TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 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

17.3.2022

Kybersää helmikuu 2022

Tietomurrot ja -vuodot

- Savonia-ammattikorkeakoulu kertoi joutuneensa kyberhyökkäyksen kohteeksi.
- Kunta-alaan kohdistui laajahko tietojenkalastelukampanja joka johti useampaan onnistuneeseen tietomurtoon.

Huijaukset ja kalastelut

- Huijaukset internetin myyntipalstoilla ovat jatkuneet vilkkaina.
- Sosiaalisen median tunnuksia kaapataan uusilla metkuilla.

Haittaohjelmat ja haavoittuvuudet

- Haittaohjelmia on kohdistettu Ukrainalaisia organisaatiota kohtaan.
- Linuxin kernelissä on erittäin kriittinen haavoittuvuus, joka mahdollistaa käyttöoikeuksien korottamisen.

IoT

- Useita kriittisiä haavoittuvuuksia löydettiin mm. IoT-järjestelmien hallinnointiin ja etävalvontaan käytetystä integrointialustasta.

Verkkojen toimivuus

- Verkkojen toimivuus Suomessa on tällä hetkellä hyvä.
- Palvelunestohyökkäys vaikutti laajasti pankin toimintaan.
- Palvelunestohyökkäysten trendi kuitenkin tasaista aaltoilua.

Vakoilu

- Ukrainassa on havaittu Venäjän hyökkäyksen jälkeen useita tietoja tuhoavia haittaohjelmia, kalastelua sekä palvelunestohyökkäyksiä.
- Yhdysvalloissa kerrottiin merkittävistä puolustusteollisuuteen ja media-alaan kohdistuneista vakoilutapauksista.
- Iranilainen MuddyWater-ryhmä vakoilee aktiivisesti monia toimialoja.

TRAFICOM

17.3.2022

Kuukauden tunnuslukuja

2x

Kyberturvallisuuskeskukselle ilmoitettujen huijausyrityksien määrät ovat kaksinkertaistuneet joulukuun 2021 jälkeen.

1

Ukrainan sota aiheuttaa lieveilmiöitä maailmalla. Kyberturvallisuuskeskus julkaisi ohjeen johdolle ja asiantuntijoille kyberturvallisuuden vahvistamiseksi.

27002

Tietoturvallisuuden hallinnan standardisarjaan kuuluvasta hallintakeinojen standardista ISO/IEC 27002 ilmestyi uusi versio helmikuussa.

Ukrainan sodan vaikutukset Suomen kyberturvallisuuteen

- Suomessa kyberturvallisuuden tilanne on tällä hetkellä vakaa. Viestintäverkot toimivat normaalisti.
- Kyberturvallisuuskeskus julkaisi ohjeet organisaatioiden johdolle ja asiantuntijoille kyberturvallisuuden vahvistamiseksi.
  - Uudessa ohjeessa kehotetaan aktiivisesti tarkastelemaan organisaation kaikkia tietojärjestelmiä ja tietoliikenneyhteyksiä, joita organisaatio käyttää sisäisesti omassa toiminnassaan ja joiden kautta organisaatio tarjoaa asiakkailleen palveluja.
  - Tutustu ohjeeseen https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille

Analyysi

- Kyberhyökkäyksiä ja muita kybermaailman ilmiöitä tapahtuu jatkuvasti. Tämän hetken tapahtumia ei voida automaattisesti yhdistää osaksi Ukrainan sotaa. Mikäli organisaatio on tietoturvaloukkauksen uhrina, tulee sen tehdä tietoturvatutkinta. Tämän lisäksi suosittelemme rikosilmoituksen tekoa sekä ilmoittamista Kyberturvallisuuskeskukselle.
- Kybermaailman ilmiöt voivat mahdollisesti vaikuttaa myös kriittiseen infrastruktuuriin sekä toiminnan ja tuotannon jatkuvuuteen.
- Organisaatioiden kyberturvallisuuden varautuminen on syytä laittaa kuntoon hyvän sään aikana, koska ilmiöt voivat näkyä nopeina ja ennakoimattomina muutoksina.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

2

Johtaminen ja riskienhallinta. Toimintaympäristön nopeat muutokset koettelevat organisaatioiden riskienhallintaa kyberturvallisuudessa. Johdon vastuulla on varmistaa riskienhallinnan vaikuttavuus.

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

17.3.2022

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Digitaalisuus läpileikkaa koko organisaation toimintaa ja erilaiset tapahtumat voivat vaikuttaa merkittävästi organisaation jatkuvuuden- ja riskienhallintaan.

- Muutokset kansainvälisten ilmiöiden kehityksessä näkyvät vaihtelevilla voimakkuuksilla Suomessa
- Esimerkiksi pitkittynyt koronaviruspandemia, talouden äkilliset muutokset, luonnonilmiöt, energian hinnannousu, sekä ennakoimaton kansainvälinen turvallisuustilanne näkyvät vaikeasti ennakoitavina kehityskulkuina, ja muutokset saattavat tapahtua nopeastikin
- Epävarmuustekijöillä voi yksistään olla isoja vaikutuksia organisaatioiden toimintaan. Yhdessä nämä ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia myös kyberturvallisuuden toimintaympäristössä
- Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön aiheuttamat uhkat kriittisille prosesseille

CASE

Toimitusketjut häiriintyivät koronapandemian alkaessa vakavasti. Esimerkiksi puolijohteiden saatavuus on ollut jo pidemmän aikaa huono eikä sirupula näytä helpottamisen merkkejä vielä lähikuukausina. Organisaatiot saattavat joutua odottamaan uusia laitteita kuukausikaupalla ja siten joutua käyttämään elinkaaren päässä olevia laitteita pidempään ja uusien suojausratkaisujen rakentamisessa kestää suunniteltua pidempään. Laitekaupoilla kannattaakin olla tarkkana, sillä saatavuushäiriöt ja hintojen nousu houkuttelevat markkinoille myös halpoja kopioita.

2. Johtamisella riskienhallintaa

Monen organisaation riskienhallinta ei pysy digitalisaation vauhdissa. Digitaalisia ratkaisuja otetaan käyttöön sokkona ilman riskien ymmärtämistä ja arviointia. Lopputulos saattaa olla riskialtis niin kansalaisen, organisaation itsensä kuin koko yhteiskunnan kannalta.

Organisaation riskienhallinta on viime kädessä johdon vastuulla. Johdon tulee seurata riskienhallinnan toteutumisesta vähintään:

- **Toimintaympäristön määrittely**. Organisaation tulee tunnistaa sen kriittiset prosessit ja mitä uhkia toimintaympäristö muodostaa
- **Riskien arviointi.** Organisaation on edellisen vaiheen pohjalta tunnistettava ja arvioitava riskit, sekä miten ne vaikuttavat kriittisiin prosesseihin
- **Riskien käsittely.** Kun riskit on arvioitu, organisaation tulee toteuttaa riittävät hallintatoimenpiteet riskien vaikutusten vähentämiseksi
- **Seuranta ja katselmointi.** Organisaation tulee seurata riskienhallintatoimenpiteiden vaikuttavuutta. Toimintaympäristön muutoksia ja omaa varautumista riskeihin tulee jatkuvasti seurata ja katselmoida

CASE

Esimerkkiskenaariossa organisaatio ei ole analysoinut toimintaympäristöään, eikä siten ole kyennyt arvioimaan sen vaikutuksia kriittisiin prosesseihinsa. Puutteellinen digitaalinen ratkaisu otetaan käyttöön tiedostamatta uhkaa. Riski, joka olisi ollut tunnistettavissa, realisoituu. Organisaation kriittinen prosessi pysähtyy, aiheuttaa mittavan mainehaitan sekä taloudelliset menetykset. Myös asiakkaiden tiedot ovat vaarantuneet. Riskin hallintatoimenpiteiden kustannukset olisivat olleet murto-osan asian korjaamisesta aiheutuneista kuluista.

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
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja-tietomurroilta ja https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

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

- Savonia-ammattikorkeakouluun on kohdistui kyberhyökkäys.
  - Itä-Suomen poliisilaitos tiedotti 16.2.2022 jatkavansa Savonia-ammattikorkeakouluun kohdistunutta epäiltyä törkeää tietomurron, törkeää tietojärjestelmän häirinnän ja törkeää datavahingonteon tutkintaa.
  - Tämänhetkisen tiedon mukaan tietomurron kohteena oleva tietomäärä on pieni, eikä se ole kohdistunut arkaluontoisiin tietoihin.
  - Uutislähteiden mukaan kyseessä on kiristyshaittaohjelmaisku, joka on lukinnut verkkolevyillä sijainneita tiedostoja ja niiden avaamiseksi vaadittiin bitcoin-lunnaita. Iskun seurauksena opettajat eivät ole päässeet käsiksi kaikkiin tiedostoihin.

Analyysi

- Oman digitaalisen ympäristön tunteminen on tärkeää.
- Kiristyshaittaohjelma on rikolliselle tuottoisa tapa toteuttaa rikos ja sen riskit ovat vähäiset.
- Kiristyshaittaohjelma on helppo toteuttaa ja kohdentaa kerta toisensa jälkeen eri vastaanottajille.
- Tee poliisille rikosilmoitus, jos epäilet joutuneesi tai olet joutunut onnistuneen tietomurron uhriksi.

Tietomurrot ja –vuodot

- Kunta-alaan kohdistui laajahko tietojenkalastelukampanja joka johti useampaan onnistuneeseen tietomurtoon.
  - Suomessa oli helmikuussa aktiivinen kalastelukampanja, joka suuntautui etenkin kunta-alan toimijoihin.
  - Tutusta sähköpostiosoitteesta tuli tietoja kalasteleva viesti.
    - Linkin syyksi mainittiin lasku tai jokin muu työhön liittyvä dokumentti. Linkin klikkaaminen vei kalastelusivustolle, jossa pyrittiin saamaan haltuun kohteen tunnukset.
  - Tietojen hyödyntäminen uusien viestien lähettämiseen oli tässä kalastelukampanjassa aktiivista ja nopeaa.

Analyysi

- Kaksivaiheisen tunnistautumisen käyttöönotto on merkittävä keino estää rikollisten mahdollisuuksia hyödyntää tietojenkalastelua ja tehdä tietomurtoja.
- Tietojenkalastelun nopea havaitseminen auttaa vahinkojen ennaltaehkäisyssä. Tietojenkalastelu on usein onnistuneen tietomurron ensimmäinen vaihe.
- Tietomurto on rikoslaissa määritelty rangaistava teko ja myös tietomurron yritys on rangaistavaa.
- Suosittelemme tekemään rikosilmoituksen myös tietomurron yrityksistä.

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

- Murrettuja sähköpostitilejä on käytetty toimitusjohtajahuijauksiin, jossa johtajan nimissä yritetään maksattaa valelaskuja.
  - Onneksi työntekijät ovat useimmiten tarkkoina eikä vääriä laskuja makseta rikollisten käyttämille tileille.
- Tilausansoja on viritetty tekstiviestihuijauksilla K-marketin arvonnan nimissä.
- Pornokiristyksissä uhataan paljastaa arkaluontoisia tietoja, ellei uhri maksa lunnaita. Kaikki on huijausta.

Pankkitunnuskalastelu on kansainvälistä rikollisuutta

- Pankkikalastelussa on urkittu lähes kaikkien verkkopankkien kirjautumistunnuksia: OP, Nordea, Danske Bank, Säästöpankki.
- Pankkitunnusten kalastelu on kansainvälistä rikollisuutta, jossa käytetään laajasti eri maissa toimivien pankkien nimiä.
- Suomessa näkyi helmikuussa mm. Belgian postin nimissä lähetettyjä huijausviestejä.

Myyntipalstahuijaukset

- Huijareita liikkuu internetin myyntipalstoilla.
- Kyberturvallisuuskeskukselle ilmoitettujen huijausyrityksien määrät ovat kaksinkertaistuneet joulukuun 2021 jälkeen.
- Huijausyrityksessä tarkoituksena on saada myyjän pankkitiedot huijarin haltuun.
- Erilaisilla myyntialustoilla, kuten Tori.fi ja Facebook Marketplace on liikkunut viime aikoina kuriiriteemaisia huijauksia.

Kuriirihuijaukset etenevät samalla kaavalla:

1. Myyjä on laittanut esineen myyntiin.
2. Ostajaehdokas ottaa yhteyttä pikaviestinsovelluksessa (usein WhatsApp), ja kyselee tuotteen kunnosta.
3. Ostaja tarjoutuu ostamaan tuotteen kuriiripalvelun avulla.
4. Ostaja lähettää linkin kuriiripalvelun verkkosivuille, josta voi lunastaa rahat ja varata ajan.
5. Kuriiripalvelun sivustolle täytyy syöttää luottokorttitiedot maksun suorittamista varten, myyjä syöttää tiedot.
6. Myyjän syöttämät tiedot ovat nyt rikollisen hallussa.

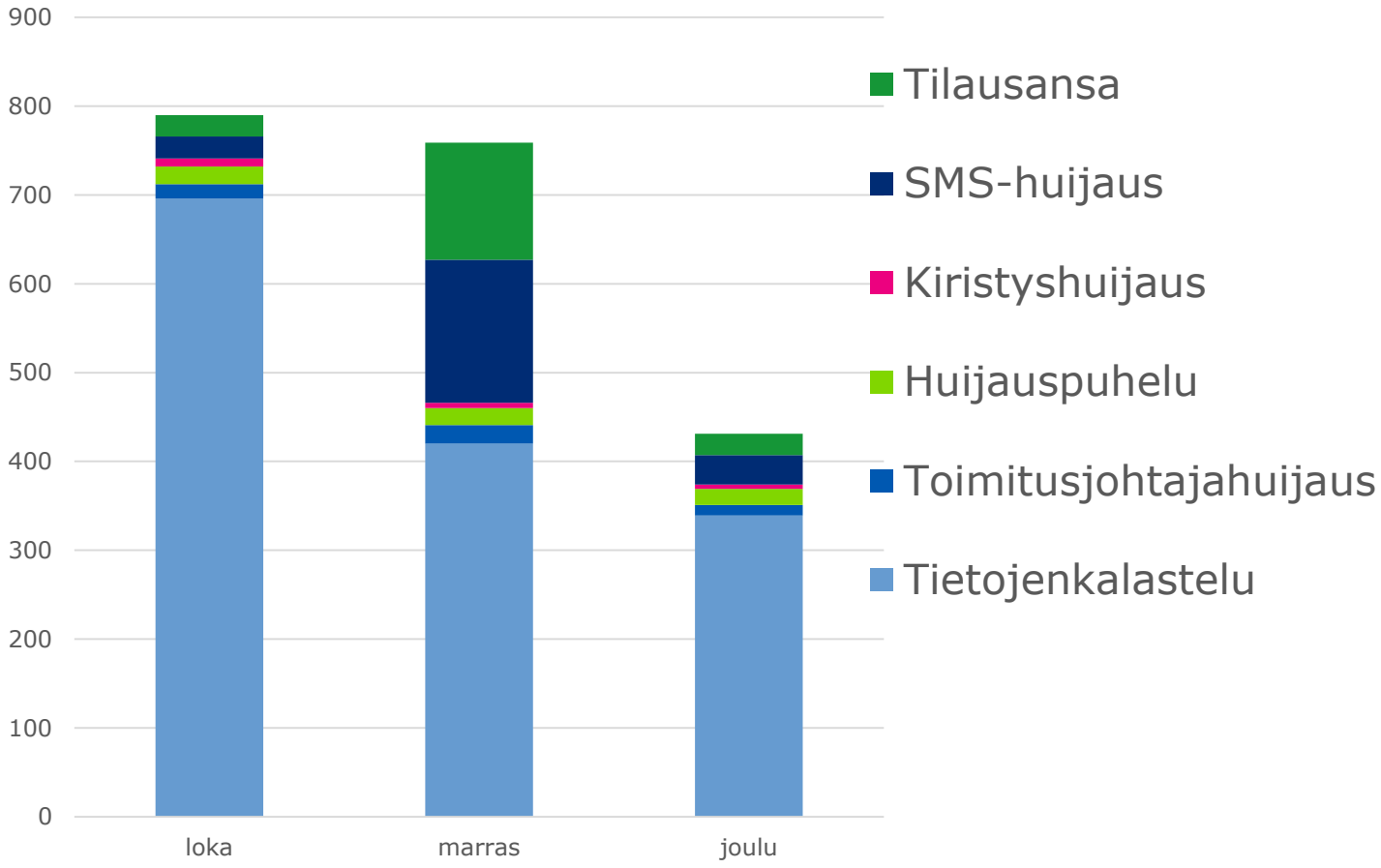
Huijaukset ja kalastelut

- Sometilikaappaukset jatkuvat.
  - Facebook- ja Instagram-tilejä on varastettu edelleen helmikuussa.
  - Samanlainen hyökkäystapa on jatkunut jo pitkään: Murretulta tililtä lähetetään viesti, jossa kysellään vastaanottajan puhelinnumeroa. Seuraavaksi urkitaan kaksivaiheisen tunnistautumisen koodi väittämällä sitä "arvontakoodiksi".
  - Uusin muunnelma samasta huijauksesta on nyt osallistuminen kokkikilpailuun, jossa voi voittaa 8200 euroa. Tälläkään kertaa puhelimeen tuleva koodi ei liity mihinkään kilpailuun, vaan sen avulla rikollinen kaappaa tilin omaan haltuunsa.
  - Rikollisen motiivi on urkkia haltuunsa uhrien luottokorttinumeroita ja viedä niillä rahaa.

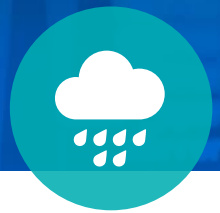
Suojaa tilisi jo etukäteen

- Kaapatun sometilin palauttaminen on työlästä ja hidasta.
- Etukäteen suojautuminen ja varautuminen voi säästää isoilta harmeilta ja ikävyyksiltä.
- Katso Kyberturvallisuuden neuvot tilien suojaamiseksi: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi
- Tutulta kaveriltakin tullut viesti voi olla huijarin kirjoittama. Älä luovuta tietoja äläkä koodeja. Tunnista huijaukset: https://www.kyberturvallisuuskeskus.fi/fi/ttn_20012022

Käsiteltyjä huijaustapauksia Q4/2021



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



Haittaohjelmat ja haavoittuvuudet

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

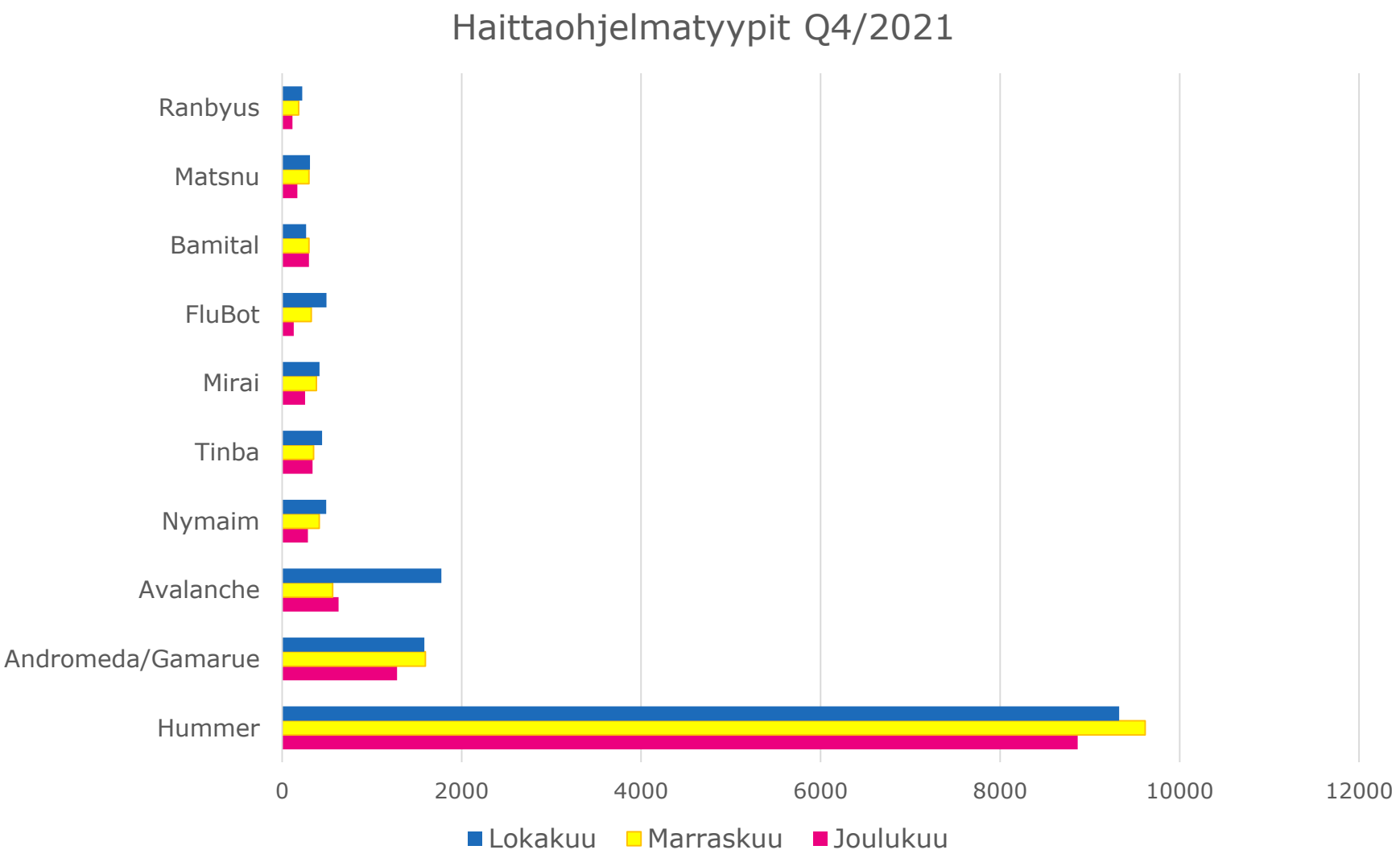
Haittaohjelmat

- Haittaohjelmia on kohdistettu erityisesti Ukrainalaisia organisaatiota kohtaan.
  - Tammikuun puolivälissä MSTIC (Microsoft Threat Intelligence Center) kertoi löytäneensä WhisperGate-haittaohjelman.
    - WhisperGate on tehty erityisen tuhoisaksi ja sen tarkoitus on saada kohteena olleet laitteet käyttökelvottomiksi.
  - HermeticWiper-haittaohjelmaa kohdistetaan Windows-laitteisiin, joissa muokataan käynnistyssektoria (MBR) niin että käynnistyminen estyy.
  - Conti-rikollisryhmän tietoja vuodettiin julkisuuteen ryhmässä työskentelevän henkilön toimesta.
    - Tietovuodossa vuodettiin ainakin Conti- ja Trickbot-haittaohjelmien lähdekoodit, salauksen purkuavain ja ryhmittymän sisäistä viestinvaihtoa.

Analyysi

- Tuhoisa haittaohjelma voi pahimmillaan vaarantaa organisaatioiden päivittäisen toiminnan.
- Haittaohjelma voi myös vaikuttaa tiedon saatavuuteen ja mikäli varmuuskopiot eivät ole eristettynä omassa ympäristössään voi haittaohjelma tuhota tai lukita myös ne.
- Ukrainalaisia organisaatiota kohtaan tehdyt kyberhyökkäykset voivat vaikuttaa myös muiden maiden organisaatioihin.

Autoreporterin haittaohjelmahavainnot



3kk

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

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Niistä voi lukea tarkempia tietoja kotisivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Haavoittuvuus

- Linuxin kernelissä erittäin kriittinen haavoittuvuus.
  - Linuxin kernelissä 5.8 versiosta ylöspäin on löydetty kriittinen haavoittuvuus (CVE-2022-0847), joka mahdollistaa käyttöoikeuksien korottamisen.
  - Haavoittuvuus vaikuttaa myös Android-laitteisiin.
  - Tämä haavoittuvuus on nimetty “Dirty Pipe”:ksi ja se mahdollistaa paikallisille käyttäjille root-oikeuksien hankkimisen.
  - Haavoittuvuuteen on jo julkaistu hyväksikäytön mahdollistava esimerkkikoodi.
  - Haavoittuvuus muistuttaa 2016 korjattua “Dirty COW”-haavoittuvuutta.

Analyysi

- Tämä haavoittuvuus on erityisen huolestuttava verkkopalveluita tarjoaville tahoille, jotka tarjoavat pääsyä Linuxin shellin kautta.
- Linux on viimeisen vuoden aikana julkaissut useita käyttöoikeuksien korottamisen mahdollistavia haavoittuvuuksia.
- Päivitykset tulisi asentaa viipymättä.

Kuukauden haavoittuvuusjulkaisut

- Kriittinen SAP-haavoittuvuus tulisi päivittää välittömästi (3/2022).
- Kriittinen haavoittuvuus Adobe Commerce- ja Magento-verkkokauppa-alustoissa (4/2022).
- Useita haavoittuvuuksia yleisesti käytetyssä PTC Axeda -alustassa (5/2022).

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

Analyysi

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

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 5 kpl (tilanne 15.3.2022).**
  - 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

Automaatio ja IoT

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.

IoT

- Erilaisten järjestelmien hallinnointiin ja valvontaan käytetystä PTC:n Axeda –integrointialustasta löydettiin useita kriittisiä haavoittuvuuksia. Haavoittuvuuden mahdollistavat hyökkääjälle komentojen suorittamisen etänä.
- Axedan alustalla valvotaan lukuisia erilaisia järjestelmiä ja se voi olla niissä ohjelmallisesti mukana.
- Erityisesti lääkinnällisissä laitteissa on hyödynnetty paljon Axedan alustaa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_5/2022

Analyysi

- Laitevalmistajien tulee selvittää onko heillä Axedan haavoittuvaa alustaa omissa ratkaisuissaan käytössä. Näihin palveluihin tulee julkaista korjaukset heti kun mahdollista.
- Organisaatioiden tulee etsiä omista ympäristöistään mahdolliset haavoittuvat toteutukset ja seurata laitevalmistajien julkaisemia päivityksiä. Organisaatiot ovat voineet toteuttaa omien järjestelmien valvontaa Axedan alustalla, ja näiden tilanne pitää selvittää.
- Suosittelemme laitevalmistajia hyödyntämään SBOM-materiaaliluetteloa. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-hallintaan-sbommin-varmasti?

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

- Tammikuussa yleisissä viestintäpalveluissa oli 2 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 1, C: 1
  - Viat johtuivat ohjelmisto- tai konfiguraatiovirheistä
- Verkkojen toimivuus Suomessa on tällä hetkellä hyvä.
- Satelliittiyhteyksiä tarjoava Viasat ilmoitti yhteysongelmista KA-SAT-verkossaan Ukrainassa ja muualla Euroopassa .
  - Häiriöiden taustalla oli ulkoinen vaikuttaminen kyberhyökkäyksellä.
  - https://www.zdnet.com/article/viasat-confirms-cyberattack-causing-outages-across-europe/

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa oli vuonna 2021 keskimäärin hyvä.
- Kuukaudessa on keskimäärin noin kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

Palvelunestohyökkäykset

- Palvelunestohyökkäyksiä ilmoitetaan meille tasaiseen tahtiin.
  - Helmikuu oli palvelunestohyökkäysten osalta rauhallinen – tammikuussa hyökkäyksistä ilmoitettiin aktiivisemmin.
- Nordean palveluihin kohdistunut hyökkäys nousi laajasti mediaan maaliskuun alussa.
  - Hyökkäys esti tavallisten käyttäjien tunnistautumispalveluja.
  - Laaja spekulaatio hyökkäyksestä ja ajankohdasta käynnistyi välittömästi.

Analyysi

- Palvelunestohyökkäyksiä ei voida automaattisesti liittää osaksi Ukrainan tapahtumia tai osaksi niiden heijastevaikutuksia.
- Hyökkäysten alkuperää on yleisesti hankala selvittää, koska lähdeosoitteiden takana voi olla saastunut laite, joka on osa hyökkäyksessä käytettyä bottiverkkoa.

Palvelunestohyökkäykset

- Palvelunestohyökkäykset ovat olleet osa Ukrainan sodan kyberhäiriköintiä.
  - Monet hallinnon ja finanssisektorin organisaatiot Ukrainassa vastaanottivat palvelunestohyökkäyksiä juuri ennen Venäjän hyökkäystä
  - Palvelunestohyökkäyksistä raportoitiin jo viikkoja ennen fyysistä hyökkäystä.
  - Hyökkäyksissä käytettiin esimerkiksi Katana-nimistä Botnetiä ja samoihin aikoihin Ukrainan kansalaiset vastaanottivat tekstiviestillä ilmoituksia, että pankkiautomaatitkaan eivät toimisi.
    - https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/

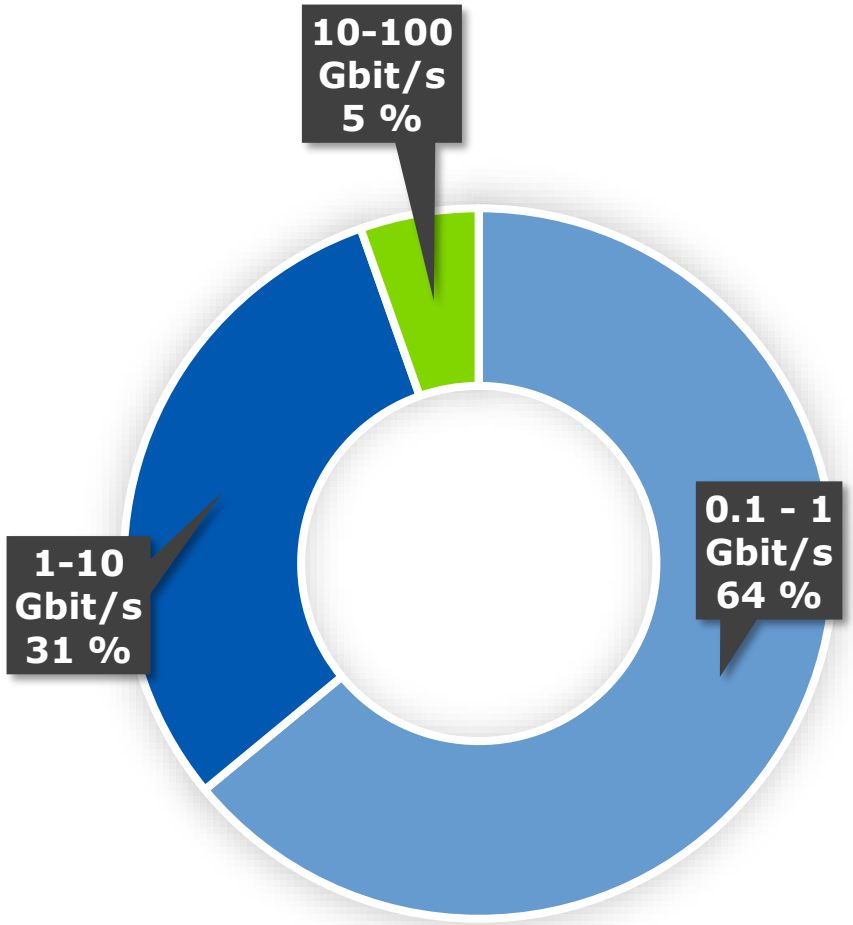
Analyysi

- Palvelunestohyökkäykset ovat osa nykyaikaista kybersodankäyntiä.
  - Niillä voidaan lamauttaa tärkeitä palveluja tai aiheuttaa hämmennystä kansalaisten keskuudessa.
  - Tavallinen kansalainen on tottunut siihen, että verkkopalvelut ovat aina saatavilla.
- Mediassa on kerrottu Venäjään kohdistuneista palvelunestohyökkäyksistä.
  - Erilaiset ryhmittymät ovat kohdistaneet palvelunestohyökkäyksiä ja häiriköintiä venäläisille uutissivustoille ja kansalliseen televisioon.
  - Esimerkit osoittavat omien kotimaisten palveluiden suojaamisen tärkeyden.

Palvelunestohyökkäysten tunnuslukuja

3kk

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



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q4/2021 - tilasto päivitetään kvartaaleittain.)

Vakoilu

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

Vakoilu

- Ukrainaan on kohdistunut sekä Venäjän hyökkäyksen jälkeen että jo ennen sitä erilaisia kyberhyökkäyksiä.
- Ukrainalaisiin organisaatioihin kohdistettuja, tietoja tuhoavia haittaohjelmia on havaittu ainakin neljää erilaista tämän tilannekuvakatsauksen laadintahetkeen mennessä.
  - WhisperGate-haittaohjelma tunnistettiin tammikuussa, HermeticWiper- ja IsaacWiper-nimillä kutsutuista haittaohjelmista uutisoitiin helmikuussa ja tuoreimpana ESET:n tutkijat havaitsivat CaddyWiper-haittaohjelman levitysyrityksiä Ukrainassa maaliskuun puolivälissä.
  - Haittaohjelmia on ESET:n mukaan havaittu rajallisessa joukossa ukrainalaisia korkean profiilin organisaatioita. Ainakin osassa kohteena on ollut valtionhallinto, mutta kaikkien haittaohjelmien kohdalla kohdeorganisaatioita ei ole tarkemmin kuvattu.
  - Tietoja tuhoavien haittaohjelmien tarkoituksena on estää kohdejärjestelmän toiminta ja tuhota tiedostoja ja tällä tavoin haitata tai lamauttaa kohdeorganisaation toimintaa.
- Myös muuta kybervaikuttamista havaitaan Ukrainassa säännöllisesti.
  - Valtionhallintoon ja pankkeihin on kohdistunut palvelunestohyökkäyksiä, joiden liikenne on ollut lähtöisin Venäjältä.
  - Ukrainalaisiin valtionhallinnon organisaatioihin ja ukrainalaisille sotilaille on lähetetty kalasteluviestejä.
- Ilmeisesti ukrainalaisten pakolaisten liikkeisiin liittyviä tietoja puolestaan on haviteltu mahdollisesti murretulta ukrainalaiselta sähköpostitililtä muualle Eurooppaan lähetetyillä kalasteluviesteillä.

Analyysi

- Organisaatioiden, joilla on toimintaa tai liittymäpintoja Ukrainaan, on syytä varautua Ukrainassa tapahtuvien kyberhyökkäysten seurannaisvaikutuksiin. Myös tahattomat sivuosumat ovat mahdollisia.
- Esimerkiksi Yhdysvallat on lisäksi kannustanut kriittisen infrastruktuurin organisaatioita varmistumaan siitä, että niiden varautuminen uhkiin on ajan tasalla. Se varoitti yrityksiä esimerkiksi mahdollisesta hybridivaikuttamisesta.

Vakoilu

- Yhdysvaltojen tietoturvaviranomainen CISA tiedotti helmikuussa Venäjän valtion tukemien toimijoiden toteuttamista tietomurroista puolustushallinnon kumppaneiden ja puolustusteollisuuden organisaatioiden järjestelmiin.
  - Kohteina oli ollut sekä pienempiä että suurempia organisaatioita ja eri tyyppisiä toimintoja.
- Hyökkääjät olivat päässeet käsiksi esimerkiksi sähköposteihin ja dokumentteihin.
  - Hyökkääjät saivat käsiinsä luokittelemattomia asiakirjoja, joista on mahdollista päätellä tietoja esimerkiksi maan puolustuksesta, sekä liikesalaisuuksia sisältäviä tietoja.
  - Murtoyrityksiä on havaittu vähintään tammikuusta 2020 lähtien ja aina helmikuuhun 2022 asti.
- Jalansijan saamisessa organisaatioiden järjestelmiin hyödynnettiin esimerkiksi salasanojen koneellista arvaamista (brute force), kohdistettua kalastelua ja tunnettuja haavoittuvuuksia.
  - Varastettuja käyttäjätunnuksia hyödynnettiin pääsyn saamiseksi yritysten Microsoft 365 -ympäristöihin.

Analyysi

- Puolustusteollisuus on kybervakoilun näkökulmasta erityisen kiinnostava toimiala.
- Yhdysvaltojen viranomaiset ovat arvioineet, että vaikka asiakirjat ja sähköpostit, joihin tietomurroissa oli päästy käsiksi, eivät olleet salassa pidettäviä, voivat ne tarjota hyökkääjälle merkittävää informaatiota puolustuksen yksityiskohdista, kuten asejärjestelmien kehityksestä ja viestintäjärjestelmien suunnitelmista.

Vakoilu

- Iraniin liitetty MuddyWater-ryhmä on vakoillut julkishallinnon ja kriittisen infrastruktuurin organisaatioita eri puolilla maailmaa.
  - Yhdysvaltojen ja Britannian tietoturvaviranomaiset tiedottivat toiminnasta helmikuun lopulla.
- Kohteena on ollut organisaatioita muun muassa puolustusteollisuudesta, viestintäteknologian, öljy- ja kaasusektorilta ja julkishallinnosta Aasiassa, Afrikassa, Euroopassa ja Pohjois-Amerikassa.
- MuddyWater tunnetaan myös nimillä Static Kitten, MERCURY, Earth Vetala, Seedworm ja TEMP.Zagros.
- Se on tietoturvaviranomaisten havaintojen mukaan hyödyntänyt viime aikoina useita eri haittaohjelmaperheitä toiminnassaan.
- Ryhmä on muun muassa pyrkinyt varastamaan tietoja ja hankkimaan pääsyn kohdejärjestelmiin.

Analyysi

- MuddyWater-ryhmä hyödyntää usein tunnettuja haavoittuvuuksia ja avoimen lähdekoodin työkaluja kohdejärjestelmiin tunkeutumisessa.
- Vaikka valtiollisilla toimijoillaan voi olla käytössään myös aiemmin tuntemattomia työkaluja ja haittaohjelmia tai niin sanottuja nollapäivä-haavoittuvuuksia, auttaa myös tunnetuilta uhkilta suojautuminen merkittävästi puolustautumaan APT-toimijoita vastaan.

Vakoilu

- Iso yhdysvaltalainen mediayhtiö News Corp on joutunut kybervakoilun uhriksi.
  - Murto oli tapahtunut tammikuussa, ja se oli kohdistunut yhteen yhtiön pilvipalveluntarjoajista.
- Tietomurrossa hyökkääjä pääsi käsiksi muun muassa The Wall Street Journalin ja New York Postin toimittajien ja työntekijöiden sähköposteihin ja asiakirjoihin.
- Yhtiön mukaan tietomurron taustalla ovat Kiinan valtion tukemat tahot.
- Kyseessä ei ole ensimmäinen kerta, kun The Wall Street Journal on ollut vakoilun kohteena.
  - Myös vuonna 2013 kerrottiin siihen kohdistuneesta vakoilusta, jossa Kiinan liitetyt hyökkääjät pyrkivät seuraamaan toimituksen Kiinaan liittyvää uutistyötä. Tällöin kohteena oli WSJ:n lisäksi myös mm. New York Times.

Analyysi

- Valtioiden etuja ajavaa kybervakoilua voi kohdistua monenlaisiin yrityksiin ja organisaatioihin hyvin eri tyyppisistä syistä.
- Perinteisin motivaatio kybervakoilulle on tiedonhankinta poliittisesta päätöksenteosta, valtionhallinnon toiminnasta ja varautumisesta, mutta vakoilun tavoitteena voi olla myös teollisuusvakoilu tai esimerkiksi kuvatun kaltainen tiedonhankinta.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

- Datasäädös: Komissio ehdottaa toimenpiteitä oikeudenmukaisen ja innovatiivisen datatalouden edistämiseksi.
  - Komissio ehdottaa uusia sääntöjä siitä, kuka voi käyttää ja saada käyttöönsä EU:ssa talouden eri aloilla tuotettua dataa. Lehdistötiedotteen mukaan datasäädöksellä turvataan oikeudenmukaisuus digitaalisessa toimintaympäristössä, edistetään kilpailukykyisiä datamarkkinoita, avataan mahdollisuuksia datavetoiselle innovoinnille ja parannetaan datan saatavuutta yleisesti.
  - Lue lisää: https://ec.europa.eu/commission/presscorner/detail/fi/ip_22_1113

Oikeudelliset asiat

- Tiedonhallintalain arviointikertomus 2020-2021 on julkaistu 18.2.2022.
- Arviointien perusteella tiedonhallinnan järjestäminen tiedonhallintalain mukaisesti vaihtelee tiedonhallintayksiköittäin. Osa organisaatioista on toteuttanut lain vaatimuksia jo etupainotteisesti ja osa on vasta käynnistämässä tai parhaillaan toteuttamassa toimintaansa lain mukaiseksi. Yleisesti ottaen valtion virastoilla tiedonhallintalain vaatimusten toteuttaminen on edennyt jonkin verran kuntia nopeammin.
- Lue lisää: https://julkaisut.valtioneuvosto.fi/handle/10024/163840

ISO 27000 -standardisarja

- ISO 27000 -standardiperhe päivittyy.
- Hallintakeinojen standardista ISO/IEC 27002 ilmestyi uusi versio helmikuussa.
  - Kontrollien kokonaismäärä on vähentynyt, mutta niiden soveltamisala organisaation tietoturvallisuudessa on aiempaa laajempi.
  - Kontrollit on jaoteltu uudella tavalla ennalta ehkäiseviin, havaitseviin ja korjaaviin kontrolleihin, ja lisäksi esim. ihmisiin, teknologioihin ja prosesseihin.
  - Myös kokonaan uusia kontrolleja on lisätty 12 kappaletta, kuten threat intelligence, pilvipalveluiden tietoturvallisuus sekä verkkoliikenteen suodatus.
- ISO/IEC 27002:n uudistuminen vaatii myös päästandardin ISO/IEC 27001 päivittämistä kevään kuluessa: muutokset ovat kevyitä ja koskevat terminologiaa ja viittauksia.
  - Liite A viittaa vastedes suoraan nyt päivitettyyn hallintakeinojen standardiin ISO/IEC 27002.

JulKri

- Julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristö Julkri on tulossa lausuntokierrokselle. Julkrin valmistelusta vastaa Julkisen hallinnon tiedonhallintalautakunta.
- Julkri on arviointikriteeristö salassa pidettävälle tiedolle, jota ei ole turvaluokiteltu.
- Viranomaisen ja kansainvälisen turvaluokitellun tiedon käsittelyä on entuudestaan ohjattu KaTaKrilla ja pilvipalveluympäristössä PiTuKrilla. Julkri siis täyttää arviointikriteeristöjen katvealueen.
- JulKrin kehitystyö on osa laajempaa julkisen hallinnon digitaalisen turvallisuuden Haukka-hanketta.
- Julkri on tavoitteena ottaa käyttöön keväällä 2022. Sitä voidaan hyödyntää esimerkiksi palveluntuottajan tietoturvallisuuden tason arvioinnissa.

Arjen kyberturvallisuus

Nasevia neuvoja tiliesi turvaamiseksi

- Verkkopalveluissa käytettäviä tilejä yritetään murtaa ja ottaa haltuun usein eri keinoin.
- Tutustu Kyberturvallisuuskeskuksen ennalta varautumisen neuvoihin. Lue lisää:https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

Näin pidät huolta tietoturvallisuudesta kotona ja työpaikalla

- Huolellisuudella ja muutamalla perustaidolla voit turvata tietosi verkossa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

Neuvot identiteettivarkauksien ja tietovuotojen uhreille

- Käy tutustumassa Kyberturvallisuuskeskuksen neuvoihin vahingon tapahduttua tai vaikka jo ennakkoon.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kysymyksia-ja-vastauksia-identiteettivarkauden-tai-tietovuodon-uhrille

Varo huijareita internetin myyntialustoilla

- Kyberturvallisuuskeskukselle ilmoitettujen huijausyrityksien määrät ovat kaksinkertaistuneet joulukuun 2021 jälkeen. Huijausyrityksessä tarkoituksena on saada myyjän pankkitiedot huijarin haltuun.
- Ole valppaana ja kyseenalaista miksi ostaminen pitää tehdä kuriiripalvelun kautta.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ttn_04032022

Uutisia Kyberturvallisuuskeskuksesta

EU:n uudet langattomien laitteiden tietoturvavaatimukset parantavat tietoturvallisuutta

- EU-alueella markkinoille saatettavien langattomien laitteiden tulee täyttää EU:n yhtenäiset tietoturvavaatimukset 1.8.2024 alkaen.
- Tämä merkitsee isoa muutosta laitevalmistajille, joiden täytyy huomioida uudet vaatimukset laitteiden suunnittelussa.
- https://www.traficom.fi/fi/ajankohtaista/eun-uudet-langattomien-laitteiden-tietoturvavaatimukset-parantavat-yksityisyyden

Onnistunut kyberharjoitus alkaa huolellisella valmistautumisella

- Tänä vuonna kyberharjoitteluun liittyvissä vinkeissä keskitytään harjoittelua edeltäviin vaiheisiin.
- Artikkelissa käydään läpi muutamia kybermaturiteetin peruspilareja, jotka edistävät organisaation kokonaisvaltaista tietoturvaa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/onnistunut-kyberharjoitus-alkaa-huolellisella-valmistautumisella

Traficom julkaisi suosituksen teleoperaattoreille keinoista kansainvälisten huijaussoittojen estämiseksi

- Liikenne- ja viestintävirasto Traficom antoi operaattoreille uuden suosituksen eri keinoista estää soittajan numeron väärentäminen ja huijaussoittojen välittäminen puhelun vastaanottajille Suomessa.
- Suositus on merkittävä, koska sen käyttöönotto teleoperaattoreilla vähentää huijaussoittojen määrää huomattavasti.
- https://www.traficom.fi/fi/ajankohtaista/suositus-teleoperaattoreille-keinoista-kansainvalisten-huijaussoittojen-estamiseksi

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