TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 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

TRAFICOM

16.6.2022

Kybersää toukokuu 2022

Tietomurrot ja -vuodot

- Sosiaalisen median tileille on kohdistunut tietomurtoja tai niiden yrityksiä.
- Onnistuneet kalastelut ovat johtaneet Office 365 –tilien murtoihin ja tileiltä lähetettäviin viesteihin.

Huijaukset ja kalastelut

- Tuhansittain tekstiviestejä väärennetty tilausvahvistuksiksi Wallpaper-taustakuvapalvelun ja Dorgames-pelipalvelun nimissä.
- Verottajan nimissä kalastellaan pankkitunnuksia.

Haittaohjelmat ja haavoittuvuudet

- FluBot-haittaohjelmaa levittänyt infrastruktuuri ei ole enää aktiivinen ja asiasta tehty varoitus on poistettu.
- Uusi ohje auttaa kiristyshaittaohjelman kohteeksi joutunutta organisaatiota.

Automaatio ja IoT

- Saksan tietoturvallisuusviranomainen BSI on julkaissut tietoturvasertifikaatin kuluttajien älylaitteille.
- Rikollista toimintaa voidaan peittää hyväksikäyttämällä normaalien tietoturvakontrollien ulkopuolella olevia IoT-järjestelmiä.

Verkkojen toimivuus

- Toukokuussa verkot toimivat kiitettävästi Suomessa.
- Palvelunestohyökkäyksiä ilmoitettiin, mutta suuremmilta vaikutuksilta vältyttiin.

Vakoilu

- APT41 eli Winnti on pyrkinyt vakoilemaan teollisuusalan yrityksiä eri puolilla maailmaa.
- Venäjään julkisuudessa liitettyjen ryhmittymien aktiivisuus jatkuu Euroopassa, ja kyberhyökkäyksiä nähdään edelleen myös Ukrainassa.

TRAFICOM

16.6.2022

Kuukauden tunnuslukuja

1.6

Poliisi tiedotti 1.6. että FluBot-haittaohjelmaa levittävä infrastruktuuri ajettiin alas kansainvälisessä viranomaisoperaatiossa. Haittaohjelma ei ole tällä hetkellä aktiivinen.

28

Liikenne- ja viestintäviraston määräys 28 viestintäverkkojen ja -palveluiden yhteentoimivuudesta on uudistettu. Operaattoreilla on jatkossa velvollisuus estää soittajan numeron väärentäminen ja huijaussoittojen välittäminen puhelun vastaanottajille.

2

Toukokuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä, mikä on selvästi vähemmän kuin keskimäärin.

Poistimme varoituksen 1/2022 FluBot haittaohjelmaa levitetään jälleen tekstiviestitse

- Julkaisimme keltaisen varoituksen Flubotista 10.5.2022
- Haittaohjelmaa levittävissä viesteissä viitattiin ääniviestiin tai vastaamattomaan puheluun. Linkin takaa tarjottiin Android-puhelimille asennettavaksi haittaohjelma ja muille tietojenkalastelua.
- FluBot-haittaohjelma varasti puhelimesta erilaisia tietoja ja levitti itseään puhelimesta lähetettyjen viestien avulla ympäri maailmaa.
- Varoitus poistettiin, koska haittaohjelmaa levittävä infrastruktuuri ajettiin alas kansainvälisessä viranomaisoperaatiossa. Haittaohjelma ei ole tällä hetkellä aktiivinen.
- Katso lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ttn_02062022

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Digitaalisuus läpileikkaa koko organisaation toimintaa ja muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaation jatkuvuuteen ja riskienhallintaan.

2

Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä.

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

16.6.2022

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Digitaalisuus läpileikkaa koko organisaation toimintaa ja muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaation jatkuvuuteen ja riskienhallintaan.

- Sota Ukrainassa vaikuttaa myös Suomessa. Esimerkiksi talouden äkilliset muutokset ja energian hinnannousu näkyvät vaikeasti ennakoitavina kehityskulkuina. Muutokset saattavat tapahtua nopeasti ja heijastua myös digitaalisen maailman toimivuuteen.

- Epävarmuustekijöillä voi olla isoja vaikutuksia organisaatioiden toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön aiheuttamat uhkat kriittisille prosesseille.

- Kansainvälinen tilanne vaikuttaa väistämättä myös digitaaliseen maailmaan ja kyberuhkilta varautumiseen. On tärkeää, että organisaatioiden johto ja asiantuntijat tarkastelevat kyberturvallisuuden suojauskäytäntöjään sekä ylläpitävät niitä aktiivisesti. Tutustu johdon ja asiantuntijoiden ohjeeseen.(1)

CASE

Nato-jäsenhakemuksen seurauksena Suomeen voidaan kohdistaa erilaista kybervaikuttamista sekä informaatiovaikuttamista verkossa.

Vaikuttaminen voi näkyä esimerkiksi palvelunestohyökkäyksinä.

Palvelunestohyökkäyksillä saadaan näkyvyyttä, mutta niiden vaikutukset eivät useimmiten ole laajoja ja pitkävaikutteisia. Tällä hetkellä Suomen kyber-turvallisuustilanne on vakaa ja verkot toimivat normaalisti.

2. Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa

Kyberturvallisuus on organisaatioiden rajat ylittävää. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä. Tiedonvaihto on tärkeää eri toimijoiden välillä kokonaistilannekuvan rakentamiseksi.

- Jokainen organisaatio on tärkeä pala kokonaisturvallisuuden ketjussa, joka rakennetaan yhteistyöllä eri toimijoiden välillä.
- Omien sidosryhmien tunteminen on keskeistä. Jos organisaatio on kyberhyökkäyksen kohteena on tärkeä ymmärtää, miten tilanne voi vaikuttaa sidosryhmiin tai toisinpäin. Yhteistyö verkostoissa onkin keskiössä.
- Tiedonvaihtoverkostojen tarkoitus on mahdollistaa tietoturva-asioiden luottamuksellinen käsittely osallistujien kesken sekä organisaatioiden tietoturvaosaamisen lisääminen ja kokonaistilannekuvan kehittäminen.
- Avoin ja ajankohtainen tiedonjako vähentää uhkien vaikutuksia ja kustannuksia. Toisilta oppiminen on myös kustannustehokasta, kun muiden ei tarvitse keksiä uudelleen toisaalla jo käytössä olevaa ratkaisua.
- Ilmoita Kyberturvallisuuskeskukselle, joka kokoaa kybertilannekuvaa Suomesta!

CASE

ISAC-tiedonvaihtoryhmät (ISAC=Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-ryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä. Ryhmät kehittävät myös edustamansa toimialan ja yhteiskunnan kyberturvallisuutta esimerkiksi toteuttamalla toimialaansa liittyviä riskianalyysejä, tutkimuksia ja ohjeistusta.(1)

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.[(3)] [(4)]

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

- Toukokuussa tehtiin ilmoituksia tavalliseen tapaan.
  - Yksityishenkilöiden sosiaalisen median tileille on tehty murtoja ja niiden yrityksiä tavalliseen tapaan.
  - Ilmoituksissa korostuvat Instagram- ja Facebook-tilien murrot ja murtojen yritykset.
  - O365-kalasteluiden onnistumisen seurauksena sähköpostitilejä on onnistuttu murtamaan ja tileiltä on lähetetty eteenpäin viestejä.

Analyysi

- Erilaisiin huijauksiin kannattaa edelleen varautua. Kalasteluiden ja huijauksien seurauksena voi tapahtua myös tietomurto.
- Murrettuja sähköpostiosoitteita voidaan käyttää laskutuspetoksiin.
  - Onnistuneiden laskutuspetoksien todennäköisyydet kasvavat lomakauden aikana sijaisjärjestelyiden vuoksi.
  - Sijaisten ohjeistaminen oman yrityksen toimintatavoista on tärkeää.
  - Sijaisia kannattaa muistuttaa, että epäselvät laskut ja tilinumeroiden muutokset kannattaa varmistaa soittamalla.

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

- Toukokuu alkoi tekstiviestimyrskyllä.
  - Kyberturvallisuuskeskukselle raportoitiin heti toukokuun ensimmäisellä viikolla satoja tekstiviestejä, joissa väitettiin uhrin tilanneen taustakuvapalvelun.
  - Huijausviestissä ollut peruutuslinkki ei peruuttanut mitään, vaan vei tilausansaan. Wallpaper-niminen taustakuvapalvelu oli vain huijausta.
  - Myöhemmin kuvapalveluhuijaus vaihtui Dorgames-nimiseksi pelihuijaukseksi, joka toimi samalla tavalla.
  - Huijaustekstiviestejä lähetettiin viikossa satoja tuhansia.

Veronpalautusviestit ovat huijausta

- Verohallinnon nimissä lähetetyt tekstiviestit lupailevat veronpalautuksia, mutta viestin linkki johtaa tietojenkalastelusivulle.(2)
- Huijauslinkin takana uhria pyydetään kirjautumaan pankkitunnuksilla verottajan sivulle, mutta todellisuudessa verkkosivulle syötetyt pankkitunnukset päätyvät rikollisen käsiin.
- Aidoissa Verohallinnon lähettämissä viesteissä ei ole koskaan suoraa linkkiä OmaVeroon.

Huijaukset ja kalastelut

- Huijauspuheluita Kongosta.
  - Ns. häläripuhelut soivat vain kerran tai pari ja katkeavat ennen kuin niihin ehtii vastata. Hälärihuijausten ideana on houkutella soittamaan takaisin kalliiseen ulkomaan numeroon.
  - Toukokuussa Suomeen on tullut paljon häläripuheluita Kongon suuntanumerosta. Niihin ei kannata soittaa takaisin.
  - Suomen teleoperaattorit pystyvät tunnistamaan automaattisesti hälärihuijauksia lähettäviä numeroita ja estämään huijauksia, joita olisi muuten voinut tulla Suomeen paljon nykyistä enemmän.
  - Puheluun vastaaminen Suomessa on aina maksutonta ja vaaratonta, joten hälärihuijauksista ei kannata hätääntyä.

Verkon kirpputoripalveluissa huijauksia

- Verkon osto- ja myyntipalstoilla on edelleen paljon huijareita.
- Myynti-ilmoituksiin tulee vastauksia huijareilta, jotka tarjoutuvat ostamaan tuotteen kuriiripalvelun kautta.
- Postin nimen lisäksi käytetään myös pienempien kuljetuspalveluiden nimiä, kuten Fiuge.
- Aidoilla kuriiripalveluilla ei kuitenkaan ole huijausten kanssa mitään tekemistä. Huijarin antamat linkit johtavat tietojenkalastelusivulle, jossa uhrilta kalastellaan luottokorttinumeroita.

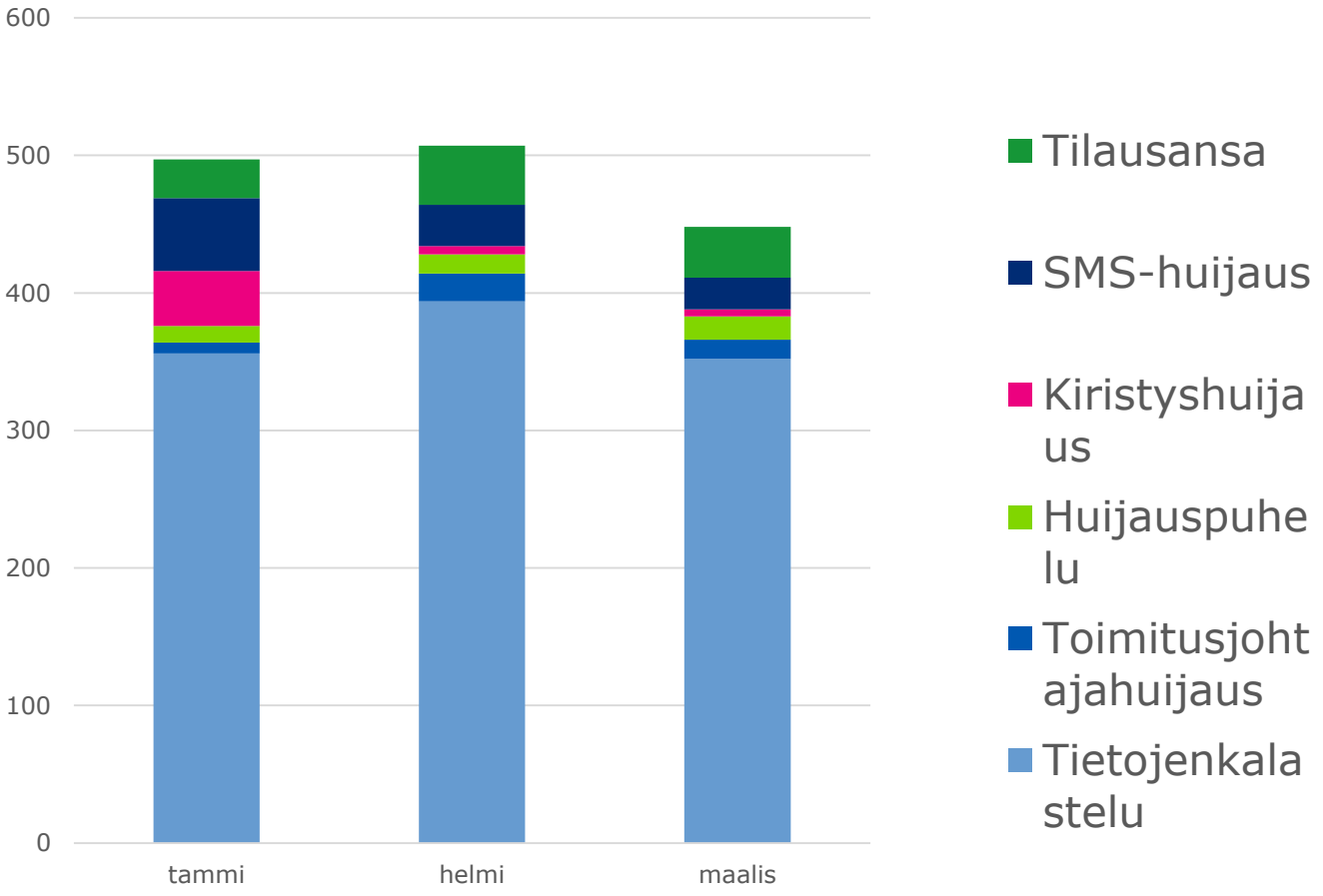
Huijaukset ja kalastelut

- Laaja kirjo myös monenlaisia muita huijauksia ollut liikkeellä.
  - Toukokuuta väritti poikkeuksellisen runsas rykelmä työtarjoushuijauksia ja tilausansa-tekstiviestejä, mutta samaan aikaan myös muut huijaukset ovat jatkuneet.
  - Pankkikalastelua on tehty kaikkien pankkien ja verottajan nimissä myös turvapostiksi väärennetyillä viesteillä.
  - Pornokiristykset ovat taas aktivoituneet. Huijausviesteissä väitetään, että uhrista on tehty pornovideo ja vaaditaan lunnaaksi virtuaalivaluuttaa.
  - Yrityksiltä, yhdistyksiltä ja jopa seurakunnilta on koetettu huijata rahaa erilaisilla petoksilla esiintyen johtajan nimissä.

Kirjoitusvirhe voi viedä huijaukseen

- Eri palveluiden nimen lähellä olevia verkko-osoitteita rekisteröidään usein huijauksiin.
- Esimerkiksi palvelu.com-sivua voi muistuttaa huijaussivu palelu.com, pakvelu.com, palvrlu.com, tai muu vastaava kirjoitusvirhe.
- Oikean palvelun vierestä huijarin rekisteröimä osoite vie usein erilaisiin huijauksiin tai muuhun haitalliseen verkkosisältöön.

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

- FluBot-haittaohjelman levityksestä ilmoittava varoitus on poistettu.
  - Android-laitteisiin kohdistuva haittaohjelma varastaa tietoja käyttäjän laitteelta ja sitä levitetään SMS ja MMS -viestien kautta.
  - Toukokuussa suomalaiset operaattorit suodattivat satoja tuhansia FluBot-haittaohjelman lähettämiä tekstiviestejä ja multimediaviestejä.
  - Nopeat suodatustoimet toimivat ja ne hidastivat haittaohjelman leviämistä. Toukokuun 2022 loppuun mennessä havainnot uusista haittaohjelmatartunnoista loppuivat.
  - FluBot-kampanjat ovat olleet aktiivisia joulukuusta 2020 alkaen, Suomessa niistä on julkaistu varoitukset 06/2021 ja 12/2021. Toukokuun kampanjasta saimme yli 500 ilmoitusta.

Analyysi

- FluBot-haittaohjelma ajettiin alas kansainvälisessä poliisioperaatiossa 1.6.(3)
- Rikollisten saattaminen rikosvastuuseen on yhä kesken. Europol vastaa tutkinnasta.

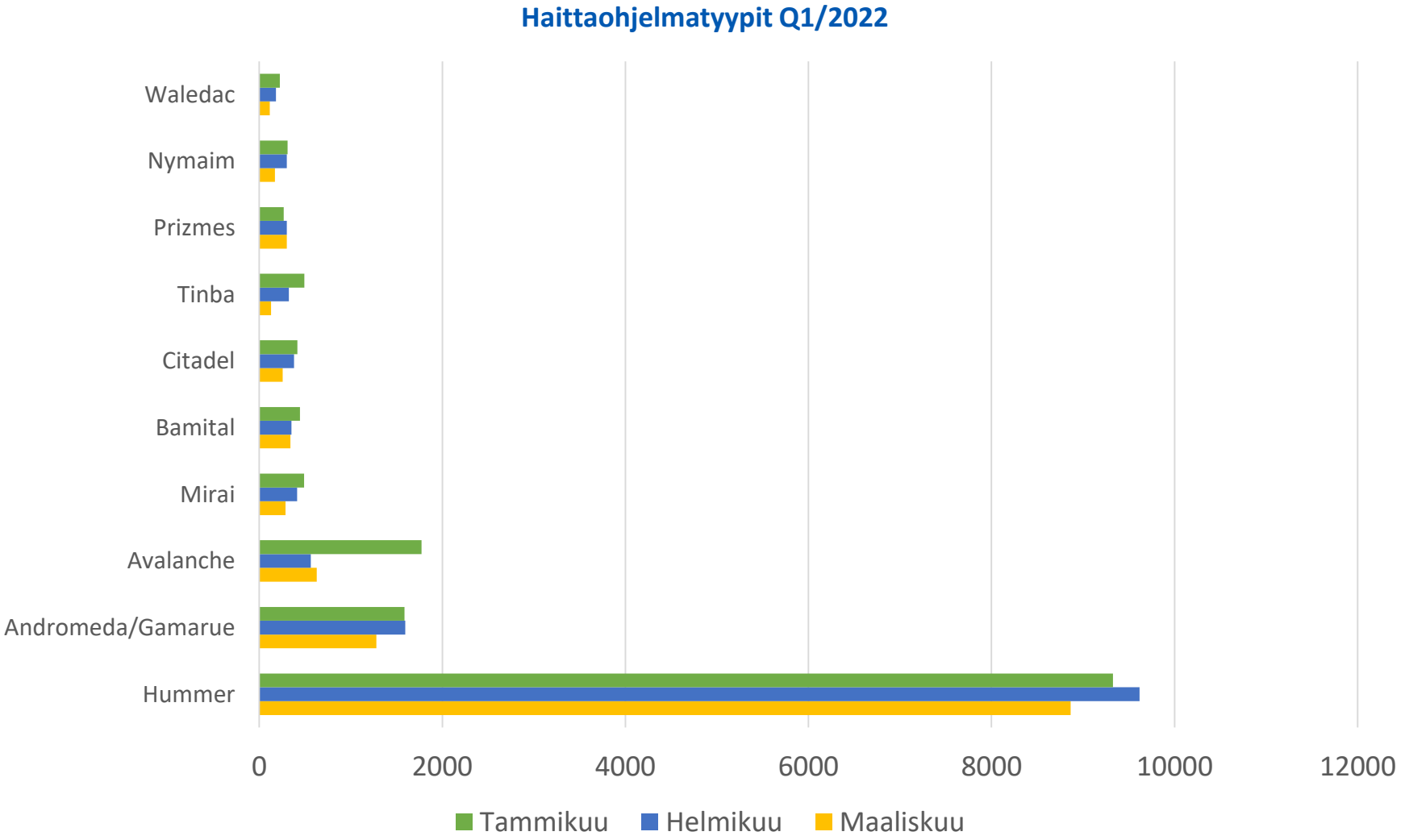
Haittaohjelmat

- Uusi ohje auttaa kiristyshaittaohjelman kohteeksi joutunutta organisaatiota.(4)
  - Ohje antaa neuvoja tilanteessa, jossa kiristyshaittaohjelma uhkaa organisaation toimintaa. Ohje on suunnattu organisaatioiden johdolle ja vastuuhenkilöille.
  - Ohjeessa keskitytään erityisesti toimintaan kiristyshaittaohjelman aiheuttaman kyberhyökkäyksen tapahtuessa.
  - Ohjeessa käsitellään myös tärkeimpiä varautumistoimenpiteitä ja tilanteen jälkeen tehtäviä jälkitoimia.

Analyysi

- Kiristyshaittaohjelma tai lunnastroijalainen on kyberhyökkäys, jossa hyökkääjät pyrkivät salaamaan organisaation datan salausalgoritmilla ja vaativat lunnaita tietojen palauttamista vastaan.
- Riski kiristyshaittaohjelman kohteeksi joutumisesta on kasvanut viime vuosina merkittävästi.

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.(5)

Haavoittuvuus

- F5 BIG-IP:n haavoittuvuutta on jo hyväksikäytetty.
  - Etänä hyväksikäytettävää haavoittuvuutta CVE-2022-1388 on Palo Alton artikkelin mukaan skannattu aktiivisesti ja käytetty jo hyväksi.(6)
  - Päivitykset tulisi asentaa niin pian kuin mahdollista.

Analyysi

- Haavoittuvuus mahdollistaa komentojen suorittamisen etänä.
- Rikolliset voivat käyttää haavoittuvuutta hyväkseen ohittaakseen kokonaan tunnistautumisen.
- Mielivaltainen koodin syöttäminen haavoittuvassa järjestelmässä on myös mahdollista.
- Haavoittuvuuden skannaus ja hyväksikäyttö on ollut aktiivista.
- Haavoittuvuudelle on annettu 9.8-arvo CVSS-luokituksessa.

Kuukauden haavoittuvuusjulkaisut

- VMwaren kriittiseksi luokiteltu päivityspaketti korjaa haavoittuvuuksia useista tuotteista (9/2022).
  - Yhtä haavoittuvuutta hyväksikäyttämällä käyttöliittymään verkon yli käsiksi pääsevä hyökkääjä voi saada pääkäyttäjätason oikeudet ilman todentamista.
- Uusi haavoittuvuus Microsoftin työkalussa mahdollistaa hyökkäykset haitallisten Microsoft Office -dokumenttien avulla (10/2022).
- Kriittinen haavoittuvuus Atlassian Confluence -tuotteissa mahdollistaa hyökkäykset ilman tunnistautumista (11/2022).

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

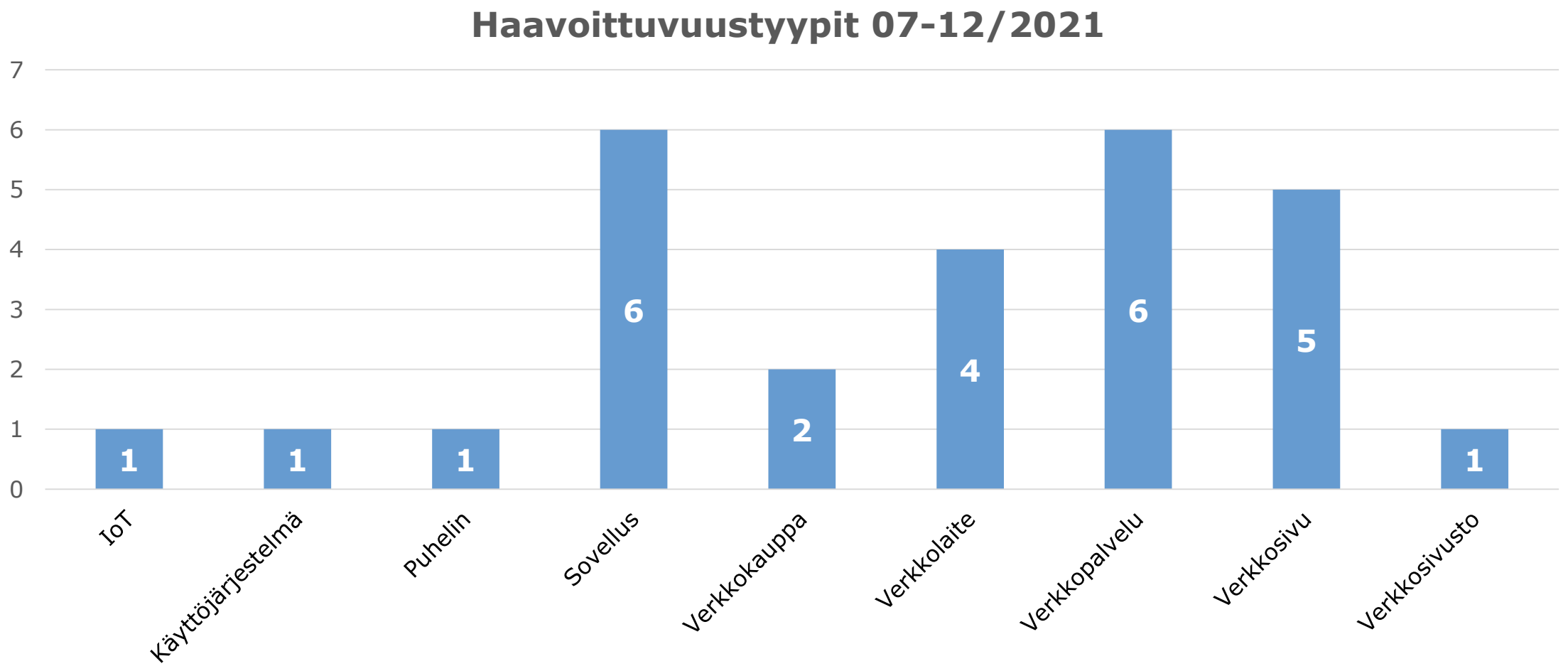
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **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 11 kpl (tilanne 14.6.2022).**
  - 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 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

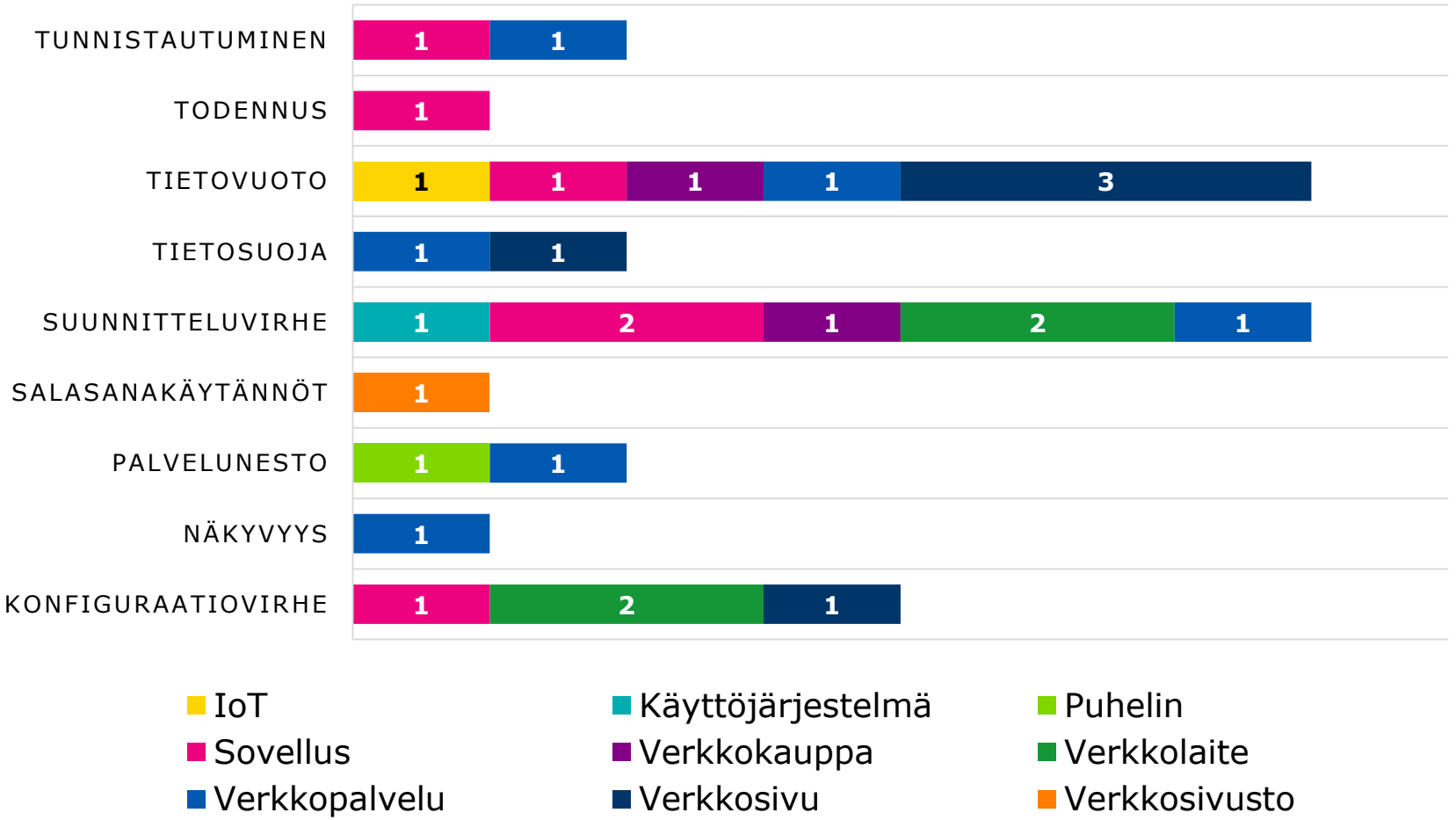
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat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



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Tutustu aiheeseen tarkemmin haavoittuvuuskoordinaation sivuilla.(7)

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.

Saksalainen IoT-merkki kuluttajatuotteille

- Saksan turvallisuusviranomainen BSI on julkaissut tietoturvamerkin (IT-Sicherheitskennzeichen) kuluttajien älytuotteille.
- Merkki on maailman kolmas viranomaismerkki kuluttajien IoT-laitteille Traficomin Tietoturvamerkin ja Singaporen kyberturvallisuusviranomaisen CSA:n IoT Cybersecurity Labelin jälkeen.
- BSI:n merkin vaatimukset perustuvat Traficomin ja Singaporen tavoin ETSIn standardiin EN 303 645 sekä teknisiin ohjeisiin ETSI TS 103 701 ja BSI TR-03173.
  - Merkin hakeminen on vapaaehtoista ja sitä voi hakea älytelevisioille, kaiuttimille, kameroille, älyleluille sekä robotti-imureille ja robottiruohonleikkureille.
  - Merkin käyttöön liittyy markkinavalvontamekanismi. Tuotteen vaatimustenmukaisuus varmistetaan/tarkistetaan säännöllisesti. Lisäksi BSI voi tarkastaa tuotteen, mikäli ilmenee seikkoja, jotka viittaavat siihen, että valmistajan lupausta ei ole noudatettu.

Analyysi

- Viranomaiset kiinnittävät yhä enemmän huomiota kuluttajatuotteiden kyberturvallisuuteen.
- Kuluttajatuotteiden kyberturvallisuuteen on tulossa myös pakottavaa EU-sääntelyä.
- Traficom on ollut kehityksen kärjessä luomallaan Tietoturvamerkillä.(8)
- Organisaatioiden, valmistajien ja myyjien on syytä valmistautua täyttämään myös pakollisia vaatimuksia ja kehittää omaa kyberturvallisuusosaamistaan.

IoT – IoT-laitteet rikollisessa toiminnassa

- Tietoturvayhtiö Mandiant kertoi rikollisryhmästä, joka oli asentanut tuntemattomalla tavalla tehdyn tietomurron jälkeen takaovia mm. organisaatioiden NAS-verkkotallennusjärjestelmiin.(9)
- Verkkotallennusjärjestelmät eivät aina tue tietoturvatyökaluja kuten virustorjuntaa. Rikollisryhmä loi takaoven kautta hankalasti havaittavia tunneleita uhrien ympäristöihin.
- Takaovia hyödyntäen ryhmä pystyi pysymään huomaamattomana uhrien ympäristöissä useiden kuukausien ajan.
- Komentopalvelimina käytettiin mm. saastutettuja neuvotteluhuoneiden kamerajärjestelmiä ja IoT/IP-kameroita. Kamerat olivat yhteydessä internetiin ja niissä saattoi olla päivittämättömät laiteohjelmistot.
- Mandiant arveli, että IoT-kameroiden haltuunotto tapahtui oletussalasanojen väärinkäytön avulla.

Analyysi

- Rikollista toimintaa voi peittää kierrättämällä liikennettä saastutettujen IoT-laitteiden kautta. Tässä tapauksessa liikenne kulki mm. vakoilun kohteena olleen uhriorganisaation verkkotallennusjärjestelmän ja toisen uhriorganisaation neuvotteluhuoneen kameroiden välillä.
- Yritysten verkkolevyjen ja IoT-järjestelmien liikenne voi olla hyvä kierrättää verkkoliikennettä monitoroivien työkalujen kautta.
- Suosittelemme tarkastelemaan omien IoT-järjestelmien näkyvyyden internetiin. Samoin laitteiden oletussalasanat on aina syytä vaihtaa.
- SUPO:n havaintojen perusteella murrettuja kotireitittimiä ja verkkotallennusjärjestelmiä on hyödynnetty kybervakoiluoperaatioissa myös Suomessa.(10)

Automaatio – Kriittisen infran suojaaminen

- HybridCOE julkaisi raportin kriittisen infrastruktuurin suojaamisesta. Raportti sisältää tietoa mm. automaatiojärjestelmiin kohdistuvista uhkista, jo nähdyistä hyökkäyksistä ja järjestelmien suojaamisen haasteista.
- Raportin mukaan teknologiat, joilla pyritään varmistamaan teollisten ympäristöjen turvallisuus (safety), luotettavuus (reliability) ja tehokas käyttö, ovat joutuneet ammattitaistoisten hyökkääjien kohteiksi.
- Teollisuusautomaatioon kohdistuneita hyökkäyksiä on verrattain vähän verrattuna muihin ympäristöihin kohdistuneisiin hyökkäyksiin.
- Raportin mukaan kriittiseen infrastruktuuriin kohdistuneet hyökkäykset tulevat aina yllätyksenä, vaikka parhaita kyberturvallisuuskäytäntöjä olisi pyritty noudattamaan.
  - Yhdeksi syyksi esitetään ettei tiettyjä uhkia ole pidetty riittävän realistisina.

Analyysi

- Kriittisen infrastruktuurin suojaamisessa on tärkeintä tietää kriittisimmät suojattavat kohteet. Näiden löytämisessä voi hyödyntää Kybermittari –työkaluamme.(11)
- Kuten raportissakin mainitaan, IT-keskeinen ajattelutapa, jossa vain tiedon suojaamiseen panostetaan, ei riitä kriittisen infrastruktuurin suojaamiseksi. Myös fyysisten järjestelmien ja prosessien toimivuuden varmistaminen on otettava huomioon.
- Kyberturvallisuuskeskuksen sivuilta löytyy eri hankkeissa toteutettuja materiaaleja kriittisen infran turvaamiseksi.(12)

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

- Toukokuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 0, C: 2.
  - Kahden vikatapauksen syinä olivat sähkövika ja ohjelmistovika.
- Ylen artikkelissa operaattoreiden edustajat kertovat verkkojen tilanteesta ja varautumisesta kotimaassa.(13)
  - Jos sabotaasi tai myrsky katkoo sähköt suomalaiselta tukiasemalta, akuista riittää virtaa vähintään kolmeksi tunniksi. Monissa Euroopan maissa akkuja ei ole ollenkaan.
  - Artikkelissa todetaan myös, että Venäjän hyökkäyssodasta huolimatta Ukrainan verkot ovat toimineet yllättävän hyvin.

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.

Palvelunestohyökkäykset

- Toukokuussa saimme ilmoituksia palvelunestohyökkäyksistä alkuvuotta vähemmän.
  - Muutamalla hyökkäyksellä oli pieniä vaikutuksia palveluiden toimintaan. Osa ilmoitetuista palvelunestohyökkäyksistä voi liittyä haktivismiin, josta kerroimme viime kybersäässä.(14)
- Vaikutuksia aiheuttaneet palvelunestohyökkäykset ovat aiempaa useammin vahingollisempia sovellustason hyökkäyksiä.
  - Perinteiset volyymiin perustuvat palvelunestohyökkäykset tukkivat kaistan massiivisella liikennemäärällä. Sovellustason palvelunestohyökkäykset pyrkivät aiheuttamaan haittaa esimerkiksi erilaisin kyselyin tai pyynnöin palvelua kohtaan.
  - Organisaatiot ovat varautuneet torjumaan volyymitason hyökkäyksiä, mutta sovellustason hyökkäykset esimerkiksi verkkosivuihin voivat aiheuttaa haittaa mikäli niitä ei ole suojattu.

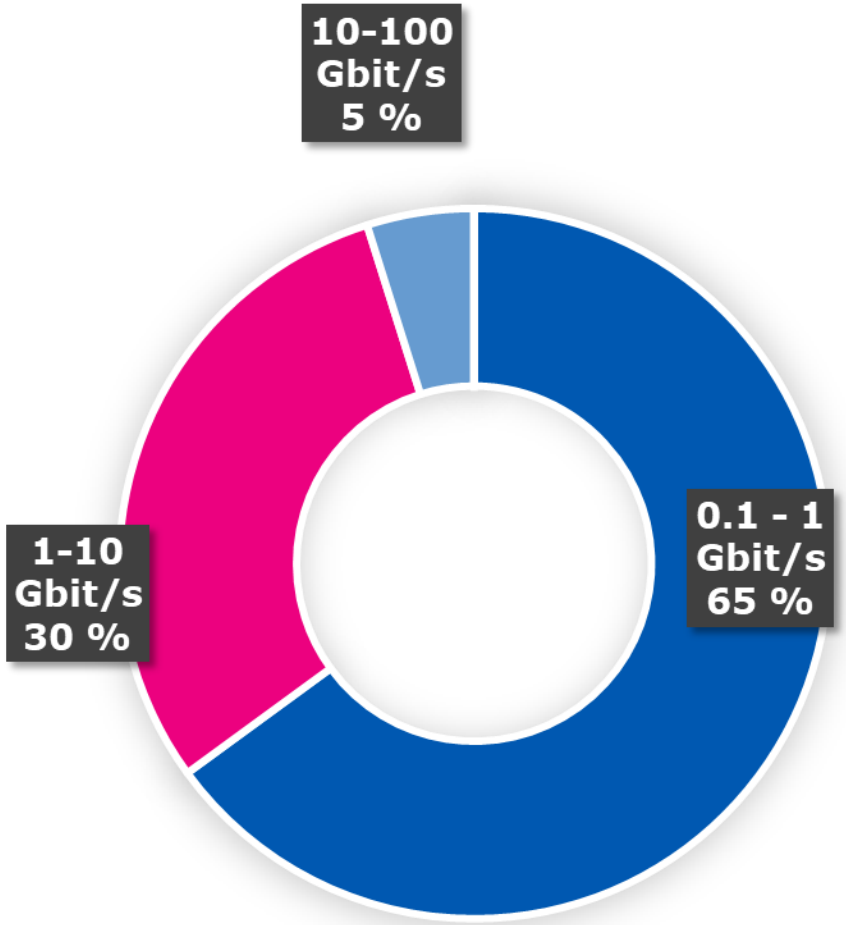
Analyysi

- Organisaatioiden tulee varautua myös sovellustason palvelunestohyökkäyksiin.
  - Klassiset volyymihyökkäykset eivät välttämättä enää aiheuta vahinkoa, mikäli niiltä on suojauduttu asianmukaisesti.
  - Meille ilmoitettujen palvelunestohyökkäysten volyymi on ollut keskimäärin 30 Gbit/s. Se tulisi pystyä torjumaan, mikäli tavanomaisen suurilta palvelunestohyökkäyksiltä halutaan varautua.
- Pelkkä volyymitason suojautuminen ei välttämättä riitä, jos organisaation palveluihin kuuluu esimerkiksi verkkosivu, jonka tulee olla saatavilla 24/7.
  - Sovellustason hyökkäykset voivat aiheuttaa suurtakin haittaa. Niiden torjuminen ilman harjoittelua ja prosesseja voi olla hyökkäyksen alkuvaiheessa työlästä.
  - Taitavat hyökkääjät voivat myös muuttaa hyökkäystapaa kesken tapahtumien, mikäli he havaitsevat organisaation torjuneen hyökkäyksen hetkellisesti.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 126 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q1/2022.
- Noin 75% hyökkäyksistä oli kestoltaan 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

- Kiinaan julkisuudessa liitettyjen hakkeriryhmien kohteina on ollut organisaatiota niin Euroopassa, Pohjois-Amerikassa kuin esimerkiksi Venäjälläkin.
- Kiinalaisryhmä APT41 eli Winnti on pyrkinyt niin kutsutulla CuckooBees-operaatiolla vakoilemaan teollisuusalan yrityksiä Pohjois-Amerikassa, Euroopassa ja Aasiassa.(15)
  - Tuotekehitys- ja liiketoimintatietoja on pyritty varastamaan ainakin puolustus-, energia- ja ilmailu- ja avaruusteollisuuden yrityksiltä sekä lääkeyhtiöiltä.(16)
- Tietoturvayhtiö CheckPointin mukaan kiinalainen Twisted Pandaksi nimetty toimija on lähettänyt kohdistettuja kalasteluviestejä ainakin kahteen venäläiseen puolustusteollisuuden tutkimuslaitokseen.(17)
  - Kampanja on osa kesästä 2021 jatkunutta kokonaisuutta.
  - CheckPointin mukaan Twisted Pandan toiminnassa on havaittu mahdollisia yhtäläisyyksiä sekä APT10:een (Stone Panda) että Mustang Pandaan, jotka molemmat yhdistetään julkisuudessa Kiinaan.

Analyysi

- Kiinalaisiin ryhmiin liitettyjen kybervakoilukampanjoiden kohteina ovat tyypillisesti yritykset ja erilaiset tuotekehitykseen, liiketoimintaan ja yrityssalaisuuksiin liittyvät tiedot.
- Kiinalaisryhmät myös saattavat jakaa ja käyttää uudelleen toistensa työkaluja, mikä voi hankaloittaa attribuutiota.

Vakoilu

- Venäjään julkisuudessa liitettyjen kybervakoiluryhmittymien aktiivisuus Euroopassa jatkui toukokuussa.
  - Tietoturvayhtiö Sekoia selvitti Turla-ryhmän keränneen tietoa myös Itävallan keskuskauppakamarin ja Virossa toimivan maanpuolustusoppilaitoksen järjestelmistä osana aiemmin raportoitua operaatiota. Turla yhdistetään julkisuudessa Venäjän FSB:hen.(18)
  - Nobelium (APT29, Cozy Bear) puolestaan on jatkanut kohdistettujen kalasteluviestien lähettämistä eri tyyppisiin kohteisiin. Toukokuun loppupuolella kampanjassa lähetettiin viestejä Microsoftin tietoturvatutkintatiimin mukaan yli 150 organisaatioon. Ryhmä hyödynsi kampanjassa sähköpostimarkkinointialustaa.
- Venäläiset kyberryhmät ovat jatkaneet aktiivisesti hyökkäyksiä myös Ukrainassa.(19)
  - Esimerkiksi Sandworm-ryhmältä havaittiin uusi versio tietojentuhoamisoperaatioihin liittyvästä ArguePatch-haittaohjelmasta, ja Gamaredon-ryhmä puolestaan on jatkanut haitallisten sähköpostiviestien lähettämistä.

Analyysi

- Kohdistettujen kalasteluviestien lähettämiseen tai haitallisen sisällön jakamiseen voidaan hyödyntää myös aitoja palveluita.
- Jos vihamielinen taho onnistuu saamaan pääsyn luotetun toimijan tilille, voi se lähettää viestejä myös luotettujen kumppanien nimissä.

Vakoilu

- Kybervakoilu on ollut aktiivista myös Aasian suunnalla. Tekijät ovat osassa vielä tuntemattomia, mutta osan operaatioista tietoturvatutkijat yhdistävät Kiinaan.
  - Moshen Dragon -nimellä kutsuttu ryhmä on vakoillut aasialaisia teleoperaattoreita. Operaatiossa on hyödynnetty tietoturvaohjelmistojen käyttämien kirjastojen kaappaamista. Ryhmän on havaittu käyttävän erilaisia kiinalaisryhmiin liitettyjä haittaohjelmia (esim. ShadowPad ja PlugX).(20)
  - Override Panda (Naikon, Bronze Geneva) on puolestaan lähettänyt kohdistettuja kalasteluviestejä toistaiseksi tuntemattomalle kohteelle. Uhkatoimijan kohteet ovat historiallisesti painottuneet aasialaisiin valtionhallintoihin.
  - Operation Restylink -kampanjassa pyrittiin vakoilemaan japanilaisia yrityksiä kuluvan vuoden huhtikuusta lähtien ja mahdollisesti jo aiemmin. Operaation taustalla olevasta uhkatoimijasta ei ole varmuutta.(21)
  - Sidewinder-ryhmä on toteuttanut kahdessa vuodessa lähes tuhat hyökkäystä, joiden kohteina ovat pääosin olleet Pakistanin, Bangladeshin ja muiden Etelä-Aasian maiden armeija ja viranomaiset. Maasta, josta käsin ryhmä operoi, ei ole varmuutta.(22)
  - Cisco Talos puolestaan kertoi todennäköisesti Bitter APT:n kampanjasta, joka on ollut käynnissä viime vuoden elokuusta ja kohdistunut Bangladeshin hallintoon. Bitter APT:n arvioidaan olevan eteläaasialainen uhkatoimija, jonka kohteina ovat olleet mm. energia-ala ja valtionhallinnot Kiinassa, Pakistanissa ja Saudi-Arabiassa.(23)

Analyysi

- APT-toimijoiden toiminta seuraa tiiviisti valtioiden intressejä. Tästä syystä ryhmien toiminta voi painottua alueellisesti tiettyihin maihin tai maanosiin, vaikka internet mahdollistaisi hyökkäämisen mihin tahansa päin maailmaa.

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

- Komissio ehdottaa uutta EU-lainsäädäntöä lapsiin kohdistuvan seksuaaliväkivallan torjumiseksi.(24)
  - Asetusehdotuksen mukaan palveluntarjoajien tulee arvioida ja pienentää riskejä sekä tunnistaa verkossa tapahtuva lapsiin kohdistuva seksuaaliväkivalta, ilmoittaa siitä ja poistaa sitä todistava kuvamateriaali.
  - Ehdotuksella perustettavan EU-torjuntakeskuksen tehtävänä on vastaanottaa ja analysoida palveluntarjoajilta tulevia ilmoituksia virheellisten ilmoitusten tunnistamiseksi sekä toimittaa asiaankuuluvat ilmoitukset toimivaltaisille valvontaviranomaisille.
  - Velvoitteet koskevat säilytys- ja henkilöviestintäpalveluja EU:ssa tarjoavia tahoja, sovelluskauppoja sekä internetyhteyden tarjoajia.
  - Ehdotus täydentää digipalveluasetuksella (DSA) käyttöön otettavaa yleistä kehystä.

Oikeudelliset asiat

- Neuvosto hyväksyi EU:n datahallintosäädöksen (DGA).[(25)]
  - Datahallintosäädöksellä edistetään datan liikkumista julkisen ja yksityisen sektorin välillä luomalla raamit datan turvalliselle jakamiselle.
  - Sen tavoitteena on muun muassa:
    - Helpottaa tiettyjen julkisen sektorin hallussa olevien suojattujen datan luokkien uudelleenkäyttöä.
    - Lisätä luottamusta datan välityspalveluihin.
    - Edistää datan vastikkeetonta lahjoittamista eli data-altruismia yleisen edun mukaisiin tarkoituksiin.
  - Uusia sääntöjä sovelletaan 15 kuukauden kuluttua asetuksen voimaantulosta.

Oikeudelliset asiat

- Liikenne- ja viestintäministeriössä valmistellaan lainsäädäntöä viranomaisten yhteistoiminnasta yhteiskunnan kriittisten toimintojen kannalta merkittävissä tietoturvaloukkaustilanteissa.
  - Liikenne- ja viestintäministeriö pyytää lausuntoja luonnoksesta hallituksen esitykseksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain ja henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamiseksi.(26)
  - Lausuntokierros on käynnissä 26.7.2022 asti.
  - Esityksen tavoitteena on muun muassa:
    - Parantaa yhteiskunnan turvallisuutta ja perusoikeuksien, erityisesti luottamuksellisen viestinnän suojan toteutumista.
    - Luoda selkeät edellytykset viranomaisten tiedonvaihdolle vakavien tietoturvaloukkausten selvittämisessä.
    - Keventää virka-apumenettelyn päätöksentekoprosessia Liikenne- ja viestintäviraston osalta.

Oikeudelliset asiat

- EU:n neuvosto ja Euroopan parlamentti alustavaan yhteisymmärrykseen EU:n kyberturvallisuusdirektiivistä (NIS 2 direktiivi).(27)
  - Uusi kyberturvallisuusdirektiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi).
  - Ehdotus tuo yhteiskunnan tietyille kriittisille sektoreille kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoitteet kyberhäiriöistä.
  - Sääntelyn soveltamisala laajenee koskemaan uusia sektoreita ja toimijoita, kuten julkishallintoa, elintarvikealaa ja jätehuoltoa.
  - Direktiivillä perustetaan Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU CyCLONe), jossa Suomea edustaa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus.
  - Direktiivi on tarkoitus julkaista syksyllä 2022.

Oikeudelliset asiat

- Liikenne- ja viestintäviraston määräys 28 viestintäverkkojen ja -palveluiden yhteentoimivuudesta on uudistettu.(28)
  - Operaattoreilla on jatkossa velvollisuus estää soittajan numeron väärentäminen ja huijaussoittojen välittäminen puhelun vastaanottajille.
  - Määräyksen tavoitteena on estää suomalaisten numeroiden käyttö kansainvälisessä tietoverkkorikollisuudessa ja vähentää ulkomailta tulevia huijauspuheluita.
  - Velvoitteet estää väärennettyjen numeroiden käyttö astuvat voimaan asteittain: kiinteän verkon numeroiden osalta 1.7.2022 ja matkapuhelinnumeroiden osalta 2.10.2023.

Oikeudelliset asiat

- Liikenne- ja viestintäviraston uudistettu määräys 72 B sähköisistä tunnistus- ja luottamuspalveluista on julkaistu.(29)
  - Määräys tuli voimaan 1.6.2022. Aikaa toteuttaa tietyt mm. avaintenvaihtoon liittyvät toimenpiteet on 1.6.2023 asti. Käyttäjälle on jatkossa näytettävä tunnistustapahtuman yksilöintitieto sekä tieto palvelusta, johon hän on tunnistautumassa.
  - Lisäksi tietoliikenteen salausvaatimuksia uudistetaan ja tietoliikenteen osapuolten varmistamista vahvistetaan.
- Tiedonhallintolautakunnan antama suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri) on julkaistu.(30)
  - Arviointikriteeristö tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita.
  - Julkria voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Arjen kyberturvallisuus

Pornokiristyksiä runsaasti liikkeellä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten eli "pornokiristys" -huijausviestien lähettelyssä. 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

Tietoturvailmiöt jotka muuttivat maailmaa – videosarja julkaistu

- Uudessa videosarjassamme käydään läpi viisi merkittävää kybertapausta viime vuosikymmeneltä.
- Lue lisää ja katso videot: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvailmiot-jotka-muuttivat-maailmaa

Kyberturvallisuus rakennetaan yhteistyöllä

- Suomen poliisi on osallistunut kansainväliseen, Europolin koordinoimaan operaatioon, jossa ajettiin alas poikkeuksellisen vakavia tuhoja aiheuttanut Flubot-vakoiluhaittaohjelma.
- Lue lisää: https://poliisi.fi/-/tekstiviestihuijausten-takana-ollut-flubot-vakoiluhaittaohjelma-ajettiin-alas-viranomaisyhteistyolla

Uutisia Kyberturvallisuuskeskuksesta

Uusi ohje auttaa kiristyshaittaohjelman kohteeksi joutunutta organisaatiota

- Riski kiristyshaittaohjelman kohteeksi joutumisesta on kasvanut viime vuosina merkittävästi.
- Uusi ohjeemme antaa neuvoja tilanteessa, jossa kiristyshaittaohjelma uhkaa organisaation toimintaa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-ohje-auttaa-kiristyshaittaohjelman-kohteeksi-joutunutta-organisaatiota

Harjoitusten ja yhteistoiminnan merkitys korostuu kyberturvallisuudessa

- Kyberturvallisuuteen kohdistuvat uhat ja häiriöt herättävät juuri nyt paljon mielenkiintoa.
- Kyberturvallisuuskeskuksen ylijohtaja Sauli Pahlman korostaa yhteistoiminnan merkitystä kyberhäiriötilanteisiin varautumisessa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/harjoittelu-viimeistelee-varautumisen

Kyberharjoitusten skenaariopankki - apua harjoitussisällön suunnitteluun

- Uusi kyberharjoitusten skenaariopankki -palvelumme sisältää aiemmin julkaistuja ja uusia skenaarioideoita kyberharjoituksen suunnittelun tueksi.
- Skenaariopankin tarkoitus on helpottaa harjoituksen ideointia ja sisällön suunnittelua.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberharjoitusten-skenaariopankki-apua-harjoitussisallon-suunnitteluun

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) Isac-tiedonvaihtoryhmät https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

2) Verohallinnon tiedote huijausviesteistä https://www.vero.fi/tietoa-verohallinnosta/uutishuone/lehdist%C3%B6tiedotteet/2022/verohallinnon-nimiss%C3%A4-liikkuu-edelleen-huijaustekstiviestej%C3%A4---tuhoa-viesti-ilmoita-oma-tilinumero-omaverossa/

3) Poliisin tiedote FluBotista https://poliisi.fi/-/tekstiviestihuijausten-takana-ollut-flubot-vakoiluhaittaohjelma-ajettiin-alas-viranomaisyhteistyolla

4) Ohje kiristyshaittaohjelman kohteeksi joutuneelle organisaatiolle https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-ohje-auttaa-kiristyshaittaohjelman-kohteeksi-joutunutta-organisaatiota

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

6) Palo Alto Networks haavoittuvuustiedote https://unit42.paloaltonetworks.com/cve-2022-1388/

7) Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

8) Tietoturvamerkki www.tietoturvamerkki.fi

Lähdeluettelo

9) Mandiant: UNC3524: Eye Spy on Your Email https://www.mandiant.com/resources/unc3524-eye-spy-email

10) Suojelupoliisi: Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun https://supo.fi/-/ulkomaiset-tiedustelupalvelut-kayttavat-yritysten-ja-yksityishenkiloiden-verkkoreitittimia-kybervakoiluun

11) Kyberturvallisuuskeskuksen Kybermittari https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

12) Kyberturvallisuuskeskuksen materiaaleja kriittisen infran turvaamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/materiaaleja-kriittisen-infran-turvaamiseen

13) Yle: Venäjä ei murtanut Ukrainan selkärankaa eikä sen nettiyhteyttä https://yle.fi/uutiset/3-12439958

14) Kybersää, huhtikuu 2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20huhtikuu%202022.pdf

15) The Record: Researchers uncover years-long espionage campaign targeting dozens of global companies https://therecord.media/operation-cuckoobees-apt41-cybereason-winnti-group

16) Bleepingcomputer: Chinese 'Space Pirates' are hacking Russian aerospace firms https://www.bleepingcomputer.com/news/security/chinese-space-pirates-are-hacking-russian-aerospace-firms/

Lähdeluettelo

17) Check Point Research unveils a Chinese APT espionage campaign against Russian state-owned defense institutes https://blog.checkpoint.com/2022/05/19/twisted-panda-check-point-research-unveils-a-chinese-apt-espionage-campaign-against-russian-state-owned-defense-institutes/

18) Bleepingcomputer: Russian hackers perform reconnaissance against Austria, Estonia https://www.bleepingcomputer.com/news/security/russian-hackers-perform-reconnaissance-against-austria-estonia/

19) Cybersecurityhelp: Russia-linked Armageddon APT using occupied Kherson as a lure in attacks targeting Ukraine https://www.cybersecurity-help.cz/blog/2643.html

20) Security Affairs: China-linked Moshen Dragon abuses security software to sideload malware http://securityaffairs.co/wordpress/130851/apt/moshen-dragon-targets-telcos.html

21) NTT: Operation RestyLink: APT campaign targeting Japanese companies https://insight-jp.nttsecurity.com/post/102hojk/operation-restylink-apt-campaign-targeting-japanese-companies

22) The Register: APT gang 'Sidewinder' goes on two-year attack spree across Asia https://www.theregister.com/2022/05/12/sidewinder_apt_attack_spree/

23) Talos: Bitter APT adds Bangladesh to their targets https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

Lähdeluettelo

24) Euroopan komissio: Lapsiin kohdistuvan seksuaaliväkivallan torjunta: Komissio ehdottaa uusia sääntöjä lasten suojelemiseksi https://ec.europa.eu/commission/presscorner/detail/fi/ip_22_2976

25) Eurooppa-neuvosto: Neuvostolta datahallintosäädös https://www.consilium.europa.eu/fi/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/

26) Lausuntopyyntö luonnoksesta hallituksen esitykseksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain ja henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=9075c982-8f70-417c-a428-535c126cb0f7

27) Eurooppa-neuvosto: Vahvempi kyberturvallisuus ja häiriönsietokyky koko EU:hun – neuvoston ja Euroopan parlamentin alustava yhteisymmärrys https://www.consilium.europa.eu/fi/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

28) Traficom ja suomalaiset teleoperaattorit yhteistyössä numeron väärentämistä vastaan asiakkaiden eduksi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-ja-suomalaiset-teleoperaattorit-yhteistyossa-numeron-vaarentamista-vastaan

29) Traficom: sähköinen tunnistaminen https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

30) Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) https://julkaisut.valtioneuvosto.fi/handle/10024/164183