TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 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

Kybersää joulukuu 2021

Tietomurrot ja -vuodot

- Useita ilmoituksia sosiaalisen median tilien kaappaamisesta tai kaappausyrityksistä
- Monivaiheinen tunnistautuminen tulisi ottaa mahdollisuuksien mukaan käyttöön kaikissa sosiaalisen median palveluissa

Huijaukset ja kalastelut

- Myyntipalstat houkuttelevat huijareita.
- Ponnahdusviestit painostavat uudenlaisiin tilausansoihin.
- Erilaiset puhelinhuijaukset ovat lisääntyneet.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen Log4shell-haavoittuvuus Apache Log4j –komponentissa.
- FluBot-kampanjaan liittyen on Suomessa suodatettu miljoonia tekstiviestejä.

IoT ja automaatio

- Iso-Britanniassa on kuluttajien älylaitteita koskeva lakiehdotus, joka pakottaisi poistamaan helpot oletussalasanat ja ilmoittamaan tietoturvapäivitysten saatavuudesta myynnin jälkeen
- Tutkijat ovat selvittäneet kyberansoilla motivaatiota hyökätä IoT-laitteisiin

Verkkojen toimivuus

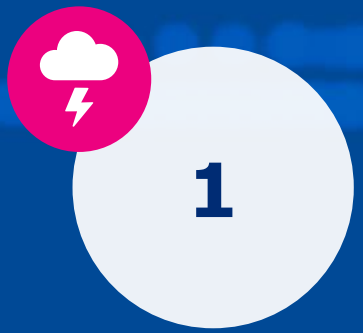
- Marraskuussa yleisissä viestintäpalveluissa oli 4 merkittävää toimivuushäiriötä.
- AWS-palveluissa häiriöitä.
- Palvelunestohyökkäykset vaikuttivat mm. ICT-palveluntarjoajiin.

Vakoilu

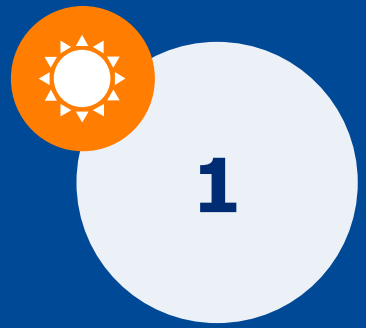
- Microsoft otti haltuunsa NICKEL-toimijan käyttämiä verkkosivuja ja heikensi näin 29 maahan kohdistunutta vakoiluoperaatiota.
- Mobiililaitteiden vakoilu nousi jälleen otsikoihin.
- APT31 on hyödyntänyt murrettuja pienreitittimiä haitallisen liikenteen reitittämiseen.

Kuukauden tunnuslukuja

FluBot-mobiilihaittaohjelma vaivaa edelleen suomalaisia. Operaattoreiden tekemät torjuntatoimet ovat kuitenkin vähentäneet viestien määrää.



Log4shell-nimellä tunnettu ohjelmistohaavoittuvuus on erittäin vakava. Haavoittuvuus koskee log4j-ohjelmistoa, joka on laajasti käytössä ICT-ympäristöissä ja pilvipalveluissa ja riski kohdistuu siksi suomessa suureen määrään organisaatioita.



Traficom on antanut koronatodistuksen lukijalle tietoturvamerkin. Koronatodistuksen lukijalla luetaan EU:n koronatodistus. Suomessa koronapassina toimii EU:n koronatodistus, joka on saatavilla Omakannasta. Koronatodistuksen lukijalla luetaan todistuksen QR-koodi, jolloin ruudulle tulee hyväksytty tai hylätty merkintä.

Julkaisimme varoituksen 4/2021 Varo tekstiviestitse levitettävää haittaohjelmaa

- Julkaisimme keltaisen varoituksen 25.11.2021.
- Tekstiviestitse leviävä FluBot-haittaohjelmakampanja on edelleen aktiivinen.
- Ilmoitusmäärät levitysyrityksistä ovat laskeneet joulukuussa merkittävästi kertoo operaattoreiden antamat tiedot sekä ilmoitusten vähäinen määrä, joita Kyberturvallisuuskeskukselle on tullut.
- Haittaohjelma voi varastaa tietoja laitteelta ja lähettää laitteesta haittaohjelmaa levittäviä huijaustekstiviestejä.
- Aiemmilla kerroilla haittaohjelma pyrki lähettämään tuhansia viestejä uusille uhreille. Operaattorit kertovat suodattaneensa miljoonia tekstiviestejä, joiden kautta on yritetty levittää haittaohjelmaa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/varo-tekstiviestitse-levitettavaa-haittaohjelmaa

Julkaisimme punaisen varoituksen 5/2021 Log4j-komponentin haavoittuvuus on aktiivisen hyväksikäytön kohteena - päivitä välittömästi!

- Julkaisimme keltaisen varoituksen 10.12.2021. Varoitus muutettiin punaiseksi 13.12.2021, sillä ylläpitäjiltä vaaditaan nopeaa reagointia.
- Internetpalveluissa erittäin laajasti käytetyn, haavoittuvan Log4j-komponentin hyväksikäyttötapauksia havaitaan jatkuvasti lisää.
- Julkisten tietojen perusteella haavoittuvuus on koskenut isoa osaa internetin palveluita. Tarkennamme haavoittuvuustiedotettamme, kun lisätietoja julkaistaan.
- Kyberturvallisuuskeskus tiedotti haavoittuvuudesta 13.12. pidetyssä videoneuvottelussa, jonka tallenteen voi katsoa rajoitetun ajan täältä: https://youtu.be/wDp3BBuEChw
- Lue lisää:
  - https://www.kyberturvallisuuskeskus.fi/fi/varoitus_5/2021
  - https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_38/2021

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

Käyttäjätunnukset ovat organisaation arvokasta tietoa Käyttäjätunnusten kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle.

3

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

Symbolit

Uusi

Päivitetty

4

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

5

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

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

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.

2. Käyttäjätunnukset ovat organisaation arvokasta tietoa

Käyttäjätunnusten 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 organisaatioihin kuin yksityishenkilöihin. Se on helppoa ja yksinkertaista, jolla saadaan merkittävää hyötyä.
- Tunnuksia pyritään myös arvaamaan koneellisesti (password spray tai brute force) tai hyödyntämään erilaisia salansanatietovuotoja.
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi kaksi- tai monivaiheinen tunnistautuminen on käytössä.
- Tunnusten ja oikeuksien käytöstä tulee kertyä riittävän tarkkaa lokia, jota analysoidaan poikkeamien varalta. Lokien tulee olla myös riittävän pitkään (esim. 6kk) käytössä jälkikäteen tehtävän selvittelyn vuoksi.

CASE

Microsoftin mukaan valtion tukemat hakkeriryhmät tavoittelevat käyttäjien salasanoja ja tunnuksia hyödyntäen nk. password spray menetelmää. Se on hyökkääjälle tehokas ja vähän resurssia vaativa keino. Microsoft arvioi, että yli kolmasosa tilien vaarantumisesta on password spary-hyökkäyksiä, vaikka tällaisten hyökkäysten onnistumisprosentti tilien kohdalla on 1 %, elleivät organisaatiot käytä teknisiä kontrolleja, joiden avulla voidaan estää ja havaita tunnusten käyttö. Havaintomme mukaan myös suomalaisiin organisaatioihin kohdistuu password spray-hyökkäyksiä

3. 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.

4. 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.

5. 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.

Tietomurrot ja -vuodot

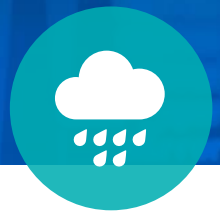
Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

Tietomurrot ja -vuodot

- Sosiaalisen median tilejä on kaapattu.
  - Kyberturvallisuuskeskukseen on ilmoitettu joulukuun aikana kymmeniä tapauksia, joissa sosiaalisen median tili on murrettu.
  - Ilmoituksia on tehty eniten Facebook- ja Instagram-tilimurroista.
  - Facebookin Messenger-sovellusta on myös hyödynnetty kalastelussa, jonka onnistuessa tili on kaapattu rikollisten haltuun.
  - Yksittäisiä ilmoituksia on myös LinkedIn-murroista sekä eri sosiaalisen median tilien nimissä tapahtuvasta tunnusten kalastelusta.

Analyysi

- Ota mahdollisuuksien mukaan käyttöön kaksi- tai useampivaiheinen tunnistautuminen (2FA, MFA).
- Yritä ottaa tili takaisin haltuun kyseisen palvelun automaattityökalujen kautta.
- Varo myös väärennettyjä huijausviestejä.
- Monessa palvelussa on automaattisia varoitustoimintoja käytössä salasanojen vaihdoista ja uusista kirjautumisista.
- Ota yhteyttä palvelun ylläpitoon tilin palauttamisprosessin aloittamiseksi, jos automaattityökalut eivät toimi.



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.

Pankkitietojen kalastelut

- Myynti-ilmoitukset houkuttelevat huijareita
  - Tori.fi:n ja Facebookin myynti-ilmoitukset ovat houkutelleet vastauksia huijareilta. Huijarit vastaavat WhatsAppilla tai Messengerillä ja yrittävät urkkia maksukorttitietoja.
  - Huijari sanoo maksavansa kaupat Postin palvelun avulla. Huijarin antama linkki ei kuitenkaan johda Postin sivulle, vaan väärennetylle kalastelusivulle.
- Pankkitunnusten kalastelu jatkuu.
  - Verkkopankkitunnuksia on jälleen kalasteltu huijareiden sähköposti- ja tekstiviesteillä.
  - Viesteissä on linkki pankin tai OmaKanta-palvelun kirjautumissivun näköiseksi väärennettyyn tietojenkalastelusivuun.

Analyysi

- Huijarille on hyötyä myös tyhjästä pankkitilistä. Vaikka luulisi, ettei tyhjän tilin verkkopankkitunnusten menettämisellä ole suurta väliä, siitä voi silti koitua paljon harmia.
- Huijari voi käyttää haltuunsa saamiaan tiliä rahanpesuun. Tilin kautta kuljetetaan rikoksella saatuja varoja.
- Rahanpesuun käytetty muulitili joutuu kiinni jäädessään pankkien mustalle listalle ja tilin omistajalle seuraa menetetystä tilistä hankaluuksia.

Huijaukset ja petokset

- Ponnahdusviestit vievät tilausansaan
  - Uutena riesana on nähty sitkeästi ruutuun pomppivat selaimen ponnahdusviestit, jotka nalkuttavat käyttäjälle jonkin sovelluksen tai käyttöjärjestelmän päivittämisestä tekstiviesti lähettämällä.
  - Käyttäjä painostetaan ponnahdusviesteillä, kunnes hän lähettää vaaditun tekstiviestin.
  - Lähetetty tekstiviesti ei kuitenkaan päivitä mitään, vaan tilaa liittymälle turhan kuukausilaskutettavan palvelun.
- Uhkaavia kiristysviestejä
  - WhatsAppilla on lähetetty uhkaavia kiristysviestejä, jossa uhataan perheenjäsenten kidnappauksella, ellei uhri maksa 1500 euron lunnaita.
  - Uhkaavia viestejä on tullut Meksikon suuntanumerosta suomalaisiin numeroihin.

Analyysi

- Laskutuspetoksia tehdään väärillä verkkotunnuksilla.
- Ns. typosquatting on tapa rekisteröidä huijauskäyttöön verkkotunnus, joka muistuttaa kohdeyrityksen verkkotunnusta. Nopeasti luettuna se voi näyttää samalta kuin alkuperäinen.
- Väärällä verkkotunnuksella lähetetään valelaskuja yrityksen asiakkaille.
- Tunnusta käytetään myös yrityksen omien työntekijöiden harhautukseen esiintymällä yrityksen johtajana, joka maksattaa laskuja huijarin tilille.
- Ns. toimitusjohtajapetoksissa yritetyt petokset voivat olla hyvinkin suuria.

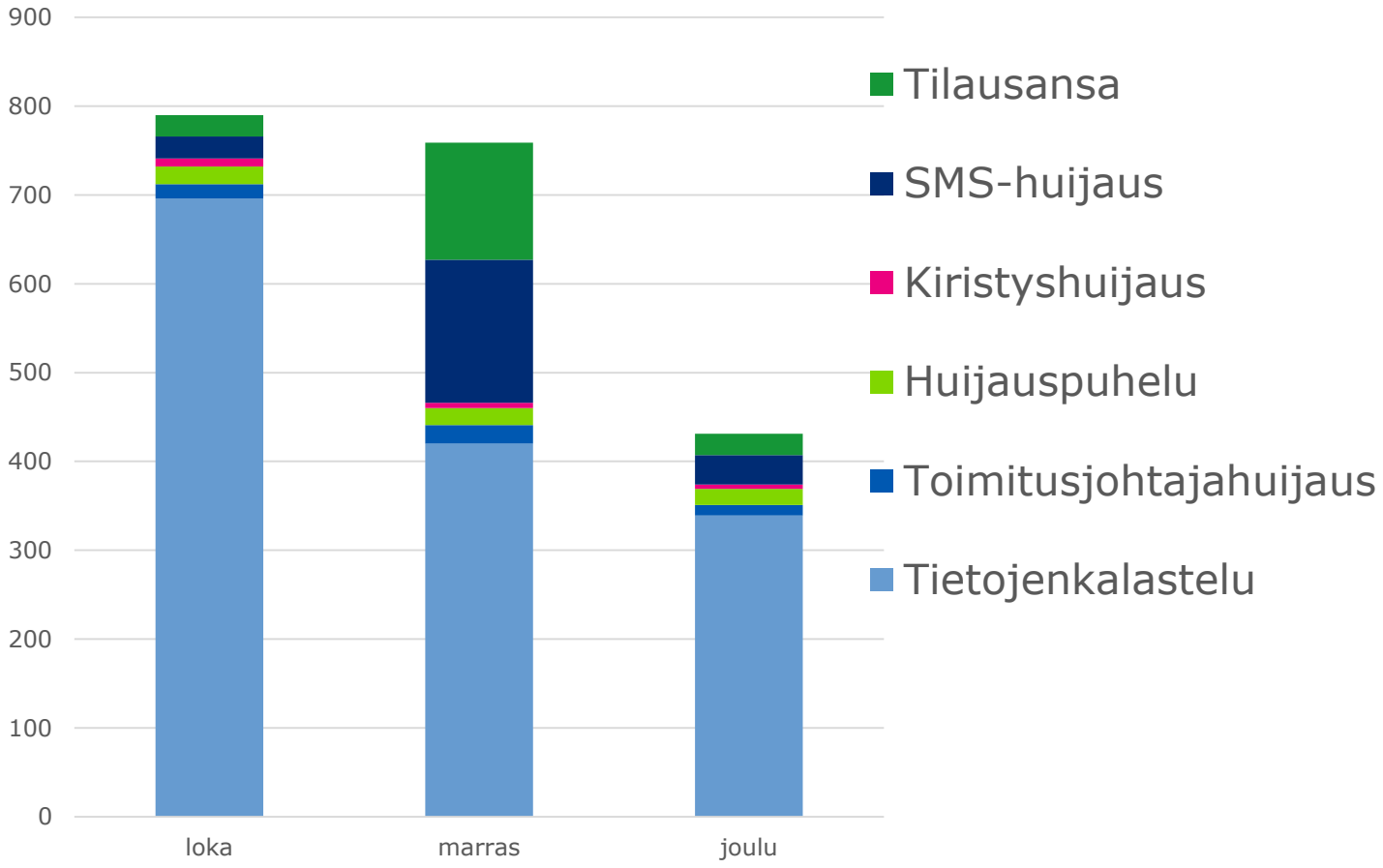
Puhelinhuijaukset

- Huijauspuheluita eri kielillä
  - Nauhoitetuissa huijausviesteissä on esiinnytty poliisina. Suomalaisista matkapuhelinnumeroista on soiteltu huijausviestejä, joissa englanninkielinen ääni väittää soittavansa poliisilaitokselta. Viestit ovat huijausta.
  - Venäjänkielinen huijari on lähestynyt puhelimitse Suomessa asuvia venäjänkielisiä. Puheluissa on esiinnytty eri pankkien edustajana, tarjottu sijoituspalveluita ja kalasteltu pankkitunnuksia.
  - Teknisen tuen huijauksissa on esiinnytty myös operaattorin edustajana.
  - Ulkomaisena poliisiviranomaisena esiintynyt soittaja on koettanut huijata pääsyä tietokoneelle ja verkkopankkiin.
  - Nauhoitetuissa huijaussoitoissa on esiinnytty myös suun terveyden tutkijoina ja kaupiteltu sähköhammasharjoja.

Analyysi

- Robottipuheluista ilmoittaminen on hiljalleen yleistynyt.
- Nauhoitetuissa robottipuheluissa ollaan tekevinään markkinatutkimusta, kyselyä tai muuta vuorovaikutteista yhteydenottoa.
- Numeronäppäimillä annetut vastaukset eivät välttämättä edes vaikuta mihinkään.
- Laki sähköisen viestinnän palveluista (2014/917) kieltää 24 luvun 200 § automatisoitujen puheviestien käytön suoramarkkinointiin ilman asiakkaan ennakkosuostumusta.

Käsiteltyjä huijaustapauksia Q4/2021



- Vuoden 2021 viimeisen neljänneksen ilmiöitä ovat:
  - Haittaohjelman aiheuttamat hujaustekstiviestit näkyivät korostetusti kaikkien operaattoreiden SMS-liikenteessä marraskuusta alkaen.
  - Joulukuun loppua kohti operaattoreiden suodatustoimet saivat huijaus-SMS-viestit kuriin.
  - Pankkitunnusten kalastelu on jatkunut tasaisen laajana koko kvartaalin.

Haittaohjelmat ja haavoittuvuudet

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

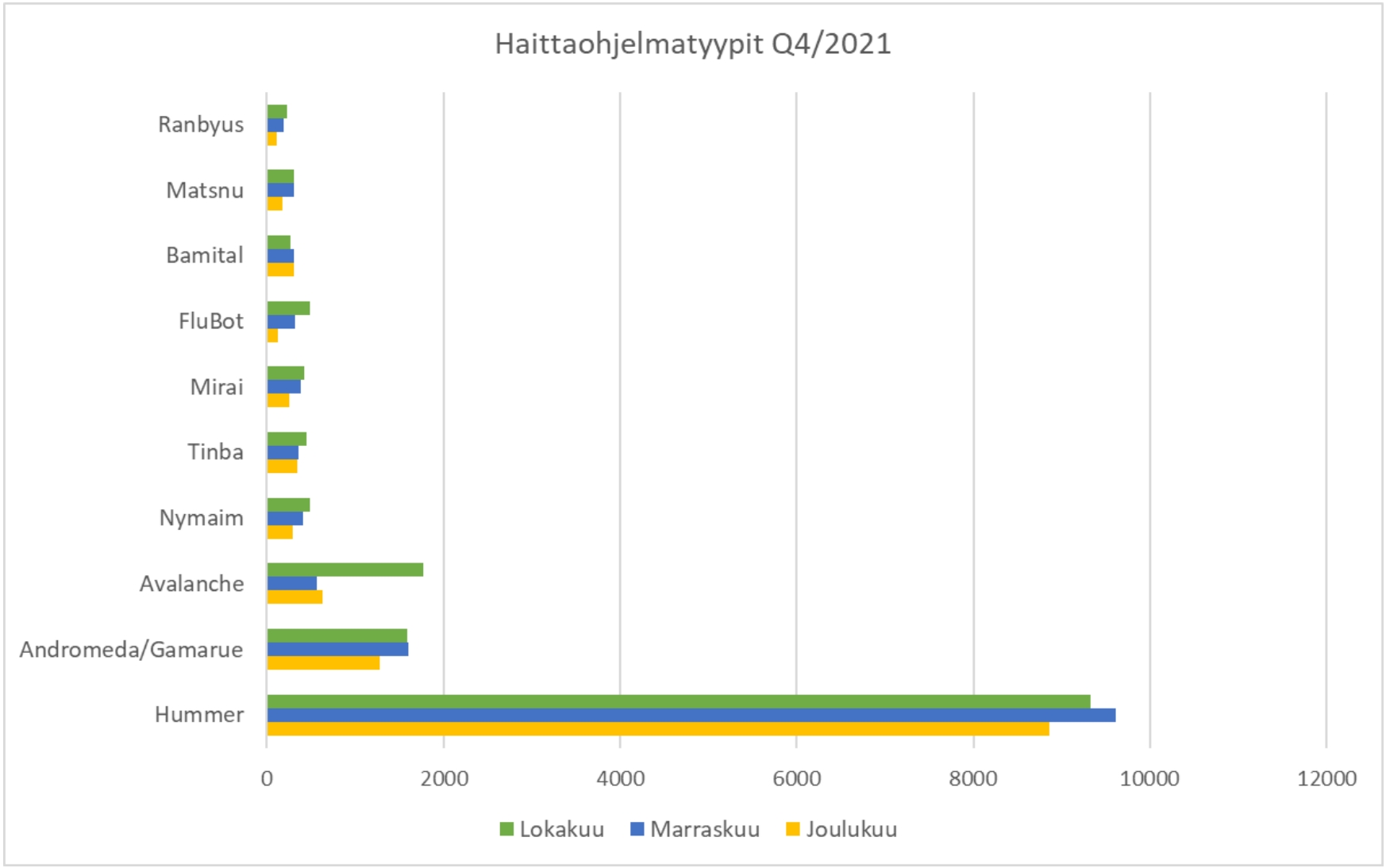
Haittaohjelmat

- FluBot-kampanjaan liittyen on Suomessa suodatettu miljoonia tekstiviestejä
  - Kyberturvallisuuskeskukselle tehtävät ilmoitusmäärät ovat laskeneet tasaisesti.
  - Taustalla on operaattoreiden hyvä suodatuskyky.
  - Kyberturvallisuuskeskukselle on tehty viimeisimmästä FluBot-kampanjasta yli 2200 ilmoitusta 25.11.2021 alkaen.

Analyysi

- Suomessa teleoperaattorit ovat ottaneet käyttöön aktiivisia suodatustoimia, joilla FluBot-haittaliikenteeksi tunnistettuja tekstiviestejä voidaan suodattaa.
- Suodatustoimet ovat tehonneet hyvin ja haittaohjelman aiheuttamat vahingot ovat kääntyneet laskuun.

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. Niistä voi lukea tarkempia tietoja kotisivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

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

Haavoittuvuus

- Kriittinen Log4shell-haavoittuvuus Apache Log4j –komponentissa.
  - Haavoittuvia palveluita skannataan internetissä jatkuvasti, hyväksikäyttöyrityksiä ja tietomurtoja on jo tapahtunut Suomessakin.
  - Kyberturvallisuuskeskukselle on ilmoitettu muutama tietomurto, joissa on asennettu esimerkiksi Kinsing ja Mushtik -haittaohjelmia.
  - Haavoittuvuuden kautta hyökkääjä voi suorittaa haluamaansa Java-koodia Log4j-prosessin oikeuksilla.
- Log4shell haavoittuvuuden hyväksikäyttö on myös valtiollisten toimijoiden keinovalikoimassa.

Analyysi

- Ilmoita Log4Shell-havainnoista Kyberturvallisuuskeskukselle
- Uusimmat tiedot päivitämme 10.12.2021 julkaistuun haavoittuvuustiedotteeseemme
  - https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_38/2021
- Kyberturvallisuuskeskus suosittelee päivitystä versioon log4j-2.17.1.

Joulukuun haavoittuvuusjulkaisut

- Vuoden 2021 aikana julkaisimme 38 haavoittuvuustiedotetta.
  - Joulukuussa julkaistut tiedotteet olivat osa marraskuun Kybersäätä.

- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

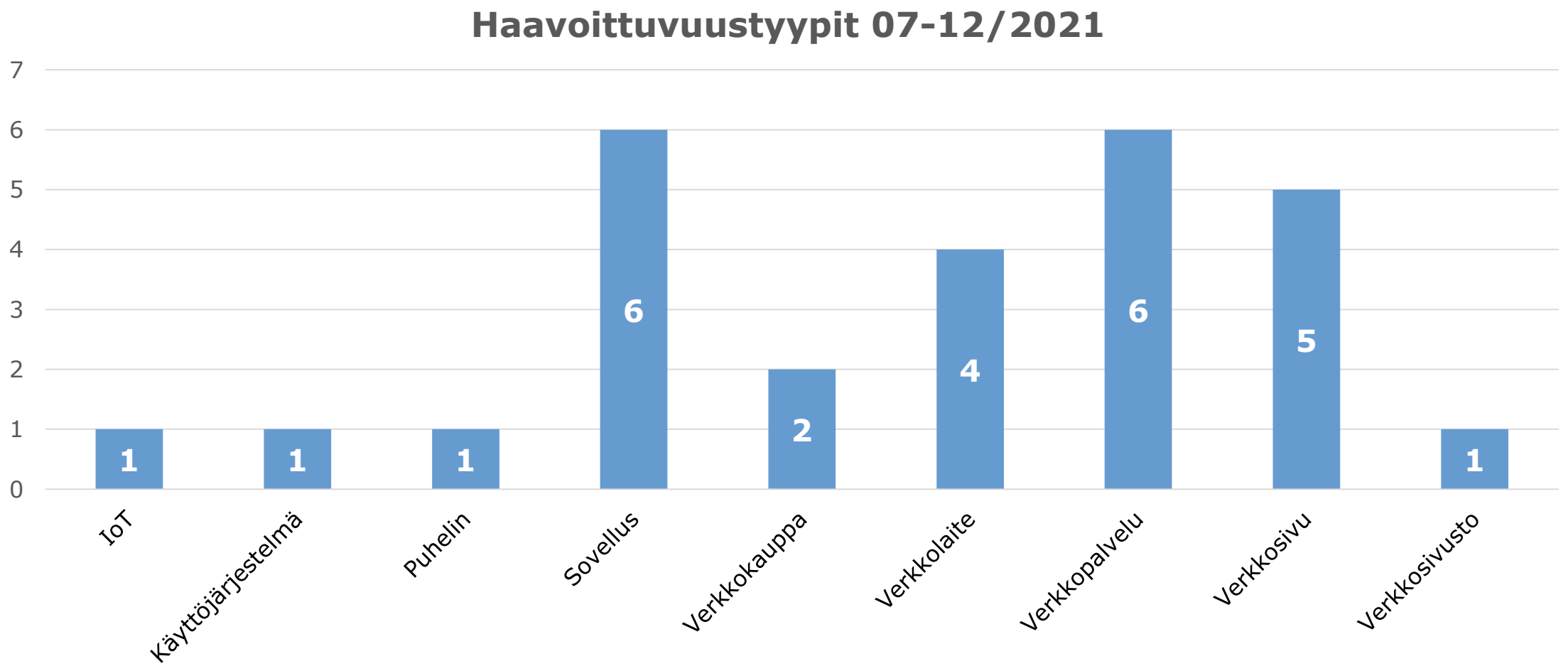
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 38 kpl (tilanne 31.12.2021)**
  - 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

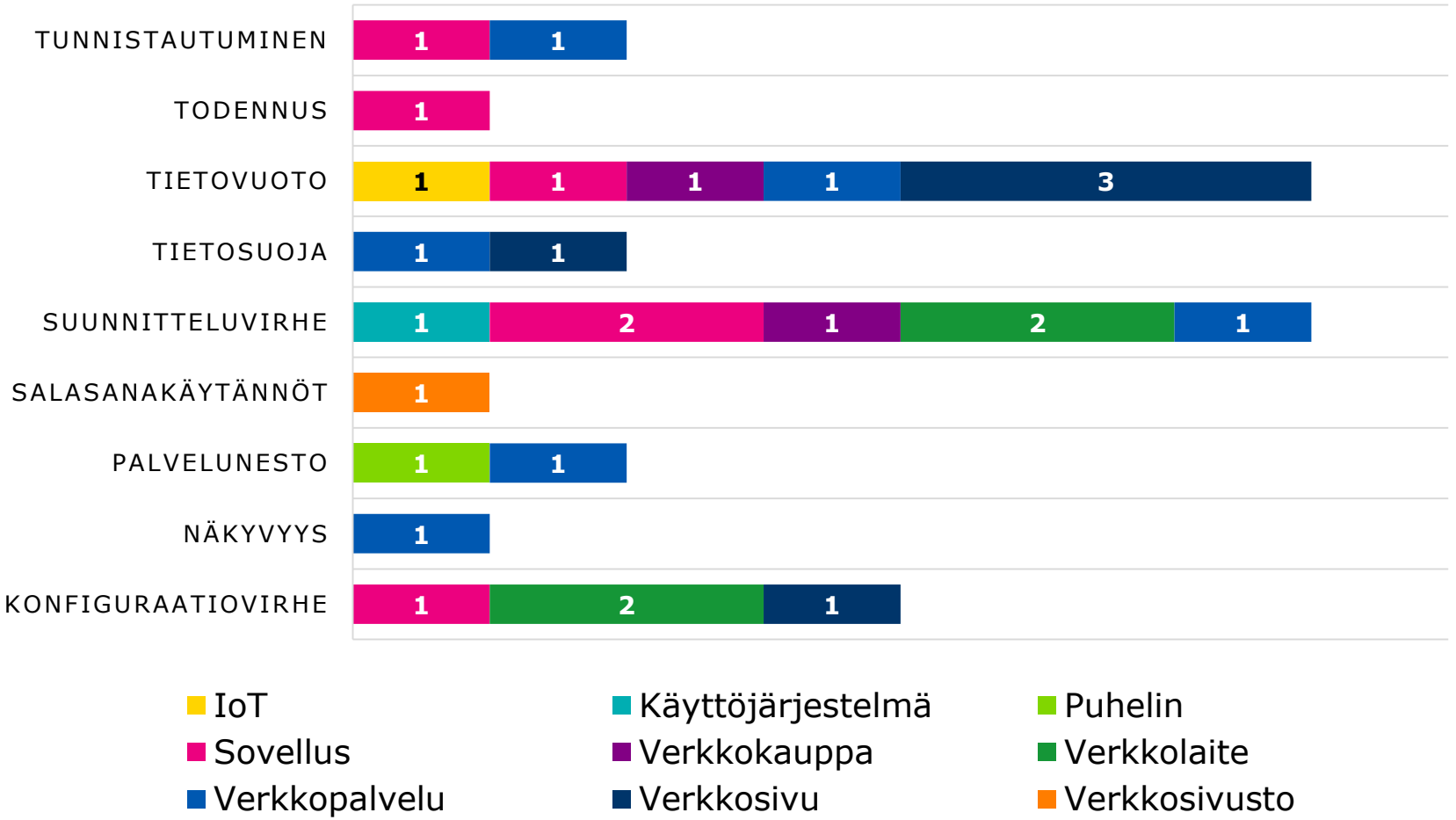
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat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

Automaatio ja IoT

- Yhdysvaltalaistutkijat ovat selvittäneet IoT-laitteisiin hyökkäävien motiiveja.
  - Kolmivuotisessa tutkimuksessa rakennettiin laaja ympäristö, jossa kyberansat naamioitiin tavallisiksi IoT-kuluttajatuotteiksi. Osumia ansoihin tuli tutkimuksen aikana yli 22 miljoonaa.
  - Kyberansat määriteltiin poikkeuksellisesti vastaamaan hyökkääjien toimenpiteisiin. Näin saatiin tietoa hyökkääjien tavoitteista.
  - Valtaosa hyökkääjistä pyrki keräämään tietoa kohteen laitekokoonpanosta tai saamaan käyttöoikeudet laitteeseen kokeilemalla tavallisia käyttäjätunnus-salasana-yhdistelmiä.
  - Kaapatut laitteet valjastettiin pääasiassa kybervaluuttojen louhintaan ja osaksi bottiverkkoa palvelunestohyökkäyksissä.
  - https://www.bleepingcomputer.com/news/security/honeypot-experiment-reveals-what-hackers-want-from-iot-devices/

Analyysi

- Vaikka hyökkääjiä oli paljon, heidän toimintatapansa olivat keskenään hyvin samankaltaisia. Valtaosa käyttää vain automatisoituja yleisesti tunnettuja hyökkäysmenetelmiä.
- Hyvin tunnetut suojautumiskeinot ovat siis tehokkaita:
  - Vaihda oletussalasanat yksilöllisiin ja asenna uudet turvapäivitykset heti.
  - Pidä IoT-laitteet omassa verkossaan erillään kriittisistä kohteista.
  - Tarkkaile IoT-laitteitasi aktiivisesti hyökkäyksien varalta.

Automaatio ja IoT

- Iso-Britanniassa on valmisteltu järeää lakiehdotusta älylaitteiden tietoturvasta.
  - Tuoteturvaa ja televiestintäinfrastruktuuria koskeva sääntely mahdollistaa jopa 10 miljoonan punnan tai liikevaihdosta 4 prosentin suuruisen sakon antamisen.
  - Laki kieltää helposti arvattavat oletussalasanat laitteissa. Myöskään laitteiden oletusasetusten palautus ei saa asettaa laitteeseen heikkoa salasanaa.
  - Kuluttajille pitää kertoa ostohetkellä, kuinka pitkään tietoturvapäivityksiä on saatavilla.
  - Lisäksi tietoturvatutkijoille pitää ilmoittaa yhteyspiste, johon löydetyistä haavoittuvuuksista voidaan ilmoittaa.
  - https://www.bbc.com/news/technology-59400762

Analyysi

- Kuluttajatuotteiden tietoturva on muuttumassa laatutekijästä pakolliseksi ominaisuudeksi, joka on edellytys markkinoilla pysymiselle.
- Iso-Britannian säädös heijastaa voimakkaasti kansainvälisesti jaettua näkemystä siitä, että vahvat salasanat, tietoturvapäivitykset ja haavoittuvuuksien hallinta muodostavat kivijalan älylaitteiden tietoturvalle.

Automaatio ja IoT

- Saksassa useiden rakennusten kiinteistöautomaatiojärjestelmät päätyivät rikollisen hallintaan.
  - https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems
- KNX-teknologialla toteutetut kohteet olivat tavoitettavissa internetistä, eikä niihin ei ollut muistettu asettaa ollenkaan luvattomat muutokset estävää salasanaa.
- Vasta apuun palkattu tietoturvayritys sai murrettua hyökkääjän asettaman salasanan sekä palautettua kiinteistöjen järjestelmät niiden oikean omistajan haltuun.

Analyysi

- Tapaus on hyvä esimerkki siitä, että hyödynnettävät teknologiat tulee tuntea ja niiden käyttöönoton yhteydessä on aina muistettava huolehtia myös tietoturvasta.
- Tämän hyökkäystavan yleistyminen riippuu siitä, voiko hyökkääjä saada sillä uhrilta rahaa. Vaikka hyökkäystapa jäisi erikoisuudeksi, tällaisen hyökkäyksen toteutuminen esimerkiksi maanalaisissa tiloissa voi olla yksittäiselle uhrille vakavaa.

Automaatio ja IoT

- Kuluttajien älylaitteissa on havaittu käyttäjän ja tämän läheisten yksityisyyden vaarantavia puutteita.
  - Fisher-Pricen aikuisille tarkoitettu nostalgialelupuhelin muodostaa turvattoman bluetooth-yhteyden mihin tahansa lähietäisyydellä olevaan laitteeseen.
    - Lelua voi käyttää oman älypuhelimen puheluiden soittamiseen ja vastaamiseen.
    - Haavoittuvuus mahdollistaa ulkopuoliselle laitteeseen soittamisen ja altistaa saman talouden lapset etäkuuntelulle ja yhteydenotoille.
    - https://www.pentestpartners.com/security-blog/audio-bugging-with-the-fisher-price-chatter-bluetooth-telephone/
  - Applen AirTag-jäljitinsensoria on käytetty luksusautojen jäljittämiseen ja varastamiseen.
    - Autoihin on kiinnitetty sensori julkisella paikalla, minkä jälkeen hyökkääjät ovat käyttäneet sitä paikantamiseen.
    - https://arstechnica.com/cars/2021/12/apple-airtags-being-used-by-thieves-to-track-high-end-cars-to-steal/

Analyysi

- Älylaitteiden hallinta ja yhteydet muihin laitteisiin tulee muodostaa siten, että se on mahdollista vain käyttäjälle itselleen.
- Älylaitteiden käyttäminen muille vahingollisella tavalla tulee pyrkiä estämään jo suunnitteluvaiheessa.
- Vanhempien tulee huolehtia lastensa lelujen tietoturvasta ja varmistua siitä, etteivät lapset pääse käyttämään aikuisten älylaitteita ilman valvontaa.

Automaatio ja IoT

- Kyberturvallisuus on nousemassa keskiöön autoteollisuudessa.
  - Kyberrikollisten kiinnostuksen autoja kohtaan ennakoidaan nousevan suurten riskien ja monien hyökkäysvektorien vuoksi.
  - Jakamistalouden kehitys ja uudet palvelumuodot haastavat käyttäjäoikeuksien hallinnan, käyttäjän tunnistamisen sekä tietosuojakäytännöt.
  - Kyberturvallisuuden huomioinnin merkitys kehitysprosessin alusta lähtien kasvaa jatkuvasti ja kyberturvallisuudesta on tulossa vaatimus kansainvälisille markkinoille pääsyyn ja autoteollisuuden menestymiselle.
  - https://www.darkreading.com/vulnerabilities-threats/cybersecurity-takes-the-wheel-as-auto-industry-s-top-priority

Analyysi

- Älyominaisuuksien menestyksekäs hyödyntäminen autoissa edellyttää kokonaisvaltaista kyberturvallisuuden hallintaa.
- Haavoittuvuuksien ja toimitusketjujen hallinta, asiakasdatan käsittely ja riittävät salauskäytännöt säilyttävät merkityksensä myös älyliikenteessä.
- Monimutkainen toimintaympäristö vaatii erityistä huomiointia kyberturvallisuusominaisuuksien toteuttamisessa.
- Halvat IoT-sensorit voivat tehdä mahdolliseksi mielikuvituksellisiakin rikoksia ja ainakin voivat helpottaa perinteisten rikosten tekemistä.

Automaatio

- Log4shell-haavoittuvuudella on iso vaikutus tuotantoympäristöihin
  - Tietoturvayhtiö Dragos arvioi vuoden 2021 lopussa löydetyn Log4shell-haavoittuvuuden olevan merkittävä myös monien kriittisten toimialojen tuotantoympäristöissä.
  - Haavoittuvuutta on mahdollista hyödyntää etänä ja sen luonne tekee hyökkäyksen tunnistamisesta vaikeaa
  - Verkkojen tehokas eriyttäminen vähentää haavoittuvuuden vaikutusta. Tuotantoympäristöjen sovellusten osaksi upotettu haavoittuva Log4j-versio voi kuitenkin altistaa toteutukset hyökkääjälle.
  - https://www.dragos.com/blog/industry-news/implications-of-log4j-vulnerability-for-ot-networks/

Analyysi

- Korjausurakka on niin suuri, että haavoittuvia Log4j-komponentteja sisältäviä tuotteita tulee olemaan käytössä vielä vuosien ajan.
- Organisaatioiden tulee:
  - varautua lähivuosina aktiivisesti jatkuviin haavoittuvuuden hyödyntämisyrityksiin.
  - etsiä aktiivisesti niin ostetuista kuin sisäisestikin kehitetyistä sovelluksista haavoittuvaa Log4j-komponenttia sekä päivittää se tarvittaessa.

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

- Marraskuussa yleisissä viestintäpalveluissa oli 4 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 0, C: 4
- Erilaiset katkokset jakaantuivat maantieteellisestikin pitkin Suomea.
  - Vaikutukset koskivat matkaviestinverkosta kiinteään laajakaistaan ja yksittäiseen radiokanavaan. Kahdessa häiriössä syynä oli jonkinlainen ohjelmistohäiriö.
- AWS-palveluiden katkoksista uutisoitiin joulukuussa.
  - US-EAST-1 -alueen viat aiheuttivat erilaisiin palveluihin katkoksia.
- Tänä vuonna merkittäviä häiriöitä on 73kpl, joten lukema on hieman suurempi kuin viime vuoden 67kpl.

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa oli vuonna 2021 keskimäärin hyvä.
- Kuukaudessa on keskimäärin vajaat 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.

Palvelunestohyökkäykset

- Palvelunestohyökkäyksiä ICT-palveluntarjoajia kohtaan.
  - Hyökkäykset ovat vaikuttaneet myös asiakkaiden palveluihin.
  - Erilaisia torjuntatoimia voi joutua tekemään äkillisesti palvelunestohyökkäyksen tapahtuessa.
  - Vaikka palvelunestohyökkäyksiin on jo varauduttu teknisesti, on myös valmistauduttava torjumaan hyökkäystä uusilla tavoilla, jos sen aiheuttamia vaikutuksia ei nykyisillä menetelmillä onnistuta torjumaan.
- Saimme ilmoituksia ilkivaltaisista palvelunestohyökkäyksistä
  - Hyökkäysten motiivina voi olla esimerkiksi tietyn verkkopalvelun häiritseminen.
  - Saamme tasaisin väliajoin ilmoituksia verkkopeleihin liittyvistä palvelunestohyökkäyksistä, joissa vastustajalle tilataan verkosta pelihetkiin vaikuttava hyökkäys.
- Noin 36% meille ilmoitetuista hyökkäyksistä (Q4/2021) Suomessa oli kooltaan yli 1 Gbit/s. Ilmoitettujen hyökkäysten perusteella skaala ulottuu vuonna 2021 jopa 260 Gbit/s tasolle asti.

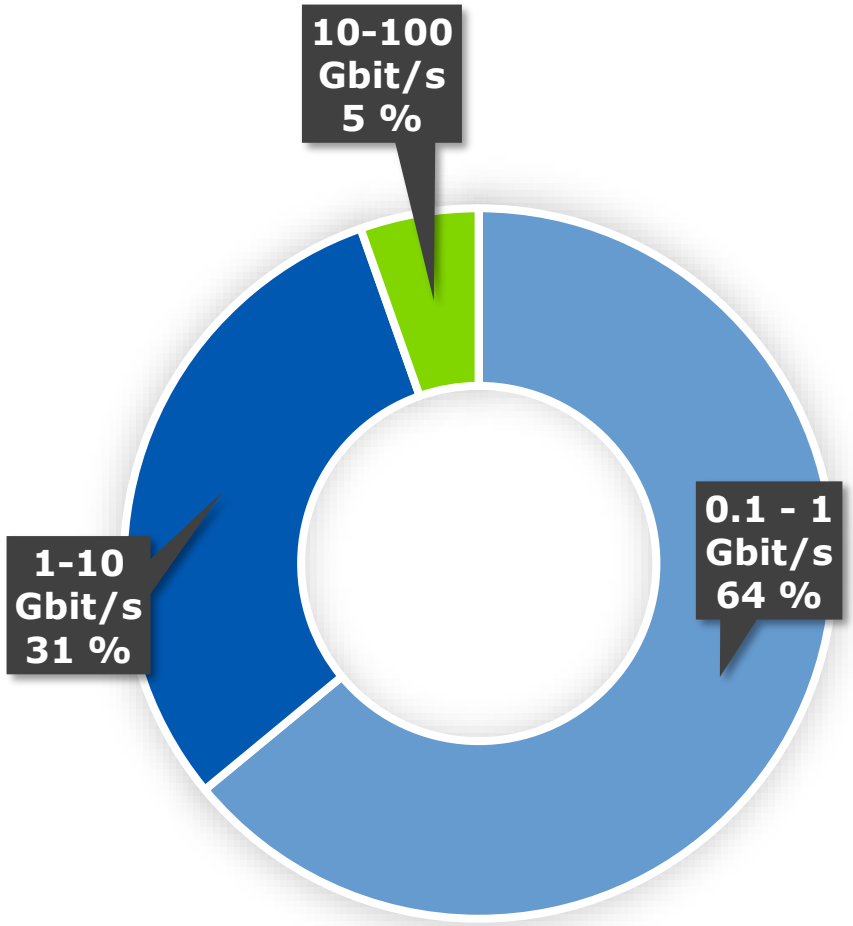
Analyysi

- Organisaatioiden tulisi tarkkailla ulospäin suuntautuvaa liikennettä kurkkaamalla konepellin alle.
  - Haittaohjelmat saatetaan havaitaan palvelimilla mm. prosessorikuorman kasvulla tai haitallisiin osoitteisiin liikennöinnistä, mutta palvelunestohyökkäykseen valjastetut palvelimet voivat vaatia liikenteen profiilien tarkkailua.
- Haavoittuvuuksien hallinta osoittautuu tärkeäksi myös palvelunestohyökkäysten kannalta.
  - Pidä palvelimet päivitettyinä, jotta ne eivät murrettuina osallistu toisten organisaatioiden häirintään.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 149,6 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q4/2021.
- Noin 74% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q4/2021 - 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

- Mobiililaitteiden vakoilu kaupan olevilla kehittyneillä vakoiluohjelmilla on noussut jälleen otsikoihin.
- Vakoiluohjelmistoistaan tunnetun NSO Groupin Pegasus-haittaohjelmaa on hyödynnetty maailmalla jälleen esimerkiksi oppositiopoliitikkojen vakoiluun.
  - Citizen Lab paljasti, että vakoilun kohteena ovat olleet muun muassa puolalainen oppositiopoliitikko, joka osallistui oikeistohallitusta vastustavan kampanjan toteuttamiseen, puolalainen syyttäjä sekä puolalainen oppositiopuolueen asianajaja.
  - Lisäksi Apple varoitti joukkoa Yhdysvaltojen valtionhallinnon työntekijöitä siitä, että näiden laitteille on murtauduttu. Kohteena olleet työntekijät ovat työskennelleet Ugandaan liittyvien aiheiden parissa.
- Toisinajattelijoihin ja toimittajiin kohdistuneesta vakoilusta nousi esiin myös Cytrox-nimisen yhtiön Predator-vakoiluohjelman käyttö. Toisen uhreista laitteelle oli samanaikaisesti asennettu sekä Pegasus että Predator, ja niitä operoivat eri tahot.
- Uutisointi on saanut myös valtiot reagoimaan vakoilutyökaluilla käytävään kauppaan: esimerkiksi NSO Groupin kotimaa Israel ilmoitti kiristävänsä rajat ylittävän hyökkäystyökalujen myynnin ehtoja.

Analyysi

- Vakoiluohjelmistoja ostavat autoritääriset valtiot hyödyntävät tuotteita muun muassa toisinajattelijoiden, poliittisten vastustajien, toimittajien ja aktivistien vakoiluun.
- Toimintaa voidaan pyrkiä rajoittamaan poliittisin ja lainsäädännöllisin toimin, mutta on epäselvää, millaiset vaikutukset erilaisilla toimenpiteillä lopulta on.

Vakoilu

- Ranskalainen tietoturvaviranomainen ANSSI julkaisi tietoja APT31:n kampanjasta, jossa ryhmittymä oli hyödyntänyt muun muassa pienreitittimien haavoittuvuuksia hyökkäysinfrastruktuurinsa luomiseen.
  - Reitittimien muodostamaa verkostoa hallittiin Pakdooriksi nimetyn haittaohjelman avulla, josta ANSSI on julkaissut analyysin.
- ANSSI:n mukaan operaation kohdejoukosta ei ole ollut tunnistettavissa kohdistusta tiettyihin sektoreihin tai aihepiireihin, vaan hyökkääjä vaikuttaa murtaneen opportunistisesti kohteita ja hyödyntäneen sen jälkeen saamaansa pääsyä jatkotunkeutumiseen valitsemissaan kohteissa.
- ANSSI on seurannut operaatiota vuoden 2021 ajan, ja joulukuun raportti on jatkoa kesällä 2021 kerrotuille tiedoille.

Analyysi

- APT31 on pyrkinyt reitittämään haitallisen liikenteen samassa maassa sijaitsevien kotireitittimien kautta menevänä liikenteenä todennäköisesti sulautuakseen muun verkkoliikenteen joukkoon. Kotimaisen internetpalvelun-tarjoajan kautta menevä liikenne ei näytä epäilyttävältä esimerkiksi lokeja analysoidessa.
- Tämä tarkoittaa samalla sitä, että liikenteen maantieteellinen rajaus ei rajoituskeinona toimi tämän tyyppisissä hyökkäyksissä eikä rajaavana tekijänä tietomurtoepäilyjä tutkittaessa.

Vakoilu

- Microsoft kertoi onnistuneesti heikentäneensä Kiinaan liitetyn NICKEL-ryhmittymän operaatiota, joka on kohdistunut maailmalla ainakin 29 maahan. Kohdemaista kolmannes on ollut Euroopassa.
  - Yhtiö otti oikeuden päätöksellä haltuunsa ryhmittymän käyttämiä verkkosivuja, ja teki näin käyttö-kelvottomaksi osan toimijan hyökkäysinfrastruktuurista.
  - Microsoftin mukaan kyseiset verkkosivut olivat keskeinen osa NICKELin viimeaikaista operaatiota.
  - Kohteisiin tunkeuduttiin päivittämättömän Microsoft Exchangen tai Sharepointin kautta tai hyödyntäen etäkäyttöratkaisujen haavoittuvuuksia.
- NICKEL on Microsoftin antama nimi Kiinasta käsin toimivalle ryhmälle, jonka toiminnassa on yhtiön mukaan yhtäläisyyksiä ainakin APT15:n, APT25:n ja KeChangin kanssa.
- Microsoftin mukaan ryhmän kohteita ovat valtionhallinnot, diplomaatit ja kansalaisjärjestöt Euroopassa sekä Etelä- ja Pohjois-Amerikassa.

Analyysi

- Myös laajoja valtiollisia operaatioita voidaan väliaikaisesti estää tai häiritä konkreettisilla toimenpiteillä, kuten hyökkäysinfrastruktuurin haltuunotoilla.
- Avainasemassa puuttumisessa on yhteistyö operaatioiden tunnistamiseksi, analysoimiseksi ja niihin reagoimiseksi, minkä vuoksi on tärkeää, että havaituista kohdistetuista hyökkäyksistä raportoidaan eteenpäin, jotta näihin toimenpiteisiin voidaan ryhtyä.

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

Vastaamolle huomautus ja seuraamusmaksu tietosuojarikkomuksista

- Tietosuojavaltuutetun toimisto on määrännyt Psykoterapiakeskus Vastaamolle 608 000 euron suuruisen hallinnollisen seuraamusmaksun yleisen tietosuoja-asetuksen säännösten rikkomisesta.
- Ratkaisun taustana tietoturvayhtiö Nixun lokakuussa 2020 valmistunut tekninen tutkinta.
- Vastaamon oman selvityksen mukaan toimenpiteitä tietoturvaloukkausten havaitsemiseksi ja selvittämiseksi tehtiin, mutta puutteellisen dokumentaation ja lokitietojen säilyttämisen takia tätä oli vaikea osoittaa ja katsottiin päätöksessä jääneen epäselväksi.
- Potilastietojärjestelmän palvelimen ylläpidossa ei noudatettu turvallisen palvelun ylläpidon parhaita käytäntöjä ja suojausmenetelmiä. Laiminlyöntejä oli mm. henkilötietojen turvallisessa käsittelyssä ja tietoturvaloukkausten ilmoitusmenettelyssä.
- Laiminlyöntejä pidettiin erittäin vakavina ja huolimattomuutta tietojen suojauksessa törkeänä. Menettelyä ilmoitusvelvollisuuden laiminlyönnin osalta pidettiin tahallisena.
- Päätös ei ole vielä lainvoimainen, annettu 7.12.2021
- Linkki: https://finlex.fi/fi/viranomaiset/tsv/2021/20211183

Oikeudelliset asiat

Henkilötunnusjärjestelmän uudistaminen etenee

- Henkilötunnusjärjestelmän uudistamista on valmisteltu kahdessa vaiheessa, joista ensimmäinen käynnistyi jo 1.9.2017.
- Esityksen tavoitteena on uudistaa henkilötunnusjärjestelmää mahdollistamalla henkilötunnuksen myöntäminen ulkomaalaisille nykyistä laajemmin, mahdollistamalla sähköinen etärekisteröityminen väestötietojärjestelmään mobiilisovellusta käyttäen, sekä ehkäistä henkilötunnusten käyttöä tunnistuskäytössä.
- Tavoitteena mahdollistaa kokonaan uuden yksilöintitunnuksen käyttöönotto yksilöiväksi tunnisteeksi henkilötunnuksen rinnalle. Asiasta on esitetty eriävä mielipide valmistelussa.
- Lakiluonnosten lausuntoaika on 4.3.2022 saakka. Lopullinen hallituksen esitys on tarkoitus antaa eduskunnalle syksyllä 2022 ja ehdotettujen lakimuutosten olisi tarkoitus tulla voimaan 1.1.2023. Sukupuolineutraalia henkilötunnusta koskevat muutokset tulisivat voimaan 1.1.2027.

Arjen kyberturvallisuus

Vuoden vaihtuessa on hyvä tarkistaa omien tilien turvallisuusasetukset

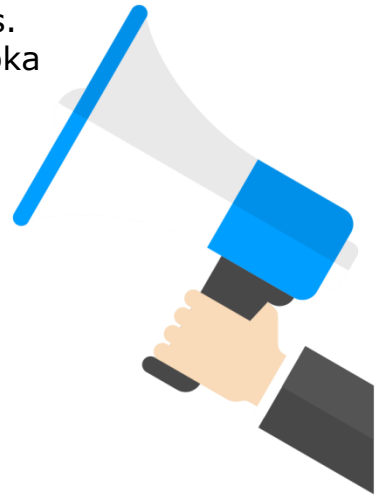
- Meillä on paljon erilaisia palveluita ja some-tilejä käytössä. Nyt onkin hyvä päivittää niiden salasanat ja ottaa monivaiheinen tunnistautuminen käyttöön alkavan vuoden kunniaksi.
- Katso vinkit! https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

Etätyöt jatkuvat monella - pidäthän huolta tietoturvasta myös kotona.

- Huolellisuudella ja muutamalla perustaidolla voit turvata tietosi verkossa. Kun käytät maalaisjärkeä, kunnollisia salasanoja ja päivität sovelluksesi sekä laitteesi ajallaan, olet jo hyvässä kyberturvassa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

Koronatodistuksen lukijalle Tietoturvamerkki!

- Koronatodistuksen lukijalla luetaan EU:n koronatodistus. Suomessa koronapassina toimii EU:n koronatodistus, joka on saatavilla Omakannasta. Koronatodistuksen lukijalla luetaan todistuksen QR-koodi, jolloin ruudulle tulee hyväksytty tai hylätty merkintä.
- https://tietoturvamerkki.fi/fi/tuote-koronatodistuksen-lukija/



Kuluttajille mahdollisuus tarkastaa tekstiviestillä matkapuhelinsopimuksensa voimassaolo

- Kuluttaja voi vuoden 2022 alusta lähtien tarkastaa matkapuhelimensa määräaikaisen liittymäsopimuksen päättymispäivän tekstiviestillä. Kuluttaja voi lähettää tekstiviestin SOPIMUS (tai ruotsiksi ABONNEMANG) numeroon 18321, ja hän saa välittömästi vastauksena tekstiviestin, joka kertoo määräaikaisen sopimuksen päättymispäivän
- https://www.traficom.fi/fi/ajankohtaista/kuluttajille-mahdollisuus-tarkastaa-tekstiviestilla-matkapuhelinsopimuksensa

Uutisia Kyberturvallisuuskeskuksesta

Kyberturvallisuuskeskus on julkaissut oppaan: Tunnisteet ja tietosuoja Anonymisointi ja sen rajat

- Raportissa tarkastellaan sekä teknisiä että muita keinoja järjestää tiedonvaihtoa siten, että tiedon käyttöarvo ei kärsi liiaksi.
- Tarkastelussa käydään läpi keskeisimmät aiheeseen liittyvät tieteelliset tutkimukset, anonymisointiin tarjolla olevat työkalut sekä tärkeänä osana tietosuojaan liittyvää lainsäädäntöä.
- Erityisesti tarkastellaan tietoverkkojen tunnisteita tietoturvatyöhön liittyen mutta periaatteet ovat sovellettavissa muillekin aloille.
- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tunnisteet%20ja%20tietosuoja.pdf

Neljä neuvoa onnistuneen kyberharjoituksen järjestämiseen

- Kyberharjoittelu on hyödyllinen tapa tunnistaa organisaation toiminnan kehityskohteita ja testata olemassa olevien prosessien tehokkuutta. Kokemuksemme mukaan onnistuneissa kyberharjoituksissa toistuvat kerta toisensa jälkeen neljä tärkeää kokonaisuutta.
- Lue lisää harjoituksen järjestämisestä täältä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nelja-neuvoa-onnistuneen-kyberharjoituksen-jarjestamiseen

Kiinteiden laajakaistaverkkojen rakentamiselle lisärahoitusta - ensimmäisten hankealueiden kuuleminen käynnistyy

- Liikenne- ja viestintävirasto Traficom käynnistää ripeästi uuden laajakaistatukihankkeen hankealueiden kuulemiset jo ennen helmikuun alussa voimaan tulevaa laajakaistatukilakia.
- Tukiohjelmalle on haettu rahaa EU:n elpymisvälineestä lähes 50 miljoonaa euroa. Maakunnat ja kunnat ovat nyt avainasemassa, jotta tukirahat saadaan hyödynnettyä.
- https://www.traficom.fi/fi/ajankohtaista/kiinteiden-laajakaistaverkkojen-rakentamiselle-lisarahoitusta-ensimmaisten

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