TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 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

12.5.2022

Kybersää huhtikuu 2022

Tietomurrot ja -vuodot

- Kuntien ja kaupunkien sähköpostitileille on murtauduttu ja tileiltä on lähetetty runsaasti kalasteluviestejä.
- Sosiaalisen median tileihin kohdistuu edelleen tietomurtoja ja niiden yrityksiä.

Huijaukset ja kalastelut

- Fenton-huijauksissa lähetettiin tuhansittain valheellisia työtarjouksia ja houkuteltiin pyramidihuijaukseen.
- Wallpaperga-huijausviesteissä uhri huijataan klikkaamaan linkkiä, jolla perutaan maksullinen tilaus.

Haittaohjelmat ja haavoittuvuudet

- Kyberturvallisuuskeskus on jälleen saanut muutamia havaintoja Emotet-haittaohjelmasta.
- Tekstiviestien välityksellä leviävä FluBot-mobiilihaittaohjelma on aktivoitunut jälleen Suomessa.

Automaatio ja IoT

- Nähtävissä on useita merkkejä, että kyberhyökkäykset automaatiojärjestelmiin tulevat lisääntymään.
- Älykkäiden valaistusjärjestelmien valmistaja meni konkurssiin - käyttäjät eivät pysty enää säätämään valojaan.

Verkkojen toimivuus

- Kahdeksan merkittävää vikaa.
- Verkot toimivat edelleen normaalisti ja tilanne on hyvä.
- Palvelunestohyökkäykset valtionhallintoon puhuttivat.

Vakoilu

- Kyberhyökkäysten määrä on Ukrainassa moninkertaistunut sodan aikana. Myös teollisuusautomaatio on hyökkäysten kohteena.
- Lukuisat APT-ryhmät ovat huhtikuussa jatkaneet länsimaihin kohdistuvaa vakoilua. Ryhmät hyödyntävät vakoilussa muun muassa Ukrainan sotaa.

TRAFICOM

12.5.2022

Kuukauden tunnuslukuja

8.4

Palvelunestohyökkäys vaikutti usean valtionhallinnon verkkosivun saatavuuteen.

1

Saimme ensimmäiset ilmoitukset Flubot-haittaohjelman aktivoitumisesta ja julkaisimme siitä keltaisen varoituksen, joka edellyttää käyttäjiltä yleistä varovaisuutta.

49

Digi- ja väestötietoviraston sekä Kyberturvallisuuskeskuksen yhteisessä pilottiprojektissa kartoitettiin haavoittuvuuksia yhteensä 49 kunnan ja sote-toimijan julkisessa verkossa sijaitsevista järjestelmistä ja digitaalisista palveluista. Havainnot toimitettiin kunnille ja sote-toimijoille, jotka pystyivät tietojen perusteella tekemään korjaavia toimenpiteitä.

Julkaisimme varoituksen 1/2022 FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse

- Julkaisimme keltaisen varoituksen 10.5.2022.
- FluBot-haittaohjelmakampanja on aktivoitunut jälleen. Kyberturvallisuuskeskus on vastaanottanut runsaasti ilmoituksia aiheesta.
- Haittaohjelma on kohdistettu Android-laitteille. Haittaohjelman tarkoitus on varastaa tietoja laitteelta ja sitä levitetään tekstiviestien ja multimediaviestien kautta.
- Viestin teemana voi olla esimerkiksi saapunut ääniviesti, vastaamaton puhelu tai ilmoitus saapuneesta lähetyksestä. Viestissä käyttäjää pyydetään avaamaan linkki.
- Huijausviesteissä olevia linkkejä ei tule avata. Pelkkä linkin avaaminen ei vielä asenna haittaohjelmaa laitteelle.
- Lue lisätietoja ja tarkemmat ohjeet: https://www.kyberturvallisuuskeskus.fi/fi/varoitus_1/2022

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

12.5.2022

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

Mahdollisen 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.(2)

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

- Useilla sektoreilla on tapahtunut normaalia sähköpostitilien tietomurtoja tai niiden yrityksiä.
  - Kyberturvallisuuskeskukselle on ilmoitettu huhtikuun aikana normaalia enemmän sähköpostitilien tietomurtoja tai niiden yrityksiä.
  - Sektoreissa ovat korostuneet julkishallinto ja etenkin kunta-alan toimijoilta tulleet ilmoitukset.
  - Murrettuja tilejä on voitu väärinkäyttää kalasteluviestien lähettämiseen.

Analyysi

- Netissä on tarjolla palveluita, joiden avulla voi selvittää, ovatko omat tiedot päässeet vuotamaan.
- Palveluun voi syöttää sähköpostiosoitteensa, sitten sitä etsitään listoilta, joille on kerätty vuotaneita tietoja.
- Mikäli oma sähköposti löytyy tällaiselta listalta on tärkeää vaihtaa palvelun salasana viipymättä ja varmistaa, että samaa salasanaa ei ole käyttänyt muissa palveluissa.
- Monivaiheisen tunnistautumisen käyttöönotto parantaa merkittävästi myös sähköpostitilien suojausta.

Tietomurrot ja –vuodot

- Sosiaalisen median tilit tietomurtojen kohteena.
  - Yksityisten kansalaisten, yrittäjien ja yritysten Facebook- ja Instagram-tilejä on aktiivisesti kalasteltu ja kaapattu.
  - Organisaatioiden olisi hyvä muistuttaa työntekijöitään ottamaan käyttöön monivaiheinen tunnistautuminen myös työn ulkopuolisissa asioissa.(5)
  - Työntekijän tilillä saatetaan myös hallinnoida organisaation virallista tiliä.

Analyysi

- Murrettuja sosiaalisen median tilejä voidaan käyttää petoksen tekemiseen tai johtamaan muita ihmisiä harhaan.
- Kaupallisessa käytössä olevat tilit, joilla on paljon seuraajia voivat joutua rikollisten kiinnostuksen kohteeksi myös taloudellisten motiivien vuoksi.
- Omia tunnuksia tai salasanoja ei tulisi luovuttaa muiden käyttöön. Myös monivaiheinen tunnistautuminen on tärkeä turvallisuutta parantava ominaisuus.

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

- Pankkikalastelua liikkeellä.
  - Pankkitunnuksia on kalasteltu jälleen kaikkien kotimaisten liikepankkien nimissä.
  - Turvapostiksi väärennettyjä kalasteluviestejä on lähetetty mm. OmaSP:n nimissä.
  - Edelleen suuri osa kalasteluviesteistä lähetetään sähköpostilla, mutta myös tekstiviesteillä on kasvava rooli pankkikalasteluviesteissä.
  - Kanta-palvelun etsiminen Bing-hakukoneesta on johtanut etsijän pankkitunnusten kalastelusivulle.

Analyysi: Toimitusjohtajahuijauksia

- Toimitusjohtajahuijauksia on kohdistettu jälleen erilaisiin organisaatioihin oppilaitoksista pörssiyrityksiin.
- Ulkomaalaisen yhteistyökumppanin murrettua sähköpostitiliä oli käytetty väärennetyn huijauslaskun lähettämiseen.
- Riittävän pieniä laskutuseriä on katsottu läpi sormien ja hyväksytty normaalin laskutuskäytännön vastaisesti.
- Suoranaisten valelaskujen lisäksi uhreja pyydetään ostamaan lahjakortteja.

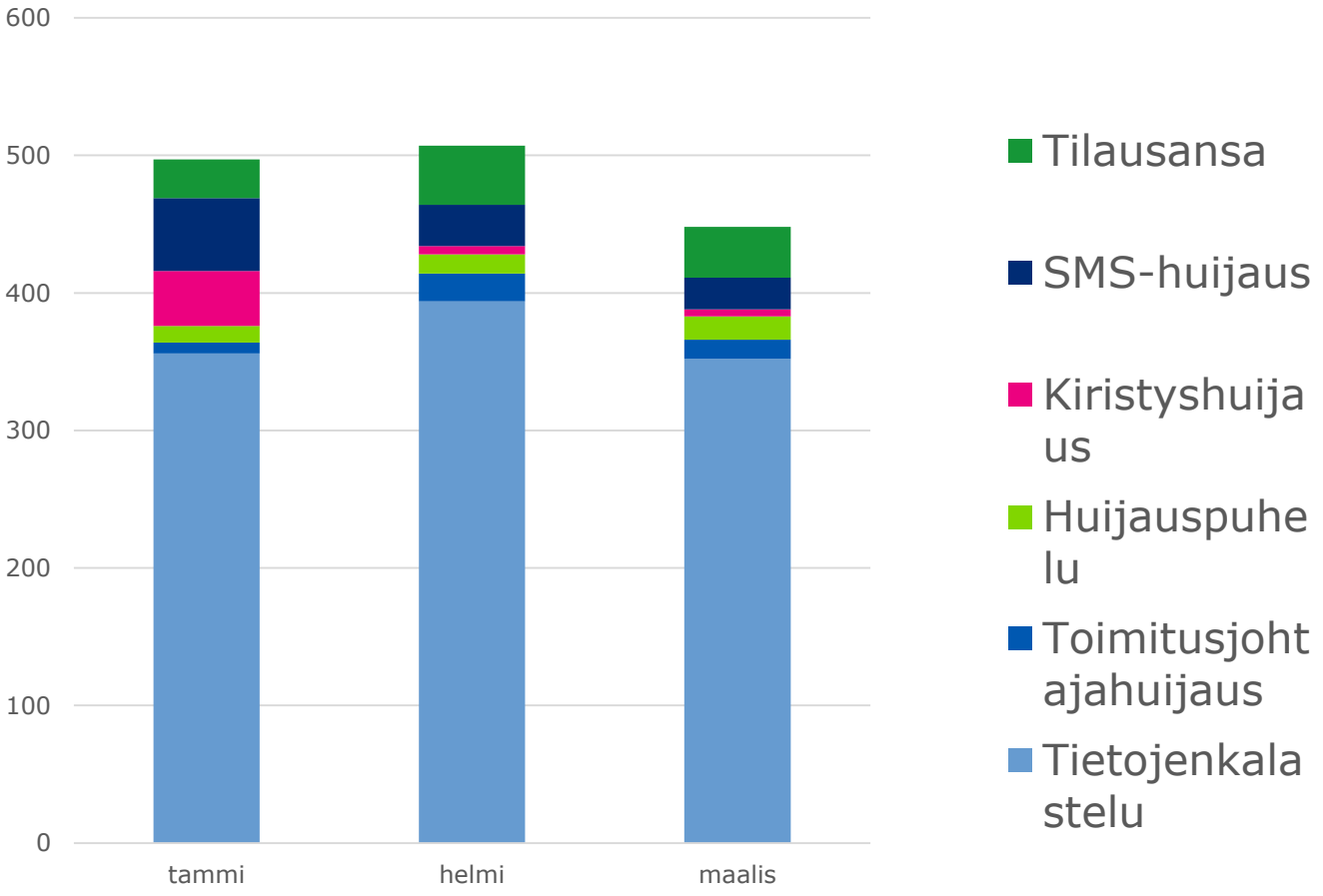
Huijaukset ja kalastelut

- Tekstiviestiepidemia työtarjousteemalla.
  - Huhtikuun alkupuolella suomalaisten puhelimiin alkoi sadella viestejä, joissa kerrottiin osa- ja kokoaikaisesta työstä.
  - Viesti mainostaa työtä jolla voisi ansaita 10-200 euroa päivässä.
  - Huijausviestejä saattoi tulla WhatsAppilla, iMessagella tai muulla viestisovelluksella.
  - Viestiin vastaamalla pääsi juttelemaan ilmeisen hyvin tehdyn automaatin kanssa, joka antoi uhrille rekisteröitymislinkin.
  - Rekisteröitymissivulla kysyttiin puhelinnumeroa ja uhri otettiin mukaan pyramidihuijaukselta vaikuttavaan palveluun puhelinsovelluksen avulla.

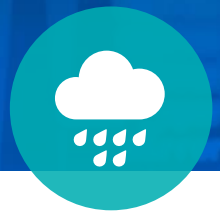
Analyysi: tilausvahvistushuijauksia

- Tilausvahvistukseksi väärennettyjä tekstiviestejä on lähetetty puhelimiin tuhatmäärin. Tarkoituksena on säikyttää uhri klikkaamaan linkkiä ja muka perumaan tilaus.
- Viestissä väitettiin, että henkilö oli tilannut 50 euron hintaisen kuukausilaskutettavan Wallpaperga-taustakuvapalvelun.
- Huijausviestissä kerrotun peruutuslinkin takana saattoi olla haittaohjelman latauspalvelu.
- Peruutuslinkki on yksi keino useiden joukossa, jolla yritetään saada vastaanottaja haitalliselle sivustolle.

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.

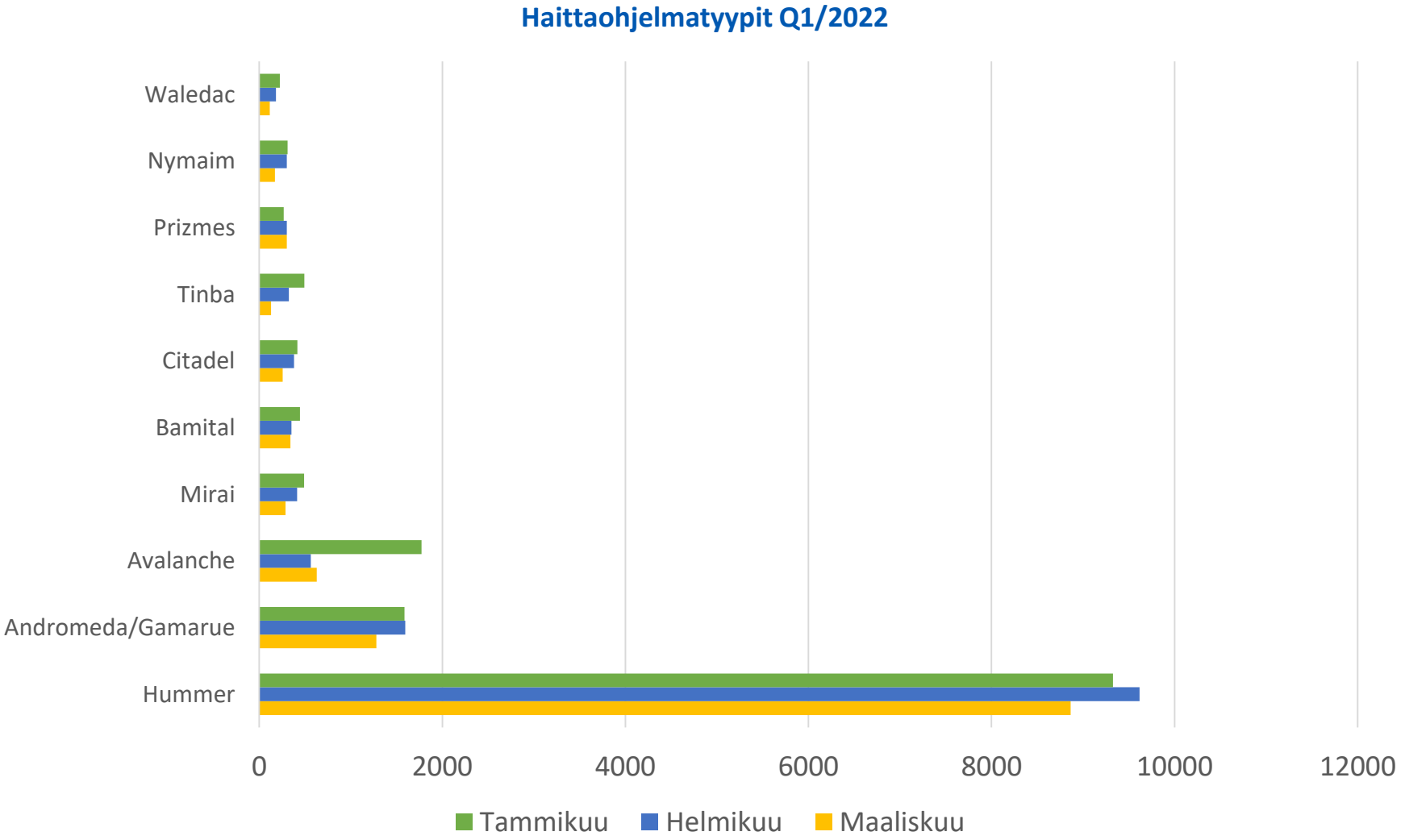
Haittaohjelmat

- Emotet on aktivoitunut uudelleen.
  - Kyberturvallisuuskeskus on jälleen saanut muutamia havaintoja Emotet-haittaohjelmasta.
  - Emotet-haittaohjelma leviää sähköpostitse. Se varastaa työasemalta tietoja, sähköposteja, yhteystietolistoja, salasanoja, maksutietoja ja muuta dataa.
  - Toistaiseksi tapausmäärät ovat pysyneet maltillisina, eikä Emotet vaikuta Suomessa vielä kovin vahvasti.

Analyysi

- Emotet levisi aiemmin vuonna 2020, jolloin sen toiminta hetkellisesti lakkasi, koska haittaohjelmaverkosto otettiin haltuun kansainvälisessä viranomaisoperaatiossa.
- Nyt näyttää siltä, että rikolliset ovat onnistuneet aloittamaan toimintansa uudelleen.
- Emotet voi ladata työasemalle esim. kiristyshaittaohjelman. Haittaohjelmaa on levitetty aikaisemmin myös suomalaisten organisaatioiden nimissä.

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.(6)

Haavoittuvuus

- Yhdysvaltain tietoturvaviranomainen CISA ylläpitää Shields Up –sivustoa[7], jolla on mm. hyväksikäytettyjen haavoittuvuuksien lista.
  - Listalla on yli 600 haavoittuvuutta.
  - Listalla olevat haavoittuvuudet ovat sellaisia, joiden hyväksikäyttötapauksia on havaittu.
  - Listaa päivitetään usein ja vanhin haavoittuvuus listalla on vuodelta 2008.

Analyysi

- CISA on todennut, että organisaatioiden tulisi olla nyt erityisen valppaina kyberympäristössä toimiessaan.
- Sivustolla on paljon ohjeita ja työkaluja, joilla organisaatioita pyritään avustamaan oman turvallisuuden ja varautumisen parantamisessa.
- Rikollisen tahon hyödyntämät haavoittuvuudet ovat usein vanhoja jo tiedossa olevia, mutta paikkaamattomia haavoittuvuuksia.

Kuukauden haavoittuvuusjulkaisut

- Oraclen Java-ohjelmistokirjastossa kriittinen haavoittuvuus (7/2022).
  - Vaikuttaa siltä, että haavoittuvien kohteiden löytäminen vaatii rikollisilta vaivannäköä.
  - Haavoittuvuus mahdollistaa allekirjoituksen tarkastuksen ohittamisen.
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

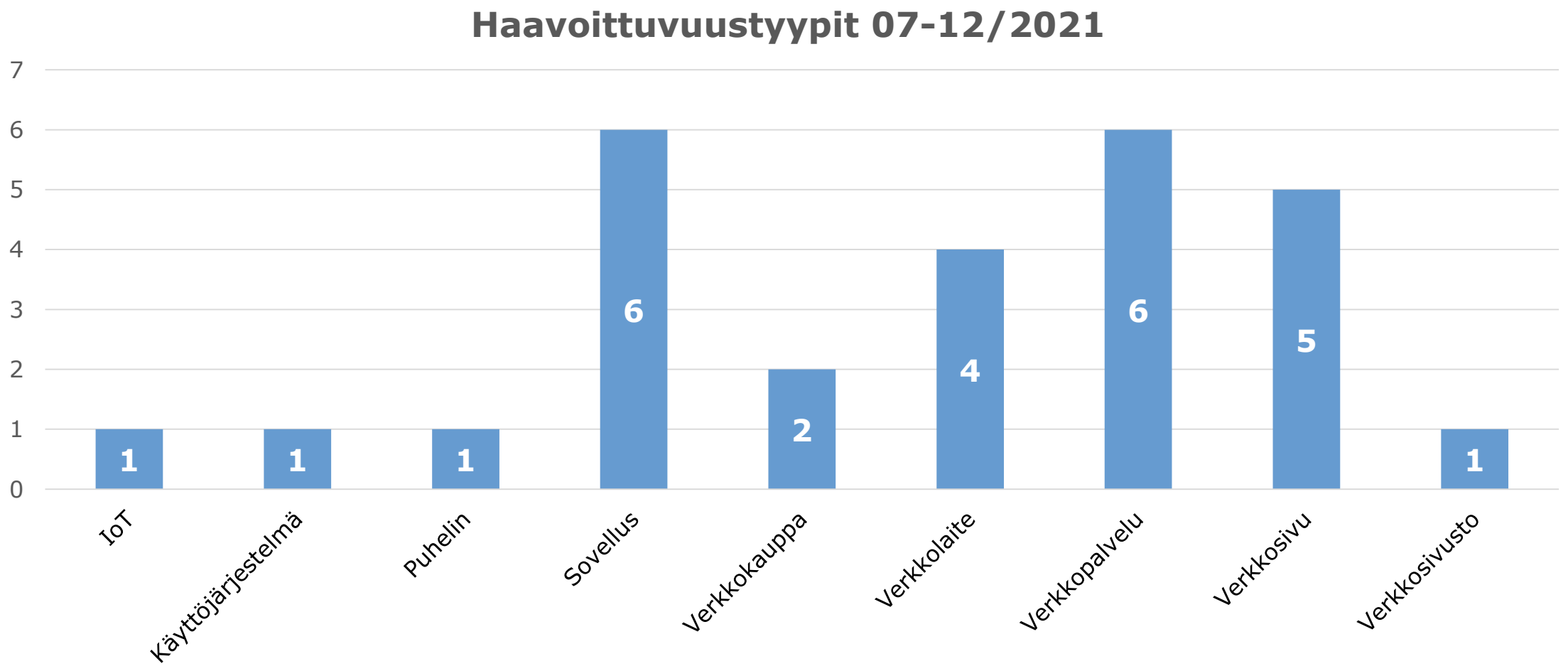
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **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 7 kpl (tilanne 10.5.2022).**
  - 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

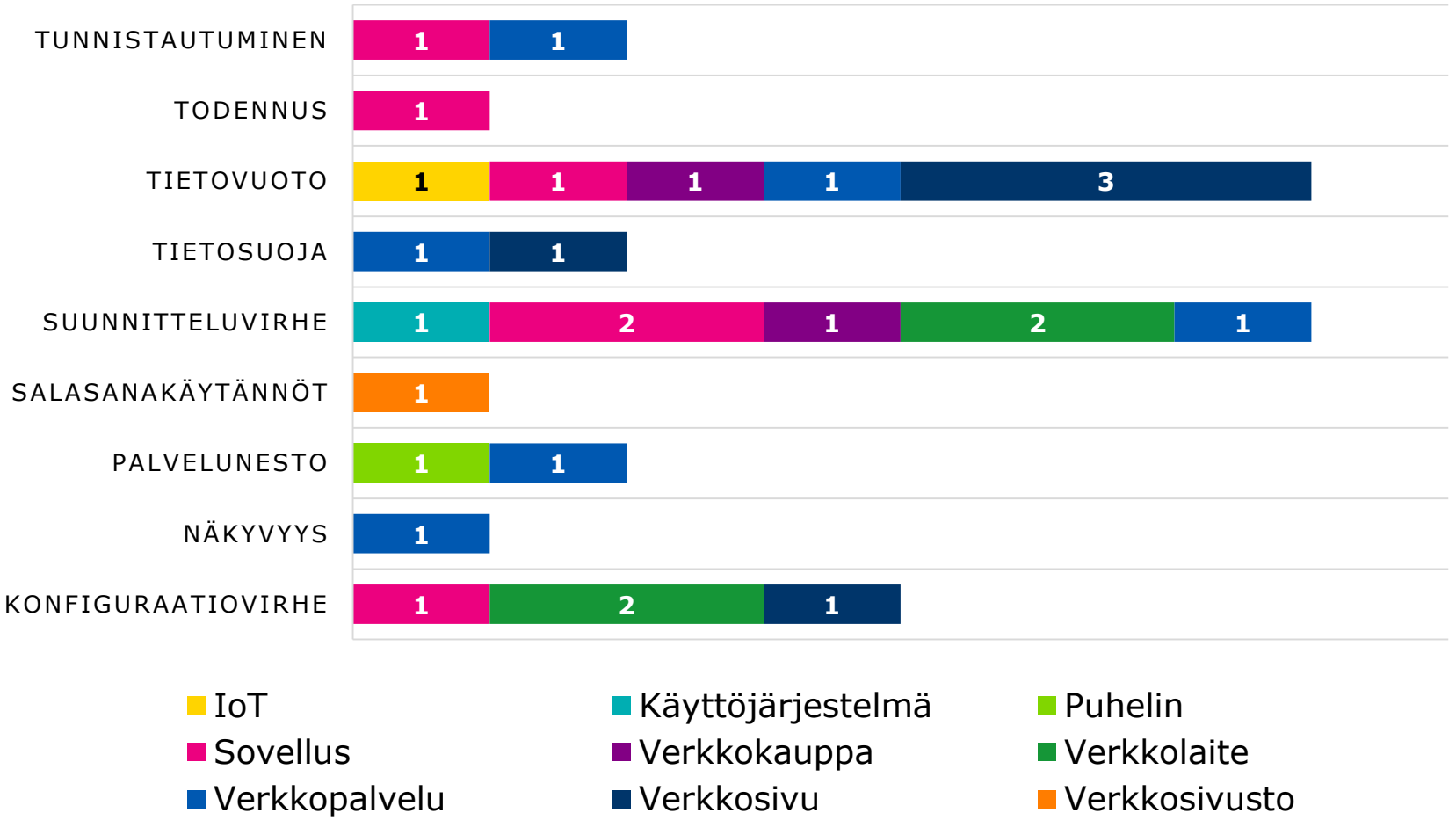
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat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

Haavoittuvuuskoordinaatiota on esitelty laajemmin verkkosivuillamme.(8)

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

- Kriittisen infrastruktuurin käyttämiin automaatiolaitteisiin suoraan kohdistettuja haittaohjelmia on havaittu vuoden 2010 Stuxnet-tapauksen jälkeen verrattain vähän.
- Tuoreiden havaintojen perusteella suoraan automaatiojärjestelmiin suunnatut kyberuhat olisivat kuitenkin lisääntymässä.(9)
  - FBI varoitti aiemmin keväällä, että kyberrikolliset kehittävät suoraan automaatioympäristöihin suunnattuja haittaohjelmia.
  - Ukraina ilmoitti torjuneensa maassa kahden miljoonan ihmisen sähkönjakeluun kohdistetun automaatiohyökkäyksen, jossa yritettiin käyttää Industroyer.v2 -haittaohjelmaa.(10)
  - Tietoturvayritykset ilmoittivat löytäneensä joukon työkaluja, jotka helpottavat kyberoperaatioita eri valmistajien automaatioympäristöissä. Ne mahdollistavat myös näiden ympäristöjen turvajärjestelmiin vaikuttamisen vaarantaen siten pahimmillaan myös ihmisten turvallisuuden.

Analyysi

- Aiemmin myös kriittisen infrastruktuurin organisaatioiden tietoturvapoikkeamat ovat lähes poikkeuksetta kohdistuneet näiden perustietotekniikkaan.
- Automaatioympäristöjen monimutkaisuus ja yksilölliset ratkaisut ovat saattaneet suojata niitä, koska kyberrikolliset ovat saaneet saman tuoton helpommin toimistoympäristöistä.
- Tilanteessa on nähtävissä nyt muutoksen merkkejä kriittisen infrastruktuurin merkityksen korostuessa geopoliittisten jännitteiden lisääntymisen myötä.
- Eri maiden asevoimat panostavat nyt myös voimakkaasti kriittiseen infrastruktuuriin suunnattujen kyberaseiden kehittämiseen.(11)

IoT

- IoT-alustan tarjoajan turvallisuus vaikuttaa käyttäjän turvallisuuteen.
  - Valaistuksen ohjaus- ja muita älytuotteita koteihin kehittävä Insteon meni konkurssiin eivätkä käyttäjät voi enää ohjata ostamiaan laitteita.(12) (13)
  - Ruotsissa hälytysjärjestelmiä ja -palveluita myyvän Verisuren työntekijöiden epäillään salakatselleen asiakkaita kotien turvakameroilla.(14)

Analyysi

- IoT-laitteet ja -palvelut sulautuvat osaksi päivittäistä elämäämme.
- Monissa tuotteissa käytetään pilvipalveluita. Niihin liittyvät käytännöt eivät useinkaan ole kuluttajan arvioitavissa tai kuluttajat eivät ymmärrä etsiä asioista tietoa.
- Valmistajien ja myyjien tulisi kertoa käyttäjille turvallisuudesta ja tietosuojasta proaktiivisesti.
- Katso Kyberturvallisuuskeskuksen neuvot pilvipalveluiden turvallisuuteen yksityishenkilöille, pienyhteisölle ja yrityksille.(15)
- Microsoft on julkaissut neuvoja IoT:n valmistajille ja käyttäjäorganisaatioille.(16)

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

- Huhtikuussa yleisissä viestintäpalveluissa oli 8 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 1, C: 7
- Häiriöiden syinä olivat mm. kaapelikatko, ohjelmistovirhe, laitevika ja sähkökatko.
  - Muutamat vioista kestivät useita tunteja, mutta vakavimmilta vaikutuksilta vältyttiin.
  - Sääilmiöt eivät vaikuttaneet verkkojen toimivuuteen tässä kuussa.
- Verkkojen toimivuus Suomessa on tällä hetkellä hyvä.
- Ranskassa katkottiin tärkeitä kuitukaapeleita presidentinvaalien jälkeen.(17)

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa oli vuonna 2022 keskimäärin hyvä.
- Kuukaudessa on keskimäärin noin kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat meille, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

ICT-palveluiden toimivuus

- Verkkohäiriö aiheutti ongelmia turvapuhelinten toimintaan. Turvapuhelimia käytetään esimerkiksi senioreiden tai muiden ulkopuolista apua tarvitsevien henkilöiden arjessa.
  - Verkkohäiriön vaikutukset turvapuhelinten kaltaisiin palveluihin voivat olla vakavia, mikäli laitteen toiminta estyy häiriön vuoksi.
- Erilaiset tekniset ongelmat eri pankkien palveluissa ovat nousseet otsikoihin viime aikoina.
  - Palvelunestohyökkäykset 8.4. valtionhallinnon verkkosivuille ja taannoinen pitkä Nordean palvelunestohyökkäyksen aiheuttama katko nostavat tällä hetkellä erilaiset häiriöt mediaan.
  - Erilaiset tekniset ongelmat ovat eri aloilla arkipäivää. Mikäli organisaatio, palveluntarjoaja tai viranomainen ei indikoi kyseessä olevan palvelunestohyökkäys – on spekulointi turhaa.

Analyysi

- Erilaiset verkkohäiriöt ja toimimattomat palvelut kotimaassa nousevat tänä vuonna esille entistäkin näkyvämmin.
  - Ihmiset ovat kiinnostuneita kyberturvallisuudesta etenkin, kun jokin meni pieleen tai palvelu ei toimi.
  - Näinä aikoina jokainen toimimaton palvelu tai erikoinen poikkeama osoitetaan herkästi ilkeämielisen tahon suorittamaksi.

Palvelunestohyökkäykset

- Palvelunestohyökkäyksiä valtionhallintoon 8.4.
  - Hyökkäykset vaikuttivat hetkellisesti esimerkiksi puolustus- ja ulkoministeriön sivujen toimivuuteen aiheuttaen runsaasti medianäkyvyyttä.
  - Kyseisenä iltapäivänä Ukrainan presidentti Volodymyr Zelenskyi piti eduskunnalle puheen, joka aiheutti spekulaatiot palvelunestohyökkäysten ajankohdasta ja tarkoitusperistä.
  - ” – Palvelunestohyökkäykset ovat ehkä internetissä kaikkein tavanomaisimpia hyökkäyksiä, jotka on vieläpä todella helppo toteuttaa. Se, että aiheutetaan ikään kuin virtuaalinen liikenneruuhka, ei vaadi teknisesti paljoa.”(18)
  - Valtori tiedotti torjuneensa onnistuneesti palvelunestohyökkäyksiä samana päivänä.(19)

Analyysi

- Huhtikuun palvelunestohyökkäykset valtionhallintoon olivat näyttävä tapa aiheuttaa medianäkyvyyttä Suomessa, koska samaan aikaan Ukrainan presidentti piti odotettua puheenvuoroa eduskunnassa.
  - Palvelunestohyökkäykset ovat halpoja ja helppoja toteuttaa - ja onnistuvatkin tarkoituksessaan mikäli sivustot tai palvelut ovat pois käytöstä hetkellisesti.
- Suomessa organisaatiot ovat tunnistaneet palvelunestohyökkäykset riskiarvioissaan ja suojautuvat niihin esimerkiksi operaattoreiden tarjoamilla suodatuspalveluilla.
  - Tällöin palvelunestohyökkäys tunnistetaan automatisoidusti ja haitallinen liikenne ohjataan nopeasti roskakoriin.

Palvelunestohyökkäykset

- Ilmoituksia ilkivaltaisista palvelun häiritsemisistä.
  - Hajautettujen palvelunestohyökkäysten (DDoS) lisäksi saamme ilmoituksia erilaisista tapauksista, joissa pyritään vaikuttamaan palvelun saatavuuteen tai käytettävyyteen eri tavoin.
  - Kyberturvallisuuskeskus vastaanottaa säännöllisesti ilmoituksia, joissa esimerkiksi erilaisia tilauslomakkeita tai palautelaatikoita on käytetty väärin ja organisaatio vastaanottaa massoittain viestejä tämän vuoksi.
- Haktivismi on nostanut päätään tänä keväänä palvelunestohyökkäyksiinkin liittyen.
  - On mahdollista, että konfliktialueen ulkopuolellekin osuu esimerkiksi Killnet-ryhmittymän hyökkäyksiä.
  - Internet sodankäyntialustana on globaali, joten jokaisen organisaation tulee varautua välillisiin vaikutuksiin erilaisissa tietoturvapoikkeamissa.
  - Olemme myös nähneet hyökkäyksiä palveluntarjoajien suuntiin, jotka eivät näy loppukäyttäjälle.

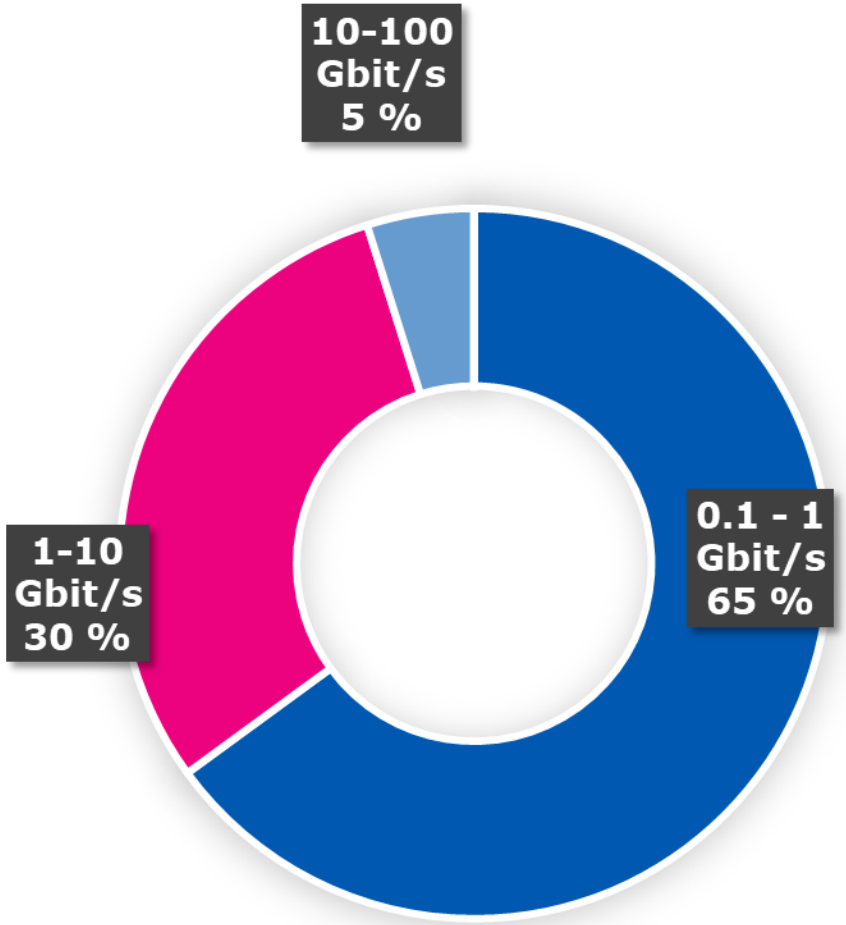
Analyysi

- Palvelunestohyökkäyksiä tapahtuu koko ajan eri puolilla. Niihin varaudutaan ja niitä torjutaan päivittäin.(20)
- Kyberympäristön luonteesta johtuen hyökkäyksen taustalla olevan toimijan osoittaminen on usein vaikeaa.
- Palvelunestohyökkäyksiä tapahtuu vuosittain pelkästään Suomessa kymmeniä tuhansia ja ne ovat arkipäivää. Tämän vuoksi organisaatioiden tulee varautua hyökkäyksiin osana päivittäistä toimintaansa ja riskienhallintaa.

Palvelunestohyökkäysten tunnuslukuja

3kk

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



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q1/2022 - tilasto päivitetään kvartaaleittain.)

Vakoilu

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

Vakoilu

- Ukrainan viranomaisten mukaan sodan aikana kyberhyökkäyksiä on tullut kolminkertainen määrä verrattuna edellisvuoden vastaavaan ajanjaksoon.
- Microsoft on havainnut Ukrainassa tänä vuonna lähes 40 tietojen tuhoamiseen pyrkivää hyökkäystä.
- Useimmissa tiedossa olevissa hyökkäyksissä on käytetty hyväksi jo aiemmin tehtyä tunkeutumista tai anastettuja käyttöoikeuksia.
- Tiedotusvälineisiin kohdistuneissa tietomurroissa tietojärjestelmissä olevia tietoja on muokattu väärän tiedon levittämiseksi.
  - Sisällön muokkaamista ei ole ennen nähty tässä laajuudessa.

Analyysi

- Etsimällä järjestelmistä merkkejä tunkeutumisesta tai jalansijan hankkimisesta, on mahdollista estää myöhemmin toteuttavaksi aiottuja kyberhyökkäyksiä.
- Kyberturvallisuuskeskus on aiemmin tänä vuonna julkaissut ohjeen kyberturvallisuuden vahvistamisesta suomalaisissa organisaatioissa.(1)

Vakoilu

- Teollisuusautomaatiojärjestelmien toimintaa häiritsemään pyrkivistä haittaohjelmista tehdään maailmalla säännöllisesti havaintoja.
- Ukrainan sodan yhteydessä on tunkeuduttu myös kriittisen infrastruktuurin kohteisiin. Tavoitteena on ollut esimerkiksi sähkönjakelun häiritseminen.
  - Huhtikuussa havaittiin esimerkiksi INDUSTROYER.v2-haittaohjelma, jolla pyrittiin ESET:n tutkijoiden mukaan häiritsemään ukrainalaisen energiayhtiön toimintaa. Haittaohjelmalla oli kyvykkyys vaikuttaa myös teollisuusautomaatiojärjestelmiin.(10)
  - Lisäksi automaatiojärjestelmiin kohdistetun INCONTROLLER-haittaohjelman kohteena olivat ainakin tietyt Schneider Electricin ja Omronin automaatioprosessien ohjaamiseen käytetyt PLC-tietokoneet.
- Myös Yhdysvaltojen tietoturvaviranomainen CISA, NSA ja FBI varoittivat teollisuusautomaatio- ja ohjausjärjestelmiin (SCADA) kohdistuvista kyberuhista.
- Lisäksi mm. Yhdysvallat, Australia, Kanada, Uusi-Seelanti ja Britannia ovat kannustaneet kriittisen infrastruktuurin organisaatioita varautumaan kohonneeseen kyberuhkaan.

Analyysi

- Vihamieliset toimijat voivat pyrkiä horjuttamaan yhteiskunnan toimintaa ja esimerkiksi kansalaisten luottamusta yhteiskuntaan häiritsemällä kriittisen infrastruktuurin toimintaa ja palveluita. Palvelut voivat olla houkuttelevia kohteita myös kiristyshaittaohjelmille.
- Kriittisen infrastruktuurin toimintojen lamauttamisella olisi laajat seuraukset yhteiskunnassa, jos sitä ei pystyttäisi ajoissa havaitsemaan ja joko estämään tai pysäyttämään.

Vakoilu

- Useat eri APT-ryhmät, jotka on julkisuudessa yhdistetty Venäjään, ovat huhtikuussa jatkaneet länsimaihin kohdistuvia kybervakoiluoperaatioitaan.
- Esimerkiksi Googlen Threat Analysis Group (TAG) -analyysiyksikkö kertoi muun muassa Turlan ja Calliston aktiivisuudesta huhtikuussa.
  - Google TAG:n mukaan Turla on jatkanut aktiivista toimintaansa Baltiassa. Muun muassa TAG:n Venäjän FSB:hen yhdistämä APT-ryhmä oli lähettänyt haitallisia sähköpostiviestejä kohteinaan puolustus- ja tietoturvaorganisaatiot.
  - Callisto-ryhmä, johon TAG viittaa nimellä COLDRIVER, puolestaan on jatkanut tunnuskalasteluun tähtäävien sähköpostiviestien lähettämistä valtion- ja puolustushallinnon virkamiehille, poliitikoille, ajatushautomoille ja kansalaisjärjestöille sekä toimittajille.
- APT29/NOBELIUM on puolestaan pyrkinyt vakoilemaan diplomaattiorganisaatioita esiintyen viesteissään lähetystöinä.
  - Ryhmä on pyrkinyt välttämään havaituksi tulemista muun muassa käyttämällä tunnettuja palveluita, kuten Trelloa, komentokanavana.

Analyysi

- Kansainvälinen turvallisuustilanne heijastuu myös kybervakoilun maailmaan, ja uusia vakoiluoperaatioita paljastuu tiiviiseen tahtiin.
- Tätä voivat selittää esimerkiksi aktiivisempi tai näkyvämpi kybervakoilun keinojen käyttäminen, tietoturvatalojen ja kansainvälisen yhteisön aktiivisuus kybervakoilukampanjoiden tutkimisessa tai madaltunut kynnys havaituista operaatioista julkisuuteen kertomisessa.

Vakoilu

- Myös muiden toimijoiden kybervakoilukampanjoita havaitaan säännöllisesti Euroopassa. Esimerkiksi kiinalaiset ryhmät ovat olleet aktiivisia Euroopassa, mukaan lukien Ukrainassa ja Venäjällä.
- Viestien aiheet tai sisällöt ovat viime aikoina liittyneet joissain tapauksissa esimerkiksi Ukrainan sotaan tai kansainväliseen turvallisuustilanteeseen.
- Esimerkiksi kiinalainen APT-ryhmä Mustang Panda on hyödyntänyt viesteissään Ukrainan sotaan liittyviä teemoja houkutellakseen vastaanottaja lataamaan haitallista sisältöä laitteelleen.
  - Mustang Panda on lähettänyt haitallisia viestejä myös venäjää puhuville vastaanottajille.

Analyysi

- Kohdistetuissa kalasteluviesteissä tai sähköpostitse tapahtuvissa haittaohjelman levitysyrityksissä hyödynnetään usein ajankohtaisia tai vastaanottajalle muutoin mielenkiintoisia teemoja. Tätä on nähty niin koronapandemian alkuaikoina kuin Ukrainan sotaan liittyen.
- Kalasteluviestien uskottavuutta voidaan lisätä esimerkiksi rekisteröimällä sähköpostitilejä tunnettujen henkilöiden tai organisaatioiden nimissä.

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.

PRS-palvelun käyttöönotto etenee

- Lakimuutokset ovat lausuttavana PRS-palvelun käyttöön ottamiseksi ja tietoyhteiskuntamaksun korottamiseksi.
  - Liikenne- ja viestintäministeriö pyytää lausuntoja hallituksen esityksestä, jolla muutettaisiin sähköisen viestinnän palveluista annettua lakia sekä Liikenne- ja viestintävirastosta annettua lakia. Lausuntoja voi antaa 13.6.2022 saakka.
  - Tavoitteena on tehdä vaadittavat lainsäädäntömuutokset, jotta Galileo-satelliittipaikannusjärjestelmän julkisesti säännelty palvelu (Public Regulated Service, PRS-palvelu) on mahdollista ottaa Suomessa kansallisesti käyttöön vuoden 2025 aikana.
  - Tutustu asiaan tarkemmin lausuntopalvelun verkkosivuilla: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=cc1d86b3-3695-438c-8aaf-8428bfca47cb

Säädösvalmistelua

- Hallituksen esitys eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta (HE 63/2018).
  - Esitys on annettu eduskunnalle 28.4.2022. Esitykseen voi tutustua tarkemmin Eduskunnan verkkosivuilla https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_63+2022.aspx
  - Esityksessä mm. ehdotetaan lisättäväksi valmiuslakiin uusi erityisesti hybridiuhkatilanteisiin tarkoitettu poikkeusolomääritelmä.
  - Esityksen mukaan poikkeusoloina pidettäisiin, sen lisäksi mitä lain 3 §:ssä nykyään säädetään, myös muuta julkisen vallan päätöksentekokykyyn, yhteiskunnan kriittisen infrastruktuurin toimivuuteen, yleiseen järjestykseen ja turvallisuuteen tai rajaturvallisuuteen kohdistuvaa uhkaa, tapahtumaa, toimintaa tai näiden yhteisvaikutusta, joka erityisen vakavasti ja olennaisesti vaarantaa kansallista turvallisuutta, yhteiskunnan toimintakykyä tai väestön elinmahdollisuuksia.

Säädösvalmistelua

- Digipalvelusäädös etenee.
  - Euroopan komissio antoi joulukuussa 2020 ehdotuksen digipalvelusäädökseksi. Se sisältää laajasti säännöksiä internetin välityspalvelujen, kuten pilvipalvelujen ja verkkoalustojen, turvallisuuden ja avoimuuden parantamiseksi.
  - EU:n digipalvelusäädöksestä (Digital Services Act, DSA) on päästy alustavaan sopuun kolmikantaneuvotteluissa EU:n neuvoston ja Euroopan parlamentin kesken.
  - Liikenne- ja viestintäministeriö toimitti 16.3.2022 eduskunnalle valtioneuvoston kirjelmää täydentävän selvityksen komission ehdotuksesta digipalvelusäädökseksi.
  - EU:ssa pyritään saamaan neuvottelut päätökseen ja asetus valmiiksi kevään 2022 aikana.
  - Digipalvelusäännöksestä on kerrottu tarkemmin Liikenne- ja viestintäministeriön verkkosivuilla https://www.lvm.fi/-/digipalvelusaados-etenee-saadoksesta-paasty-alustavaan-sopuun-kolmikantaneuvotteluissa-1729784

Ajankohtaista tietosuojavaltuutetulta

- Tietosuojavaltuutetun toimisto on vastaanottanut kaksi ilmoitusta helsinkiläishotelleihin kohdistuneista tietoturvaloukkauksista.
  - Vuotaneita tietoja ovat tietosuojavaltuutetun toimiston tämänhetkisen tiedon mukaan ainakin asiakkaan nimi, syntymäaika, yhteystiedot sekä tietoja virallisista asiakirjoista.(21)
  - Tutustu neuvoihin tietovuodon kohteeksi joutuneille.(22)
- Apulaistietosuojavaltuutetulta huomautus ulkoministeriölle tietoturvaloukkausilmoitusten määräaikojen noudattamatta jättämisestä.(23)
  - Ulkoministeriö ilmoitti tammikuussa 2022 tietosuojavaltuutetun toimistolle joutuneensa NSO Groupin Pegasus-vakoiluhaittaohjelmasta johtuneen tietoturvaloukkauksen kohteeksi.
  - Apulaistietosuojavaltuutettu katsoo, että ulkoministeriön olisi tullut noudattaa yleisessä tietosuoja-asetuksessa säädettyjä määräaikoja tietoturvaloukkauksesta ilmoittamiseen valvontaviranomaiselle ja kohteeksi joutuneille henkilöille.

Arjen kyberturvallisuus

Vinkkejä informaatiovaikuttamisen tunnistamiseksi

- Julkaisimme ohjeen informaatiovaikuttamisen kohtaamiseen.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohje-vinkkeja-informaatiovaikuttamisen-tunnistamiseksi-ole-tarkkana

Työtarjousteemaisia huijausviestejä liikkeellä

- Viesteissä tarjotaan osa-aikatyötä. Viestit ovat huijausta eikä niihin vastaamista suositella.
- Lue lisää: https://www.is.fi/digitoday/tietoturva/art-2000008777733.html

Palvelunestohyökkäyksiä tapahtuu Suomessa kymmeniä tuhansia vuosittain – määrät lisääntyvät

- Palvelunestohyökkäykset ja niiden torjunta ovat arkipäivää. Julkaisussamme on hyödyllistä tietoa hyökkäyksistä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkayksia-tapahtuu-suomessa-kymmenia-tuhansia-vuosittain-maarat

Uutisia Kyberturvallisuuskeskuksesta

Suomi ja Ruotsi tekevät laajaa ja monipuolista yhteistyötä varautumiskysymyksissä

- Maiden varautumisasioista vastaavien viranomaisten päälliköt tapasivat Helsingissä perjantaina 29.4.
- Kahdenvälinen tapaaminen oli ensimmäinen laatuaan ja asialistalla olivat niin yhteiskunnan siviilivalmius ja varautuminen, huoltovarmuus kuin kyberasiatkin.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomi-ja-ruotsi-tekevat-laajaa-ja-monipuolista-yhteistyota-varautumiskysymyksissa

ICT-alan toinen lakko alkoi maanantaina 9.5

- Lakon on tarkoitus jatkua kaksi viikkoa ja se voi vaikuttaa palveluntarjoajien toimintaan.
- Lakko koskee kaikkia teleoperaattoreita, verkonrakennusyhtiöitä ja niiden alihankkijayrityksiä, joissa noudatetaan Ammattiliitto Pron ja Palvelualojen työnantajaliitto Paltan välistä työehtosopimusta.
- Sopimuksen piirissä on noin 12 000 toimihenkilöä ja asiantuntijaa. Alan työehtosopimusneuvotteluja on käyty joulukuusta lähtien.
- https://yle.fi/uutiset/3-12043017/64-3-75968

Cyber Security Nordic –messut järjestetään neljättä kertaa 12.-13. toukokuuta

- Neljännen kerran järjestettävät messut kokoavat yhteen kyberalan osaajia ja toimijoita niin yksityiseltä kuin julkiselta sektorilta.
- Kyberturvallisuuskeskus on esillä messuilla yhteistyössä Digi- ja väestötietoviraston kanssa.
- Case Finland – lessons learned from latest global cyberthreats – paneelikeskustelussa on mukana myös Arttu Lehmuskallio Kyberturvallisuuskeskuksesta
- https://cybersecuritynordic.messukeskus.com/

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

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

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

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

5) Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

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

7) CISA Shields Up –sivusto https://www.cisa.gov/shields-up

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

Lähdeluettelo

9) Joint Cybersecurity Advisory https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf

10) Welivesecurity, Industroyer2: Industroyer reloaded https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

11) USSOCOM https://media.defense.gov/2022/Apr/28/2002985725/-1/-1/1/SOCOM_22D_R1.PDF

12) Insteon Blames Abrupt Shutdown on Failed Effort to Find a Buyer https://uk.pcmag.com/smart-home/139876/smart-home-company-insteon-shuts-down-servers-without-warning

13) Shameful: Insteon looks dead—just like its users' smart homes https://arstechnica.com/gadgets/2022/04/shameful-insteon-looks-dead-just-like-its-users-smart-homes/

14) Aftonbladet: Skandaali Verisuressa: työntekijöiden kerrotaan katselleen asiakkaiden alastonkuvia – yhtiö selvittää https://www.is.fi/digitoday/art-2000008769860.html

15) Ohjeita pilvipalveluiden turvallisuudesta yksityishenkilöille, pienyhteistölle ja yrityksille https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjeita-pilvipalvelujen-turvallisuudesta-yksityishenkiloille-pienyhteisoille-ja

16) Microsoft best practices for managing IoT security concerns https://www.microsoft.com/security/blog/2022/04/25/microsoft-best-practices-for-managing-iot-security-concerns/

17) Multiple fibers cut across France, impacting several cities https://www.datacenterdynamics.com/en/news/multiple-fibers-cut-across-france-impacting-several-cities/

Lähdeluettelo

18) Tietoturva-asiantuntija kyberiskusta: Kuin joku olisi käynyt töhrimässä ilmoitustaulua https://www.is.fi/digitoday/art-2000008740603.html

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

20) Palvelunestohyökkäyksiä tapahtuu Suomessa kymmeniä tuhansia vuosittain - määrät lisääntyvät https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkayksia-tapahtuu-suomessa-kymmenia-tuhansia-vuosittain-maarat

21) Tietosuojavaltuutetun toimisto https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-on-vastaanottanut-kaksi-ilmoitusta-helsinkilaishotelleihin-kohdistuneista-tietoturvaloukkauksista-tutustu-neuvoihin-tietovuodon-kohteeksi-joutuneille

22) Neuvoja tietovuodon kohteeksi joutuneille https://tietosuoja.fi/-/neuvoja-tietovuodon-kohteeksi-joutuneille

23) Tietosuojavaltuutetun toimisto https://tietosuoja.fi/-/apulaistietosuojavaltuutetulta-huomautus-ulkoministeriolle-tietoturvaloukkausilmoitusten-maaraaikojen-noudattamatta-jattamisesta