TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 2021

#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

TRAFICOM

Kybersää elokuu 2021

Tietomurrot ja -vuodot

- Verkkotunnus Vastaamohaku.com rekisteröitiin elokuun loppupuolella, verkkotunnus ajettiin alas muutamaa päivää myöhemmin
- Kuukauden aikana on raportoitu useampia murtoja käyttäjätileille kalastelun seurauksena

Huijaukset ja kalastelut

- Pankkitunnusten kalastelu muuttuu koko ajan paremmin tehdyksi.
- Hakukoneisiin on syötetty sekä väärennettyjä tuloksia että mainoksia, jotka johtavat oikean palvelun sijasta tietojenkalasteluun.

Haittaohjelmat ja haavoittuvuudet

- Poistimme Android-haittaohjelmia koskevan varoituksen 17.8.
- PrintNightmare-haavoittuvuuskokonaisuus on vieläkin ajankohtainen
- Atlassian Confluence-haavoittuvuuden aktiivista hyväksikäyttöä

Automaatio

- Paljon vakavia haavoittuvuuksia, joita pyritään hyödyntämään aktiivisesti
- ETSI on julkaissut teknisen spesifikaation IoT-kuluttajalaitteiden tietoturvan arvioimisesta

Verkkojen toimivuus

- Neljä merkittävää toimivuushäiriötä
- Murrettuja Confluence-palvelimia käytettiin palvelunestohyökkäyksiin.
- Syksy saapuu ja tuo tullessaan hyökkäilyjä oppimisympäristöjä kohtaan. Muistuta koululaistasi, että tietoverkkojen häirintä on rikos.

Vakoilu

- Kiinalaistoimijat ovat pyrkineet vuosien ajan tunkeutumaan teleoperaattoreiden järjestelmiin Aasissa vastaavin menetelmin kuin Hafnium-operaatiossa.
- Keväällä nähty kampanja, jossa sähköpostitse pyrittiin asentamaan laitteelle Cobalt Strike -haittaohjelma, kohdistui Euroopassa ainakin Slovakiaan.

TRAFICOM

16.9.2021

Kuukauden tunnuslukuja

200%

Meille ilmoitettujen pankkikalasteluiden määrä tuplaantui. Tämä tarkoittaa myös valitettavasti sitä, että rikolliset ovat saaneet varastettua lisää rahaa.

1

BadAlloc-haavoittuvuus koskee monia reaaliaikakäyttöjärjestelmiä. BlackBerryn QNX-reaaliaikakäyttöjärjestelmän tiettyjen versioiden todettiin olevan alttiita BadAlloc-haavoittuvuudelle. BadAlloc-haavoittuvuuskokonaisuuden avulla on mahdollista suorittaa etäkomentoja verkossa oleviin laitteisiin.

0

Flubot-epidemia saatiin kuriin elokuussa, sillä heinäkuun jälkeen emme ole saaneet uusia ilmoituksia haittaohjelman levittämisestä. Siksi myös kesän aikana ollut varoitus saatettiin poistaa.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

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.

2

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta. Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

3

Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät. Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

Symbolit

Uusi

Päivitetty

4

Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää. Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

5

Etätyö tuli jäädäkseen – niin myös riskit. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

3kk

TRAFICOM

16.9.2021

1. 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

Microsoft tiedotti 2.3. Exchange-sähköpostipalvelimien kriittisistä haavoittuvuuksista ja niiden aktiivisesta hyväksikäytöstä. Kyberturvallisuuskeskus havaitsi suomessa aluksi lähes 300 haavoittuvaa Exchange-palvelinta. Mukana oli myös palvelimia, joihin oli jo murtauduttu haavoittuvuutta hyväksi käyttäen. Suomalaisten organisaatioiden haavoittuvat Exchange-palvelimet oli päivitetty huhtikuun alkuun mennessä. Organisaatioiden kyky reagoida kriittisiin haavoittuvuuksiin, päivityksiin sekä tietomurtojen tutkintaan nousi tärkeäksi osaksi Exchange-haavoittuvuuksien hoidossa.

2. Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta

Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

- Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Toiminta on aktiivista ja kehittyy jatkuvasti.

CASE

Palvelunestohyökkäyksillä kiristäminen nousi maailmalla ilmiönä loppu-vuodesta 2020 ja ilmiö rantautui myös Suomeen. Kyberturvallisuuskeskus on saanut ilmoituksia myös vuonna 2021 aiheeseen liittyen.

Yleisesti organisaatio vastaanottaa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Kiristysviestin lähettämisen aikoihin on joissain tapauksissa tehty myös palvelunestohyökkäys viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, mikäli lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

3. Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät

Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

- Pilvipalveluratkaisuiden hahmottaminen on vaikeaa, koska ympäristö on laaja. Siirtyminen pilveen on jäänyt puolitiehen ja tietojärjestelmien migraatio on jäänyt viimeistelemättä. Vanhoja palveluita voidaan edelleen hyväksikäyttää.
- Aivan kuten perinteisessä tietoverkossa, mikäli hyökkääjä onnistuu pääsemään pilven reunalle, voi sen kautta levittäytyä myös organisaation muihin verkon segmentteihin pilven ulkopuolellakin.
- Tarve kehittää yleisesti hyväksytyt tietoturvavaatimukset pilvipalveluille.
- Suomessa pilven tietoturvavaatimuksia on lähestytty esim. PITUKRI https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkosivuiltamme-neuvoja-pilvipalveluiden-turvalliseen-kayttoon

CASE

Alkuvuonna 2021 laajamittainen Microsoft Exchange -sähköpostipalvelimien tietomurtoaalto pyyhkäisi myös Suomen yli. Tietomurtoaaltoa tutkittaessa paljastui, että kaikilla pilvipalveluiden käyttöön siirtyneillä organisaatioilla oli edelleen käytössään myös murrettavissa oleva perinteinen Exchange-sähköpostipalvelin. Osalla palvelin oli edelleen jossain marginaalisessa käytössä ja osalla se oli yksinkertaisesti unohdettu sulkea pilvimigraation lopuksi. Kaikkiin palvelimiin kuitenkin murtauduttiin. Tapaus on surullinen esimerkki siitä, kuinka loppumetreillä kesken jäänyt teknologiamuutos jättää ovet auki hyökkääjille.

4. Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

- Organisaatiot ostavat yhä enemmän palveluita ulkoisilta palveluntarjoajilta.
- Organisaatioiden olisi keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä ymmärtää kolmannen osapuolen tietoturvan taso. Esimerkiksi:
  - Konsultit ja heidän oman organisaation sisäiset järjestelmät.
  - Laitteistot ja palvelut joita voidaan käyttää joko osana omaa tuotetta tai palvelukokonaisuutena, tai ostettuna palveluna.
  - Organisaation tulee ymmärtää alihankinnanketju, myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Erityisesti hankintavaiheessa tällaisen tekeminen on oleellista.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos (kyber)turvallisuutta ei ole huomioitu.

CASE

Viime joulukuussa paljastunut Yhdysvaltojen hallintoon ja lukuisiin yrityksiin iskenyt SolarWinds-hyökkäys on merkittävä tietoturvatapaus. Tietomurron ja vakoilun mahdollistanut takaovi onnistuttiin levittämään tuhansiin organisaatioihin, joita oli myös Suomessa. Erilaiset toimitus- ja alihankintaketjut voivat mahdollistaa hyökkääjille keinon päästä huomaamattomammin varsinaiseen kohteeseensa tai saamaan samalla kertaa pääsyn laajaan kohdejoukkoon.

5. Etätyö tuli jäädäkseen – niin myös riskit

Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

- Vuonna 2020 siirryttiin kiireen vilkkaa etätöihin. Osa toimijoista rakensi etätyöjärjestelynsä kiireessä kirjavien viritysten varaan. Näiden väliaikaisten ratkaisujen kuntoon laittamisessa kestää vielä pitkään.
- Laaja siirtymä etätyöhön näkyi maaliskuussa 2020 suojattomien laitteiden määrän selvänä kasvuna Suomen verkoissa. Verkkoon avoimilla laitteilla ja laitteiden suojattomilla etäyhteyspalveluilla tarkoitetaan tässä yhteydessä esimerkiksi avoimia etätyöpöytäyhteyksiä ja tiedostonjakopalveluja (esim. RDP, VNC ja SMB).
- Kesän 2021 jälkeen organisaatioissa ollaan todennäköisesti hybridiratkaisussa, jossa osa tekee töitä etänä ja osa toimistolla. Tässä tulee huomioida myös se, että koronan alussa tehdyt nopeat etätyöratkaisut tarkastellaan ja varmistetaan niiden tietoturvallisuus, jotta tietoturva huomioidaan ja voidaan taata pysyvämmässä mallissa.

CASE

Suojelupoliisin tiedote: Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. Suojelupoliisi on havainnut, että suomalaista infrastruktuuria hyödyntävä kybervakoilu on lisääntynyt. Erityisesti autoritaaristen valtioiden tiedustelupalvelujen kybervakoiluoperaatioissa on käytetty hyväksi kymmeniä suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia liittämällä ne osaksi operaatiossa käytettävää infrastruktuuria.

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.

TRAFICOM

16.9.2021

Tietomurrot ja –vuodot

- Kuukauden aikana on raportoitu useampia murtoja käyttäjätileille kalastelun seurauksena
  - Esimerkiksi tuhansien seuraajien Instagram-tilejä on kaapattu niiden omistajilta.
  - Tilin kaappauksen jälkeen uhrilta on kiristetty rahaa, jotta kaapattu tili palautetaan oikealle omistajalleen.
  - Instagram-tilejä on kaapattu muun muassa lähettämällä väärennetty ”copyright violation” -sähköpostiviesti, jossa oleva linkki johtaa tunnusten kalasteluun.

Analyysi

- Monivaiheisen tunnistautumisen käyttö estäisi monet käyttäjätilien murrot.
- Kalastelun uhka koskee sekä paikallisia että pilviympäristöjä.
- Tilejä on käytetty hyväksi mm. kalastelunviestien lähettämiseen.

Tietomurrot ja –vuodot

- Verkkotunnus vastaamohaku.com rekisteröitiin elokuun loppupuolella
  - Kyseisestä osoitteesta oli tehty osoitteen uudelleenohjaus, joka mahdollisti normaalilla verkkoselaimella TOR-verkossa olevaa sivun katselun. Sivulla avautui Vastaamon tietojen hakuun luotu hakukone.
  - Hakukoneella oli mahdollista hakea Vastaamon julkisuuteen päätyneistä tiedosta tuloksia esimerkiksi nimellä, paikkakunnalla tai postinumerolla.
  - Tiedot eivät ole uusia, vaan kyseessä ovat aiemmin julkisuuteen vuotaneet tiedot.
  - Tietoja voi olla hankala poistaa ja niiden takana olevaa tahoa jäljittää.

Analyysi

- Jos kohtaat varastettuja tietoja verkossa, älä lue, kommentoi tai jaa niitä.
- On todennäköistä, että tiedot ilmestyvät silloin tällöin näkyviin internetiin ja niiden lopullinen poistaminen on mahdotonta.
- Vastaamohaku.com –osoite ajettiin alas jo muutamaa päivää myöhemmin.

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

- Ärhäkkää pankkitunnusten kalastelua
  - Pankkitunnuksia kalasteltiin kaikkien Suomessa toimivien liikepankkien nimissä.
  - Huolellisesti tehtyjä pankkikalastelusivuja nähtiin paljon OP:n ja Nordean kirjautumissivuiksi väärennettyinä.
  - Pankkikalasteluun johtavia huijausviestejä levitettiin tekstiviesteinä tuhatmäärin.
  - Toinen yleisesti nähty huijaustapa oli hakukonetuloksiin ujutetut kalastelusivulinkit.
  - Kaapatuilla pankkitunnuksilla anastettiin elokuussa kymmeniä ja satoja tuhansia euroja.

Analyysi

- Hakukonetulosten väärentäminen on yleistynyt kalastelulinkkien levitystapana.
- Rikollinen syöttää hakukoneisiin linkkejä joko optimointimekanismeilla tai ostamalla hakukoneesta mainostilaa.
- Kun selaimeen syöttää pelkän pankin nimen eikä verkkopankin osoitetta, verkkoselain ohjaa ensin hakukoneeseen. Hakukoneessa oleva väärennetty linkki vie kalastelusivulle, jonka avulla rikollinen saa kaapattua pankkitunnukset.
- Pankkien nimien lisäksi hakukonetuloksia ja mainoksia on myrkytetty julkispalveluiden nimillä, kuten Omakanta.

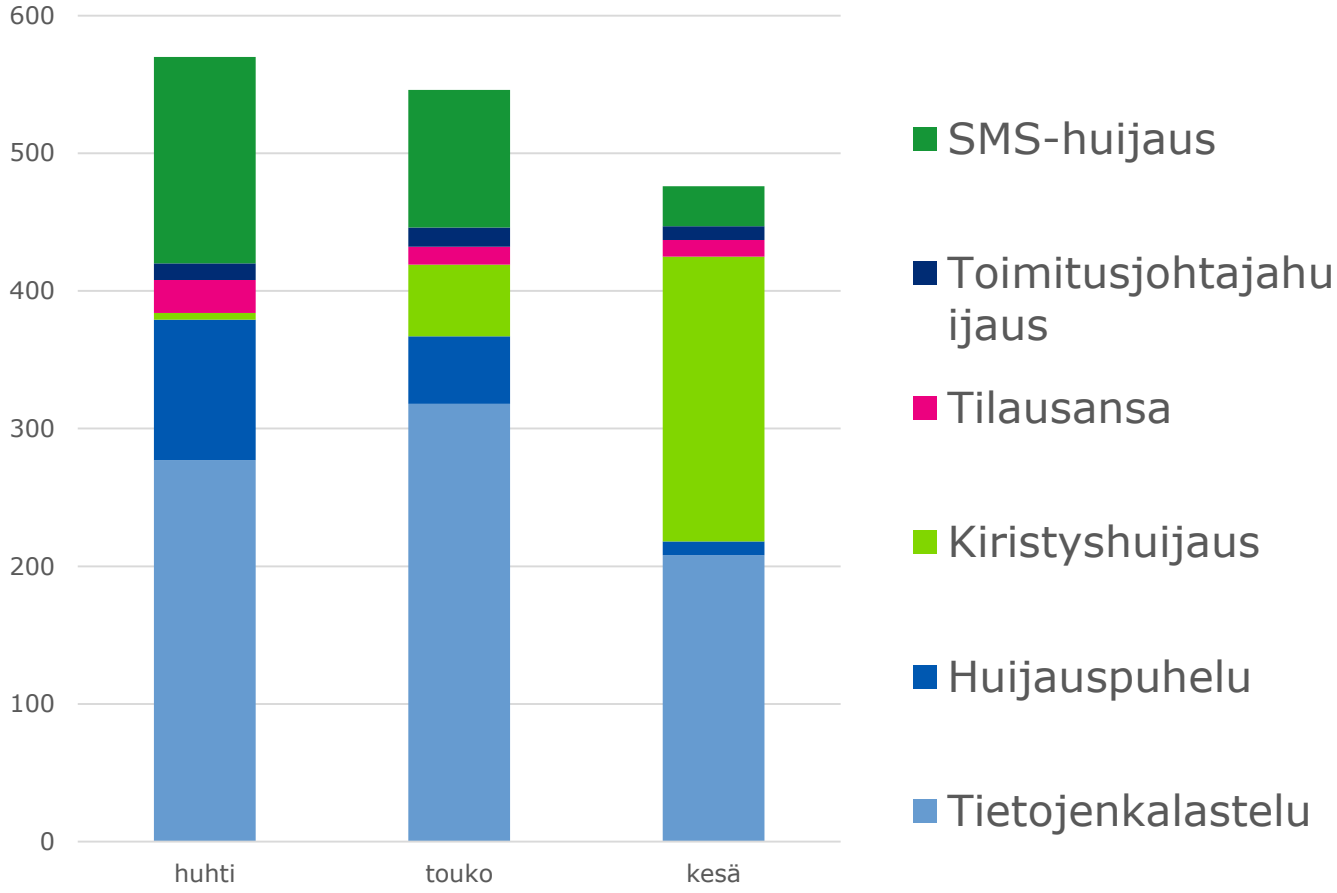
Huijaukset ja kalastelut

- Tunnuskalasteluja operaattoreiden nimissä
  - Elokuussa nähtiin paljon DNA/Welhon nimissä tulleita kalasteluhuijauksia.
  - Sama huijaustapa toistui myöhemmin Elisan kirjautumissivuiksi naamioituneina tunnuskalasteluina.
  - On mahdollista, että pian myös muiden operaattoreiden nimissä voidaan nähdä samanlaista tunnusten kalastelua.

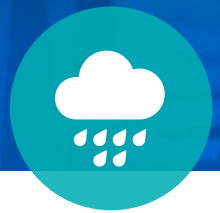
Analyysi

- Oppilaitosten tunnukset kiinnostavat tietojenkalastelijoita
- Useita satoja Oulun yliopiston verkon käyttäjätunnuksia ja salasanoja päätyi tietojen kalastelijalle
- Opiskelijoiden tai henkilökuntaan kuuluvien käyttäjätunnus-salasana-pareja on päätynyt vääriin käsiin 700–800 kappaletta.
- Tietomurtajan huijausviestillä käsiinsä saamia tunnuksia on käytetty lähinnä uusien kalasteluviestien lähettämiseen.
- https://yle.fi/uutiset/3-12083922

Käsiteltyjä huijaustapauksia Q2/2021



- Vuoden toisen neljänneksen 2021 ilmiöitä ovat:
  - Kiristyshuijaukset esiintyivät kausittain aalloissa. Tämä näkyy päivitetyssä tilastossa, jossa kesäkuun pornokiristysaalto, näkyy kiristyshuijausten määrän merkittävässä kasvussa.
  - Pankkikalastelu on toinen, jota esiintyy aalloissa ja erittäin aktiivisesti.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.



Haittaohjelmat ja haavoittuvuudet

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

TRAFICOM

16.9.2021

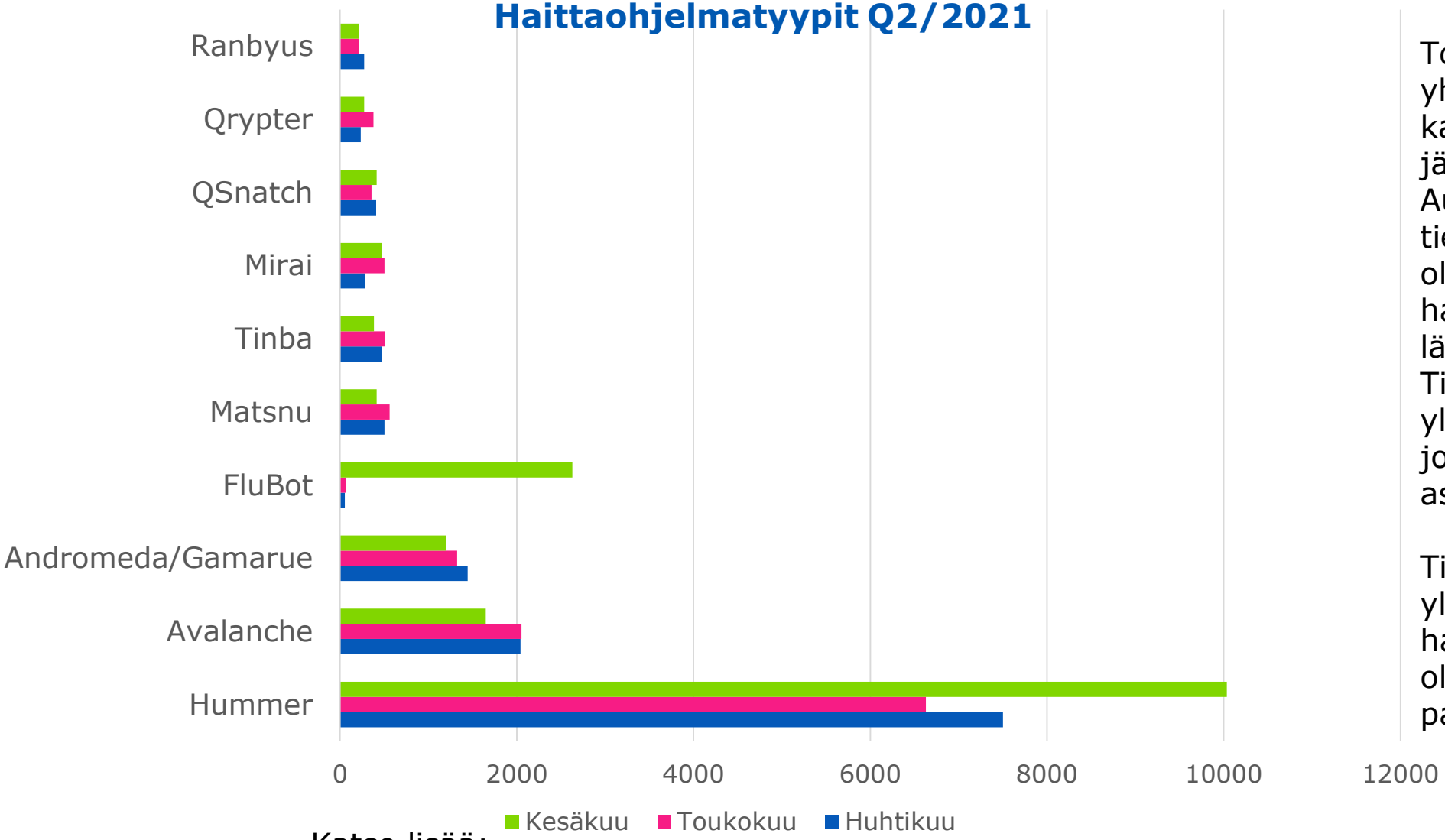
Haittaohjelmat

- Poistimme Android-haittaohjelmia koskevan varoituksen 17.8.
  - Heinäkuussa uudelleen aktivoitunut, erittäin aktiivisena tapahtunut haittaohjelman levityskampanja on nyt rauhoittunut.
  - Ilmoitusmäärät haittaohjelmaa levittävistä tekstiviesteistä ovat laskeneet merkittävästi ja Autoreporter-järjestelmämme havainnot haittaohjelmaliikenteestä vähenevät tasaisesti.
  - FluBot-nimistä Android-haittaohjelmaa levitettiin erittäin aktiivisesti tekstiviestien avulla kesäkuun alkupuolella.

Analyysi

- Varoituksen julkaisun jälkeen saimme haittaohjelman levityksestä enimmillään noin 900 ilmoitusta päivässä.
- Uusien haittaohjelmien levitysyritysten kanssa tulee olla edelleen valppaana.

Autoreporterin haittaohjelmahavainnot



Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Autoreporter-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.

Katso lisää:
https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot

Haavoittuvuus

- PrintNightmare-haavoittuvuuskokonaisuus on edelleen ajankohtainen
  - Microsoft julkaisi 11.8.2021 haavoittuvuuden CVE-2021-36958 joka mahdollistaa käyttövaltuuksien korottamisen paikallisesti haavoittuvuuden avulla.
  - Haavoittuvuuskokonaisuuden kaikille haavoittuvuuksille ei toistaiseksi ole korjausta ja suosituksena on edelleen Print Spooler -palvelun käytöstä poistaminen
  - Päivitimme alkuperäistä haavoittuvuustiedotettamme: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_19/2021

Analyysi

- PrintNightmare nimellä kulkeva haavoittuvuuskokonaisuus on ollut monitahoinen ja tapaukseen liittyy useita eri CVE-tunnuksia.
- Valmistajan viestintää haavoittuvuuskokonaisuudesta kannattaa seurata edelleen aktiivisesti.

Kuukauden haavoittuvuusjulkaisut

- Nokia 8 Sirocco-puhelimista korjattu WPA/WPA2 Enterprise-verkoissa esiintyvä haavoittuvuus (23/2021)
- Kriittinen haavoittuvuus sulautettujen järjestelmien käyttöjärjestelmässä (24/2021)
- Atlassian Confluence-tuotteen haavoittuvuutta hyväksikäytetään aktiivisesti (25/2021)
  - Haavoittuvuuden kriittisyysluokitusta nostettiin toimittajan taholta julkaisun jälkeen.
  - Kyberturvallisuuskeskus on yrittänyt ottaa yhdessä operaattoreiden kanssa yhteyttä tahoihin, joilla on haavoittuva versio vielä käytössä.
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Analyysi

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

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

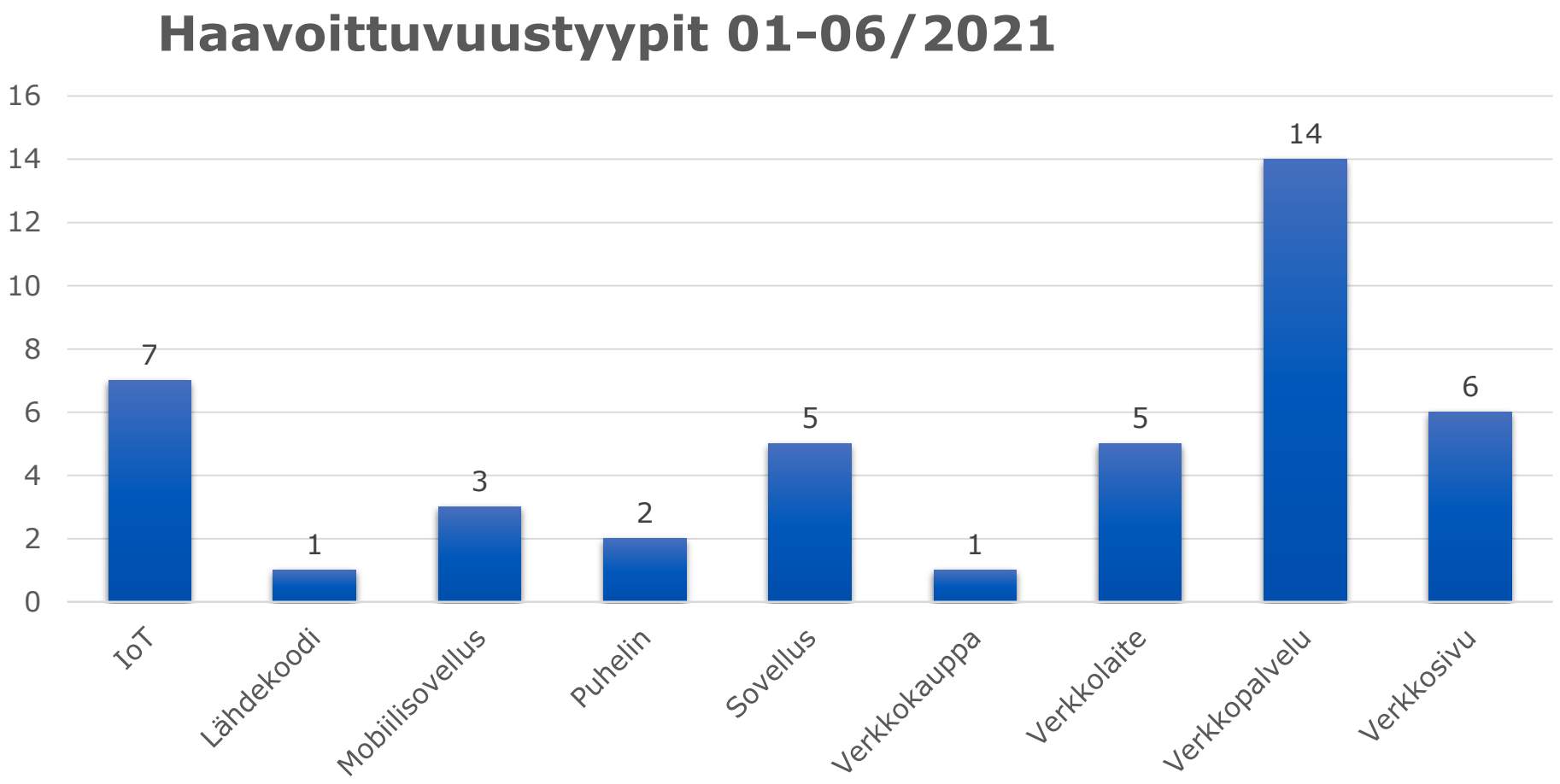
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta
- **Haavoittuvuustiedotteita tänä vuonna 27 kpl (tilanne 14.9.2021)**
  - 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 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

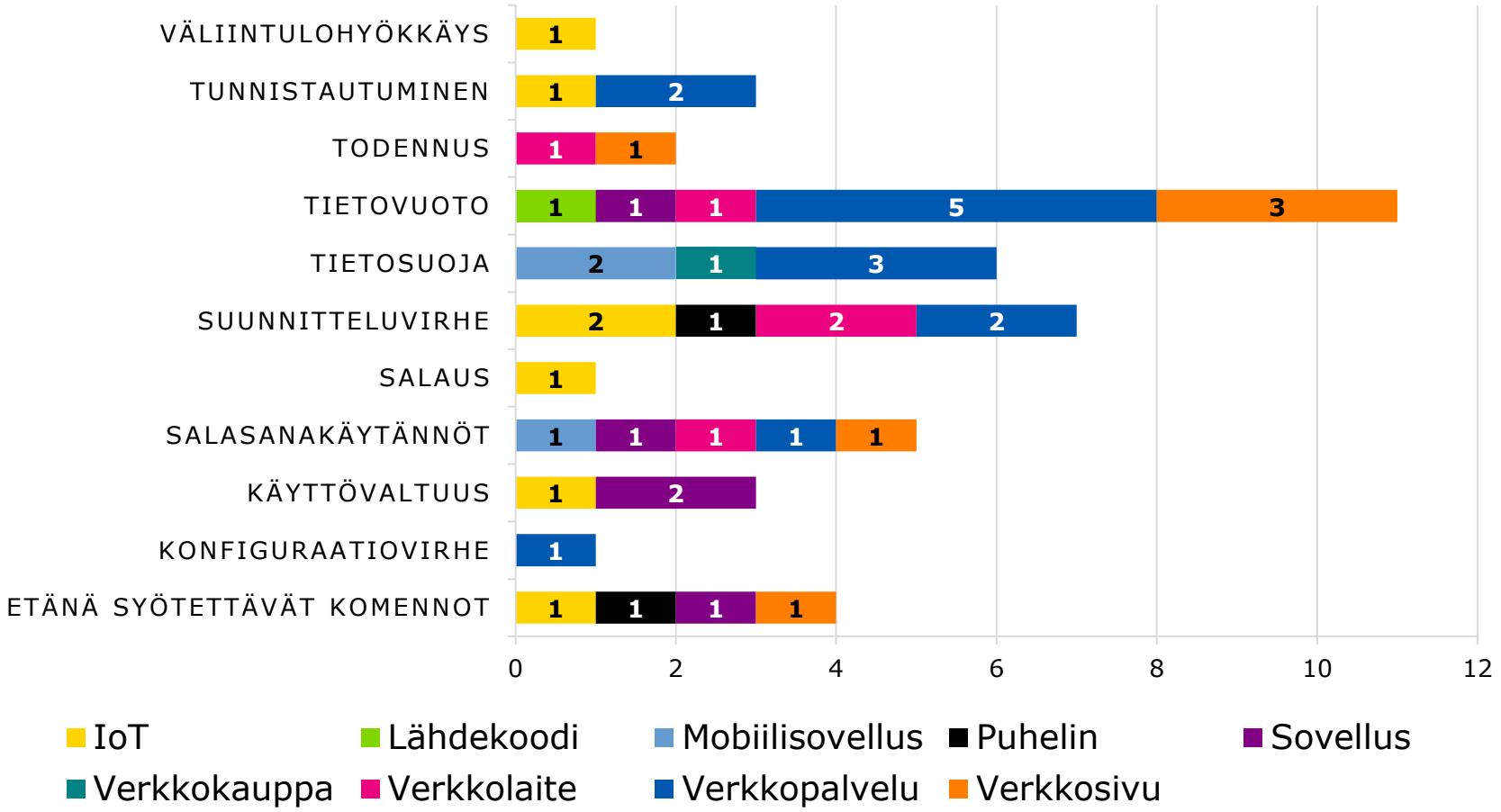
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat 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

6kk



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Tutustu aiheeseen tarkemmin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

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

- DDoS-hyökkäyksiä tekevä rikollisryhmä otti mielenkiinnon kohteekseen Realtekin haavoittuvia siruja käyttäviä laitteita
  - Näitä laitteita raportoitiin olleen satoja tuhansia.
  - Haavoittuvien laitteiden etsiminen ja hyväksikäyttöyritykset alkoivat pian sen jälkeen, kun haavoittuvuudet kuvaava raportti oli julkaistu.
  - https://therecord.media/hundreds-of-thousands-of-realtek-based-devices-under-attack-from-iot-botnet/

Analyysi

Päivityksen tarjoamisen ja haavoittuvuuden julkistamisen välille on hyvä jättää riittävästi aikaa, jotta päivitykset saadaan asennettua riittävän laajasti ennen kuin haavoittuvuuksia aletaan väärinkäyttää.

Automaatio – NicheStack

- NicheStack-TCP/IP-toteutuksesta löytyi 14 haavoittuvuutta, jotka saivat nimen INFRA:HALT.
- NicheStack-toteutus on käytössä etenkin sulautetuissa järjestelmissä, esimerkiksi teollisuusautomaatiolaitteissa ja kriittisessäkin infrastruktuurissa.
- Forescoutin ja kumppanien Project Memoria on tuottanut haavoittuvuusraportteja jo aiemmin.
- Edelliset vuoden sisällä julkaistut haavoittuvuusjoukot saivat nimekseen AMNESIA:33, NUMBER:JACK, NAME:WRECK ja nyt INFRA:HALT.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_22/2021

Automaatio – Bad Alloc

- BadAlloc-haavoittuvuus koskee monia reaaliaikakäyttöjärjestelmiä. BlackBerryn QNX-reaaliaikakäyttöjärjestelmän tiettyjen versioiden todettiin olevan alttiita BadAlloc-haavoittuvuudelle.
- BadAlloc-haavoittuvuuskokonaisuuden avulla on mahdollista suorittaa etäkomentoja verkossa oleviin laitteisiin.
- Haavoittuvuuden vaikutukset ovat tuotekohtaisia. Tyypillisin vaikutus on se, että sopivan haitallista syötettä lähettämällä laitteen toiminta voi estyä, eli voi syntyä palvelunestotila. Silloin laite ei kykene valvomaan tai ohjaamaan vastuullaan olevaa prosessia.
- BadAlloc-haavoittuvuus koskee monia muitakin reaaliaikakäyttöjärjestelmiä kuin QNX:ää.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_24/2021

IoT-haavoittuvuuksien hallinta

- Tunne ympäristösi ja tunnista haavoittuvat laitteet/järjestelmät
- Arvioi haavoittuvan järjestelmän vaikutukset ja riskit riittävän hyvin ennen kuin teet suojaustoimenpiteitä
- Selvitä ja listaa haavoittuvat järjestelmät. Varmista järjestelmätoimittajilta, että haavoittuvuudet korjataan tai päivitä laite itse, mikäli se on mahdollista.
- Poista turhat portit, palvelut ja verkkorajapinnat käytöstä (BadAlloc: kuten DNSv4 client tai HTTP-palvelin)
- Estä DNSv4-liikenne, ellei sitä tarvita (BadAlloc)
- Eristä ja eriytä verkot toisistaan, varmista ettei haavoittuvaan laitteeseen ole suoraa pääsyä julkisesta verkosta
- Käytä hyväksyttyjä listoja (BadAlloc: esim. HTTP-yhteyksien suhteen)
- Jos järjestelmää on voitava käyttää etänä, tee tämä turvallisesti esim. VPN:n kautta. Pidä myös VPN-ratkaisut päivitettynä.
- Monitoroi ja estä haitallinen liikenne (BadAlloc: kuten haitalliset IPv4/TCP ja ICMPv4 -paketit)
- Tee laitteille mahdollisuuksien mukaan haavoittuvuusskannaus ja monitoroi normaalia tarkemmin liikennettä haavoittuviin laitteisiin
- Jos mahdollista, aseta laitteissa ASLR päälle, jotta järjestelmän osoiteavaruus muuttuisi hyökkääjälle tuntemattomaksi (NicheStack)

IoT

- ETSI (European Telecommunications Standards Institute) julkaisi IoT-kuluttajalaitteiden tietoturvan arvioimista käsittelevän teknisen spesifikaation ETSI TS 103 701 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
  - Tekninen spesifikaatio on ladattavissa osoitteesta: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
  - Spesifikaatio tukee aiemmin ilmestyneen standardin ETSI EN 303645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements soveltamista määrittelemällä menetelmiä vaatimustenmukaisuuden arviointiin.
  - Sekä Traficomin Tietoturvamerkki että Singaporen kyberturvallisuusviranomaisen CSA:n IoT-kuluttajatuotteiden tietoturvan sertifiointiohjelma nojaavat standardiin.

Analyysi

- IoT-tuotteiden tietoturvan virallinen standardointityö etenee antaen valmistajille välineitä tietoturvan varmistamiseen.
- Standardit mahdollistavat tietoturvatason parantamisen ja auttavat valmistautumaan myös tulevaisuuden pakottavaan sääntelyyn.

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

- Elokuussa yleisissä viestintäpalveluissa oli neljä merkittävää toimivuushäiriötä. Häiriöiden kohteet ja syyt olivat kaikki erilaisia.
  - Vakavuusluokat: A: 0, B: 2, C: 2
- Muissa ICT-palveluissa ei elokuun aikana ollut uutiskynnystä ylittäneitä toimivuushäiriöitä.

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa on vuonna 2021 ollut keskimäärin hyvä.
- Kuukaudessa on keskimäärin vajaat kuusi merkittävää toimivuushäiriötä.
- Elokuu oli hellävarainen pilvipalveluille. Viime aikoina jossakin suurista pilvipalveluista on ollut häiriö vähintään kerran kuukaudessa.

Palvelunestohyökkäykset

- Elokuussa Kyberturvallisuuskeskukselle raportoitiin muutamia palvelunestohyökkäyksiä. Useimmat hyökkäyksistä ovat pieniä ja lyhytkestoisia.
- Julkishallinnon palveluun osuu ajoittain palvelunestohyökkäyksiä, mutta ne saadaan pääsääntöisesti torjuttua tehokkaalla pakettipesuripalvelulla. Myös elokuussa näin on tapahtunut useita kertoja.
- Atlassian Confluence -palvelimien uusimmasta haavoittuvuudesta seurasi useita tietomurtoja suomalaisillekin palvelimille. Osaa näistä murretuista palvelimista käytettiin myös palvelunestohyökkäyksen välikappaleena.
- Noin 25% hyökkäyksistä (Q2/2021) Suomessa oli kooltaan yli 1 Gbit/s. Ilmoitettujen hyökkäysten perusteella skaala ulottuu jopa 260 Gbit/s tasolle asti.

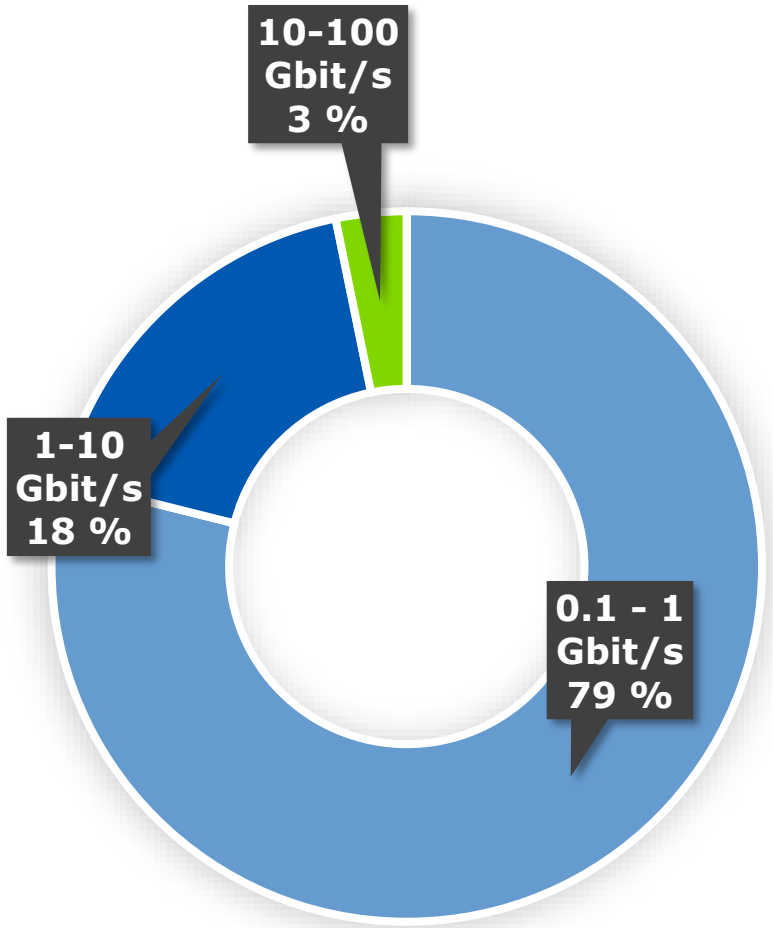
Analyysi

- Syksyn tulon huomaa myös hyökkäysten aktivoitumisesta oppimispalveluita ja opintohallintojärjestelmiä kohtaan.
- Koululaisille ja muille hakkeroinnin alkeisiin tutustuville kannattaa muistuttaa, että tietoverkkojen häirintä on laitonta ja siitä koituvista rikosoikeudellisista seuraamuksista aiheutuu paljon harmia myöhemmässä elämässä.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 260 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2/2021.
- Noin 72% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(q2/2021 - tilasto päivitetään kvartaaleittain.)

TRAFICOM

Vakoilu

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

Vakoilu

- Keväällä nähdyn kohdistetun kalastelukampanjan kohteista saatiin lisätietoja, kun tietoturvayhtiö ESET kertoi operaation näkyneen ainakin Slovakiassa ja todennäköisesti myös Tsekeissä.
  - APT29 toteuttamaksi epäillyssä kampanjassa uhriorganisaatioihin tunkeuduttiin hyödyntäen kohdistettua kalastelua tai Cobalt Strike -haittaohjelman asentavaa haitallista sähköpostiviestin liitetiedostoa.
  - Slovakiaan kohdistettuja viestejä lähetettiin Slovakian NSA:n nimissä. Lisäksi ESET:n tutkijat löysivät muita Slovakiaan kohdistettuja haitallisia tiedostoja läheisesti muistuttavia viestejä, joista ainakin yksi viittasi siihen, että operaatio oli kohdistunut myös Tsekkeihin.
- Aiemmin on kerrottu kampanjan näkyneen ainakin 13 Euroopan maassa.

Analyysi

- APT29 tunnetaan myös mm. nimillä The Dukes ja Cozy Bear. Julkisissa lähteissä sen on arvioitu linkittyvän Venäjän tiedustelupalveluun SVR:hen.
- Kampanja oli käynnissä tiettävästi ainakin helmikuusta heinäkuuhun.

Vakoilu

- Kiinalaistoimijat pyrkivät vuosien ajan tunkeutumaan teleoperaattoreiden järjestelmiin hyödyntäen vastaavia menetelmiä kuin keväällä nähty Hafnium-operaatio, kertoo tietoturvayhtiö Cybereason.
  - Hafnium-operaatiossa hyödynnettiin Microsoft Exchange -sähköpostipalvelun nollapäivähaavoittuvuuksia.
- Cybereasonin analysoiman kampanjan kohdeorganisaatiot ovat olleet Itä-Aasiassa toimivia teleoperaattoreita.
  - Cybereason arvioi, että hyökkääjien tavoitteena on ollut saada jalansija ja pitkäaikainen pääsy kohteena olleiden teleoperaattoreiden järjestelmiin. Tavoitteena on ollut kerätä tietoa muun muassa puhelutiedoista.
- Cyberasonin mukaan on tunnistettavissa ainakin kolme toisistaan eroavaa, mutta osin samoja menetelmiä hyödyntänyttä toimijaryhmää (nk. Soft Cell, Naikon APT ja Emissary Panda eli APT27). Yhtiö kutsuu kokonaisuutta nimellä Deadringer.

Analyysi

- APT-toimijoilla on kyvykkyys ottaa nopeasti mukaan keinovalikoimaansa uusia paljastuvia nollapäivähaavoittuvuuksia. Esimerkiksi Microsoft Exchangesta paljastuvat haavoittuvuudet ovat hyökkääjille kiinnostavia.

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

- Traficom antanut uutta ohjeistusta evästeiden käyttöön liittyen.
- Evästeohjeistuksen tarkoituksena selventää evästeiden käyttöön ja suostumuksen pyytämiseen liittyviä oikeudellisia reunaehtoja.
  - Selainasetusten kautta ei ole mahdollista antaa pätevää suostumusta evästeiden käytölle.
  - Evästeiden käyttöön tulee pyytää käyttäjän suostumus, ellei eväste ole välttämätön palvelun perustoiminnallisuuden kannalta.
  - Käyttäjälle tulee tarjota mahdollisuus hallinnoida palvelun eri tyyppisiä evästeitä sekä mahdollisuus muuttaa tai peruuttaa antamansa suostumuksen.
- Ks. lisätietoa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/evasteneuvontamme-uusittu

Analyysi

- Uuden evästeohjeistuksen tavoitteena on pyrkiä yhtenäistämään eriäviä evästekäytäntöjä eri palveluissa ja sivustoilla.
- Ohjeistus tarjoaa palveluntarjoajille apua hyvien ja lainmukaisten evästeratkaisujen toteuttamiseen.
- Käyttäjän yksityisyyden suojan kunnioittaminen on keskeisessä roolissa.

Oikeudelliset asiat

- Toisiolain siirtymäaikaa jatketaan vuodella
  - Ks. lisätietoa: https://stm.fi/web/stm/-/toisiolain-siirtymaaikaa-jatketaan-vuodella

- Tietosuojavaltuutetun toimisto tehostaa ETA-maiden ulkopuolelle tehtävien henkilötietojen siirtojen valvontaa
  - Ks. lisätietoa: https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-tehostaa-eta-maiden-ulkopuolelle-tehtavien-henkilotietojen-siirtojen-valvontaa

Arjen kyberturvallisuus

Poistimme Android-haittaohjelmia koskevan varoituksen

- FluBot-nimistä Android-haittaohjelmaa levitettiin erittäin aktiivisesti tekstiviestien avulla kesäkuun alkupuolella.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/poistimme-android-haittaohjelmia-koskevan-varoituksen

Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten eli "pornokiristys" -huijausviestien lähettelyssä. Viestejä on lähetetty viime päivinä runsaasti myös hyvin suomeksi käännettyinä. Ne ovat huijausta, eikä huijareille pidä missään nimessä maksaa lunnaita.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita

Uusi puhelin koululaiselle

- Tietoturvasta huolehtiminen on tärkeä kansalaistaito myös lapsille. Taitojen omaksuminen alkaa heti, kun lapsi saa älylaitteen käteensä, ja kehitys jatkuu läpi elämän.
- Tutustukaa ohjeisiin yhdessä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tekemista-lapsille

Evästeneuvontamme on uusittu

- Olemme julkaisseet uudistettua neuvontaa evästeiden ja muiden palvelun käyttöä kuvaavien tietojen tallentamisesta käyttäjän päätelaitteelle sekä näiden päätelaitteella olevien tietojen käytöstä. Näin tuemme sekä verkkopalvelujen tarjoajia että käyttäjiä evästekäytännöissä ja lainsäädännön soveltamisessa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/evasteneuvontamme-uusittu

Uutisia Kyberturvallisuuskeskuksesta

CERT-FI 20 vuotta: Älä mokaa luottamusta - kybervirkaihmisen oppi numero 1

- Juhlavuotemme muisteloissa palataan vuosiin 2017 ja 2018. Wannacry-haittaohjelma heilutteli verkkoja, ja Lahden kaupungin it-palvelut olivat vaikeuksissa. Aikoja muistelevat nyt Lasse Laukka, Ericssonin tuotetietoturvan operatiivinen johtaja sekä Jarmo Lahtiranta, Insta Digitalin kyberturvallisuusasiantuntija. Virkatöissä tärkeintä on luottamuksen vaaliminen, eikä pidä unohtaa teksti-tv:n sivua 863.
- Lue koko tarina: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-ala-mokaa-luottamusta-kybervirkaihmisen-oppi-numero-1

CERT-FI 20 vuotta: Kyberosaajan virka antaa ja ottaa - joskus voi olla tuumaustupakan paikka

- Nyt muistellaan CERT-aikoja vuosikymmenten kokemuksella. Tietoturvapäivystäjän työ on itsenäistä ja vastuuta on paljon. Vaikka tiukat kybertuulet puhaltaisivat, ammattilaisen on pystyttävä tekemään nopeita ja isojakin päätöksiä. Hyvät stressinhallintataidot ovat tärkeitä. Tällä kertaa tietoturvamuistoihin palaavat Huoltovarmuuskeskuksen varautumispäällikkö Jarna Hartikainen ja tietoturva-asiantuntijat Erika Suortti-Myyry Nixu oyj:stä sekä Sami Orasaari SSVP Finland Oy:stä.
- Lue koko tarina: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-kyberosaajan-virka-antaa-ja-ottaa-joskus-voi-olla-tuumaustupakan

Kyberturvallisuusohjeita eri kohderyhmille

- Tietoturvaosaaminen on tärkeä kansalaistaito, joka koskee sekä aikuisia että lapsia. Olemme koonneet ohjeita sivuillemme, joihin suosittelemme tutustumaan.
- Digitaalinen yhteiskunta tarvitsee yhä enemmän asiantuntijoita, jotka pystyvät tulkitsemaan ajankohtaisia kyberturvallisuuden ilmiöitä ja ratkomaan niihin liittyviä ongelmia. Myös organisaatiot ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä. Ohjeemme on suunnattu myös organisaatioille ja ammattilaisille.
- https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

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