TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 2022

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen huolestuttava vakava

Kybersää maaliskuu 2022

Tietomurrot ja -vuodot

- Yksityishenkilöiden sosiaalisen median tileille on tehty runsaasti tietomurtoja ja tietomurtojen yrityksiä.

Huijaukset ja kalastelut

- Huijausviestejä lähetettiin poliisin nimissä sekä Suomessa että muualla Euroopassa
- Toimitusjohtajahuijauksia kohdistetaan taas kaikkiin organisaatioihin harrastekerhoista pörssiyrityksiin.

Haittaohjelmat ja haavoittuvuudet

- Useita ilmoituksia viesteistä, joissa on linkki OneDrive-tiedostonjakopalveluun.
- Useita ilmoituksia Emotet-haittaohjelman levitysyrityksistä sähköpostitse Suomessa.

Automaatio ja IoT

- Teollisuusautomaation seurantaraportit osoittavat kehitystä kyberturvallisuuskyvykkyydessä.

Verkkojen toimivuus

- Seitsemän merkittävää toimivuushäiriötä.
- Sähkökatkokset, laiteviat ja muutostyöt häiriöiden aiheuttajina.
- Palvelunestohyökkäyksiä raportoitiin eri sektoreilta aiempaa aktiivisemmin.

Vakoilu

- Venäjään liitettyjen toimijoiden tekemiä kyberhyökkäyksiä ja niiden yrityksiä nähdään Ukrainan lisäksi myös länsimaissa.
- FBI esti APT-ryhmä Sandwormin hallinnassa olevaksi epäillyn ja saastutetuista reitittimistä koostuneen bottiverkon käytön pahantahtoiseen toimintaan.

TRAFICOM

14.4.2022

Kuukauden tunnuslukuja

Maaliskuussa Suomen viestintäverkoissa oli yhteensä seitsemän merkittävää toimintahäiriötä. Yleensä häiriöitä on kuukaudessa keskimäärin kuusi kappaletta.

FBI esti APT-ryhmä Sandwormin hallinnassa olevaksi epäillyn bottiverkon käytön pahantahtoiseen toimintaan.

Keskimääräisen palvelunestohyökkäyksen kesto ensimmäisen vuosineljänneksen aikana oli noin 15 minuuttia.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

2

Johtaminen ja riskienhallinta. Toimintaympäristön nopeat muutokset koettelevat organisaatioiden riskienhallintaa kyberturvallisuudessa. Johdon vastuulla on varmistaa riskienhallinnan vaikuttavuus.

3

Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon. Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

Symbolit

Uusi

Päivitetty

4

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille! Tarve kyberturvallisuuden osaajille monipuolistuu uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

5

Käyttöoikeudet ovat avaimet organisaatioon. Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

TRAFICOM

14.4.2022

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Digitaalisuus läpileikkaa koko organisaation toimintaa ja erilaiset tapahtumat voivat vaikuttaa merkittävästi organisaation jatkuvuuden- ja riskienhallintaan.

- Muutokset kansainvälisten ilmiöiden kehityksessä näkyvät vaihtelevilla voimakkuuksilla Suomessa
- Esimerkiksi pitkittynyt koronaviruspandemia, talouden äkilliset muutokset, luonnonilmiöt, energian hinnannousu, sekä ennakoimaton kansainvälinen turvallisuustilanne näkyvät vaikeasti ennakoitavina kehityskulkuina, ja muutokset saattavat tapahtua nopeastikin
- Epävarmuustekijöillä voi yksistään olla isoja vaikutuksia organisaatioiden toimintaan. Yhdessä nämä ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia myös kyberturvallisuuden toimintaympäristössä
- Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön aiheuttamat uhkat kriittisille prosesseille

CASE

Toimitusketjut häiriintyivät koronapandemian alkaessa vakavasti. Esimerkiksi puolijohteiden saatavuus on ollut jo pidemmän aikaa huono eikä sirupula näytä helpottamisen merkkejä vielä lähikuukausina. Organisaatiot saattavat joutua odottamaan uusia laitteita kuukausikaupalla ja siten joutua käyttämään elinkaaren päässä olevia laitteita pidempään ja uusien suojausratkaisujen rakentamisessa kestää suunniteltua pidempään. Laitekaupoilla kannattaakin olla tarkkana, sillä saatavuushäiriöt ja hintojen nousu houkuttelevat markkinoille myös halpoja kopioita.

2. Johtamisella riskienhallintaa

Monen organisaation riskienhallinta ei pysy digitalisaation vauhdissa. Digitaalisia ratkaisuja otetaan käyttöön sokkona ilman riskien ymmärtämistä ja arviointia. Lopputulos saattaa olla riskialtis niin kansalaisen, organisaation itsensä kuin koko yhteiskunnan kannalta.

Organisaation riskienhallinta on viime kädessä johdon vastuulla. Johdon tulee seurata riskienhallinnan toteutumisesta vähintään:

- **Toimintaympäristön määrittely**. Organisaation tulee tunnistaa sen kriittiset prosessit ja mitä uhkia toimintaympäristö muodostaa
- **Riskien arviointi.** Organisaation on edellisen vaiheen pohjalta tunnistettava ja arvioitava riskit, sekä miten ne vaikuttavat kriittisiin prosesseihin
- **Riskien käsittely.** Kun riskit on arvioitu, organisaation tulee toteuttaa riittävät hallintatoimenpiteet riskien vaikutusten vähentämiseksi
- **Seuranta ja katselmointi.** Organisaation tulee seurata riskienhallintatoimenpiteiden vaikuttavuutta. Toimintaympäristön muutoksia ja omaa varautumista riskeihin tulee jatkuvasti seurata ja katselmoida

CASE

Esimerkkiskenaariossa organisaatio ei ole analysoinut toimintaympäristöään, eikä siten ole kyennyt arvioimaan sen vaikutuksia kriittisiin prosesseihinsa. Puutteellinen digitaalinen ratkaisu otetaan käyttöön tiedostamatta uhkaa. Riski, joka olisi ollut tunnistettavissa, realisoituu. Organisaation kriittinen prosessi pysähtyy, aiheuttaa mittavan mainehaitan sekä taloudelliset menetykset. Myös asiakkaiden tiedot ovat vaarantuneet. Riskin hallintatoimenpiteiden kustannukset olisivat olleet murto-osan asian korjaamisesta aiheutuneista kuluista.

3. Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon

Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena.
- Vuonna 2020 siirryttiin kiireen vilkkaa etätyö-moodiin. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.
- 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.
- Valtiolliset toimijat ovat tyypillisesti ensimmäisten joukossa hyödyntämässä uusia haavoittuvuuksia kybervakoiluun ja vaikuttamiseen. Valtiollisilla toimijoilla on myös riittävät resurssit päivitysten takaisinmallintamista varten uusien hyökkäysten mahdollistamiseksi kriittisissä ohjelmistoissa

CASE

Atlassian Confluence Server ja Data Center -tuotteista löydettyä haavoittuvuutta (CVE-2021-26084) hyväksikäyttämällä hyökkääjä pystyi suorittamaan etänä omaa ohjelmakoodiaan palvelimella ilman tunnuksia. Poikkeavan tapauksesta tekee se, että valmistaja julkaisi päivitykset ja ilmoitti alustavasti, ettei haavoittuvuus ollut kriittinen. Aluksi arvoitiin, että järjestelmään pääsemiseksi tarvitaan käyttäjätunnus. Kaksi päivää myöhemmin havaittiin, että tunnuksia ei tarvita lainkaan, vaan haavoittuvuuden hyväksikäyttö on helpompaa. Tästä syystä valmistaja muutti haavoittuvuuden arvion kriittiseksi.

4. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisäävät entisestään tarvetta erilaisille osaajille. Yritykset eivät etsi pelkkiä koodareita. Tulevaisuudessa laaja-alaisemmalle digitalisaation, kyberturvallisuuden ja datan osaamiselle on entistä enemmän kysyntää.

- **Osaamisen saaminen riittävälle tasolle kestää vielä pitkään.** Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla
  - Arviomme mukaan lyhyen aikavälillä tarvitaan erityisesti teknisiä osaajia, jotka osallistuvat tietoturvatutkintaan sekä ennaltaehkäisevään työhön
  - Pitkällä aikavälillä osaajatarve monipuolistuu ja esimerkiksi hallinnollisia osaajia tarvitaan lisää
- Osaajapula ei ole kiinni pelkästään määrästä, vaan myös laadusta! Osaaminen ei saisi henkilöityä liikaa, jotta jatkuvuus voidaan turvata kaikissa tilanteissa. Organisaation tietoturvan hallinta tulee osallistaa ja kouluttaa osaksi kaikkien työntekijöiden päivittäistä toimintaa
- Johdon tulee ymmärtää ja varmistaa riittävä osaaminen organisaatiossa kyberturvallisuusosaajien kysynnän kasvaessa. On tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa, sekä miten se hankitaan

CASE

2020 vuoden digibarometrin teemana oli kyberturvallisuus. Suomen tilanne on tutkimuksen mukaan kohtuullisen hyvä, mutta verrokkimaat uhkaavat karata etumatkalle. Erityisesti suurimmilla yrityksillä vaikuttaa olevan kirittävää. Kaikkiaan suomalaisissa yrityksissä esimerkiksi tietovuodot olivat yleisempiä kuin Euroopassa keskimäärin. Barometrissa selvitettiin Suomen kyberturva-alan osaamisvajetta. Kyselyn mukaan noin 60 prosenttia on kokenut osaajapulaa ja työvoiman saatavuus koettiin merkittävimmäksi yksittäiseksi alan kasvua hidastavaksi tekijäksi. (Digibarometri 2020)

5. Käyttöoikeudet ovat avaimet organisaatioon

Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

- Tunnuskalastelua tehdään monella eri tavalla ja eri laitteiden kautta. Sitä kohdistetaan sekä organisaatioihin että yksityishenkilöihin. Tunnuksia ja niihin liittyviä salasanoja yritetään lisäksi aktiivisesti murtaa automaattisin työkaluin. Jos avaimet viedään, tulee asiaan reagoida välittömästi!
- On hyvä pohtia, millaiset käyttöoikeudet omilla työntekijöillä tai ulkoistetuilla palveluntarjoajilla on yrityksen hallussa olevaan tietoon. Organisaation käyttäjillä tulee olla mahdollisimman rajoitetut, kuten perustason, käyttöoikeudet. Pääkäyttäjä-tason oikeuksien käyttö tulee olla erityisen suojattua ja kontrolloitua
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi monivaiheinen tunnistautuminen (MFA) on käytössä. Lisätietoja on saatavissa Kyberturvallisuuskeskuksen verkkosivuilta (1) (2)

OHJE

Jos käyttöoikeudet joutuvat vääriin käsiin, tulee toimia nopeasti.

1. Lukitse tunnus välittömästi!
2. Sulje kirjautunut murtaja pois organisaation palveluista.
3. Selvitä, mitä on tapahtunut ja tee toipumissuunnitelma.
4. Ota yhteys Kyberturvallisuuskeskukseen.
5. Kun voidaan varmistua, että rikollinen on häädetty, tulee käyttäjän vaihtaa salasana ja tunnuksen voi avata uudelleen

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

- Tietomurtoja tehty sosiaalisen median tileille
  - Yksityishenkilöiden sosiaalisen median tileille on tehty runsaasti tietomurtoja ja tietomurtojen yrityksiä.
  - Huijausyrityksessä murretulta tililtä lähetetään viesti, jonka tavoitteena on saada vastaanottajan Facebook-tili haltuun uhrin puhelinnumeron ja kaksivaiheisen tunnistautumisen vahvistuskoodin avulla.

Analyysi

- Kaapatuista tileistä on myös pyydetty lunnaita, joilla tilin saisi palautettua oikealle omistajalleen. Lunnaiden maksamista ei suositella.
- Kaapattuja tilejä käytetään edelleen pankki- ja maksukorttitietojen kalasteluun ja rahan varastamiseen.
  - Kyberturvallisuuskeskus tarjoaa neuvoja tilien suojaamiseksi ja palauttamiseksi.(3)
  - Kaksivaiheisen tunnistautumisen käyttöönottoon löytyy neuvoja Kyberturvallisuuskeskuksen ohjeesta.(4)

Huijaukset ja kalastelut

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

Huijaukset ja kalastelut

- Toimitusjohtajahuijauksia moniin organisaatioihin.
  - Toimitusjohtajahuijauksissa huijari tekeytyy organisaation johtajaksi ja lähestyy huijausviestillä taloushallinnon työntekijöitä.
  - Huijauksen tarkoituksena on saada työntekijä siirtämään rahaa jollain verukkeella huijarin kertomalle tilille.
  - Huijausviesti voi tulla monella eri tavalla: sähköpostilla, pikaviestimellä, puhelimella, tai muulla kommunikaatiolla. Huijari yrittää luoda uskottavan keskustelun johtajan ja työntekijän välille, jotta rahansiirto vaikuttaisi asialliselta.
  - Maaliskuussa rikolliset yrittivät huijata monenlaisia organisaatioita harrastekerhosta oppilaitokseen ja apteekista insinööritoimistoon.
  - Jopa eri tietoturvayrityksien uusia työntekijöitä on yritetty naruttaa rahansiirtoihin.

Analyysi

- Toimitusjohtajahuijauksiin käytetään väärennettyjä viestejä, jopa puheluita.
- Väärennetyt puhelut tulevat ulkomaisista puhelukeskuksista, mutta ne voi väärentää näyttämään Suomesta tulevalta.
- Suomalaiseen tytäryhtiöön tuli huijauspuhelu, joka oli väärennetty näyttämään tulevan yrityksen oman pääkonttorin vaihteesta.
- Teleoperaattorien uudella suosituksella pyritään vähentämään ja estämään väärennettyjä puheluita.

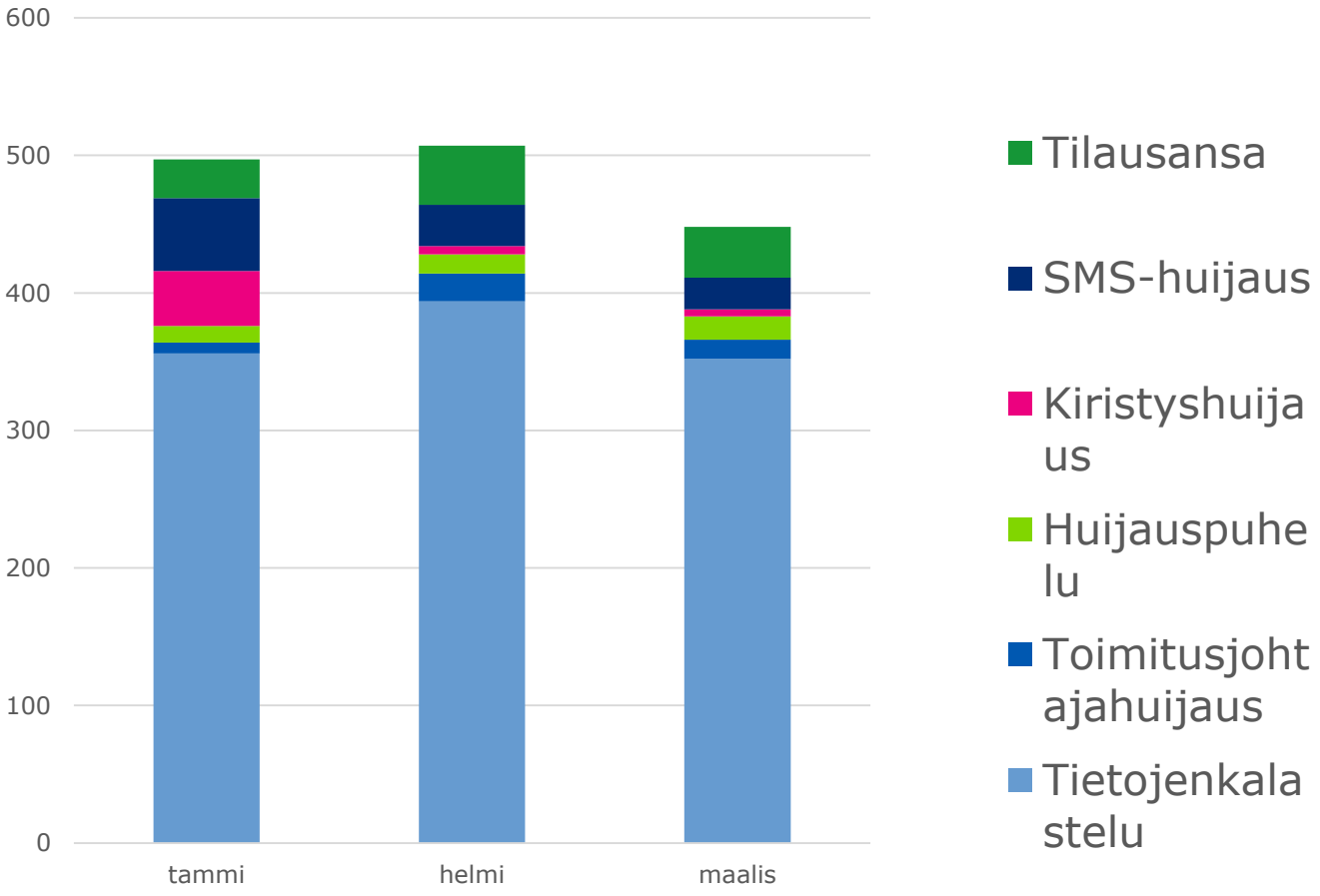
Pankkitietoja kalastellaan

- Pankkikalastelu on jatkunut aktiivisena.
  - Eri verkkopankkien kirjautumistietoja on kalasteltu huijausviesteillä sekä sähköpostitse että tekstiviesteillä tässäkin kuussa.
  - Tekstiviestihuijauksia on lähetetty myös verohallinnon ja Postin nimissä.
- Eri antivirustuotteiden, kuten Norton ja McAfee, nimissä liikkuu paljon huijauksia. Huijarin lähettämä tekstiviesti varoittaa tuotteen tilauksen päättyvän pian, ja kehottaa uusimaan tilauksen linkin kautta.
- Keskusrikospoliisi ilmoitti poliisin nimissä lähetetyistä huijausviesteistä, joissa huijari esitti poliisia. (5) (6)
  - Erisisältöisiä ja eri osoitteista lähetettyjä huijausviestejä yhdisti otsikon teksti "artikla 360”.
  - Europol on varoittanut vastaavista huijausviesteistä poliisin nimissä myös muualla Euroopassa.

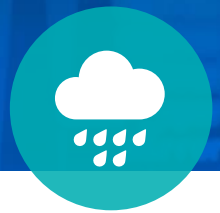
Ukrainan sotaa käytetään huijauksiin

- Huijarit pyrkivät hyödyntämään kansainvälisiä tapahtumia ja käyttämään hyväkseen ihmisten halua auttaa. Niin myös Ukrainan sodassa.
- Ukrainan sodan verukkeella on levitetty haittaohjelmia ja kalasteltu rahaa huijareille.
- Ukrainan tapahtumien myötä väärennettyä sähköpostiliikennettä tuntuu liikkuvan aiempaa enemmän.
- Oman organisaation sähköpostien väärinkäyttöä voi estää asettamalla verkkotunnuksen SPF/DKIM/DMARC-asetukset kohdalleen.

Käsiteltyjä huijaustapauksia Q1/2022



- Vuoden 2022 ensimmäisen neljänneksen ilmiöitä ovat:
  - Pankkitunnusten kalastelu ja tilausansat ovat jatkuneet aktiivisina.
  - Huijauspuhelut ovat vähentyneet edellisestä vuodesta, mutta eivät kuitenkaan kadonneet.
  - Huijauksiin käytetään kaikkia viestivälineitä sähköposteista ja tekstiviesteistä pikaviestimiin ja puheluihin.



Haittaohjelmat ja haavoittuvuudet

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

Haittaohjelmat

- Laaja haittaohjelmanlevityskampanja.
  - Kyberturvallisuuskeskukseen on tehty useita ilmoituksia viesteistä, joissa on linkki OneDrive-tiedostonjakopalveluun.
    - Linkin kautta levitetään QakBot-haittaohjelmaa.
  - Viestien lähettäjien osoitteet on väärennetty ja viestit näkyvät osana aitoja sähköpostikeskusteluketjuja.

Analyysi

- Haittaohjelmaa levitetään samalla mallilla kuin 2020 Suomeen iskenyttä Emotet-haittaohjelmaa.
  - Jollakin tavalla varastettuun postikeskusteluun tulee väärennetystä lähteestä uusi viesti, jossa pyydetään lataamaan tiedosto.
  - Tiedostosta uhrin Windows-laitteeseen tarttuisi QakBot-haittaohjelma.

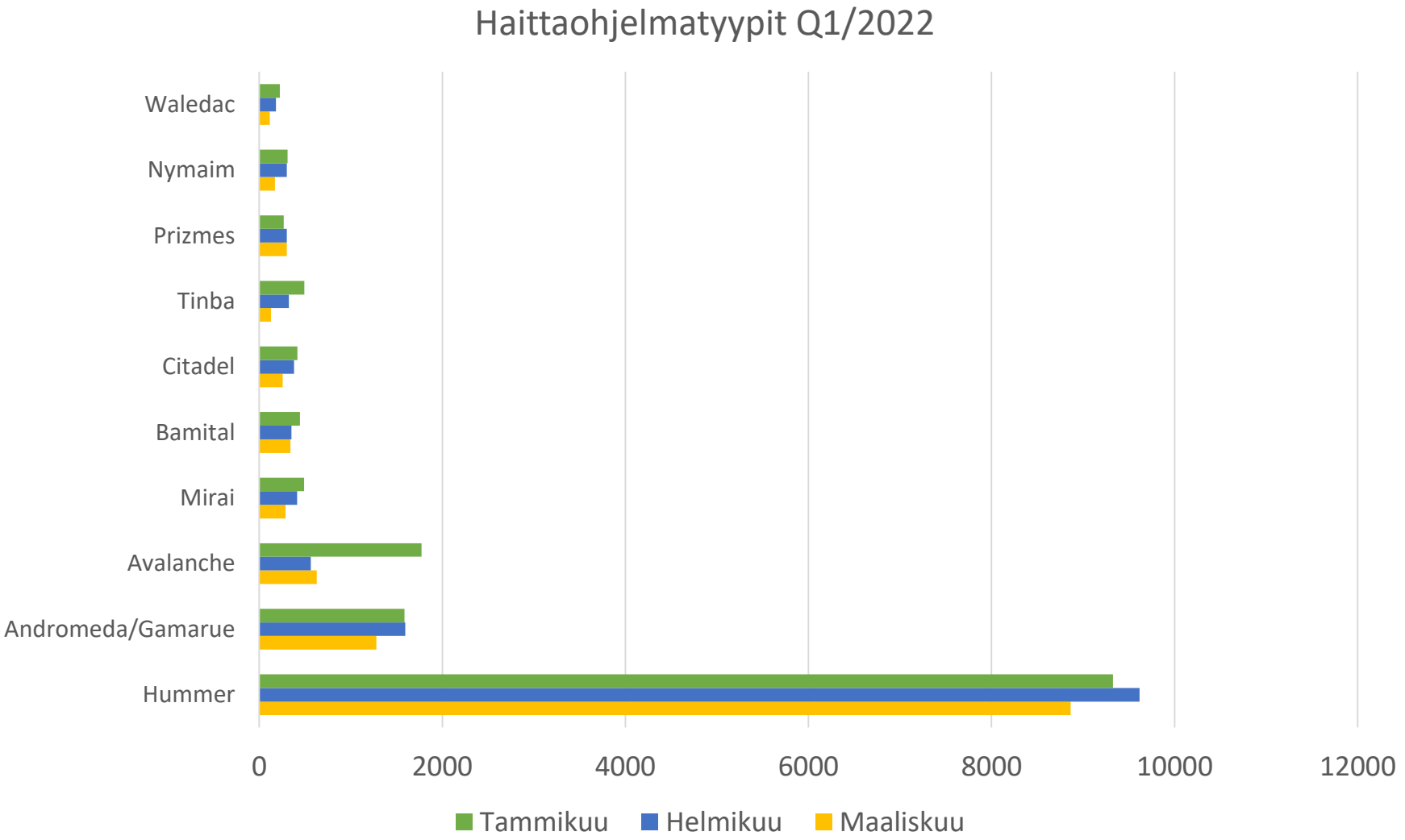
Haittaohjelmat

- Emotet-haittaohjelma on palannut.
  - Kyberturvallisuuskeskus on saanut useita ilmoituksia Emotet-haittaohjelman levitysyrityksistä sähköpostitse Suomessa.
  - Onnistuneita haittaohjelmatartuntoja ei ole tiedossa. Sähköpostiliitteet ja -linkit on syytä tarkistaa erityisen huolellisesti.
  - Emotet-haittaohjelmaverkosto otettiin viranomaisten haltuun kansainvälisessä poliisioperaatiossa tammikuussa 2021, minkä jälkeen Emotet oli voitettu hetkellisesti.

Analyysi

- Emotet muistetaan siitä, että se leviää sähköpostitse massoittain ympäri maailmaa.
- Kun Emotet-haittaohjelma on asentunut koneelle, saattaa se tarjota Malware-as-a-Service -palvelua eli mahdollisuuden esimerkiksi kiristyshaittaohjelmaryhmille jalansijaan kohdeorganisaation verkossa.

Autoreporterin haittaohjelmahavainnot



Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyberturvallisuuskeskuksen verkkosivuilla.(7)

Kuukauden haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus Spring-sovelluskehyksessä (6/2022).
  - Haavoittuvuuden kohteena olevaa Spring -kirjastoa käytetään laajasti erilaisissa verkon sovelluksissa ja palveluissa.
  - Skannaus ja hyväksikäyttöyritykset ovat lisääntyneet viime viikon (vko 13) jälkeen.
- Haavoittuvuuksista löytyy lisätietoja osoitteesta www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Analyysi

- Päivitykset tulee asentaa viipymättä, koska haavoittuvuuksien hyväksikäyttö on todella nopeaa.
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa.

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

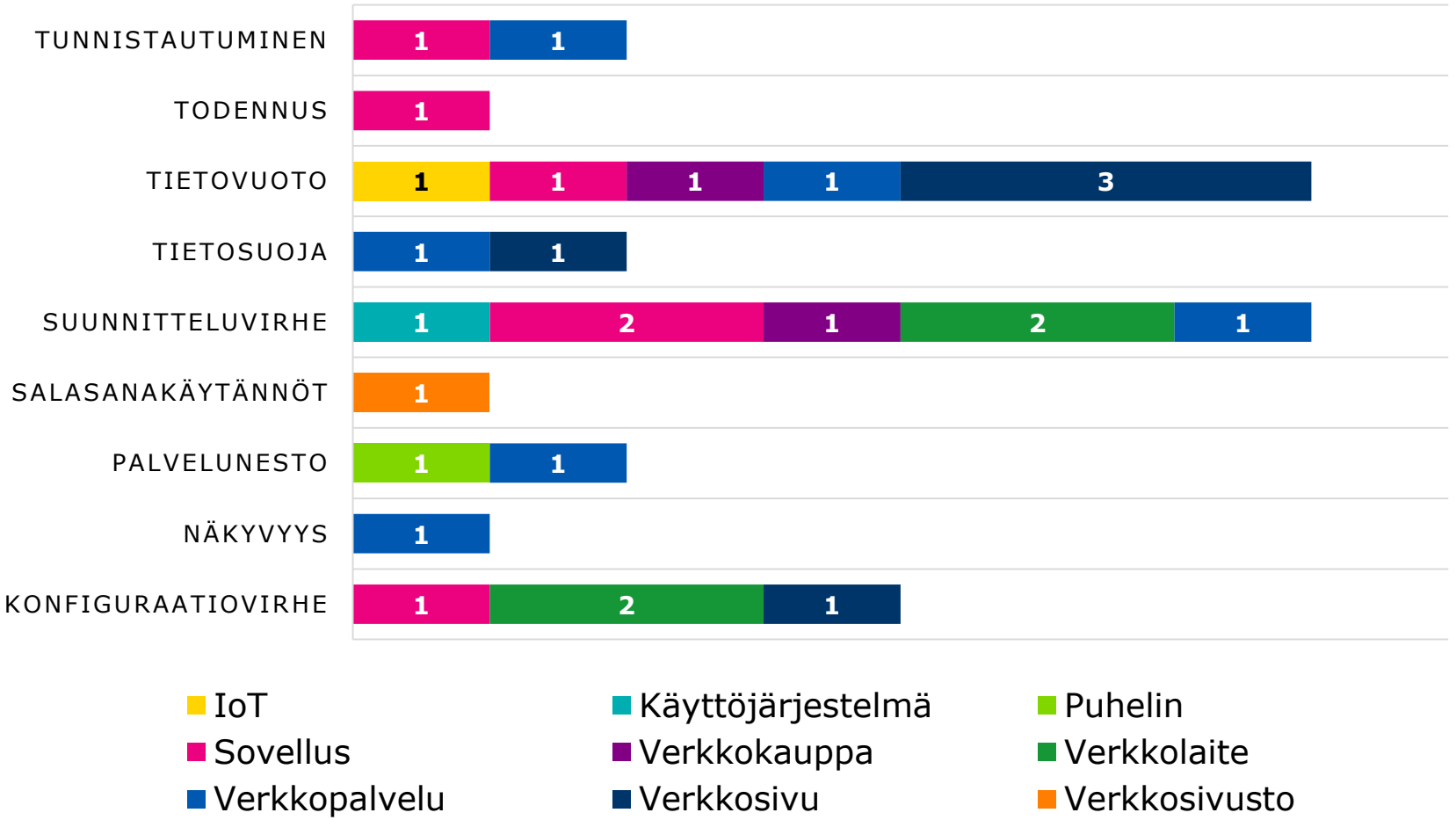
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 6 kpl (tilanne 12.4.2022)**
  - Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet.
- **Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista.**
  - Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta.
  - Kooste julkaistaan lähes päivittäin ja sen voi tilata kotisivuiltamme. (8)

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat usein toistuva ongelma. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy kovakoodattu oletussalasana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanakäytännöissä esim. salasanan vaatimusten vai vaihto-ominaisuuksien osalta.
- IoT- ja verkkolaitteiden testaus on yleistä tietoturvatutkijoiden keskuudessa. Laitteiden turvallisuuden parantaminen on tärkeää verkossa ja kotona käytössä olevien laitteiden määrien jatkuvan kasvun vuoksi.
- Kyberturvallisuuskeskus saa haavoittuvuuksista ilmoituksia laidasta laitaan. Mikäli sinä tai organisaatiosi tarvitsette apua haavoittuvuuden löytyessä, haavoittuvuuden koordinoinnissa tai esimerkiksi CVE-tunnisteen haussa – olettehan yhteydessä Kyberturvallisuuskeskukseen.
- https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Haavoittuvuuskoordinaatiota on esitelty laajemmin verkkosivuillamme.(9)

Automaatio ja IoT

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

IoT

- Yhdysvaltojen viranomaiset ilmoittivat paljastaneensa ja siivonneensa maaliskuussa 2022 saastuneiden kotireitittimien muodostaman bottiverkon.
  - Bottiverkkoa operoi Sandworm-nimellä tunnettu venäläinen valtiollinen toimija.
  - Yhdysvaltain viranomaiset onnistuivat katkaisemaan bottiverkon komentokanavan (C2) poistamalla tähän liittyvät hyökkääjän asentamat toiminnot (Cyclops Blink) saastuneilta laitteilta.(22)
- Bottiverkon hallussa oli mm. ASUS-reitittimiä ja valmistaja on julkaissut ohjeita laitteiden siivoamiseksi.(23)

Analyysi

- Miljoonat IoT-laitteet muodostavat myös rikollisryhmille sekä valtiollisille toimijoille houkuttelevan kohteen.
- Suuri joukko näiden hallussa olevia kotien laitteita muodostaa vahvan bottiverkon. Sitä taas voidaan käyttää esimerkiksi voimakkaisiin palvelunestohyökkäyksiin tai muiden hyökkäysten kybertoimintojen jälkien peittelyyn.
- Mikäli kodin reititin on vieraan tahon hallussa vaarantaa sen myös kuluttajan tietojen luottamuksellisuuden. Myös mahdolliset toimintahäiriöt kuten verkkoyhteyksien pätkiminen ovat mahdollisia.
- Kodin laitteissa tuleekin aina muistaa huolehtia mieluiten automaattisista tietoturvapäivityksistä. Laitteet tulee myös määritellä turvallisille asetuksille. Lisäksi on syytä seurata valmistajien tietoturvatiedotteita.

Automaatio

- Teollisuusautomaatioon keskittyvät tietoturvayritykset Dragos ja Claroty ovat julkaisseet vuosiraporttinsa.
  - Lukumääräisesti löydettyjen uusien teollisuusautomaation (ICS/OT) haavoittuvuuksien määrä jatkoi voimakasta kasvuaan kasinkertaistuen edellisestä vuodesta.
  - Positiivista oli, että entistä useampaan haavoittuvuuteen oli kuitenkin saatavilla valmistajan korjaus tai vähintään vaikutusten rajoittamiskeino.
  - Tietoturva-auditointien valossa ulkoisten etäyhteyksien määrä automaatioympäristöihin on lisääntynyt entisestään. Positiivisena trendinä nähtiin OT-ympäristöissä tapahtunut siirtymä kokonaan erilliseen käyttäjähallintaan. (10) (11)

Analyysi

- Automaatioympäristöjen kyberturvallisuusriskit lisääntyvät
  - Tietoturvatutkijoiden ja kyberrikollisten mielenkiinto automaatioympäristöjä kohtaan on lisääntymässä, jolloin haavoittuvuuksia julkaistaan ja myös hyödynnetään entistä enemmän.
  - Päivitysten asentaminen automaatioympäristöissä on usein haastavampaa kuin perinteisissä toimistoympäristöissä.
- Automaatioympäristöissä päivittämättömien haavoittuvuuksien vaikutuksia voidaan lieventää esimerkiksi seuraavilla keinoilla:
  - Verkon segmentoinnilla, etäyhteyksien turvallisuuden varmistamisella, tietoliikenteen rajoittamisella sekä poikkeamien havaitsemisella.
  - Oleellista on myös eriyttää organisaation toimisto- ja automaatioympäristöt niin, että samoilla laitteilla tai käyttäjätunnuksilla ei käytetä molempia ympäristöjä.

IoT

- AEG:n mikroaaltouuni alkoi virheellisen ohjelmistopäivityksen vuoksi pitää itseään höyryuunina.(12)
- Viikkojenkaan jälkeen valmistaja ei kyennyt toteuttamaan verkon yli jaeltavaa korjaavaa ohjelmistopäivitystä. Huoltohenkilöstö joutuu asentamaan korjauksen asiakkaan luona, koska tuote menetti myös verkkoyhteytensä.
- Ongelma syntyi, kun päivityksien jakelusta vastannut valmistajan henkilöstö syötti väärän tunnisteen niiden jakelusta huolehtivaan järjestelmään.
- Viikkojen ajaksi käyttökelvottomaksi mennyt laite varmasti pahoitti monen asiakkaan mielen.

Analyysi

- Tapaus on esimerkki siitä mihin älylaitteiden yleistyminen voi joskus johtaa. Kuluttajan olisikin hyvä pohtia jo ostopäätöstä tehdessään, onko ”äly"-ominaisuus todella tarpeellinen.
- Vaikka tällä kertaa ongelman syynä olikin pieleen mennyt ohjelmistopäivitys, ei se muuta yleistä suositusta asentaa ainakin tietoturvapäivitykset viipymättä.
- Älylaitteiden valmistajien tulisi huomioida niiden suunnittelussa myös epäonnistuvan päivityksen mahdollisuus. Laitteisiin tulisikin aina toteuttaa myös jonkinlainen toiminto, jolla ne olisi palautettavissa päivitystä edeltäneeseen tilaan.

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

- Maaliskuussa yleisissä viestintäpalveluissa oli 7 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 2, C: 5
  - B-vioista toinen kohdistui VoLTE-yhteyksiin ja toinen radiokanavien kuuluvuuteen Pohjois-Suomessa.
- Häiriöiden syyt vaihtelivat ja kaksi häiriöistä aiheutui sähkökatkon vuoksi.
  - Erilaiset muutostyöt aiheuttavat myös välillä häiriöitä, kun kaikki ei menekään suunnitellusti.
- Verkkojen toimivuus Suomessa on tällä hetkellä hyvä.

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa oli vuonna 2021 keskimäärin hyvä.
- Kuukaudessa on keskimäärin noin kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat meille, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

ICT-palveluiden toimivuus

- Ukraina koettaa urheasti pitää kriittisen verkkoinfrastruktuurin toiminnassa keskellä Venäjän hyökkäyssotaa.(13)
  - Koillisessa Okhtyrkan kaupungissa venäläisohjus tuhosi maan suurimman verkko-operaattorin Kyivstarin datakeskuksen.
  - Isku katkaisi kaupungin puhelinyhteydet.
- Tuoreessa raportissa kerrotaan tulipalon seurauksista yhdessä maailman suurimmassa datakeskuksessa
  - OVHcloudin datakeskuksen tulipalosta maaliskuussa 2021 on paljon opittavaa. Datakeskuksesta puuttui automaattinen sammutusjärjestelmä ja sähköjen katkaisujärjestelmä. Tulipalon sytyttyä sen sammutus oli erittäin vaikeaa. (14)

Analyysi

- Kaikkeen tulee varautua, myös datakeskusten mahdolliseen lamautumiseen.
- Ääriesimerkit maailmalta osoittavat, että kaikki on mahdollista ja ilman toimivia yhteyksiä elämä hankaloituu huomattavasti.
- Organisaationäkökulmasta kahdennetut yhteydet, toimivat palautussuunnitelmat ja poikkeamaprosessit osoittavat tärkeyttään erikoistilanteissa.

Palvelunestohyökkäykset

- Maaliskuussa vastaanotimme tavanomaista enemmän ilmoituksia palvelunestohyökkäyksistä.
  - Hyökkäyksiä raportoitiin useilta eri sektoreilta, mutta suuremmilta vaikutuksilta vältyttiin.
- Kuntasektorin toimijat ilmoittivat hyökkäyksistä, joilla oli vaikutuksia palveluiden toimintaan
- Huhtikuun 8. päivä ministeriöiden verkkosivut olivat palvelunestohyökkäysten kohteena.(15)
  - Myös Valtori kertoi torjuneensa palvelunestohyökkäyksiä 8.4.(16)

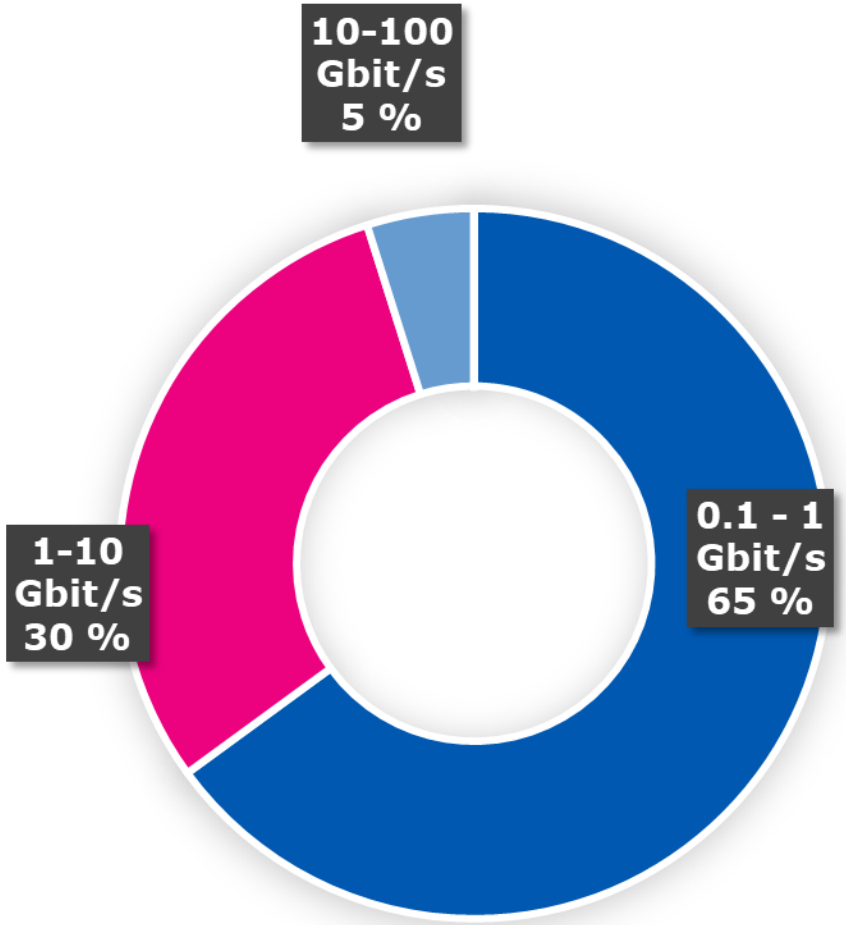
Analyysi

- Organisaatioiden on hyvä varautua palvelunestohyökkäyksiin mitigointipalvelulla, joka kestää kymmenien gigatavujen kokoiset hyökkäykset.
  - Organisaation tietoliikenneyhteyksien on myös kestettävä tämän kokoiset hyökkäykset; mikäli yhteys on 10G ja hyökkäys 30Gbit/s - voi hyökkäys aiheuttaa väliaikaisen putkitukoksen.
  - Vastaanottamiemme ilmoitusten perusteella 30Gbit/s-kokoinen hyökkäys on ollut yleisin meille organisaatioilta ilmoitettu kokoluokka.
- Palvelunestohyökkäys on helppo ja näyttävä tapa aiheuttaa hämmennystä ja uutisointia, mikäli kohteena on jokin tunnettu taho.
- Palvelunestohyökkäyksellä verkkosivuille ei kuitenkaan aiheuteta kuin ajallinen katkos sivun saatavuuteen - ellei hyökkäyksellä ole välillisiä vaikutuksia muihinkin palveluihin samasta osoitteesta johtuen.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 126 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q1/2022.
- Noin 75% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q1/2022 - 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

- Kybervakoilu ja informaatiovaikuttaminen ovat jatkuneet aktiivisina Ukrainassa.
  - Myös muiden kuin Venäjään liitettyjen ryhmien kybervakoilu on lisääntynyt Ukrainassa.
- Huhtikuun alkuun mennessä Ukrainassa on havaittu 7 eri tuhoamishaittaohjelmaa useilla eri toimialoilla.
- Venäjään liitettyjen toimijoiden tekemien kyberhyökkäysten määrä on lisääntynyt länsimaissa.
  - Länsimaisiin organisaatioihin kohdistuvilla hyökkäyksillä tarkoitetaan tässä yhteydessä kohteiden kartoitusta, julkisissa verkoissa olevien järjestelmien (erityisesti VPN) murtoyrityksiä ja haitallisia sähköposteja.
- Myös venäläisiin organisaatioihin on tehty lukuisia tietomurtoja. Ainakin osa hyökkäyksistä on tehty todennäköisesti haktivistien toimesta.

Analyysi

- Koska erilaisia murtoyrityksiä ja kartoitusta nähdään myös länsimaisissa organisaatioissa, on nyt viimeistään aika tarkastella oman organisaation varautumista mahdollisiin kyberhyökkäyksiin.
- Kyberturvallisuuskeskus on aiemmin tänä vuonna julkaissut ohjeen kyberturvallisuuden vahvistamisesta suomalaisissa organisaatioissa.(17)

Vakoilu

- Britannian ja Yhdysvaltojen viranomaiset varoittivat bottiverkosta, jonka epäiltiin olevan Venäjään liitetyn APT-ryhmän Sandwormin hallinnassa.
- Bottiverkko koostui Cyclops Blink -haittaohjelmalla saastuteista pienreitittimistä, joita voidaan käyttää esimerkiksi yrityksissä ja kodeissa.
  - Tiedossa on, että bottiverkkoon on kuulunut ainakin WatchGuardin ja Asuksen laitteita.
  - Murrettujen Asuksen laitteiden osallisuudesta bottiverkkoon kertonut Trendmicro on lisäksi todennut saaneensa viitteitä myös ainakin yhden muun valmistajan laitteisiin pureutuvasta haittaohjelmaversiosta, mutta valmistajaa ei ole kerrottu julkisuuteen vahvistetun haittaohjelmanäytteen puuttumisesta johtuen.
- FBI otti huhtikuun alussa haltuunsa bottiverkon komentopalvelimia ja esti näin sen hyödyntämisen pahantahtoisilta toimijoilta.
- Murretuista verkkolaitteista koostuvia bottiverkkoja voitaisiin hyödyntää esimerkiksi muita organisaatioita vastaan tehtävissä kyberhyökkäyksissä.

Analyysi

- APT-toimijat voivat hyödyntää muita kuin varsinaisiin kohteisiinsa liittyviä haavoittuvia laitteita osana hyökkäysinfrastruktuuriaan.
- Kodin ja yrityksen laitteiden ohjelmistoversioiden ajantasaisuudesta huolehtiminen, oletussalasanojen vaihtaminen ja sen varmistaminen, että niiden hallintapaneeleihin ei päästä käsiksi suoraan internetistä, ovat tärkeä osa laitteen suojaamista pahantahtoisilta toimijoilta.

Tietoturva-alan kehitys, sääntely ja standardit

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

- Neuvosto ja Euroopan parlamentti yhteisymmärrykseen digimarkkinasäädöksestä.
- 25.3.2022 saavutettu alustava poliittinen yhteisymmärrys EU:n digimarkkinasäädöksestä (Digital Markets Act).
- Tavoitteena määritellä selkeät säännöt suurille verkkoalustoille ja turvata oikeudenmukainen ja toimiva kilpailu digitaalisilla markkinoilla.
  - Ns. portinvartijan asemassa oleville suurille yrityksille voidaan asettaa erityisvelvoitteita koskien näiden tarjoamia ydinalustapalveluita.
  - Ydinalustapalveluihin kuuluvat mm. markkinapaikat ja sovelluskaupat, hakukoneet, verkkoyhteisöpalvelut, pilvipalvelut, mainospalvelut ja verkkoselaimet.
- Kyse on EU-asetuksesta, jota tullaan soveltamaan sellaisenaan kaikissa jäsenmaissa.(18)

Oikeudelliset asiat

- Euroopan komissio ja Yhdysvallat sopineet periaatetasolla uudesta ”Privacy Shield 2.0” –sopimuksesta.
- Tarkoituksena sopia sääntelykehyksestä, jonka puitteissa datan siirto EU:n alueelta Yhdysvaltoihin on mahdollista niin ettei EU-kansalaisten tieto- ja yksityisyydensuoja vaarannu.
- EUT kumosi edellisen Privacy Shield –sopimuksen EU:n tietosuoja-asetuksen vastaisena vuonna 2020.(19)

Oikeudelliset asiat

- Tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri) on kommentointikierroksella 19.4. asti.(20)
- Arviointikriteeristön tavoitteena tukea julkishallinnon tietoturvallisuuden kehittämistä ja arviointia.
- Julkri toimii apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.
- Kriteerit on ryhmitelty viiteen osa-alueeseen:
  - Hallinnollinen turvallisuus
  - Fyysinen turvallisuus
  - Tekninen turvallisuus
  - Varautuminen ja jatkuvuudenhallinta
  - Tietosuoja

Oikeudelliset asiat

- Luonnos Suomen digitaaliseksi kompassiksi lausuttavana 13.5. asti.(21)
- Tavoitteena on luoda kansallinen kokonaiskuva ja yhtenäinen tilannekuva Suomen digitalisaatiokehityksestä.
- Digitaalisessa kompassissa on määritelty tavoitteet ja lähivuosien toimenpiteet kohti vuotta 2030.
- Digikompassin laatimisen tarkoituksena on myös vahvistaa yhteistä ymmärrystä digitalisaation ja datatalouden hyödyistä, käsitteistä ja suunnasta kansallisesti sekä osana EU:ta.
- Suomen digikompassi muodostuu EU:n digikompassin mukaisesti neljästä osa-alueesta:
  - Osaaminen
  - Digitaalinen infrastruktuuri
  - Yritysten digitalisaatio
  - Digitaaliset julkiset palvelut

Arjen kyberturvallisuus

Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi

- Monivaiheisella tunnistautumisella tarkoitetaan sitä, että henkilöllisyytesi varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä. Lähes kaikki käyttäjätilien kaappausyritykset voidaan estää monivaiheista tunnistautumista käyttämällä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Varo huijareita internetin myyntialustoilla!

- Huijausyrityksessä tarkoituksena on saada myyjän pankkitiedot huijarin haltuun.
- Ole valppaana ja kyseenalaista miksi ostaminen pitää tehdä kuriiripalvelun kautta.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ttn_04032022

Näin suojaudut nettihuijaukselta

- Verkossa on runsaasti huijareita, jotka haluavat rahasi tai tietosi. Huijausviestejä satelee sähköpostitse, tekstiviestitse ja puhelimitse.
- Nettihuijariin voit törmätä lähes missä vain: keskustelu-, deitti-, osto- ja myyntipalstoilla sekä verkkokaupoissa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Uutisia Kyberturvallisuuskeskuksesta

Tietoturvan vuosi 2021 -katsaus julkaisu

- Katsaus kertaa vuoden tärkeimmät tapahtumat ja kertoo kybertapausten voimakkaasta kasvusta.
- Kyberturvallisuuskeskuksen käsittelemien tietoturvatapahtumien määrä räjähti voimakkaaseen kasvuun viime vuonna.
- Kyberturvallisuuskeskuksen toiminta painottuu kasvavassa määrin vakavien ja yhteiskunnan kannalta merkittävien kyberhäiriöiden ennaltaehkäisyyn.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-vuosi-2021-kertaa-vuoden-tarkeimmat-tapahtumat-ja-kertoo-kybertapausten

Suomi vahvasti mukana Euroopan 6G-taajuustyössä

- Kuudennen sukupolven matkaviestinteknologiaa eli 6G:tä innovoidaan jo aktiivisesti. Euroopan komissio keskittyy aluksi 6G-teknologian kehitysaskeliin Euroopassa ja valmistelee tiekarttaa 6G:n käyttöönotolle.
- Liikenne- ja viestintävirasto Traficom sekä liikenne- ja viestintäministeriö osallistuvat 6G-taajuustyöhön taajuuksien tehokkaan käytön ja tulevaisuuden laajakaistaverkkojen sekä palveluiden kehityksen varmistamiseksi.
- https://www.traficom.fi/fi/ajankohtaista/suomi-vahvasti-mukana-euroopan-6g-taajuustyossa

Kuntien tietoverkoista etsittiin ja korjattiin haavoittuvuuksia

- Kuntien sekä sosiaali- ja terveysalan toimijoiden digitaalisista palveluista etsittiin haavoittuvuuksia kartoituksella, jonka toteuttivat Digi- ja väestötietovirasto sekä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.
- Kunnat ja sote-toimijat saivat ajantasaista tietoa palveluidensa haavoittuvuuksista ja pystyivät sen perusteella tekemään tarvittavat korjaukset ja siten parantamaan palveluiden turvallisuutta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digipalveluiden-haavoittuvuuksien-tunteminen-tarkeampaa-kuin-koskaan-kuntien

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)
  - Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi
  - Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo

1) Kyberturvallisuuskeskus: Suojautuminen Microsoft Office 365 –tunnusten kalastelulta ja tietomurroilta
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja-tietomurroilta

2) Kyberturvallisuuskeskus: Opas tietomurtojen havaitsemiseen
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

3) Kyberturvallisuuskeskuksen neuvot tilien suojaamiseksi ja palauttamiseksi https://www.kyberturvallisuuskeskus.fi/fi/ttn_20012022

4) Ohjeet kaksivaiheisen tunnistautumisen käyttöönottoon https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

5) Poliisin varoitus poliisijohdon nimissä lähetetyistä huijausviesteistä
https://poliisi.fi/-/poliisi-varoittaa-poliisijohdon-nimissa-lahetetyista-huijausviesteista

6) Keskusrikospoliisin varoitus sen nimissä lähetetyistä huijaussähköposteista
https://poliisi.fi/-/varoitus-krp-n-nimissa-lahetetyista-huijaussahkoposteista-ala-avaa-liitteita-poista-viestit

7) Autoreporterin tiedot https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

8) Haavoittuvuuksien uutiskirjeen tilaaminen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Lähdeluettelo

9) Haavoittuvuuskoordinaation esittely https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

10) Dragos cybersecurity year 2021 in review https://www.dragos.com/year-in-review/

11) HelpNetSecurity: ICS vulnerability disclosures surge 110% over the last four years https://www.helpnetsecurity.com/2022/03/08/ics-vulnerability-disclosures-grew/

12) Whitegoodsnow: AEG combi microwave unusable after update: device thinks it is a steam oven https://whitegoodsnow.com/2022/03/19/aeg-combi-microwave-unusable-after-update-device-thinks-it-is-a-steam-oven/

13) Forbes: Ukraine’s Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/?sh=1f546e065a4c

14) The Register: OVHcloud datacenter 'lacked' automatic fire extinguishers, electrical cutoff https://www.theregister.com/2022/03/22/ovhcloud_fire_datacenter_report/

15) Yle: Valtioneuvoston ja ministeriöiden verkkosivuihin kohdistunut palvelunestohyökkäys on ohi https://yle.fi/uutiset/3-12396843

Lähdeluettelo

16) Valtorin verkkosivupalveluun kohdistuneet palvelunestohyökkäykset torjuttu onnistuneesti https://valtori.fi/-/valtorin-verkkosivupalveluun-kohdistuneet-palvelunestohyokkaykset-torjuttu-onnistuneesti

17) Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille

18) Eurooppa-neuvosto: Neuvosto ja Euroopan parlamentti yhteisymmärrykseen digimarkkinasäädöksestä https://www.consilium.europa.eu/fi/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/

19) Euroopan komissio: European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

20) Tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri), kommentointipyyntö https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=b56988ec-85e8-4317-aab4-948b265d7b19

21) Luonnos Suomen digitaaliseksi kompassiksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=d77ee4a5-6d68-44cd-b8c1-0957ca01b2ac

Lähdeluettelo

22) United States department of Justice: Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate (GRU) https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

23) ASUS product security advisory https://www.asus.com/content/ASUS-Product-Security-Advisory/