TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 2020

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

Kybersää elokuu 2020

Tietomurrot ja -vuodot

- Norjan parlamentti tietomurron kohteena.
- Yli 900 murretusta Pulse Secure VPN –palvelimesta saatuja tietoja julkaistu internettiin.
- Onnistuneiden kalasteluiden seurauksena Office 365 – tietomurtojen määrät kasvavat

Huijaukset ja kalastelut

- Huijareiden härskiydellä ei ole rajaa: ”Huijauksissa menetettyjen rahojen palautuspalvelu” huijaa uudestaan jo huijattuja uhreja.
- Tietojenkalastelu on ammattirikollisten aktiivisesti käyttämä työkalu.

Haittaohjelmat ja haavoittuvuudet

- EMOTET leviää Suomessa ja maailmalla, julkaisimme keltaisen varoituksen aiheesta.
- Useita kriittisiä haavoittuvuuksia, jotka suositellaan päivittämään nopealla aikataululla.

Automaatio

- Tietoturvatutkijat löysivät satoja tuhansia haavoittuvia tulostimia verkosta.
- Ensimmäinen virallinen standardi IoT-kuluttajalaitteiden tietoturvallisuudesta julkaistiin.

Verkkojen toimivuus

- Vain neljä merkittävää yleisten viestintäpalveluiden häiriötä.
- CenturyLinkin häiriö 30.8. vaikutti maailmanlaajuisesti
- Nettiä sensuroitu Valko-Venäjällä
- Palvelunestohyökkäysten osalta rauhallista Suomessa, mutta hyökkäyksillä uhkailu noususSa.

Vakoilu

- Toimeksiantopohjaiset kohdistetut hyökkäykset voivat uhata erityisesti liiketoimintakriittistä tietoa, mutta tilaustyönä tehtävät hyökkäykset ovat mahdollisia myös valtionhallintoa ja diplomaattikohteita vastaan.
- Toisaalta valtiollisen kyberhyökkäyksen motiivina voi olla myös rahan ansainta.

Varoitus 1/2020 Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa

- Emotet-haittaohjelmaa levitetään sähköpostitse suomalaisten organisaatioiden nimissä.
- Hyökkäyskampanja on näkynyt aktiivisena 17.8.2020 alkaen ja se on jatkunut myös syyskuussa.
- Keltainen varoituksemme kertoo tilanteesta, jossa käyttäjien ja ylläpitäjien on noudatettava yleistä varovaisuutta tai valmistauduttava mahdollisiin korjaaviin toimiin.
- Lue koko varoitus: https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

Kuukauden tunnuslukuja

YLI 120%

OLEMME SAANEET KYBERTURVALLISUUTTA KOSKEVIA ILMOITUKSIA MERKITTÄVÄSTI ENEMMÄN ELOKUUSSA 2020 KUIN 2019. KUUKAUSI EI OLE POIKKEUKSELLINEN VAAN ILMOITUSTEN MÄÄRÄ ON KASVANUT 2020 VUODEN AIKANA.

2,5%

INTERNETLIIKENTEEN LASKU ELOKUUN LOPUSSA CENTURYLINKIN HÄIRIÖN VUOKSI, JOKA VAIKUTTI MAAILMANLAAJUISESTI.

31.8.

KORONAVILKKU OTETTIIN KÄYTTÖÖN. TEIMME SOVELLUKSELLE TIETOTURVA-ARVIOINNIN JA TOTESIMME SEN TURVALLISEKSI KÄYTTÄÄ.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

2

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

3

Haavoittuvuuksien hyväksikäyttö on nopeaa, mikä edellyttää nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

kohonnut

laskenut

ennallaan

Keltainen = uutta/ päivitettyä*

4

Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako. Kyberuhkien vaikutuksia ei osata ennakoida ja epäselvyydet palveluiden hallinnan vastuunjaossa heikentävät tietoturvaa.

5

Lokitietojen puutteellisuus on riski monessa organisaatiossa. Puutteellisen lokitietojen keruun, seuraamisen ja säilyttämisen takia poikkeamatilanteita ei kyetä havainnoimaan tai selvittämään.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia toimijoita tulee jatkuvasti. Esimerkkinä tästä on ICS-toimijoihin kohdistuva EKANS.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.

CASE

Satelliittipaikannuslaitteita valmistava Garmin joutui 23.7. WastedLocker-kiristyshaittaohjelman uhriksi. Hyökkäys keskeytti Garminin palvelut useaksi päiväksi ja vaikutti muun muassa älyurheilukellojen toimintaan sekä ilmailun navigointiin ja palveluihin.

Lunnasvaatimuksen kerrotaan olleen 10 miljoonaa dollaria. Uutissivusto Bleepingcomputer sai haltuunsa Garminin käyttämän palautustyökalun, joka viittaa siihen, että Garmin olisi maksanut lunnaat.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

Tietojenkalastelu ja muu käyttäjien manipulointi (social engineering) on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

- Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. Tyypillisesti rikolliset kalastelevat suomalaisilta Office 365 –tuotteiden ja sähköpostin käyttäjätunnuksia ja salasanoja.
- Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua ja käyttäjän manipulaatiota opitaan tunnistamaan koulutuksen avulla, jolloin tietojenkalastelu jää vain yritykseksi.

CASE

Rikollinen onnistui tunkeutumaan yrityksen toimipisteen yhteisosoitteeseen Office 365 –tietojenkalastelun avulla. Sähköpostitililtä lähetettiin 800 kalasteluviestiä uusille uhreille. Lisäksi rikollinen oli luonut uusia käyttäjätilejä yrityksen ympäristöön murretun yhteistilin laajojen oikeuksien kautta.

Office 365 –kalastelua tapahtuu edelleen aktiivisesti. Monivaiheinen tunnistautuminen on tärkein keino suojautua sähköpostin tietomurrolta, vaikka tunnukset olisikin syötetty tietojenkalastelusivulle.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Haavoittuvuuksien hyväksikäyttö on nopeaa, mikä edellyttää nopeita päivityksiä tai muita toimenpiteitä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- 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.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

Yritys jättää lomakaudella verkkolaitteen kriittisen haavan päivittämättä. Myöhemmin havaitaan, että haavaa on hyväksikäytetty ja yritys on joutunut kyberhyökkäyksen kohteeksi. Tältä tilanteelta oltaisiin vältytty, mikäli yritys olisi tuntenut oman verkkoympäristönsä ja päivittänyt haavoittuvuuden välittömästi. Verkossa olevat laitteet tulee siis päivittää mahdollisimman pian haavan julkaisun jälkeen!

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako. Kyberuhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Epäselvyydet palveluntoimittajan, alihankkijoiden ja tilaajan vastuiden välillä heikentävät organisaation tietoturvan hallintaa.

- Tietoturvaloukkauksiin vastaamista tai niistä toipumista ei usein suunnitella riittävästi ennakkoon. Häiriön iskiessä siitä palautumisen monimutkaisuus ja työläys yllättävät.
- Tehdyt suunnitelmat tulee testata ja niitä pitää harjoitella.
- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä. Vastuut tulisi tehdä selväksi viimeistään hankinnan sopimusvaiheessa.

CASE

Organisaatio käyttää pilvipohjaista sovellusta (Software as a Service, SaaS) raporttien tekoon kumppaneidensa kanssa. Erään raportin julkaisussa tapahtuneiden epäselvyyksien johdosta pilvipalveluntarjoajaa pyydetään toimittamaan lokitiedot kyseisen raportin käsittelystä. Palveluntarjoaja vastaa, etteivät he voi luovuttaa lokitietoja, sillä heidän jaettuja resursseja käyttävät palvelut eivät erottele eri asiakkaiden lokitietoja. Tältä tilanteelta oltaisiin voitu välttyä, jos tämä vastuunjakoon liittyvä asia olisi sovittu jo sopimuksentekovaiheessa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

5

Lokitietojen puutteellisuus on riski monessa organisaatiossa.
Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään mikäli oikeiden järjestelmien tai sovellusten lokitietoja
ei kerätä, seurata ja säilytetä riittävän kauan.

- Kattavan lokienhallinnan avulla tietomurto on mahdollista havaita jo alkuvaiheessa. Pahimmillaan joissain tapauksissa ei lokitietojen riittämättömyydestä johtuen koskaan saada selville milloin, miten ja kuinka laajalti ympäristöön on tunkeuduttu.
- Organisaatioiden on tunnistettava mitkä ovat heille keskeiset järjestelmät ja sovellukset tietoturvaloukkausten havainnoinnissa ja selvittämisessä sekä huolehdittava riittävästä lokitietojen keräämisestä ja niiden riittävän pitkästä varastoinnista.
- Tietoturvaloukkauksen selvitykseen tarvittavia lokitietoja olisi hyvä säilyttää vähintään vuoden verran.

CASE

Yrityksen etäkäyttöpalvelussa on havaittu kirjautumiseen viittaavaa liikennettä epäilyttävästä lähteestä. Palvelusta ei kuitenkaan kerätä kirjautumislokeja, joten tapausta ei voida selvittää tämän pidemmälle.

Organisaation Windows-ympäristössä vain epäonnistuneista kirjautumisyrityksistä tehdään lokimerkintä. Tunkeutujan anastamilla tai itse luomilla tunnuksilla tehdyt kirjautumiset jäävät piiloon eikä tunkeutumisen laajuutta pystytä selvittämään.

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

- Norjan parlamentti, Suurkäräjät, kertoi joutuneensa tietomurron kohteeksi.
  - Hyökkäyksessä joidenkin parlamentin jäsenten ja työntekijöiden sähköpostitileille oli murtauduttu.
  - Mediatietojen mukaan tietomurron uhreja oli ainakin kahdesta eri puolueesta.
  - Parlamentin edustajan mukaan luvattomat kirjautumiset tileille havaittiin nopeasti, mutta tarkkaa tietoa siitä, mihin kaikkeen tietoon tunkeutujat olivat ehtineet päästä käsiksi, ei vielä parlamentin järjestämän tiedotustilaisuuden aikaan ollut.
  - Norjan turvallisuuspalvelu PST on kertonut aloittavansa tietomurron tutkinnan sen selvittämiseksi, oliko hyökkäyksen taustalla valtiollinen toimija.

ANALYYSI

- Tietomurtojen nopea havaitseminen edesauttaa vahinkojen rajaamista ja helpottaa hyökkäyksen tutkintaa. Tämä vaatii organisaatiolta kykyä havainnoida poikkeamia, kuten tavallisuudesta poikkeavia kirjautumisia.
- Lokien avulla on mahdollista jälkikäteen selvittää, mitä esim. sähköpostitilillä on tapahtunut. On tärkeää tietää, mitä kaikkea tietoa lokitetaan, minne nämä tiedot arkistoidaan ja miten kauan ne säilyvät.

Tietomurrot ja -vuodot

- Office 365 -tunnusten kalastelu johtaa säännöllisesti tietomurtoihin.
  - Onnistuneet Office 365 -tietomurrot suomalaisiin organisaatioihin ovat näkyneet kalasteluviesteinä.
  - Kyberturvallisuuskeskukseen tehtyjen Office 365 -tietomurtoilmoituksien määrät kaksinkertaistuneet heinäkuusta elokuuhun.
  - Saapuneista kalasteluviesteistä kannattaa ilmoittaa mahdolliselle uhrille ja sitten Kyberturvallisuuskeskukseen, jotta lisävahinkojen syntyminen voidaan estää.

ANALYYSI

- Lomakauden päättyminen ja ihmisten lomalta palaaminen selittää osin Office 365 -murtojen kasvua kesäkauden jälkeen.
- Monivaiheisen tunnistautumisen (MFA) käyttöönotto on tärkeä osa tietomurtojen estämisessä. Monivaiheinen käyttäjän tunnistaminen suojaa käyttäjätiliä väärinkäytöltä silloin, kun käyttäjän salasana on paljastunut sivullisille.

Tietomurrot ja -vuodot

- Verkossa julkaistiin maailmalta tiedot yli 900 murretusta Pulse Secure VPN –palvelimesta.
  - Haavoittuvuus altisti palvelimet murroille, haavoittuvuuteen on julkaistu korjaava päivitys jo 2019, mainitsimme asiasta myös elokuun 2019 Kybersäässä.
  - Yksittäisiä tapauksia myös Suomessa.
  - Tiedot sisälsivät mm. IP-osoitteet, palvelimien SSH-avaimet, lista palvelimien käyttäjistä ja salasana-tiivisteistä, admin-tilien tiedot, viimeisimmät kirjautumiset, käyttäjänimet ja selkokieliset salasanat.

ANALYYSI

- Vanhatkin päivitykset tulisi ladata, sillä uudet päivitykset eivät välttämättä sisällä kaikkien vanhojen päivityksien korjauksia.
- Suosittelemme aikataulun tekemistä, jotta päivitykset varmasti suoritetaan ajallaan.
- Lue aiheesta lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuspaivitykset-juoksukisa-hyvaksikayttoa-vastaan

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:

Huijaukset ja kalastelut

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

Huijaukset ja kalastelut

- Office 365 –tietojenkalastelua on lähetetty taas monenlaisille organisaatioille: ydistyksille, virastoille, isoille ja pienille yrityksille ja julkishallinnon toimijoille. Kalastelu myös johtaa säännöllisesti tietomurtoihin.
  - Elokuussa kalasteluepidemia riehui mm. kiinteistöhuoltoyhtiöiden sähköposteissa.
- Taas uudenlainen huijaustapa on ”Huijauksissa menetettyjen rahojen palautuspalvelu”.
  - Jo kertaalleen huijattuja uhreja yritetään huijata vielä lisää.
- WhatsApp-varmistuskoodeja on yritetty kalastella, jotta sillä voisi kiertää kaksivaiheisen tunnistautumisen.

ANALYYSI

- Laskutuspetoksia on elokuussakin yritetty saada aikaan johtajien nimiin tekaistuilla sähköposteilla. Tällä kertaa yksikään meille raportoitu toimitusjohtajahuijaus ei onnistunut!
  - Arvioimme, että tietoisuus eri huijauksista on lisääntynyt, koska niistä on ollut eri kanavissa tietoa ja yritykset myös itse tiedottavat tärkeästä asiasta organisaatiossa. Näin on vältytty onnistuneilta huijauksilta.
- Muita laskutushuijauksia on yritetty mm. valelaskuilla Verohallinnon nimissä.

Teknisen tuen nimissä soittelu jatkuu

- Kyberturvallisuuskeskus on saanut kevään tauon jälkeen jälleen paljon ilmoituksia yrityksiltä ja yksityishenkilöiltä teknisen tuen huijaussoitoista. Puheluita soitetaan sekä kotimaisista numeroista että ulkomaan suuntanumeroista.
  - Yhteistä tapauksille on soittajan halu saada ”asiakkaan” koneelle etähallintayhteys, jolla uhrin tietoihin pääsee käsiksi. Etäyhteyteen käytetään TeamVieweria tai muuta vastaavaa etähallintasovellusta.
  - Puhelinhuijauksia tehdään edelleen eniten Microsoftin tueksi tekeytyen. Jotkut huijarit väittävät olevansa operaattorin tai ”oman organisaatiosi” mikrotuesta.

ANALYYSI

- Valvomaton pääsy organisaation työasemalle määrittämättömäksi ajaksi on merkittävä tietoturvariski.
- Yrityksen tulee varmistaa keinot selvittää tapaus jälkikäteen. Uhri harvoin pystyy kertomaan tarkasti, mitä etäyhteyden kautta tehtiin teknisen selvittämisen mahdollistamiseksi.
- On tärkeä varmistaa lokituksen toimivuus, jotta mahdollinen onnistunut huijaus ja koneelle pääsy voidaan jälkikäteen selvittää niiden avulla.
- Turvallisuuskulttuurin merkitys korostuu: jos oviakaan ei avata tuntemattomalle, miksi tietokoneelle pitäisi päästä tuntematon taho?
- Yksityishenkilön ei ole tarpeen säilyttää käyttämätöntä etähallintaohjelmaa asennettuna laitteella.

Ammattirikolliset kalastelevat tietoja

- Tietojenkalastelu on keskeinen väline ammattirikollisten työkalupakissa. Sillä saa kerättyä tietomurtoihin tarvittavia tietoja, pankkitunnuksia, organisaatiorakenteita, henkilötietoja, käyttäjätunnuksia ja salasanoja.
- Pankkitietoja kalastellaan lähettämällä huijaussähköpostia, jossa pyydetään linkin kautta kirjautumaan sivustolle.
- Lue Tietoturva Nyt! -artikkelimme Neuvoja epäilyttävien sivujen tunnistamiseksi: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi

ANALYYSI

- Siinä, missä sähköpostihuijauksia voi tehdä vain lähettelemällä sähköpostia, onnistunut tietojenkalastelu vaatii laajempaa valmistelua ja huijaussivustojen laatimista.
- Monet näistä huijaussivustoista näyttävät hyvin uskottavilta. Sivut on tehty taitavasti ja niitä voi olla mahdoton tunnistaa nopealla katselulla. Takana voi olla kansainvälinen ammattirikollisryhmä.
- On tärkeä pohtia, mitä kautta sivulle surffaa ja välttää esimerkiksi sähköpostin kautta tulleita linkkejä ja kirjautua sivulle aina palveluntarjoajan osoitteen kautta.

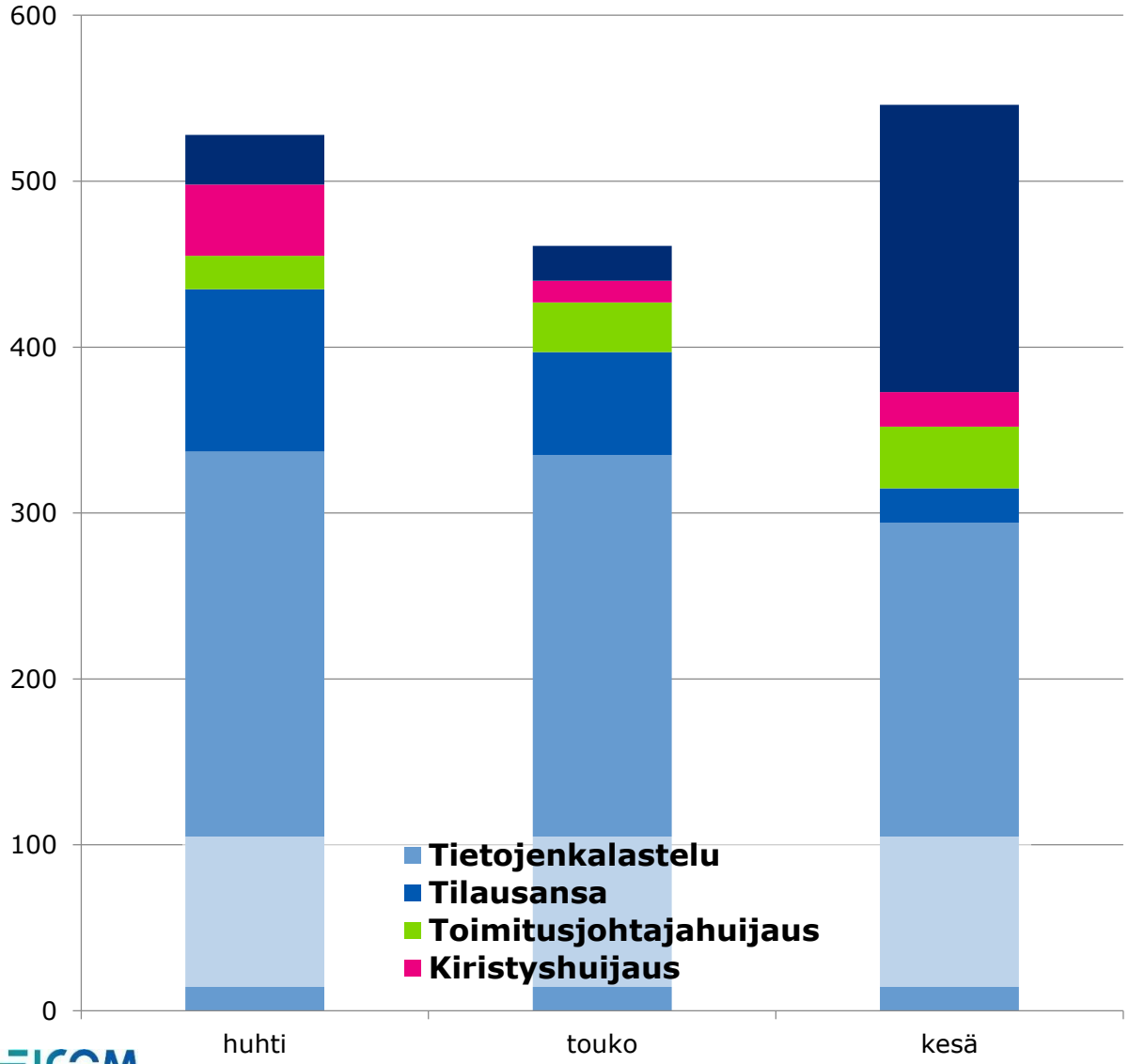
Office 365 tietojenkalastelu

- Office 365 tietojenkalastelu on edelleen yleistä. Alkuvuodesta tietojenkalastelu rauhoittui hieman, mutta vain hetkellisesti.
- Havaintona on, että tietojenkalasteluviestit sisältävät liitteen, jonka lähdekoodi on sumutettu (muutettu symboliseen konekieliseen muotoon).
- Yhden yrityksen murrettu sähköpostilaatikko poikii tyypillisesti tuhansia uusia tietojenkalasteluviestejä saman toimialan muihin yrityksiin. Uudet tietomurrot alkavat vaikuttaa epidemialta.

ANALYYSI

- Mikäli yritys on joutunut onnistuneen kalastelun kohteeksi, tulisi sillä olla keinot jäljittää tapausta.
- Uusimissa tapauksissa ongelmana on ollut se, että olemassa olevat mekanismit, kuten sähköpostisuodattimet, eivät tunnista haitallista liitettä. Näiden lisäksi tulisi olla käytössä myös muita keinoja.
  - Lokitietojen merkitys on tärkeä, jotta tiedon lähteelle päästään jälkikäteen.
  - Tunnusten hyödyntämistä voidaan osin estää käyttämällä monivaiheista tunnistautumista.
- Onnistuneen tietojenkalastelun seurauksena kalastelu voi levitä myös uhrilta seuraavalle. Tällöin vaikutuksia on myös moniin muihin. **Mikäli siis olet joutunut tietojenkalastelun uhriksi, tee siitä ilmoitus myös Kyberturvallisuuskeskukselle.**

Käsiteltyjä huijaustapauksia Q2/2020



- Toisen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Teknisen tuen huijauspuhelut
  - Huijaukset Postin nimissä (kts. lisää aiheesta Toukokuun kybersää)
- Toimitusjohtajahuijaukset kohdistuvat yrityksiin ja organisaatioihin. Väärennetyt viestit tähtäävät laskutuspetokseen. Huijausyritysten määrä on kohonnut kesälomakaudella, mutta valveutuneisuus on estänyt niiden onnistumisen.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.
- Tilausansoja suunnataan kaikille kuluttajille esiintyen mm. Postin, Gigantin, tai muiden tuotemerkkien nimissä. Niiden määrä on vähentynyt seurantajaksolla (Q2)

Q2/2020 - tilasto päivitetään kvartaaleittain

Haittaohjelmat ja haavoittuvuudet

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

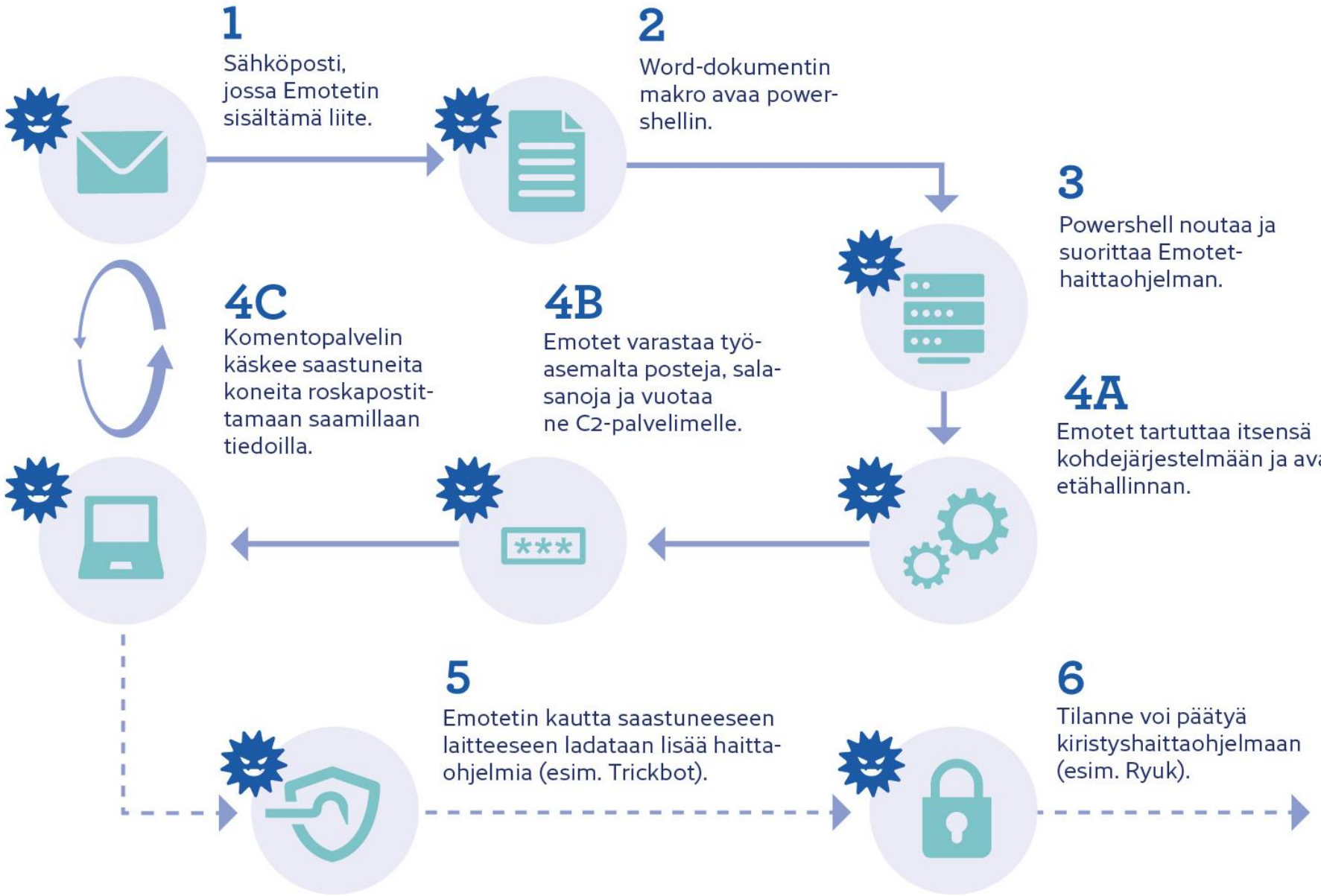
Haittaohjelmat

- Julkaisimme keltaisen eli vakavan varoituksen: Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa.
  - Emotet:n saastuttamalta työasemalta varastetaan tietoja.
  - Emotet:n kautta voi koneelle tulla muitakin haittaohjelmia ja tartunta voi johtaa kiristyshaittaohjelmaan.
  - Emotet-haittaohjelmaa levitetään murrettujen verkkosivustojen kautta myös suomalaisilla sivustoilla.
  - Vaikka nimi sähköpostissa on oikein, lähettäjän tietoihin ei voi eikä tule luottaa.
    - Aiemmin luotuun sähköpostiketjuun saapuva viesti voi valheellisesti näyttää tulevan tutulta henkilöltä.
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

ANALYYSI

- Sähköpostien linkit ja tiedostot ovat haittaohjelmatartunnoissa merkittävässä roolissa, sähköpostin suodatukseen kannattaa panostaa ja olla tietoinen siitä, mitä päästetään läpi ja miksi
- Office-ohjelmissa käyttäjää yritetään huijata sallimaan makrojen tai muiden sisältöjen toiminta, koska niiden salliminen mahdollistaa haittaohjelman lataamisen koneelle

Emotet-haittaohjelmatartunnan eteneminen



TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Haavoittuvuudet

- Uusia Ripple20–haavoittuvia laitteita lähinnä teollisuusjärjestelmissä.
  - Päivitimme tiedotettamme uusien laitteiden osalta https://www.kyberturvallisuuskeskus.fi/fi/treckin-tcpip-toteutuksesta-loydetty-lukuisia-haavoittuvuuksia (20/2020)
  - Myös kesäkuun Kybersäässä on haavoittuvuutta käsitelty.
- Citrix on julkaissut kriittisen haavoittuvuuden ja päivityksen päätelaitteiden hallintajärjestelmään, Citrix Endpoint Managementin paikallisiin asennusratkaisuihin.
  - Lue haavoittuvuudesta: https://www.kyberturvallisuuskeskus.fi/fi/kriittinen-haavoittuvuus-citrix-endpoint-managementin-paikallisissa-asennuksissa (28/2020)
- Keskustelupalstojen alustaratkaisu vBulletinista löytynyt nollapäivähaavoittuvuus ohittaa aiemmin julkaistun korjauksen Remote Code Execution -haavoittuvuuteen (CVE-2019-16759).
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/kriittinen-haavoittuvuus-vbulletinssa (27/2020)

ANALYYSI

- Haavoittuvuuksien hyväksikäyttö tapahtuu nopeasti, kun haavoittuvuus on tullut julkisuuteen, päivitysprosessien tulisi olla suhteutettuna tähän ja nopea päivittäminen saattaa pelastaa isommilta vahingoilta.
- Uusiakin haavoittuvuuksia skannataan aktiivisesti, joten tietoturvapäivitysten asentaminen on ensiarvoisen tärkeää.

Automaatio

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

Automaatio

- Tietoturvatutkijat löysivät satoja tuhansia haavoittuvia tulostimia verkosta.
  - Haltuun yritettiin ottaa 50 000 laitetta ja yli puolet yrityksistä onnistui.
  - Turvattomat tulostimet tallentavat tietoa käsittelemistään tiedostoista ja vaarantavat yrityksen tietoturvan ja tietosuojan.
  - Tulostimien faksiominaisuutta on myös käytetty pääsynä yrityksen sisäverkkoon.

ANALYYSI

- Kyberturvallisuuskeskuksen havaintojen mukaan myös Suomessa satoja haavoittuvia tulostimia.
- Organisaatiossa pitää olla ymmärrys, mistä sen tietotekninen ympäristö käytännössä koostuu.
- Tietoturvallisuuden ja laitehallinnan tulisi kattaa kaikki verkkoon kytketyt laitteet - ei ainoastaan tietokoneita. Tämä on myös osa riskienhallintaa.
- Tulostimen ei tulisi toimia takaovena rikollisille yrityksen tietoihin!

IoT:n standardointi

- Heinäkuussa julkaistiin ensimmäinen virallinen standardi IoT-kuluttajalaitteiden tietoturvallisuudesta, ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things.
  - Myös Traficomin Tietoturvamerkin vaatimukset perustuvat standardiin.
- Kansainvälisessä standardoinnissa ISO/IEC:n tietoturvakomiteassa on myös uusia työkohteita IoT:ssa.
  - ISO/IEC CD 27400.2 Cybersecurity – IoT security and privacy – Guidelines
  - ISO/IEC WD 27402 Cybersecurity — IoT security and privacy — Device baseline requirements
  - ISO/IEC WD 27403.2 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

ANALYYSI

- IoT-osio palautettiin osaksi Kybersäätä, koska yritykset hyödyntävät sitä eri toiminnoissaan.
- Organisaatioissa heikko IoT voi vaarantaa koko organisaation toiminnan, kuten mikä tahansa muukin turvaton teknologia. Ymmärrys omasta digitaalisesta ympäristöstä tulee olla keskiössä, jotta taataan liiketoiminnan jatkuvuus.
- IoT-ratkaisujen lisääntyminen näkyy (tietoturva)standardoinnin kehittymisenä.

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

- Elokuussa Suomessa oli neljä merkittävää yleisten viestintäpalveluiden häiriötä
  - Kaksi niistä johtui valokuitujen katkeamisista maanrakennustöissä.
- Yhdysvaltalaisen suuren internetpalveluntarjoaja CenturyLinkin palveluissa oli laajavaikutteinen häiriö 30.8.2020
  - Häiriö vaikutti myös moniin suomalaisten käyttämiin internetin palveluihin kuten verkkopelialustoihin ja Amazoniin. Korkean saatavuustason internetpalveluita tarjoava Cloudflare havaitsi koko internetin liikennemäärän tippuneen 2,5 % häiriön seurauksena.
  - Häiriön syy oli ilmeisesti inhimillinen virhe CenturyLinkin liikenteen ja palomuurien säätämisessä.

ANALYYSI

- Merkittäviä häiriöitä oli elokuussa keskimääräistä vähemmän. Kuukausittainen määrä todennäköisesti kasvaa tästä seuraavina kuukausina parilla kappaleella.
- CenturyLinkin palveluiden häiriö korostaa viestintäpalveluiden ylläpitotöiden huolellisen suunnittelun ja testaamisen tärkeyttä.

Verkkojen toimivuus

- Valko-Venäjällä viranomaiset ovat estäneet viestintäpalveluiden käyttöä elokuisten presidentinvaalien alla ja niiden jälkeen esiintyneiden mielenosoitusten aikana.
  - Estot ovat ilmeisesti teknisesti kohdistuneet internetin nimikyselyihin (DNS), joista estoilla on suodatettu ainakin sosiaalisen median palveluita ja hallinnosta kriittisesti kirjoittavia verkkosivustoja koskevia kyselyitä. Kun käyttäjien päätelaitteet eivät estojen vuoksi saa vastauksia nimikyselyihin, ne eivät pysty ottamaan yhteyttä palveluihin.
  - Estojen ilmeinen tarkoitus on tiedonkulkua vaikeuttamalla haitata mielenosoitusten järjestämistä.

ANALYYSI

- Tapahtumat korostavat internetin tärkeyttä vapaalle tiedonkululle. Suurten mielenosoitusten järjestäminen estoista huolimatta osoittaa, että kattavien ja pitävien estojen toteuttaminen on hyvin vaikeaa.
- Vastaavia rajoitustoimia on käytetty kevään aikana myös esimerkiksi Intian Kashmirissa, jossa pitkäaikaiset levottomuudet ovat kääntyneet väkivallaksi.

Palvelunestohyökkäykset

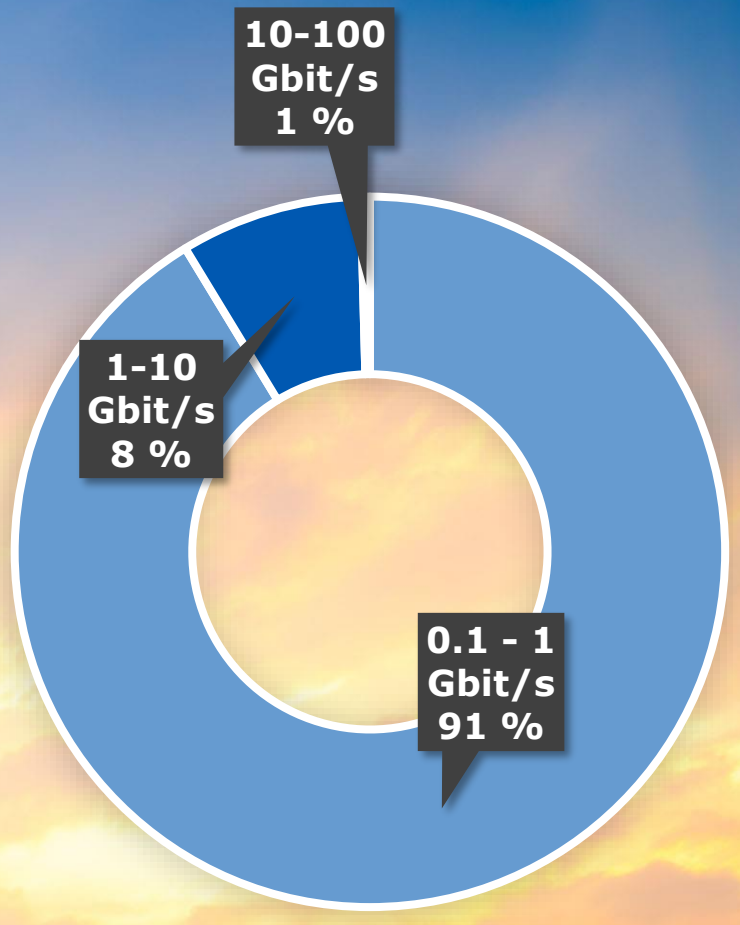
- Elokuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäyksillä uhkailu ja lunnasrahojen vaatiminen ovat yleistyneet maailmalla.
  - On tapauksia, joissa organisaatioon on kohdistunut palvelunestohyökkäys. Tämän jälkeen sähköpostitse on uhkailtu suurella palvelunestohyökkäyksellä mikäli vaadittuja lunnasrahoja ei maksettaisi.
  - Uhattuja hyökkäyksiä on toteutettu ulkomailla ja hyökkäyksillä on ollut laajoja vaikutuksia. Hyökkäykset ovat olleet tekniseltä toteutukseltaan vaikeita torjua.
- Maailmalla palvelunestohyökkäysten trendi on ollut nousussa sekä hyökkäysten koon että keston osalta.
  - Suurilta volumetrisiltä hyökkäyksiltä suojautuminen voidaan toteuttaa tehokkaasti internet-palveluntarjoajien tarjoamien DDoS-suojauspalveluiden avulla.

ANALYYSI

- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volumetriset että sovellustason hyökkäykset.

Palvelunestohyökkäysten tunnuslukuja

- 59 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2 aikana 2020.
- Noin 54% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTO-HYÖKKÄYSTEN VOLYYMIT (Q2/2020 - 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

- Teollisuusvakoilua saatetaan tehdä myös tilaustyönä, arvioi muun muassa tietoturvayhtiö Kaspersky.
  - Kaspersky kertoi elokuussa uusia tietoja DeathStalker-nimisestä ryhmästä, jonka pääasiallisina kohteina vaikuttavat olevan finanssialaan liittyvät teknologiayhtiöt (*fintech*), lakifirmat ja finanssialan neuvontapalveluja tarjoavat organisaatiot. Ryhmän on kuitenkin havaittu kohdistaneen toimiaan ainakin kerran myös diplomaattikohteeseen. Kaspersky arvioikin, että ryhmä todennäköisesti toimii joko toimeksiantojen pohjalta tai vaihtoehtoisesti pyrkii myymään hankkimiaan tietoja eteenpäin.
  - Vastaavaa toimintamallia on aiemmin epäilty myös mm. RedCurl-nimellä tunnetun hakkeriryhmän kohdalla, jonka uhreja ei vaikuta yhdistävän muu kuin mahdollisesti arvokas tieto – vaihtelu on huomattavaa niin maantieteellisesti kuin toimialoittainkin.

ANALYYSI

- Toimeksiantopohjainen toiminta heikentää ennakoitavuutta siten, että organisaatioiden voi olla entistä vaikeampi priorisoida toimenpiteitään.
- Samat uhkat ja hyökkäysmenetelmät voivat kohdistua useisiin eri sektoreihin ja eri tyyppiseen toimintaan, eikä kehittyneen hyökkäyksen taustalla välttämättä tarvitse olla valtiollista intressiä.

Vakoilu

- Pohjois-Koreaan yhdistetyn Lazarus-ryhmän toiminnasta saatiin elokuussa lisätietoja, kun F-Secure kertoi omista tutkimustuloksistaan.
  - F-Securen tutkimassa kampanjassa hyökkääjän kohteena olivat virtuaalivaluuttamarkkinat.
  - Aiemmin kesällä tietoturvayhtiö ESET kertoi ilmailu- ja avaruusteknologiasektorin ja puolustusteollisuuden organisaatioihin kohdistetusta kampanjasta, jossa kohteita lähestyttiin liike-elämään ja työnhakuun keskittyvässä yhteisöpalvelussa LinkedInissä valheellisen työtarjouksen turvin. Näin uhri saatiin avaamaan joko suoraan LinkedInissä tai sähköpostitse lähetetty haitallinen liitetiedosto.
  - ESET arvioi, että operaation taustalla vaikuttivat olevan pohjoiskorealaiset toimijat. Tavoitteena arvioitiin olevan tiedon varastaminen, jonka lisäksi hyökkääjä yritti lopuksi laskutuspetosta.
  - F-Securen mukaan operaatioita yhdisti esimerkiksi hyökkääjän tapa hyödyntää LinkedIniä hyökkäyksen ensimmäisen vaiheen toteuttamisessa.

ANALYYSI

- Sosiaalisen median palveluita voidaan hyödyntää kohdistettujen hyökkäysten toteuttamisessa sekä suoraan että taustatietojen lähteenä.
- Lazarus-ryhmän yhtenä keskeisenä tavoitteena vaikuttaa edelleen olevan taloudellisen hyödyn hankkiminen valtion lukuun.

Tietoturva-alan kehitys

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

Oikeudelliset asiat

- EU:n komissiolla on käynnissä 2.10.2020 asti julkinen kuuleminen osana eIDAS-asetuksen käynnissä olevaa arviointia.

ANALYYSI

- eIDAS-asetus koskee rajat ylittävää sähköistä tunnistamista ja eräitä muita sähköisiä palveluita kuten sähköisiä allekirjoituksia, aikaleimoja ja verkkosivuvarmenteita.
- Avoin julkinen kuuleminen on suunnattu mm. yksityishenkilöille ja yrityksille, joihin eIDAS-asetus vaikuttaa. Kannustamme osallistumaan kuulemisiin. Verkkosivulla on nähtävissä myös muiden antamia lausuntoja.
- Komission kysely löytyy seuraavasta osoitteesta https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

Oikeudelliset asiat

- EU:n komissiolla on käynnissä 2.10.2020 asti julkinen kuuleminen NIS-direktiivin osalta.

ANALYYSI

- NIS-direktiivi koskee yhteiskunnan toiminnan kannalta kriittisten verkko- ja tietojärjestelmien tietoturvallisuutta, varautumista, riskienhallintaa ja merkittävistä häiriöistä ilmoittamista
- Avoin julkinen kuuleminen on suunnattu mm. organisaatioille, joihin NIS-direktiivi vaikuttaa. Kannustamme osallistumaan kuulemisiin. Verkkosivulla on nähtävissä myös muiden antamia lausuntoja.
- Komission kysely löytyy seuraavasta osoitteesta https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive/public-consultation

Arjen kyberturvallisuus – epäilyttävä elokuu

Teknisen tuen huijauspuhelut jatkuvat

- Kansalaisiinkin kohdistuvissa niin kutsutuissa tech support scam –huijauspuheluissa esiintyy uusia ilmiöitä: Huijari voi esiintyä suomalaisen teleoperaattorin edustajana, ja huijauspuhelua saattaa edeltää niin kutsuttu häläripuhelu.
- Älä anna pääsyä tietokoneelle tai mitään tietoja huijarille. Puheluun vastaaminen ei ole vaarallista.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa

Tietoturva on ykkösjuttu myös mobiilisovelluksissa

- Miten tavallinen käyttäjä pystyy poimimaan turvalliset mobiilisovellukset sovellusmerestä?
- Tietoturvamerkki näyttää tietä kohti älylaitteiden tietoturvaa
- Lue lisää: https://www.traficom.fi/fi/ajankohtaista/blogit/tietoturva-ykkosjuttu-myos-mobiilisovelluksissa

Bluetoothin turvallinen käyttö älylaitteissa

- Suomen korona-altistuksia jäljittävä sovellus auttaa katkaisemaan tartuntaketjuja ja hillitsemään viruksen leviämistä. Jäljittäminen perustuu Bluetooth Low Energy (BLE) –tekniikkaan
- Onko bluetoothin käyttö turvallista. Lue lisää artikkelistamme, jossa korjataan oletuksia ja annetaan vastauksia yleisiin kysymyksiin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/bluetoothin-turvallinen-kaytto-alylaitteissa

WhatsApp-tilien vahvistuskoodeja kalastellaan Suomessa

- WhatsAppin käyttäjien on tärkeää tunnistaa tekstiviestillä lähetettävien vahvistuskoodien kalasteluyritykset ja suojautua kalasteluyrityksiltä ottamalla kaksivaiheinen tunnistautuminen käyttöön.
- Nappaa vinkit talteen ja suojaa oma tilisi: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/whatsapp-tilien-vahvistuskoodeja-kalastellaan-suomessa

Ajankohtaista Kyberturvallisuuskeskuksesta

Älä anna päivitysprosessin lomailla suvena

- Kriittisten haavoittuvuuksien päivittäminen on tärkeää - myös kesäaikana. Ovathan prosessit kunnossa ja sijaisjärjestelyt mietittynä työntekijöiden lomaillessa?
- Päivityksiä tulee tasaiseen tahtiin myös lomakaudella ja haavoittuvuuksien hyväksikäyttöä tapahtuu nopealla syklillä haavojen julkaisemisen jälkeen.
- Tietoturva nyt! –julkaisu aiheesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ala-anna-paivitysprosessin-lomailla-suvena

Selvitys ICT-alan nousevien teknologioiden vaikutuksista ympäristön- ja ilmastonmuutokseen

- Selvityksessä arvioitiin nousevien tieto- ja viestintäteknologia-alan teknologioiden aihealueiden ilmasto- ja ympäristövaikutuksia.
- Selvityksen tavoitteena oli kunkin aihealueen osalta tunnistaa ilmaston- ja ympäristönmuutoksen näkökulmasta merkittäviä teknologioiden sovelluskohteita, tarkastella teknologioiden ilmaston- ja ympäristönmuutosta hillitseviä ja kiihdyttäviä vaikutuksia 2020 ja 2035
- https://www.traficom.fi/sites/default/files/media/publication/ICT_ilmastovaikutukset_selvitys_Traficom_julkaisuja_244_2020_17.8.20.pdf

Verkostoissa kyberturvallisuuden haasteita ratkotaan yhdessä.

- Kyberturvallisuuskeskuksen ylijohtaja Kalle Luukkainen toivoo verkostotoimintaan mukaan enemmän yritysten ylintä johtoa.
- Olemme Suomessa verkostoituneet kyberturvallisuusasioissa ihmisten kesken poikkeuksellisen hyvin. Kansainvälisesti vertaillen meillä yhteydenpito viranomaisten ja yritysten välillä on välitöntä ja tiivistä. Alan luottamusverkostoja on useita erilaisia, ja jokaisella on oma tarkoituksensa.
- Tutustu: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkostoissa-kyberturvallisuuden-haasteita-ratkotaan-yhdessa

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)