TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 2020

Kybersää toukokuu 2020

Tietomurrot ja -vuodot

- Office 365 –tietomurtojen määrä alkuvuoden tasolla.
- Kuntasektorin toimijoihin kohdistui tietomurto ja sen yritys.
- Useaan suurteholaskentaympäristöön on kohdistunut ulkomailla tietomurtoja

Huijaukset ja kalastelut

- Posti-aiheella levitetyt tekstiviestihuijaukset sisältävät haittaohjelman mobiililaitteelle.
- Toimitusjohtajahuijaukset ja muut laskutuspetokset lisääntyvät taas lomakauden lähestyessä.

Haittaohjelmat ja haavoittuvuudet

- Ransomware-toimijat huutokauppaavat varastettuja tietoja tavoitteenaan rahastaa tiedoilla.

Automaatio

- Suomalaiseen kriittisen infran järjestelmään tehtiin kiristyshaittaohjelmahyökkäys.
- Automaatiojärjestelmiin on hyökätty toistuvasti myös valtioiden välisten konfliktien yhteydessä

Verkkojen toimivuus

- Vain 3 merkittävää toimivuushäiriötä
- Valokuidun katkeaminen Pasilassa 7.5. haittasi laajasti junaliikennettä.
- Toukokuu oli palvelunestohyökkäysten osalta rauhallinen.

Vakoilu

- Sandworm-ryhmän varoitetaan pyrkineen tunkeutumaan haavoittuviin Exim-sähköpostipalvelimiin ainakin elokuusta 2019 lähtien.
- Kriittisen infrastruktuurin järjestelmät ovat houkuttelevia tunkeutumiskohteita APT-ryhmille.

Kuukauden tunnuslukuja

115 000 €

SUMMA, JOKA MENETETTIIN OSANA ONNISTUNUTTA LASKUTUSPETOSTA

3

VAIN KOLME TOIMINTAHÄIRIÖTÄ VERKOISSA TOUKOKUUN AIKANA. MÄÄRÄ ON TAVANOMAISTA VÄHEMMÄN TOIMIVUUSHÄIRIÖITÄ YLEISISSÄ VIESTINTÄPALVELUISSA

4

ILMOITUKSIA KYBERTURVALLISUUSKESKUKSELLE KIRISTYSHAITTAOHJELMISTA, JOILLA OLI MERKITTÄVÄT VAIKUTUKSET YRITYKSEN TIETOIHIN JA TOIMINTAYMPÄRISTÖÖN

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

2

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

3

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

- Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. Tyypillisesti rikolliset kalastelevat suomalaisilta Office 365 –tuotteiden ja sähköpostin käyttäjätunnuksia ja salasanoja.
- Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua opitaan tunnistamaan koulutuksen avulla ja tämä auttaa siihen, että tietojenkalastelu jää vain yritykseksi.

CASE

Vappuvisassa tunnistettiin huijauksia

Kyberturvallisuuskeskus julkisti vappuviikolla leikkimielisen kuvavisailun, jonka takana oli kuitenkin vakava asia: huijauksiin tehdyt tietojenkalastelusivut.

Lähes 3700 vastaajaa yritti tunnistaa kuvista, onko verkkosivu aito vai huijarin tekemä tietojenkalastelusivu. Kuten vastaajat saivat huomata, pelkästä kuvasta on vaikea tunnistaa petkutusta, vaan rinnalle tarvitaan muutakin tietoa.

Lue lisää artikkelistamme: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vappuvisan-tulokset-petkuhuiputusta-vaikea-tunnistaa

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan seurauksena.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja. Jos rikolliset havaitsevat huonosti suojatun ympäristön kiristämisen arvoiseksi, siihen saatetaan kohdistaa Big Game Hunting –toimintaa.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia toimijoita tulee jatkuvasti. Esimerkkinä tästä on ICS-toimijoihin kohdistuva EKANS.
- Kiristyshyökkäysten uutena ilmiönä uhataan julkaista hyökkääjän haltuun saamia tietoja lunnasvaatimuksen tehostamiseksi.

CASE

Amerikkalainen ICT-palveluntarjoaja Cognizant joutui Maze-kiristyshaittaohjelman uhriksi. Tapaus ei koskettanut vain yritystä itseään vaan kiristyshaittaohjelman vaikutukset ulottuivat asiakkaisiin saakka. Yritys on arvioinut, että se käyttää 50-70 miljoonaa dollaria seuraavan kolmen kuukauden aikana hyökkäyksen aiheuttamien vahinkojen korjaamiseksi. Tämän lisäksi kuluja kertynee juridisista, konsultoinnista ja hyökkäyksen selvittämiseen liittyvistä kuluista. Maze paitsi lukitsee uhrin koneiden tiedostot, se myös ottaa niistä kopiot hyökkääjälle.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja tunnistavat kohteet, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Hyökkäyksissä käytetyt järjestelmähaavoittuvuudet ovat usein olleet 2-6 kk vanhoja haavoittuvuuksia, joihin on ollut saatavilla korjaus jo pitkään, mutta syystä tai toisesta haavoittuvuutta ei ole korjattu.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

Palvelinten ylläpitoon käytetystä Saltstack Salt -hallintakehikosta korjattiin kriittisiä haavoittuvuuksia huhtikuun lopulla. Ensimmäiset automatisoidut hyökkäykset havaittiin vain pari päivää myöhemmin. Hyökkääjä asensi virtuaalivaluuttaa louhivan haittaohjelman kaikkiin hallinnan piirissä oleviin palvelimiin. Verkkoon auki olevia palveluita löytyi yli 6000.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä, jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä.
- Yleinen puute on jättää keräämättä ja tarkkailematta tietoturvalokeja. Lokien jatkuvan tarkkailun avulla tietojärjestelmän omistaja voi havaita lievät tietoturvaloukkaukset ja järjestelmän heikkoudet ennen kuin kukaan ehtii käyttää niitä suurempaan vahingontekoon. Lokeja tarvitaan myös loukkausten selvittämiseen jälkikäteen.
- Lisäksi käytöstä poistuvien palveluiden alasajo tulee tehdä huolella. Jos alasajotoimenpiteitä ei tehdä johdonmukaisesti loppuun asti, voi taustalle jäädä pyörimään käyttämättömiä palveluita, jotka voivat aiheuttaa merkittäviä tietoturvariskejä organisaatiolle.

Korona-aikana epäselvän vastuunjaon lisäksi nousee esille resurssien riittävyys sekä erilaisten varautumissuunnitelmien tärkeys. Pandemian aikana henkilöstöllä on keskeinen rooli, jotta toiminnot saadaan pidettyä yllä ja resurssien tulee olla riittävät kaikissa tilanteissa. Vaikutuksia saattaa olla myös tuotantoketjuissa, jolloin normaalisti saatava tuote jääkin tulematta, millä on vaikutuksia organisaation toimintaan.

CASE

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

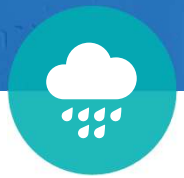
5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

- Tietoturvaloukkauksista toipumista ei usein suunnitella huolellisesti ennakkoon. Suunnitelmat ovat vain luokkaa "palautetaan tiedot varmuuskopioista". Palautumisen tärkeysjärjestyksiä, resursseja ja aikajänteitä ei mietitä ennakkoon.
- Häiriön iskiessä palautumisen monimutkaisuus ja työläys yllättävät. Jos palautuminen olisi suunniteltu ennakolta paremmin, myös varautuminen häiriöihin ja niiden ennaltaehkäisyyn olisi parempaa.
- Kyberturvallisuuskeskus on julkaissut yritysten hallituksille suunnatun kyberturvallisuutta käsittelevän oppaan. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa työkaluja ja tukea organisaation kyberturvallisuuden parantamiseen.
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

CASE

Organisaatioiden kyvyssä hallita kyberriskejään on selviä puutteita. Tyypillisesti organisaatiot eivät osaa ennalta arvioida kyberuhkien toteutumisen vaikutuksia päivittäiseen toimintaan. Tämän seurauksena on, että kyberriskit ja niiden vaikutukset aliarvioidaan eikä niiden hallintaan osoiteta riittävästi resursseja.



Tietomurrot ja -vuodot

Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

Tietomurrot ja vuodot

- Kyberturvallisuuskeskukseen ilmoitettujen Office 365 -tietomurtojen määrä on edelleen alkuvuoden tasolla.
  - Maaliskuussa ollut ilmoitusmäärän lasku johtui todennäköisesti koronatilanteesta, kun myös verkkorikolliset joutuivat muuttamaan toimintatapoja karanteenista johtuen.
  - Kyberturvallisuuskeskus on julkaissut ohjeen Office 365 -ympäristön koventamisesta. Se on saatavilla suomen-, ruotsin- ja englanninkielisenä. Ohje löytyy osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/organisaatio-torju-office-365-tunnusten-kalastelu-oppaamme-avulla

ANALYYSI

- Monivaiheinen tunnistautuminen estäisi suurimman osan tietomurroista.
- Office 365 -tietomurtojen määrä pysyy korkeana, koska verkkorikolliset kokevat niillä saadun hyödyn riittävän suureksi suhteessa vaadittuihin toimenpiteisiin.
- Lisäksi Office 365 -tietomurrot nähdään helppona tapana murtautua moniin tietojärjestelmiin.

Tietomurrot ja vuodot

- Suomalaisiin kunnallisen alan toimijoihin kohdistui tietomurto sekä tietomurron yritys
  - Kaupungin omistaman palvelun verkkoon kohdistui onnistunut tietomurto. Verkon eri osien eriyttäminen esti suuremmilta vahingoilta.
  - Toisen suomalaisen kaupungin omistaman tytäryhtiön käyttäjätunnus ja salasana saatiin selville tunnusten kalastelun avulla. Käytössä ollut monivaiheinen tunnistautuminen esti kuitenkin varsinaisen tietomurron.

ANALYYSI

- Eri torjuntamenetelmät suojaavat tietomurroilta sekä niiden aiheuttamilta vahingoilta. Eri havainnointimenetelmät mahdollistavat tietoturvapoikkeaman nopean havainnoinnin ja siten mahdollistaa paremman reagoinnin.
- Hyvin suunnitelluilla verkoilla ja eri toiminteiden verkko-osien erottamisella pystytään rajoittamaan onnistuneen tietomurron aiheuttamia vahinkoja ja nopeuttamaan toipumista.

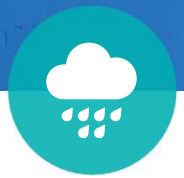
Tietomurrot ja vuodot

- Useaan kansalliseen suurteholaskentaympäristöön on kohdistunut ulkomailla tietomurtoja
  - Murrettuja suurteholaskentaympäristöjä on käytetty mm. virtuaalivaluuttojen louhintaan.
  - Tietomurtojen uhreja löytyi ainakin Aasiasta, Euroopasta ja Pohjois-Amerikasta.
  - Kyberturvallisuuskeskuksen tietoon ei ole tullut vastaavia tapauksia Suomessa.
  - Lue aiheesta lisää esimerkiksi https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/

ANALYYSI

- Kyberrikolliset pyrkivät hyödyntämään erilaisia laskentaympäristöjä virtuaalivaluuttojen louhimiseen.
- Taloudellisen hyödyn tavoittelu on todennäköisin syy tietomurtoihin ja muuhun kyberrikollisuuteen.

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:



Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyksiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnus- ja maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

Huijaukset ja kalastelut

- Perinteisiä huijauksia on maustettu ja tehostettu korona-aiheilla.
- Toimitusjohtajahuijauksia ja muita laskutuspetoksia on tehostettu oikean näköisillä mutta vähän väärin kirjoitetuilla verkkotunnuksilla (typosquat).
- Teknisen tuen helpdesk-huijaukset alkoivat uudestaan pitkän tauon jälkeen.
  - Helmikuuta riivanneet huijauspuhelut loppuivat maaliskuun lopussa, mutta toukokuussa niitä on alkanut jälleen tulla.

ANALYYSI

- Unohdetun salasanan palautustoimintoa käytetään yhdessä kaapatun sähköpostitilin kanssa: Kaapatun tilin avulla voi päästä käsiksi moniin muihin palveluihin.
- Office 365 -tunnuksia kalastellaan javascript-liitteillä, joka sisältää kalastelusivun. Tällainen kalasteluviesti läpäisee sähköpostisuodattimia geneeristä viestiä helpommin.
- Murrettuja verkkosivuja käytetään säännöllisesti sekä kotimaisten pankkitunnusten että suosittujen palveluiden käyttäjätunnusten kalasteluun.

Posti-aiheisia huijauksia

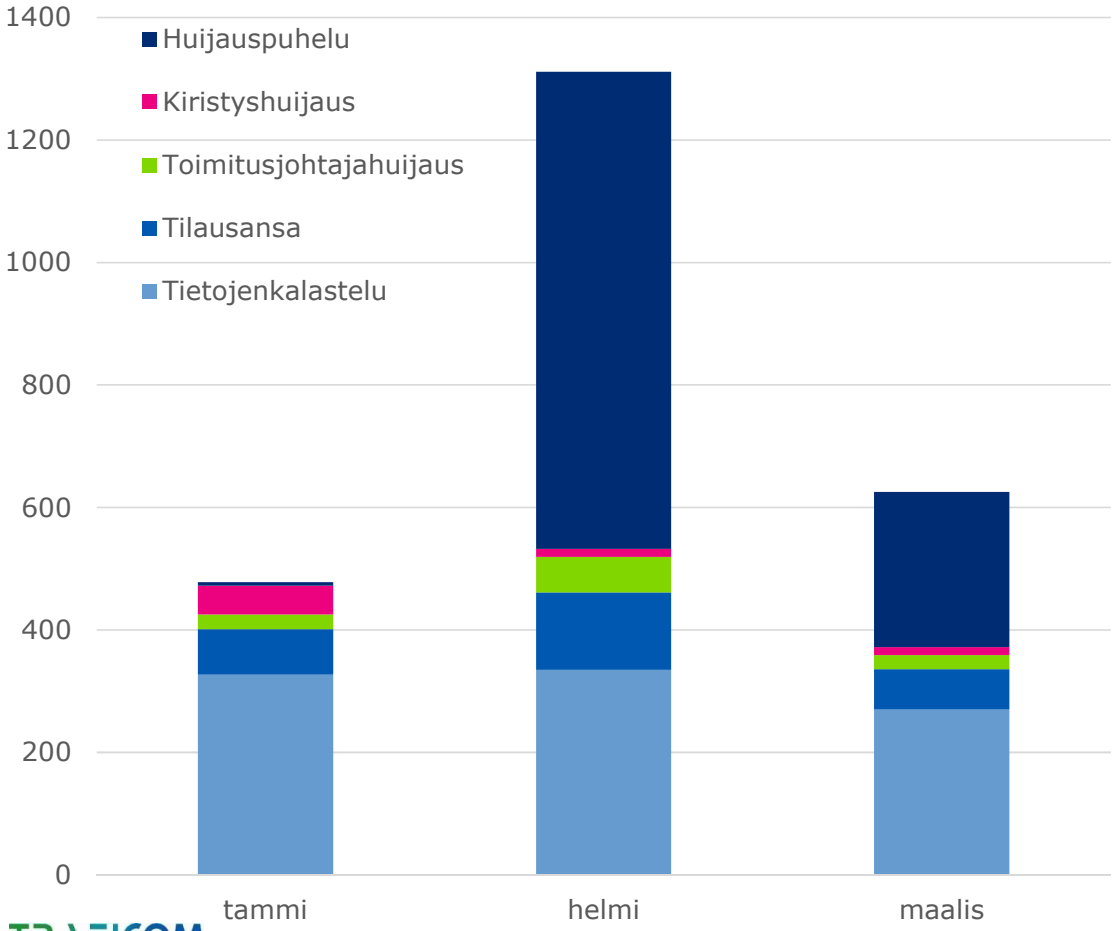
- Postin nimissä liikkuu nyt tietojenkalastelua ja tilausansahuijauksia tekstiviestien välityksellä. Huijaustyyppejä on ainakin kolme. Huijauksia yhdistää se, että huijarit lähettävät syötti-tekstiviestejä, jotka houkuttelevat vierailemaan Posti-teemaisella huijaussivustolla.
- Tekstiviestin vastaanottajan halutaan uskovan, että hänelle on saapunut paketti tai muu lähetys. Huijaussivustojen ulkoasu muistuttaa erehdyttävästi aitoja Postin sivuja. Huijauslinkki voi johtaa

1. tilausansaan
2. tietojenkalasteluun ja petokseen
3. haittaohjelmaan, joka leviää edelleen tekstiviestin välityksellä

ANALYYSI

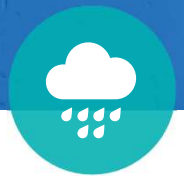
- Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus
- Älä klikkaa tekstiviesteissä olevia linkkejä, sillä puhelimella huijaussivua on vaikea erottaa aidosta.
- Älä klikkaa linkkiä, vaan suunnista suoraan Postin omaan lähetyksenseurantaan, jonne voit syöttää seurantakoodin.

Käsiteltyjä huijaustapauksia Q1/2020



- Alkuvuoden 2020 näkyvin trendi ovat olleet huijauspuhelut:
  - Helpdesk-huijari yrittää saada uhrin tietokoneen haltuunsa ja varastaa siten tietoja ja rahaa.
  - Hälärihuijauksissa uhri yritetään saada soittamaan takaisin kalliiseen ulkomaan numeroon tai satelliittipalveluun.
- Kiristyshuijaukset ovat sähköposteja, joissa huijari uhkailee jollain tai väittää saaneensa uhrin koneen haltuunsa ja vaatii lunnaita.
- Toimitusjohtajahuijaukset kohdistuvat yrityksiin ja organisaatioihin. Väärennetyt viestit tähtäävät laskutuspetokseen.
- Tilausansoja suunnataan kaikille kuluttajille esiintyen mm. Postin, Gigantin, tai muiden tuotemerkkien nimissä. Useimmat tekstiviestihuijaukset johtavat tilausansaan.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja, joilla järjestelmiin pääsee.

Q1/2020 - tilasto päivitetään kvartaaleittain



Haittaohjelmat ja haavoittuvuudet

Haittaohjelmissa ja haavoittuvuuksissa käsitellään aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

Haittaohjelmat ja haavoittuvuudet

- Sähköposteissa jaetaan haitallisia liitetiedostoja ja linkkejä tavalliseen tapaan
  - Todennäköisesti Emotet-haittaohjelmaa yritetään levittää vanhan sähköpostiketjun jatkoksi lähetetyillä huijausviesteillä.
  - Pilvipalvelutoimittajan alustalla jaettiin merkittäviä määriä erilaisia haittaohjelmia. Olemme olleet yhteydessä palvelutoimittajaan ja pyytäneet poistamaan haittaohjelmia jakavat sivustot verkosta.
- Haitallisten Excel 4.0 -makrojen levitys lisääntynyt
  - Haittaohjelmien torjuntaohjelmilla vaikeuksia tunnistaa joitain hyökkäystapoja.

ANALYYSI

- Haitallista sisältöä levitetään myös tunnettujen pilvipalvelujen kautta eli luotettavalta näyttäväänkin linkkiin tulee suhtautua varauksella
- Rikolliset testaavat jatkuvasti uusia hyökkäystapoja, uusimpana esimerkkinä jo iäkkään Excel 4.0 version makrojen käyttö haittaohjelman levittämisessä.

Haittaohjelmat ja haavoittuvuudet

- Viikon aikana useita havaintoja kiristyshaittaohjelmatartunnoista tai niiden levittämisestä
  - Kriittisen infrastruktuurin hallintalaitteeseen asentui Suomessa kiristyshaittaohjelma
  - Kansainvälisesti useita merkittäviä kiristyhaittaohjelmahavaintoja
- Posti-teemaisella tekstiviestihuijauksella levitetään myös haittaohjelmaa Android-puhelimiin (ks. huijaukset ja kalastelut)
- REvil Ransomware Gang on aloittanut huutokaupat tietomurroilla saaduilla tiedoilla
  - Revil/Sodinokibi kiristyshaittaohjelmalla yleensä kiristetään uhrilta lunnaita, joten huutokauppojen tavoitteena on lisätä uhrin maksuhalukkuutta. https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/
  - Myös muut kiristyshaittaohjelmat kryptaavat tiedot usein vasta kun merkittävä määrä tietoa on kopioitu järjestelmästä https://www.kroll.com/en/insights/publications/cyber/latest-maze-ransomware-ttps

ANALYYSI

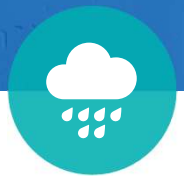
- Yritysten maksuvalmius tai halukkuus on vähentynyt, jonka vuoksi rikolliset käyttävät uusia tapoja hyödyntää ja myydä tietomurrossa saatua tietoa.
- Kiristyshaittaohjelmat ovat tunnistettu merkittäväksi riskiksi liiketoiminnalle

Haittaohjelmat ja haavoittuvuudet

- Android käyttöjärjestelmästä on löydetty kriittinen haavoittuvuus (CVE-2020-0096), jonka avulla haitallinen Android-sovellus voi tekeytyä toiseksi sovellukseksi ja pyytää uusia käyttöoikeuksia sovellukselle tai esittää käyttäjälle väärennetyn kirjautumisruudun. (StrandHogg 2.0)
  https://www.kyberturvallisuuskeskus.fi/fi/strandhogg-20-haavoittuvuus
  - Google on julkaissut haavoittuvuuden korjaavan päivityksen (Ulkoinen linkki)Android-versioille 8.0, 8.1 ja 9 (CVE-2020-0096). Google Play Protect -palvelu havaitsee myös StrandHogg 2.0 -haavoittuvuutta hyväksikäyttävät sovellukset.
- iOS:n uusimmista versiosta löytyi suojausten ohittamisen (Jailbreak) mahdollistava haavoittuvuus (23.5.), joka koskee iOS versioita 11-13.5 https://www.wired.com/story/apple-ios-unc0ver-jailbreak/
  - Apple on julkaissut päivityksen: https://support.apple.com/fi-fi/HT211214

ANALYYSI

- Sovellusten käyttöoikeuksia Kannattaa yrittää rajoittaa, mikäli se on mahdollista.
- Tarkista ennen uuden laitteen ostoa, miten laitteen ohjelmistolle on saatavilla päivityksiä myös tulevaisuudessa.



Automaatio

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai vastaavan tuotantolaitoksen palveluita tai laitteita.

Automaatio

- Kriittisen infrastruktuurin hallintalaitteeseen asennettu Suomessa kiristyshaittaohjelma. Kiristyshaittaohjelma pääsi asentumaan hallintalaitteen huonosta eristyksestä johtuen.
  - Hallintalaitteiden käyttöjärjestelmän haavoittuvuudet helpottivat tunkeutumista.
  - Haittaohjelma ei vaikuttanut itse automaatiojärjestelmään, mutta sen etähallinta keskeytyi. Automaatiojärjestelmän ylläpitoa jouduttiin tekemään useita päiviä paikan päältä.
  - Toimivat varmuuskopiot nopeuttivat ja helpottivat hallintaympäristön palautumista.

ANALYYSI

- Laitteiden päivityksistä ja verkkojen eristämisestä tulee huolehtia.
- Varmuuskopioista huolimatta automaatiojärjestelmän ja sen valvonnan palautumisessa voi kestää pitkään.
- Mikäli laitteelle ei ole saatavilla enää päivityksiä niin sitä pitää erityisesti suojata.

Automaatio

- Toukokuun aikana on julkaistu useita kansainvälisiä julkaisuja automaatioympäristöjen parhaista käytännöistä
  - Cybersecurity Best Practices for Industrial Control Systems (22.5.)
    https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems
  - Studies in secure system design (22.5.)
    https://www.ncsc.gov.uk/blog-post/studies-in-secure-system-design
  - COVID-19 – Remote Access to Operational Technology Environments (22.5.)
    https://www.cyber.gov.au/advice/covid-19-remote-access-to-operational-technology-environments
- Viime kuussa Kybersäässä esiteltyyn Israelin vesihuollon tapaukseen liittyen on tehty kyberhyökkäys iranilaisen sataman järjestelmiin.
  https://www.hs.fi/ulkomaat/art-2000006512971.html

ANALYYSI

- Automaatiojärjestelmien yhteiskunnallinen merkitys on lisääntynyt ja niiden kyberturvallisuutta kehitetään ja ohjeistetaan.
- Järjestelmiin on hyökätty toistuvasti myös valtioiden välisten konfliktien yhteydessä.

Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.

Verkkojen toimivuus

- Yleisissä viestintäpalveluissa oli toukokuussa vain kolme merkittävää häiriötä.
  - Häiriöt koskivat antennitelevisiopalveluita ja matkaviestinverkkojen palveluita.
- Muiden ICT-palveluiden huomattavat häiriöt
  - Valokuidun katkeaminen Pasilassa 7.5. vaikutti laajasti junaliikenteen ohjaamiseen ja valvontaan Suomessa.

ANALYYSI

- Yleisten viestintäpalveluiden toimivuus paranee koko ajan.
- Toisaalta yhteiskunnan kannalta merkittävät palvelut ovat koko ajan riippuvaisempia ICT-palveluiden häiriöttömästä toiminnasta.
- Yritysten ja julkishallinnon omaan käyttöönsä hankkimien ICT-palveluiden toimivuus ei ole samoin säädeltyä kuin yleisten viestintäpalveluiden toimivuus, mutta omistajien kannattaa soveltaa niihin samanlaisia varmistuksen periaatteita.

Verkkojen toimivuus

- Varautumista ja salaliittoteorioita:
  - Tietoverkot ja -palvelut koronan aikaan. 26.5.2020. https://www.varmuudenvuoksi.fi/aihe/kyber/454/tietoverkot_ja_-palvelut_koronan_aikaan
  - 5G mast set aflame in leafy Liverpool district, half an hour's walk from Penny Lane. 27.5.2020. https://www.theregister.co.uk/2020/05/27/5g_mast_arson_liverpool/

ANALYYSI

- Tieto- ja viestintätekniikat ja niiden toimivuuden eteen pitkäjänteisesti tehty varautumistyö ovat auttaneet yhteiskuntia jatkamaan työntekoa ja vapaa-ajan viettoa samalla, kun fyysistä kanssakäyntiä on jouduttu rajusti rajoittamaan viruksen leviämisen estämiseksi.
- Jotkin salaliittoteoreetikot väittävät 5G-tekniikan ja radioaaltojen edistävän koronaviruksen leviämistä.
- Koronavirus on virus, joka leviää ihmisestä toiseen pisaratartuntana aivastuksen, yskimisen tai uloshengityksen kautta, ei 5G verkkojen kautta.
- Jotkin ääriliikkeet vastustavat 5G-tekniikkaa jopa sabotaasein. Samankaltaista vastustusta on taannoin nähty myös muiden matkaviestinverkkotekniikoiden suhteen.

Palvelunestohyökkäykset

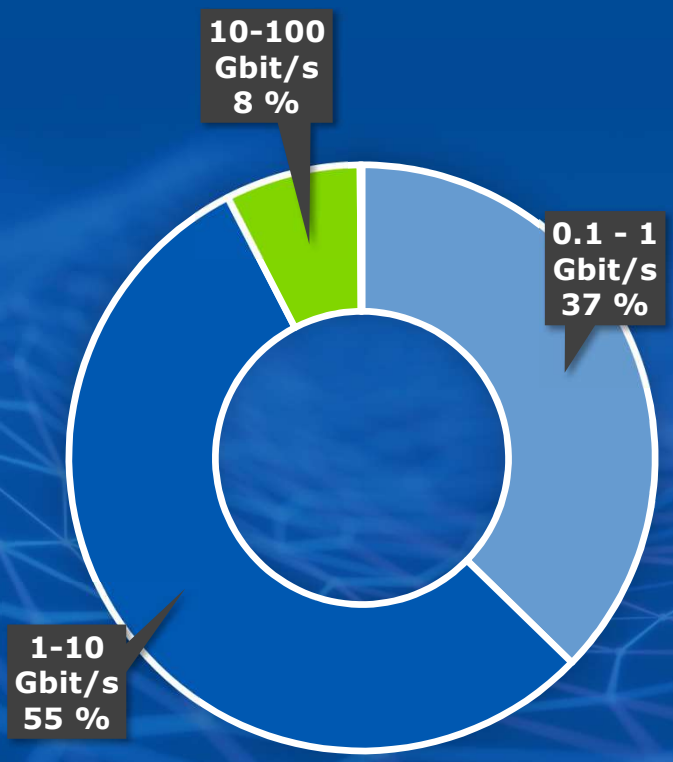
- Toukokuu oli palvelunestohyökkäysten osalta rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
- Raportoiduissa hyökkäyksissä on käytetty mm. sovellustason hyökkäyksiä.
  - Tällaisilta hyökkäyksiltä suojautuminen edellyttää verkkosivun toiminnan suunnittelua siten, että esimerkiksi palvelua runsaasti kuormittavat HTTP-pyynnöt voidaan suodattaa tai niiden lukumäärää rajoittaa.

ANALYYSI

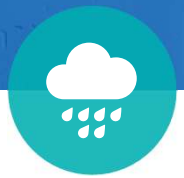
- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volymetriset että sovellustason hyökkäykset.

Palvelunestohyökkäysten tunnuslukuja

- 161 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys alkuvuonna 2020.
- Noin 80% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTO-HYÖKKÄYSTEN VOLYYMIT (Q1/2020 - TILASTO PÄIVITETÄÄN KVARTAALEITTAIN.)



Vakoilu

Vakoiluosiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen.

Vakoilu

- Toukokuussa julkaistiin uusia tietoja useiden eri Venäjään liitettyjen ryhmien toiminnasta.
  - Yhdysvaltojen turvallisuusviranomainen NSA varoitti, että aiemmin muun muassa sähköverkkojen häirintään Ukrainassa yhdistetty Sandworm-ryhmä on pyrkinyt ainakin vuoden 2019 elokuusta lähtien tunkeutumaan Exim-sähköpostipalvelimille siitä löytynyttä haavoittuvuutta hyödyntäen.
  - Berserk Bear -hakkeriryhmän uutisoitiin pyrkineen tunkeutumaan joihinkin Saksan kriittisen infrastruktuurin toimijoiden järjestelmiin tietojen varastamiseksi tai saadakseen jalansijan niissä. Asiasta uutisoi Cyberscoop-verkkojulkaisu.
  - ESET julkaisi analyysin Turla-ryhmän käyttämästä, päivitetystä ComRAT-haittaohjelmasta, jota käytetään takaporttina kohdejärjestelmään.

ANALYYSI

- APT-toimijoiden toiminnan kohdistus voi elää ja vaihtua ajan mittaan. Lisäksi toimijat kehittävät jatkuvasti työkalujaan ja toimintatapojaan.
- Erityisesti internetistä käsin saavutettavissa olevat palvelut on syytä päivittää viipymättä, kun niissä havaittuihin haavoittuvuuksiin julkaistaan päivityksiä.

Vakoilu

- Erilaisista sosiaalisessa mediassa julkaistuista tiedoista voi olla pääteltävissä paljon myös päivityksen varsinaiseen aiheeseen liittymättömiä asioita, jos julkaisija ei ota niitä huomioon.
  - Esimerkiksi tutkivan journalismin sivusto Bellingcat kertoi toukokuussa, kuinka virtuaaliseen olutpäiväkirja Untappdiin tehdyistä merkinnöistä pystyi päättelemään tietoja esimerkiksi sotilastukikohdista ja -operaatioista. Lisäksi palveluun ladatuista kuvista oli nähtävissä esimerkiksi salassa pidettäviksi luokiteltuja tietoja.
  - Analyysin pohjana käytettiin julkisia olutarvioita, joiden sijainniksi oli merkitty jokin armeijan käytössä oleva sijainti. Näiden tietojen pohjalta pystyttiin löytämään henkilöitä, jotka olivat väitetysti oleilleet kyseisissä paikoissa. Henkilöiden olutkirjauksia tarkastelemalla pystyttiin tunnistamaan esimerkiksi henkilöiden työhön ja vapaa-aikaan liittyvää matkustamista sekä muihin tietoihin yhdistämällä löytämään heidän asuinpaikkojaan tai tietoja läheisistä.

ANALYYSI

- Organisaatioiden työntekijät voivat epähuomiossa jakaa erilaisissa sosiaalisen median palveluissa tietoja, jotka joko itsessään tai yhdistettynä muista lähteistä saataviin tietoihin paljastavat organisaatiosta, sen toiminnasta tai työntekijästä itsestään tietoja, joita ei ole tarkoitettu ulkopuolisten saataville.
- Huomiota kannattaa kiinnittää mm. sijaintitietojen ja kuvien julkaisemiseen.

Vakoilu

- Lähi-idässä on uutisoitu kriittisen infrastruktuurin häirintään liittyvistä kyberhyökkäyksistä.
  - Huhtikuun lopussa uutisoitiin israelilaisiin vesilaitoksiin kohdistuneesta kyberhyökkäyksestä, jonka kohteena olivat tiettävästi veden jakeluun, jätevesien käsittelyyn ja kemikaalien annosteluun liittyvät järjestelmät. Hyökkäys onnistuttiin tiettävästi torjumaan ennen kuin vahinkoa ehti aiheutua.
  - Toukokuussa kerrottiin vastaavasti, että iranilaisen sataman järjestelmiin olisi tehty kyberhyökkäys, joka vaikutti vakavasti sataman toimintakykyyn.

ANALYYSI

- Kriittisen infrastruktuurin järjestelmät ovat houkuttelevia tunkeutumiskohteita APT-ryhmille.
- Esimerkiksi energia- ja logistiikkasektorin toimintoihin vaikuttamalla pystytään konfliktitilanteessa häiritsemään yhteiskunnan toimintaa.

Vakoilu

- COVID-19-tautiin liittyvät teemat, kuten rokote- ja muu tutkimus, pysyvät todennäköisesti edelleen eri toimijoiden kiinnostuksen kohteena, ja riskinä on, että kybervakoilua käytetään yhtenä keinona tiedon hankkimiseksi.
  - Esimerkiksi Yhdysvallat ja Iso-Britannia ovat varoittaneet terveydenhuoltosektoriin ja koronavirukseen ja sen hoitoon liittyvään tutkimukseen ja tietoon kohdistuvasta valtiollisesta kybervakoilusta.
- Myöskään COVID-19-aiheinen kohdistettu tietojenkalastelu tai haittaohjelmien levittäminen eivät uhkina ole poistuneet.

ANALYYSI

- COVID-19-aiheiden parissa työskentelevien organisaatioiden on syytä olettaa, että tutkimus- ja kehitystoimintaan liittyviin tietoihin voidaan yrittää päästä käsiksi kybervakoilun keinoin. Tietoa voidaan pyrkiä hankkimaan esimerkiksi rokote- ja lääketutkimuksesta, diagnostiikasta tai muusta tutkimus- ja tuotekehitystiedosta.
- Työntekijöitä on myös syytä ohjeistaa tarkkaavaisuuteen kohdistetun tietojenkalastelun tai tietomurtoyritysten varalta sekä ilmoittamaan havainnoistaan matalalla kynnyksellä.

Tietoturva-alan kehitys

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficom antoi 4.5.2020 uuden määräyksen (M71) verkkotietojen ja verkon rakentamissuunnitelmien toimittamisesta. Määräyksen vaatimukset kohdistuvat sektorirajat ylittäen viestintä-, energia-, vesihuolto- ja liikenneverkkotoimijoihin.

ANALYYSI

- Määräyksen tarkoituksena on ennen kaikkea vähentää maanrakennustöistä verkkoinfrastruktuurille aiheutuvia vikatilanteita sekä edistää verkkojen yhteisrakentamista ja –käyttöä.
- Määräys tuli voimaan 1.6.2020. Fyysistä infrastruktuuria ja aktiivisia verkon osia koskevat velvoitteet tulevat kuitenkin voimaan vasta 1.10.2022, jolloin tietojen tulee olla toimitettu Sijaintitietopalveluun.
- Tutustu tarkemmin määräykseen ja sen perusteluihin: https://www.finlex.fi/fi/viranomaiset/normi/480001/45988

Arjen kyberturvallisuus – turvallisempi toukokuu

Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus

- Postin nimissä liikkuu nyt tietojenkalastelua ja tilausansahuijauksia tekstiviestien välityksellä. Huijaustyyppejä on ainakin kolme.
- Tarkastathan aina, että vierailemasi verkko-osoite on oikeasti sen organisaation osoite, jossa luulet vierailevasi.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

Elämänturvasovellukselle Suomen ensimmäinen mobiilisovellukselle myönnetty Tietoturvamerkki

- Kuluttajalle Tietoturvamerkki on tae siitä, että tuotteeseen ja palveluun liittyviin tietoturva-asioihin on kiinnitetty huomiota.
- https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/tiedotteet/tiedotteet/uutinen/1509564728604

Katsaus digi- ja kyberturvallisuuden maailmaan

- Digi- ja väestövirasto on julkaissut yhdessä Cyber Watchin kanssa katsauksen digi ja kybermaailman turvallisuuteen
- Kuuntele myös Kyberturvallisuuskeskuksen asiantuntijan vinkit
- https://www.cyberwatchfinland.fi/news/toukokuu-2020-katsaus-digi-ja-kyberturvallisuuden-maailmaan/

Digitaalinen vainoaminen ja erilaiset tavat häiritä verkossa

- Mitä tehdä? Mitä mikäkin asetus tarkoittaa. Disobey Outreach on ideoinut ja toteuttanut tekniseen suojautumiseen tarkoitetun oppaan, josta löydät ohjeita yleisimpiin haasteisiin
- https://40291b6e-2498-452e-8476-47c138a692fc.filesusr.com/ugd/dace2c_28b7a0d2ff6f48768472ad1a96177fc8.pdf

Ajankohtaista Kyberturvallisuuskeskuksesta

CinCan (Continuous Integration for the Collaborative Analysis of Incidents) -projekti on tullut päätökseen

- Projektin tarkoituksen oli kehittää työkaluja ja menetelmiä CSIRT-toimijoiden teknisen tutkinnan työnkulkujen automaation ja uhkatiedon laadun arviointiin.
- Toukokuussa järjestettiin kaksivuotisen projektin loppuseminaari, mutta erillisiä työpajoja hankkeen tiimoilta jatketaan
- Katso lisää: https://cincan.io/

Hajautettu nimipalvelu välittäjien käyttöön

- Suurin uhka verkkotunnusten toimivuudelle on palvelunestohyökkäys verkkotunnuksen omia nimipalvelimia kohtaan. Tällainen hyökkäys onnistuessaan estää www-sivuille pääsyn, sähköpostin käytön sekä taustajärjestelmien toimivuuden.
- Ainoa tehokas keino ehkäistä nimipalveluun kohdistuvia palvelunestohyökkäyksen vaikutuksia on käyttää suorituskyvyltään tehokasta anycast-tekniikalla hajautettua nimipalvelua.
- Traficom on ottanut käyttöön verkkotunnusvälittäjille maksuttoman hajautetun Anycast -nimipalvelun.
- https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon

Viestintäkampanja yhteistyössä KRP:n kanssa

- Kyberturvallisuuskeskus ja Keskusrikospoliisi haluavat yhdessä muistuttaa yleistyvistä kyberilmiöistä ja -uhista.
- Viikon aikana (1.-5.6.) julkaistiin joka päivänä tietoisku molempien sosiaalisenmedian kanavissa
- https://twitter.com/CERTFI/status/1267365306571411456
- https://www.facebook.com/NCSC.FI/

Sinustako arjen kybersankari? – Spoofy-mobiilipeli koululaisille

- Spoofy-mobiilipeli opettaa lomaileville alakoululaisille hauskalla tavalla salasanoihin, yksityisyyteen ja netin käytöstapoihin liittyviä digitaalisen turvallisuuden perustaitoja sekä huijauksilta ja nettikiusaamiselta suojautumista

- CGI:n yhdessä Traficomin ja Valtion kehitysyhtiö Vaken toteuttaman Spoofy-pelin voi ladata ilmaiseksi Google Play -kaupasta ja Applen App Storesta
- **Hyvää kyberturvallista kesää!**

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)