TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 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

15.9.2022

Kybersää elokuu 2022

Tietomurrot ja -vuodot

- Olemme saaneet useita ilmoituksia suomalaisten organisaatioiden tietojärjestelmiin kohdistuneista kirjautumisyrityksistä.
- Pienten yritysten verkkotunnuksia ja sosiaalisen median käyttäjätilejä kaapattu.

Huijaukset ja kalastelut

- Pankkitunnuskalastelu on keskittynyt pääosin tekstiviesteihin, kun taas tilausansat ovat vaihtuneet tekstiviesteistä sähköposteihin.
- Puheluiden väärentämisen estämiseen tähtäävä Traficomin määräys 28 on vähentänyt teknisen tuen huijauspuheluita.

Haittaohjelmat ja haavoittuvuudet

- Ilmoituksia kiristyshaitta-ohjelmahavainnoista suomalaisissa tai Suomessa toimivissa organisaatioissa.
- Päivitysten asentaminen on edelleen tärkeää. Haavoittuvuuksia hyväksikäytetään nopeasti julkitulon jälkeen.

Automaatio ja IoT

- Tietoturvamerkin seminaarissa 29.9. käsittelyssä tulevat pakolliset EU-tietoturvavaatimukset IoT-tuotteille.
- Tutkijat löysivät haavoittuvuuksia lähes kaikista tarkastelemistaan 4G- ja 5G- IoT-rajapinnoissa.

Verkkojen toimivuus

- Kolme merkittävää toimivuushäiriötä joukkoviestintäpalveluissa.
- Palvelunestohyökkääjät aktivoituivat elokuussa.
- Kyberturvallisuuskeskukselle raportoitiin tuplasti enemmän palvelunestohyökkäystapauksia, kuin kesäkuukausina.

Vakoilu

- Tietoja tuhoavia haittaohjelmia on havaittu ainakin 25 maassa vuoden ensimmäisen puoliskon aikana.
- APT-toimijoiden kiinnostus organisaatioiden pilvipalveluita ja kirjautumistietoja kohtaan on pysynyt edelleen korkeana.

Kuukauden tunnuslukuja

2X

Elokuussa Kyberturvallisuuskeskukselle raportoitiin kaksinkertainen määrä palvelunestohyökkäyksiä kesä-heinäkuuhun verrattuna.

30%

Suomen kyberuhkatason katsotaan nousseen. Esimerkiksi kiristyshaittaohjelmien määrä on kasvanut tänä vuonna 30% verrattuna vastaavaan ajankohtaan viime vuonna.

28

Määräys 28 viestintäverkkojen ja -palveluiden yhteentoimivuudesta uudistettiin, ja sen avulla suomalaisista numeroista soitettuja huijauspuheluita on saatu vähennettyä merkittävästi.

Tietoturvamerkki-seminaari 2022

- Tietoturvamerkki-seminaari pidetään 29.9.2022 kello 13–16 seuraavin sisällöin:
  - Elokuussa 2024 älylaitteille tulee pakollisia EU:n laajuisia tietoturvavaatimuksia. Mitä suomalaisyritysten on hyvä tietää? Miten tietoturva kytkeytyy kilpailukykyyn ja yritysten vastuullisuuteen?
  - Tilaisuudessa kuulemme Euroopan komission, Googlen, Polarin ja SOK:n asiantuntijoiden näkemyksiä Secure by Designista ja vastuullisuudesta.
- Voit osallistua tilaisuuteen Tennispalatsissa tai seurata etänä.
- Ohjelma: https://tietoturvamerkki.fi/fi/tietoturvamerkki-seminaari-2022/tietoturvamerkki-seminaarin-ohjelma
- Ilmoittautuminen: https://link.webropolsurveys.com/Participation/Public/2df40cc3-af9b-4e58-97b8-3a40d0ad7436?displayId=Fin2603004

Tietoturva

Top 5 kyberuhat - lähitulevaisuudessa (6kk-2v)

1

Talouden ja politiikan ilmiöt vaikuttavat voimakkaasti kyberturvallisuuteen. Digitaalisuus läpileikkaa koko organisaation toimintaa. Muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaatioiden jatkuvuuteen ja riskienhallintaan.

2

Suomeen kohdistuneen kyberuhkatason katsotaan nousseen. Lisääntyneen haitallisen liikenteen ja kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

3

Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista. Esimerkiksi käyttäjäoikeuksien hallinta, ohjelmistojen ajantasaisuuden ylläpito ja hyvä tietoturvakulttuuri ovat kyberturvallisuuden kivijalkaa.

Symbolit

Uusi

Päivitetty

4

Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä. Tehokas tiedonvaihto parantaa kaikkien kyberturvallisuutta.

5

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.

1. Talouden ja politiikan ilmiöt vaikuttavat voimakkaasti kyberturvallisuuteen.

Muutokset kansainvälisessä turvallisuustilanteessa on hyvä huomioida myös organisaatioiden jatkuvuuden- ja riskienhallinnassa. Nyt on hyvä hetki päivittää riskienhallintasuunnitelmat vastaamaan muuttunutta turvallisuustilannetta.

- Venäjän hyökkäys Ukrainaan heijastuu myös kyberturvallisuuteen. Esimerkiksi sodan aiheuttamat muutokset talouteen, energian hinnan nopea nousu ja informaatioympäristön herkkyys näkyvät vaikeasti ennakoitavina kehityskulkuina, jotka ulottuvat myös digitaaliseen maailmaan.
  - Energiamarkkinoiden vaihteleva ja ennakoimaton tilanne voi vaikuttaa myös kyberturvallisuuteen. Energiamarkkinoihin vaikuttamista kybertoimintaympäristössä ei voi sulkea pois.
  - Mahdollinen sähkön sääntely voi aiheuttaa vaikutuksia myös kyberturvallisuuteen ja ICT-palveluiden toimivuuteen.
- Epävarmuustekijöillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

CASE

Suomen NATO-jäsenyysprosessin aikana Suomea kohtaan voidaan kohdistaa erilaista kyber-vaikuttamista sekä verkossa tapahtuvaa informaatio-vaikuttamista. Vaikuttaminen voi näkyä esimerkiksi palvelunesto-hyökkäyksinä. Palvelunesto-hyökkäyksillä saadaan hetkellisesti näkyvyyttä, mutta niiden vaikutukset eivät useimmiten ole laajoja tai pitkävaikutteisia.

2. Suomeen kohdistuneen kyberuhkatason katsotaan nousseen.

Kyberhyökkäykset ovat lisääntyneet maailmanlaajuisesti kuluvan vuoden aikana. Samalla niitä kohdistuu kasvavassa määrin myös Suomeen. Merkittävät poliittiset ratkaisut tai suurten organisaatioiden päätökset saattavat aktivoida ja motivoida hyökkääjiä.

- Kyberturvallisuuskeskus on tämän johdosta arvioinut kyberturvallisuuden uhkatason nousseen Suomessa.
- Merkittävä uhka organisaatioille ovat kiristyshaittaohjelmat, joiden määrä kasvaa jatkuvasti. Kuluneen kesän aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.
- Erityisesti huoltovarmuuden kannalta kriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.[1]

OHJE

Kesän aikana merkittäviä organisaatioita on joutunut kiristyshaittaohjelmien uhriksi Suomessa. Vaikutukset eivät ole olleet organisaatioita lamauttavia, ja toimintaa on kyetty jatkamaan.

Oikeanlaiset suojaustoimet, varautuminen ja hyvä jatkuvuudenhallinta pienentävät hyökkäysten vaikutuksia sekä riskiä joutua uhriksi. Lisäksi ne helpottavat organisaation palautumista takaisin normaaliin tilaan.

3. Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Organisaation kyberturvallisuuden kivijalka rakennetaan arkisilla kyberturvallisuuden toiminnoilla. Edelleen suurin osa tietoturvapoikkeamista olisi vältettävissä tavanomaisilla keinoilla, kuten ohjelmistopäivityksillä, hyvillä salasanakäytänteillä ja tietoturvakulttuurilla.

- Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.
- Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon saatetaan jättää auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu. Kun suojaustoimet ja ylläpito ovat puutteellisia, koko organisaatio altistuu tietoturvapoikkeamille.
- Tietojen kalastelu on edelleen helppo ja yleinen tapa rikolliselle pyrkiä organisaatioon sisälle. Tietoisuuden lisääminen organisaatiossa auttaa tunnistamaan epäilyttävän toiminnan.
- Kyberturvallisuuskeskus tarjoaa organisaatioille runsaasti käytännön ohjeita kyberturvallisuuden parantamiseksi.[2]

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. 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.[3]

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää 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 määrästä vaan 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.

Tietomurrot ja -vuodot

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

TRAFICOM

15.9.2022

Tietomurrot ja -vuodot

- Useita erilaisia tietomurtotapauksia elokuussa.
  - Pienten yritysten verkkotunnuksia on kaapattu.
  - Sosiaalisen median käyttäjätilien menetyksistä tulee edelleen ilmoituksia.

Analyysi

- Tietomurtojen torjunnan kannalta on erittäin tärkeää pitää järjestelmien ja laitteiden päivitykset ajan tasalla.
- Haavoittuvilla järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi.
- Käytä mahdollisuuksien mukaan myös monivaiheista tunnistautumista.
  - Käyttäjätunnuksen ja salasanan haltuunsa saaneen hyökkääjän tulee saada haltuunsa vielä monivaiheisen tunnistautumisen kertakäyttökoodi onnistuakseen tietomurrossa.

Tietomurrot ja -vuodot

- Elokuun aikana kirjautumisyritykset suomalaisten organisaatioiden tietojärjestelmiin lisääntyivät selvästi
  - Usea organisaatio kertoi havainneensa esimerkiksi VPN-palveluihinsa tehtyjen kirjautumisyritysten lisääntyneen elokuun aikana selvästi. Kirjautumisyrityksiä voidaan pitää tietomurron yrityksenä, sillä onnistunut kirjautuminen johtaa tietomurtoon.
  - Kirjautumisyritysten hienovaraisuus vaihtelee. Osa on selvästi tehty vältellen hälytysten syntymistä.
  - Uudelleen vuosien hiljaiselon jälkeen ovat pinnalle nousseet myös siirrettävät muistivälineet murtoketjujen ensimmäisenä askeleena.
  - Näissä tapauksissa muistivälineellä oleva haittaohjelma pyrkii hyödyntämään Windows-apuohjelmia varsinaisten pysyvän jalansijan haittaohjelmakomponenttien asentamiseksi.

Analyysi

- Kybervaikuttamisen suhteen Suomessa on havaittavissa uhkatason nousua.
- Uhkatason nousuun on syytä varautua mm. parantamalla lokienvalvontaa sekä huolehtimalla toimivista varmuuskopioista.
- Julkaisimme aiheesta myös Tietoturva Nyt!-artikkelin.[1]

Tietomurrot ja -vuodot

- Zimbra-sähköpostijärjestelmän haavoittuvuutta käytettiin sähköpostipalvelinten murtoon myös Suomessa.
  - Haavoittuvuus sekä sen korjaava paikkaus julkaistiin jo keväällä. Päivittämättömyyttä hyödynnettiin elokuussa.
  - Etenkin verkkoon näkyvät laitteet on syytä pitää päivitettynä.
  - Sähköpostipalvelimen murto aiheuttaa vakavan tietovuodon uhkan, koska ulkopuolisten tahojen haltuun päätyvät myös palvelimella olevat sähköpostit.

Analyysi

- Suuri osa haavoittuvuuksia hyödyntävistä tietomurroista voitaisi estää etenkin verkkoon näkyvien laitteiden pitämisellä päivitettynä.
- Tietomurroissa käytetään onnistuneesti jopa vuosia vanhoja haavoittuvuuksia.
- Epäiltäessä tietomurtoa on aina syytä tehdä tietoturvatutkinta. Tällä pystytään poissulkemaan tietomurto tai mahdollisesti selvittämään sen laajuus ja vaikutukset.

Huijaukset ja kalastelut

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

Huijaukset ja kalastelut

- Toimitusjohtajahuijauksia kohdistunut useisiin organisaatioihin.
  - Yrityksiin ja muihin organisaatioihin kohdistuu edelleen runsaasti toimitusjohtajahuijauksina tunnettuja laskutuspetoksia.
  - Uhreiksi on valittu organisaatioita laidasta laitaan, ja tavat lähestyä uhria vaihtelevat. Lähestymistapana on ollut esimerkiksi "Voitko tehdä kansainvälisen pankkisiirron Puolaan tänään?", "Voitko ostaa nopeasti nipun iTunes-lahjakortteja”.
  - Viesti voi tulla selvällä suomen kielellä sähköpostilla, WhatsAppilla, tai tekstarilla organisaation johtajan nimissä laskuja käsittelevälle työntekijälle.
  - Jotkut valmistelevat huijausta huolellisesti, toiset kokeilevat kepillä jäätä, mutta tarkoitus on aina sama: huijari yrittää saada helppoa rahaa. Menetelmät vaihtelevat.

Analyysi

- Tietojenkalasteluviesteillä koetetaan kalastella yritysten ja organisaatioiden verkkoon ja postilaatikoihin pääsytunnuksia ja salasanoja.
- Tietojenkalastelu on lisääntymässä sekä valtionhallinnon, koulutussektorin että yksityisen sektorin puolella.
- Myös viihdetilien – kuten Netflix – ja erilaisten pelitilien – kuten Steam – tunnuksia kalastellaan aktiivisesti.

Huijaukset ja kalastelut

- Pankkitunnuksia kalastellaan aktiivisesti.
  - Pankkitunnukset ovat rikolliselle haluttu saalis: niillä pääsee heti käsiksi uhrin rahoihin.
  - Tekstiviestikalasteluista valtaosa on tällä hetkellä pankkitunnusten kalastelua. Tunnuksia kalastellaan kiivaasti kaikkien liikepankkien nimissä.
  - Verottajan nimissä huijaaminen on rikolliselle vielä tehokkaampaa kuin yksittäisen pankin tunnusten kalastelu: viranomaisen kirjautumissivuksi väärennetyllä kalastelusivulla voi kalastella kerralla kaikkien pankkien tunnuksia.
  - Pankkitunnuksia koetetaan kalastella myös kaapatuilla sosiaalisen median tileillä. Kalastelulinkkejä lähetetään keksityistä syistä kaapatun tilin kontaktilistalle.

Analyysi

- Aiemmin tekstiviestihuijauksia on käytetty kaikenlaisiin tilausansoihin eri tuotemerkkien nimissä, mutta elokuussa tilausansat ovat olleet enimmäkseen McAfeen nimissä lähetettyjä sähköposteja.
- Posteissa huijataan, että virusturvatuotteen voimassaolo on vanhentunut, vaikka viestin vastaanottaja ei sellaista olisi koskaan käyttänytkään.
- Myös HalpaHallin nimissä on lähetetty tilausansoihin johtavia huijausviestejä.

Huijaukset ja kalastelut

- Kiristysviestejä edelleen liikkeellä eri tahojen nimissä.
  - Poliisin nimissä lähetetään kirjavia liitetiedostoja, joissa on erilaisia leimoja ja korkeiden poliisiviranomaisten nimiä. Uhria uhataan erilaisilla syytteillä, mutta viestit ovat huijausta ja liitetiedostot harmittomia.
  - Pornokiristysviesteistä on jälleen tehty kymmenittäin ilmoituksia Kyberturvallisuuskeskukselle. Ilmoituksia tulee laidasta laitaan ja niitä yhdistää se, että kaikki ovat takuuvarmaa huijausta.
  - Vastaanottajina on mitä tahansa satunnaisia sähköpostiosoitteita, mitä ikinä on millekään listalle haalittu tai keksitty: yksittäisiä kansalaisia, organisaatioita, ryhmäpostilaatikoita, reitittimen hallinta- tai ylläpitotunnuksia ja muita laiteosoitteita, jotka eivät varmastikaan ole voineet syyllistyä rikoksiin.

Analyysi

- Kiristysviestien teemat vaihtelevat, mutta niiden perustavoite on sama.
- Yhteistä huijauksille on, että huijari luo niissä huijauksen kohteena olevalle ihmiselle häpeän ja kiireen tuntua ja voi väittää murtautuneensa viestin vastaanottajan laitteelle.
- Viranomaisen nimissä lähetetyissä huijausviesteissä pyritään hyötymään auktoriteetista uskottavuuden tuojana.
- Huijarin tavoitteena on taloudellinen hyöty.

Huijaukset ja kalastelut

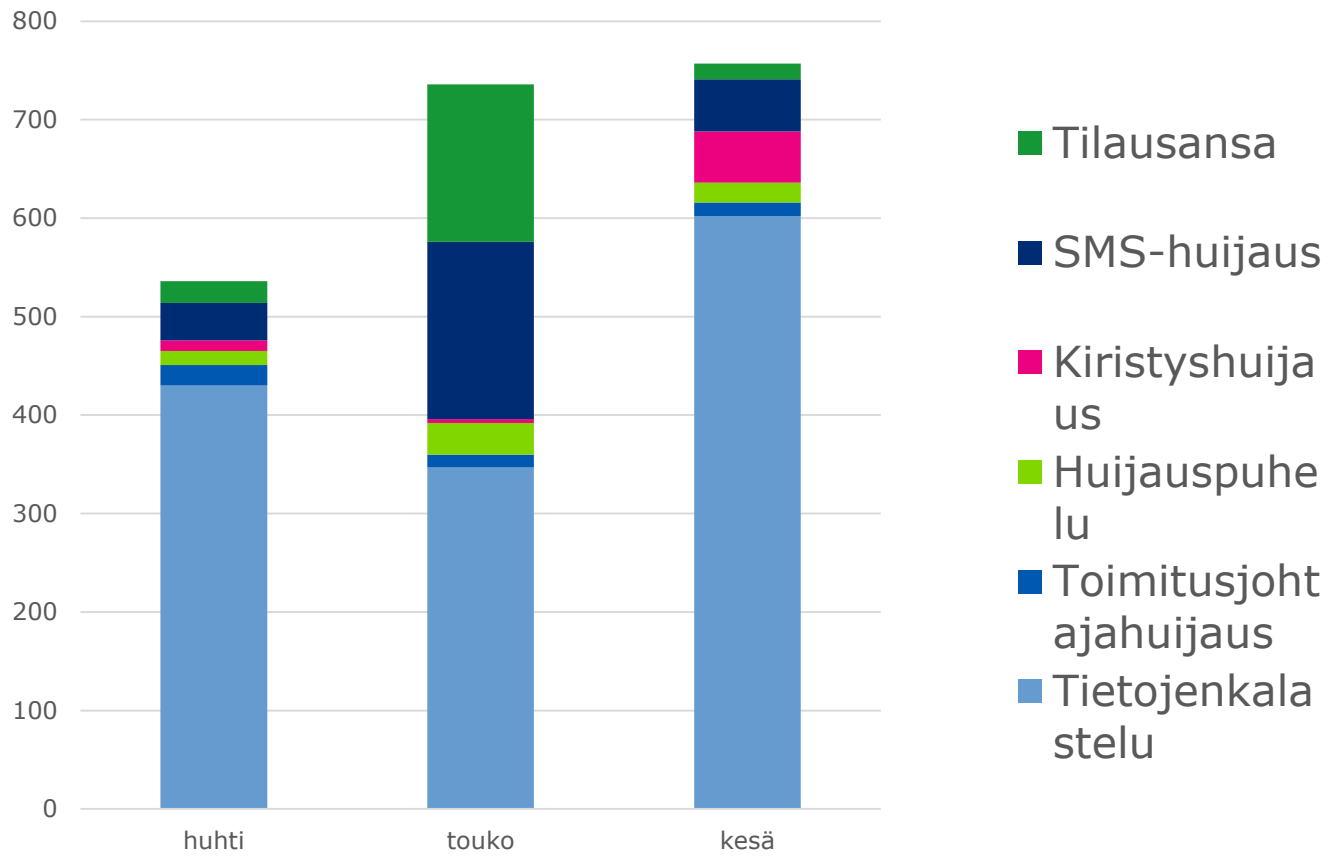
- Eri teemoilla toistuvat huijauspuhelut ovat yleinen ilmiö. Soittaja väittää esimerkiksi, että uhrin tietokoneella on tietoturvaongelma ja pyytää avaamaan koneen korjatakseen sen, jonka jälkeen huijari pyrkii ottamaan etähallinnan käyttöön.
- Puhelut näyttävät tulevan suomalaisesta tai ulkomaalaisesta puhelinnumerosta.
- Huijarit ovat puhuneet useimmiten englantia. Soitot ovat huijauksia ja todennäköisesti soitettu väärennetyistä puhelinnumeroista.
- Puheluun vastaaminen ei ole vaarallista. Huijarin kanssa jutellessa pidä huoli siitä, ettet anna pankkitietojasi, et kuvia henkilöpapereistasi, etkä päästä huijaria hallitsemaan tietokonettasi.

Analyysi

- Sääntelyn uudistuksella ja teleoperaattoriyhteistyöllä pyritään vähentämään huijaussoittojen määrää.
- Liikenne- ja viestintävirasto Traficomin 16.5.2022 uudistama määräys 28 antoi operaattoreille uudet velvoitteet estää soittajan numeron väärentäminen ja huijaussoittojen välittäminen puhelun vastaanottajille.
- Suomalaisista numeroista soitettuja huijauksia on saatu karsittua minimiin uudistusten myötä.[(4)]

Käsiteltyjä huijaustapauksia Q2/2022

3kk



- Vuoden 2022 toisen neljänneksen ilmiöitä ovat:
  - Pankkitunnusten kalastelu ja tilausansat ovat jatkuneet aktiivisina.
  - Toukokuun SMS-huijausten piikki johtui taustakuva- ja pelipalveluaiheisista tilausansoista.
  - Huijauspuheluiden määrä on pysynyt edelleen matalana.
  - Ilmoitettujen toimitusjohtajahuijausten määrä ei merkittävästi lisääntynyt lomakauden alusta huolimatta.

Haittaohjelmat ja haavoittuvuudet

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

TRAFICOM

15.9.2022

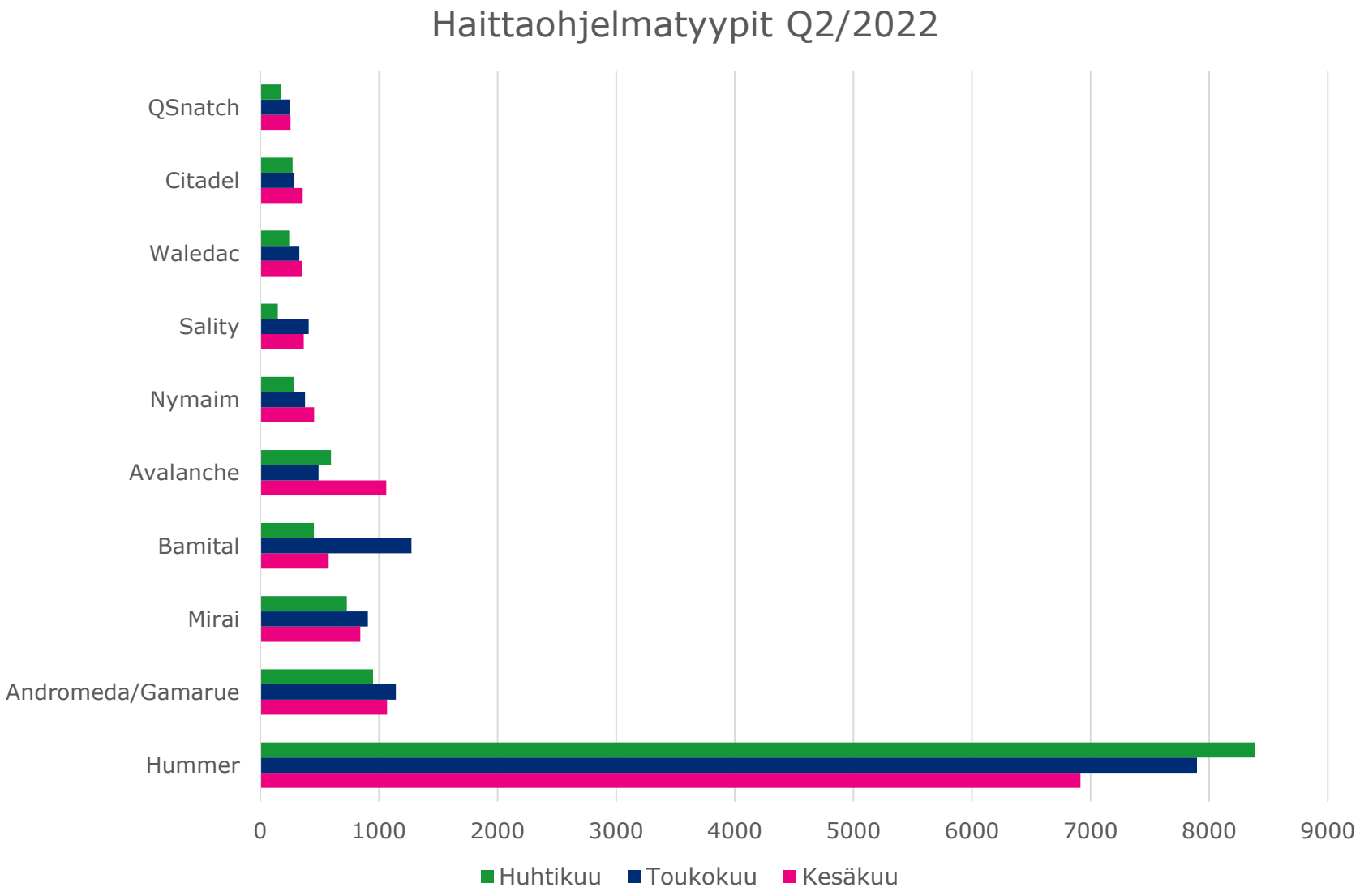
Haittaohjelmat

- Kiristyshaittaohjelmien aktiivinen toiminta jatkui Suomessa elokuussa.
  - Kaiken kokoiset organisaatiot voivat joutua hyökkäyksen kohteeksi. Hyökkäyksessä rikollinen tunkeutuu organisaation järjestelmiin ja levittäytyy organisaation verkkoon. Lopulta hyökkääjä käynnistää kiristyshaittaohjelman siten salaten tiedostoja, jonka jälkeen salauksen purkamisesta yleensä vaaditaan lunnaita.
  - Kiristyshaittaohjelmista tehdään vuosittain joitakin kymmeniä ilmoituksia Kyberturvallisuuskeskukselle. Vuoden 2022 aikana olemme havainneet n. 30% kasvun viime vuoden vastaavaan ajankohtaan verrattuna.
  - Kesäkuussa 2022 julkaisemamme ohje auttaa kiristyshaittaohjelmien uhriksi joutuneita organisaatioita.[(5)]

Analyysi

- Onnistunut kiristyshaittaohjelmakampanja voi lamauttaa organisaation toiminnan.
- Oikeaoppinen varautuminen kiristyshaittaohjelmahyökkäyksiin parantaa selvästi organisaatioiden tietoturvatasoa ja sietokykyä niin kiristyshaittaohjelmia kuin muitakin mahdollisia hyökkäyksiä vastaan.
- Kiristyshaittaohjelmat saattavat levitä helpommin työntekijöiden palatessa lomilta. Kirjoitimme aiheesta vuonna 2020. Organisaatioiden voi olla hyvä tehdä ja jakaa tietoturvaohjeita lomalta palaaville työntekijöille.

Autoreporterin haittaohjelmahavainnot



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

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Niistä voi lukea tarkempia tietoja kotisivuiltamme.[(6)] [(7)]

Haavoittuvuus

- Atlassianin Bitbucket Server tuotteessa kriittinen haavoittuvuus (CVSS 9.9)
  - Päivitys on uusimpiin versioihin saatavilla.[8]
- Lisätietoa viikkokatsauksessa 35/2022.[9]
  - Google Chrome –selaimen vanhoista versioista löydetty uusia, merkittäviä haavoittuvuuksia.
  - Android-käyttöjärjestelmän julkaistut, kriittisimmät haavoittuvuudet koskivat Bluetooth standardista löytyneitä haavoittuvuuksia, jotka mahdollistavat etäältä tapahtuvan hyökkäyksen.
  - Apple on julkaissut tietoja kriittisistä haavoittuvuuksista, jotka on korjattu viimeisimmissä päivityksissä.

Analyysi

- Päivitykset on ajettava riittävän nopeasti myös keskitetyn hallinnan piirissä oleville laitteille.
- Esimerkiksi CISA:n known exploited vulnerabilities catalog –sivusto antaa tietoa haavoittuvuuksien hyödyntämisestä päivitystarpeen kriittisyyden arviointia varten.[10]

Kuukauden haavoittuvuusjulkaisut

- Kriittiseksi luokiteltu VMware-päivityspaketti korjaa haavoittuvuuksia useista tuotteista (13/2022).
  - VMware julkaisi päivityspaketin, joka korjaa VMware Workspace ONE Access, VMware Identity Manager ja VMware vRealize Automation –tuotteista kriittiseksi luokitellun haavoittuvuuden CVE-2022-31656.
  - Haavoittuvuuteen on olemassa toimiva hyväksikäyttökeino ja havainnollistava esimerkkikoodi.[(11)]
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

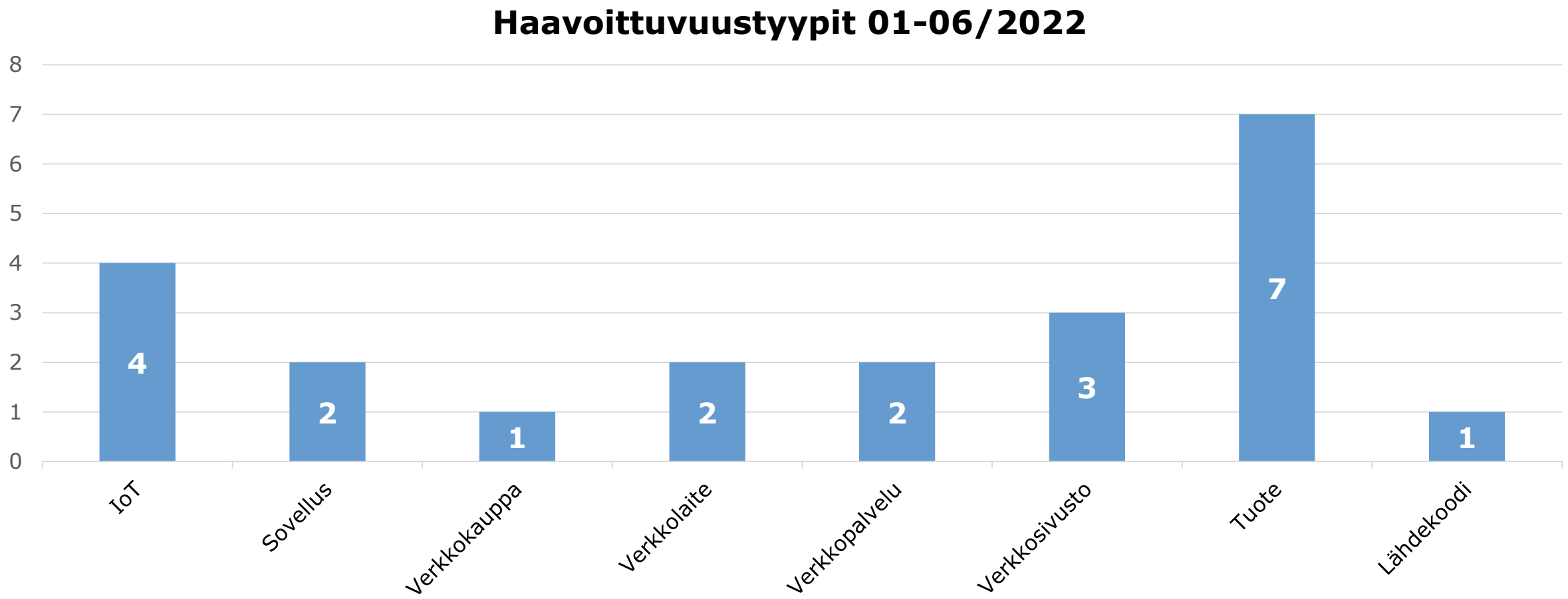
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 13 kpl (tilanne 12.9.2022).**
  - 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

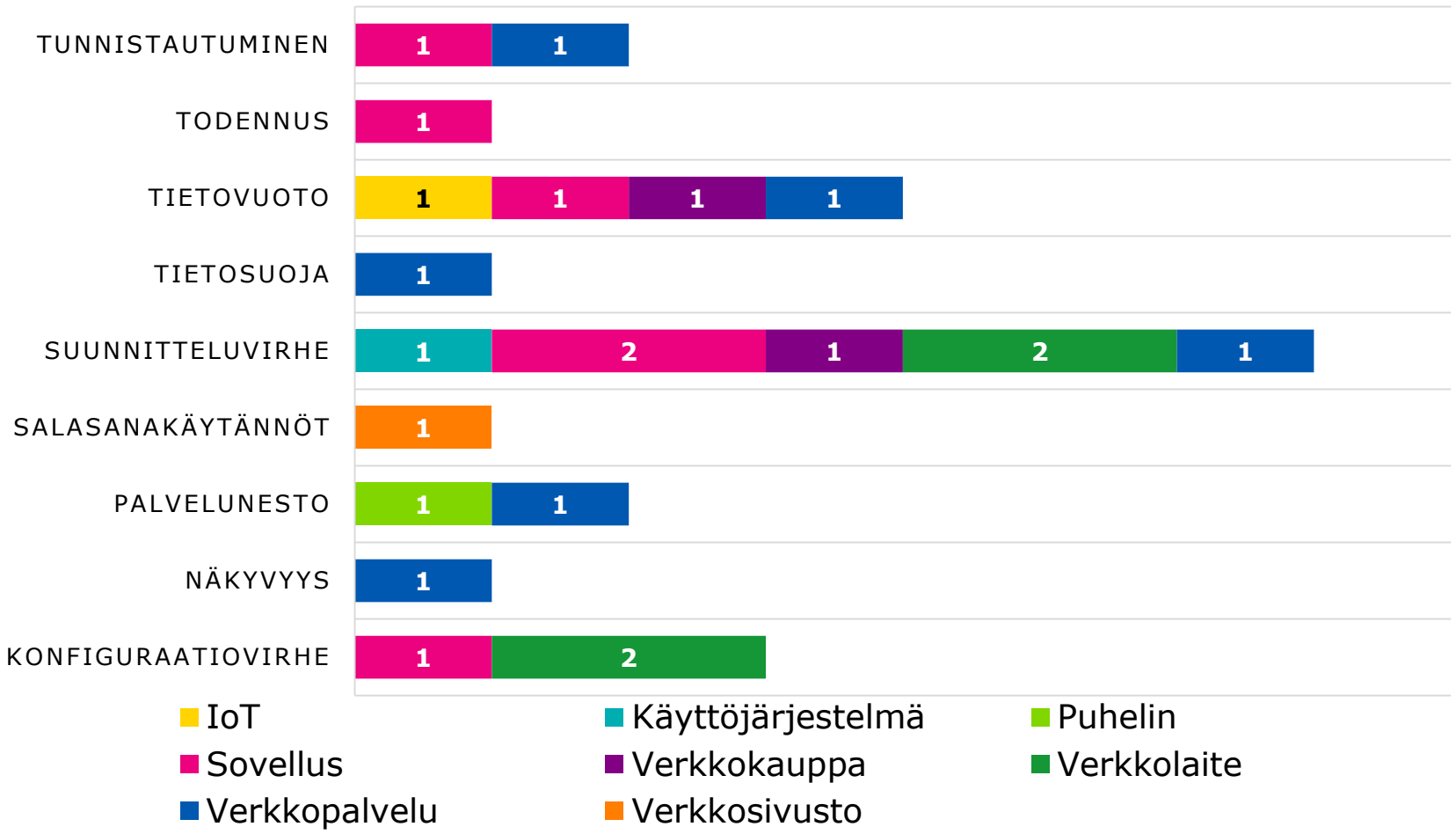
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuoden 2022 ensimmäiseltä vuosipuolikkaalta.

Haavoittuvuuskoordinaatiota on esitelty laajemmin verkkosivuillamme.[(12)]

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.

TRAFICOM

15.9.2022

IoT

- Tietoturvamerkki-seminaari[13] pidetään 29.9.2022 kello 13–16 seuraavin sisällöin:
  - Elokuussa 2024 älylaitteille tulee pakollisia EU:n laajuisia tietoturvavaatimuksia. Mitä suomalaisyritysten on hyvä tietää? Miten tietoturva kytkeytyy kilpailukykyyn ja yritysten vastuullisuuteen?
  - Tilaisuudessa kuulemme Euroopan komission, Googlen, Polarin ja SOK:n asiantuntijoiden näkemyksiä Secure by Designista ja vastuullisuudesta.
- Voit osallistua tilaisuuteen Tennispalatsissa tai seurata etänä.
  - Ohjelma: https://tietoturvamerkki.fi/fi/tietoturvamerkki-seminaari-2022/tietoturvamerkki-seminaarin-ohjelma
  - Ilmoittautuminen : https://link.webropolsurveys.com/Participation/Public/2df40cc3-af9b-4e58-97b8-3a40d0ad7436?displayId=Fin2603004

Lisätietoa

- IoT-laitteille on tulossa pakollisia tietoturvavaatimuksia EU:sta ja Tietoturvamerkki-seminaarissa on mahdollista kuulla niistä tuoreeltaan.
- Helmikuussa voimaan tulleet Radiolaitedirektiivin (RED) tietoturvavaatimukset parantavat käyttäjien yksityisyyttä ja suojaavat viestintäverkkoja. Lisäksi ne estävät taloudelliseen hyötyyn tähtääviä petoksia, joissa hyödynnetään verkkoon liitettyjä laitteita.
- RED tietoturvavaatimuksia sovelletaan 1.8.2024 lähtien.
- Kyberresilienssiasetuksen (CRA) luonnosesitys julkaistaan syyskuussa. Asetuksen tavoitteena on sisällyttää kyberturvavaatimukset jokaiseen verkkoon kytkettävään laitteeseen.[14]
- Valmistajien kannattaa olla hyvissä ajoin liikkeellä ja varmistaa omien tuotteiden vaatimustenmukaisuus.

IoT

- Kesäkuussa julkaistiin standardi ISO/IEC 27400, joka sisältää ohjeet IoT-ratkaisujen tietoturva- ja tietosuojariskien arviointiin, periaatteisiin ja hallintakeinoihin.[19]
- Standardissa on huomioitu IoT:n erityispiirteet:
  - eri tahojen (IoT-laitteiden, gatewayn, käyttäjien sekä alijärjestelmien) suuri määrä, hajautettu toteutus, suuri hyökkäyspinta, palvelun elinkaaren hallinta ja laaja sidosryhmäverkosto.[15]
- Tulevina vuosina ISO 27k tietoturvastandardit täydentyvät seuraavilla IoT-standardeilla:
  - ISO/IEC 27402 - IoT-laitteen perustason tietoturvavaatimukset.[16]
  - ISO/IEC 27403 - ohjeet kuluttajien IoT-laitteiden tietoturvan ja yksityisyyden riskien arviointiin ja hallintakeinojen tunnistamiseen.[17]
  - ISO/IEC 27404 - yleinen tietoturvamerkki kuluttajien IoT-laitteille perustuen kansainvälisiin tietoturvavaatimuksiin.[18]

Analyysi

- ISO/IEC 27000 -sarjan standardit keskittyvät hallinnolliseen tietoturvaan ja sisältävät ohjeistusta tietoturva- ja tietosuojariskien arviointiin sekä hallintakeinojen valintaan.
- IoT-palvelun ekosysteemi on monimutkainen ja toimijoiden verkosto laaja. Standardi selkiyttää IoT-ekosysteemiä ja luo yhteisen tavan siitä puhumiseen.
- Standardeissa on kuvattu eri toimijoiden roolit ja vastuut, jotta IoT-palvelun tietoturva toteutuisi sen koko elinkaaren ajan.
- IoT:n teknisiä tietoturvavaatimuksia kannattaa tarkistaa ETSI EN 303 645 ja ISA/IEC 62443 standardeista.

IoT

- Berliinin teknillisen yliopiston tutkijat esittelivät elokuussa Black Hat –tietoturvakonferenssissa löytämiään haavoittuvuuksia teleoperaattorien tarjoamista 4G- ja 5G-verkkojen palveluiden rajapinnoista (API).[20]
- Näitä teknologioita käytetään avaamaan operaattorin hallinnassa olevien verkkojen toimintoja kolmansille palveluita tarjoaville osapuolille.
- Tutkijat löysivät lähes jokaisesta analysoimastaan palvelurajapinnasta yleisesti tunnettuja haavoittuvuuksia liittyen esimerkiksi tunnistamiseen ja valtuuttamiseen sekä syötteentarkastukseen erilaisten injektiohaavoittuvuuksien muodossa. Löydetyt haavoittuvuuden mahdollistavat esimerkiksi hyökkäyksiä toisia käyttäjiä tai itse palvelualustoja sekä niiden taustalla olevia 4G- ja 5G-verkkoja vastaan.

Analyysi

- Tutkijat suosittelevat lääkkeeksi parempaa tietoturvallisuuden huomioimista näitä rajapintoja kehitettäessä. Huomio tulisi keskittää yleisen hyökkäyspinta-alan pienentämiseen, pahantahtoisen toiminnan parempaan havaitsemiseen, pääsynhallintaan, syötteiden tarkastamiseen sekä rajapintojen tietoturvatestaukseen. Myös näiden palvelualustojen sovelluskehittäjät kaipaisivat selvästi lisää tietoturvakoulutusta.
- Liikenne- ja viestintävirasto Traficom on julkaissut vuonna 2019 selvityksen 5G:n kyberturvallisuudesta, joka tukee sekä julkishallinnon että yritysmaailman riskienhallintaa, varautumista ja niiden välistä vuoropuhelua.[21]
- Traficom on myös järjestänyt vuodesta 2019 alkaen 5G Cyber Security Hackathon -tapahtumia, joissa tietoturvatutkijat ovat voineet laboratorioympäristössä etsiä haavoittuvuuksia eri valmistajien 5G-toteutuksista.[22]

Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.

TRAFICOM

15.9.2022

Verkkojen toimivuus

- Elokuussa verkot toimivat vakaasti.
  - Poikkeamien vakavuusluokat: A: 1, B: 1, C: 1
- Yhteinen nimittäjä näille kolmelle joukkoviestintäpalveluihin vaikuttaneille häiriöille oli erilaiset laite- tai ohjelmistoviat.
  - Viat aiheuttivat hetkellisiä katkoksia radio ja tv -lähetyksissä eri puolilla Suomea.
- Kesän voidaan todeta olleen rauhallinen verkkojen osalta ja erilaisilta myrskyvahingoiltakin vältyttiin.
- Viranomaisverkko Virve siirtyy radioverkosta mobiiliverkkoon.
  - Artikkelissa kerrotaan Virve-verkosta, jolla on käyttäjiä yli 50 000 ja sen viesti- ja puhelumäärät ovat viikkotasolla miljoonaluokassa.[23]

Analyysi

- Ensi talvena myös verkkojen toimivuus korostuu.
  - Suomessa verkkojen toimivuus on turvattu tarvittavilla vara- ja varmistusratkaisuilla, mutta ylimääräiset sähkökatkot voisivat silti aiheuttaa häiriöitä verkko-operaattoreille.
  - Fingrid kertoo sivustollaan tulevan talven tilanteesta.[24]
- Kuukaudessa tapahtuu keskimäärin noin kuusi merkittävää toimivuushäiriötä.

ICT-palveluiden toimivuus

- Turun yliopistollinen keskussairaala kertoi tietojärjestelmähäiriöstään.
  - Pieleen mennyt IT-järjestelmäpäivitys johti hetkelliseen potilastietojärjestelmien toimimattomuuteen.[25]
- S-Pankissa tunnistautumiseen liittyvä järjestelmähäiriö.
  - Häiriö esiintyi 20.4.-5.8.2022 ja se vaikutti osaan asiakkaita.
  - Osalla asiakkaista oli mahdollisuus kirjautua toisen asiakkaan verkkopankkiin ja väärinkäytöksiä havaittiin pieni määrä.[26]

Analyysi

- Etukäteen toimivaksi testatut järjestelmäpäivitykset voivat silti aiheuttaa erilaisia vikatapauksia organisaatioille.
- On erittäin tärkeää testata ja suunnitella etukäteen myös palautumiskeinot ja toimenpiteet.
- Järjestelmäpäivityksen aiheuttama vikatila keskellä yötä voi olla haastava tilanne, mikäli palautuminen ei onnistukaan toivotusti.

Palvelunestohyökkäykset

- Elokuussa palvelunestohyökkäyksiä ilmoitettiin tuplasti enemmän, kuin kesä- ja heinäkuussa.
  - Palvelunestohyökkäykset vaikuttivat esimerkiksi eri verkkosivujen ja palveluiden toimintaan.
  - Raportoiduissa palvelunestohyökkäyksissä ei mässäilty liikenteen volyymilla, vaan hyökkäykset onnistuivat osassa tapauksia aiheuttamaan häiriöitä muilla teknisillä keinoilla.
- Eduskunnan verkkosivuille tehty hyökkäys 9.8. oli näyttävä tapa saada palvelunestohyökkäys nousemaan mediaan.
  - Hyökkäys aiheutti hetkellisesti Eduskunnan verkkosivujen kaatumisen.
  - Venäläinen ryhmittymä ilmoitti tehneensä hyökkäyksen, koska Suomi on liittymässä Natoon.[27]

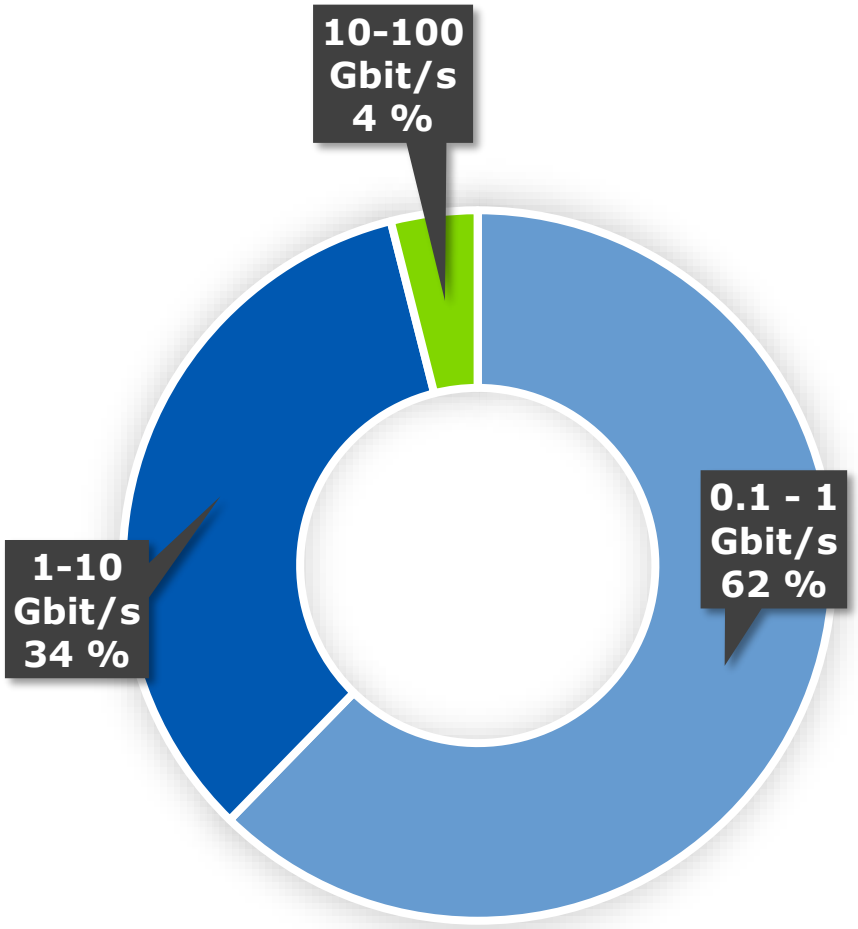
Analyysi

- Palvelunestohyökkäyksiä tapahtuu verkossa ja Suomessa päivittäin. Erilaiset ryhmittymät uhkailevat palvelunestohyökkäyksillä verkossa ja joskus toteuttavatkin niitä.
- Palvelunestohyökkäys on halpa ja helppo tapa aiheuttaa näkyvää haittaa verkossa, mutta yleensä ne aiheuttavat vain hetkellisiä saatavuusongelmia verkkosivuille.[28]
- Kyberturvallisuuskeskus listattiin myös elokuussa haittaryhmittymän sivulla palvelunestohyökkäyksen kohteeksi - merkkejä hyökkäyksestä ei havaittu.[29]
- Viime aikoina palvelunestohyökkäyksiä on pelillistetty erilaisilla sosiaalisen median alustoilla, joilla ryhmittyvät kannustavat ihmisiä liittymään hyökkäyksiin.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 119 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2/2022.
- Noin 79% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q2/2022 - 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

- Tietoturvayhtiö Fortinetin mukaan tietoja tuhoavia haittaohjelmia on havaittu vuoden ensimmäisen puoliskon aikana Ukrainan lisäksi 24 maassa.
  - Lukemaa selittää osaltaan mm. satelliittien toimintaan vaikuttanut AcidRain-haittaohjelma, joka kohdistui satelliittiyhteyksiin, mutta vaikutti muun muassa tuulivoimaloihin Saksassa.
  - Lisäksi Ukrainassa käytetyt tietoja tuhoavat haittaohjelmat ovat voineet aiheuttaa vaikutuksia myös muissa maissa.
- Myös Fortinet pitää merkillepantavana sitä, että uusien tunnistettujen tietoja tuhoavien haittaohjelmien määrä oli alkuvuonna poikkeuksellisen suuri aiempiin vuosiin verrattuna.
  - Tätä selittää Venäjän ja Ukrainan välinen sota, johon on liittynyt tietoja tuhoavien haittaohjelmien hyödyntämistä erityisesti Ukrainassa.

Analyysi

- Tietoja tuhoava haittaohjelma haittaa vakavasti organisaation toimintaa ja voi jopa estää sen.
- Erona kiristyshaittaohjelmiin on se, että tekijällä ei ole aikomustakaan pystyä palauttamaan tiedostoja, vaan kyse on puhtaasta sabotaasista.
- Joissain tapauksissa tietoja tuhoava haittaohjelma saattaa myös tehdä koko laitteen käyttökelvottomaksi.

Vakoilu

- Venäjän ulkomaantiedusteluun julkisuudessa yhdistetty APT29-ryhmä (Nobelium, Cozy Bear) on kehittänyt menetelmiään sekä Microsoft 365 -pilviympäristöihin kohdistuvissa hyökkäyksissä että on-premises-ympäristöissä.
  - Tietoturvayhtiö Mandiant kertoo APT29:n murtaneen epäaktiivisten tilien salasanoja sekä ottaneen niissä itse käyttöön monivaiheisen tunnistautumisen ja saaden sen avulla laajemman pääsyn organisaation verkkoon.
  - APT29:n oli lisäksi havaittu poistaneen kohdetileillä käytöstä Purview Audit -työkalun (aiemmin *Advanced Audit*), jotta uhriorganisaatio ei pystyisi selvittämään, mitä sähköposteja hyökkääjä on käsitellyt.
  - Lisäksi Microsoftin mukaan APT29:n uusi MagicWeb-työkalu mahdollistaa tunkeutumisen jälkeisen lateraalisen leviämisen, pysyvän jalansijan saavuttamisen ja tietojen keruun manipuloimalla autentikointiprosessia AD FS -palvelimen käyttämää kirjastoa muokkaamalla.
- Niin ikään Venäjään yhdistetty Callisto-ryhmä, jota aiheesta raportoinut Microsoft kutsuu nimellä SEABORGIUM, on jatkanut kohdistettua kalastelukampanjaa. Kampanja on kohdistunut yli 30 organisaatioon.
  - Kalastelun kohteet ovat tyypillisesti Nato-maita tai Pohjoismaita, Baltian maita tai Itä-Eurooppaa.
  - Callisto voi kohdistaa kalastelua myös merkittävässä asemassa olevien henkilöiden henkilökohtaisille sähköpostitileille.

Analyysi

- Monivaiheisen tunnistautumisen käyttöönotto kannattaa toteuttaa ns. väliaikaisella pääsyllä (*temporary access pass*). Tällöin MFA:n käyttöönotto itsessään vaatii jo oman MFA-koodin, eikä hyökkääjä pysty ottamaan käyttöön MFA:ta pelkästään käyttäjän kirjautumistiedoilla.[30]
- Lisäksi pääkäyttäjätilien vahva suojaus vahvoilla salasanoilla, monivaiheisella tunnistamisella ja muilla mahdollisilla menetelmillä on tärkeää, jotta estetään kuvatun kaltaisten toimenpiteiden tekeminen hyökkääjältä.

Vakoilu

- Kiinaan liitettyjen APT-ryhmien kampanjoita oli elokuussa esillä useita.
- Kiinaan liitetty toimija on esimerkiksi kohdistanut haitallisten sähköpostien kampanjan Australian hallintoon, mediaorganisaatioihin ja Eteläkiinanmeren tuulivoimaloita huoltaviin yrityksiin.
  - Kampanjaa tutkineet Proofpoint ja PwC arvioivat taustalla olevan mahdollisesti APT40.
- Winnti- ja APT41-nimillä tunnettu, niin ikään Kiinaan yhdistetty APT-ryhmä puolestaan on tiettävästi vakoillut ainakin 13 kohdetta eri puolilla maailmaa.
  - Kohdetoimialojen joukossa on ollut muun muassa julkinen sektori, teollisuustuotanto, terveydenhuolto ja logistiikka.
- Kiinan valtion tuella operoivaksi arvioitu RedAlpha-ryhmä puolestaan on pyrkinyt varastamaan humanitaaristen organisaatioiden, ajatushautomoiden ja valtionhallinnon organisaatioiden kirjautumistietoja osana monivuotista vakoilukampanjaa.

Analyysi

- Kirjautumistietojen varastaminen on yksi APT-toimijoiden yleisistä keinoista saada pääsy kohteena oleviin tietoihin tai järjestelmiin.
- Elokuussa esillä olleissa kampanjoissa merkillepantavaa on muun muassa vakoilun kohteena olevien organisaatioiden toimialojen laaja jakauma – vakoilun kohteeksi voi joutua monesta syystä.

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.

TRAFICOM

15.9.2022

Oikeudelliset asiat

Tunnistuspalveluiden avaintenvaihdon tietoturvaa kehitetään Traficomissa – luottamusverkoston rajapintasuosituksen päivitys lausuttavana.

- Luottamusverkostoon kuuluvien tunnistuspalvelun tarjoajien on mm. tarjottava tekniset rajapinnat, jotka luovat edellytykset tunnistuspalveluita tarjoavien ja niitä hyödyntävien toimijoiden väliselle toiminnalle.
  - Suositus on tarkoitettu luottamusverkostoon kuuluville tunnistuspalvelun tarjoajille.
- Suositukseen ehdotetaan lisättäväksi uusi kappale 4, jossa käsitellään OpenID Connect Federation määrittelyn (osien) käyttöä luottamusverkostossa.
  - Tarkoitus ei ole ottaa OpenID Connect Federation määrittelyä käyttöön kokonaisuudessaan.
  - Tarkoitus kirjata minimivaatimukset, jotka tulisi ottaa huomioon sanomatason salaus- ja allekirjoitusavainten hallinnan automatisoimiseksi.
- Luonnos Liikenne- ja viestintäviraston suosituksen 213/2021 S Luottamusverkoston rajapinnasta muuttamiseksi julkaistu lausuntopalvelussa ja lausuntoaika päättyy 30.9.2022.[(32)]

Oikeudelliset asiat

Suositus salassa pidettävien asiakirjojen käsittelystä lausuttavana.[(32)]

- Suosituksen tavoitteena on opastaa salassa pidettävien asiakirjojen (tietojen), käsittelyssä sekä käsittelyä koskevien vaatimusten täyttämisessä.
- Suositus on tarkoitettu ensisijaisesti tiedonhallintayksiköille ja viranomaisille, mutta suositusta voivat hyödyntää elinkeinoelämän toimijat ja muut, jotka käsittelevät viranomaisten salassa pidettäväksi määrittelemiä asiakirjoja.
- Suosituksessa kuvataan salassa pidettävien asiakirjojen käsittelyn lainsäädännölliset perusteet, suosituksen suhde muihin tiedonhallintalautakunnan suosituksiin, käsittelyä koskevat lainsäädäntöön perustuvat vähimmäisvaatimukset ja niiden riskilähtöisen täydentämisen sekä suositukset salassa pidettävien tietojen suojaamiseksi.
  - Salassa pidettävien asiakirjojen suojaaminen huomioidaan koko niiden elinkaaren ajan.
- Tiedonhallintalautakunnan tietoturvallisuusjaosto pyytää huomioita suositusluonnoksesta 21.9.2022 mennessä.

Oikeudelliset asiat

Suomen digitaalisen kompassin 2. luonnos lausuttavana 16.9. asti.[33]

- Digitalisaation ja datatalouden murroksessa menestymiseksi ja kansallisen digitalisaatiokehityksen ohjaamiseksi Suomelle ollaan laatimassa vuoteen 2030 ulottuvaa kansallista strategista etenemissuunnitelmaa - digitaalista kompassia.
  - Tavoitteena luoda digitalisaatiolle ja datataloudelle yhteinen kansallinen visio ja tavoitteet vuoteen 2030.
- Digikompassi muodostuu neljästä osa-alueesta: osaaminen, digitaalinen infrastruktuuri, yritysten digitalisaatio ja digitaaliset julkiset palvelut.
- Digikompassi tukee valtionhallinnon toimien priorisointia, resurssien kohdentamista ja yhteiskunnallisen vaikuttavuuden arviointia sekä Suomen aseman arviointia suhteessa kansainväliseen kehitykseen.

Oikeudelliset asiat

US CLOUD-Act voi ulottua Euroopassa sijaitsevaan dataan.

- Eurooppalaiset yhtiöt, joiden datan käsittely tapahtuu Euroopassa, voivat joissain tapauksissa olla Yhdysvaltojen CLOUD-Act lain soveltamisalan piirissä.
- Yhdysvaltojen hallinnolla voi CLOUD-Actin nojalla olla tietyin edellytyksin pääsy eurooppalaisilla palvelimilla olevaan dataan.
- Alankomaiden kyberturvallisuusviranomainen NCSC-NL on selvittänyt asiaa asianajotoimiston avulla.
- Asian analyysi osoittaa, että datan omistajan tai käsittelijän on haastavaa tietää, kohdistuuko palveluun tai palvelun tarjoajaan velvoittavaa sääntelyä myös Euroopan ulkopuolelta.
- Blogikirjoitus ja arviomuistio saatavilla NCSC-NL:n verkkosivuilta.[(34)]

Oikeudelliset asiat

Hallituksen esitys laeiksi maa-asemista ja eräistä tutkista sekä avaruustoiminnasta annetun lain muuttamisesta ja sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta annettu eduskunnalle.[(35)]

- Hallituksen esityksessä esitetään säädettäväksi laki maa-asemista ja eräistä tutkista ja muutettavaksi avaruustoiminnasta annettua lakia ja sakon täytäntöönpanosta annettua lakia.
- Laissa säädettäisiin maa-aseman tai tutkan perustamisen sekä maa-asema- ja tutkatoiminnan luvanvaraisuudesta. Lupaviranomaisena toimisi Liikenne- ja viestintävirasto.
  - Luvan edellytyksenä olisi erityisesti toiminnan riskittömyys kansallisen turvallisuuden kannalta ja tiettyjen teknisten turvallisuusvaatimusten täyttyminen. Luvan käsittelyä varten pyydettäisiin lausuntoa turvallisuusviranomaisilta. Toiminnanharjoittaja olisi velvollinen raportoimaan toiminnastaan ja asiakkaistaan lupaviranomaiselle.
- Lisäksi esitetään muutettavaksi avaruustoiminnasta annettua lakia lisäämällä lakiin säännökset, jotka koskevat satelliittikaukokartoituksen harjoittamista. Satelliittikaukokartoituksen harjoittaminen olisi luvanvaraista. Lupaviranomaisena toimisi työ- ja elinkeinoministeriö, joka toimii myös avaruustoiminnan lupaviranomaisena.
  - Luvan edellytyksenä olisi erityisesti toiminnan riskittömyys kansallisen turvallisuuden kannalta ja tiettyjen teknisten turvallisuusvaatimusten täyttyminen. Luvan käsittelyä varten pyydettäisiin lausuntoa turvallisuusviranomaisilta. Toiminnanharjoittaja olisi velvollinen raportoimaan toiminnastaan ja asiakkaistaan lupaviranomaiselle.
- Lait on tarkoitettu tulemaan voimaan mahdollisimman pian.

Arjen kyberturvallisuus

Äly- ja digilaitteetkin kuuluvat kierrätykseen

- Vanhat sähkö- ja elektroniikkalaitteet jäävät usein pöytälaatikkoon pölyttymään.
- Käytöstä pois jääneet laitteet sisältävät paljon käyttökelpoisia arvometalleja. Kun kierrätämme nämä materiaalit, vauhditamme kestävää digitalisaatiota ja esimerkiksi liikenteen sähköistymistä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/aly-ja-digilaitteetkin-kuuluvat-kierratykseen

Salasanat haltuun – vinkkejä hyviin salasanoihin

- Tärkeät tiedot ja digitaalinen omaisuus kannattaa suojata mahdollisimman huolellisesti, jotta ne eivät päädy vääriin käsiin. Ohjeessa kerromme turvallisista tunnistautumiskäytännöistä ja annamme vinkkejä salasanojen hallintaan.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

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

Nasevia neuvoja tiliesi turvaamiseksi

- Verkkopalveluissa käytettäviä tilejä yritetään murtaa ja ottaa haltuun usein eri keinoin. Tähän artikkeliin on koostettu lyhyet ohjeet ennakkoon suojautumisen kannalta, sekä mitä tehdä murron tapahduttua.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

Uutisia Kyberturvallisuuskeskuksesta

Kyberturvallisuuskeskus aloitti uuden viikkokatsauksen julkaisemisen

- Viikkokatsauksessa jaamme tietoa ajankohtaisista kyberilmiöistä suomen kielellä. Viikkokatsaus on tarkoitettu laajalle yleisölle kyberturvallisuuden ammattilaisista tavallisiin kansalaisiin.
- Viikkokatsaus julkaistaan joka torstai.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-362022

Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt

- Kyberhyökkäykset ovat lisääntyneet maailmanlaajuisesti kuluvan vuoden aikana. Samalla niitä kohdistuu hiljaisemman kevään jälkeen kasvavassa määrin myös Suomeen.
- Kyberturvallisuuskeskuksen saamien ilmoitusten mukaan suomalaisiin organisaatioihin kohdistuvissa kyberhyökkäyksissä, erityisesti haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten lukumäärät ovat kasvaneet.
- https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

Kansainvälinen tiedonvaihtoprotokolla (TLP) päivittyi versioon 2.0

- Kansainvälinen poikkeamanhallinnan ja turvallisuuden foorumi (FIRST) on julkaissut uuden version vuonna 2017 esitellystä liikennevaloprotokollasta (TLP - Traffic Light Protocol).
- Liikennevaloprotokollan tarkoituksena on ollut yhdenmukaistaa tiedonvaihtokäytäntöjä sekä parantaa kansainvälisten ja kansallisten julkisen sekä yksityisen sektorin toimijoiden välistä tiedonvaihtoa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kansainvalinen-tiedonvaihtoprotokolla-tlp-paivittyi-versioon-20

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) Kyberturvallisuuskeskuksen tiedote kohonneesta kyberuhkatasosta https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

2) Kyberturvallisuuskeskuksen ohjeet ja oppaat https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

3) ISAC-ryhmät https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

4) Uudistettu määräys 28 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-ja-suomalaiset-teleoperaattorit-yhteistyossa-numeron-vaarentamista-vastaan

5) Toiminta kiristyshaittaohjelmatilanteessa – johdon ohje https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toiminta%20kiristyshaittaohjelmatilanteessa%20-%20johdon%20ohje.pdf

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

7) Traficomin haittaohjelmahavainnot https://tieto.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot

8) Bitbucket Server and Data Center Advisory 2022-08-24 https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-advisory-2022-08-24-1155489835.html

Lähdeluettelo

9) Kyberturvallisuuskeskuksen viikkokatsaus 35/2022
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-uusi-viikkokatsaus-352022

10) CISA known exploited vulnerabilities catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog

11) VMWARE esimerkkikoodi https://www.vmware.com/security/advisories/VMSA-2022-0021.html

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

13) Tietoturvamerkki –seminaari https://tietoturvamerkki.fi/fi/tietoturvamerkki-seminaari-2022

14) POLITICO's back-to-school policy briefing: What you need to know (and worry about) https://www.politico.eu/article/politicos-back-to-school-policy-briefing-what-you-need-to-know-and-worry-about/

15) ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines https://www.iso.org/standard/44373.html

16) ISO/IEC CD 27402.2 Cybersecurity — IoT security and privacy — Device baseline requirements
https://www.iso.org/standard/80136.html

17) ISO/IEC CD 27403.2 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
https://www.iso.org/standard/78702.html

Lähdeluettelo

18) ISO/IEC 27404 — Information security — Security techniques — Universal cybersecurity labelling framework for consumer IoT https://www.iso27001security.com/html/27404.html

19) ISO/IEC 27400:2022 — Cybersecurity — IoT security and privacy — Guidelines https://www.iso27001security.com/html/27400.html

20) Blackhat, Attacks from a New Front Door in 4G & 5G mobile networks https://i.blackhat.com/USA-22/Wednesday/US-22-Shaik-Attacks-From-a-New-Front-Door-in-4G-5G-Mobile-Networks.pdf

21) Liikenne- ja viestintävirasto julkaisi selvityksen 5G:n kyberturvallisuudesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-julkaisi-selvityksen-5gn-kyberturvallisuudesta-0

22) Liikenne- ja viestintävirasto Traficom järjestää maailman ensimmäisen 5G:n kyberturvallisuutta koskevan hackathonin Oulussa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-traficom-jarjestaa-maailman-ensimmaisen-5gn

23) Yle: Virve harppaa radiopuhelimesta älypuhelimeen https://yle.fi/uutiset/3-12593038

24) Fingrid: tietoa sähköpulasta https://www.fingrid.fi/kantaverkko/tietoa-sahkopulasta/

25) Turun Sanomat: Tyksin laaja tietojärjestelmähäiriö korjattu, kertynyttä ruuhkaa päästään purkamaan https://www.ts.fi/uutiset/5737546

Lähdeluettelo

26) S-Pankin tunnistautumisessa järjestelmähäiriö kesällä https://www.s-pankki.fi/fi/tiedotteet/2022/s-pankin-tunnistautumisessa-jarjestelmahairio-kesalla--tilanne-on-korjattu-ja-kaikkiin-asiakkaisiin-joita-hairio-koski-ollaan-yhteydessa/

27) Yle: Venäläinen hakkeriryhmä ilmoittautui eduskunnan sivujen kaatajaksi https://yle.fi/uutiset/3-12569629

28) Palvelunestohyökkäykset ovat arkipäivää Suomessa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa

29) Venäläinen hakkeriryhmä väittää tehneensä jo toisen palvelunestohyökkäyksen – kohteena valtioneuvoston julkaisuarkisto https://yle.fi/uutiset/3-12571164

30) Configure Temporary Access Pass in Azure AD to register Passwordless authentication methods https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-temporary-access-pass#create-a-temporary-access-pass

31) Luottamusverkoston OIDC-rajapintasuosituksen päivitys https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=292b91d3-6f72-4cef-9750-8d1b947109ab

32) Suositus salassa pidettävien asiakirjojen käsittelystä https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=8425202b-6f15-4ef7-a8cf-f50a378c698b

33) Suomen digitaalinen kompassi, 2. luonnos https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=03e2914d-c51b-4534-9785-2a5f84861c05

Lähdeluettelo

34) NCSC-NL: How the CLOUD-Act works in data storage in Europe https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe

35) Hallituksen esitys HE 113/2022 https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_113+2022.aspx