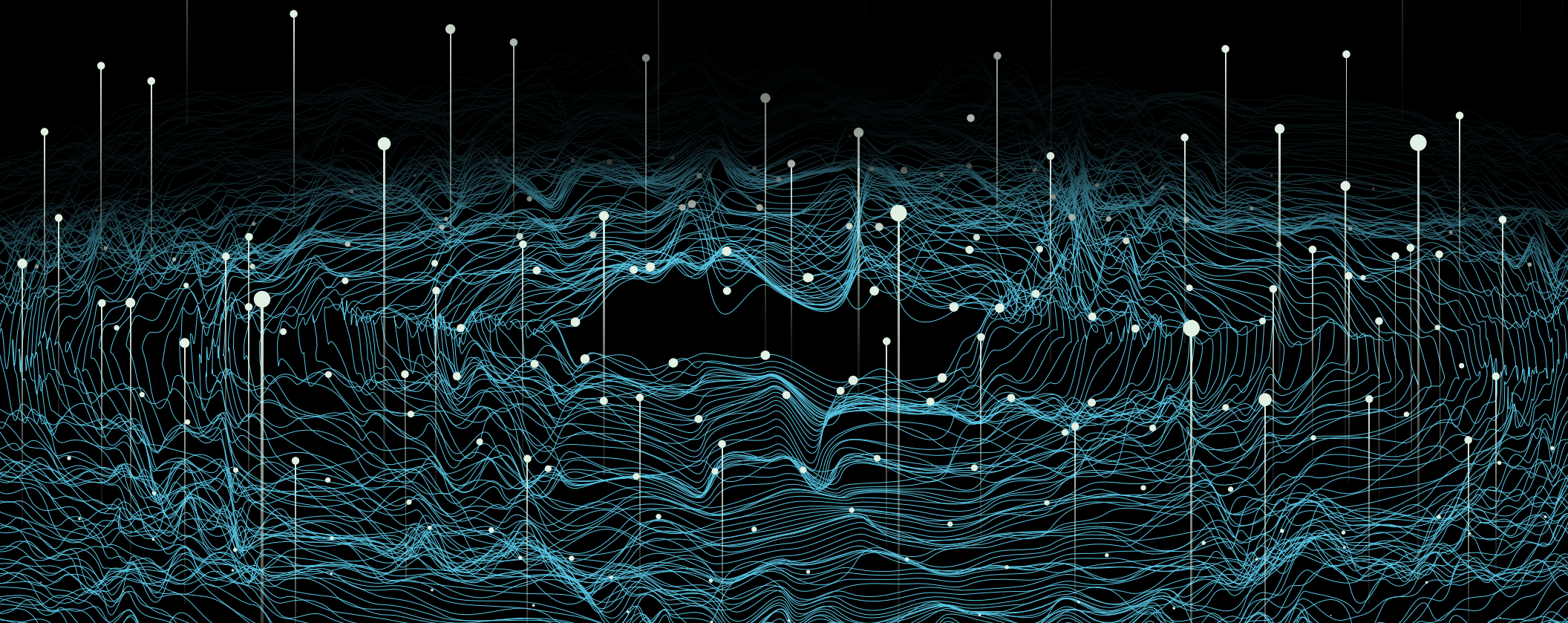
Microsoft

MICROSOFT SECURITY INTELLIGENCE REPORT

OSA 24

TAMMI–JOULUKUU 2018



Sisällysluettelo

Tekijät . . . 3

Esipuhe . . . 4

LUKU I: Kiristysohjelmat, kryptovaluutan louhinta ja raha . . . 6

Kiristysohjelmahyökkäykset ovat laskussa . . . 7

Kryptovaluutan louhinta on kasvussa . . . 10

Selainpohjaiset kryptovaluutan louhijat: uudenlainen uhka . . . 11

Ei-toivotun kryptovaluutan louhinnan vaikutukset . . . 12

LUKU II: Ohjelmistojen toimitusketjut vaarassa . . . 13

Luottamus vaarassa . . . 16

Ei vain ohjelmistoja: toimitusketjujen murtaminen pilviobjektien kautta . . . 17

Kyberrikollisuuden tutkiminen: Asiantuntijapalvelut . . . 18

LUKU III: Tietojenkalastelu on edelleen ongelma . . . 19

Tietojenkalastelu oli edelleen suosittu hyökkäystapa vuonna 2018 . . . 20

Kyberrikollisuuden tutkiminen: Valmistava teollisuus . . . 23

LUKU IV: Haittaohjelmat ympäri maailmaa . . . 24

Kyberrikollisuuden tutkiminen: Rahoituspalvelut . . . 27

Opastus . . . 28

Tietolähteet . . . 33

Tämä asiakirja on tarkoitettu vain tiedoksi. MICROSOFT EI ANNA TÄMÄN ASIAKIRJAN TIEDOILLE MITÄÄN NIMENOMAISIA, EPÄSUORIA TAI LAKISÄÄTEISIÄ TAKUITA.

Tämä asiakirja on vain tiedoksi. Asiakirjassa olevat tiedot ja ilmaistut näkemykset, mukaan lukien verkko-osoitteet ja muut viittaukset verkkosivuihin, voivat muuttua ilman erillistä ilmoitusta. Asiakirjan käyttö on lukijan omalla vastuulla.

Copyright © 2019 Microsoft Corporation. Kaikki oikeudet pidätetään.

Muut tässä asiakirjassa mainitut yritysten ja tuotteiden nimet voivat olla omistajiensa tavaramerkkejä.

Tekijät

Abhishek Agrawal
Sisällön varmistus

David Fantham
Sisällön varmistus

Debraj Ghosh
Microsoft-tietoturvan markkinointi

Diana Kelley
Cybersecurity Solutions Group

Elia Florio
Windowsin aktiivinen puolustus

Eric Avena
Windows Defenderin tutkimusryhmä

Eric Douglas
Windows Defenderin tutkimusryhmä

Francis Tan Seng
Windows Defenderin tutkimusryhmä

Jonathan Trull
Cybersecurity Solutions Group

Joram Borenstein
Cybersecurity Solutions Group

Karthik Selvaraj
Windows Defenderin tutkimusryhmä

Kasia Kaplinska
Microsoft-tietoturvan markkinointi

Kristina Laidler
Security Incident Response

Matt Duncan
Windowsin aktiivisten puolustustietojen suunnittelu ja analyysi

Mark Simos
Cybersecurity Solutions Group

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft-tietoturvan markkinointi

Ram Pliskin
Azuren tietoturva

Ryan McGee
Microsoft-tietoturvan markkinointi

Seema Kathuria
Cybersecurity Solutions Group

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defenderin tutkimusryhmä

Volv Grebennikov
Bing

Yaniv Zohar
Azuren tietoturva

Esipuhe

Tervetuloa Microsoft Security Intelligence Reportin (SIR) 24. osan pariin. Tietoturvasta vastaavana arkkitehtinä luen tällaisia raportteja ymmärtääkseni hieman paremmin nykyistä turvallisuusympäristöä. Saan niistä käytännöllisiä neuvoja ja tietoja, jotka auttavat puolustautumaan uhkilta ja suojaamaan organisaatioita tehokkaammin.

SIR-tiimin lähestymistapa kyberturvallisuuden parantamiseen on koulutus. Tiimi on käynyt läpi koko vuoden aikana kertyneen datan ja laatinut yhteenvedon tärkeimmistä huomiosta.

Raportti sisältää huomioita, jotka on koottu vuoden aikana suoritettujen tietoturvadata-analyysien ja käytännön tilanteiden avulla. Analysoituun dataan lukeutuu 6,5 biljoonaa uhkasignaalia, jotka Microsoftin pilvipalvelut tunnistavat päivittäin. Lisäksi näkemykset perustuvat tuhansien tietoturvatutkijoiden ja vastuuhenkilöiden tutkimuksiin ja reaalimaailman kokemuksiin. Vuonna 2018 hyökkääjät pyrkivät useilla keinoilla varastamaan asiakkaiden ja organisaatioiden dataa ja resursseja. Niihin sisältyi sekä uusia (mm. kryptovaluutan louhinta) että vanhoja (mm. tietojenkalastelu) menetelmiä. Hybridihyökkäykset, kuten Ursnif-kampanja, yhdistivät sosiaalisia ja teknisiä lähestymistapoja. Koska puolustajat pystyvät nyt älykkäämmin torjumaan kiristysohjelmia, jotka ovat erittäin näkyviä ja häiritseviä hyökkäyksen muotoja, rikolliset ovat nyt siirtyneet yhä suuremmassa määrin kryptovaluuttaa louhiviin "häiveohjelmistoihin". Valitettavasti nekin ovat hyökkääjille taloudellisesti kannattavia.

Tämä muutos voi tuntua turhauttavalta – ikään kuin hyökkääjät olisivat aina yhden askeleen edellä. Toisesta näkökulmasta kehityskulku on kuitenkin ollut myönteinen. Kyberturvallisuuden ammattilaiset ovat pakottaneet hyökkääjät muuttamaan toimintatapaansa ja vähentämään kiristysohjelmien käyttöä.

Kyberrikollisuus on lisääntynyt myös toimitusketjuissa. Yksi merkittävimmistä tapauksista oli Dofoil-kybervaluutan louhintaohjelmisto, joka iski 6. maaliskuuta 2018. Leviäminen sai alkunsa tartunnan saaneesta vertaisverkkosovelluksesta. Toimitusketjussa ongelmia on esiintynyt muuallakin kuin sovelluksissa. Niihin lukeutuvat myös pilvipalvelut, vahingolliset selainlaajennukset, tartunnan saaneet Linux-tietovarastot sekä moduulit, joihin on lisätty takaoviohjelmia. Näihin uhkiin vastaamiseksi organisaatiot ovat siirtymässä kohti mallia, jossa toimitusketjut ovat läpinäkyviä ja luotettuja.

Data on mahtava asia, ja toisinaan se auttaa selvittämään, mitä organisaatiossa on oikeasti tapahtunut. Siksi olemme sisällyttäneet tähän raporttiin tunnistus- ja vastetiimimme (Detection and Response Team, DART) kokemuksia kentältä. Kerromme esimerkiksi, kuinka suuri valmistavan teollisuuden yritys onnistui estämään monivaiheisen tietojenkalastelukampanjan, joka oli vaivannut yritystä useiden kuukausien ajan. Kerromme myös rahoituspalveluyrityksistä, jotka ovat lopultakin pystyneet poistamaan uhkaavat toimijat järjestelmistään edistyneiden tutkimustyökalujen ja päätepisteiden valvonnan avulla.

Viimeisenä muttei vähäisempänä on huomioitava, että tietojenkalasteluviestien avaamiset ovat kasvussa – mutta yhä useammin koneoppimismallit tunnistavat tällaiset viestit ennen kuin ne saapuvat käyttäjän postilaatikkoon, ja nämä mallit pystyvät estämään vahinkoja avaamisen jälkeenkin. Lisää hyviä uutisia? Yhä useammat yritykset ovat ottaneet käyttöön monimenetelmäisen todennuksen ja vähentäneet sen myötä tunnistetietojen kalastelun vaikutuksia.

Hyökkääjät etsivät erilaisia mahdollisuuksia. Mitä enemmän tiedämme heidän tekniikoistaan ja taidoistaan, sitä parempia puolustusmekanismeja pystymme rakentamaan ja sitä nopeammin pystymme vastaamaan. Pienillä mutta tärkeillä askeleilla voi olla valtava merkitys organisaation kokonaisvaltaisten kyberturvallisuusvalmiuksien kannalta. Siksi muuttuvan haittaohjelma- ja hyökkäysympäristön syväluotauksen lisäksi löydät tästä raportista suositeltuja toimenpiteitä sekä muita parhaita käytäntöjä. Kun itse olin mukana käytännön työssä, juuri tällaisista ohjeista oli minulle eniten hyötyä taistelussa kyberrikollisuutta vastaan. Toivomme, että ne osoittautuvat hyödyllisiksi myös omassa työssäsi.

Diana Kelley
Microsoft Cybersecurity Field CTO

P.S. Pyrimme jatkuvasti parantamaan SIR-tiimin toimintaa. Jos haluat antaa palautetta, älä epäröi ottaa meihin yhteyttä.

LUKU I

Kiristysohjelmat, kryptovaluutan louhinta ja raha

Vuoden 2017 merkittävimpiin tietoturvahaasteisiin lukeutuivat kiristysohjelmat. Paljon näkyvyyttä saaneiden maailmanlaajuisten WannaCrypt- ja Petya-tartuntojen myötä haittaohjelmistot, jotka lukitsevat tai salaavat tietokoneen ja vaativat rahaa tietojen palautuksesta, tulivat yleiseen tietoisuuteen. Monet arvioivat, että tulevaisuudessa nämä ongelmat vain pahenisivat. Sen sijaan vuonna 2018 kiristysohjelmia tuli esille huomattavasti aiempaa vähemmän.

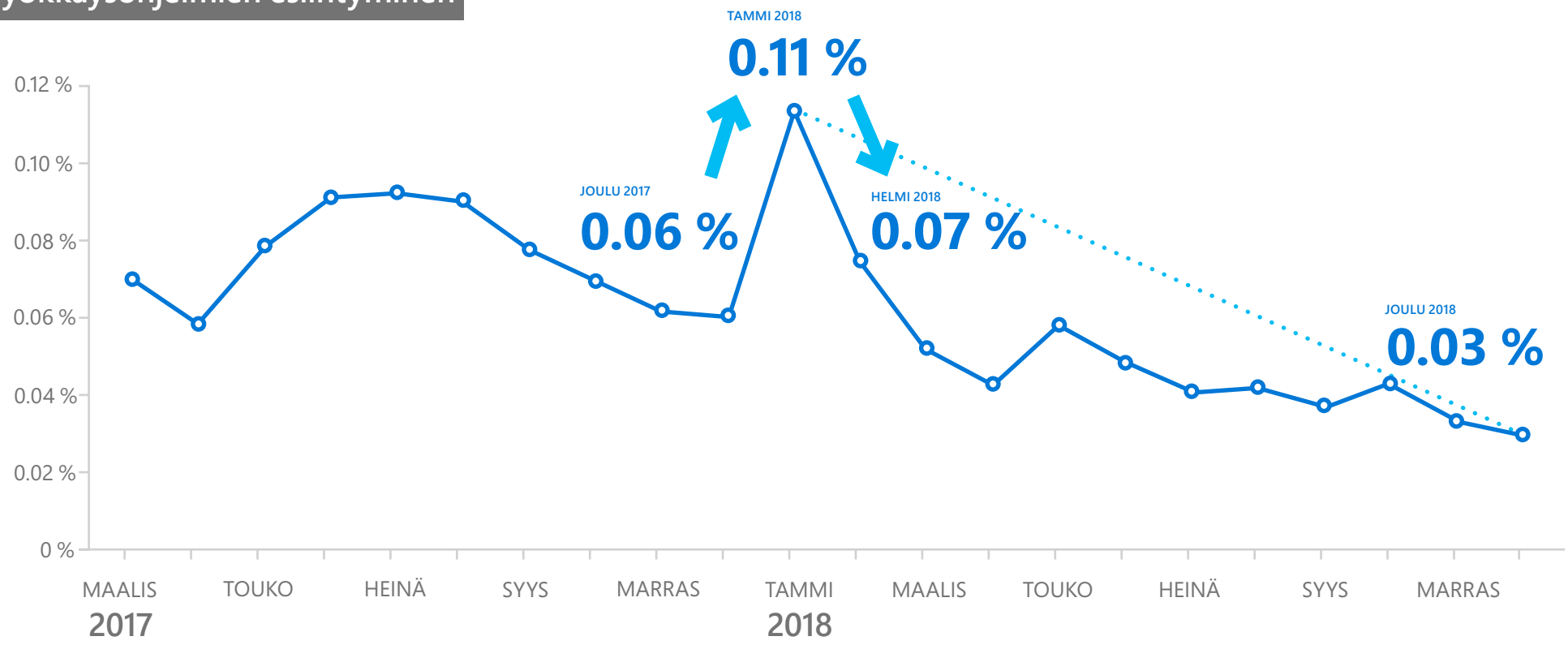
Kiristysohjelmien harvinaistuminen johtui osaltaan paremmasta tunnistuksesta ja koulutuksesta, joiden vuoksi hyökkääjien oli vaikeampaa hyötyä niistä. Tämän seurauksena hyökkääjät alkoivat keskittyä kiristysohjelmien sijasta esimerkiksi kryptovaluutan louhintaan, jossa hyökkääjät käyttävät uhrien laskentaresursseja digitaalisen rahan hankintaan. Muutos ilmentää perustavalla tavalla useimpien taloudellista hyötyä tavoittelevien kyberrikollisten opportunismia. He usein tavoittelevat helpoiten saatavilla olevia voittoja, ja kun kyberrikollisuuden kannattavuus muuttuu, he mukautuvat nopeasti tähän muutokseen.

KIRISTYSOHJELMAHYÖKKÄYKSET OVAT LASKUSSA

Yli kymmenen vuotta sitten perinteiset hakkerit ja pilailijat, jotka hallitsivat haittaohjelmien varhaista alamaailmaa, korvautuivat järjestäytyneellä rikollisuudella ja muilla voittoa tavoittelevilla intresseillä. Varhaiset haittaohjelmatartunnat olivat usein huomiota tavoittelevia ja selvästi ilmeneviä, kun taas voittoa tavoittelevat haittaohjelmat pyrkivät toimimaan hiljaa ja huomiota herättämättä, jotta ne pystyvät mahdollisimman pitkään jatkamaan toimintaansa: roskapostitusta, arkaluonteisten tietojen varastamista, palvelunestohyökkäyksiä ja muita vahingollisia toimia.

Kiristysohjelmat rikkoivat tämän trendin. Sen sijaan, että ne yrittäisivät toimia huomiota herättämättä, avoimet kiristysohjelmat epäävät uhrilta oikeuden tietokoneen ja tärkeiden tiedostojen käyttöön, ellei hän suostu maksamaan lunnaita. (Usein ongelma jatkuu lunnaiden jälkeenkin – hyökkääjät eivät useinkaan palauta tietokonetta entiselleen edes maksun jälkeen.) Kun kiristysohjelmat olivat suosituimmillaan vuonna 2017, näytti siltä, että tällaiset avoimet hyökkäykset edustaisivat hyökkäystekniikoissa uuden vaiheen alkua. Uusimmat tiedot kuitenkin osoittavat, että kiristysohjelmien määrä saattaa olla laskussa. Hyökkääjät ovat yhä suuremmassa määrin palaamassa aiempiin toimintatapoihinsa, jotka ovat huomaamattomampia. He pyrkivät välttämään tunnistuksen, jotta he pystyvät tehokkaammin suorittamaan esimerkiksi kryptovaluutan louhinnan kaltaisia hyökkäyksiä. Vaikka kiristysohjelmia on havaittu vähemmän, tämä ei välttämättä tarkoita, että iskut eivät enää ole yhtä vakavia.

Hyökkäysohjelmien esiintyminen

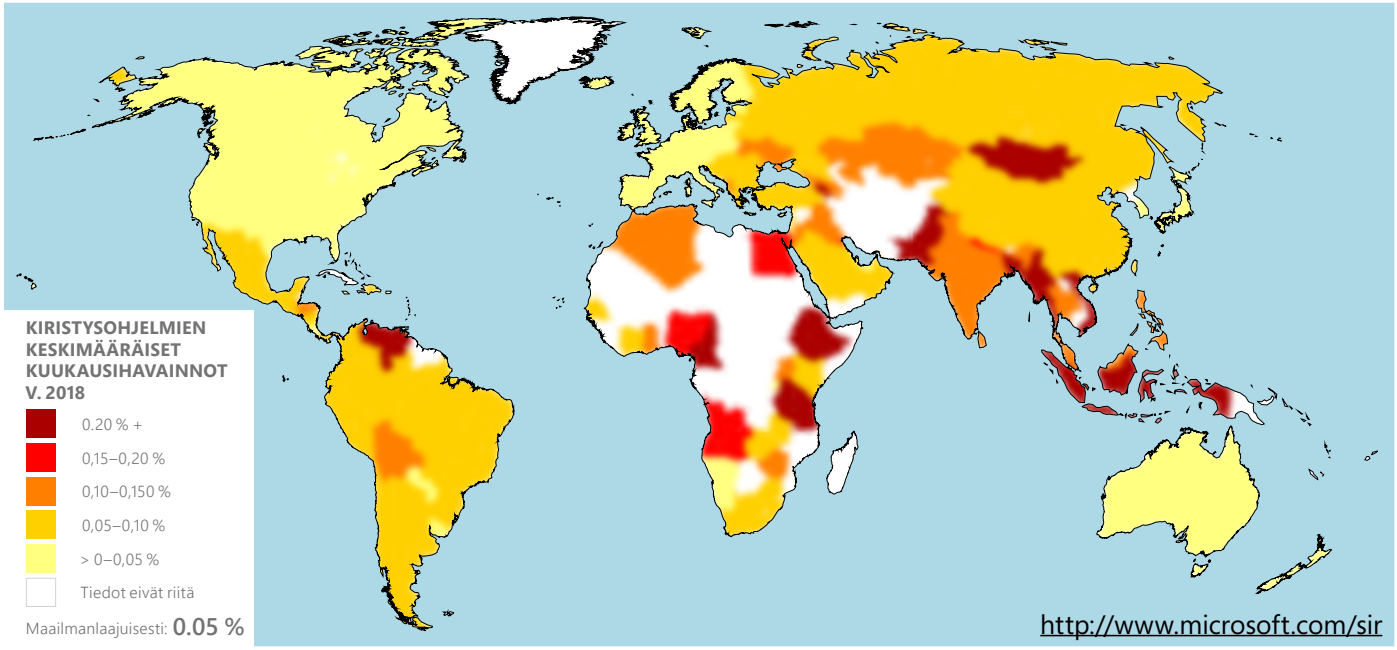


Kiristysohjelmistoja havaittiin noin 60 prosenttia vähemmän verrattaessa maaliskuuta 2017 ja joulukuuta 2018, joskin tämän kauden aikana määrä lisääntyi hetkellisesti joitakin kertoja.

KUVA 1.

Kiristysohjelmien havainnot aikavälillä maaliskuu 2017 – joulukuu 2018

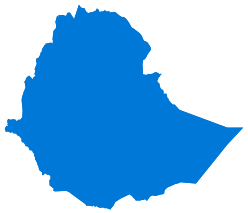
Tähän laskevaan trendiin vaikuttaa todennäköisesti useita tekijöitä, mutta Microsoftin tietoturvatutkijat epäilevät, että ensisijainen syy on loppukäyttäjien ja organisaatioiden suurempi tietoisuus asiasta. Kiristysohjelmauhkiin reagoidaan entistä älykkäämmin ja toiminta on varovaisempaa. Tärkeitä tiedostoja myös varmuuskopioidaan enemmän, jotta ne voidaan palauttaa kiristysohjelman hyökätessä. Kuten aiemmin mainitsimme, kyberrikolliset ovat opportunisteja.



KUVA 2.

Kiristysohjelmien keskimääräiset kuukausihavainnot maailmanlaajuisesti maittain/alueittain vuonna 2018

KIRISTYSOHJELMISTA ENITEN KÄRSINYT MAA: ETIOPIA



Keskimääräiset kuukausihavainnot: **0.77 %**

Viisi sijaintia, joissa kiristysohjelmia havaittiin kuukaudessa eniten vuonna 2018, olivat Etiopia (0,77 prosenttia keskimääräisistä kuukausihavainnoista), Mongolia (0,46 %), Kamerun (0,41 %), Myanmar (0,33 %) ja Venezuela (0,31 %). Kussakin näistä maista kiristysohjelmien havaintoja oli 0,31 % tai enemmän.[1] Muutama vuosi sitten kiristysohjelmat keskittyivät usein vauraisiin maihin ja vauraille alueille, kuten Eurooppaan ja Pohjois-Amerikkaan. Kun kiristysohjelmien suosio hyökkääjien keskuudessa on laskenut, niiden esiintyminen on alkanut muistuttaa entistä useammin muille haittaohjelmille tyypillistä kuviota.

Vähiten kiristysohjelmia esiintyi vuonna 2018 Irlannissa (0,01 %), Japanissa (0,01 %), Yhdysvalloissa (0,02 %), Britanniassa (0,02 %) ja Ruotsissa (0,02 %). Kussakin näistä maista esiintymisprosentti oli 0,02 % tai pienempi samana ajanjaksona. Paikoissa, joissa kiristysohjelmia esiintyy vähän, kyberturvallisuuden infrastruktuurit ovat usein kehittyneitä ja käytössä on vakiintuneita ohjelmia kriittisen infrastruktuurin suojaukseen. Lisäksi kansalaisille tarjotaan perustietoa tietoturvasta.

ALAVIITTEET

[1] Esiintymisprosentti kuvaa sitä, kuinka suuri osuus Microsoftin reaaliaikaisia tietoturvatuotteita käyttävistä tietokoneista ilmoittaa haittaohjelmahavainnosta. Uhan kohtaaminen ei tarkoita, että tietokone on saanut tartunnan. Vain tietokoneet, joiden käyttäjät ovat valinneet tietojen toimittamisen Microsoftille, otetaan huomioon kohtaamissuhdetta laskettaessa.

KRYPTOVALUUTAN LOUHINTA ON KASVUSSA

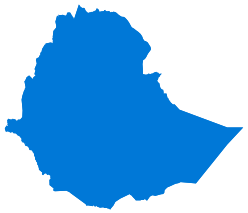
Kryptovaluutta on virtuaalista rahaa, jota voidaan käyttää anonyymisti tuotteiden ja palveluiden ostamiseen sekä verkossa että fyysisessä maailmassa. Erilaisia kryptovaluuttoja on lukuisia, mutta ne kaikki perustuvat lohkoketjuteknologiaan. Siinä jokainen tapahtuma tallennetaan hajautettuun tilikirjaan, jota ylläpitävät tuhannet tai miljoonat tietokoneet ympäri maailmaa. Uusia kolikoita luodaan eli "louhitaan" monimutkaisia laskutoimituksia suorittavilla tietokoneilla. Nämä laskutoimitukset toimivat myös lohkoketjutapahtumien vahvistuksina.

Kryptovaluutan louhinta voi olla erittäin tuottoisaa. Vuonna 2018 yksittäinen Bitcoin (joka on vanhin ja suosituin kryptovaluutta) oli arvoltaan useita tuhansia Yhdysvaltain dollareita. Vaadittavat laskutoimitukset voivat kuitenkin kuluttaa runsaasti resursseja, ja mitä enemmän kolikoita louhitaan, sitä enemmän resursseja vaaditaan uusiin kolikoihin. Bitcoinin kaltaisten suosittujen valuuttojen tapauksessa kolikoiden tuottoisa louhinta on lähes mahdotonta, ellei käyttäjä pysty hyödyntämään valtavia laskentaresursseja, jotka ovat useimpien yksilöiden ja pienten ryhmien saavuttamattomissa. Tästä syystä laittomia voittoja tavoittelevat hyökkääjät käyttävät yhä useammin haittaohjelmia, jotka valjastavat uhrien tietokoneet kryptovaluutan louhintaan. Näin he pystyvät hyödyntämään satojentuhansien tietokoneiden laskentatehoa yhden tai kahden tietokoneen sijasta. Vaikka vähäinen tartunta onnistuttaisiin havaitsemaan, kryptovaluutan nimettömyys vaikeuttaa vastuullisten tahojen selvittämistä.

Vuonna 2018 kryptovaluutan louhintahavaintojen prosenttiosuus oli 0,12 % verrattuna kiristysohjelmahavaintojen 0,05 prosenttiin. Monet tekijät vaikuttavat louhintaa suorittavien haittaohjelmien yleistymiseen. Kiristysohjelmista poiketen kryptovaluutan louhinta ei edellytä tietokoneen käyttäjän toimia. Louhija toimii taustalla, kun käyttäjä suorittaa muita tehtäviä tai ei käytä tietokonetta, eikä sitä välttämättä pysty huomaamaan, ellei se heikennä tietokoneen suorituskykyä merkittävästi. Tämän seurauksena käyttäjät eivät välttämättä ryhdy mihinkään toimenpiteisiin ongelman korjaamiseksi, ja louhija voi jatkaa toimintaansa pitkäänkin hyökkääjän hyväksi.

Niin ikään monet "käyttövalmiit" tuotteet kryptovaluuttojen salaiseen louhintaan vaikuttavat tähän trendiin. Kryptovaluutan louhintaohjelmistojen laajan saatavuuden vuoksi aloituskynnys on matala. Kyberrikolliset paketoivat niitä uudelleen haittaohjelmistoiksi ja toimittavat niitä pahaa-aavistamattomien käyttäjien tietokoneisiin. Aseiksi muutetut louhijat jaellaan uhreille hyökkääjille tyypillisillä taktiikoilla, joihin lukeutuvat sosiaalinen manipulointi, haavoittuvuuksien hyväksikäyttö ja ohiajolataukset (drive-by downloads). Kun louhintaohjelmisto on asennettu, se toimii uhrien tietokoneiden taustalla ja suorittaa lohkoketjulaskentaa hyökkääjän hyväksi.

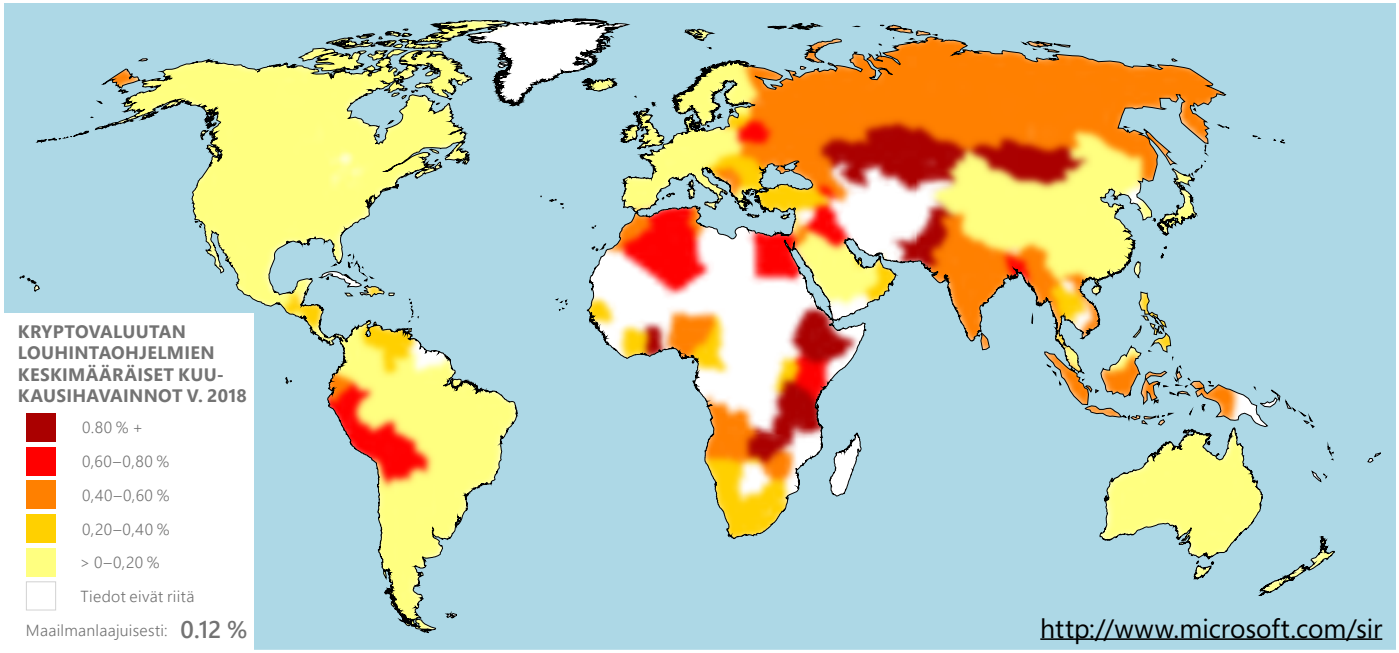
MAAT, JOISSA KRYPTOVALUUTAN LOUHINTAOHJELMIA ON HAVAITTU ENITEN



Etiopia: 5.58 %

Tansania: 1.83 %

Pakistan: 1.47 %



KUVA 3.

Kryptovaluutan louhintaohjelmien keskimääräiset kuukausihavainnot maailmanlaajuisesti maittain/alueittain vuonna 2018

MAAT, JOISSA KRYPTOVALUUTAN LOUHINTAOHJELMIA ON HAVAITTU VÄHITEN

Irlanti: 0.02 %

Japani: 0.02 %

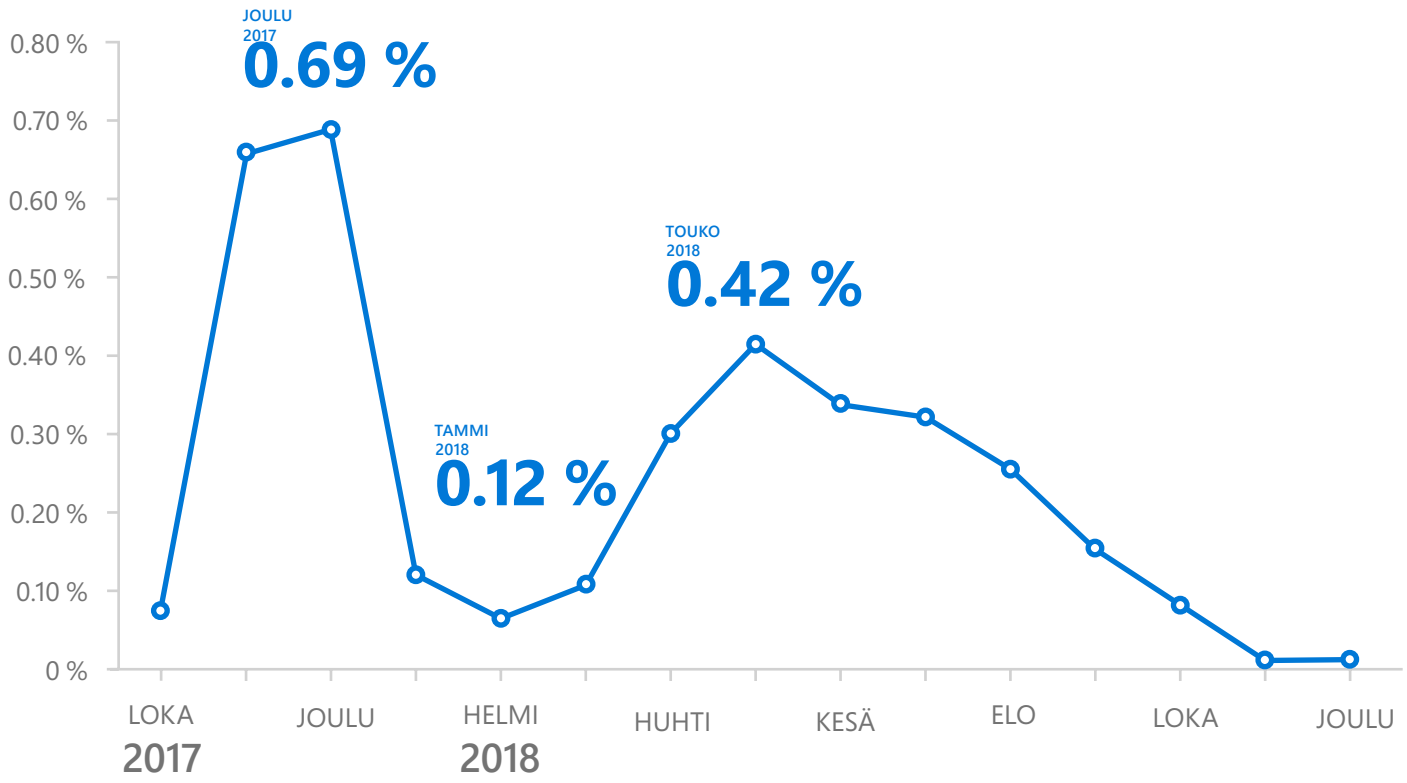
Yhdysvallat: 0.02 %

Viisi sijaintia, joissa kryptovaluutan louhintaohjelmia havaittiin kuukaudessa eniten vuonna 2018, olivat Etiopia (5,58 %), Tansania (1,83 %), Pakistan (1,47 %), Kazakstan (1,24 %) ja Sambia (1,13 %). Kussakin näistä maista kryptovaluutan louhintaohjelmien havaintoja oli 1,13 % tai enemmän. Vähiten kryptovaluutan louhintaohjelmia esiintyi vuonna 2018 Irlannissa, Japanissa, Yhdysvalloissa ja Kiinassa. Kussakin näistä maista esiintymisprosentti oli n. 0,02 % samana ajanjaksona.

SELAINPOHJAISET KRYPTOVALUUTAN LOUHIJAT: UUDENLAINEN UHKA

Tässä luvussa esitetyt tilastot käsittelevät haitallisia kryptovaluutan louhintaohjelmia, jotka on suunniteltu asennettavaksi uhrien tietokoneille haittaohjelmina. Eräät merkittävimmistä kryptovaluuttaa louhivista uhkista ovat kuitenkin täysin selainpohjaisia, eikä niiden asentamiselle ole missään vaiheessa tarvetta. Useat palvelut mainostavat selainpohjaista kryptovaluutan louhintaa keinona, jolla verkkosivustojen omistajat voivat tehdä rahaa sivustojensa liikenteellä ilman mainontaa. Sivuston omistajat lisäävät sivuillensa JavaScript-koodia, joka louhii kryptovaluuttaa taustalla, kun käyttäjä on sivustolla. Tuotot jaetaan sivuston omistajan ja tämän palvelun kesken. Valitettavasti hyökkääjät ovat nopeasti ryhtyneet hyödyntämään näitä kryptovaluutan louhintapalveluita. Loppukäyttäjiltä ei

Brocoiner-havainnot



kysytä lupaa. Usein kryptovaluutan louhintakoodia lisätään täysin asiallisille verkkosivustoille omistajien tietämättä. Nämä selainpohjaiset louhijat eivät edellytä murtautumista loppukäyttäjän tietokoneeseen. Ne toimivat millä tahansa alustalla, jolla on käytössä JavaScriptiä tukeva verkkoselain. Kryptovaluuttaa louhivien troijalaisten tavoin selainpohjaiset louhijat voivat merkittävästi heikentää tietokoneen suorituskykyä ja kuluttaa ylimääräistä sähköä, kun käyttäjä vierailee haittaohjelman sisältävällä verkkosivulla.

KUVA 4.

Havainnot yleisimmästä selainpohjaisesta Brocoiner-louhintaohjelmasta

EI-TOIVOTUN KRYPTOVALUUTAN LOUHINNAN VAIKUTUKSET

Ilmeisin haitta ei-toivotusta kryptovaluutan louhinnasta on laskentaresurssien kulutus, joka voi tuhlata sähköä ja heikentää tietokoneen suorituskykyä merkittävästi. Käyttäjille ja organisaatioille voi aiheutua kryptovaluutan louhinnasta myös muita riskejä, mukaan lukien seuraavat:

Hyökkääjä saa jalansijan ja voi tulevaisuudessa aiheuttaa lisävahinkoa.
Muiden haittaohjelmien tavoin kryptovaluutan louhijat voivat toimia hyökkääjien aloituskohtina. Kun tietokone louhii taustalla kryptovaluuttaa, kyberrikolliset saavat lisätietoa ympäristöstä ja voivat mahdollisesti hyödyntää tietoturvan haavoittuvuuksia muihin tarkoituksiin.

Internetiin liitettyihin laitteisiin voidaan tunkeutua, ja ne voidaan muuntaa kryptovaluuttaa louhiviksi boteiksi.
Monista tällaisista laitteista puuttuvat sisäänrakennetut suojausmekanismit, kuten haittaohjelmien tunnistus, mikä voi tehdä niistä hyökkääjien näkökulmasta haluttuja kohteita.

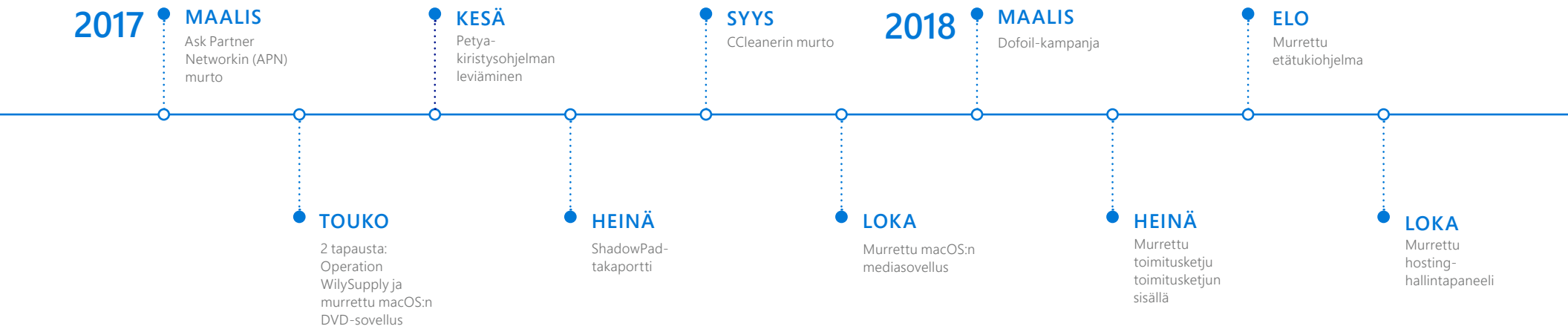
Koneiden vahingoittaminen.
Useita kuukausia tai vieläkin pitempään toimivat kryptovaluutan louhintaohjelmistot voivat heikentää suorituskykyä. Liiallisen virrankulutuksen ja suoritinkäytön tuottama lämpö voi vahingoittaa tietokoneita.

LUKU II

Ohjelmistojen toimitusketjut vaarassa

Microsoft on jo vuosien ajan jäljittänyt haitallisia toimijoita, jotka käyttävät toimitusketjuihin murtautumista hyökkäystensä aloituskohtana. Toimitusketjuhyökkäyksessä hyökkääjä keskittyy legitiimin ohjelmistojulkaisijan kehitys-tai päivitysprosessin murtamiseen.

Onnistuessaan hyökkääjä voi lisätä legitiimiin sovellus- tai päivityspakettiin haitallisen komponentin, joka sitten jaellaan ohjelmiston käyttäjille. Haitallista koodia suoritetaan tämän jälkeen samalla luottamuksella ja samoilla käyttöoikeuksilla kuin varsinaista ohjelmistoa. Ohjelmistojen toimitusketjuhyökkäysten määrä on lisääntynyt viime vuosina, ja siitä on tullut monien kyberturvallisuutta käsittelevien keskustelujen ja IT-osastojen merkittävä huolenaihe.



KUVA 5.

Ohjelmistojen toimitusketjuhyökkäykset v. 2017–2018

MERKITTÄVIMMÄT OHJELMISTOJEN TOIMITUSKETJUHYÖKKÄYKSET V. 2017

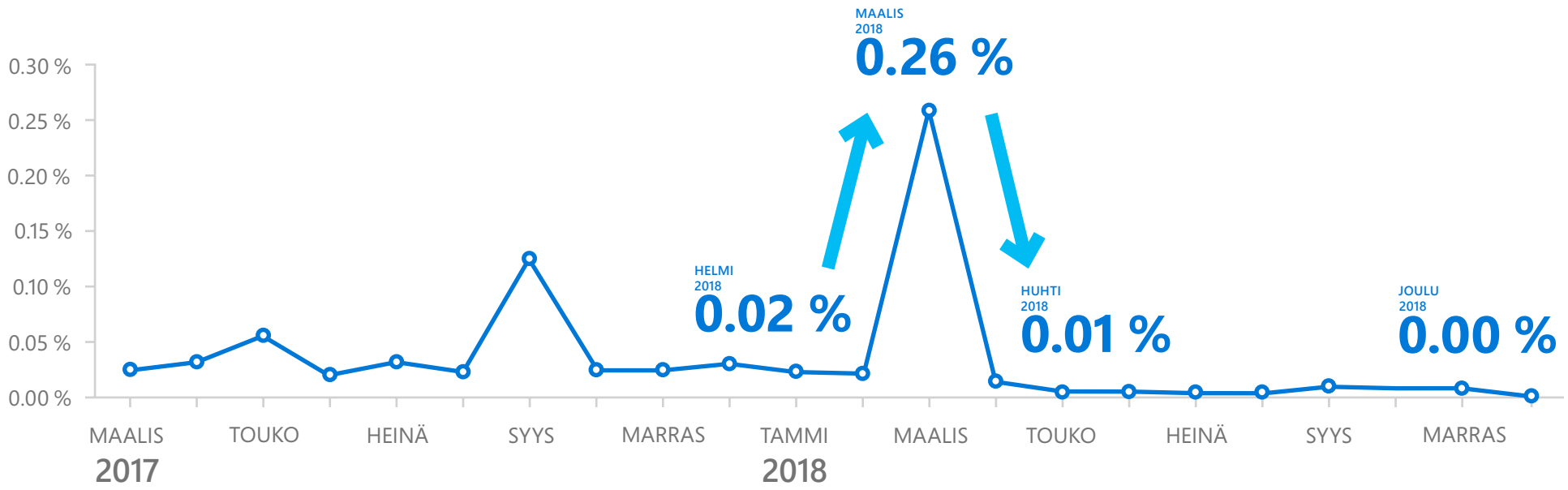
Vuonna 2017 toimitusketjuhyökkäyksistä aiheutui useita julkisuutta saaneita tapauksia. Tunnetuin on Petya-kiristysohjelmiston leviäminen kesäkuussa. Sen ensimmäiset tartunnat jäljitettiin suositun veroilmoitusohjelmiston päivitysprosessiin Ukrainassa. Toukokuussa Operation WilySupply onnistui murtamaan tekstieditorin päivitysohjelmiston ja asentamaan takaportin rahoitus- ja IT-alalla toimiviin kohdeorganisaatioihin. Heinäkuussa takaportti nimeltä ShadowPad piilotettiin palvelimen hallintaohjelmistopakettiin. Sen avulla hyökkääjät pystyivät asentamaan muita haitallisia toimintoja, jotka varastivat dataa ja suorittivat muita rikollisia toimia. Syyskuussa suosittu freeware-työkalu CCleaner murrettiin, ja sen käyttäjäkunnalle toimitettiin takaportilla varustettu versio.

Vuoden 2018 ensimmäinen merkittävä ohjelmistojen toimitusketjuhyökkäys tapahtui 6. maaliskuuta, kun Windows Defender ATP esti laajan yrityksen toimittaa Dofoil-troijalaista (tunnetaan myös nimellä Smoke Loader). Suuri haittaohjelmahyökkäys jäljitettiin tartutettuun vertaissovellukseen. Sovelluksen päivityspaketti korvattiin haitallisella paketilla, joka latasi vuorostaan Dofoil- aittaohjelmiston asentavaa saastunutta koodia. Edistynyt troijalainen louhi kryptovaluuttaa ja sisälsi hienostuneita prosessienvälisen injektion tekniikoita, selviytymismekanismeja ja pakoilumenetelmiä.

KUVA 6.

Vuoden 2018 Dofoil (Smoke Loader) -havainnoissa näkyy estettyjen tapausten piikki maaliskuun kohdalla.

Dofoil-havainnot



Kampanjan ensimmäisten 12 tunnin aikana Windows Defender Antivirus -virustorjunta esti maailmanlaajuisesti yli 400 000 tartuntayritystä. Globaaleista havainnoista 73 % tehtiin Venäjällä, 18 % Turkissa ja 4 % Ukrainassa.

Useiden muidenkin hyökkäysten tunnistettiin vuonna 2018 käyttävän murrettuja ohjelmistojen toimitusketjuja välitysmekanismeina, mukaan lukien seuraavassa taulukossa kuvatut:

Jakso	Hyökkäys	Kuvaus	Murretut ohjelmistot
Maaliskuu 2018	Kryptovaluutan louhintakampanja Dofoil (Microsoftin raportoima).	Hyökkääjät tartuttivat vertaisjärjestelmäsovelluksen päivitysprosessin ja asensivat Dofoilin, joka asensi vuorostaan kryptovaluuttaa louhivan haittaohjelman.	Vertaisverkkosovellus.
Heinäkuu 2018	Murrettu toimitusketjun sisäinen toimitusketju (Microsoftin raportoima).	Hyökkääjät mursivat PDF-muokkausohjelman toimittajan ja sen erään ohjelmistotoimittajakumppanin jaetun infrastruktuurin.	PDF-muokkaussovellus ja kolmannen osapuolen toimittajakumppani.
Elokuu 2018	Murrettu etätukiohjelma (Operation Red Signature, Trend Micron ja IssueMakersLabin raportoima).	Etätukiratkaisujen toimittajan päivityspalvelin murrettiin, ja sen kautta välitettiin etäyhteystyökalua nimeltä 9002 RAT.	Etätukiohjelma.
Lokakuu 2018	Murrettu hosting-hallintapaneeliratkaisu (ESETin raportoima).	Hosting-hallintapaneeliratkaisun asennuskomentosarjaa muokattiin siten, että se varasti tunnistetiedot.	Hosting-hallintapaneeliratkaisu.

KUVA 7.

Muut ohjelmistojen toimitusketjuhyökkäykset v. 2018

LUOTTAMUS VAARASSA

Toimitusketjuhyökkäykset ovat kavalia, koska ne hyödyntävät käyttäjien ja IT-osastojen luottamusta käytössä oleviin ohjelmistoihin. Murretut ohjelmistot ovat usein toimittajan allekirjoittamia ja sertifioimia, eivätkä ne anna välttämättä mitään merkkejä ongelmasta. Näin ollen tartunnan tunnistaminen on huomattavasti vaikeampaa. Ne voivat vahingoittaa toimitusketjujen ja niiden asiakkaiden suhteita, olipa kyse yritys- tai kotikäyttäjistä. Ohjelmistoja tartuttamalla sekä toimitus- ja päivitysinfrastruktuureita heikentämällä toimitusketjuhyökkäykset vaikuttavat organisaatioiden toimittamien tuotteiden ja palveluiden eheyteen ja tietoturvaan.

Toimitusketjuhyökkäykset ovat kohdistuneet monenlaisiin ohjelmistoihin sekä eri sektoreilla ja maantieteellisillä alueilla toimiviin organisaatioihin. Toimitusketjuhyökkäysten ongelma koskee koko toimialaa ja edellyttää useiden sidosryhmien huomiota, mukaan lukien koodia kirjoittavat ohjelmistokehittäjät ja toimittajat, ohjelmistojen asennuksia hallinnoivat järjestelmänvalvojat sekä tietoturvayhteisö, joka havaitsee nämä hyökkäykset ja luo ratkaisuja niiltä suojautumiseen.

EI VAIN OHJELMISTOJA: TOIMITUSKETJUJEN MURTAMINEN PILVIOBJEKTIEN KAUTTA

Toimitusketjuhyökkäyksistä seuraava luottamuksen heikentyminen on vielä vakavampaa ja monimutkaisempaa pilvipalveluiden tapauksessa. Tätä monimutkaisuutta ilmentävät useat pilviobjektien, pilvipalveluiden ja pilvi-infrastruktuurien murrot vuonna 2018:

- Tartutetut Chrome-laajennukset asensivat napsautuspetoksia suorittavia haittaohjelmia (ICEBRGin raportoima)
- Useat murretut Linux-tietovarastot (raportoitu eräillä verkon keskustelufoorumeilla)
- Haitallisia WordPressin laajennuksia käytettiin erilaisiin haittatoimintoihin – hyökkääjät pystyivät mm. julkaisemaan sisältöä WordPress-sivustoilla (Wordfencen raportoima)
- Haitalliset Docker-näköistiedostot sisälsivät komentosarjan, joka latasi kryptovaluutan louhintaohjelmiston ja lähetti sen Docker Hub -tilille (Fortinetin ja Kromtechin raportoima)
- Kirjoitusvirhettä hyödyntävä haitallinen paketti virallisessa Python-tietovarastossa; paketti sisälsi komentosarjan, jolla ladattiin leikepöydällä olevia kryptovaluutan louhintaosoitteita kaappaava haittaohjelma (Mediumin raportoima)
- Murrettu StatCounter-komentosarja tarjosi hyökkääjille mahdollisuuden injektoida haitallinen komentosarja StatCounteria käyttäville verkkosivustoille (ESETin raportoima)
- Useita tapauksia, joissa npm-moduuleihin lisättiin takaportti (The npm Blog, Medium). Takaporttia hyödyntämällä hyökkääjä pystyi esimerkiksi lisäämään haluamaansa koodia käynnissä olevalle palvelimelle ja suorittamaan sitä.

Nämä tapaukset osoittavat, kuinka toimitusketjujen murtaminen voi merkittävästi laajentaa hyökkäyksen pinta-alaa. Suojaamattomat pilviobjektit voivat toimia odottamattomina aloituspisteinä. Esimerkiksi Docker Hub -tapauksessa hyökkäyksessä käytetty tili latasi Docker-näköistiedostoja, jotka sisälsivät piilotetun takaoven kryptovaluutan louhintaan. Docker-näköistiedostoja ylläpidettiin Docker Hubissa lähes vuoden ajan, ja niitä ladattiin miljoonia kertoja pahaa-aavistamattomien järjestelmänvalvojien ja käyttäjien toimesta.

Toimitusketjun riskit ulottuvat pilvessä sijaitsevaan koodiin, avoimen lähdekoodin ratkaisuihin, web-kirjastoihin, palvelukomponentteihin ja muihin pilviobjekteihin. Nämä riskit sekä julki tulleiden ohjelmisto- ja laitteistotoimittajien toimitusketjumurtojen suuri vaihtelu ovat yhdessä tehneet toimitusketjuhyökkäyksistä laaja-alaisen uhkan. Vaikka tällaisten hyökkäysten koko kirjolle ei ole tarjolla yksittäistä ratkaisua, organisaatioiden on kehitettävä ennaltaehkäisevää suojausta ja murtojen jälkeisiä tunnistustoimia laitteisto- ja ohjelmistotoimittajien, avoimen lähdekoodin ohjelmistotoimittajien sekä pilvipalvelu- ja infrastruktuuritoimittajien toimitusketjuihin kohdistuvien murtojen varalta.

DART tutkii kyberrikollisuutta

Microsoftin tunnistus- ja vastetiimi (Microsoft Detection and Response Team, DART) on globaali kyberturvallisuuden asiantuntijoista ja haittaohjelmien torjujista koostuva tiimi, joka auttaa organisaatioita tunnistamaan ja tutkimaan kyberturvallisuuden ongelmia ja vastaamaan niihin. Tässä luvussa on tuotu esille eräitä asiakastapauksia, joita DART käsitteli viime vuoden aikana. Siitä tulevat esille hyökkäysten yleiset trendit sekä se, kuinka Microsoft ja asiakkaat ovat onnistuneet torjumaan niitä.

ASIANTUNTIJAPALVELUITA TARJOAVA ORGANISAATIO KOKI KANSALLISVALTION SUORITTAMAN HYÖKKÄYKSEN, JOSSA DATAA VARASTETTIIN HUOMAAMATTA

Asiantuntijapalveluita tarjoavaan organisaatioon kohdistui kehittynyt valtiollisen toimijan rahoittama edistynyt pitkäkestoinen hyökkäys (Advanced Persistent Threat, APT), jonka avulla onnistuttiin hankkimaan organisaation etuoikeutettujen käyttäjien tunnistetietoja. Hyökkääjät pääsivät verkkoon käyttämällä spray-tyyppistä salasanahyökkäystä. Pienellä joukolla heikkoja tai yleisesti käytössä olevia salasanoja (esim. "p@ssword" ja "123456") pyrittiin murtamaan suurta joukkoa käyttäjätilejä ja hankkimaan Office 365:n järjestelmänvalvojan tunnistetiedot. (Spray-tyyppisiä salasanahyökkäyksiä käytetään tunnistusten välttämiseksi, sillä tilikohtaisten sisäänkirjautumisyritysten määrää on rajoitettu.) Verkkoon tunkeutumisen jälkeen tämä APT-hyökkäys keräsi automaattisesti perusteellista tietoa työntekijöiden postilaatikoista. Useista yrityksen sisäisistä torjuntayrityksistä huolimatta hyökkääjä onnistui pysyttelemään verkossa yli 200 päivän ajan. Hyökkäykseen kuului myös organisaation toimitusketjuohjelmiston hyödyntäminen ja datan automaattinen luvaton siirto.

Koska organisaatio epäili asiakastietojensa murtamista, se pyysi DART-tiimiä tutkimaan asiaa ja estämään lisävahingot. DART tunnisti kohteena olevat Office 365 -postilaatikoiden haut, murretut tilit sekä hyökkääjän käyttämät komento- ja hallintakanavat. Tämän tapauksen keskeinen opetus oli, että pilvipalveluita on suojattava identiteettipohjaisilta uhkilta ja hyökkäyksiltä erilaisia hallintatoimia soveltamalla. Organisaatio otti käyttöön monimenetelmäisen todennuksen (MFA), ehdolliset käyttöoikeuskäytännöt tietyille pilvisovelluksille sekä Office 365 -lokikirjauksen. Vastaavilta uhkilta suojautuakseen tulevaisuudessa organisaatio saattaa myös ottaa käyttöön päätepisteiden uhkien tunnistus- ja vasteratkaisun (threat detection and response, EDR). Sen avulla organisaatio voi tunnistaa hyökkääjiä, jotka yrittävät hyödyntää sen verkkoa. Lisäksi esitimme kyseiselle organisaatiolle suosituksen siitä, että se nimeää pilvipalveluita hallinnoivan yksikön tai globaalin identiteettitiimin, joka hallitsee ja valvoo asianmukaisia käyttäjien todennuskäytäntöjä. Näin organisaatio pystyy valvomaan tietoturvavalmiuksiaan paremmin ja vähentämään riskejä tehokkaammin.

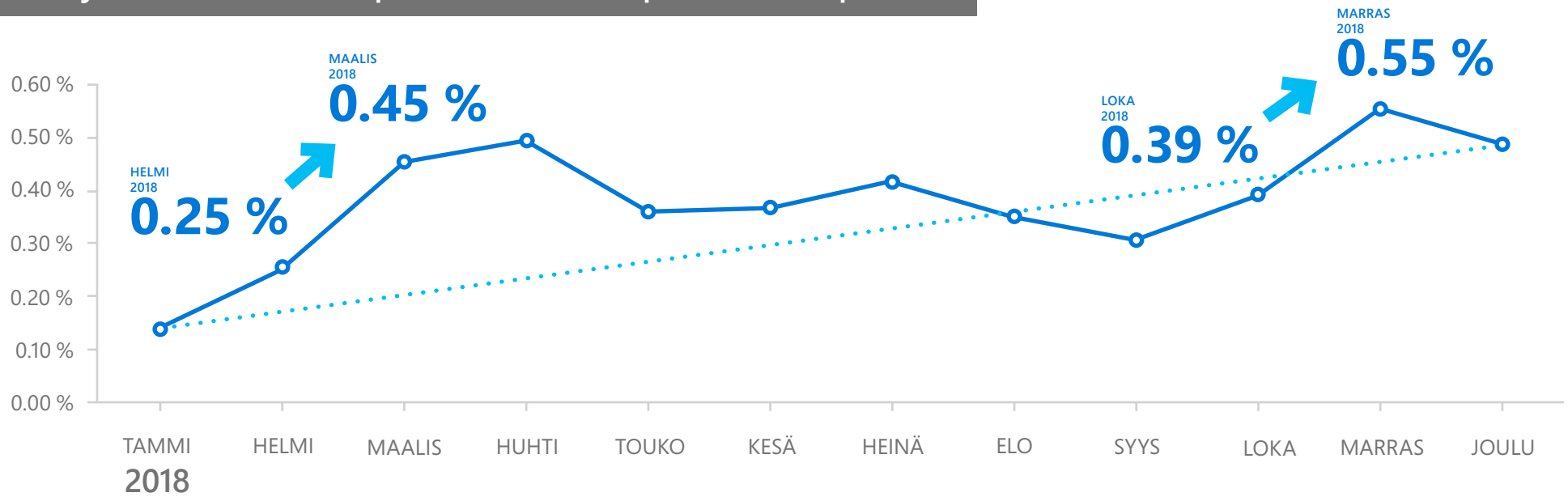
LUKU III

Tietojenkalastelu on edelleen ongelma

Vuonna 2018 Microsoftin uhka-analyytikot ovat nähneet todisteita siitä, että tietojenkalastelu on edelleen hyökkääjien suosiossa. Tietojenkalastelu tulee olemaan ongelma myös tulevaisuudessa, sillä siihen liittyy inhimillisiä päätöksiä ja arvioita. Kyberrikolliset pyrkivät houkuttelemaan uhrejaan kaikin keinoin.

Tietojenkalastelu on edelleen kasvussa

Tietojenkalasteluviestien prosenttiosuus saapuvista sähköposteista



KUVA 8.

Tietojenkalasteluviestit vuonna 2018

TIETOJENKALASTELU OLI EDELLEEN SUOSITTU HYÖKKÄYSTAPA VUONNA 2018

Microsoft analysoi ja skannaa Office 365:ssä yli 470 miljardia sähköpostiviestiä joka kuukausi tietojenkalastelun ja haittaohjelmien varalta. Sen ansiosta analyytikot saavat merkittävää tietoa hyökkääjien trendeistä ja tekniikoista. Tietojenkalastelua sisältävien saapuvien sähköpostien määrä kasvoi 250 prosenttia vuoden 2018 tammikuun ja joulukuun välillä. Tietojenkalastelu on edelleen yksi tärkeimmistä hyökkäystavoista, jota käytetään sellaisten haittaohjelmien toimitukseen, joita ei ole vielä pystytty torjumaan. Uusilla tietojenkalastelun vastaisilla toimilla, tunnistusmenetelmillä, tutkimuksilla ja vastevalmiuksilla Microsoft on jatkuvasti vahvistanut ohjelmistojensa käyttäjien puolustusasemaa näitä hyökkäyksiä vastaan.

Tietojenkalastelun hyökkäystapojen kehitys

Tietojenkalastelulta suojaavien työkalujen ja tekniikoiden kehittyessä hyökkääjät ovat joutuneet itsekin mukautumaan. Tietojenkalasteluhyökkäyksistä on tullut entistä monimuotoisempia. Tämä tarkoittaa, että hyökkääjät eivät käytä yksittäistä URL-osoitetta, verkkotunnusta tai IP-osoitetta sähköpostien lähettämiseen, vaan käytössä on vaihteleva infrastruktuuri, jossa on useita hyökkäyspisteitä. Myös hyökkäysten luonne on muuttunut: nykyaikaiset tietojenkalastelukampanjat vaihtelevat muutaman minuutin lyhytkestoisista hyökkäyksistä paljon pitempiin kampanjoihin, joiden volyymit ovat mittavia. Toiset hyökkäykset ovat sarjallisia variantteja: hyökkääjät lähettävät sähköpostia lyhyissä erissä useina peräkkäisinä päivinä.

Lisäksi Microsoft on havainnut trendin, jossa hyökkääjät käyttävät ylläpidettyä infrastruktuuria ja muita julkisia pilvi-infrastruktuureita. Legitiimien sivustojen ja resurssien joukkoon piiloutumalla ne pystyvät helpommin välttämään tunnistuksen. Hyökkääjät esimerkiksi käyttävät yhä useammin julkisia asiakirjojen jakosivustoja sekä yhteistyösivustoja ja -palveluita, joiden kautta he jakelevat haitallisia toimintoja sekä käyttäjätietoja varastavia väärennettyjä kirjautumislomakkeita. Lisäksi murrettuja tilejä käytetään yhä useammin haitallisten sähköpostien välittämiseen sekä organisaatioiden sisä- että ulkopuolelle.

Tietojenkalastelua tapahtuu niin kohdennetuilla kuin laajamittaisilla kampanjoilla

Muiden haittaohjelmien tavoin tietojenkalastelukampanjat vaihtelevat kohdennetuista kampanjoista laajapohjaisiin, yleisluontoisiin hyökkäyksiin. Vaikka pitkälle kehitetyt hyökkäykset tuottavat suurempia voittoja yksittäistä tiliä kohti, yleisluontoisemmat hyökkäykset kohdistuvat laajempaan käyttäjäjoukkoon, vaikka niiden tilikohtaiset voitot jäävät pienemmiksi.

Esimerkki kehittyneestä ja kohdennetusta kampanjasta on Ursnif. Siinä hyökkääjät lokalisoivat asiakirjan tiedostonimen kohteen kannalta tutun organisaation tai toimialan tyyliseksi. Tällaiset hyökkäykset eroavat suuresti laajapohjaisista kampanjoista – ne näyttävät aidommilta ja luotettavammilta.

Eräät vuoden 2018 laajapohjaiset kampanjat liittyivät yritysten sähköpostien murtamiseen (BEC), tunnettujen brändien, verkkotunnusten ja käyttäjien jäljittelyyn kohdeorganisaatioissa sekä kehittyneisiin tekeytymiskampanjoihin. Verkkotunnuksen jäljittely on yleinen hyökkäystaktiikka, jolla organisaatiot yritetään saada uskomaan siihen, että sähköposti on luotettava ja syytä avata.

Tietojenkalastelun syötit ovat moninaisia

Microsoftin tutkijat ovat havainneet, että kampanjoissa käytetään monia eri tyyppisiä tietojenkalastelun syöttejä tai toimintoja, mukaan lukien seuraavat:

- **Verkkotunnukseksi tekeytyminen** (sähköpostin verkkotunnus vastaa täydellisesti alkuperäistä verkkotunnusta)
- **Verkkotunnuksen jäljittely** (sähköpostin verkkotunnus muistuttaa suuresti alkuperäistä verkkotunnusta)[2]
- **Käyttäjäksi tekeytyminen** (sähköposti näyttää tulevan henkilöltä, johon luotat)
- **Tekstisyötit** (tekstiviesti näyttää tulevan legitiimiltä lähteeltä, esimerkiksi pankilta, julkishallinnon virastolta tai toiselta yritykseltä – tällä yritetään kasvattaa luottamusta pyyntöihin, joilla uhria pyydetään lähettämään arkaluonteista tietoa, kuten käyttäjätunnuksia, salasanoja tai luottamuksellisia taloustietoja)
- **Tunnistetietojen kalastelulinkit** (sähköposti sisältää linkin sivulle, joka muistuttaa legitiimin sivuston kirjautumissivua, jotta käyttäjät antaisivat kirjautumistietonsa)
- **Tietojenkalasteluliitteet** (sähköposti sisältää haitallisen liitetiedoston, ja lähettäjä houkuttelee uhria avaamaan sen)
- **Linkit väärennettyihin pilvitallennussijainteihin** (sähköpostin lähettäjä näyttää legitiimiltä – viestissä kehotetaan käyttäjää antamaan oikeudet ja/tai syöttämään esim. tunnistetietonsa, ja vastineeksi hän saa käyttöoikeuden väärennettyyn pilvitallennussijaintiin)

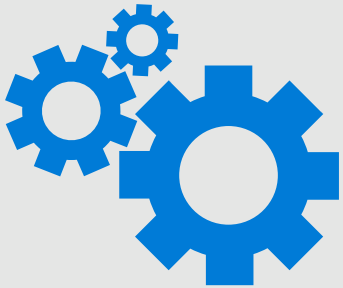
Organisaatioiden näkökulmasta tämä hyökkääjien käyttämien potentiaalisten syöttien moninaisuus tekee tietojenkalastelun torjumisesta entistä monimutkaisempaa.

ALAVIITTEET

[2] Verkkotunnuksen jäljittely voi muistuttaa verkkotunnukseksi tekeytymistä (täysin alkuperäistä vastaavaa nimeä) siinä poikkeustapauksessa, että verkkotunnus näkyy sähköpostiviestin näyttönimessä.

DART tutkii kyberrikollisuutta

SUUREEN VALMISTAVAN TEOLLISUUDEN ORGANISAATIOON ISKETTIIN KOHDENNETUILLA TIETOJENKALASTELUVIESTEILLÄ



Eräs valmistavan teollisuuden organisaatio kärsi useiden kuukausien ajan monivaiheisesta tietojenkalastelukampanjasta. Tämä lähestymistapa ei ole poikkeuksellinen. Ensimmäisen vaiheen aikana hyökkääjä suorittaa tiedustelua ja toisessa vaiheessa kohdistaa hyökkäyksen korkeassa asemassa toimiviin henkilöihin. Kampanjan ensimmäisessä osassa hyödynnettiin tunnettua tietojenkalastelukeinoa. Pienelle, kohdennetulle joukolle lähetettiin sähköpostiin upotettu linkki huijaussivustolle. Sähköpostissa väitettiin, että kohdehenkilön oli tarkastettava tärkeä sähköinen asiakirja. Vastaanottaja saisi siihen käyttöoikeudet omilla toimialueen tunnistetiedoillaan. Todellisuudessa "tärkeän asiakirjan" tarkastusta varten luotu väärennetty aloitussivu keräsi tunnistetiedot ja antoi hyökkääjälle käyttöoikeudet eri puolilla maailmaa sijaitseville Office 365 -tileille. Tietojenkalastelukampanjan toisessa vaiheessa samanlaisia sähköposteja lähetettiin korkeassa asemassa toimiville henkilöille. Tämän tavoitteena oli hankkia oikeudet vieläkin arvokkaampiin tietoihin. Microsoft toimi yhteistyössä tämän asiakkaan kanssa tietojenkalastelukampanjan toisessa vaiheessa. Tapauksen keskeinen opetus on se, että tietojenkalastelu on tänäkin päivänä yksi tehokkaimmista hyökkäyskeinoista, ja käyttäjät ovat edelleen heikoin lenkki. Käyttäjien kouluttaminen tietojenkalastelun varalta, hyökkääjien tunnistamiseen ja torjuntaan soveltuvat työkalut sekä järjestelmien säännölliset korjauspäivitykset ovat tärkeitä osa-alueita. Jos organisaatiossa ei puututa näistä yhteenkään, se on potentiaalisesti haavoittuvassa asemassa.

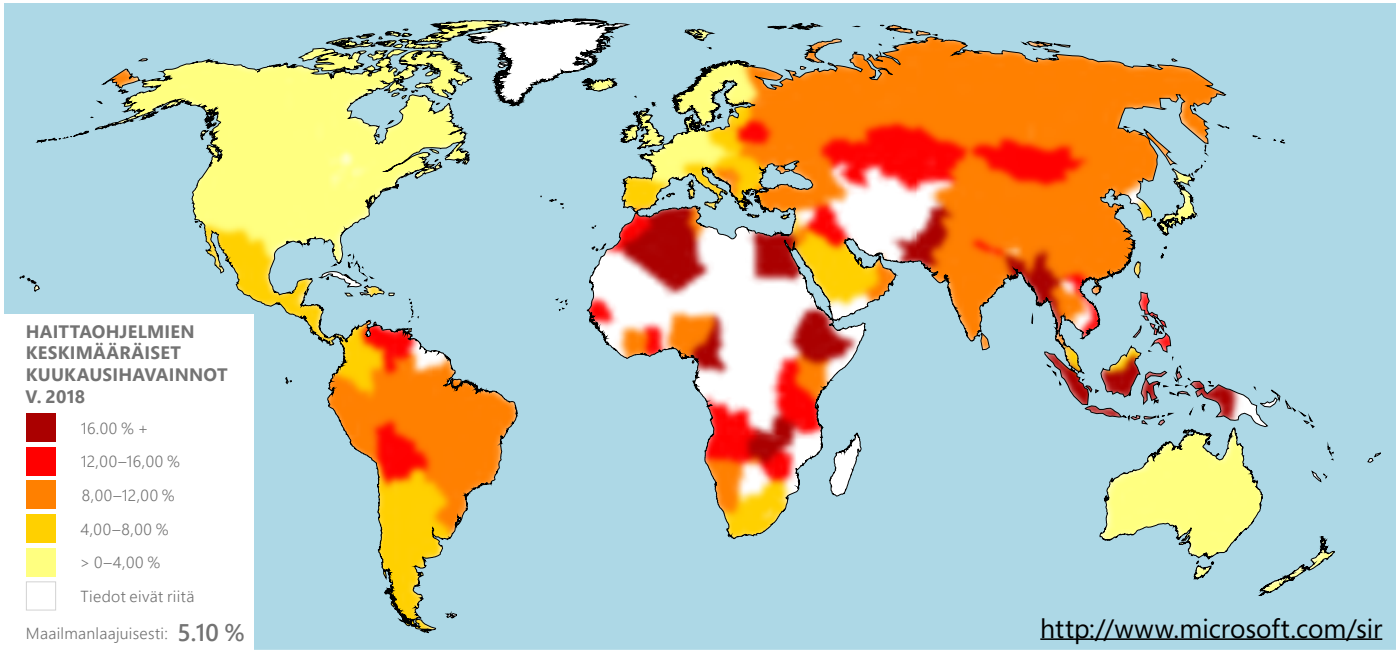
Tässä tapauksessa asiakkaan tärkeimpänä prioriteettina oli välitön tarve evätä murrettujen tilien käyttöoikeudet. Yhdessä Azure Identity- ja Office 365 -tiimien kanssa DART laati suunnitelman, jolla hyökkääjä poistettiin verkosta. Samalla komento- ja hallintakanavan kaikkea liikennettä ryhdyttiin valvomaan uudella Microsoft Azure Log Analytics -ratkaisulla. Tiimi pystyi ratkaisemaan ongelman vain kolmessa tunnissa. Hyökkääjän pääsy estettiin, ja organisaatio pystyi keskittymään vahinkojen arviointiin ja palautumiseen. DART käytti Azure Log Analytics -työkaluja selvittäessään hyökkääjän käyttäytymistä. Tämän myötä organisaatiolle paljastui monia määrityksiin liittyviä ongelmia. DART tunnisti esimerkiksi aukkoja kriittisten palvelinten korjauspäivityksissä sekä löysi verkosta tietokoneita, jotka välittivät tietoa tunnetuille haitallisille Internet-isännille. Lisäksi se löysi useita tärkeitä palvelimia, joita ei ollut suojattu haittaohjelmilta.

LUKU IV

Haittaohjelmat ympäri maailmaa

Haittaohjelmat aiheuttavat riskejä organisaatioille ja yksityishenkilöille heikentyneen käytettävyyden, tietojen menetyksen, immateriaalioikeuksilla suojatun omaisuuden varastamisen, rahallisten tappioiden ja stressin muodossa. Lisäksi ne voivat jopa vaarantaa ihmishenkiä. Microsoft käyttää monenlaisia työkaluja ja tekniikoita haittaohjelmatartuntojen tunnistamiseen, estämiseen ja poistamiseen mistä tahansa.

Haittaohjelmahavaintojen määrä vaihteli vuonna 2017 n. 5 prosentista yli 7 prosenttiin. Alkuvuonna 2018 luvut nousivat, mutta loppuvuoden aikana ne laskivat hieman yli 4 prosenttiin. Mahdollisia syitä haittaohjelmien havaintojen kokonaismäärän laskulle vuonna 2018 ovat Windows 10:n yleistyminen sekä Windows Defender -suojauksen käytön lisääntyminen. Haittaohjelmien havaintomäärät perustuvat siihen, kuinka moni Windows Defender -virustentorjuntaa käyttävistä koneista raportoi haittaohjelmahavainnoista kuukauden aikana. Niihin sisältyvät Defenderin torjumat tartuntayritykset.



KUVA 9.

Haittaohjelmien keskimääräiset kuukausihavainnot maailmanlaajuisesti maittain/alueittain vuonna 2018

Viisi sijaintia, joissa haittaohjelmia havaittiin kuukaudessa eniten vuonna 2018, olivat Etiopia (keskimäärin 26,33 % kuukauden aikana), Pakistan (18,94 %), Palestiinalaisalueet (17,50 %), Bangladesh (16,95 %) ja Indonesia (16,59 %). Kussakin näistä maista haittaohjelmien havaintoja oli tällä kaudella keskimäärin 16,59 % tai enemmän. Tartuntamäärät korreloivat yleensä vahvasti yhteiskunnan kehityksen ja teknologiavalmiuksien kanssa. Kaikki maat, joissa havaintoja oli eniten vuonna 2018, sijoittuvat vuoden 2017 ICT-indeksin alimpaan 40 prosenttiin. Indeksiä julkaisee YK:n alainen Kansainvälinen televiestintäliitto.

Viisi sijaintia, joissa haittaohjelmia havaittiin kuukaudessa vähiten samana ajanjaksona, olivat Irlanti (1,26 %), Japani (1,51 %), Suomi (1,74 %), Norja (1,79 %) ja Alankomaat (1,82 %). Kussakin näistä maista haittaohjelmien havaintoja oli tällä kaudella keskimäärin 1,82 % tai vähemmän. Näissä paikoissa kyberturvallisuuden infrastruktuurit ovat usein kehittyneitä ja käytössä on vakiintuneita ohjelmia kriittisen infrastruktuurin suojaukseen. Lisäksi kansalaisille tarjotaan perustietoa tietoturvasta.

MAAT, JOISSA HAITTAOHJELMIA ON HAVAITTU ENITEN

Etiopia: **26.33 %**

Pakistan: **18.94 %**

Palestiinalaisalueet: **17.50 %**

DART tutkii kyberrikollisuutta

USEAT RAHOITUSALAN ORGANISAATIOT KOKIVAT KANSALLISVALTIOIDEN TOTEUTTAMIA HYÖKKÄYKSIÄ, JOTKA HÄIRITSIVÄT TOIMINTAA

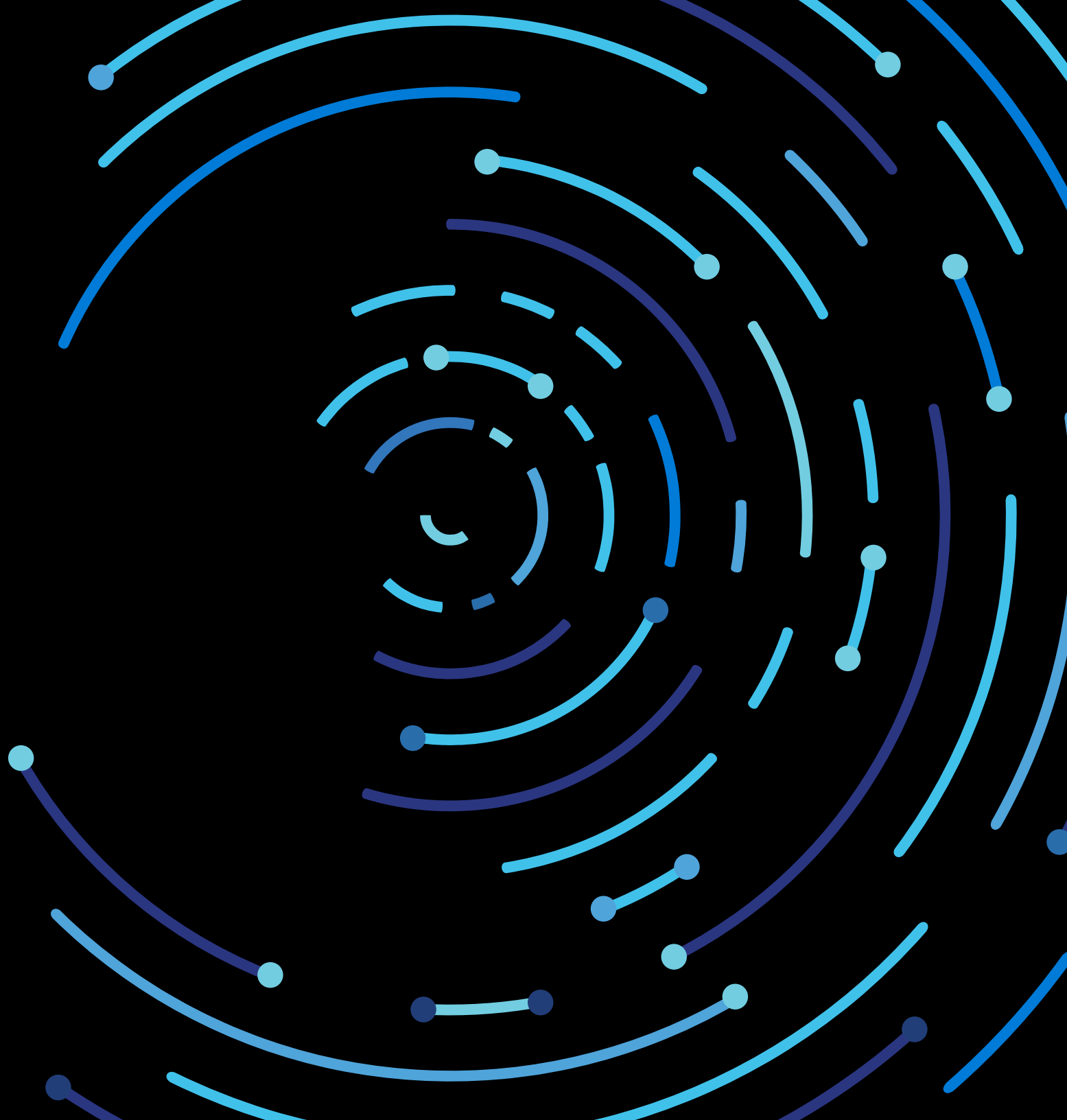
DART kohtasi yhden tuhoisimmista näkemistään tapauksista, kun useisiin rahoituspalveluita tarjoaviin organisaatioihin hyökättiin valtiollisen toimijan rahoittamalla edistyneellä pitkäkestoisella hyökkäyksellä (APT). Kyse oli eri ryhmästä kuin aiemmin mainitussa asiantuntijapalveluorganisaatioon kohdistuvassa hyökkäyksessä, mutta toimintatavat olivat samantapaiset.

Tällä hyökkäyksellä onnistuttiin hankkimaan järjestelmänvalvojan oikeudet, kun tartunnan alkulähteenä toiminut kone saastutettiin erittäin kohdennetulla ja piilotetulla takaportilla. Se toimitettiin mahdollisesti luotettavaksi naamioidun tietojenkalasteluviestin avulla. Tämän seurauksena hyökkääjä suoritti useita petollisia tapahtumia ja siirsi suuria rahasummia ulkomaisille pankkitileille. Joissakin tapauksissa hyökkääjää ei havaittu yli 100 päivään. Kun hyökkääjä ymmärsi, että toiminta oli havaittu, se otti nopeasti käyttöön esivalmistellun hyökkäysmenetelmän. Hyökkääjä toimitti tuhoisan haittaohjelmiston yli puoleen ympäristön koneista. Asiakkaiden toiminta keskeytyi usean päivän ajaksi.

Näistä tapauksista opittiin useita keskeisiä asioita. Ensimmäinen oli se, että ohjelmiston elinkaaren hallinta on erittäin tärkeää. Järjestelmien (käyttöjärjestelmien ja tietoturvan) säännöllisistä päivityksistä, korjauksista ja auditoinneista on huolehdittava. Yhdessä tapauksessa organisaation Linux-järjestelmäympäristössä oli poikkeuksellisen suuri määrä täysin hallitsemattomia työkuormia, minkä seurauksena se oli erittäin altis hyökkäyksille. Toinen opetus oli se, että on tärkeää säilyttää varmuuskopioita järjestelmän tiedoista offline-sijainnissa, mikäli ensisijaiset tiedot menetetään. Lisäksi opittiin, että perinteiset virustentorjuntaratkaisut eivät välttämättä riitä hyökkääjien toiminnan selvittämiseen.

Normaaliin toimintaan palaaminen oli näiden organisaatioiden tärkein prioriteetti. DART auttoi palauttamaan palveluiden toiminnan tutkimalla ensin hyökkäyksen vaikutuksia ja ryhtymällä sitten tarvittaviin torjuntatoimiin, mukaan lukien haittaohjelmien poistaminen tartutetuista järjestelmistä sekä järjestelmien entisöinti normaaliin tilaan. Tiimi myös koulutti asiakkaita käyttämään Microsoftin uhkientunnistustyökaluja (mm. EDR), jotta ne pystyvät havaitsemaan verkoistaan poikkeavuuksia ja hyökkääjien toimintatapoja. DART korosti päätepisteiden valvonnan tärkeyttä puolustauduttaessa kehittyneitä ja kohdennettuja hyökkäyksiä vastaan. Perinteiset virustentorjuntaratkaisut eivät välttämättä havaitse niitä.

Opastus



Opastus

Organisaation sietokyvyn ja merkityksellisen riskienhallinnan kehittäminen edellyttää tietoturvaan sellaista lähestymistapaa, johon sisältyvät yhtä lailla ennaltaehkäisy, tunnistus ja reagointi. Olemme järjestäneet seuraavat ehdotukset tietoturvan parhaiksi käytännöiksi ja hallintatoimiksi näihin luokkiin.

ENNALTAEHKÄISY:

Ennaltaehkäisevät hallintatoimet ovat avainasemassa puolustuksen kokonaisstrategiassa. Oikeat investoinnit voivat kasvattaa kyberrikollisten hyökkäyskustannuksia ja ylläpitää näitä korkeita kustannuksia myös pitemmällä aikavälillä (ilman, että ammattimaisen analyytikon on valvottava ja tulkittava tuotostietoja.) Ennaltaehkäisevän valvonnan investoinnit on syytä kohdentaa tekniikoihin, jotka voidaan toteuttaa pienimmillä kustannuksilla. Niiden avulla voidaan tasaisesti torjua edullisia mutta tehokkaita hyökkäystekniikoita.

Ennaltaehkäisyssä on hyvä huomioida neljä asiaa:

1. **Tietoturvan puhtaus on ratkaisevan tärkeää. Kuten osasta tämän raportin esimerkeistä voi havaita, yleiset puhtausongelmat voivat heikentää myös edistyneitä tietoturvaominaisuuksia. Seuraavien vinkkien noudattaminen voi auttaa vähentämään riskejä:**

- Vältä tuntemattomien maksuttomien ohjelmien ja/tai piraattiohjelmien käyttöä. Käytä vain luotettavista lähteistä peräisin olevia ohjelmistoja.

- Vähennä tunnistetietojen varkausriskejä mm. suojaamalla etuoikeutettujen järjestelmänvalvojien tilit. Lisätietoja saat lukemalla tämän blogiartikkelin, jossa on kuvattu Microsoftin soveltamia periaatteita ja työkaluja omien tietoturvavalmiuksiensa parantamiseksi. Artikkelissa on myös kuvattu etenemissuunnitelmia, jotka auttavat sinua suunnittelemaan omia hankkeitasi.

- Sovella ohjelmistotoimittajien kuvailemia tietoturvallisia määritysten perustasoja.

- Pidä koneet ajan tasalla ottamalla nopeasti käyttöön uusimmat käyttöjärjestelmä- ja sovelluspäivitykset. Asenna välittömästi kriittiset suojauspäivitykset käyttöjärjestelmiin, selaimiin ja sähköpostiohjelmiin. Eristä (tai poista käytöstä) koneet, joiden ohjelmistoja ei voi päivittää tai korjata.

- Käytä kehittyneitä sähköposti- ja selainsuojauksia. Ota käyttöön tietoturvallinen sähköpostiyhdyskäytävä, joka sisältää edistyneitä uhkien torjuntaominaisuuksia ja pystyy puolustautumaan nykyaikaisilta tietojenkalastelun varianteilta.

- Ota isäntäkoneissa käyttöön haittaohjelmien torjunta ja verkkopuolustus, jotta pystyt hyödyntämään lähes reaaliaikaisia torjuntavastauksia pilvestä (jos ratkaisusi tukee niitä).

2. **Ota käyttöön käyttöoikeuksien valvonta. Huomioi seuraavat tekijät:**

- Sovella mahdollisimman vähäisten käyttöoikeuksien periaatetta. Tämä tarkoittaa verkon segmentointia, paikallisten järjestelmänvalvojien oikeuksien poistamista loppukäyttäjiltä sekä erityistä varovaisuutta myönnettäessä käyttöoikeuksia tietokoneen sovelluksille.
- Rajoita sovellusten lataaminen luotettaviin lähteisiin (viralliseen sovelluskauppaan).
- Ota käyttöön vahvat koodin eheyskäytännöt, joilla rajataan käyttäjien käytettävissä olevia sovelluksia. Jos mahdollista, ota käyttöön tietoturvaratkaisu, joka rajoittaa järjestelmän ytimessä (kernelissä) suoritettavaa koodia ja voi estää allekirjoittamattomia komentosarjoja sekä muuta koodia, johon ei luoteta. Käytä sallittujen sovellusten luetteloa.
- Lisätietoa ohjelmistojen toimitusketjuhyökkäyksistä ja niiltä suojautumisesta saat tästä Microsoftin tutkijoiden kirjoittamasta blogiartikkelista.

3. **Ota varmuuskopioita.**

- Luo tuhoutumattomia varmuuskopioita kriittisistä järjestelmistäsi ja tiedoistasi.
- Varmuuskopioi tiedot automaattisesti pilvipalveluihin. Kopioi paikalliset tiedot säännöllisesti soveltamalla 3-2-1-sääntöä. Säilytä tiedoista kolme varmuuskopiota kahdessa eri tallennusmuodossa ja ainakin yksi varmuuskopio toimipaikan ulkopuolella.

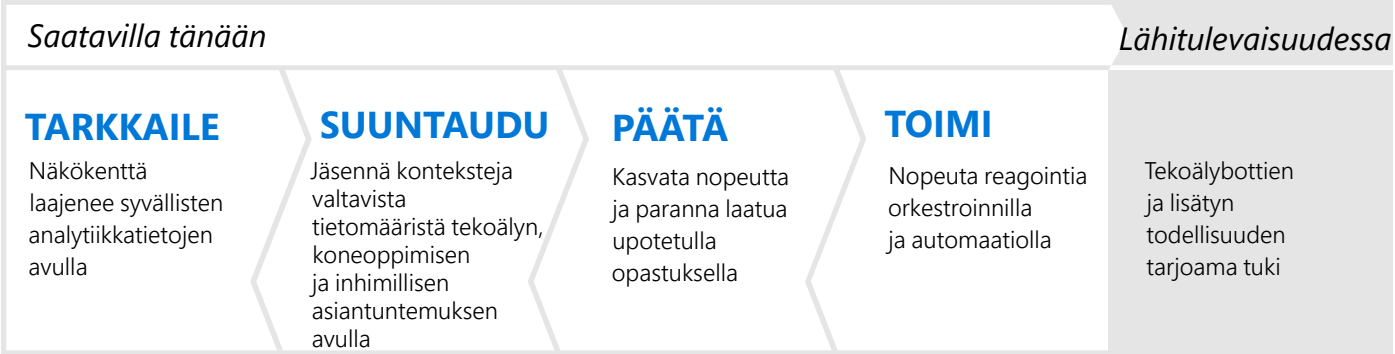
4. **Kiinnitä asioihin huomiota ja ryhdy toimiin, jos epäilet jotakin.**

- Opeta työntekijöitä varomaan epäilyttäviä viestejä, jotka pyytävät arkaluonteista tietoa. Ohjeista heitä toimimaan oikealla tavalla ja raportoimaan näistä asioista välittömästi organisaation tietoturvatiimille. Koulutus voi myös auttaa sosiaalisen manipuloinnin ja uskottavalta vaikuttavan tietojenkalastelun torjumisessa.
- Ole varovainen avatessasi web-linkkejä. Tietoturvallisten selauskäytäntöjen noudattaminen sekä sellaisten ratkaisujen käyttö, jotka varoittavat turvattomista sivustoista varoittavien tai estävät niiden käytön, voivat auttaa vähentämään kryptovaluutan louhintasivustojen kohtaamista.
- Jos tietokone toimii poikkeuksellisen hitaasti, etsi siitä epäilyttäviä käynnissä olevia tiedostoja. Voit myös vapaasti lähettää näytteen käyttöjärjestelmän toimittajalle. Voit lähettää Microsoftille tiedostoja haittaohjelma-analyysia varten osoitteessa https://www.microsoft.com/wdsi/filesubmission.

HAVAITSEMINEN JA REAGOINTI:

Havaitseminen ja reagointi parantavat vikasietoisuutta lyhentämällä aikaa, jonka hyökkääjä pystyy käyttämään resurssejasi. Tämä vähentää hyökkääjän sijoituksen tuottoa kasvattamalla kustannuksia (hyökkääjän on yritettävä uudelleen tai muutettava toimintaansa) sekä heikentämällä tuloksia (tavoitteiden saavuttaminen on epätodennäköisempää).

Sama pilviteknologia, joka tukee yrityksiä markkinoiden tarpeisiin vastaamisessa, voi myös auttaa tietoturvatiimejä taistelemaan tehokkaammin hyökkääjiä vastaan.



KUVA 10.

Tietoturvakeskusten (SOC) kehityskaari

Tietoturvakeskusten (SOC) kehityskaareen tutustuminen paljastaa, että teknologia on jatkuvasti kasvattanut SOC-päätösten ja -toimenpiteiden nopeutta ja laatua. Monet näistä innovaatioista liittyvät "OODA-silmukkaan" (Observe Orient Decide Act = Tarkkaile, Suuntaudu, Päätä, Toimi), jonka esitteli ensimmäisenä Yhdysvaltain armeijan eversti John Boyd.[3]

TARKKAILE – Tietoturvakeskukset voivat hyödyntää valtavaa määrää tietoturva-analytiikkaa (joka on saatavilla Microsoftilta ja muilta lähteiltä). Sen avulla ne voivat merkittävästi laajentaa näkökenttäänsä niin organisaation sisäisen tilanteen kuin ulkoisen ympäristön osalta.

SUUNTAUDU – Kun uudet tietolähteet tulevat valmiiksi ylityöllistettyjen tietoturvakeskusten saataville, koneoppiminen (tekoälyn alijoukko) muodostuu tärkeäksi työkaluksi, jolla näitä valtavia tietojoukkoja voidaan järkeistää ja jonka avulla voidaan tunnistaa tutkimisen arvoisia poikkeamia. Tietoturvatoimittajat (mukaan lukien Microsoft) ovat ottaneet käyttöön koneoppimisteknologiaa, jonka avulla tapahtumat voidaan priorisoida nopeasti (ja nämä yksittäiset tapahtumat voidaan yhdistää kokonaistapauksiksi).

PÄÄTÄ – Koska hyökkäysten laajuus ja monimutkaisuus voi helposti ylikuormittaa tietoturvakeskuksen, analyytikkojen ja vastehenkilöstön on pystyttävä tekemään useita päätöksiä ja toimimaan nopeasti hälytys- ja tunnistustilanteissa. Microsoft ja muut toimittajat ovat integroineet automatisoituja tutkintavalmiuksia ja ohjeistuksia, joiden avulla analyytikot voivat nopeasti tehdä hyviä päätöksiä (mm. eristämällä mahdollisesti tartunnan saaneita tai murrettuja laitteita). Tällä hetkellä automaatio keskittyy matalan prioriteetin tapausten nopeaan ratkomiseen, jotta erikoisosaamista voidaan suunnata monimutkaisempiin ongelmiin.

TOIMI – Vastaus edellyttää nopeaa ja tarkkaa toimintaa, jossa sovelletaan useita teknologioita ja alustoja. Tämä on mahdollista tietoturvan orkestroinnin ja vasteautomaation avulla. Microsoft ja monet muut toimijat investoivat edelleen näiden teknologioiden kehittämiseen. Niihin sisältyvät nykyaikaisten uhkien tunnistusratkaisut sekä automaattiset vasteratkaisut.

ALAVIITTEET

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

Eräitä muita nykyaikaiseen tietoturvakeskukseen vaikuttavia trendejä ovat seuraavat:

- **Hälytyssyötteiden laatu on tärkeämpää kuin määrä** – kun organisaatioilta aiemmin "puuttui tietoa", nykyään niillä on käytössään "liikaa tietoa". Siksi pitkälle erikoistuneiden tietoturva-analyytikkojen ajasta ja huomiosta on tullut yhä arvokkaampaa. Tämän seurauksena tason 1 ja 2 analyytikkojen toimia edellyttävien hälytysten laatua on pitänyt parantaa. Vaikka ylimääräisistä datasyötteistä on aina apua tutkimuksissa ja aktiivisessa uhkien metsästyksessä, Microsoft-konsernin IT-tietoturvakeskus mittaa analyytikkojen vastausta edellyttävien aitojen syötehälytysten lukumäärää (ja vaatimus aitojen tapauksien osuudesta on tällä hetkellä vähintään 90 %).

- Datan painovoima – Suurten tietojoukkojen (kuten suojaustietojen) analytiikkaa on vaikea suorittaa ilman pääsyä taustalla olevaan raakadataan. Mitä enemmän suojaustietoja on saatavilla, sitä taloudellisempaa ja käytännöllisempää on suorittaa tietoturva-analytiikkaa pilvessä sen sijaan, että dataa käsiteltäisiin paikallisessa järjestelmässä. Tämä johtaa todennäköisesti sellaisten SIEM- ja SOC-arkkitehtuurien kehitykseen, joihin voi sisältyä SIEM-hybridimalleja tai natiivitasoisen SIEM-pilven käyttöönotto palveluna.

- **Syvällinen konteksti** – Tämäntyyppiset havainnot ovat paljon hyödyllisempiä, koska ne pystyvät korreloimaan tietojoukkoja tehokkaammin. Vaikka perinteiseen verkkoliikenteeseen pohjautuvilla tunnistuksilla on edelleen jonkin verran arvoa tietoturvan kannalta, verkkoliikenteen raakadatasta puuttuu tyypillisesti konteksti, jonka avulla legitiimit toiminnot voidaan erotella poikkeavasta toiminnasta. Meidän nähdäksemme tietoturvakeskukset hyötyvät paljon enemmän monipuolisesti kontekstualisoiduista havainnoista, kuten seuraavista:

  - **Päätepisteiden tunnistus- ja vasteratkaisut (EDR),** jotka tarjoavat syvällisen kontekstin isännän toiminnalle
  - Identiteettiin perustuvat havainnot, jotka sisältävät tietoa käyttäjän normaaleista todennuskuvioista (sijainnit, ajat, käytetyt palvelut jne.) ja soveltavat käyttäytymisanalytiikkaa

Hyökkääjien on vaikeampi kiertää näitä monipuolisesti kontekstualisoituja havaintoja, koska heidän on pyrittävä jäljittelemään paljon monimutkaisempaa toimintaa (muutaman IP-liikennettä koskevan teknisen määritteen sijasta).

Asiakkaiden vakavista tietomurroista olemme myös oppineet sen, kuinka vaikeaa on vastata tapauksiin nopeasti, jos IT-toiminnot ovat osittain tai kokonaan ulkoistettuja. Suosittelemme IT-ulkoistussopimustesi, palvelutasosopimustesi (SLA) sekä toimitusketjusi tarkastamista ja sen varmistamista, että ne pystyvät vastaamaan mahdollisiin tietoturvaongelmiin nopeasti. Lisätietoa suorittamistamme asiakkaiden tapaustutkimuksista saat Incident Response Reference Guide (IRRG) -oppaastamme osoitteessa https://aka.ms/IRRG.

Tietolähteet

Tietolähteet

Microsoft on kerännyt Microsoft Security Intelligence Reportissa hyödynnettyjä tietoja erilaisten Microsoft-tuotteiden ja -palveluiden kautta, kuten Microsoftin tietosuojalausunnossa on esitetty. Tämän datan avulla saamme arvokasta tietoa tuotteidemme ja palveluidemme tietoturvasta ja toiminnasta sekä pystymme hankkimaan yleistasoisia näkemyksiä kyberuhkien kehittymisestä. Dataan sisältyy analytiikkaa seuraavista lähteistä:[4]

- **Azure Security Center** on palvelu, jonka avulla organisaatiot voivat estää uhkia, havaita ne ja vastata niihin tarjoamalla entistä paremman näkyvyyden pilvityökuormien suojaamiseen ja kehittyneen analytiikan ja uhkatietojen käyttämiseen hyökkäysten tunnistamiseen.

- **Bing** on Microsoftin haku- ja päätöskone, joka suorittaa vuosittain miljardeja web-sivujen skannauksia etsiessään haitallista sisältöä. Kun tällaista sisältöä havaitaan, Bing näyttää käyttäjille varoituksia tartuntojen estämiseksi.

- **Exchange Online** on Microsoftin ylläpitämä sähköposti- ja tuottavuuspalvelu. Exchange Onlinen haittaohjelmiston torjunta- ja roskapostin torjuntapalvelut skannaavat miljardeja viestejä vuosittain tunnistaakseen ja estääkseen roskapostia ja haittaohjelmistoa.

- **Haittaohjelmistojen poistotyökalu** (MSRT) on maksuton työkalu, jonka Microsoft on suunnitellut tunnistamaan ja poistamaan tiettyjä yleisiä haittaohjelmistoperheitä asiakkaiden tietokoneista. Haittaohjelmiston poistotyökalu on lähinnä julkaistu tärkeänä päivityksenä Windows Updaten, Microsoft Updaten ja Automatic Updaten kautta. Versio tästä työkalusta on saatavilla Microsoft Download Centeristä. MSRT ei korvaa ajan tasalla olevaa reaaliaikaista virustentorjuntaratkaisua.

- **Microsoft Safety Scanner** on maksuton ladattava tietoturvatyökalu, joka suorittaa tarveperusteisia skannauksia ja auttaa poistamaan haittaohjelmistoja ja muita vastaavia ohjelmistoja. Microsoft Safety Scanner ei korvaa ajan tasalla olevaa virustorjuntaratkaisua, koska se ei tarjoa reaaliaikaista suojausta eikä se voi estää tietokonetta saamasta tartuntaa.

ALAVIITTEET

[4]On tärkeää huomioida, että tämä data käsitellään tiukkojen tietosuoja- ja säädösvaatimusten mukaisesti, ennen kuin sitä käytetään tietoturvan parantamiseen.

- **Microsoft Security Essentials** on maksuton, helposti ladattava reaaliaikainen suojaustuote, joka tarjoaa perustason tehokkaan virus- ja vakoiluohjelmistosuojauksen Windows Vistalle ja Windows 7:lle.

- **Microsoft System Center Endpoint Protection** (aiemmin Forefront Client Security ja Forefront Endpoint Protection) on yhdistetty tuote, joka tarjoaa suojan haittaohjelmistoja ja ei-toivottuja ohjelmistoja vastaan yritysten työasemille, kannettaville tietokoneille ja palvelinkäyttöjärjestelmille. Se käyttää Microsoft Malware Protection Enginen ja Microsoftin virustentorjunnan allekirjoitustietokantaa toimittaakseen reaaliaikaista, ajastettua ja pyydettäessä toimivaa suojausta.

- **Office 365** on Microsoft Office -tilauspalvelu organisaatioille ja kotikäyttäjille. Tiettyihin tilauspaketteihin sisältyy Office 365 Advanced Threat Protection -käyttöoikeus.

- **Windows Security** on Windows 10:n ominaisuus, joka huolehtii haittaohjelmien ja ei-toivottujen ohjelmien skannauksesta ja poistosta reaaliaikaisesti. Lisäksi Windowsin uusin versio hyödyntää asiakkaiden tietoturvan parantamiseksi monipuolista kontekstitietoa, mukaan lukien koneen määritystiedot, laitteen suorituskyky ja kunto sekä muut vastaavat tiedot. Samalla tarjoamme asiakkaille mahdollisuuden saada paremman käsityksen Windows 10:n tietosuojasta. Tästä blogiartikkelista saat lisätietoa Microsoftin toimintatavoista.

- **Windows Defender Advanced Threat Protection** on uusi palvelu, joka sisältyy Windows 10 Anniversary Update -päivitykseen ja uudempiin versioihin. Sen avulla yritysasiakkaat voivat havaita, tutkia ja korjata kehittyneitä pysyviä uhkia ja verkkojensa tietomurtoja.

- **Windows Defender Offline** on ladattava työkalu, jonka avulla voidaan luoda käynnistettävä CD, DVD tai USB-muistitikku, jolla voidaan skannata tietokone haittaohjelmistojen ja muiden uhkien varalta. Se ei tarjoa reaaliaikaista suojaa eikä se korvaa ajan tasalla olevaa haittaohjelmiston torjuntaratkaisua.

- **Windows Defender SmartScreen** on Microsoft Edgen ja Internet Explorerin ominaisuus. Se tarjoaa käyttäjille suojaa tietojenkalastelusivustoja ja haittaohjelmistoja ylläpitäviä sivustoja vastaan. Microsoft ylläpitää tietokantaa tietojenkalastelu- ja haittaohjelmistosivustoista, joista Microsoft Edgen, Internet Explorerin ja muiden Microsoftin tuotteiden ja palveluiden käyttäjät ilmoittavat. Kun käyttäjä yrittää käydä sivustolla, joka on tietokannassa, ja suodatin on käytössä, selain näyttää varoituksen ja estää sivulle siirtymisen.