet brugbarhed, datatab, tyveri af immaterielle rettigheder, økonomiske tab og bekymringer – og det kan endda sætte menneskers liv på spil. Microsoft anvender et bredt udvalg af værktøjer og teknikker til at identificere, blokere og fjerne malwareinfektioner, uanset hvor de findes.

Antallet af malwarehændelser lå i niveauet fra omkring 5 procent til over 7 procent i 2017. I begyndelsen af 2018 var tallet steget, men faldt så igen til lige over 4 procent det meste af året. Nogle mulige årsager til det samlede fald i antallet af malwarehændelser i 2018 er den stigende indførelse af Windows 10 og den øgede brug af Windows Defender til beskyttelse. Antallet af hændelser er den procentdel af computere, der kører Windows Defender Antivirus. som rapporterede om malware i løbet af måneden, herunder inficeringsforsøg, som Defender blokerede.



FIGUR 9.

Gennemsnitligt antal månedlige malwarehændelser på verdensplan efter land/region i 2018

De fem steder, der havde det højeste antal malwarehændelser i perioden fra januar til december 2018, var Etiopien (gennemsnitligt antal hændelser pr. måned på 26,33), Pakistan (18,94), Palæstinensiske territorier (17,50), Bangladesh (16,95) og Indonesien (16,59), som alle havde et gennemsnitligt antal hændelser pr. måned på ca. 16,59 procent eller derover i perioden. Infektionstallene har en tendens til at hænge nøje sammen med menneskelige udviklingsfaktorer og teknologisk parathed i et samfund. Alle steder med det højeste antal hændelser i 2018 lå blandt de nederste 40 procent af lande og regioner i ICT-indekset (Information and Communications Technologies) for 2017, som er udgivet af FN's Internationale Telekommunikations Union (ITU).

De fem steder med det laveste antal malwarehændelser i den samme periode var Irland (1,26), Japan (1,51), Finland (1,74), Norge (1,79) og Holland (1,82), som alle havde et gennemsnitligt antal hændelser pr. måned på 1,82 procent eller derunder i perioden. Disse steder har en tendens til at have en fuldt udviklet infrastruktur og veletablerede programmer til beskyttelse af kritisk infrastruktur og kommunikation med deres borgere om grundlæggende sikkerhed.

GENNEMSNITLIGT ANTAL HÆNDELSER PR. MÅNED FOR LANDE, DER ER MEST PÅVIRKEDE AF MALWARE

Etiopien: **26,33 %**

Pakistan: **18,94 %**

Palæstinensiske territorier: **17,50 %**

Undersøgelse af cyberangreb med DART

FLERE FINANSIELLE ORGANISATIONER OPLEVEDE NATIONALSTATANGREB, DER FORSTYRREDE DRIFTEN

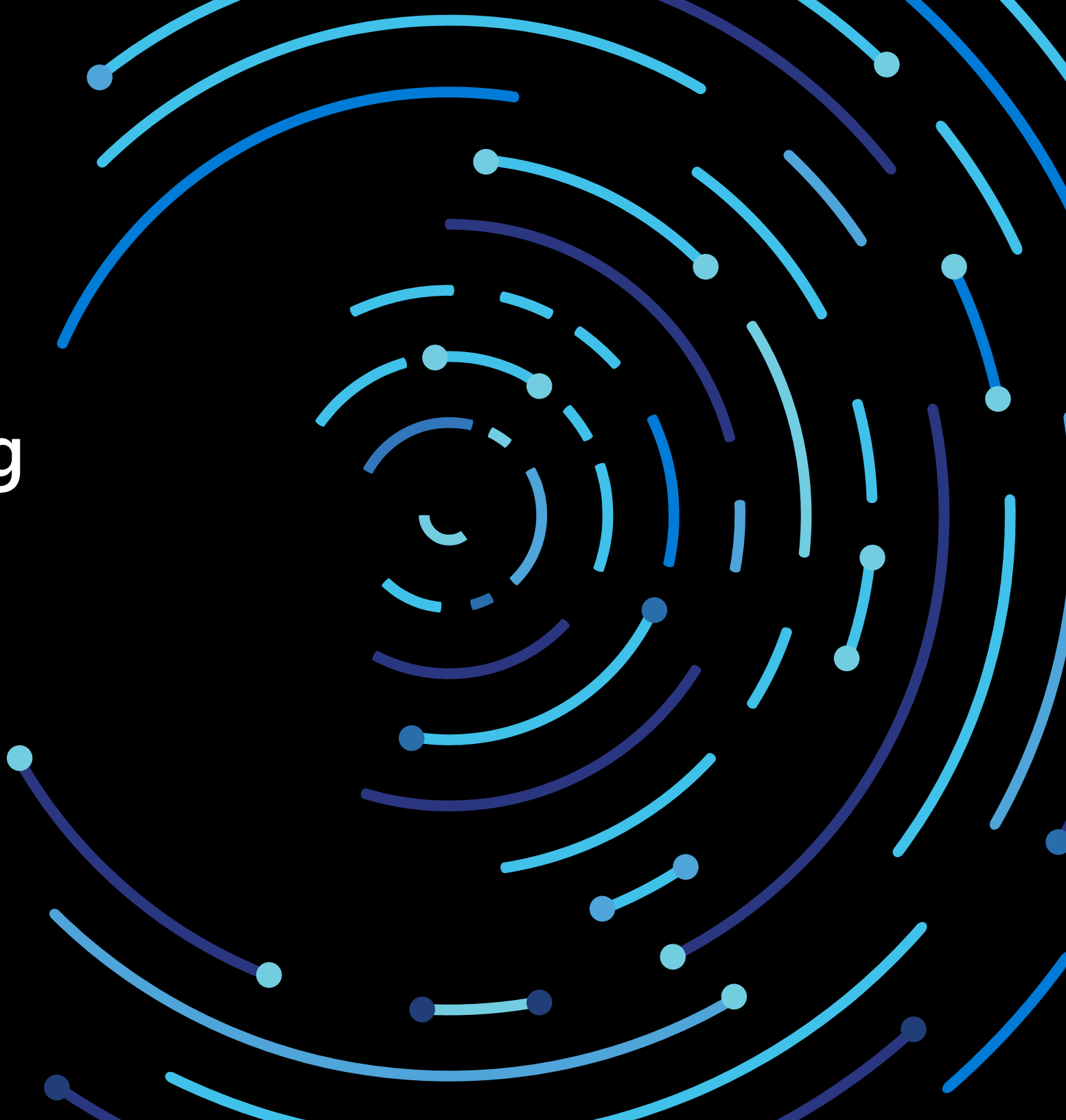
I en af de mest destruktive hændelser, DART har oplevet, blev flere finansielle organisationer ramt af en statssponsoreret APT (en anden gruppe end den, der var målrettet mod den organisation, der udbyder professionelle tjenester, som blev omtalt tidligere), der fungerede på samme måde.

Denne APT fik administratoradgang efter at have inficeret en patient zero-maskine med et yderst målrettet, skjult bagdørsimplantat, der formentlig blev leveret via en spear phishing-mail. Derefter udførte APT'en flere svigagtige transaktioner og overførte store kontantbeløb til udenlandske bankkonti. I nogle tilfælde forblev hackeren uopdaget i mere end 100 dage.
Da hackeren fandt ud af, at han eller hun var blevet opdaget, udførte hackeren hurtigt et planlagt angreb, der leverede destruktiv malware til mere end halvdelen af systemerne i miljøet. Disse kunders drift blev afbrudt i flere dage.

Disse hændelser mundede ud i nogle erfaringer for kunderne. Den første var, at livscyklusadministration af software er særlig vigtigt, og det indebærer at sørge for, at systemerne opdateres (operativsystemer og sikkerhed), programrettes og revideres regelmæssigt.
I et tilfælde var en organisations Linux-systemmiljø, som et virkelig stort antal workloads kørte på, fuldkommen ikke-administreret, hvilket betød, at det var ekstremt sårbart over for angreb. Den anden erfaring var, at det er vigtigt at bevare sikkerhedskopier af systemdata på en offline-placering i tilfælde af, at de primære data går tabt. En anden erfaring var, at traditionelle antivirusløsninger muligvis ikke er tilstrækkelige, hvis man har brug for at kende til skadelig aktivitet.

For disse organisationer var den højeste prioritet at vende tilbage til normal driftstilstand. DART hjalp med at gendanne tjenester ved først at undersøge indvirkningen og derefter udføre de nødvendige afhjælpningshandlinger, som f.eks. at fjerne malware fra de påvirkede systemer og genoprette dem til en sund tilstand. Teamet uddannede desuden kunderne i, hvordan de kan bruge Microsofts værktøjer til trusselsundersøgelse, f.eks. EDR og andre, så de kan holde øje med unormal adfærd hackeraktivitet i deres netværk. DART understregede, at endpoint-overvågning er afgørende for at forsvare sig mod avancerede, målrettede angreb, der muligvis ikke opdages af traditionelle antivirusløsninger.

Vejledning



Vejledning

Opbygning af organisatorisk modstandsdygtighed og meningsfuld risikoreduktion kræver en sikkerhedstilgang, der omfatter forebyggelse samt opdagelse og respons. Vi har arrangeret følgende foreslåede bedste fremgangsmåder og kontroller for sikkerhed i disse kategorier.

FOREBYGGELSE:

Forebyggende kontroller spiller en vigtig rolle i den overordnede forsvarsstrategi, da de rigtige investeringer kan øge omkostningerne for angreb for cyberkriminelle og bevare disse øgede omkostninger for angreb over tid (uden at det kræver, at en ekspertanalytiker overvåger og fortolker resultatet). Investeringer i forebyggende kontrol bør målrettes mod teknikker med de laveste omkostninger, så man konstant fjerner billige og effektive angrebsteknikker.

Man bør overveje følgende fire ting i forbindelse med forebyggelse:

1. **Sikkerhedshygiejne er afgørende. Som det ses af nogle af de cyberhændelser, der er beskrevet i denne rapport, kan almindelige sikkerhedshygiejneproblemer underminere avancerede sikkerhedsfunktioner, så følgende tips kan medvirke til at mindske risikoen:**

- Undgå at bruge ukendt gratis og/eller piratkopieret software. Brug kun software fra pålidelige kilder.

- Sørg for at mindske risikoen for tyveri af legitimationsoplysninger, herunder beskyttelse af privilegerede administratorkonti. Du kan lære, hvordan dette gøres, ved at læse denne blog, der indeholder beskrivelse af nogle principper og værktøjer, som Microsoft har brugt til at vejlede og forbedre vores eget sikkerhedsforsvar, og nogle foreskrevne køreplaner, der kan hjælpe dig med at planlægge dine egne initiativer.

- Anvend sikre udgangspunkter for konfiguration, der leveres af dine softwareleverandører.

- Hold maskinerne opdaterede ved at hurtigt at installere de nyeste opdateringer af operativsystemer og applikationer, og installér straks kritiske sikkerhedsopdateringer til operativsystem, browsere og mail. Isoler (eller fjern) maskiner, som der ikke kan opdateres eller udføres programrettelser på.

- Implementer avanceret mail- og browserbeskyttelse. Installér en sikker mailgateway, der har avancerede funktioner til trusselsbeskyttelse, for at forsvare dig mod moderne phishing-varianter.

- Aktivér host-antimalware og netværksforsvar for at få blokeringsrespons i næsten realtid fra cloud-løsningen (hvis det er tilgængeligt i din løsning).

2. **Implementer adgangskontroller. Overvej følgende:**

   - Anvend princippet om færrest mulige rettigheder, som indebærer implementering af netværkssegmentering, fjernelse af lokale administratorrettigheder fra slutbrugere og forsigtighed ved tildeling af rettigheder til alle applikationer, der kører på computeren.
   - Begræns download af applikationer, så der kun kan downloades fra pålidelige kilder (en officiel appbutik).
   - Indfør stærke politikker for kodeintegritet, herunder begrænsning af de applikationer, som brugere kan køre. Indfør om muligt en sikkerhedsløsning, der begrænser den kode, der kører i systemets kerne, og kan blokere ikke-signerede scripts og andre former for upålidelig kode. Brug whitelisting af applikationer.
   - Læs denne blog fra Microsofts forskere for at få mere at vide om angreb på softwareforsyningskæder og om, hvordan du kan beskytte dig mod dem.

3. **Behold sikkerhedskopier.**

   - Opret sikkerhedskopier, der ikke kan destrueres, af dine kritiske systemer og data.
   - Brug cloud storage-tjenester til automatisk sikkerhedskopiering af data online. For data, der opbevares on-premises, skal du regelmæssigt sikkerhedskopiere vigtige data ved hjælp af 3-2-1-reglen. Opbevar tre sikkerhedskopier af dine data på to forskellige storage-typer og mindst én sikkerhedskopi på en ekstern placering.

4. **Vær opmærksom, og reager, hvis du har mistanke om problemer.**

   - Lær medarbejderne at være opmærksomme på mistænkelig kommunikation, der kræver afgivelse af følsomme oplysninger, og instruer dem i, hvordan de skal reagere og indrapportere denne type kommunikation til organisationens sikkerhedsteam øjeblikkeligt. Uddannelse kan også medvirke til at forhindre social engineering- og spear phishing-angreb.
   - Vær forsigtig, når du klikker på weblinks. Hvis man øver sikre webbrowsingvaner og bruger løsninger, der sender advarsler om eller blokerer adgang til usikre websteder, kan det mindske sandsynligheden for at man støder på websteder, der har relation til kryptovaluta-mining.
   - Hvis en computer kører usædvanligt langsomt, skal du lede efter mistænkelige filer, der kører, og du er velkommen til at sende et eksempel til leverandøren af operativsystemet. Du kan sende filer til Microsoft med henblik på malwareanalyse på https://www.microsoft.com/wdsi/filesubmission.

REGISTRERING OG RESPONS:

Registrering og respons bidrager til modstandsdygtighed ved at begrænse det tidsrum, hvor hackeren har adgang til dine ressourcer. Det mindsker hackerens investeringsafkast ved både at øge hackerens omkostninger (hackeren er nødt til at forsøge igen og ændre sine aktiviteter) og mindske udbyttet (begrænser sandsynligheden for, at hackeren når sit mål).

Den cloud-teknologi, der giver virksomhedsorganisationer mulighed for at imødekomme markedets behov bedre, kan også hjælpe sikkerhedsafdelinger med bedre at bekæmpe hackere.

FIGUR 10.

Udviklingen af SOC'er

Når vi ser på udviklingsbanen for SOC'er (Security Operations Centers), ser vi, at teknologi konstant øger hastigheden og kvaliteten i forhold til SOC-beslutninger og -handlinger. Mange af disse nyskabelser kan knyttes til hver fase af den cyklus med "Observer, Beslut, Orienter og Reager", der er dokumenteret af USAF-oberst John Boyd.[3]

OBSERVER – SOC'er kan udnytte den enorme mængde efterretningsoplysninger, der er tilgængelige (fra Microsoft og andre kilder), hvilket øger deres synsfelt dramatisk både i selve organisationen og det eksterne miljø.

ORIENTER DIG – efterhånden som disse nye datakilder bliver tilgængelige for allerede overbelastede SOC'er, bliver machine learning (en undergruppe af kunstig intelligens) et vigtigt værktøj til at ræsonnere over disse massive datasæt og identificere anomalier, der er værd at undersøge. Sikkerhedsleverandører (herunder Microsoft) har indført maskinlæringsteknologi for hurtigt at kunne prioritere hændelser (og hjælpe med at samle disse individuelle hændelser til holistiske hændelser).

– angrebenes mængde og kompleksitet kan hurtigt overbelaste en SOC, og derfor er analytikere og hændelsesrespons-enheder nødt til at træffe beslutninger og reagere hurtigt på advarsler og opdagelser. Microsoft og andre leverandører har integreret automatiske undersøgelsesfunktioner samt vejledning, der kan hjælpe analytikere med hurtigt at træffe gode beslutninger (f.eks. for at isolere potentielt inficerede eller kompromitterede enheder). I øjeblikket har automatiseringen fokuseret på hurtig løsning af hændelser med lav prioritet, så specialiserede færdigheder kan anvendes på mere komplekse problemer.

REAGER – reaktioner kræver hurtig og præcis udførelse på tværs af mange teknologier og platforme, og det er det, som automatiseringsteknologier til sikkerhedsorkestrering og respons muliggør. Microsoft og mange andre investerer fortsat i disse teknologier, herunder moderne løsninger til trusselsregistrering og automatisk reaktion.

FODNOTER

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

Andre tendenser, som gælder for en moderne SOC, er:

- **Kvalitet frem for kvantitet af advarselsfeeds** – efterhånden som organisationer går fra at administrere "ikke nok data" til at administrere "for mange data", bliver højt specialiserede SOC-analytikeres tid og opmærksomhed mere og mere værdifuld. Dette skaber et øget behov for kvalitet i de advarsler, der kræver handling fra niveau 1- og niveau 2-analytikere. Yderligere datafeeds er altid nyttige i forbindelse med undersøgelser og proaktiv jagt, men Microsofts virksomheds-it-SOC måler det faktiske positive antal advarselsfeeds, der kræver reaktion fra en analytiker (og det kræver i øjeblikket et ægte positivt antal på 90 % eller derover).

- Datatyngde – det er vanskeligt at analysere store datasæt (inklusive sikkerhedsdata) uden at have adgang til de underliggende rå data. Efterhånden som flere sikkerhedsdata bliver tilgængelige, bliver det mere økonomisk og praktisk muligt at foretage sikkerhedsanalyserne i cloud-løsningen i forhold til at hente disse data tilbage til et on-premises-system. Dette vil højst sandsynligt føre til udvikling af SIEM- og SOC-arkitekturer, der kan omfatte hybride SIEM-metoder eller indførelse af indbygget cloud-SIEM som en tjeneste.

- **Høj kontekst** – denne type registreringer er meget mere anvendelige på grund af deres evne til at sammenholde datasæt mere effektivt. Traditionelle registreringer baseret på netværkstrafik giver stadig en vis sikkerhedsværdi, men rå netværkstrafik mangler typisk kontekst, der gør det muligt at skelne mellem legitim aktivitet og unormal aktivitet. Vi oplever, at SOC'er får langt mere værdi ud af kontekstrige registreringer som:

  - **EDR-løsninger (Endpoint Detection and Response)**, der har omfattende kontekst om host-aktiviteten
  - Identitetsbaserede registreringer, der omfatter oplysninger om normale brugergodkendelsesmønstre (placeringer, tidspunkter, tjenester, der er opnået adgang til osv.), og anvender adfærdsanalyser

Disse kontekstrige registreringer er vanskeligere at undgå for modstandere, fordi de er nødt til at efterligne en langt mere kompleks funktion (i forhold til nogle få tekniske attributter for IP-trafik).

Noget andet, vi har lært af store brud på sikkerheden hos kunder, er, at det er vanskeligt at reagere hurtigt på hændelser, når it-funktionerne er helt eller delvist udliciterede. Vi anbefaler, at I gennemgår jeres it-udliciteringskontrakter og SLA'er (serviceniveauaftaler) samt jeres forsyningskædeleverandører for at sikre, at de er kompatible med hurtig reaktion på sikkerhedsproblemer. Du kan finde flere oplysninger om, hvad vi har lært af undersøgelser hos vores kunder, i referencevejledningen om hændelsessvar (IRRG) på https://aka.ms/IRRG.

Datakilder

Datakilder

Microsoft har indsamlet de data, der er inkluderet i Microsoft Security Intelligence-rapporten, under leveringen af en lang række Microsoft-produkter og -tjenester som beskrevet i Microsofts erklæring om beskyttelse af personlige oplysninger. Disse data giver os værdifulde oplysninger om sikkerheden og driften for vores produkter og tjenester samt et indblik i det generelle landskab for cybersikkerhedstrusler. Disse data omfatter analyser fra følgende kilder:[4]

- **Azure Security Center** er en tjeneste, der hjælper organisationer med at forhindre, opdage og reagere på trusler ved at skabe øget indblik i sikkerheden for cloud-workloads og bruge advanced analytics og trusselsefterretninger til at opdage angreb.

- **Bing** er det søge- og beslutningsprogram, der foretager milliarder af websidescanninger pr. år for at finde skadeligt indhold. Når denne type indhold registreres, viser Bing advarsler til brugerne for hjælpe med at forhindre infektion.

- **Exchange Online** er den Microsoft-hostede mail- og produktivitetstjeneste. Exchange Online-antimalware- og -antispamtjenester scanner milliarder af meddelelser hvert år for at identificere og blokere spam og malware.

- **Malicious Software Removal Tool** (MSRT) er et værktøj uden omkostninger, som Microsoft har udviklet til at hjælpe med at identificere og fjerne specifikke udbredte malwarefamilier fra kundecomputere. MSRT udgives primært som en vigtig opdatering via Windows Update, Microsoft Update og Automatiske opdateringer. En version af værktøjet er også tilgængelig via Microsoft Download Center. MSRT er ikke en erstatning for en opdateret antivirusløsning i realtid.

- **Microsoft Sikkerhedsscanner** er et sikkerhedsværktøj, der kan downloades uden omkostninger, og som leverer scanning efter behov og hjælper med at fjerne malware og anden skadelig software. Microsoft Sikkerhedsscanner er ikke en erstatning for en opdateret antivirusløsning i realtid, da den ikke tilbyder beskyttelse i realtid og ikke kan forhindre, at en computer inficeres.

FODNOTER

[4]Det er vigtigt at vide, at disse data altid går gennem strenge grænser for databeskyttelse og overholdelse af standarder, inden de bruges til sikkerhedsformål.

- **Microsoft Vigtige sikkerhedsindstillinger** er et produkt til beskyttelse i realtid, der nemt kan downloades uden omkostninger. Det giver grundlæggende og effektiv antivirus- og antispywarebeskyttelse til Windows Vista og Windows 7.

- **Microsoft System Center Endpoint Protection** (tidligere Forefront Client Security og Forefront Endpoint Protection) er et samlet produkt, der giver beskyttelse mod malware og uønsket software til virksomhedscomputere, bærbare computere og serveroperativsystemer. Det bruger Microsoft Malware Protection Engine og Microsoft-antivirussignaturdatabasen til at levere realtids-, planlagt og on-demand-beskyttelse.

- **Office 365** er Microsoft Office-abonnementstjenesten til organisationer og private brugere. Udvalgte abonnementsplaner indeholder adgang til Office 365 Advanced Threat Protection.

- **Windows Security** i Windows 10 leverer realtidsscanning og -fjernelse af malware og uønsket software. Derudover udnytter den nyeste version af Windows omfattende kontekstafhængige data som f.eks. maskinkonfiguration, enhedens ydeevne og status samt andre lignende oplysninger for at forbedre sikkerheden for kunderne. Samtidig giver vi kunderne mulighed for at blive mere informerede om beskyttelsen af deres personlige oplysninger i Windows 10. Læs denne blog for at få mere at vide om nogle af de måder, Microsoft gør dette på.

- **Windows Defender Advanced Threat Protection** er en tjeneste, der er indbygget i Jubilæumsopdatering til Windows 10 og nyere versioner. Denne tjeneste giver virksomhedskunder mulighed for at registrere, undersøge og afhjælpe vedvarende avancerede trusler og brud på datasikkerheden i deres netværk.

- **Windows Defender Offline** er et værktøj, der kan downloades og bruges til at oprette en cd, dvd eller et USB-flashdrev, der kan startes fra, for at scanne en computer for malware og andre trusler. Det yder ikke beskyttelse i realtid og er ikke en erstatning for en opdateret antimalwareløsning.

- **Windows Defender SmartScreen**, som er en funktion i Microsoft Edge og Internet Explorer, tilbyder brugerne beskyttelse mod phishing-websteder og websteder, der hoster malware. Microsoft vedligeholder en database over phishing-og malwarewebsteder, der rapporteres af brugere af Microsoft Edge, Internet Explorer og andre Microsoft-produkter og-tjenester. Når en bruger forsøger at besøge et websted i databasen med filtere t aktiveret, viser browseren en advarsel og blokerer navigation til siden.