Microsoft

MICROSOFT SECURITY INTELLIGENCE REPORT

ÅRGÅNG 24
JANUARI–DECEMBER 2018

Innehållsförteckning

Det här dokumentet är endast avsett att informera. MICROSOFT LÄMNAR INGA GARANTIER I FRÅGA OM INFORMATIONEN I DET HÄR DOKUMENTET, VARE SIG UTTRYCKLIGA, UNDERFÖRSTÅDDA ELLER LAGSTADGADE.

Det här dokumentet tillhandahålls i befintligt skick. Information och åsikter som uttrycks i detta dokument, inklusive webbadresser och andra hänvisningar till webbplatser, kan ändras utan föregående meddelande. Risken för att använda det åvilar dig.

Namnen på faktiska företag och produkter som nämns kan vara varumärken som tillhör respektive ägare.

Författare och bidragsgivare

Abhishek Agrawal
Informationsskydd

David Fantham
Informationsskydd

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
Reaktioner på säkerhetsincidenter

Matt Duncan
Windows Active Defense Data Engineering and Analytic

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

Förord

Hej och välkommen till den 24:e årgången av Microsoft Security Intelligence Report (SIR). Som säkerhetsarkitekt och utövare läser jag rapporter som denna i hopp om att förstå landskapet lite bättre och inhämta praktiska råd om hur man använder denna kunskap för att försvara och skydda organisationer mer effektivt.

SIR-teamet agerar lärare för att frammana bättre motståndskraft i denna rapport, och de har gått igenom ett års data för att ta fram de viktigaste lärdomarna.

Det du läser är insikter som hämtats från ett års analyser av säkerhetsdata och praktiska lärdomar. De data som analyseras omfattar 6,5 biljoner hotsignaler som passerar Microsofts moln varje dag samt forskning och praktiska erfarenheter som våra tusentals säkerhetsforskare och utryckningspersonal runt om i världen har rönt. Under 2018 använde angriparna en mängd fula trick i både ny (myntbrytning) och gammal (nätfiske) form i sin ständiga strävan att stjäla data och resurser från kunder och organisationer. Hybridangrepp som Ursnif-kampanjen blandade sociala och tekniska metoder. Efterhand som försvararna blev bättre på att hantera utpressningstrojaner – en synlig och störande form av angrepp – gick brottslingarna över till de mer osynliga men ändå lukrativa myntbrytarna.

Den omsvängningen kan kännas frustrerande, som om angriparna alltid ligger ett steg före. Men sedd från en annan vinkel är berättelsen positiv. Försvarare och cybersäkerhetsproffs som du har infört försvarstekniker som tvingat angriparna att ändra de nyttolaster de föredrar och överge utpressningstrojaner.

Ett annat område där cyberbrottslingar ökade sin verksamhet är försörjningskedjan. En av de mest anmärkningsvärda var myntbrytarutbrottet Dofoil, som skedde 6 mars 2018 och startades av en förgiftad peer-to-peer-app. Oron kring försörjningskedjan gick bortom appar och vidare till molnet och inkluderade skadliga webbläsartillägg, komprometterade Linux-lagringsplatser, och flera fall av moduler med bakdörrar. För att bemöta detta hot försöker organisationerna använda en öppen och betrodd modell för försörjningskedjan.

Data är bra, men ibland hjälper det att ta reda på vad som verkligen hände i en organisation. Det är därför vi har inkluderat lärdomar från fältet i vårt Detection and Response Team (DART). Dessa inkluderar historier om hur ett stort tillverkningsföretag lyckades införa kontroller för att blockera en nätfiskekampanj i flera faser som hade plågat dem i många månader, samt hur organisationer inom den finansiella tjänstesektorn slutligen lyckades klämma åt hotaktörerna i sina system med hjälp av avancerade utredningsverktyg och övervakning av slutpunkter.

Sist men inte minst fortsatte antalet nätfiskeklick att öka. Men maskininlärningsmodellerna blir bättre på att fånga upp nätfiskarna innan de når användarnas brevlådor och på att förebygga skador efter klick om de kommer så långt. Fler goda nyheter? Allt fler företag inför flerfaktorlösningar för att begränsa skadan vid stöld av autentiseringsuppgifter via nätfiske per e-post.

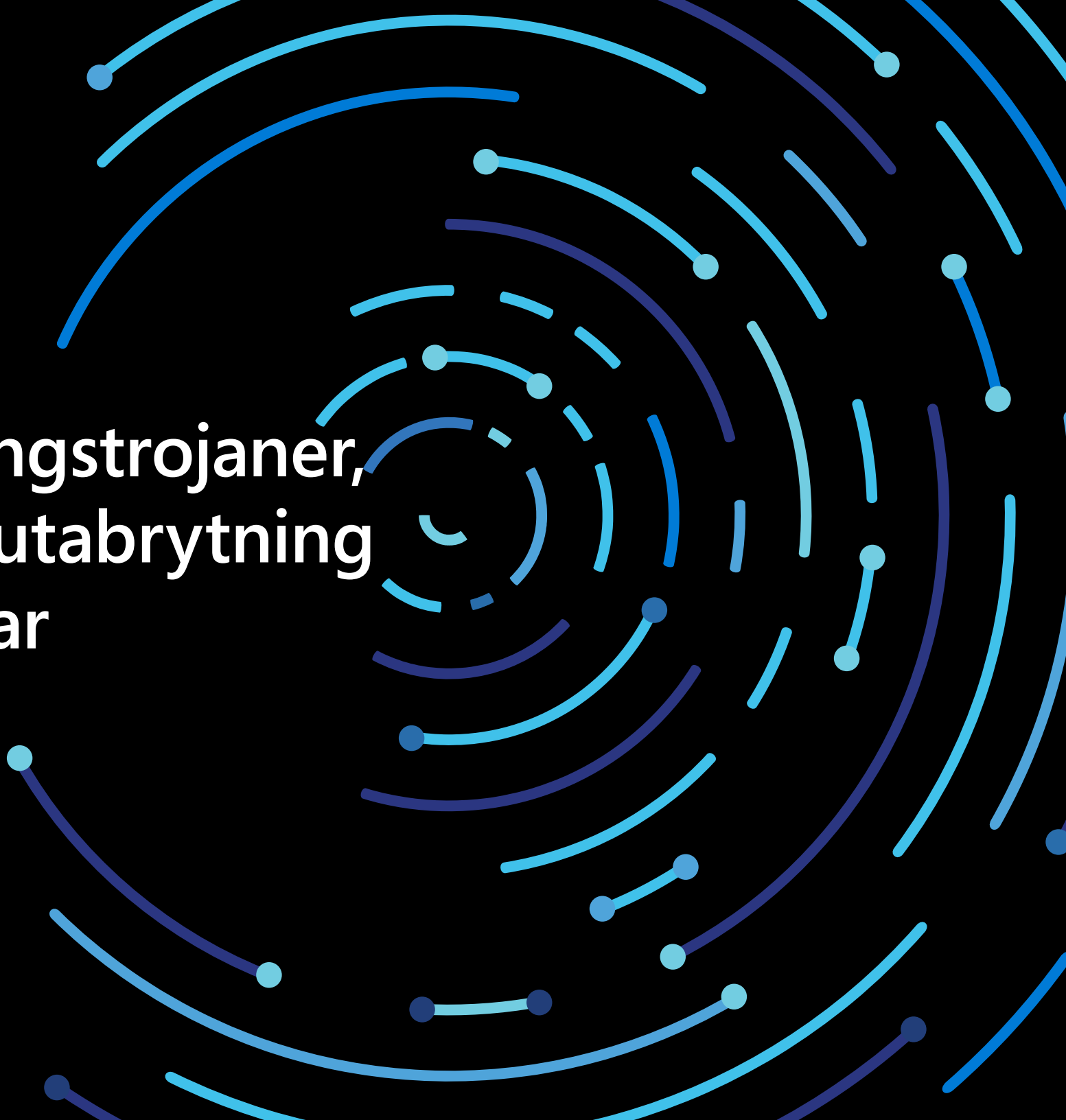
Angriparna letar efter möjligheter, så ju mer vi vet om deras metoder och hantverk, desto bättre förberedda är vi på att bygga försvar och reagera snabbt. Små viktiga steg kan göra enorm skillnad för en organisations övergripande cybersäkerhetshälsa. Det är därför du hittar rekommenderade åtgärder och andra råd om det bästa tillvägagångssättet i den här rapporten tillsammans med djupa insikter om det skiftande landskapet med skadliga program och angrepp. För när jag utövade detta var det exakt vad jag behövde i min kamp mot skurkarna. Vi hoppas att det är vad du behöver också.

Diana Kelley
Microsoft Cybersecurity Field CTO

PS. Vi är alltid ute efter att förbättra SIR. Om du har några kommentarer får du gärna ta kontakt och berätta vad du har på hjärtat.

AVSNITT I

Utpressningstrojaner, kryptovalutabrytning och pengar



De stora säkerhetsberättelserna 2017 handlade mestadels om utpressningstrojaner. Uppmärksammade och världsomspännande utbrott av WannaCrypt och Petya satte utpressningstrojaner – en typ av skadliga program som låser eller krypterar datorer och sedan kräver pengar för att återställa åtkomsten – på kartan, och många trodde att problemet bara skulle öka i framtiden. Men förekomsterna av utpressningstrojaner minskade avsevärt 2018.

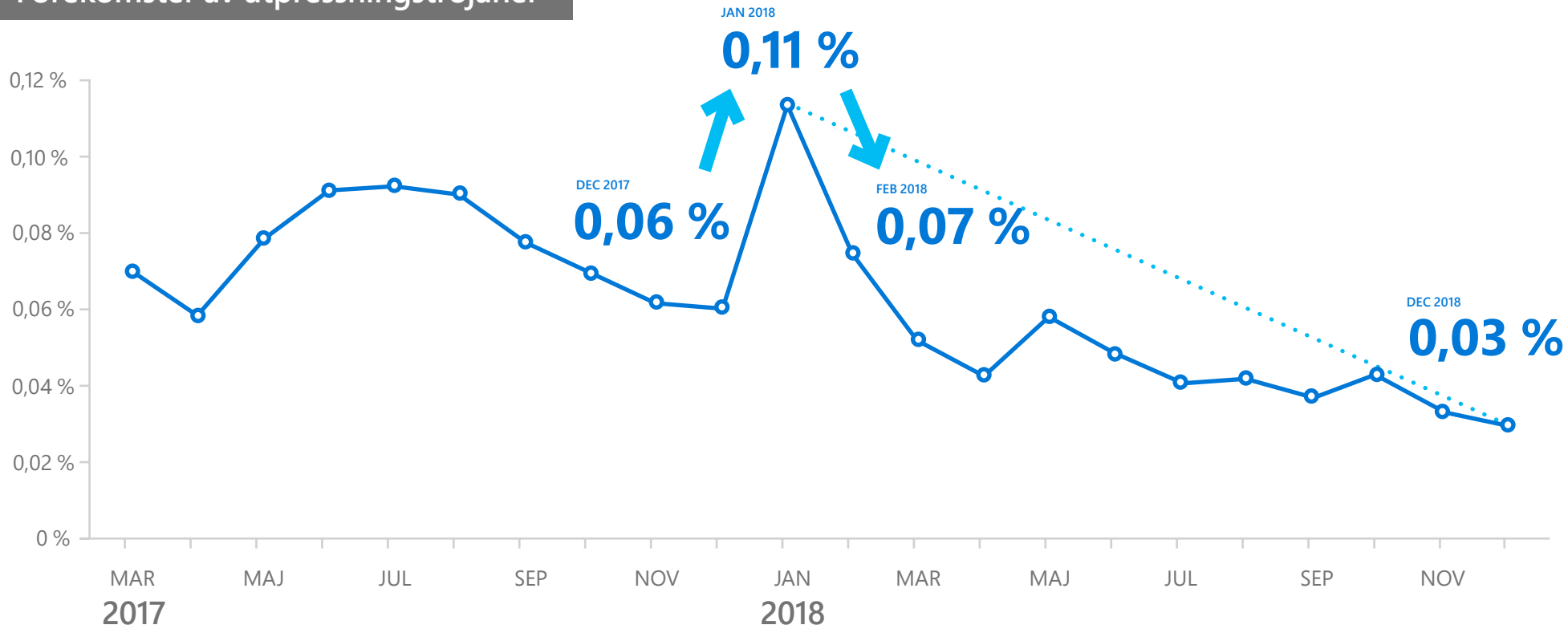
Den minskade förekomsten av utpressningstrojaner berodde delvis på förbättrade upptäcktsmöjligheter och utbildning som gjorde det svårare för angriparna att dra nytta av dem. Därför började angriparna överge utpressningstrojaner till förmån för exempelvis kryptovalutabrytning, där offrens datorresurser används för att tjäna pengar åt angriparna. Skiftet visar att de flesta vinstinriktade cyberbrottslingar i grunden är opportunister: de jagar de enklast tillgängliga pengarna, och när de ekonomiska villkoren för cyberbrott förändras anpassar de sig snabbt.

ANGREPP MED UTPRESSNINGSTROJANER PÅ NEDGÅNG

För mer än ett årtionde sedan ersattes de hackare och upptågsmakare som dominerade den tidiga undergroundkulturen av skadliga program från den organiserade brottsligheten och andra vinstorienterade intressen. Tidiga skadliga program var ofta flashiga och uppenbara, men vinstorienterade skadliga program var mycket mer benägna att verka i det tysta och undvika att väcka uppmärksamhet. De ville fortsätta skicka spam, stjäla känslig information, utföra Denial of Service-angrepp och annan skadlig aktivitet så länge som möjligt.

Utpressningstrojaner ändrade denna trend. I stället för att hålla sig dolda hindrar utpressningstrojaner helt öppet offren att komma åt sina datorer och viktiga filer tills en lösensumma betalas (och ofta även efteråt, eftersom angriparna många gånger behåller kontrollen över datorn även efter att lösensumman har betalats). När utbrottet av utpressningstrojaner nådde sin topp under 2017 såg den här typen av öppet angrepp ut att representera en ny fas i angriparnas tekniker. Men nyare uppgifter tyder på att utpressningstrojaner kan vara på nedgång. Angriparna återgår alltmer till skuggorna de har gömt sig i förut. De försöker undvika at bli upptäckta för att kunna genomföra angrepp som kryptovalutabrytning mer effektivt. Även om antalet angrepp med utpressningstrojaner har gått ned betyder det inte nödvändigtvis att angreppen har blivit mindre allvarliga.

Förekomster av utpressningstrojaner



Förekomsten av utpressningstrojaner sjönk cirka 60 % mellan mars 2017 och december 2018, med återkommande ökningar under den perioden.

BILD 1.

Angrepp med utpressningstrojaner från mars 2017 till december 2018

Det finns förmodligen många orsaker till denna totala nedgång, även om Microsofts säkerhetsforskare misstänker att en primär faktor är att både slutanvändare och organisationer blir mer medvetna om och hanterar hot från utpressningstrojaner på ett smartare sätt. Detta inkluderar att vara mer försiktiga och säkerhetskopiera viktiga filer så att de kan återställas om de blir krypterade av utpressningstrojaner. Och som tidigare har beskrivits är cyberbrottslingarna opportunistiska.

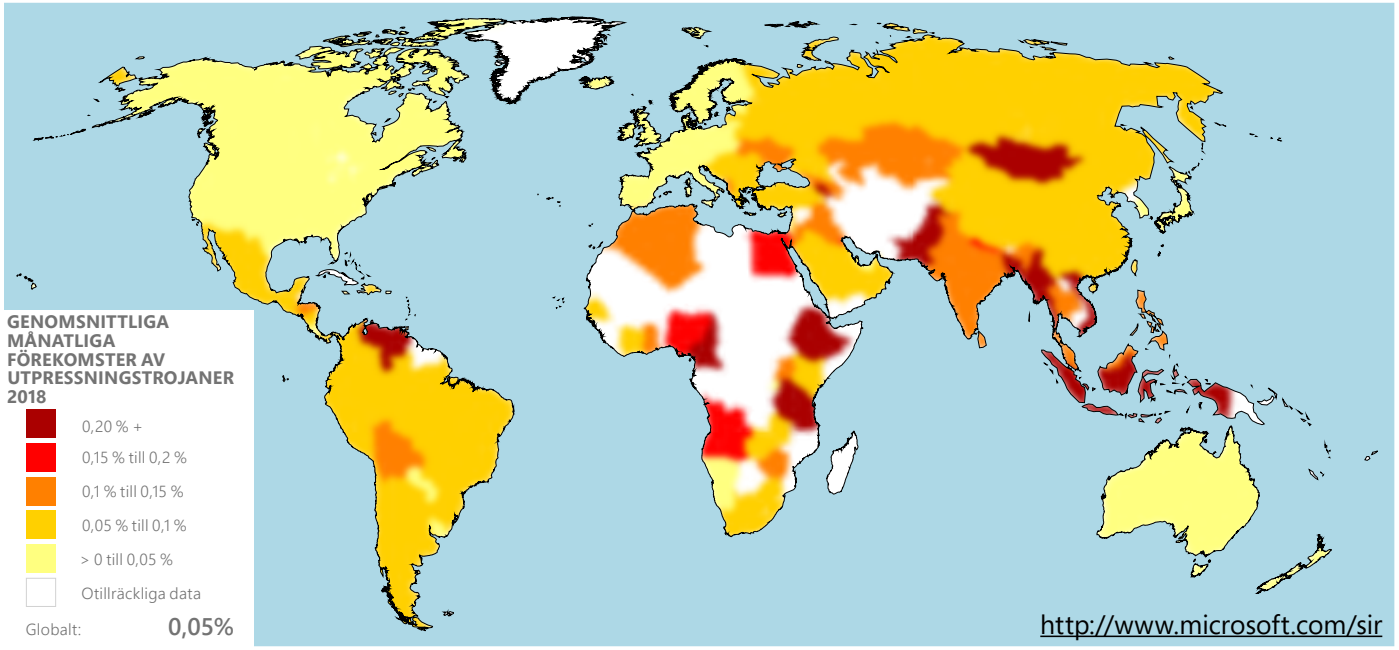
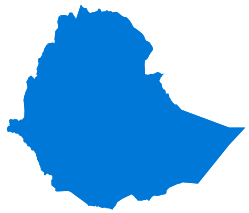


BILD 1-2.

Genomsnittligt antal angrepp av utpressningstrojaner per månad i hela världen efter land/region under 2018

DET LAND SOM PÅVERKAS MEST AV UTPRESSNINGSTROJANER: ETIOPIEN



Genomsnittliga månatliga förekomster: 0,77 %

De fem länder som har de högsta genomsnittliga månatliga förekomsterna av angrepp med utpressningstrojaner under 2018 var Etiopien (0,77 %), Mongoliet (0,46), Kamerun (0,41), Myanmar (0,33) och Venezuela (0,31), som alla hade förekomster som översteg 0,31 % under perioden.1 För några år sedan förekom angreppen med utpressningstrojaner mest i rika länder och regioner i Europa och Nordamerika, men efter hand har utpressningstrojaner börjat ratas av angriparna och angreppsmönstret har mer börjat likna mönstret hos övriga skadliga program.

De länder som hade de lägsta förekomsterna av utpressningstrojaner under 2018 var Irland (0,01), Japan (0,01), USA (0,02), Storbritannien (0,02) och Sverige (0,02 %), som alla hade förekomster på högst 0,02 % under samma period. Platser med få förekomster tenderar att ha mogna cybersäkerhetsinfrastrukturer och väletablerade program för att skydda kritisk infrastruktur och utbilda medborgarna om grundläggande säkerhet.

FOTNOTER

[1] Förekomsterna är andelen datorer som kör Microsofts realtidssäkerhetsprodukter som rapporterar ett angrepp från ett skadligt program. Att stöta på ett hot betyder inte att datorn har smittats. Endast datorer vars användare har valt att tillhandahålla data till Microsoft beaktas vid beräkning av förekomster.

KRYPTOVALUTABRYTNING PÅ UPPGÅNG

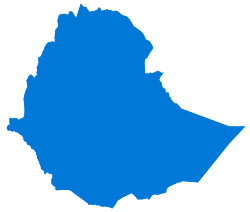
Kryptovaluta är virtuella pengar som kan användas för att köpa och sälja varor och tjänster anonymt, både på nätet och i den fysiska världen. Det finns många olika typer av kryptovalutor, men alla bygger på blockkedjeteknik. Varje transaktion registreras i en distribuerad journal som upprätthålls av tusentals eller miljontals datorer i världen. Nya mynt skapas eller "bryts" av datorer som utför komplexa beräkningar, som också verifierar blockkedjetransaktioner.

Att bryta mynt kan vara mycket lönsamt. Under 2018 var en enda Bitcoin (den äldsta och mest populära kryptovalutan) värd flera tusen dollar. Men att utföra de nödvändiga beräkningarna kan kräva stora resurser och kräver än mer varje gång ett nytt mynt bryts. För populära valutor som Bitcoin är det nästan omöjligt att bryta med vinst utan tillgång till enorma datorresurser som är långt utom räckhåll för de flesta individer och mindre grupper. Angripare som söker olovliga vinster använder därför i allt högre grad skadliga program som låter dem använda sina offers datorer för att hjälpa dem med kryptovalutabrytning. Den här metoden ger dem möjlighet att utnyttja processorkraften hos hundratusentals datorer i stället för en eller två. Även när en mindre infektion upptäcks komplicerar kryptovalutans anonyma karaktär insatserna för att spåra upp de ansvariga.

Under 2018 var de genomsnittliga förekomsterna av kryptovalutabrytning i världen 0,12 % jämfört med bara 0,05 % för utpressningstrojaner. Många faktorer bidrar till den ökade popularitet för brytning som nyttolast för skadliga program. Till skillnad från utpressningstrojaner kräver kryptovalutabrytning inga indata från användaren: det sker i bakgrunden medan användaren gör annat eller är borta från datorn, och kanske inte märks alls om det inte försämrar datorns prestanda tillräckligt. Därför är användare mindre benägna att vidta några åtgärder för att bli kvitt hotet, som kan fortsätta sin brytning till förmån för angriparen under en längre tid.

Tillgången till färdiga produkter för förtäckt brytning av många kryptovalutor är en annan drivkraft för trenden. Ingångströskeln är låg på grund av den stora tillgången till brytningsprogram som cyberbrottslingar paketerar om som skadliga program för leverans till intet ont anande användares datorer. De till vapen omgjorda brytningsprogrammen distribueras sedan till offren med hjälp av samma metoder som angriparna använder för att leverera andra hot, t.ex. social manipulation, intrång och oavsiktlig nedladdning. När brytningsprogrammet är installerat körs det i bakgrunden på offrets datorer och utför blockkedjeberäkningar, medan angriparen skördar frukterna.

GENOMSNITTLIGA MÅNATLIGA FÖREKOMSTER I LÄNDER SOM RÅKAR UT MEST FÖR KRYPTOVALUTABRYTNING



Etiopien: **5.58%**

Tanzania: **1,83 %**

Pakistan: **1,47 %**

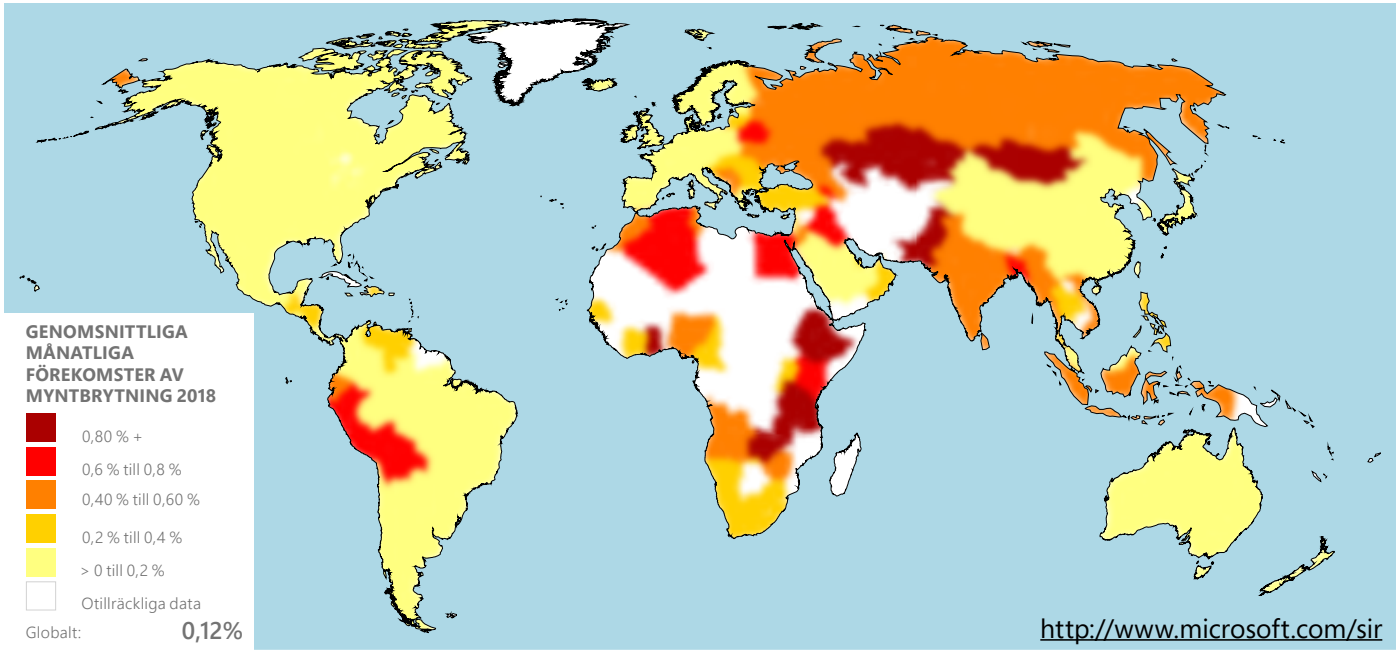


BILD 3.

Genomsnittligt antal myntbrytningsförekomster per månad i hela världen efter land/region under 2018

De fem länderna med de högsta förekomsterna av kryptovalutabrytning under 2018 var Etiopien (5,58), Tanzania (1,83), Pakistan (1,47), Kazakstan (1,24), och Zambia (1,13), som alla hade en genomsnittlig månatlig förekomst av myntbrytning på cirka 1,13 % eller mer under perioden. Länderna med de lägsta förekomsterna av myntbrytning under 2018 var Irland, Japan, USA, och Kina som alla hade genomsnittliga månatliga förekomster av myntbrytning på cirka 0,02 % under perioden.

WEBBLÄSARBASERAD KRYPTOVALUTABRYTNING: EN NY TYP AV HOT

Statistiken som presenteras i det här avsnittet omfattar skadliga kryptovalutabrytare som är avsedda att installeras på offrens datorer som skadliga program. Men några av de viktigaste hoten som gäller kryptovalutabrytning är helt webbläsarbaserade och behöver inte installeras alls. Ett antal tjänster marknadsför webbläsarbaserad kryptovalutabrytning som ett sätt för webbplatsägaren att tjäna pengar på trafik till sin webbplats utan reklam. Webbplatsägaren förväntas lägga till JavaScript-kod på sina sidor som utför kryptovalutabrytning i bakgrunden medan en användare besöker webbplatsen. Intäkterna delas mellan webbplatsens ägare och tjänsten. Tyvärr har angripare varit snabba med att dra nytta av dessa tjänster för att bryta kryptovaluta utan slutanvändarna samtycke, ofta genom att ta

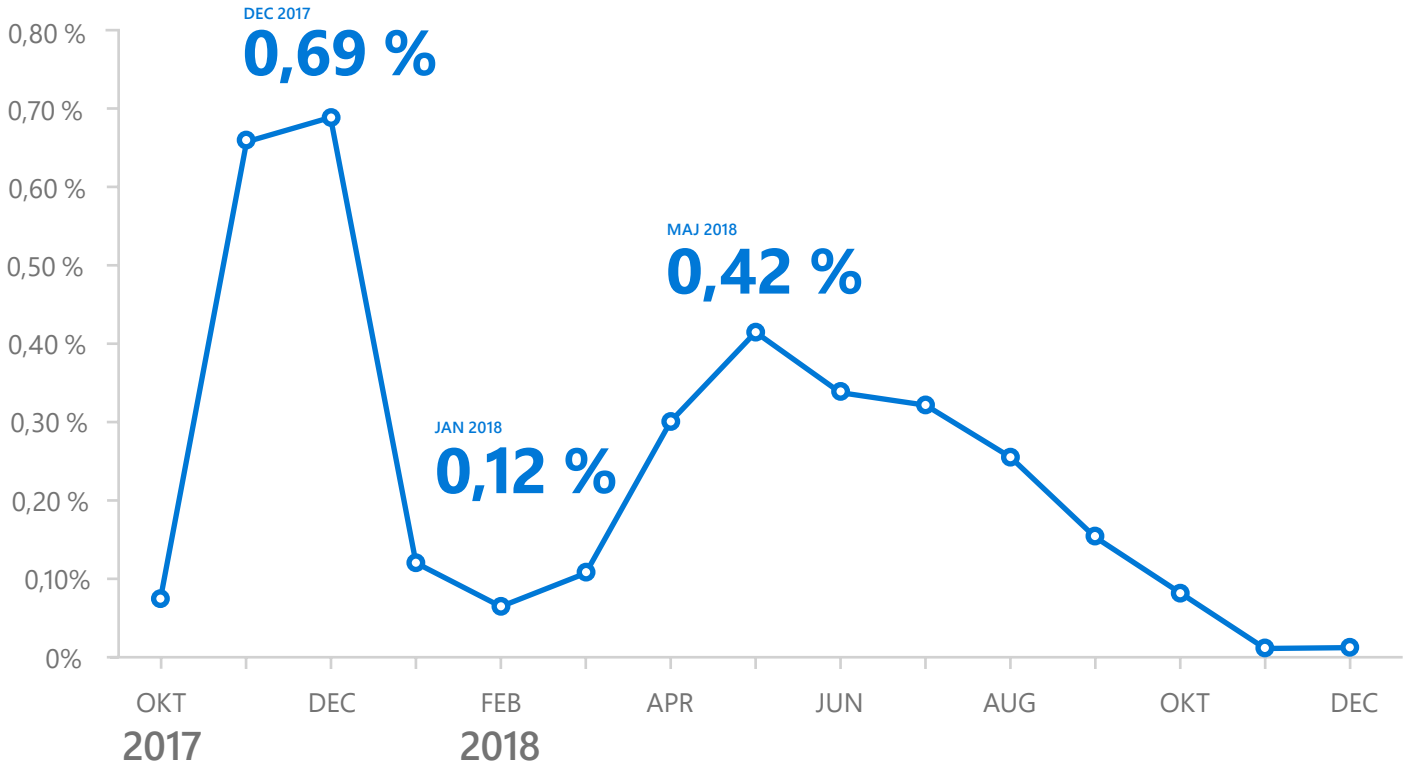
GENOMSNITTLIGA MÅNATLIGA FÖREKOMSTER I LÄNDER SOM PÅVERKAS MINST AV KRYPTOVALUTABRYTNING

Irland: 0,02 %

Japan: 0,02 %

USA: 0,02%

Förekomster av Brocoiner



sig in på legitima webbplatser och infoga brytningskoden i deras källkod. Dessa webbläsarbaserade brytare behöver inte göra intrång på slutanvändarens dator överhuvudtaget och kan köras på alla plattformar med en JavaScript-kapabel webbläsare. Liksom trojaner som bryter kryptovaluta kan webbläsarbaserade brytare avsevärt försämra datorns prestanda och slösa med elektricitet medan en användare besöker en drabbad webbsida.

BILD 4.

Förekomster av Brocoiner, den vanligaste webbläsarbaserade kryptovalutabrytaren

EFFEKTEN AV OÖNSKAD KRYPTOVALUTABRYTNING

Det mest uppenbara hotet från skadlig kryptovalutabrytning är förbrukningen av datorresurser, vilket kan slösa på el och avsevärt försämra datorns prestanda. Användare och organisationer riskerar även annat med myntbrytning:

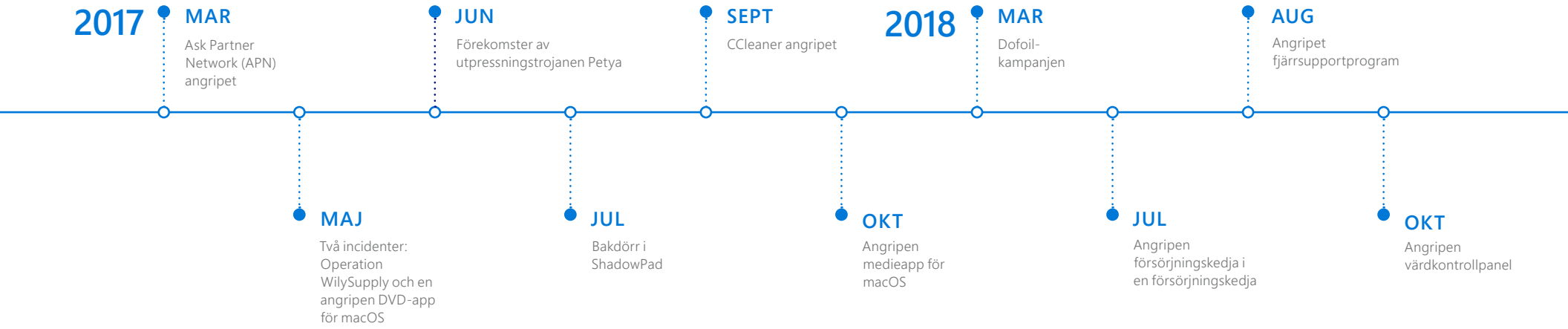
- **Få fotfäste för att göra större skada i framtiden.**
  Liksom andra former av skadliga program kan kryptovalutabrytning vara en ingång för angripare. Medan datorn bryter kryptovaluta i bakgrunden kan cyberbrottslingar undersöka miljön och eventuellt avslöja säkerhetsluckor som kan utnyttjas för andra ändamål.
- **Internetanslutna enheter kan råka ut för intrång och förvandlas till botar för kryptovalutabrytning.**
  Många sådana enheter saknar inbyggd säkerhet som identifiering av skadlig kod vilket kan göra dem till önskvärda mål för angripare.
- **Skada maskinerna.**
  Programvara för kryptovalutabrytning som körs kontinuerligt i månader eller längre kan försämra prestandan, och värmen som genereras av överdriven effektförbrukning och processoranvändning kan skada datorerna.

AVSNITT II

Programvarans försörjningskedja i riskzonen

Microsoft har i åratal spårat hotaktörer som använder intrång i försörjningskedjan som utgångspunkt för angrepp. I ett försörjningskedjeangrepp koncentrerar sig angriparen på att tränga sig in i utvecklings- eller uppdateringsprocessen för en legitim programvaruutgivare.

Om det lyckas kan angriparen infoga en komprometterad komponent i en legitim app eller ett legitimt uppdateringspaket som sedan distribueras till programvarans användare. Den skadliga koden körs sedan med samma förtroende och behörigheter som programvaran. Det ökade antalet programvarubaserade försörjningskedjeangrepp under de senaste åren har blivit ett viktigt samtalsämne för många cybersäkerhetsexperter och är en viktig oroskälla på många IT-avdelningar.



STÖRRE ANGREPP PÅ FÖRSÖRJNINGSKEDJOR FÖR PROGRAMVARA UNDER 2017

BILD 5.

Angrepp på försörjningskedjor för programvara under 2017 och 2018

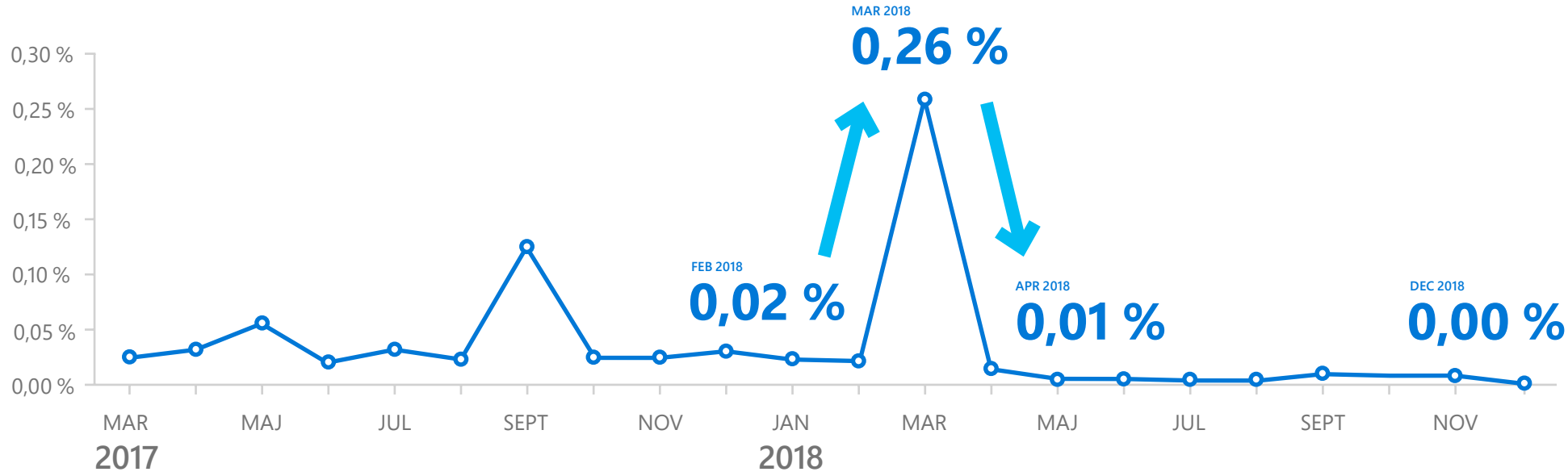
Under 2017 handlade flera uppmärksammade incidenter om angrepp på försörjningskedjor. De mest omtalade var utpressningstrojanen Petya i juni, som spårades till några initiala infektioner från en angripen uppdateringsprocess för en populär skatteredovisningsapp i Ukraina. I maj angrep Operation WilySupply en texteditors programuppdatering för att installera en bakdörr hos utvalda organisationer i finans- och IT-sektorn. I juli doldes bakdörren ShadowPad i ett programvarupaket för serverhantering och lät angripare installera ytterligare nyttolaster med skadliga program för att stjäla data och genomföra andra skadliga aktiviteter. I september angreps infrastrukturen för det populära freewareverktyget CCleaner och en version med bakdörr levererades till dess användare.

ANGREPP PÅ FÖRSÖRJNINGSKEDJOR FÖR PROGRAMVARA 2018 – GRUNDORSAKER OCH EFFEKTER

Det första stora angreppet på försörjningskedjor för programvara under 2018 inträffade 6 mars, när Windows Defender ATP blockerade en enorm kampanj för att leverera trojanen Dofoil (eller Smoke Loader). Den gigantiska kampanjen med skadliga program spårades till en förgiftad peer-to-peer-app. Appens uppdateringspaket ersattes med en skadlig version som hämtade angripen kod, som sedermera installerade Dofoil. Den sofistikerade trojanen bar en myntbrytningsnyttolast och var utrustad med avancerade tekniker för injektering mellan processer, beständighetsmekanismer och kringgåendemetoder.

BILD 6.

Trenden för förekomster av Dofoil (Smoke Loader) under 2018 visar en topp med blockerade instanser under mars



Under kampanjens första 12 timmar blockerade Windows Defender Antivirus mer än 400 000 försök till angrepp över hela världen. Ryssland stod för 73 % av de globala förekomsterna, medan Turkiet och Ukraina stod för 18 respektive 4 %.

Flera ytterligare angrepp upptäcktes där man använde angripna försörjningskedjor för programvara som leveransmekanismer under 2018, bland andra dem som beskrivs i följande tabell:

BILD 7.

Andra angrepp på försörjningskedjor för programvara under 2018

Period	Angrepp	Beskrivning	Påverkad programvara
Mars 2018	Myntbrytningskampanjen Dofoil (rapporterad av Microsoft).	Angripare förgiftade uppdateringsprocessen för en peer-to-peer-app så att Dofoil installerades. Det installerade i sin tur skadliga program för myntbrytning.	Peer-to-peer-app.
Juli 2018	Angripen försörjningskedja i en försörjningskedja (rapporterad av Microsoft).	Angripare kom åt den gemensamma infrastrukturen mellan en leverantör av en PDF-redigeringsapp och en av dess programvaruleverantörpartner.	PDF-redigeringsapp och tredjepartsleverantör.
Augusti 2018	Angripet fjärrsupportprogram (Operation Red Signature, rapporterat av Trend Micro och IssueMakersLab).	Uppdateringsservern som tillhörde en leverantör av fjärrsupportlösningar angreps och levererade sedan ett fjärråtkomstverktyg som hette 9002 RAT.	Fjärrsupportprogram.
Oktober 2018	Lösning på den angripna värdkontrollpanelen (rapporterad av ESET).	Installationsskriptet för en lösning för en värdkontrollpanel ändrades för att stjäla autentiseringsuppgifter.	Lösning för en värdkontrollpanel.

RISKERAD TILLIT

Angrepp på försörjningskedjor är försåtliga eftersom de drar nytta av den tillit som användare och IT-avdelningar har för programvaran de använder. Den komprometterade programvaran är ofta signerad och certifierad av leverantören och ger kanske ingen indikation på att något är fel, vilket gör det betydligt svårare att upptäcka infektionen. De kan skada relationen mellan försörjningskedjorna och deras kunder, oavsett om de sistnämnda är företags- eller hemanvändare. Genom att förgifta programvara och undergräva leverans- eller uppdateringsinfrastrukturer kan försörjningskedjeangreppen påverka integriteten och säkerheten hos de varor och tjänster som organisationer tillhandahåller.

Försörjningskedjeangrepp har påverkat ett brett spektrum av programvara och riktats mot organisationer i olika branscher och på olika geografiska platser. Hotet om försörjningskedjeangrepp är ett branschomfattande problem som kräver uppmärksamhet från flera intressenter, däribland programutvecklarna och leverantörerna som skriver koden, systemadministratörerna som hanterar programinstallationerna och den informationssäkerhetsgrupp som upptäcker dessa angrepp och tar fram lösningar för att skydda folk och programvara från dem.

BORTOM PROGRAMVARA: ANGREPP MOT FÖRSÖRJNINGSKEDJAN GENOM MOLNOBJEKT

Förmågan att utföra försörjningskedjeangrepp för att undergräva förtroendet förstärks och blir ännu mer komplex i molnet. Flera incidenter med angripna molnobjekt, molntjänster och molninfrastruktur under 2018 belyser denna komplexitet:

- Förgiftade Chrome-tillägg som installerade klickbaserade skadliga bedrägeriprogram (som rapporterades av ICEBRG)
- Diverse angripna Linux-lagringsplatser (rapporterade i några nätforum)
- Skadliga WordPress-instickspogram som användes för olika skadliga aktiviteter, inklusive att ge angripare möjlighet att publicera material på WordPress-webbplatser (rapporterat av Wordfence)
- Skadliga Docker-avbildningar som innehöll ett skript för att hämta skadliga program för kryptovalutabrytning och laddades upp till Docker Hub-kontot (rapporterat av Fortinet och Kromtech)
- Ett skadligt felslagspaket i den officiella Python-databasen. Paketet innehöll ett skadligt skript som laddade ner skadliga program för kapning av myntbrytningsadresser i Urklipp (rapporterat på Medium)
- Ett angripet StatCounter-skript som lät angriparen injektera ett skadligt skript på webbplatser som använder StatCounter (rapporterat av ESET)
- Flera incidenter med npm-moduler med bakdörr (npm-bloggen, Medium) som om de utnyttjas kan leda till situationer som att en angripare kan mata in godtycklig kod i en server och sedan köra den.

Dessa incidenter visar hur mycket ett angrepp på försörjningskedjan kan vidga angreppsytan. Om de inte skyddas kan molnobjekt vara oväntade ingångsvektorer. Docker Hub-incidenten innefattade t.ex. ett skadligt konto som lade upp Docker-avbildningar som innehöll en dold bakdörr för myntbrytning. Docker-avbildningarna lagrades på Docker Hub i nästan ett år, hämtades miljontals gånger och användes av intet ont anande administratörer och användare.

Riskerna med försörjningskedjan gäller även kod i molnet, öppen källkod, webbibliotek, programbehållare och andra objekt i molnet. Dessa risker och den höga graden av variation som upptäckts bland de incidenter som gällt försörjningskedjans programvara och hårdvara gör angrepp på försörjningskedjorna till en bred hotkategori. Även om det inte finns någon enskild lösning för hela spektrumet av dessa typer av angrepp, måste organisationer bygga upp preventiva skydd och metoder för att identifiera angrepp mot försörjningskedjan i efterhand från angripna hårdvaru- och programvaruleverantörer, leverantörer och uppköp, leverantörer av öppen källkod samt leverantörer av molntjänster och infrastruktur.

Utreda cyberincidenter med DART

Microsoft Detection and Response team (DART) är ett globalt team med cybersäkerhetsexperter och incidenthanterare som hjälper organisationer att upptäcka, utreda och reagera på cybersäkerhetsincidenter. Detta avsnitt belyser några av de kundcase som DART har hanterat under det senaste året. Det illustrerar vanliga angripartrender och hur Microsoft och kunderna kunde stäcka dem.

EN ORGANISATION FÖR PROFESSIONELLA TJÄNSTER DRABBADES AV ETT STATSUNDERSTÖTT ANGREPP DÄR DATA EXFILTRERADES

En organisation för professionella tjänster drabbades av ett raffinerat, statligt sponsrat avancerat beständigt hot (ABH) som fick åtkomst till organisationens privilegierade autentiseringsuppgifter. Angriparna fick tillgång till nätverket med hjälp av ett lösenordssprejangrepp. De använde ett litet antal svaga eller allmänt använda lösenord (t.ex. "p@ssword" och "123456") som de riktade mot ett stort antal användarkonton för att få tillgång till administrativa autentiseringsuppgifter för Office 365. (Lösenordssprejangrepp används för att undvika upptäckt genom att begränsa antalet inloggningsförsök för varje konto.) Efter att ha infiltrerat nätverket utförde ABH:t en genomarbetad, automatiserad exfiltrering av data från personalens brevlådor. Trots flera interna försök att slänga ut dem blev angriparna kvar i nätverket i mer än 200 dagar. Som ett led i angreppet utnyttjade motståndaren organisationens försörjningskedjeprogramvara och automatiserade dataexfiltreringen.

Eftersom de misstänkte ett intrång mot sina kunduppgifter anlitade organisationen DART-teamet för att utreda och förhindra ytterligare skador. DART identifierade riktade sökningar mot Office 365-brevlådor, angripna konton och angriparens kontroll- och angreppskanaler. Viktiga kundlärdomar från den här incidenten var att använda kontroller för att skydda molntjänster från identitetsbaserade hot och angripare. Organisationen har infört multifaktorautentisering (MFA), policyer för villkorad åtkomst för vissa molnappar samt loggning av Office 365. För att skydda sig ännu mer mot liknande hot framöver kanske organisationen kommer att införa en EDR-lösning (Endpoint Detection and Response) för att identifiera angripare som kanske försöker utnyttja deras nätverk. Dessutom har vi rekommenderat att den här organisationen utser ett molnstyrningsorgan eller ett globalt identitetsteam som ska hantera och genomdriva lämpliga policyer för användarautentisering, så att organisationen har tillsyn över sitt säkerhetsläge och kan minska risken mer effektivt.

AVSNITT III

Nätfiske är fortfarande störst

Under 2018 har Microsofts hotanalytiker sett tecken på att angriparna fortsätter att använda nätfiske som prioriterad angreppsmetod. Nätfiske kommer att förbli ett problem under överskådlig tid, eftersom det omfattar mänskliga beslut och mänskliga bedömningar. Cyberbrottslingarna ger sig inte met 60 procent någon hugger på ett bete.

Nätfiskefrekvensen är fortfarande på uppgång
Andelen inkommande e-postmeddelanden som utgör nätfiske

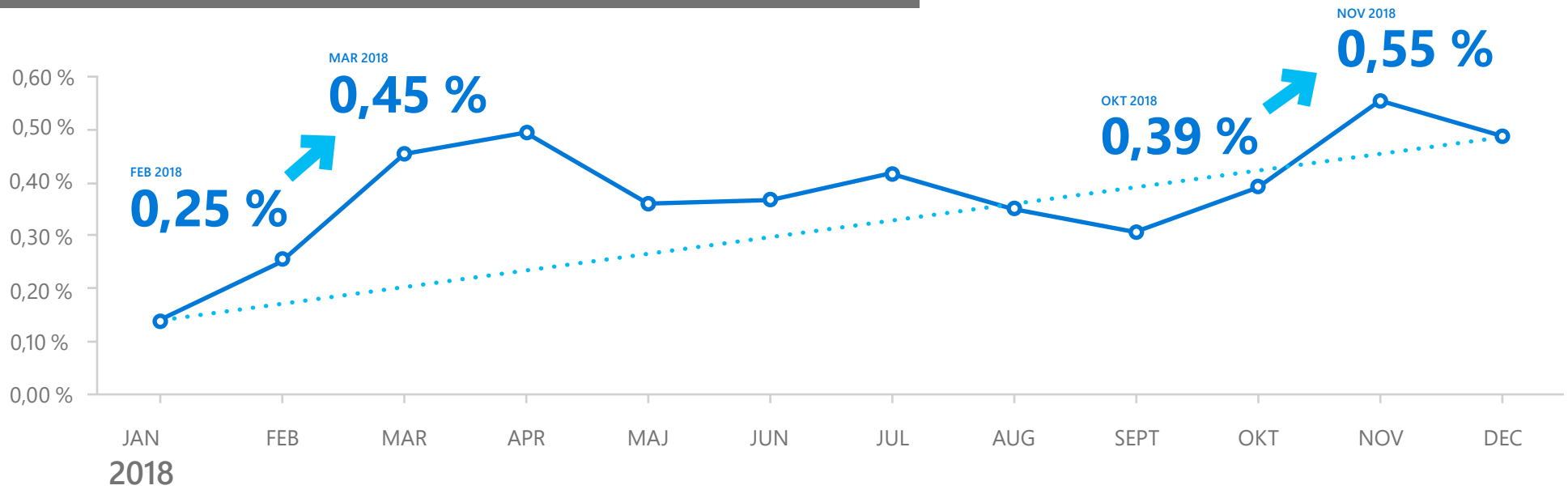


BILD 8.

Nätfiske per e-post 2018

NÄTFISKE FORTSÄTTER ATT VARA EN POPULÄR ANGREPPSVEKTOR UNDER 2018

I Office 365 analyserar och avsöker Microsoft fler än 470 miljarder e-postmeddelanden per månad efter nätfiske och skadliga program, vilket ger analytikerna goda inblickar i angreppstrender och angreppsmetoder. Andelen inkommande e-postmeddelanden som var nätfiske ökade med 250 % mellan januari och december 2018. Nätfiske är fortfarande en av de främsta angreppsvektorerna som används för att leverera skadliga nya nyttolaster förrän användarna, och Microsoft har fortsatt att försvåra dessa angrepp med ytterligare skydd mot, upptäckt av, utredning av och reaktioner mot nätfiske för att försöka skydda användarna.

Utvecklingen av nätfiskets angreppsmetoder

När verktygen och metoderna som används för att skydda folk från nätfiske blir mer raffinerade tvingas angriparna att anpassa sig. Nätfiskeangrepp har blivit alltmer polymorfa. Det innebär att angriparna inte använder en enda webbadress, domän eller IP-adress för att skicka e-post, utan utnyttjar en varierad infrastruktur med flera angreppspunkter. Själva angreppstypen har också utvecklats. Moderna nätfiskekampanjer kan vara allt från korta angrepp under bara några minuter till mycket längre kampanjer med hög volym. Andra variantangrepp sker i serier där angriparen skickar få e-postmeddelanden under flera efterföljande dagar.

Dessutom har Microsoft observerat en trend som innebär att angriparna nyttjar värdbaserad infrastruktur och annan publik molninfrastruktur, vilket gör det enklare att undvika identifiering genom att gömma sig bland legitima webbplatser och tillgångar. Angriparna använder t.ex. allt oftare populära dokumentdelnings- och samarbetswebbplatser och -tjänster för att distribuera skadliga nyttolaster och falska inloggningsformulär som används för att stjäla användares inloggningsuppgifter. Användningen av angripna konton för att skicka mer skadlig e-post både inom och utanför en organisation har också ökat.

Nätfiskekampanjer kan vara målinriktade eller breda

Precis som vid distribution av skadliga program i allmänhet kan nätfiskekampanjer variera från riktade till bredare, mer generiska angrepp. Även om mycket raffinerade nätfiskeangrepp ger större penningvinster per fiskat konto, kan mer generiska angrepp ge mindre pengar per angripet konto men rikta sig till en bredare uppsättning användare.

Ett exempel på en sofistikerad, riktad kampanj är Ursnif, där angriparna översatte dokumentets filnamn så att det skulle kunna riktas specifikt mot den utsattas bekanta organisation eller bransch. Sådana angrepp skiljer sig rejält från breda kampanjer och förefaller vara mer legitima och pålitliga.

Några av de bredare kampanjerna under 2018 var relaterade till angrepp mot affärskorrespondens och imitation av kända varumärken, domäner eller användare inom de utsedda organisationerna, samt raffinerande förfalskningskampanjer. Domänimitation är en vanlig angreppstaktik som används för att lura organisationer att tro att e-postmeddelandet är trovärdigt och bör öppnas.

Det finns många former av nätfiskebeten

Microsoft-forskare har funnit att många olika typer av nätfiskebeten eller nyttolaster används i kampanjer:

- **Domänförfalskning** (e-postmeddelandets domän matchar det ursprungliga domännamnet exakt)
- **Domänimitation** (e-postmeddelandets domän liknar det ursprungliga domännamnet)[2]
- **Användarimitation** (e-postmeddelandet verkar komma från någon man litar på)
- **Textbeten** (texten ser ut att komma från en legitim källa som en bank, myndighet eller annat företag så att påståendena verkar korrekt, och offret ombeds vanligen att lämna ut känslig information som användarnamn, lösenord eller känsliga finansiella uppgifter)
- **Länkar för stöld av inloggningsuppgifter** (e-postmeddelandet innehåller en länk till en sida som liknar en inloggningssida på en legitim webbplats, så att användarna anger sina inloggningsuppgifter)
- **Nätfiskebilagor** (e-postmeddelandet innehåller en skadlig bifogad fil som avsändaren lockar offret att öppna)
- **Länkar till falska molnlagringsplatser** (e-postmeddelandet verkar komma från en legitim källa och lockar användaren att ge tillstånd och/eller ange personlig information som autentiseringsuppgifter i utbyte mot att få komma in på en falsk lagringsplats i molnet)

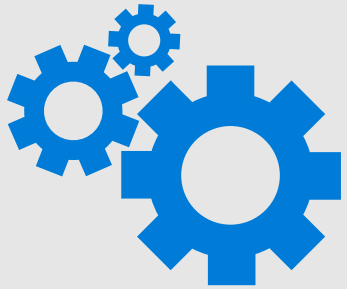
Alla dessa beten som angripare kan tänkas använda ökar komplexiteten i de nätfiskehot som organisationer måste brottas med.

FOTNOTER

[2] Domänimitation kan likna domänförfalskning (en exakt matchning av det ursprungliga domännamnet) i undantagsfallet då domänen visas i e-postnamnet.

Utreda cyberincidenter med DART

STORT TILLVERKNINGSFÖRETAG DRABBADES AV RIKTADE NÄTFISKEINCIDENTER



Ett tillverkningsföretag genomlevde en nätfiskekampanj i flera faser under ett par månader. Detta tillvägagångssätt är inte ovanligt. Under den första fasen spanar angriparen, och under den andra inriktar hen sig på värdefulla tillgångar. Under den första etappen i den här kampanjen utnyttjades en välkänd nätfiskebluff som baserades på en länk till en webbsida inbäddad i ett e-postmeddelande som skickades till en liten grupp inom företaget. E-postmeddelandet hävdade att mottagaren hade ett viktigt elektroniskt dokument som väntade på att granskas, och det enda mottagaren behövde göra för att få tillgång till det var att logga in med sina domänautentiseringsuppgifter. Den falska målsidan där mottagaren kunde läsa det så kallade ”viktiga dokumentet” sparade autentiseringsuppgifterna och gav angriparen tillgång till Office 365-konton från var som helst i världen. Den andra fasen av nätfiskekampanjen var avsedd att skicka liknande nätfiske-e-post till högt värderade personer i det angripna tillverkningsföretaget, i hopp om att få tillgång till mer värdefulla data. Microsoft samarbetade med den här kunden under den andra fasen av nätfiskekampanjen. De viktiga lärdomar kunden drog av denna incident var att nätfiske alltjämt är en av de mest effektiva angreppsmetoderna och att användarna fortfarande är den svagaste länken. Det är viktigt att lära användare att vara uppmärksamma på nätfiske, att ha verktyg för att identifiera angripare och agera och att regelbundet korrigera systemen. Organisationen kan bli sårbar om den missar bara en av de här sakerna.

I det här fallet var kunden särskilt mån om att kunna blockera åtkomsten till de angripna kontona. I samarbete med Azure Identity- och Office 365-teamen utarbetade DART en plan för att radera ut angriparen från nätverket och övervaka all trafik till kommando- och kontrollkanalen med hjälp av den nyinstallerade lösningen Microsoft Azure Log Analytics. Teamet lyckades lösa situationen på bara tre timmar. Angriparens åtkomst blockerades och företaget kunde koncentrera sig på skadebedömning och återställning. DART använde Azure Log Analytics för att spåra angriparens beteende, vilket hjälpte företaget att upptäcka många konfigurationsproblem. DART hittade t.ex. brister i korrigeringen av kritiska servrar, upptäckte datorer i nätverket som kommunicerade med kända dåliga värdar på internet och hittade flera viktiga servrar som saknade skydd mot skadliga program.

AVSNITT IV

Skadliga program i världen

Skadliga program utgör risker för organisationer och enskilda i form av minskad användbarhet, dataförlust, immaterialrättsstöld, penningförluster eller, oro och kan till och med äventyra människors liv. Microsoft använder ett brett spektrum av verktyg och tekniker för att identifiera, blockera och utrota infektioner med skadliga program var de än hittas.

Förekomsterna av skadliga program varierade mellan cirka 5 % till mer än 7 % under 2017. I början av 2018 var de förhöjda innan de minskade under större delen av året till strax över 4 %. Några möjliga orsaker till den totala minskningen av förekomsterna av skadliga program under 2018 är ökad användning av Windows 10 och Windows Defender som skydd. Förekomsterna är den andel datorer som kör Windows Defender Antivirus som rapporterade kontakter med skadliga program under månaden, inklusive infektionsförsök som Defender blockerade.

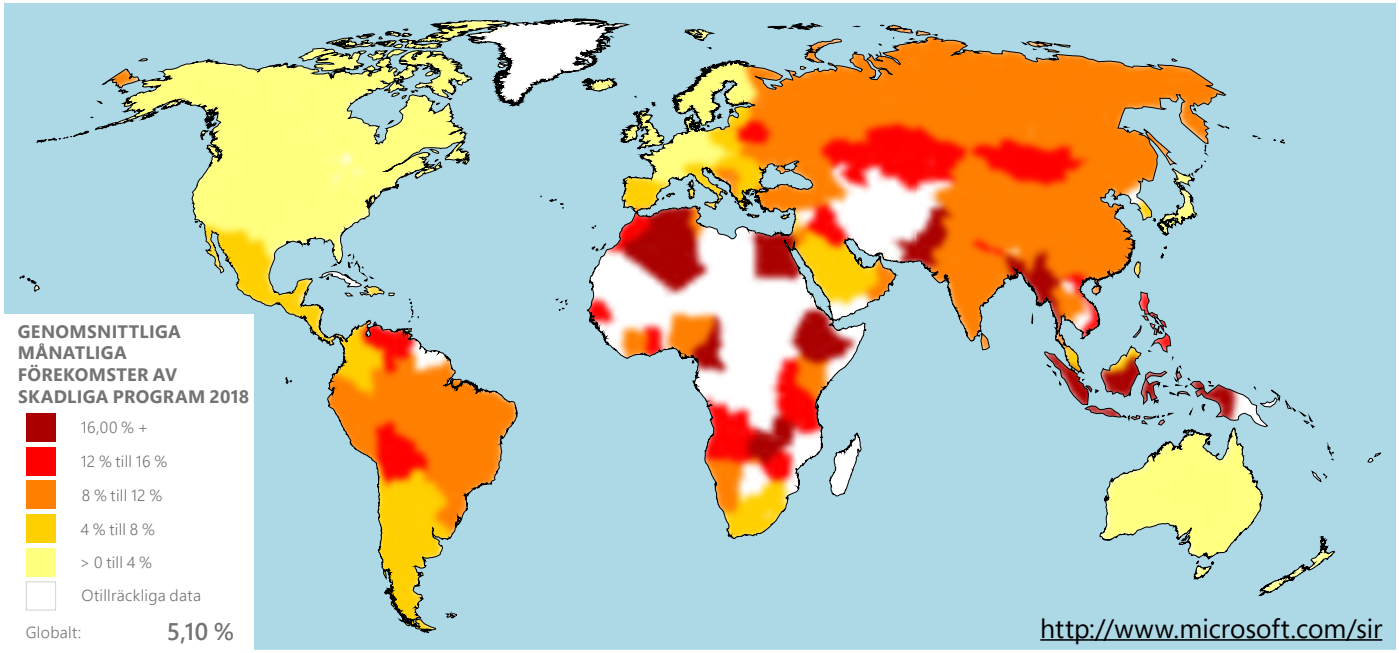


BILD 9.

Genomsnittliga månatliga förekomster av skadliga program i hela världen efter land/region under 2018

De fem platser med de högsta förekomsterna av skadliga program under perioden januari–december 2018 var Etiopien (26,33 %), Pakistan (18,94), de palestinska territorierna (17,50), Bangladesh (16,95), och Indonesien (16,59), som alla hade genomsnittliga månatliga förekomster på cirka 16,59 % eller mer under perioden. Infektionsfrekvensen brukar vara starkt korrelerad med utvecklingsgraden och teknikberedskapen i samhället. Samtliga platser med de högsta förekomsterna under 2018 rankas bland de 40 % lägsta länderna och regionerna i 2017 Information and Communications Technologies (ICT) Index, som publiceras av FN:s internationella telekommunikationsunion (ICT) .

De fem platser med de lägsta förekomsterna av skadliga program under samma period var Irland (1,26), Japan (1,51), Finland (1,74), Norge (1,79) och Nederländerna (1,82), som alla hade genomsnittliga månatliga förekomster på 1,82 % eller mindre under perioden. Dessa platser tenderar att ha mogna cybersäkerhetsinfrastrukturer och väletablerade program för att skydda kritisk infrastruktur och utbilda medborgarna om grundläggande säkerhet.

GENOMSNITTLIGA MÅNATLIGA FÖREKOMSTER I LÄNDER SOM PÅVERKAS MEST AV SKADLIGA PROGRAM

Etiopien: **26,33 %**

Pakistan: **18,94 %**

Palestinska territorierna: **17,50 %**

Utreda cyberincidenter med DART

FLERA FINANSIELLA TJÄNSTEORGANISATIONER UPPLEVDE STATSUNDERSTÖDDA ANGREPP SOM STÖRDE VERKSAMHETEN

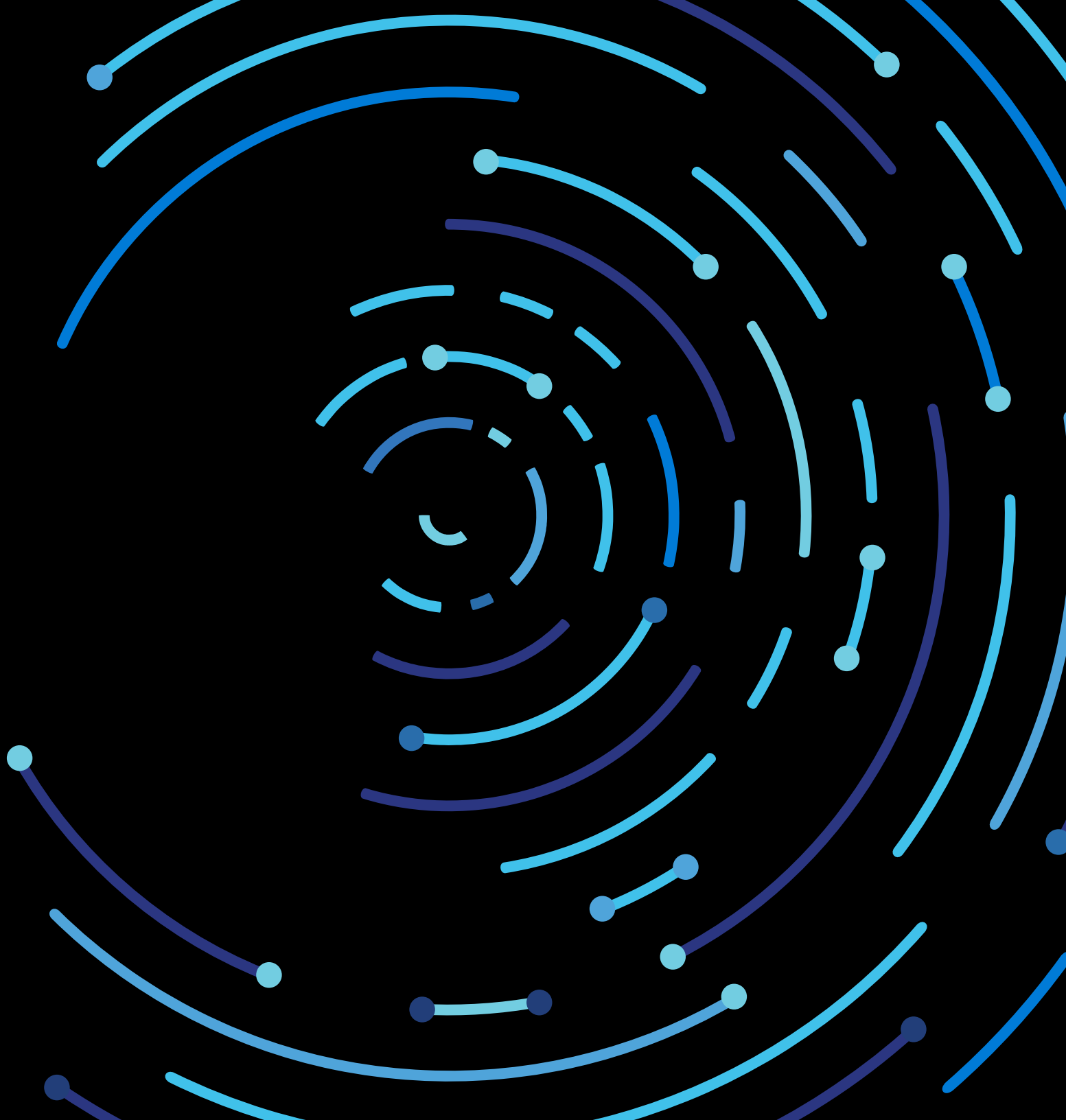
I en av de mer destruktiva incidenterna som DART har sett drabbades flera finansiella tjänsteorganisationer av ett statsunderstött ABH (en annan grupp än den som riktade in sig på den professionella tjänsteorganisationen som nämndes tidigare). Förloppet var likartat.

Detta ABH fick administrativ åtkomst efter att ha infekterat en patient noll-maskin med ett välriktat och maskerat bakdörrsimplantat som möjligen levererades genom spjutfiske-e-post. Därefter utförde ABH:t flera bedrägliga transaktioner och överförde stora summor till utländska bankkonton. I vissa fall upptäcktes angriparen inte på mer än 100 dagar. När angriparen insåg att hen upptäckts satte hen snabbt i gång ett i förväg iscensatt angrepp och skickade ut destruktiva skadliga program till mer än hälften av systemen i miljön. Dessa kunders verksamhet låg nere i flera dagar.

Dessa incidenter gav några viktiga kundlärdomar. Den första var att det är särskilt viktigt att hantera programvarans livscykel. Det omfattar att se till att system (operativsystem och säkerhet) uppdateras regelbundet, korrigeras och granskas. I ett fall hade en organisation en Linux-systemmiljö med ett exceptionellt stort antal laster som var helt ohanterad, vilket utsatte den för väldigt hög risk för angrepp. Den andra lärdomen var att det är viktigt att ha säkerhetskopior av systemdata på en annan plats offline om primära data förloras. En tredje lärdom var att traditionella antiviruslösningar kanske inte räcker om man behöver känna till vad motståndaren gör.

Att återgå till normalt driftläge hade högsta prioritet för dessa organisationer. DART hjälpte till att återställa tjänsterna genom att först undersöka effekten och sedan vidta nödvändiga avhjälpande åtgärder, som att ta bort skadliga program från de berörda systemen och försätta dem i ett felfritt tillstånd. Teamet utbildade också kunderna i att använda Microsofts hotutredningsverktyg, bland andra EDR, så att de kunde söka efter avvikande beteende och angriparaktivitet i sina nätverk. DART betonade att slutpunktsövervakning är extremt viktigt för att försvara sig effektivt mot raffinerade, riktade angrepp som kanske inte upptäcks av traditionella antiviruslösningar.

Råd



Råd

En motståndskraftig organisation och meningsfull riskminskning kräver en säkerhetsstrategi som omfattar förebyggande, upptäckt och respons. Vi har ordnat följande rekommenderade säkerhetsmetoder och kontroller i dessa kategorier.

FÖREBYGGANDE:

Förebyggande kontroller spelar en nyckelroll i en övergripande försvarsstrategi, eftersom de rätta investeringarna kan öka cyberbrottslingarnas angreppskostnader och upprätthålla de ökade angreppskostnaderna över tid (utan att kräva att en expertanalytiker övervakar och tolkar utgången). Investeringar i förebyggande kontroller bör inriktas på de billigaste teknikerna för att göra sig kvitt billiga och effektiva angreppstekniker.

Det finns fyra saker att tänka på för förebyggande:

1. **Säkerhetshygienen är extremt viktig. Som framgår av några av de cyberincidenter som beskrivs i denna rapport kan vanliga hygienproblem undergräva avancerade säkerhetsfunktioner. Att följa dessa tips kan bidra till att minska risken:**

- Undvik att använda obekanta kostnadsfria och/eller piratkopierade program. Använd endast programvara från betrodda källor.

- Minska risken för stöld av autentiseringsuppgifter, vilket inbegriper att skydda privilegierade administratörskonton. Om du vill veta hur det går till, läs den här bloggen som beskriver några principer och verktyg som Microsoft har använt för att vägleda och förbättra sin egen säkerhet, samt några normativa översikter för att hjälpa dig planera dina egna initiativ.

- Tillämpa de säkra grundkonfigurationer som dina programvaruleverantörer erbjuder.

- Håll maskinerna uppdaterade genom att snabbt installera de senaste uppdateringarna av dina operativsystem och appar, och använd omedelbart viktiga säkerhetsuppdateringar för operativsystem, webbläsare och e-post. Isolera (eller kassera) datorer som inte går att uppdatera eller korrigera.

- Implementera avancerade e-post- och webbläsarskydd. Använd en säker e-postgateway med avancerade skydd som försvarar mot moderna nätfiskevarianter.

- Slå på skyddet mot skadliga program och nätverksförsvaret på värden för att kunna blockera hot nästan i realtid med hjälp från molnet (om detta ingår i din lösning).

2. **Implementera åtkomstkontroller. Tänk på detta:**

- Tillämpa principen om lägsta behörighet, vilket inkluderar implementering av nätverkssegmentering, att inte låta slutanvändare ha lokala administratörs-behörigheter och att vara försiktig med att bevilja behörighet till appar som körs på datorn.
- Begränsa hämtning av appar så att det sker endast från tillförlitliga källor (en officiell appbutik).
- Inför kraftfulla kodintegritetspolicyer, inklusive att begränsa vilka appar som användare får köra. Använd om möjligt en säkerhetslösning som begränsar den kod som körs i systemkärnan (kerneln) och kan blockera osignerade skript och andra former av opålitlig kod. Använd vitlistning av appar.
- Om du vill veta mer om angrepp mot försörjningskedjor för programvara och hur du skyddar dig mot dem, läs den här bloggen från Microsoft-forskare.

3. **Skapa och spara säkerhetskopior.**

- Skapa förstörelsebeständiga säkerhetskopior av dina kritiska system och data.
- Använd molnlagringstjänster för automatisk säkerhetskopiering av data online. Ta regelbundet säkerhetskopior av viktiga lokala data enligt 3-2-1-regeln. Behåll tre säkerhetskopior av dina data på två olika lagringstyper och ha minst en säkerhetskopia på annan plats.

4. **Var uppmärksam och agera om du misstänker något.**

- Lär medarbetarna att vara försiktiga med suspekta meddelanden där känslig information begärs och instruera dem hur de ska reagera och rapportera dem till organisationens säkerhetsteam omedelbart. Utbildning kan också hjälpa till att minska angrepp genom social manipulation och spjutfiskeangrepp.
- Tänk efter innan du klickar på webblänkar. Att utöva säkra surfvanor och använda lösningar som varnar om eller blockerar åtkomst till osäkra webbplatser kan bidra till att minska sannolikheten för att råka hamna på webbplatser som sysslar med kryptovalutabrytning.
- Om en dator körs exceptionellt långsamt, leta då efter suspekta filer som körs. Tveka inte att lämna in ett prov till operativsystemleverantören. Du kan skicka in filer för analys av skadliga program till Microsoft på https://www.microsoft.com/wdsi/filesubmission.

DETEKTERING OCH RESPONS:

Detektering och respons bidrar till återhämtning genom att begränsa den tid som en angripare har åtkomst till resurserna. Detta minskar angriparens avkastning genom att både öka kostnaden (hen måste försöka igen eller ändra sina metoder) och minska vinsten (det begränsar sannolikheten för att hen uppnår sina mål).

Samma molnteknik som gör det möjligt för företag att tillgodose marknadens behov bättre kan hjälpa säkerhetsåtgärder att mota bort angripare bättre.

BILD 10.

Säkerhetsdriftcentralers evolution

När vi ser på hur säkerhetsdriftcentraler utvecklas märker vi att tekniken ständigt gör säkerhetsdriftcentralers beslut och åtgärder snabbare och bättre. Många av dessa innovationer kan mappas till varje steg i slingan Observera–Orientera–Besluta-Handla som dokumenterades av överste John Boyd i det amerikanska flygvapnet.[3]

OBSERVERA – Säkerhetsdriftcentraler kan utnyttja enorma mängder tillgänglig säkerhetsinformation (från Microsoft och andra källor), vilket ökar deras överblick dramatiskt inom organisationen och den yttre miljön.

ORIENTERA – Efterhand som dessa nya datakällor blir tillgängliga för redan överbelastade säkerhetsdriftcentraler, blir maskininlärning (en underkategori av artificiell intelligens) ett viktigt verktyg för att resonera kring dessa enorma datauppsättningar och identifiera avvikelser som är värda att utreda. Säkerhetsleverantörer (även Microsoft) har börjat använda maskininlärningsteknik för att snabbt prioritera händelser (och hjälpa till att sätta samman dessa enskilda händelser till holistiska incidenter).

BESLUTA – Eftersom angreppsvolymen och komplexiteten snabbt kan överbelasta en säkerhetsdriftcentral måste analytiker och incidenthanterare fatta många beslut och agera snabbt när varningar och detekteringar kommer. Microsoft och andra leverantörer har integrerat automatiserade utredningsfunktioner samt råd för att hjälpa analytiker att fatta bra beslut snabbt (för att exempelvis isolera potentiellt infekterade eller komprometterade enheter). För ögonblicket är automatiseringen inriktad på att snabbt lösa incidenter med låg prioritet så att specialfärdigheter kan tillämpas på mer komplicerade problem.

AGERA – Responsen måste genomföras snabbt och korrekt på många tekniker och plattformar, vilket är vad tekniker för säkerhetsinstrumentering och responsautomatisering möjliggör. Microsoft och många andra fortsätter att investera i dessa tekniker, inklusive modern hotidentifiering och automatiserade responslösningar.

FOTNOTER

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

Detta är några andra trender som gäller en modern säkerhetsdriftcentral:

- **Bra men inte för stora aviseringsflöden** – I takt med att organisationerna går från att ha "för lite information" till att ha "för mycket information" blir de högt specialiserade säkerhetsdriftcentralernas analytikers tid alltmer värdefull. Detta ökar behovet av att aviseringar som kräver analytikerinteraktion på nivå 1 och 2 håller hög kvalitet. Även om ytterligare dataflöden alltid är till nytta vid utredningar och proaktiv jakt, mäter Microsofts Corporate IT-säkerhetsdriftcentral den sanna positiva förekomsten av aviseringsflöden som kräver analytikers insatser (och som för närvarande kräver en sann positiv frekvens på minst 90 %).

- Datas tyngd – Det är svårt att utföra analyser av stora datamängder (inklusive säkerhetsdata) utan tillgång till underliggande rådata. När mer säkerhetsdata blir tillgängliga blir det billigare och mer praktiskt att utföra säkerhetsanalysen i molnet än att hämta tillbaka uppgifterna till ett lokalt system. Detta kommer sannolikt att leda till att SIEM- och säkerhetsdriftcentralarkitekturer utvecklas som kan omfatta SIEM-hybridmetoder eller införandet av molnbaserad SIEM som tjänst.

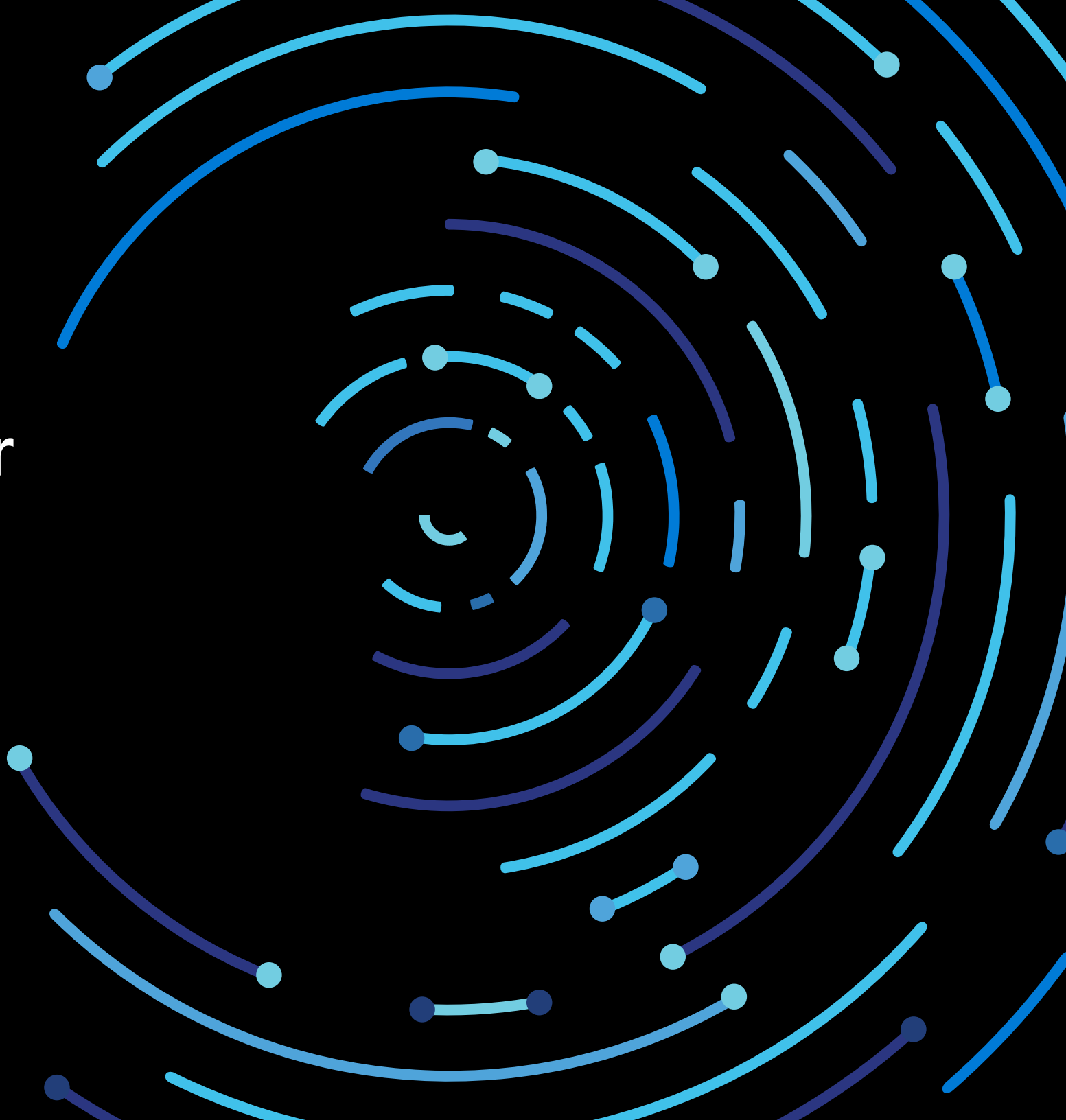
- **God kontext** – Dessa typer av detekteringar är mycket nyttigare eftersom de kan korrelera datauppsättningar mer effektivt. Medan traditionella nätverkstrafikbaserade detekteringar fortfarande har ett visst säkerhetsvärde, saknar obearbetad nätverkstrafik vanligtvis den kontext som krävs för att skilja mellan legitim och avvikande aktivitet. Vi ser hur säkerhetsdriftcentraler får ut mycket mer ur sammanhangsrika detekteringar:

  - **EDR-lösningar (slutpunktsidentifiering och svar)** med god kontextinformation om värdaktiviteten
  - Identitetsbaserade detekteringar som omfattar insikter om normala användarautentiseringsmönster (platser, tider, tjänster som används osv.) och tillämpar beteendeanalyser

Dessa kontextrika detekteringar är svårare för angriparen att kringgå, eftersom hen måste efterlikna en mycket mer komplicerad operation (kontra ett par tekniska IP-trafiksattribut).

En annan lärdom vi har dragit från allvarliga intrång hos kunderna är hur svårt det är att reagera på incidenter snabbt när IT-funktionen är helt eller delvis outsourcad. Vi rekommenderar att ni granskar era IT-outsourcingsavtal och servicenivåer samt leverantörer i försörjningskedjan för att säkerställa att de är kompatibla med snabba säkerhetsåtgärder. Fler lärdomar från våra incidentutredningar hos kunder finns i Incident Response Reference Guide (IRRG) på https://aka.ms/IRRG.

Datakällor



Datakällor

Microsoft har samlat in de data som ingår i Microsoft Security Intelligence Report genom att tillhandahålla ett brett utbud av produkter och tjänster, vilket diskuteras i Microsofts sekretesspolicy. Dessa data ger oss värdefull information om säkerheten hos och driften av våra produkter och tjänster, samt insikter om hotbilden kring cybersäkerhet i allmänhet. Dessa data innehåller analyser från följande källor:[4]

- **Azure Security Center** är en tjänst som hjälper organisationer att förebygga, upptäcka och reagera på hot genom att ge ökad insyn i säkerheten hos molnlaster och använda avancerade analyser och hotunderrättelser för att upptäcka angrepp.

- **Bing** är sök-och beslutsmotorn som utför miljarder sökningar på webbsidor per år för att söka efter skadligt innehåll. När sådant innehåll upptäcks visar Bing varningar för användare för att förhindra infektion.

- **Exchange Online** är Microsofts e-post- och produktivitetstjänst. Exchange Onlines tjänster mot skadliga program och spam söker igenom många miljarder meddelanden varje år för att identifiera och blockera spam och skadliga program.

- **Verktyget Borttagning av skadlig programvara** är ett kostnadsfritt verktyg som Microsoft har utformat för att hitta och avlägsna specifika vanliga familjer av skadliga program från kundernas datorer. Det släpps främst som en viktig uppdatering via Windows Update, Microsoft Update och automatiska uppdateringar. En version av verktyget är också tillgänglig från Microsoft Download Center. Det ersätter inte en uppdaterad realtidslösning mot virus.

- **Microsoft Safety Scanner** är ett kostnadsfritt nedladdningsbart säkerhetsverktyg som söker på begäran och hjälper till att ta bort skadliga program och annan otäck programvara. Microsoft Safety Scanner ersätter inte en uppdaterad antiviruslösning, eftersom den inte erbjuder realtidsskydd och inte kan hindra en dator från att bli infekterad.

FOTNOTER

[4]Dessa data passerar alltid strikta integritet- och efterlevnadsgränser innan de används för säkerhets skull.

- **Microsoft Security Essentials** är en kostnadsfri och realtidsbaserad skyddsprodukt som är lätt att ladda ner och ger grundläggande, effektivt skydd mot virus och spionprogram för Windows Vista och Windows 7.

- **Microsoft System Center Endpoint Protection** (tidigare Forefront Client Security och Forefront Endpoint Protection) är en enhetlig produkt som skyddar företagsdatorer, bärbara datorer och serveroperativsystem mot skadliga program och annan otäck programvara. Den använder Microsoft Malware Protection Engine och Microsofts antivirussignaturdatabas för att ge realtidsskydd både enligt schema och på begäran.

- **Office 365** är Microsoft Offices prenumerationstjänst för organisationer och hemanvändare. Vissa prenumerationsplaner ger tillgång till Office 365 Advanced Threat Protection.

- **Windows Security** i Windows 10 söker igenom och tar bort skadliga program och oönskad programvara i realtid. Dessutom utnyttjar den senaste versionen av Windows omfattande kontextuella data som maskinkonfiguration, enhetens prestanda och hälsa och annan sådan information för att öka säkerheten för kunderna. Samtidigt ger vi kunderna möjlighet att bli mer informerade om sin integritet i Windows 10. Läs den här bloggen för att se några exempel på hur Microsoft gör det.

- **Windows Defender Advanced Threat Protection** är en tjänst som är inbyggd i Windows 10 Anniversary Update och senare versioner. Med den kan företagskunder identifiera, undersöka och åtgärda avancerade beständiga hot och dataintrång i sina nätverk.

- **Windows Defender Offline** är ett nedladdningsbart verktyg som kan användas för att skapa en startbar CD, DVD eller USB-flashenhet för att söka igenom en dator efter skadliga program och andra hot. Det erbjuder inte realtidsskydd och ersätter inte en uppdaterad lösning mot skadliga program.

- **Windows Defender SmartScreen**, en funktion i Microsoft Edge och Internet Explorer, skyddar användarna mot nätfiskewebbplatser och webbplatser där skadliga program lurar. Microsoft har en databas med webbplatser för nätfiske och skadliga program som rapporteras av användare av Microsoft Edge, Internet Explorer och andra Microsoft-produkter och -tjänster. När en användare försöker besöka en webbplats i databasen med filtret aktiverat, visar webbläsaren en varning och blockerar navigeringen till sidan.