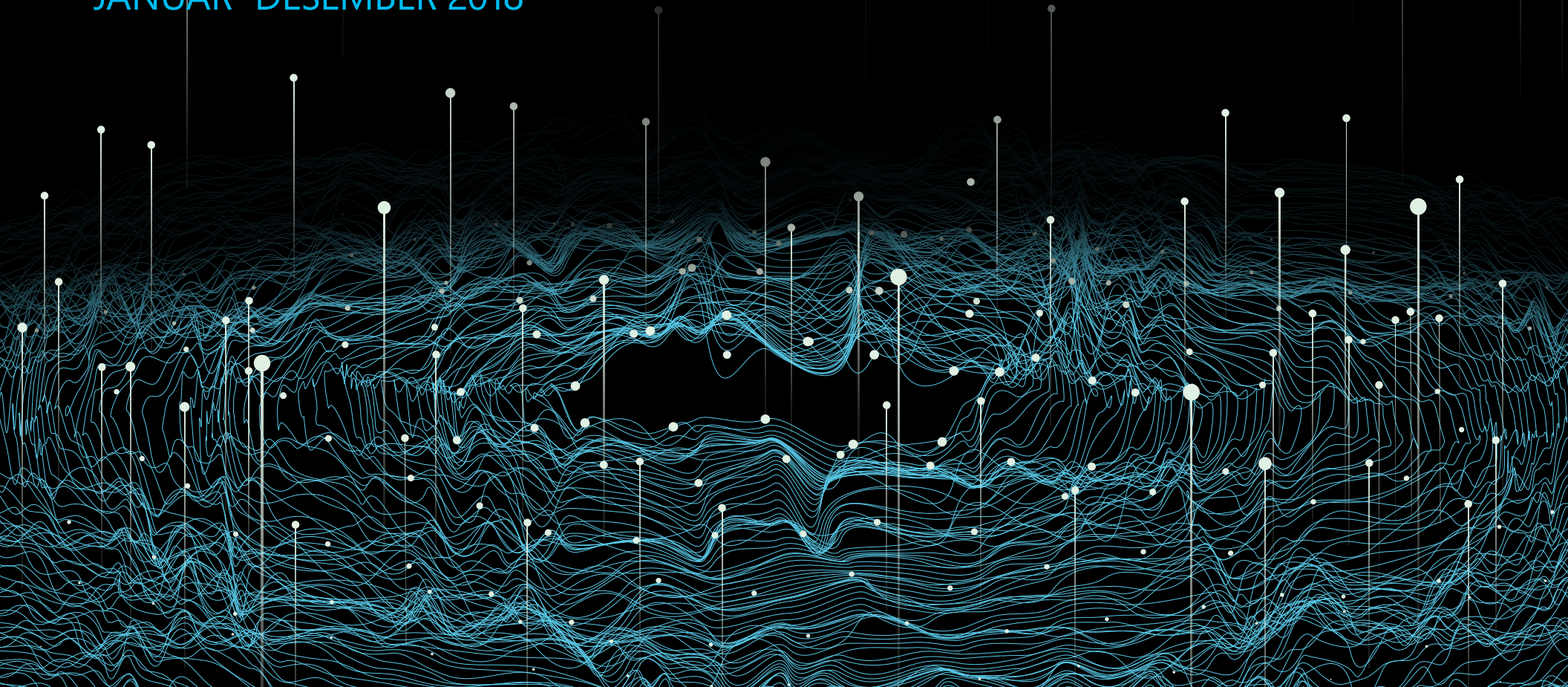




MICROSOFTS SIKKERHETSINTELLIGENSRAPPORT

VOLUM 24
JANUAR–DESEMBER 2018



Innhold



Dette dokumentet er bare ment som informasjon. MICROSOFT GIR INGEN GARANTIER, UTTRYKTE, UNDERFORSTÅTTE ELLER LOVBESTEMTE, NÅR DET GJELDER INFORMASJONEN I DETTE DOKUMENTET.

Dette dokumentet tilbys uten noen form for garanti. Informasjonen og synspunktene som uttrykkes i dokumentet, herunder nettadresser og andre henvisninger til nettsteder, kan endres uten varsel. Du har ansvaret for eventuelle risikoer ved bruk av det.

Opphavsrett © 2019 Microsoft Corporation. Med enerett.

Navn på reelle selskaper og produkter i dette dokumentet kan være varemerker tilhørende de respektive eierne.

Forfattere og bidragsytere

Abhishek Agrawal
informasjonsbeskyttelse

David Fantham
informasjonsbeskyttelse

Debraj Ghosh
markedsføring for Microsoft Security

Diana Kelley
løsningsgruppen for cybersikkerhet

Elia Florio
Windows Active Defense

Eric Avena
forskningsavdelingen for Windows Defender

Erik Douglas
forskningsavdelingen for Windows Defender

Francis Tan Seng
forskningsavdelingen for Windows Defender

Jonathan Trull
løsningsgruppen for cybersikkerhet

Joram Borenstein
løsningsgruppen for cybersikkerhet

Karthik Selvaraj
forskningsavdelingen for Windows Defender

Kasia Kaplinska
markedsføring for Microsoft Security

Kristina Laidler
responsavdeling for sikkerhetshendelser

Matt Duncan
Windows Active Defense-datateknikk og -analyse

Mark Simos
løsningsgruppen for cybersikkerhet

Paul Henry
Wadeware LLC

Pragya Pandey
markedsføring for Microsoft Security

Ram Pliskin
Azure Security

Ryan McGee
markedsføring for Microsoft Security

Seema Kathuria
løsningsgruppen for cybersikkerhet

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
forskningsavdelingen for Windows Defender

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Forord

Hei og velkommen til 24. utgave av Microsofts sikkerhetsintelligensrapport (SIR). Som profesjonell sikkerhetsarkitekt leser jeg rapporter som denne for å forstå landskapet bedre og få praktiske råd om hvordan jeg kan beskytte organisasjoner mer effektivt.

SIR-avdelingen har et klart opplæringsformål med denne rapporten: De ønsker å forbedre cybersikkerheten og har gått gjennom data for et helt år for å sile ut den viktigste lærdommen.

Det du leser i rapporten, er innsikt hentet fra et år med sikkerhetsdataanalyser og praktiske erfaringer. Blant de analyserte dataene finner vi 6,5 trillioner trusselsignaler som går gjennom Microsoft-skyen hver dag, samt forskningen og erfaringen til våre mange tusen sikkerhetsforskere og omfattende utrykningspersonell rundt om i verden. I 2018 brukte angripere en rekke skitne triks, både nye (kryptomyntutvinning) og gamle (nettfishing, i sine vedvarende forsøk på å stjele data og ressurser fra kunder og organisasjoner. Hybride angrep, som Ursnif-kampanjen, blandet sosiale og tekniske tilnærminger. Da beskyttelsen mot løsepengevirus – en høylytt og disruptiv angrepsform – ble smartere, gikk de kriminelle over til den mer skjulte, men fortsatt lønnsomme, aktiviteten kryptomyntutvinning.

Denne dreiningen kan være frustrerende fordi det oppleves som angriperne alltid ligger ett skritt foran. Men fra et annet perspektiv er faktisk dette en positiv historie. Du og andre som driver med cybersikkerhet, implementerte forsvarsteknikker som tvang angriperne til å endre sin foretrukne nyttelast og bevege seg bort fra løsepengevirus.

Et annet område der cyberkriminelle økte sin aktivitet, er forsyningskjeden. Et av de mest bemerkelsesverdige eksemplene på dette er «Dofoil coin-miner»-utbruddet, som rammet 6. mars 2018 og ble startet av en infisert node-til-node-app. Bekymringene angående forsyningskjeden gjaldt ikke bare apper, men også skyen og inkluderte skadelige nettleserutvidelser, kompromitterte Linux-repositorier og flere forekomster av moduler med bakdør. For å ta tak i denne trusselen går organisasjoner i retning av en transparent og klarert forsyningskjedemodell.

Data er supert, men noen ganger er det nyttig å finne ut hva som egentlig skjedde i en organisasjon. Det er derfor vi har tatt med felterfaringer fra vårt Detection and Response Team (DART). Disse inkluderer hvordan et stort produksjonsselskap kunne implementere kontroller for å blokkere en nettfiskingskampanje med flere faser som hadde plaget dem i månedsvis, og finansorganisasjoner som endelig klarte å utrydde trusselaktører fra systemene sine ved hjelp av avanserte undersøkelsesverktøy og endepunktsovervåking.

Sist men ikke minst: Nettfiskingsklikk fortsatte å gå opp – men maskinlæringsmodeller blir flinkere til å stoppe nettfiskingsangrep før de treffer brukerbokser, og til å forebygge skade etter klikk hvis de skulle gjøre det. Flere gode nyheter? Et økende antall selskaper innfører flerfaktorløsninger for å forhindre at nettfiskings-e-poster ikke klarer å stjele legitimasjonen de er ute etter.

Angripere ser etter muligheter, så jo mer vi vet om deres teknikker og spionasje, desto bedre rustet er vi til å bygge forsvar og reagere raskt. Små, viktige tiltak kan utgjøre en enorm forskjell i den generelle cybersikkerheten til en organisasjon. Derfor inneholder denne rapporten ikke bare grundig innsikt i det skiftende landskapet av skadelig programvare, men også anbefalte tiltak og gode fremgangsmåter. Da jeg drev med cyberforsvar i felten, var det akkurat dette jeg trengte i min kamp mot skurkene. Vi håper du har nytte av det også.

Diana Kelley

Microsoft Cybersecurity Field CTO

PS Vi er alltid opptatt av å forbedre SIR. Hvis du ønsker å gi tilbakemeldinger, er det bare å kontakte oss.



DEL I

Løsepengevirus, utvinning av kryptovaluta og penger

De store sikkerhetshendelsene i 2017 handlet for det meste om løsepengevirus. Høyprofilerte og verdensomspennende utbrudd av WannaCrypt og Petya gjorde for alvor løsepengevirus – en type skadelig programvare som låser eller krypterer datamaskiner, for så å kreve penger for å gjenopprette tilgang – allment kjent, og mange mente at problemet bare ville øke i fremtiden. I stedet **var det en betydelig nedgang i løsepengevirusangrep i 2018.**

Nedgangen i oppdagelse av løsepengevirus skyldtes delvis bedre gjenkjenning og opplæring, som gjorde det vanskeligere for angriperne å oppnå gevinst. Som følge av dette begynte angriperne å satse mindre på løsepengevirus og mer på for eksempel utvinning av kryptovaluta, som bruker ofrenes dataressurser til å lage digitale penger til angriperne. Skiftet demonstrerer hvor grunnleggende opportunistiske de fleste profittorienterte nettkriminelle er: De har en tendens til å gå etter lettjente penger, og når cyberkriminalitetens økonomi endres, følger de raskt etter.

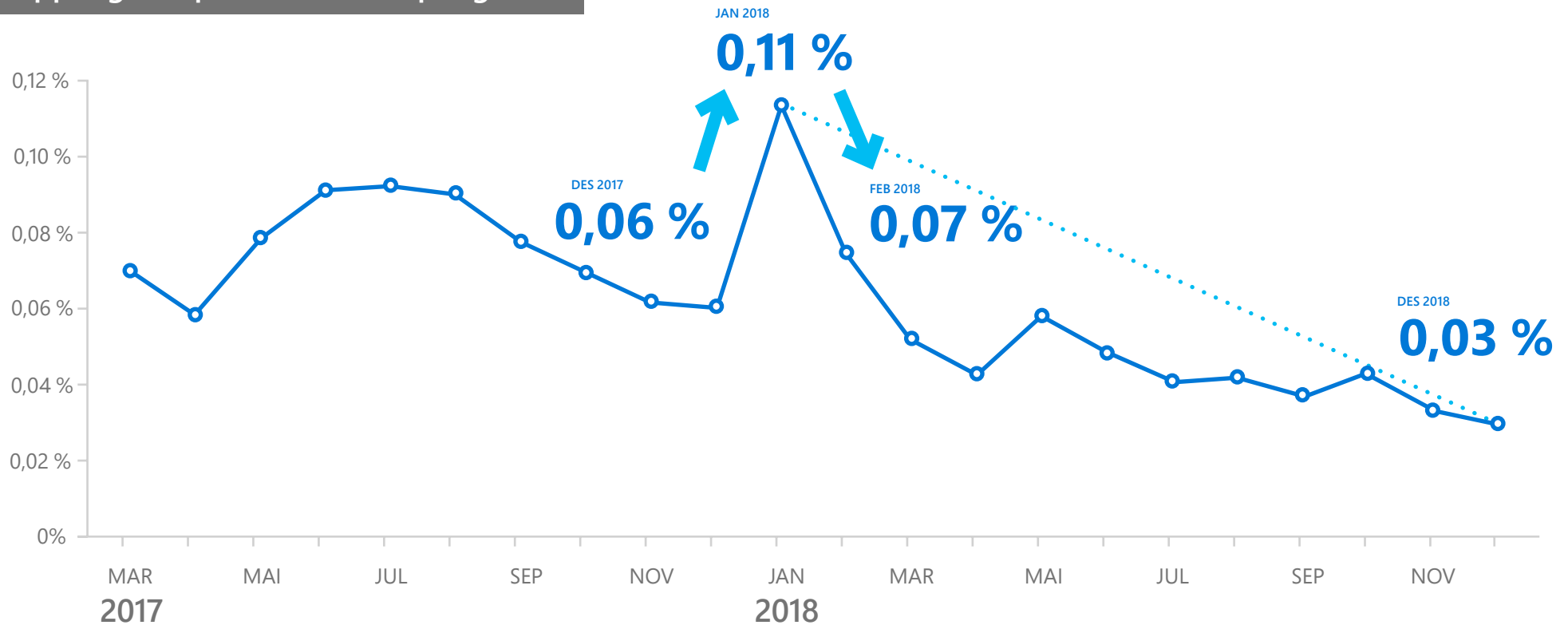
NEDGANG I ANGREP FRA LØSEPENGEVIRUS

For over ti år siden ble hackerne og spilloppmakerne som dominerte den tidlige bruken av skadelig programvare, fortrent av organisert kriminalitet og andre profittorienterte interesser. Mens tidlige utbrudd av skadelig programvare ofte var prangende og åpenlyse, er aktiviteten til profittorientert skadelig programvare vanligvis mer nedtonet for å unngå oppmerksomhet, slik at de kriminelle kan drive med ondsinnet aktivitet – sende søppelpost, stjele sensitiv informasjon, utføre tjenestenektangrep osv. – så lenge som mulig.

Løsepengevirus snur denne trenden. I stedet for å prøve å forbli uoppdaget innebærer løsepengevirus at ofrene åpenlyst nektes tilgang til datamaskiner og viktige filer helt til de betaler løsepenger (og ofte også etterpå. Angripere slipper ofte ikke kontrollen over datamaskiner selv om løsepengene blir betalt).

Løsepengevirus nådde en topp i 2017, og det så ut til at denne typen åpne angrep skulle representere en ny fase i angrepsteknikker. Men nyere data tyder på at løsepengevirus kan være på tilbakegang, og at angriperne i større grad vender tilbake til en mer luskende og hemmelig aktivitet. De forsøker å holde seg under radaren for mer effektivt å utføre angrep som blant annet kryptovalutautvinning. Men selv om det har vært en nedgang i frekvensen av oppdagede løsepengevirus, betyr ikke dette nødvendigvis at alvorlighetsgraden av angrepene har gått ned.

Oppdagelsesprosent for løsepengevirus

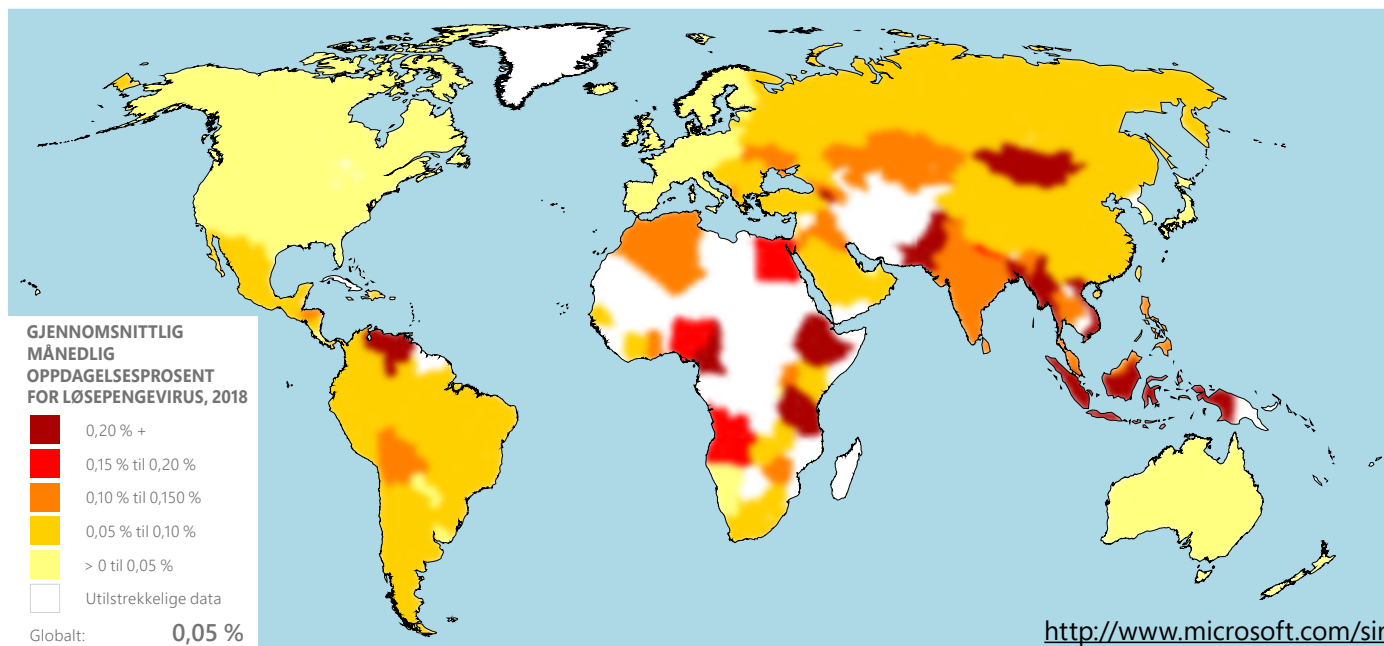


Oppdagelsesprosent for løsepengevirus **falt med ca. 60 prosent** mellom mars 2017 og desember 2018, med periodiske tilbakevendende økninger i samme periode.

▲ FIGUR 1.

Oppdagede løsepengevirus fra mars 2017 til desember 2018

Det er sannsynligvis mange grunner til denne generelle nedgangen, selv om Microsofts sikkerhetsforskere mistenker at en primærfaktor er at både sluttbrukere og organisasjoner blir mer oppmerksomme på og bedre til å håndtere trusler fra løsepengevirus – som blant annet vil si at de er mer forsiktige og flinkere til å sikkerhetskopiere viktige filer, slik at filene kan gjenopprettes hvis de er kryptert av løsepengevirus. Og som beskrevet tidligere er cyberkriminelle opportunistiske.



FIGUR 2.

Gjennomsnittlig månedlig oppdagelsesprosent for løsepengevirus på verdensbasis etter land/område i 2018

LAND MEST PÅVIRKET AV LØSEPENGEVIRUS: ETIOPIA



Gjennomsnittlig månedlig oppdagelsesprosent:

0,77 %

De fem stedene med høyest gjennomsnittlig månedlig oppdagelsesprosent for løsepengevirus i 2018 var Etiopia (gjennomsnittlig månedlig oppdagelsesprosent for løsepengevirus: 0,77 prosent), Mongolia (0,46), Kamerun (0,41), Myanmar (0,33) og Venezuela (0,31), som hver hadde en gjennomsnittlig månedlig oppdagelsesprosent for løsepengevirus på 0,31 prosent eller høyere i perioden.¹ For noen år siden var det høyest oppdagelsesprosent i rike land og områder i Europa og Nord-Amerika, men nå når løsepengevirus ikke lenger er angripernes foretrukne metode, ser vi at mønsteret for oppdagede løsepengevirus ligner mer på mønsteret for skadelig programvare som helhet.

Stedene med lavest månedlig oppdagelsesprosent for løsepengevirus i 2018 var Irland (0,01), Japan (0,01), USA (0,02), Storbritannia (0,02), og Sverige (0,02 prosent), som hver hadde en oppdagelsesprosent på 0,02 prosent eller lavere i samme periode. Steder med lav månedlig oppdagelsesprosent har vanligvis moden infrastruktur og veletablerte programmer for å beskytte viktig infrastruktur og kommunisere med innbyggerne om grunnleggende sikkerhet.

FOTNOTER

¹ Oppdagelsesprosent vil si prosentandelen av datamaskiner som kjører Microsoft-produkter med sikkerhet i sanntid og rapporterer oppdagelse av skadelig programvare. At man oppdager en trussel, betyr ikke at datamaskinen har blitt infisert. Bare datamaskiner med brukere som har valgt å oppgi data til Microsoft, er med i beregningen av oppdagelsesprosent.

UTVINNING AV KRYPTOVALUTA PÅ VEI OPPOVER

Kryptovaluta er virtuelle penger som kan brukes til å kjøpe og selge varer og tjenester anonymt, både på nettet og i den fysiske verden. Det finnes mange forskjellige typer kryptovalutaer, men de er alle basert på blokkjede-teknologi, der hver transaksjon registreres i en distribuert hovedbok som vedlikeholdes av tusener eller millioner av datamaskiner over hele verden. Nye kryptomynter opprettes, eller «utvinnes», av datamaskiner som utfører komplekse beregninger. Disse beregningene verifiserer også blokkjede-transaksjoner.

Utvinning av kryptomynter kan være svært lukrativt – i 2018 var en enkelt bitcoin-mynt, den eldste og mest populære kryptovalutaen, verdt flere tusen amerikanske dollar – men det kan være svært ressurskrevende å utføre de nødvendige beregningene, og ressursbruken bare øker på for hver nye kryptomynt som utvinnes. For populære valutaer som bitcoin er det nesten umulig å utvinne kryptomynter lønnsomt uten tilgang til enorme dataressurser. Dette gjør at aktiviteten er godt utenfor rekkevidde for de fleste enkeltpersoner og mindre grupper. Av denne grunn har angripere som søker ulovlig inntjening, i økende grad tatt i bruk skadelig programvare som gjør det mulig å bruke andres datamaskiner til å hjelpe til med å utvinne kryptomynter. Slik kan de utnytte databehandlingskraften til hundretusenvís av datamaskiner i stedet for en eller to. Selv når en mindre infeksjon oppdages, kompliserer anonymiteten til kryptovaluta arbeidet med å spore opp de ansvarlige partene.

I 2018 var gjennomsnittlig månedlig oppdagelsesprosent for utvinning av kryptovaluta 0,12 prosent på verdensbasis, sammenlignet med bare 0,05 prosent for løsepengevirus. Mange faktorer bidrar til økt popularitet av utvinning som en nyttelast for skadelig programvare. I motsetning til løsepengevirus krever ikke kryptovaluta inndata fra brukeren: Det jobber i bakgrunnen, mens brukeren utfører andre oppgaver eller er borte fra datamaskinen, og det blir kanskje ikke lagt merke til i det hele tatt med mindre det reduserer datamaskinens ytelse i tilstrekkelig grad. Derfor er det mindre sannsynlig at brukerne gjør noe for å fjerne trusselen, og aktiviteten kan fortsette til fordel for angriperen i en lengre periode.

Lett tilgjengelighet av produkter for skjult utvinning av mange kryptovalutaer er en annen pådriver av trenden. Terskelen for å starte er lav på grunn av den omfattende tilgjengeligheten av programvare, som cyberkriminelle pakker inn som skadelig programvare som leveres til intetanende brukeres datamaskiner. De armerte utvinnerne blir deretter distribuert til ofre ved hjelp av mange av de samme teknikkene som angripere bruker for å levere andre trusler, slik som sosial manipulering, utnyttelse og tilfeldig nedlasting. Etter at programvaren for utvinning er installert, kjører den i bakgrunnen på offerets datamaskin for å utføre blokkjede-behandling – og angriperen høster gevinsten.

GJENNOMSNTTLIG MÅNEDLIG OPPDAGELSESPROSENT FOR LAND SOM ER MEST BERØRT AV UTVINNING AV KRYPTOVALUTA



Etiopia:

5,58 %



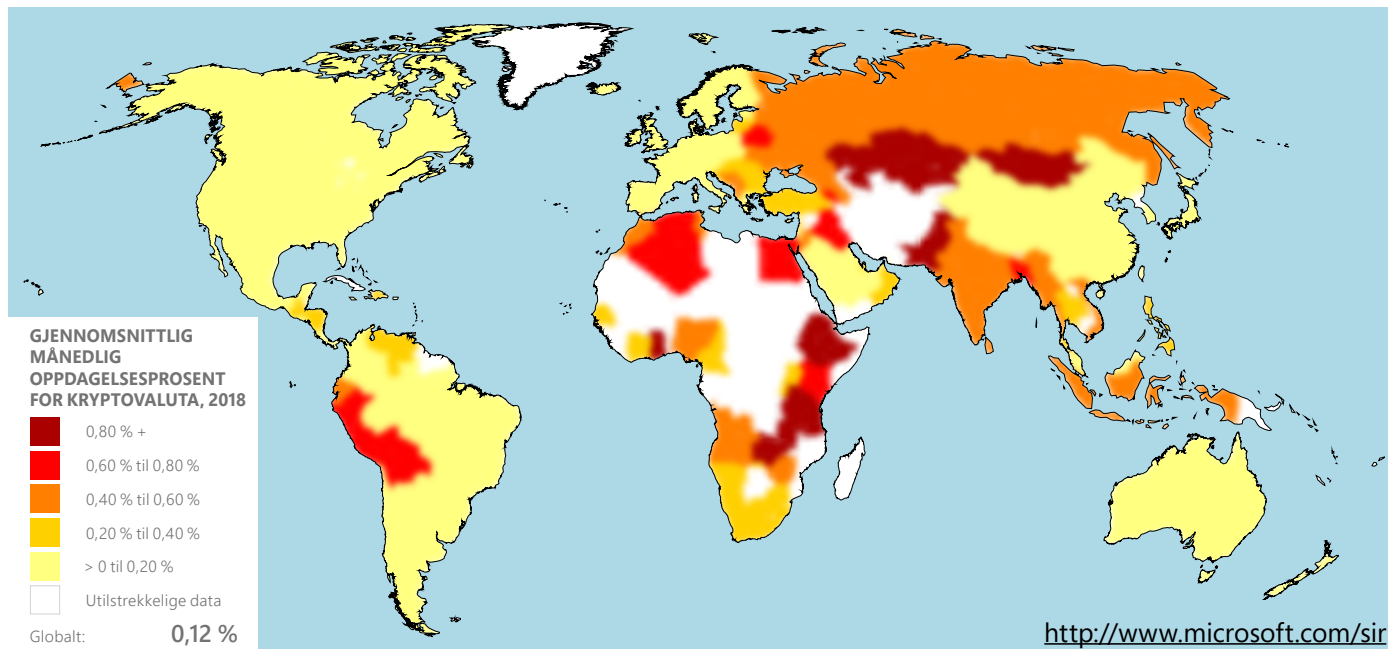
Tanzania:

1,83 %



Pakistan:

1,47 %



◀ **FIGUR 3.**

Gjennomsnittlig månedlig oppdagelsesprosent for utvinning av kryptovaluta på verdensbasis etter land/område i 2018

GJENNOMSNTTLIG MÅNEDLIG OPPDAGELSESPROSENT FOR LAND SOM ER MINST BERØRT AV UTVINNING AV KRYPTOVALUTA



Irland:

0,02 %



Japan:

0,02 %



USA:

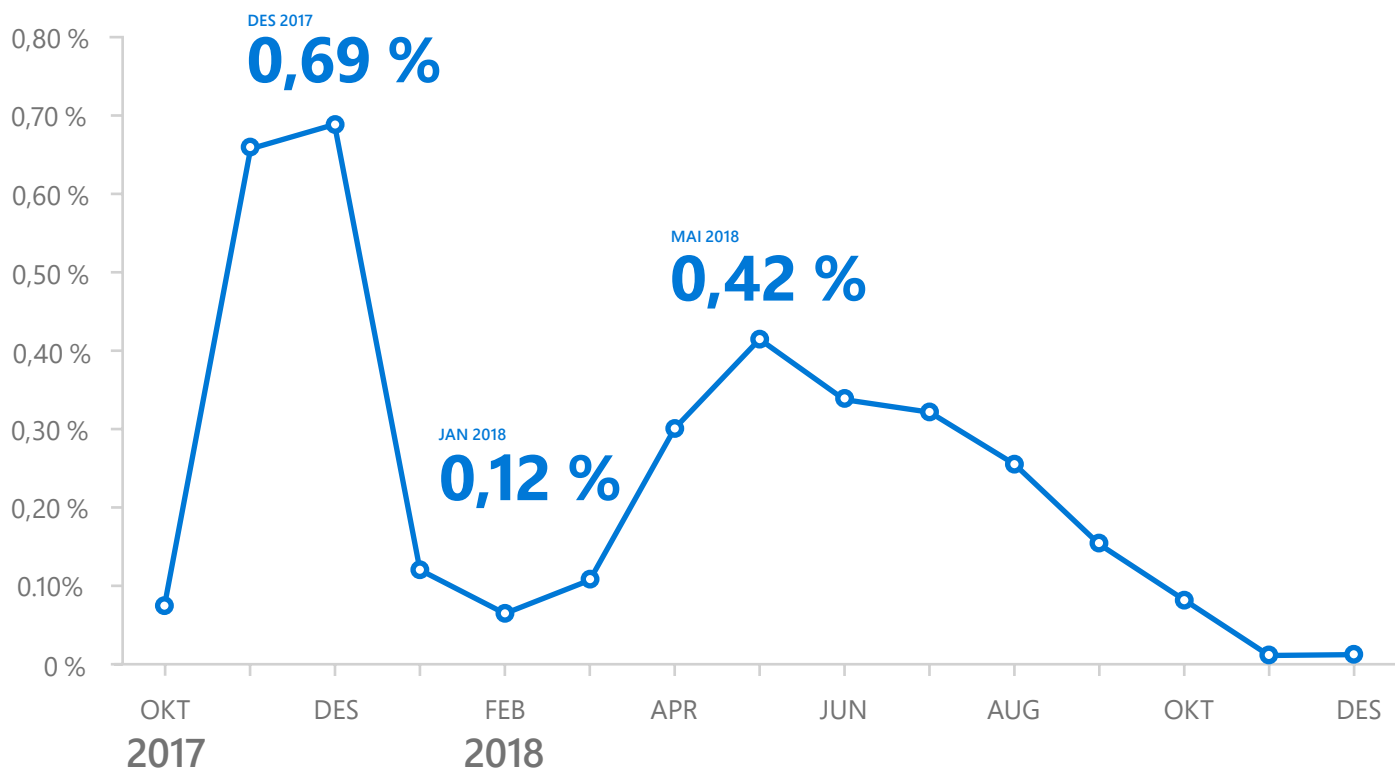
0,02 %

De fem stedene med høyest månedlig oppdagelsesprosent for utvinning av kryptovaluta i 2018 var Etiopia (5,58), Tanzania (1,83), Pakistan (1,47), Kasakhstan (1,24), og Zambia (1,13), som hver hadde en gjennomsnittlig månedlig oppdagelsesprosent på ca. 1,13 prosent eller høyere i perioden. Stedene med månedlig oppdagelsesprosent for utvinning av kryptovaluta i 2018 var Irland, Japan, USA og Kina, som hver hadde en gjennomsnittlig månedlig oppdagelsesprosent på ca. 0,02 prosent i perioden.

NETTLESERBASERT UTVINNING AV KRYPTOVALUTA: EN NY TYPE TRUSSEL

Statistikken som presenteres i denne delen, involverer skadelig utvinning av kryptovaluta som er utformet for å bli installert på ofres datamaskiner som skadelig programvare. Men noen av de mest betydningsfulle truslene om utvinning av kryptovaluta skjer utelukkende i nettlesere og trenger ikke å bli installert i det hele tatt. En rekke tjenester annonserer nettleserbasert utvinning av kryptovaluta som en måte for eiere av nettsteder å tjene penger på trafikken til nettstedene på uten bruk av reklame. Eiere av nettsteder skal liksom legge til JavaScript-kode på sidene sine som utvinner kryptovaluta i bakgrunnen mens en bruker besøker nettstedet, og inntektene deles mellom eieren av nettstedet og tjenesten. Dessverre har angripere vært raske til å dra nytte av disse tjenestene for å utvinne kryptovaluta uten

Oppdagelsesprosent for Brocoiner



å innhente samtykke fra sluttbrukerne, ofte ved å ødelegge for lovlige nettstedene og sette inn skadelig utvinningskode i kildekoden deres. Disse nettleserbaserte utvinningene trenger ikke å skade sluttbrukerens datamaskin i det hele tatt, og de kan kjøre på alle plattformer med en JavaScript-kompatibel nettleser. I likhet med trojanere som utvinner kryptovaluta, kan nettleserbasert utvinning betydelig redusere datamaskinens ytelse og overforbruke elektrisitet mens en bruker besøker en berørt nettside.

FIGUR 4.

Oppdagelsesprosent for Brocoiner, den mest utbredte nettleserbaserte utvinningen av kryptovaluta

VIRKNINGEN AV UØNSKET UTVINNING AV KRYPTOVALUTA

Den mest åpenbare trusselen ofrene står overfor fra skjult utvinning av kryptovaluta, er forbruket av dataressurser, som kan føre til overforbruk av elektrisitet og betydelig redusere datamaskinens ytelse. Brukere og organisasjoner står også overfor andre risikoer fra utvinning av kryptomynter, blant annet følgende:

- ⚠ **Å få et fotfeste for å utrette større skade i fremtiden.**
I likhet med andre former for skadelig programvare kan utvinning av kryptovaluta være et inngangspunkt for angripere. Mens datamaskinen utvinner kryptovaluta i bakgrunnen, kan cyberkriminelle lære om miljøet og muligens avdekke hull i sikkerheten for å utnytte maskinen til andre formål.
- ⚠ **Internett-tilkoblede enheter kompromitteres og blir omgjort til roboter for utvinning av kryptovaluta.**
Mange slike enheter mangler innebygd sikkerhet – for eksempel gjenkjenning av trusler om skadelig programvare – som kan gjøre dem til ønskelige mål for angripere.
- ⚠ **Maskiner skades.**
Programvare for utvinning av kryptovaluta som kjører kontinuerlig i måneder eller lenger, kan svekke ytelsen, og varmen som genereres av overdreven strømforbruk og CPU-utnyttelse, kan skade datamaskiner.

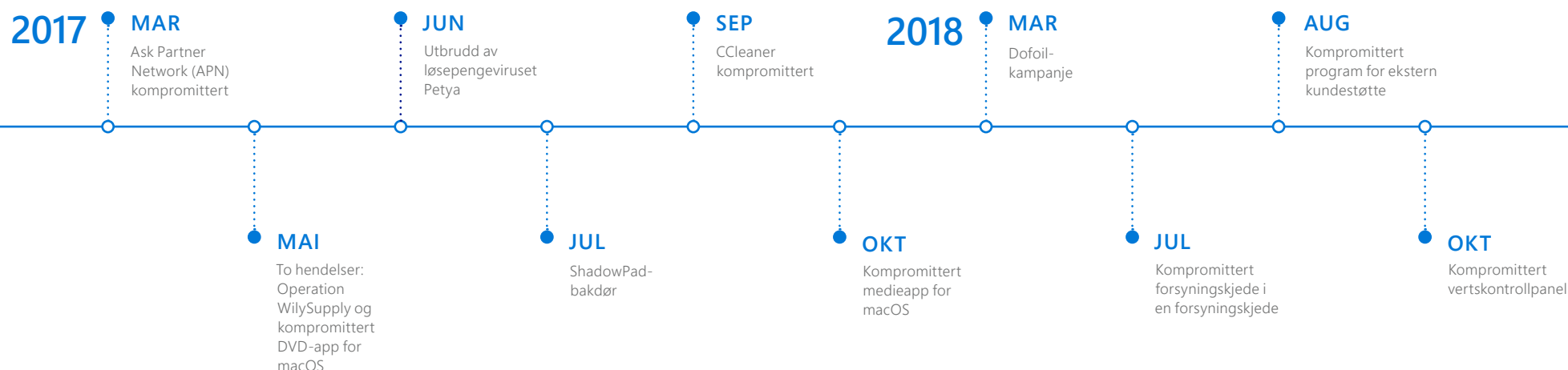


DEL II

Forsyningskjeder for programvare i fare

I årevis har Microsoft sporet trusselaktører som bruker [kompromittert forsyningskjede](#) som et inngangspunkt for angrep. I et forsyningskjedeangrep konsentrerer angriperen seg om å skade utviklings- eller oppdateringsprosessen til en lovlig programvareutgiver.

Hvis det lykkes, kan angriperen innlemme en kompromittert komponent i en lovlig app eller oppdateringspakke som deretter blir distribuert til programvarens brukere. Den skadelige koden kjører deretter med samme klarering og tillatelser som programvaren. De [siste års økende antall angrep på forsyningskjede for programvare](#) har blitt et viktig tema i mange cybersikkerhetssamtaler og er en primærkilde til bekymring i mange IT-avdelinger.



ALVORLIGE ANGREP PÅ FORSYNINGSKJEDE FOR PROGRAMVARE I 2017

I 2017 utgjorde angrep på forsyningskjede en rekke svært profilerte hendelser, og særlig [utbruddet av løsepengeviruset Petya](#) i juni, som ble sporet til innledende infeksjoner fra en kompromittert oppdateringsprosess for en populær app for skatteregnskap i Ukraina. I mai manipulerte [Operation WilySupply](#) oppdateringen av en tekstbehandlingsprogramvare til å installere en bakdør i målorganisasjoner i økonomi- og IT-sektorene. I juli ble en bakdør kalt [ShadowPad](#) gjemt i en programvarepakke for serveradministrasjon, og den tillot angripere å installere ekstra nyttelast for skadelig programvare som ble brukt til datatyveri og andre skadelige aktiviteter. I september ble infrastrukturen til det populære gratisverktøyet CCleaner kompromittert, og en [versjon med bakdør](#) ble levert til brukerne.

▲ FIGUR 5.

Angrep på forsyningskjede for programvare i 2017 og 2018

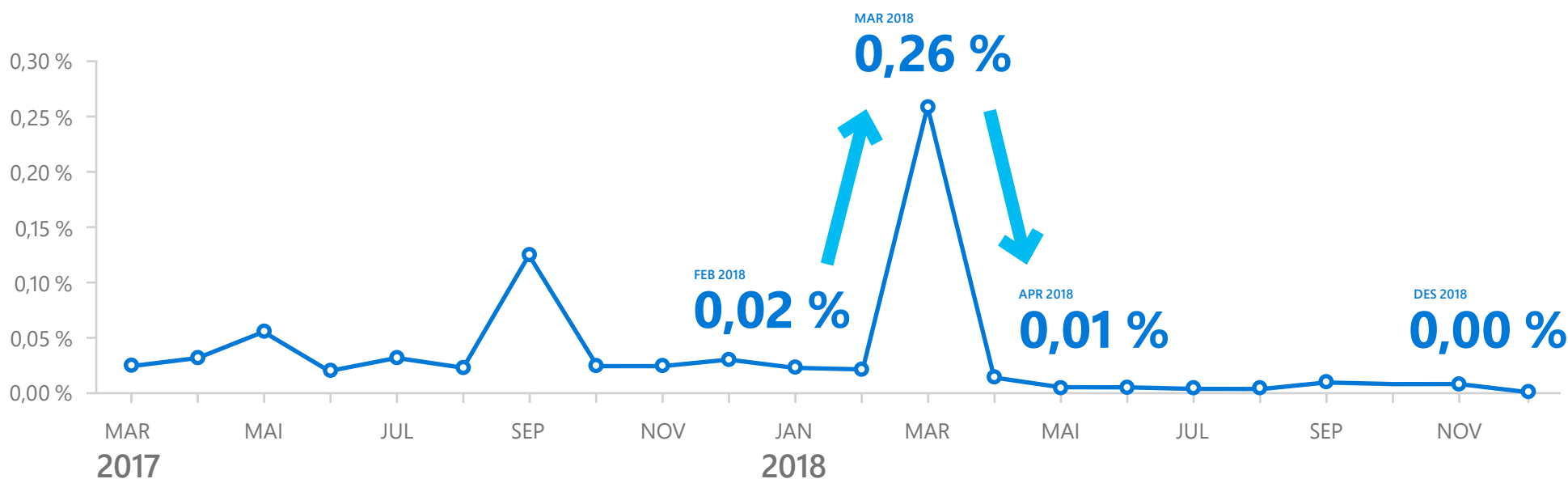
ANGREP PÅ PROGRAMVARE FOR FORSYNINGSKJEDE I 2018 – ÅRSAKER OG KONSEKVENSER

Det første alvorlige angrepet på forsyningskjedeprogramvare i 2018 skjedde 6. mars, da Windows Defender ATP blokkerte en stor annonsekampanje for å levere trojaneren Dofail (også kjent som Smoke Loader). Den store kampanjen for skadelig programvare ble sporet til en infisert node-til-node-app. Appens oppdateringspakke ble erstattet av en ondsinnet versjon som lastet ned skadelig kode, som senere installerte Dofail. Den avanserte trojaneren inneholdt en nyttelast for kryptomyntutvinning med avanserte injeksjonsteknikker for flere prosesser, utholdenhetsmekanismer og unndragelsesmetoder.

FIGUR 6.

Oppdagelse av Dofail (Smoke Loader) i 2018 viser en topp av blokkerte forekomster i mars

Oppdagelsesprosent for Dofail



I løpet av de første 12 timene av kampanjen blokkerte Windows Defender Antivirus mer enn 400 000 infeksjonsforsøk på verdensbasis. 73 prosent av globale oppdagelser skjedde i Russland, og Tyrkia og Ukraina registrerte henholdsvis 18 og 4 prosent.

Flere angrep ble oppdaget ved hjelp av kompromittert forsyningskjedeprogramvare som leveringsmekanisme i 2018, inkludert dem som er beskrevet i følgende tabell:

Periode	Angrep	Beskrivelse	Berørt programvare
Mars 2018	Dofail-kampanjen for kryptomyntutvinning (rapportert av Microsoft).	Angripere skadet oppdateringsprosessen for en node-til-node-app for å installere Dofail, som i sin tur installert skadelig programvare for kryptomyntutvinning.	Node-til-node-app.
Juli 2018	Kompromittert forsyningskjede i en forsyningskjede (rapportert av Microsoft).	Angripere skadet infrastrukturen som ble delt mellom en leverandør av en PDF-app og en av leverandørens programvareleverandørpartnere.	PDF-app og partnerleverandør.
August 2018	Kompromittert program for ekstern kundestøtte (Operation Red Signature, rapportert av Trend Micro og IssueMakersLab).	Oppdateringsserveren til en leverandør av eksterne kundestøtteløsninger ble manipulert til å levere et verktøy for ekstern tilgang kalt 9002 RAT.	Program for ekstern kundestøtte.
Oktober 2018	Kompromittert løsning for vertskontrollpanel (rapportert av ESET).	Installasjonsskriptet for en løsning for vertskontrollpanel ble endret for å stjele legitimasjon.	Løsning for vertskontrollpanel.

◀ FIGUR 7.

Andre angrep på forsyningskjede for programvare i 2018

TILLIT I FARE

Forsyningskjedeangrep er lumske fordi de utnytter tilliten som brukere og IT-avdelinger har til programvaren de bruker. Den kompromitterte programvaren er ofte signert og sertifisert av leverandøren, og viser gjerne ikke at noe er galt, noe som gjør det betydelig vanskeligere å oppdage infeksjonen. De kan skade forholdet mellom forsyningskjeder og deres kunder, enten sistnevnte er bedrifts- eller hjemmebrukere. Ved å infisere programvare og undergrave infrastruktur for levering eller oppdatering kan forsyningskjedeangrep påvirke integriteten og sikkerheten til varer og tjenester som organisasjoner tilbyr.

Forsyningskjedeangrep har påvirket et bredt spekter av programvare og målrettede organisasjoner i ulike sektorer og geografiske områder. Trusselen fra forsyningskjedeangrep er et problem i hele bransjen, og krever oppmerksomhet fra flere interessenter, blant annet programvareutviklere og leverandører som skriver koden, systemadministratorene som administrerer programvareinstallasjoner, og informasjonssikkerhetsfellesskapet som finner disse angrepene og lager løsninger for å beskytte mennesker og programvare mot dem.

IKKE BARE PROGRAMVARE: KOMPROMITTERING AV FORSYNINGSKJEDE VIA SKYOBJEKTER

Forsyningskjedeangreps mulighet til å undergrave tilliten forsterkes og gjøres enda mer kompleks i skyen. Flere tilfeller av kompromitterte skyobjekter, tjenester og infrastruktur i 2018 fremhever denne kompleksiteten:

- Infiserte Chrome-utvidelser som installerte skadelig «click-fraud»-programvare (rapportert av [ICEBRG](#))
- Ulike kompromitterte Linux-repositorier (rapportert i noen nettforumer)
- Ondsinne WordPress-programtillegg som brukes til ulike skadelige aktiviteter, blant annet til å tillate angripere å publisere innhold på WordPress-nettsteder (rapportert av [Wordfence](#))
- Ondsinne Docker-bilder som inneholdt et skript for å laste ned skadelig programvare for utvinning av kryptovaluta, og lastet opp til Docker Hub-konto (rapportert av [Fortinet](#) og [Kromtech](#))
- En ondsinnet pakke for typosquatting i det offisielle Python-repositoriet. Pakken inneholdt et ondsinnet skript som laster ned skadelig programvare som brukes til å kapre adresser for kryptovalutautvinning på utklippstavlen (rapportert på [Medium](#))
- Kompromittert skript i StatCounter som gjorde det mulig for angripere å injisere et skadelig skript på nettsteder som bruker StatCounter (rapportert av [ESET](#))

- Flere tilfeller av npm-moduler med bakdør ([The npm-bloggen](#), [Medium](#)) som hvis de utnyttes for eksempel kan føre til situasjoner der en angriper skriver inn vilkårlig kode i en aktiv server og kjører den.

Disse hendelsene viser hvordan kompromittert forsyningskjede kan utvide angrepsflaten vesentlig. Hvis de ikke sikres, kan skyobjekter fungere som uventede inngangsvektorer. Docker Hub-hendelsen involverte for eksempel en skadelig konto som lastet opp Docker-bilder som inneholdt en skjult bakdør for kryptomyntutvinning. Docker-bildene ble driftet på Docker Hub i nesten et år og ble lastet ned millioner av ganger og brukt av intetanende administratorer og brukere.

Forsyningskjederisikoer utvides til kode i skyen, åpen kildekode, nettbiblioteker, beholdere og andre objekter i skyen. Disse risikoene, kombinert med den høye graden av variasjon blant forsyningskjedehendelser for programvare og maskinvare som har kommet frem, gjør forsyningskjedeangrep til en bred trusselkategori. Selv om det ikke finnes noen enkelt løsning for hele spekteret av slike angrep, må organisasjoner bygge [forebyggende beskyttelse og registrering av angrep etter brudd](#) for forsyningskjedeangrep fra kompromittert maskinvare- og programvareleverandører, andre leverandører og anskaffelser, leverandører av programvare med åpen kildekode samt leverandører av skytjenester og infrastruktur.

Gransking av cyberkriminalitet med DART

Microsoft Detection and Response Team (DART) er en global avdeling med eksperter på cybersikkerhet og utrykningspersonell som hjelper organisasjoner med oppdagelse, etterforskning og respons på hendelser som gjelder cybersikkerheten. Denne delen fremhever noen av kundesakene som DART håndterte i fjor. Den illustrerer vanlige angrepstrender og hvordan Microsoft og kundene var i stand til å hindre dem.

PROFESJONELL TJENESTEORGANISASJON OPPLEVDE STATLIG ANGREP SOM HENTET UT DATA

En profesjonell tjenesteorganisasjon ble påvirket av en avansert, statlig sponset Advanced Persistent Threat (APT) som fikk tilgang til privilegert legitimasjon i organisasjonen. Angriperne fikk tilgang til nettverket ved hjelp av et angrep med passordspray der de brukte et lite antall svake eller mye brukte passord (f.eks. «p@ssord» eller «123456») for å målrette mot et stort antall brukerkontoer og få administratorlegitimasjon for Office 365. (Angrep med passordspray brukes for å unngå å bli oppdaget ved å begrense antall påloggingsforsøk for hver konto.) Etter å ha infiltrert nettverket utførte APT utførlig, automatisert uttrekking av data fra ansattes postbokser. Til tross for flere interne forsøk på å kaste dem ut, forble motstanderen i nettverket i mer enn 200 dager. Som en del av angrepet utnyttet motstanderen organisasjonens forsyningskjedeprogramvare og automatiserte uttrekking av data.

Fordi de mistenkte et sikkerhetsbrudd vedrørende kundedata, engasjerte organisasjonen DART-avdelingen til å granske og forhindre ytterligere skade. DART identifiserte målrettede Office 365-postbokssøk, kompromitterte kontoer og kanaler for angriperkommando og -kontroll. Viktig kundelærdom fra denne hendelsen var å ta i bruk kontroller for å beskytte skytjenester mot identitetsbaserte trusler og angripere. Organisasjonen tok i bruk flerfaktorgodkjenning (MFA), betinget tilgang for bestemte skyapper og logging av Office 365. For ytterligere å beskytte seg mot lignende trusler i fremtiden kan organisasjonen også bruke en løsning for Endpoint Threat Detection and Response (EDR) for å oppdage angripere som kanskje prøver å utnytte nettverket. Videre har vi anbefalt at denne



organisasjonen utnevner et organ for skystyring eller en global identitetsavdeling som administrerer og håndhever riktige retningslinjer for brukergodkjenning, slik at organisasjonen har oversikt over sikkerheten og mer effektivt kan redusere risikoen.



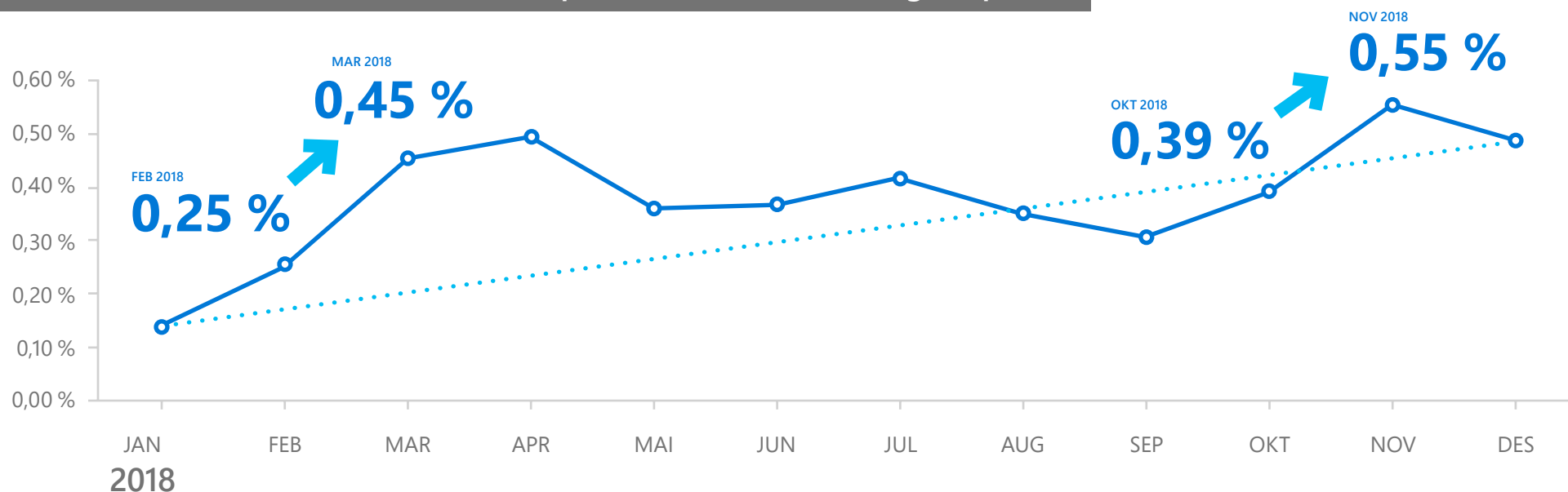
DEL III

Nettfisking er fortsatt utbredt

I 2018 har Microsofts trusselanalytikere sett bevis på at angripere fortsetter å bruke nettfisking som en foretrukket angrepsmetode. Nettfisking ser ut til å være et problem i all overskuelig fremtid fordi det innebærer menneskelige beslutninger og dømmekraft i møte med cyberkriminelles vedvarende innsats med å lure ofre.

Nettfiskingsraten er fremdeles stigende

Prosentandel av alle innkommende e-poster som er nettfiskings-e-poster



NETTFISKING FORTSETTER Å VÆRE EN FORETRUKKET ANGREPSVEKTOR I 2018

Microsoft analyserer og skanner mer enn 470 milliarder e-poster i Office 365 hver måned for å oppdage nettfisking og skadelig programvare, noe som gir analytikere betydelig innsikt i angrepstrender og -teknikker. Andelen av inngående e-poster som var nettfiskingsmeldinger, økte med 250 prosent mellom januar og desember 2018. Nettfisking er fortsatt en av de fremste angrepsvektorene som brukes til å levere skadelig nulldays nyttelast til brukerne, og Microsoft fortsetter å kjempe mot disse angrepene med flere funksjoner for nettfiskingsbeskyttelse, oppdagelse, undersøkelse og respons for å sikre brukerne.

▲ FIGUR 8.

Nettfiskings-e-poster i 2018

Utvikling av metoder for nettfiskingsangrep

Etter som verktøy og teknikker som brukes til å beskytte mot nettfisking, blir mer avanserte, tvinges angriperne til å tilpasse seg. Nettfiskingsangrep har blitt stadig mer polymorfe, noe som betyr at angripere ikke bruker en enkelt nettadresse, et enkelt domene eller en enkelt IP-adresse for å sende e-post, men gjør bruk av en variert infrastruktur med flere angrepspunkter. Selve angrepene har også utviklet seg, med moderne nettfiskingskampanjer som spenner fra korttidsangrep som er aktive bare noen minutter, til mye lengre kampanjer med høyt volum. Andre former er serielle angrepsvarianter, hvor angripere sender et lite volum av e-post i flere etterfølgende dager.

I tillegg har Microsoft observert en trend der angripere bruker vertsbasert infrastruktur og annen offentlig skyinfrastruktur, noe som gjør det enklere å unngå oppdagelse ved å skjule seg blant lovlige nettsteder og ressurser. For eksempel vil angripere i økende grad bruke populære nettsteder og tjenester for dokumentdeling og samarbeid for å distribuere skadelig nyttelast og falske påloggings skjemaer som brukes til å stjele brukerlegitimasjon. Det har også vært en økning i bruken av kompromitterte kontoer for ytterligere å distribuere skadelig e-post både i og utenfor en organisasjon.

Nettfiskingskampanjer varierer fra målrettede til omfattende

Som med distribusjon av skadelig programvare generelt varierer nettfiskingskampanjer fra målrettede til omfattende, generelle angrep. Selv om svært avanserte nettfiskingsangrep gir større pengegevinst per angrepet konto, gir mer generelle angrep mindre penger per konto, men de er rettet mot et bredere sett av brukere.

Et eksempel på en avansert, målrettet kampanje er [Ursnif](#), der angripere lokaliserte dokumentfilnavn for å være spesifikke for en kjent organisasjon eller målets bransje. Slike angrep er ganske forskjellige fra omfattende kampanjer og er tilsynelatende mer lovlige og troverdige.

Noen av de omfattende kampanjene i 2018 var knyttet til Business Email Compromise (BEC) og etterligning av kjente merkevarer, domener eller brukere i de målrettede organisasjonene og avansert kampanjeforfalskning. Domene-etterligning er en vanlig angrepstaktikk som brukes til å lure organisasjoner til å tro at e-posten er pålitelig og bør åpnes.

Nettfiskingsfeller er mangfoldige

Microsoft-forskere har funnet ut at mange ulike typer nettfiskingsfeller eller -nyttelast brukes i kampanjer, blant annet følgende:

- **Domene-forfalskning** (domenet for e-postmeldingen samsvarer nøyaktig med det opprinnelige domenenavnet)
- **Domene-etterligning** (e-postdomenet ser ut som det opprinnelige domenenavnet)²
- **Bruker-etterligning** (e-postmeldingen ser ut til å komme fra noen du stoler på)
- **Tekstmeldingsfeller** (tekstmeldingen ser ut til å komme fra en legitim kilde som en bank, offentlig etat eller annet selskap for å gyldiggjøre sine krav, og vanligvis ber de offeret om å oppgi sensitiv informasjon som brukernavn, passord eller sensitive økonomiske data)
- **Nettfiskingskoblinger for legitimasjon** (e-postmeldingen inneholder en kobling til en side som ligner på en påloggingsside for et gyldig område, slik at brukerne angir påloggingslegitimasjon)
- **Nettfiskingsvedlegg** (e-postmeldingen inneholder et skadelig filvedlegg som avsenderen lokker offeret til å åpne)

- **Koblinger til falske skylagringssteder** (e-postmeldingen ser ut til å komme fra en legitim kilde og lokker brukeren til å gi tillatelse eller angi personlig informasjon som for eksempel legitimasjon i bytte for å få tilgang til et falskt skylagringssted)

Denne variasjonen av feller som potensielt kan brukes av angripere, øker kompleksiteten til nettfiskingstrusler som organisasjoner må stri med.

FOTNOTER

² Domene-etterligning kan ligne på domene-forfalskning (eksakt samsvar med det opprinnelige domenenavnet) i unntakstilfeller der domenet vises i e-postens visningsnavn.

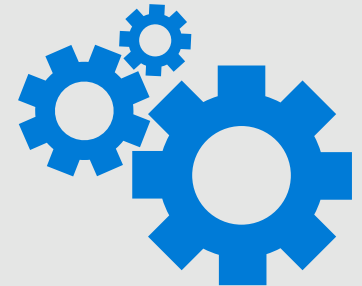
Gransking av cyberkriminalitet med DART

STOR PRODUKSJONSORGANISASJON RAMMET AV MÅLRETTEDE NETTFISKINGSHENDELSER

En produksjonsorganisasjon opplevde en nettfiskingskampanje med flere faser over en periode på noen måneder. Denne tilnærmingen er ikke uvanlig. I løpet av den første fasen vil angriperen utføre rekognosering, og i den andre fasen vil vedkommende målrette seg mot ressurser av høy verdi. I den første fasen av denne kampanjen ble det utnyttet en velkjent nettfiskingssvindler som var basert på en kobling til nettside innebygd i en e-post sendt til en liten målrettet gruppe i organisasjonen. E-posten hevdet at målet mottok et viktig elektronisk dokument til gjennomgang, og alt mottakeren måtte gjøre, var å autentisere med domene-legitimasjonen for å få adgang. Denne falske målsiden som ble oppgitt for målet for å gjennomgå det såkalt «viktige dokumentet», høstet faktisk legitimasjonen og gav angriperen tilgang til Office 365-kontoer fra hvor som helst i verden. Den andre fasen av nettfiskingskampanjen var ment å sende lignende nettfiskings-e-poster til ressurser av høy verdi i produksjonsorganisasjonen, i håp om å få tilgang til mer verdifulle data. Microsoft kommuniserte med denne klienten i den andre fasen av nettfiskingskampanjen. Viktig kundelærdom fra denne hendelsen

var at nettfisking fortsatt er en av de mest effektive angrepsmetodene, og brukere er fortsatt det svakeste leddet. Opplæring av brukere til å være skeptiske til nettfiskingssvindler, verktøy for å identifisere angriperen og handle samt systemer for regelmessig oppdatering, er viktig. Hvis organisasjonen ikke får på plass minst ett av disse tiltakene, kan den være sårbar.

I dette tilfellet var den største bekymringen til kunden et umiddelbart behov for å blokkere tilgangen til de utsatte kontoene. I samarbeid med Azure Identity- og Office 365-avdelingene utviklet DART en plan for å fjerne angriperen fra nettverket og overvåke all trafikk til kommando- og kontrollkanalen ved hjelp av den nylig distribuerte Microsoft Azure Log Analytics-løsningen. Avdelingen hjalp til med å løse situasjonen på bare tre timer. Angriperens tilgang ble blokkert, og organisasjonen kunne konsentrere seg om vurdering av skadeomfang og gjenoppretting. DART brukte Azure Log Analytics-verktøyene til å jakte på angriperens atferd, noe som bidro til å avdekke mange konfigurasjonsutfordringer for organisasjonen. DART identifiserte hull i oppdateringen på viktige servere, oppdaget datamaskiner på nettverket som kommuniserte med kjente farlige verter på Internett, og fant også flere viktige servere uten beskyttelse mot skadelig programvare.



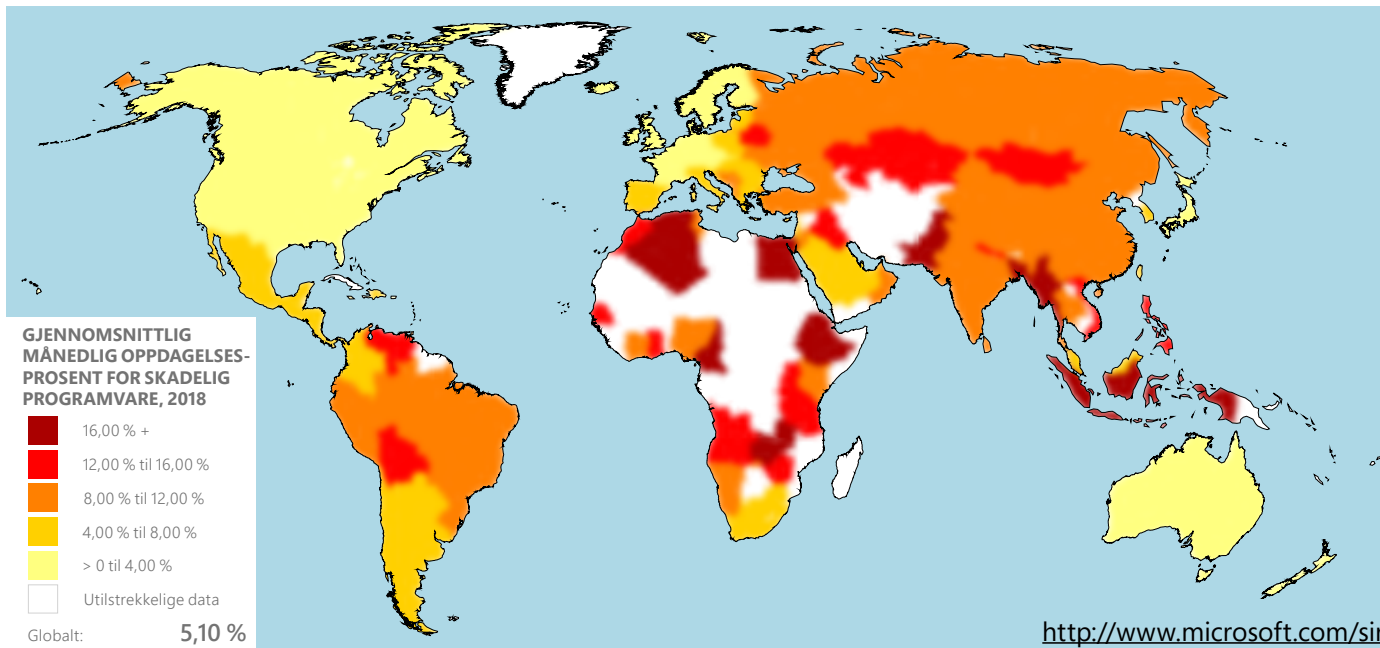


DEL IV

Skadelig programvare rundt om i verden

Skadelig programvare utgjør en risiko for organisasjoner og personer i form av nedsatt brukervennlighet, tap av data, tyveri av immaterielle rettigheter, monetære tap, stressreaksjoner, og det kan også sette menneskeliv i fare. Microsoft bruker et bredt utvalg av verktøy og teknikker for å identifisere, blokkere og utrydde infeksjoner av skadelig programvare uansett hvor de finnes.

Oppdagelsesprosenten for skadelig programvare varierte fra rundt 5 prosent til mer enn 7 prosent i 2017. Tidlig i 2018 gikk prosenten opp, før den så gikk ned i mesteparten av året, og så endte på like over 4 prosent. Noen potensielle årsaker til den generelt **lavere oppdagelsesprosenten for skadelig programvare i 2018** er økt bruk av Windows 10 og økt bruk av Windows Defender for beskyttelse. Oppdagelsesprosenten er prosentandelen av datamaskiner med Windows Defender Antivirus som rapporterte oppdaget skadelig programvare i løpet av måneden, inkludert forsøk på infisering som Defender blokkerte.



◀ **FIGUR 9.**

Gjennomsnittlig månedlig oppdagelsesprosent for skadelig programvare på verdensbasis etter land/område i 2018

De fem stedene med høyest oppdagelsesprosent for skadelig programvare i løpet av perioden januar–desember 2018 var Etiopia (gjennomsnittlig månedlig oppdagelsesprosent på 26,33 prosent), Pakistan (18,94), De palestinske territoriene (17,50), Bangladesh (16,95) og Indonesia (16,59), som alle hadde en gjennomsnittlig månedlig oppdagelsesprosent på ca. 16,59 prosent eller høyere i perioden. Infeksjonsprosenter er vanligvis sterkt relatert til faktorer i menneskelig utvikling og teknologiberedskap i et samfunn. Alle stedene med de høyeste oppdagelsesprosentene i 2018 utgjør de 40 prosent av land og områder som rangeres nederst i 2017-indeksen for informasjon- og kommunikasjonsteknologi (ICT) utgitt av FNs internasjonale teleunion (ITU).

De fem stedene med lavest oppdagelsesprosent for skadelig programvare i samme periode var Irland (1,26), Japan (1,51), Finland (1,74), Norge (1,79) og Nederland (1,82), som alle landet på et gjennomsnitt på 1,82 prosent eller mindre i perioden. Disse stedene har generelt en moden infrastruktur og veletablerte programmer for å beskytte viktig infrastruktur og kommunisere med innbyggerne om grunnleggende sikkerhet.

GJENNOMSnittlig MÅnedlig Oppdagelsesprosent for land som er mest berørt av skadelig programvare



Etiopia:

26,33 %



Pakistan:

18,94 %



De palestinske
territoriene:

17,50 %

Gransking av cyberkriminalitet med DART

FLERE ORGANISASJONER SOM TILBYR ØKONOMISKE TJENESTER, OPPLEVDE STATLIGE ANGREP SOM FORSTYRRET DRIFTEN

I en av de mer ødeleggende hendelsene DART har sett, var flere organisasjoner som tilbyr finansielle tjenester, mål for en statlig sponset APT (en annen gruppe enn den som målrettet seg mot den profesjonelle tjenesteorganisasjonen nevnt tidligere).

Denne APT-en fikk administrativ tilgang etter å ha infisert en «pasient null»-maskin med et svært målrettet, tilslørt bakdørimplantat – muligens levert via en e-post med målrettet nettfisking. Deretter utførte APT-en flere falske transaksjoner og overførte store pengesummer til utenlandske bankkontoer. I noen tilfeller forble angriperen uoppdaget i mer enn 100 dager. Etter at angriperen innså at vedkommende var oppdaget, satte angriperen raskt i gang et forhåndsorganisert angrep og leverte ødeleggende programvare til mer enn halvparten av systemene i miljøet. Disse kundenes drift var nede i flere dager.

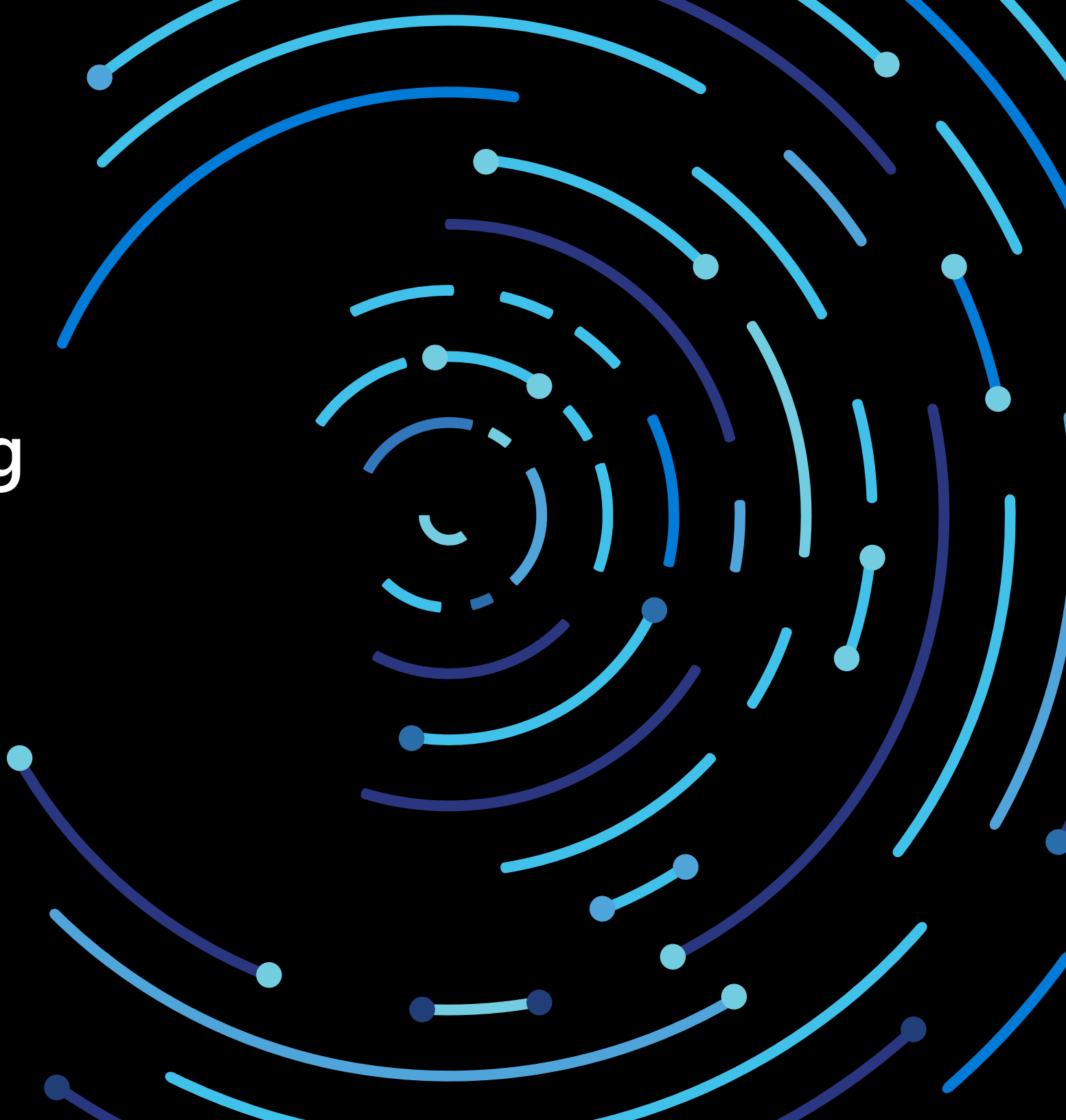
Det var viktig kundelærdom å hente fra disse hendelsene. For det første er livssyklusadministrasjon av programvare spesielt viktig, noe som omfatter å sikre at systemer jevnlig blir oppdatert (operativsystemer og sikkerhet) og revidert. Ett tilfelle gjaldt en organisasjons Linux-systemmiljø som kjørte et uvanlig stort antall arbeidsbelastninger helt uten administrativt tilsyn.

Dette medførte en svært høy risiko for angrep. En annen lærdom var at det er viktig å vedlikeholde sikkerhetskopier av systemdata på en frakoblet plassering i tilfelle de primære dataene går tapt. Nok en lærdom var at tradisjonelle antivirusløsninger kanskje ikke holder hvis du trenger å vite om fiendtlig aktivitet.

Å vende tilbake til normal driftsmodus var høyeste prioritet for disse organisasjonene. DART hjalp til med å gjenopprette tjenester ved først å undersøke konsekvensene og deretter iverksette nødvendige tiltak, for eksempel fjerne skadelig programvare fra de berørte systemene og returnere systemene til en feilfri tilstand. Avdelingen lærte også opp kunder til å bruke Microsofts-verktøy for trusselundersøkelse, inkludert EDR og andre, slik at de kunne se etter uregelmessig atferd og angriperaktivitet på nettverket. DART understreket at endepunktovervåking er avgjørende for å beskytte mot avanserte, målrettede angrep som kan forbli uoppdaget av tradisjonelle antivirusløsninger.



Veiledning



Veiledning

Utvikling av organisatorisk robusthet og velfungerende risikoreduksjon krever en sikkerhetstilnærming som omfatter forebygging, oppdagelse og respons. Vi har organisert følgende anbefalte sikkerhetsrutiner og kontroller i disse kategoriene.

FOREBYGGING:

Forebyggende kontroller spiller en viktig rolle i en overordnet forsvarsstrategi ettersom de riktige investeringene kan øke kriminelles angrepskostnader og opprettholde de økte angrepskostnadene over tid (uten at en ekspertanalytiker må overvåke og tolke ytelsen). Investeringer i forebyggende kontroll bør rettes mot lavkostteknikker for å fjerne billige og effektive angrepsteknikker.

Her er fire forebyggende hensyn:

1. Sikkerhetshygiene er avgjørende. Som vi så i noen av cyberhendelsene i denne rapporten, kan vanlige hygieneproblemer undergrave avanserte sikkerhetsfunksjoner, så ved å følge disse tipsene kan man redusere risikoer:

- Unngå å bruke ukjent kostnadsfri eller piratkopiert programvare. Bruk bare programvare fra klarerte kilder.
- Reduser risikoen for legitimasjonstyveri, inkludert sikring av privilegerte administratorkontoer. Du kan lære hvordan du gjør det, i denne [bloggposten](#), som beskriver noen prinsipper og verktøy Microsoft

har brukt for å veilede og forbedre vår egen sikkerhetsholdning, og noen normative veikart for å hjelpe deg å planlegge dine egne initiativer.

- Bruk anbefalte sikkerhetsinnstillinger fra programvareleverandørene dine.
- Hold maskiner oppdatert ved raskt å ta i bruk de nyeste oppdateringene til operativsystemer og apper, og ta umiddelbart i bruk kritiske sikkerhetsoppdateringer for OS, nettlesere og e-post. Isoler (eller trekk tilbake) maskiner som ikke kan oppdateres.
- Implementer avansert e-post- og nettleserbeskyttelse. Ta i bruk en sikker e-post-gateway som har avanserte trusselfunksjoner for å beskytte mot moderne nettfiskingsvarianter.
- Aktiver vertsbasert nettverksforsvar og beskyttelse mot skadelig programvare for å få nær sanntidsblokkering av svar fra skyen (hvis det er tilgjengelig i løsningen din).

2. Implementer tilgangskontroller. Vurder følgende:

- Bruk prinsippet om minste privilegium, som omfatter å implementere nettverkssegmentering, fjerne lokale administratorrettigheter fra sluttbrukere og utvise forsiktighet når du gir tillatelser til apper som kjører på datamaskinen.
- Last ned apper bare fra pålitelige kilder (en offisiell appbutikk).
- Ta i bruk sterke prosedyrer for kodeintegritet, blant annet begrensning av apper som brukere kan kjøre. Ta i bruk – hvis mulig – en sikkerhetsløsning som begrenser koden som kjører i systemkjernen, og kan blokkere usignerte skript og andre former for uklarert kode. Bruk hvitelister for apper.
- Hvis du vil vite mer om angrep på programvareforsyningskjeder og hvordan du beskytter deg mot dem, kan du lese denne bloggposten fra Microsoft-forskere.

3. Ta sikkerhetskopier.

- Opprett motstandsdyktige sikkerhetskopier av viktige systemer og data.
- Bruk skylagringstjenester for automatisk sikkerhetskopiering av data på nettet. For data som lagres lokalt, bør du sikkerhetskopierte viktige data regelmessig ved hjelp av 3–2–1-regelen. Ha tre sikkerhetskopier av dataene dine på to forskjellige lagringstyper, og ha minst én sikkerhetskopi på en ekstern plassering.

4. Vær oppmerksom, og handle hvis du har mistanke om noe.

- Lær de ansatte å være skeptiske til mistenkelig meldinger som ber om sensitiv informasjon, og be dem om å reagere og rapportere meldingene til organisasjonens sikkerhetsavdeling umiddelbart. Opplæring kan også bidra til å redusere sosial manipulering og målrettet nettfisking.
- Vær forsiktig når du klikker på nettkoblinger. Å ha gode Internett-vaner og bruke løsninger som advarer mot eller blokkerer tilgang til usikre nettsteder, kan redusere sannsynligheten for å havne på nettsteder tilknyttet kryptovalutautvinning.
- Hvis en datamaskin kjører svært sakte, kan du se etter kjøring av mistenkelige filer og gjerne sende et utvalg til operativsystemleverandøren. Du kan undersøke om filene er skadelig programvare ved å sende dem inn til Microsoft på <https://www.microsoft.com/wdsi/filesubmission>.

OPPDAGELSE OG REAKSJON:

Oppdagelse og respons bidrar til robusthet ved å begrense hvor lenge en angriper har tilgang til ressursene dine. Dette reduserer angriperens avkastning både ved å øke kostnadene (angriperen må prøve på nytt eller finne en ny tilnærming) og redusere gevinsten (begrenser sannsynligheten for å oppnå målet).

Den samme skyteknologien som gjør det mulig for forretningsorganisasjoner å oppfylle markedets behov, kan også hjelpe dem med å slå tilbake mot angripere.



FIGUR 10.

Utviklingsløpet til SOC-er

Som vi ser av utviklingen til Security Operations Centers (SOC-er), øker teknologi kontinuerlig hastigheten og kvaliteten på SOC-beslutninger og -handlinger. Mange av disse nyvinningene kan tilordnes hvert trinn i Observer Orient Decide Act-løkken (OODA), som ble dokumentert av U.S. Air Force-oberst John Boyd.³

OBSERVER – SOC-er kan utnytte den omfattende tilgjengelige sikkerhetsintelligensen (fra Microsoft og andre kilder) som drastisk øker synsfeltet i organisasjonen og det ytre miljøet.

ORIENTER – Når disse nye datakildene blir tilgjengelige for allerede overbelastede SOC-er, blir maskinlæring (et delsett av kunstig intelligens) et avgjørende verktøy for å spørre i disse enorme datasettene og identifisere uregelmessigheter som er verdt å undersøke. Sikkerhetsleverandørene (inkludert Microsoft) har tatt i bruk maskinlæringsteknologi for å prioritere hendelser raskt (og hjelpe med å slå sammen disse individuelle hendelsene til helhetlige hendelser).

TA BESLUTNING – Fordi angrepsvolum og -kompleksitet raskt kan overbelaste et SOC, må analytikere og utrykningspersonell ta mange

beslutninger og reagere raskt på varsler og oppdagelser. Microsoft og andre leverandører har integrerte automatiserte undersøkelsesfunksjoner, i tillegg til veiledning for å hjelpe analytikere med å ta gode beslutninger (f.eks. for å isolere potensielt infiserte eller skadde enheter). For øyeblikket er automatisering fokusert på rask løsning av hendelser med lav prioritet, slik at spesialiserte ferdigheter kan brukes på mer komplekse problemer.

HANDLE – Respons krever rask og nøyaktig utførelse på tvers av mange teknologier og plattformer, som er hva teknologier for sikkerhetsorkestrering og responsautomatisering muliggjør. Microsoft og mange andre fortsetter å investere i disse teknologiene, inkludert moderne trusselgjenkjenning og automatiserte responsløsninger.

FOTNOTER

³<http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/>

Noen andre trender som gjelder for et moderne SOC, er:

- **Kvalitet fremfor kvantitet for varslinger** – Når organisasjoner går fra å administrere «ikke nok informasjon» til å administrere «for mye informasjon», blir tiden og oppmerksomheten til høyt spesialiserte SOC-analytikere mer og mer verdifull. Dette skaper et større behov for kvalitet i varslene som krever analytikerengasjement på nivå 1 og 2. Flere datainnmatninger er alltid nyttige for undersøkelser og proaktiv jakt, men Microsofts Corporate IT SOC måler den reelle frekvensen av varslinger som krever analytikerrespons (og for øyeblikket krever 90 % eller høyere Sann positiv-prosent).
- **Datagravitasjon** – Analyser av store datasett (inkludert sikkerhetsdata) er vanskelige å utføre uten tilgang til underliggende rådata. Etter hvert som mer sikkerhetsdata blir tilgjengelig, blir det mer økonomisk og praktisk å utføre sikkerhetsanalyse i skyen i motsetning til å flytte dataene tilbake til et lokalt system. Dette vil trolig føre til utviklingen av SIEM- og SOC-arkitektur som kan inkludere hybride SIEM-tilnærminger eller bruk av Native Cloud SIEM som en tjeneste.
- **Høykontekst** – Disse oppdagelsestypene er langt nyttigere på grunn av sin evne til å koordinere datasett mer effektivt. Mens tradisjonell oppdagelse basert på nettverkstrafikk fortsatt gir

noe sikkerhetsverdi, mangler rå nettverkstrafikk vanligvis kontekst for å skille mellom lovlig aktivitet og uregelmessigheter. Vi ser at SOC-er har mye større nytte av høykontekstopdagelser som:

- **Løsninger for Endpoint Detection and Response (EDR)** som har grundig kontekst om vertsaktiviteten
- Identitetsbasert oppdagelse som inkluderer innsikt i vanlige mønstre for brukergodkjenning (steder, tidspunkter, hvilke tjenester som brukes, osv.) og bruker atferdsanalyse

Disse kontekstrike oppdagelsene er vanskeligere å unngå av motstandere fordi de må etterligne en mye mer komplisert operasjon (i motsetning til noen tekniske attributter for IP-trafikk).

En annen leksjon vi har lært av store sikkerhetsbrudd hos kunder, er vanskeligheten med å reagere raskt på hendelser når IT-funksjoner er delvis eller fullstendig utkontrahert. Vi anbefaler at du gjennomgår kontrakter for IT-utkontrahering og serviceavtaler, i tillegg til forsyningskjedeleverandører, for å sikre at de er compatible med rask sikkerhetsrespons. Hvis du vil vite mer om vår hendelsesundersøkelser hos kunder, kan du se Incident Response Reference Guide (IRRG) på <https://aka.ms/IRRG>.

Datakilder



Datakilder

Microsoft har samlet inn dataene som er inkludert i Microsofts sikkerhetsanalyserapport, ved å tilby et bredt spekter av Microsoft-produkter og-tjenester, som beskrevet i [Microsofts personvernerklæring](#). Disse dataene gir oss verdifull informasjon om sikkerheten og driften av våre produkter og tjenester samt innsikt om trussellandskapet for cybersikkerhet generelt. Disse dataene omfatter analyse fra følgende kilder:⁴

- [Azure Security Center](#) er en tjeneste som hjelper organisasjoner med å forebygge, oppdage og reagere på trusler ved å gi økt innsikt i sikkerheten til skyarbeidsbelastninger og bruke avansert analyse og trusselintelligens for å oppdage angrep.
- [Bing](#) er søke- og beslutningsmotoren som utfører milliarder av nettsideskanninger per år for å oppdage skadelig innhold. Når slikt innhold er registrert, viser Bing advarsler til brukerne for å forhindre skade.
- [Exchange Online](#) er Microsofts vertsbaserte e-post- og produktivitetstjeneste. Exchange Online-tjenestene for bekjempelse av skadelig programvare og søppelpost skanner milliarder av meldinger hvert år for å identifisere og blokkere søppelpost og skadelig programvare.
- [Malicious Software Removal Tool](#) (MSRT) er et gratis verktøy som Microsoft har utviklet for å identifisere og fjerne visse utbredte typer skadelig programvare fra kundemaskiner. MSRT er primært utgitt som en viktig oppdatering via Windows Update, Microsoft Update og automatiske oppdateringer. En versjon av verktøyet er også tilgjengelig fra Microsoft Download Center. MSRT er ikke en erstatning for en oppdatert antivirusløsning som beskytter i sanntid.
- [Microsoft Safety Scanner](#) er et nedlastbart sikkerhetsverktøy som leverer skanning etter behov og bidrar til å fjerne skadelig programvare. Microsoft Safety Scanner er ikke en erstatning for en oppdatert antivirusløsning, fordi den ikke tilbyr sanntidsbeskyttelse og ikke kan forhindre at datamaskiner blir infisert.

FOTNOTER

⁴Disse dataene går alltid gjennom strenge personvern- og samsvarsgrenser før de brukes til sikkerhet.

- [**Microsoft Security Essentials**](#) er et nedlastbart produkt som gir sanntidsbeskyttelse. Det gir grunnleggende og effektiv beskyttelse mot virus og spionprogrammer for Windows Vista og Windows 7.
- [**Microsoft System Center Endpoint Protection**](#) (tidligere Forefront Client Security og Forefront Endpoint Protection) er et enhetlig produkt som gir beskyttelse mot skadelig programvare og uønsket programvare for bedriftsdatamaskiner, bærbare datamaskiner og serveroperativsystemer. Det bruker Microsoft Malware Protection Engine og Microsofts antivirus-signatordatabase for å gi beskyttelse både i sanntid, planlagt og etter behov.
- [**Office 365**](#) er abonnementstjenesten for Microsoft Office for organisasjoner og private brukere. Utvalgte abonnementer inkluderer tilgang til Office 365 Advanced Threat Protection.
- [**Windows Security**](#) i Windows 10 skanner i sanntid og fjerner skadelig og uønsket programvare. I tillegg utnytter den nyeste versjonen av Windows omfattende kontekstdata, for eksempel [maskinkonfigurasjon](#), enhetsytelse og -tilstand samt annen slik informasjon for å forbedre kundenes sikkerhet. Samtidig gjør vi det mulig for kundene å være mer informert om personvern i Windows 10. Les [denne bloggposten](#) for å lære om noen av måtene Microsoft gjør dette på.
- [**Windows Defender Advanced Threat Protection**](#) er en tjeneste som er innebygd i jubileumsoppdateringen av Windows 10 og senere versjoner. Den gjør det mulig for bedriftskunder å oppdage, undersøke og kurere avanserte, vedvarende trusler og databrudd på nettverket deres.
- [**Windows Defender Offline**](#) er et nedlastbart verktøy som kan brukes til å opprette en oppstartbar CD, DVD eller minnepinne for å skanne en datamaskin for skadelig programvare og andre trusler. Det tilbyr ikke sanntidsbeskyttelse og er ikke en erstatning for en oppdatert løsning mot skadelig programvare.
- [**Windows Defender SmartScreen**](#), en funksjon i Microsoft Edge og Internet Explorer, gir brukerne beskyttelse mot nettfiskingsnettsteder og nettsteder som er vert for skadelig programvare. Microsoft vedlikeholder en database med nettsteder som inneholder nettfisking og skadelig programvare. Disse nettstedene rapporteres av brukere av Microsoft Edge, Internet Explorer og andre Microsoft-produkter og -tjenester. Hvis en bruker prøver å gå til et nettsted i databasen med filteret aktivert, viser nettleseren en advarsel og blokkerer navigasjon til siden.