TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 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 syyskuu 2020

Tietomurrot ja -vuodot

- Olemme vastaanottaneet tavallista enemmän ilmoituksia murretuista kotimaisista sivustoista
- Maailmalla on paljon havaintoja terveysalan toimijoihin kohdistuneista kiristyshaittaohjelmista
- Office 365 –tietomurrot jatkuvat

Huijaukset ja kalastelut

- Postin nimissä on lähetelty tuhansia tekstiviestejä, jotka johtavat sekä tilausansaan, tietojenkalasteluun että haittaohjelmaan.
- Paljastuneen kalastelusivun takaa löytyi kymmenien uhrien tiedot, joiden avulla tietomurrot saatiin katkaistua.

Haittaohjelmat ja haavoittuvuudet

- Emotet leviää aktiivisesti sähköpostien liitetiedostojen avulla myös Suomessa.
- Zerologon-haavoittuvuutta hyväksikäytetään aktiivisesti. Varmista, että kaikki toimialueen ohjauskoneet on päivitetty.

Automaatio

- Microsoftin tutkimuksessa havaittiin haavoittuvuuksia 71% tutkituista automaatiojärjestelmäverkoista.
- Kasperskyn mukaan vuoden 2020 ensimmäisellä puoliskolla, vähiten hyökkäyksiä tehtiin pohjoiseurooppalaisia automaatiojärjestelmiä vastaan.

Verkkojen toimivuus

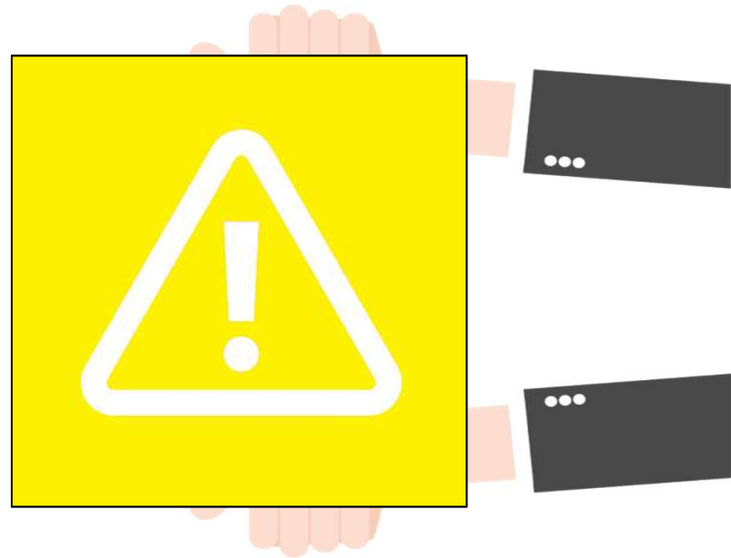
- Yhdeksän merkittävää toimivuushäiriötä, joista kolme johtui Aila-myrskystä. Muiden häiriöiden syynä useimmiten sähkönsyötön vika tai ylläpitotöissä tehty virhe.
- Palvelunestohyökkäysten osalta kohtuullisen rauhallista Suomessa, mutta hyökkäyksillä uhkailu nousussa.

Vakoilu

- Microsoft kertoi APT28-ryhmän kampanjasta, jonka pyrkimyksenä on ollut kerätä lukuisten organisaatioiden työntekijöiden salasanoja.
- Erilaisia ilmaisia tai kokeilujaksollisia palveluita voidaan hyödyntää komentokanavina haitallisen liikenteen piilottamiseksi.

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

71%

MICROSOFTIN TUTKIMISTA YLI 1 800 AUTOMAATIOJÄRJESTELMÄVERKOSTA SISÄLSI WINDOWS-JÄRJESTELMIÄ JOIDEN TUKI ON LOPPUNUT

YLI MILJOONA

VÄÄRENNETTYÄ TEKNISEN TUEN NIMISSÄ SOITETTUA PUHELUA SOITETTIIN SUOMEEN KUUKAUDEN AIKANA

NOIN 20

TIETOJENKALASTELUTAPAUSTA ONNISTUTTIIN ESTÄMÄÄN, KOSKA YKSI ORGANISAATIO ILMOITTI SAAMASTAAN KALASTELUSTA KYBERTURVALLISUUKESKUKSELLE

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 rikollisia toimijoita tulee jatkuvasti.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi. Lisäksi on havaittu että palvelunestohyökkäyksiä käytetään tehostamaan kiristyshaittaohjelmahyökkäysten lunnasvaatimuksia.

CASE

UUSI

Universal Health Services (UHS) sairaalaketjuun kohdistui syyskuussa kiristyshaittaohjelmahyökkäys. Raporttien mukaan haittaohjelma käynnistyi viikonlopun aikana ja sen vaikutukset kestivät noin viikon ajan. Tuona aikana hoitolaitokset ovat raportoidusti toimineet ilman sisäisiä IT-järjestelmiään. Lisäksi raportoitiin, että joitain potilaita on käännytetty pois taikka ohjattu toisiin sairaaloihin. UHS on varmistanut, että kiristyshaittaohjelmalla oli vaikutuksia kaikkiin heidän Yhdysvalloissa oleviin hoitolaitoksiinsa. UHS:lla on yhteensä 400 hoitolaitosta Yhdysvalloissa ja Iso-Britanniassa.

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

UUSI

Windowsiin kohdistuva Zerologon-haavoittuvuus ja sen korjaava päivitys julkaistiin elokuussa 2020. Hyväksikäyttömenetelmä tuli syyskuussa julki ja aktiivista hyväksikäyttöä havaittiin nopeasti. Mikäli haavaa ei viipymättä päivitetty heti elokuussa, hyökkääjälle mahdollistui käyttöoikeuksien laajentaminen ja toimialueen ohjauskoneen (domain controller) murtaminen ilman mitään tunnuksia.

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

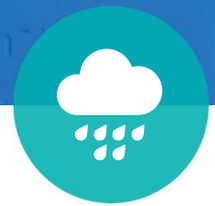
Lokitietojen puutteellisuus on riski monessa organisaatiossa.
Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään mikäli oikeiden järjestelmien tai sovellusten lokitietoja
ei kerätä, seurata ja säilytetä riittävän kauan.

- 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 ajan.

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

- Olemme vastaanottaneet tavallista enemmän ilmoituksia murretuista kotimaisista sivustoista sekä WordPress-sivustoista.
  - Kyberturvallisuuskeskukselle raportoitujen haittaohjelma- ja kalasteluviestien kautta paljastuu usein myös tietomurtoja.
- Maailmalla on tehty paljon havaintoja kiristyshaittaohjelmahyökkäyksistä.
  - Kohteena on ollut terveydenhoitoalan toimijoita, yhdessä tapauksessa kyberhyökkäys aiheutti myös potilaan kuoleman.

ANALYYSI

- Verkkosivustojen julkaisualustojen ja niiden lisäosien päivitykset on tärkeä pitää ajan tasalla.
- Otamme Kyberturvallisuuskeskuksessa mielellämme vastaan ilmoituksia haittaohjelma- tai kalasteluviesteistä, koska niiden avulla voidaan päästä myös tietomurtojen jäljille.

Tietomurrot ja -vuodot

- Saamme edelleen paljon ilmoituksia Office 365-tietomurroista.
  - Ilmoituksia onnistuneista tietomurroista ja niiden yrityksistä tulee tasaisella tahdilla.
  - Tietomurron jälkeen luottamuksellista tietoa voi paljastua ja päätyä rikollisten käsiin.
    - Tiliä ja sieltä saatuja tietoja voidaan käyttää myös rikolliseen toimintaan kuten. Laskutuspetoksiin, tietojen kalasteluun ja haittaohjelmien levitykseen.
  - Lue lisää kuinka suojautua Office 365 –tietojenkalastelulta täältä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja

ANALYYSI

- Office 365 –tapauksissa monivaiheisen tunnistautumisen käyttäminen suojaa tehokkaasti tietomurrolta.

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

- Syyskuu on ollut vilkas kaikilla huijausrintamilla. Apple ID, Netflix-tunnukset, pankkitunnukset ja maksukorttitiedot ovat kiinnostaneet huijareita kovasti.
- Pakettiteemaisia tekstiviestihuijauksia on lähetetty Postin nimissä. Huijausviestien linkit johtavat tilausansoihin, mutta linkkien takaa tarjoillaan myös Apple ID -kalastelua ja Android-haittaohjelmaa.
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus
- WhatsApp-ryhmäkeskusteluissa osallistujat näkevät toistensa puhelinnumerot. Älä päästä tuntemattomia ulkopuolisia ryhmään, sillä hän voi varastaa henkilötietoja ja täyttää ryhmän häirintäviesteillä.

ANALYYSI

- Laskutuspetoksia ja toimitusjohtajahuijauksia on syyskuussakin tehty ahkerasti. Huijarit ovat saaneet lahjakortteja tuhansien eurojen arvosta.
- Huijari lähestyy maksuliikennehenkilöstöä usein sähköpostitse johtajan nimissä, mutta myös someviestejä, pikaviestipalveluita ja muita yhteydenottomenetelmiä on kokeiltu.
- Useimmat toimitusjohtajahuijaukset onneksi jäävät yritykseksi, kiitos valveutuneen henkilökunnan.

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.

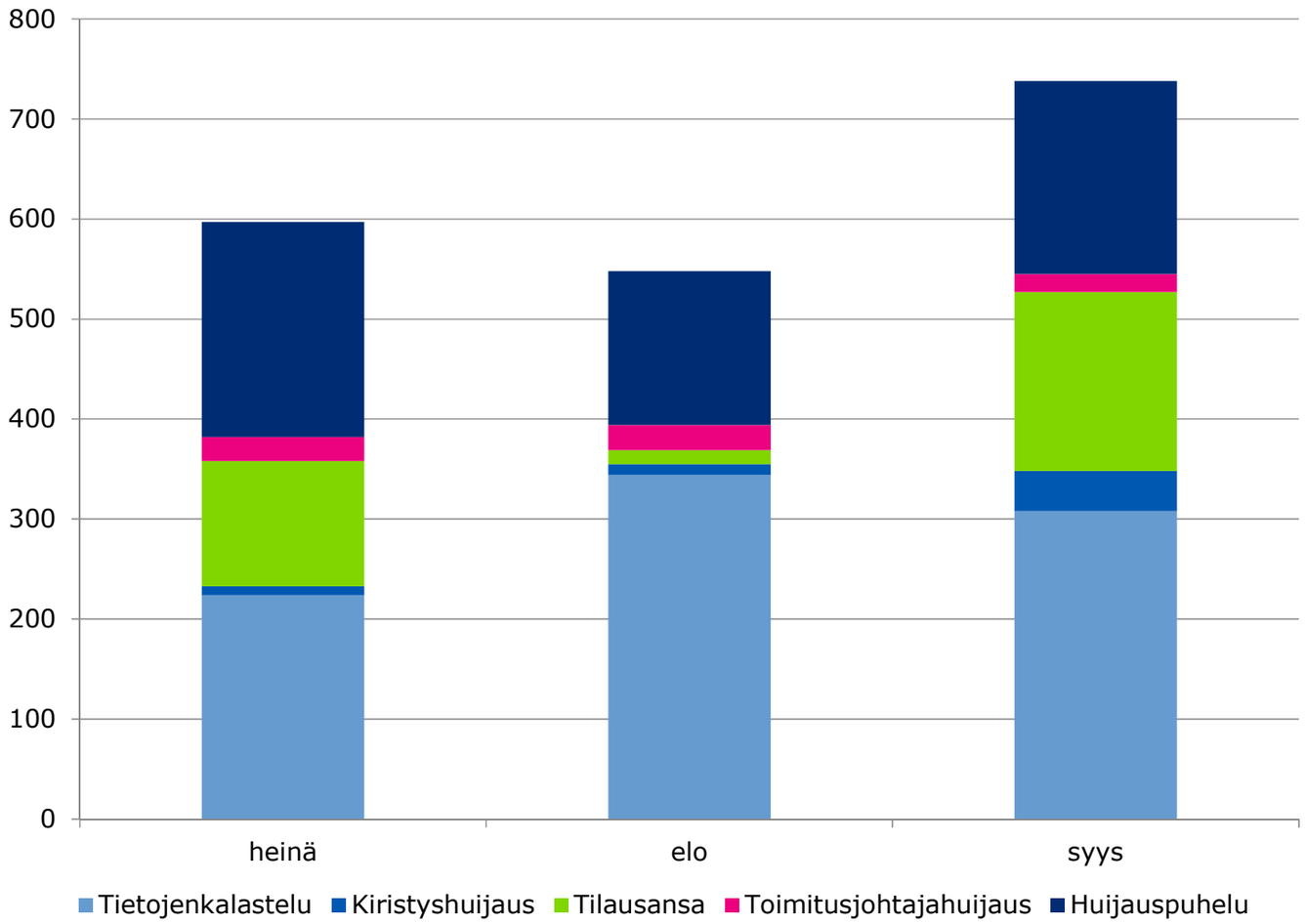
Office 365 -tietojenkalastelu

- Office 365 -tietojenkalastelu on edelleen yleistä. Alkuvuodesta tietojenkalastelu rauhoittui hieman, mutta vain hetkellisesti.
- Syyskuussa saatiin poistettua verkosta tietojenkalastelusivu, josta paljastui toistakymmentä suomalaista kalastelun uhria. Kyberturvallisuuskeskus oli yhteydessä uhriorganisaatioihin ja auttoi estämään enemmät tietojenkalastelun avulla tehdyt tietomurrot.
- Jossain tapauksessa tietomurto ja sähköpostin vakoilu on voinut jatkua kuukausia ilman että uhri huomaa sitä.

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 Q3/2020



- Kolmannen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Jatkuvat Postin nimissä tehdyt huijaukset, jotka johtavat tilausansoihin, tai puhelimen haittaohjelmaan.
  - Teknisen tuen huijauspuhelut jatkuivat edelleen.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.

Haittaohjelmat ja haavoittuvuudet

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

Haavoittuvuudet

- Kriittinen Zerologon-haavoittuvuus Windows toimialueen ohjauskoneissa (domain controller)
  - Haavoittuvuuden hyödyntäminen on erittäin helppoa ja johtaa koko toimialueen haltuunottoon.
  - Koska kyseessä on protokolla-haavoittuvuus koskee se Windows toimialueen ohjauskoneen lisäksi myös Sambaa.
  - Enforcement-moodi tulisi kytkeä päälle, ellei se ole jostain tietystä syystä poissa päältä.

- Varmista, että viimeinenkin toimialueen ohjauskone tulee päivitettyä
  - https://www.kyberturvallisuuskeskus.fi/fi/hyokkaystyokaluja-julkaistu-kriittiselle-zerologon-haavoittuvuudelle
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kriittisen-zerologon-haavoittuvuuden-aktiivinen-hyvaksikaytto-alkanut

ANALYYSI

- Haavoittuvuus tuli julkisuuteen 11.8. Havaintoja aktiivisesta hyväksikäytöstä näkyi jo kuukautta myöhemmin. Suosittelemme painokkaasti päivittämään haavoittuvuuden!
- Yhdysvalloissa annettiin 21.9. pakottava määräys (emergency directive) valtion virastoille, jolla ne velvoitettiin päivittämään haavoittuvuus muutaman päivän kuluessa.

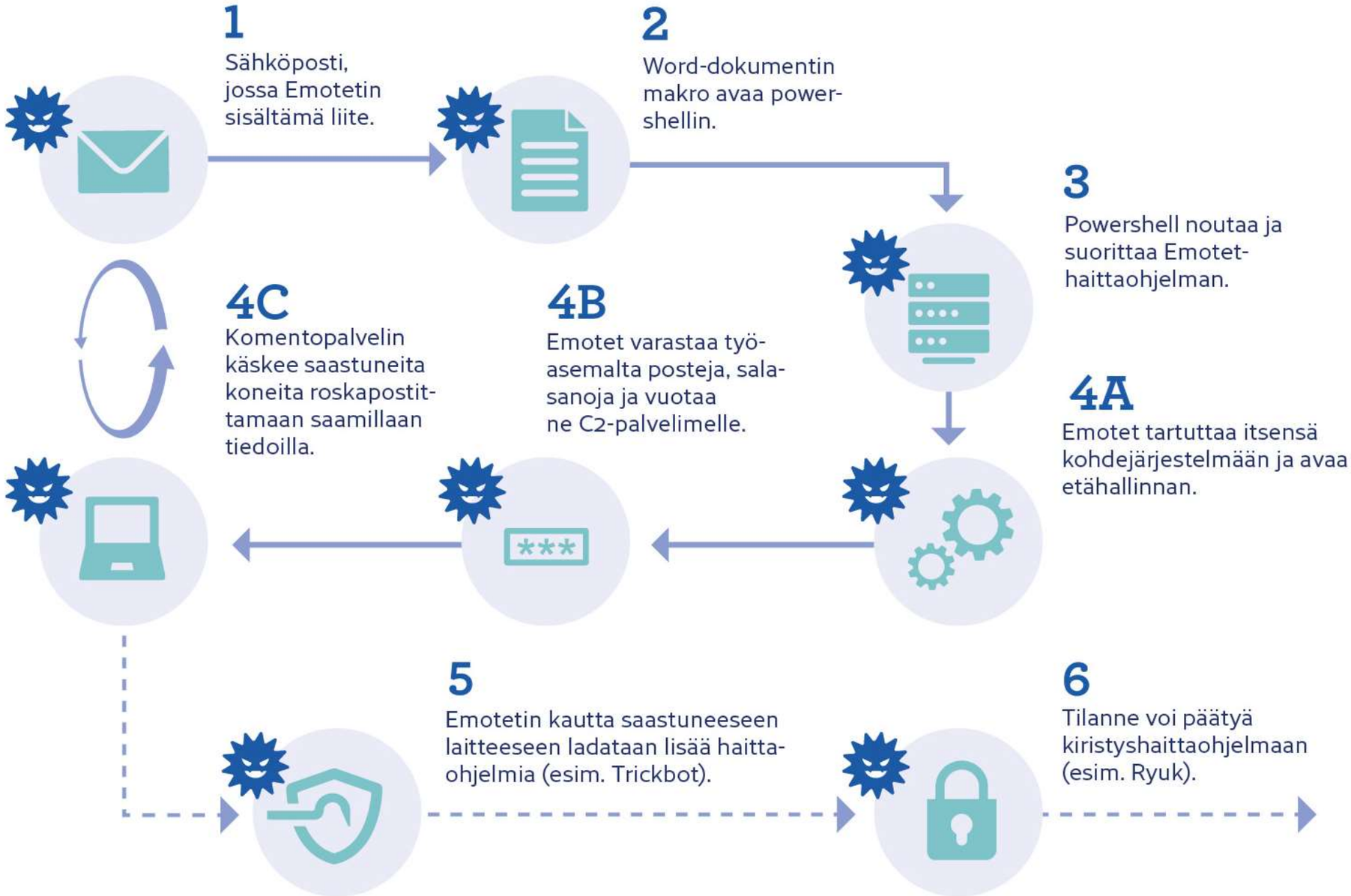
Haittaohjelmat

- Emotet-haittaohjelma leviää aktiivisesti myös Suomessa
  - Hyödyntää aitoja ja varastettuja sähköpostikeskusteluja, aitoihin viesteihin on lisätty haitallisia liitetiedostoja.
  - Emotet-tartunta voi johtaa saastuneen laitteen kautta kiristyshaittaohjelmaan.
  - Elokuussa julkaistu keltainen varoitus koskien Emotet:ia on edelleen voimassa.
    - https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa
- Kiristyshaittaohjelma havaintoja on ollut maailmalla runsaasti
  - Merkittävässä roolissa ovat järjestelmätyökalujen haitalliset käyttötavat (englanniksi ”living off the land”).
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/edistyneet-kiristyshyokkaykset-yleistyvat-varo-joutumasta-saaliiksi

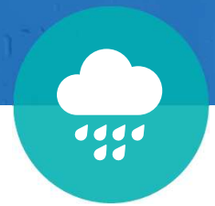
ANALYYSI

- Hyökkääjät väärinkäyttävät järjestelmätyökaluja vaikeuttaakseen havainnointia. Ne helpottavat hyökkääjän toimintaa eikä järjestelmässä aiheudu hälytyksiä turva-kontrollien toimesta.
- Tarkkailemalla järjestelmätyökalujen epänormaalia käyttöä voi havaita tartunnan tai tutkia kykenevätkö omat tietoturvaratkaisut havaitsemaan epänormaalin käytön.

Emotet-haittaohjelmatartunnan eteneminen



TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus



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 ja IoT

- Microsoftin julkaisusta Microsoft Digital Defense Report, September 2020 on poimittavissa seuraavat havainnot:
  - IoT-laitemäärä kasvaa lähivuosina kymmeniin miljardeihin. Samalla myös laitteisiin kohdistuvien hyökkäysten määrä kasvaa.
  - Suurimman uhan muodostavat väärä konfiguraatio ja haavoittuvuuksien hyväksikäyttö.
  - Tutkituista yli 1 800 automaatiojärjestelmäverkosta 71 %:ssa havaittiin tukemattomia Windows-järjestelmiä, kuten Windows 2000, Windows XP ja Windows 7.
    - Vaikka huomiotta jätetään tammikuussa 2020 vanhentunut Windows 7, tukemattomia järjestelmiä oli 62% tutkituista automaatiojärjestelmäverkoista.
- Windows XP:n lähdekoodi vuodettiin verkkoon syyskuussa.

ANALYYSI

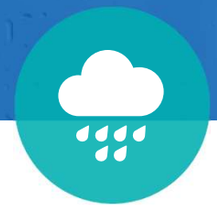
- Haavoittuvat toteutukset voivat muodostaa merkittävän riskin organisaatiolle.
- Riskien hallinta ensiarvoista: haavoittuvien toteutuksien tunnistaminen sekä suojaus ja valvonta, jos haavoittuvuuksia ei ole mahdollista korjata.
- Microsoftin raportti ladattavissa osoitteesta https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738

Automaatio

- Kasperskyn raportti automaatiojärjestelmissä havaituista tietoturvauhista
  - Vuoden 2020 ensimmäisellä puoliskolla entistä harvemmassa automaatiolaitteessa on havaittu hyökkäyksiä.
  - Kasperskyn havaintojen mukaan vähiten hyökkäyksiä tehtiin pohjoiseurooppalaisia automaatiojärjestelmiä vastaan.
  - https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/ ja tiivistelmä https://securelist.com/threat-landscape-for-industrial-automation-systems-h1-2020-highlights/98427/

ANALYYSI

Kasperskyn tunnistamaa hyökkäysten vähyyttä pohjoiseurooppalaisia automaatiojärjestelmiä vastaan selittänee yleisesti hyvä ICT-järjestelmien tietoturvan taso Pohjois-Euroopassa. Rikollisten siis lienee tuottavampaa kohdentaa aktiivisuutensa muualle.



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

- Syyskuussa yhdeksän merkittävää häiriötä yleisissä viestintäpalveluissa
- Aila-myrsky riepotteli yleisiä viestintäpalveluita erityisesti Pohjanmaalta Keski- ja Itä-Suomeen ulottuvalla alueella.
  - sähkökatkot aiheuttivat kolme merkittävää toimivuushäiriötä matkaviestinverkkojen palveluissa.
- Muista kuudesta merkittävästä häiriöstä
  - kahden syynä oli voimalaitejärjestelmän vika tärkeissä laitetiloissa.
  - kaksi johtui virheistä muutos- tai huoltotöissä.

ANALYYSI

- Teleyritysten, sähköverkkourakoitsijoiden ja pelastustoimen yhteistyö Aila-myrskyn aiheuttamien häiriöiden hallinnassa toimi hyvin.
- Telejärjestelmien voimalaitejärjestelmien vikojen pitäisi olla ennalta ehkäistävissä ja nopeasti korjattavissa. Asiaa käsitellään Viestintäviraston määräyksessä 54.
- Huolellinen muutos- ja huoltotöiden suunnittelu ja varautuminen virheisiin muutoksissa on tärkeää toimivuushäiriöiden ehkäisemisen kannalta. Asiaa käsitellään Liikenne- ja viestintäviraston määräyksessä 66.

Palvelunestohyökkäykset

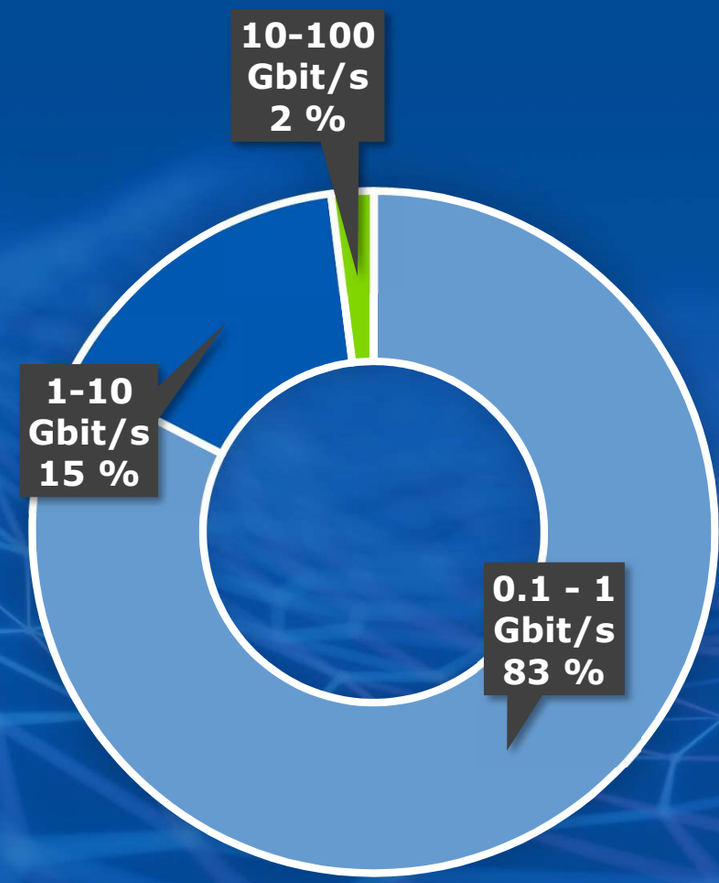
- Syyskuu oli palvelunestohyökkäysten osalta Suomessa kohtuullisen rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäyksillä uhkailu ja lunnasrahojen vaatiminen ovat yleistyneet maailmalla.
  - Uutena ilmiönä palvelunestohyökkäyksiä käytetään tehostamaan kiristyshaittaohjelmahyökkäysten lunnasvaatimuksia.
  - Ulkomailla toteutettujen hyökkäysten vaikutukset ovat vaikuttaneet myös suomalaiseen organisaatioon.
- Maailmalla palvelunestohyökkäysten trendi on ollut nousussa sekä hyökkäysten koon että keston osalta.
  - Useissa Euroopan maissa on kohdistunut myös hyökkäyksiä internetin infrastruktuuriin sekä digitaalisiin palveluihin, joilla saattoi olla laajoja vaikutuksia eri organisaatioiden toimintaan.
  - Suurilta volumetrisiltä hyökkäyksiltä suojautuminen voidaan toteuttaa tehokkaasti internet-palveluntarjoajien tarjoamien DDoS-suojauspalveluiden avulla.

ANALYYSI

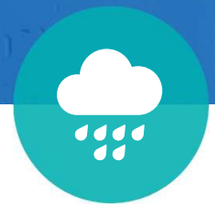
- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volumetriset että sovellustason hyökkäykset.

Palvelunestohyökkäysten tunnuslukuja

- 63 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2020.
- Noin 78% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q3/2020 - 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

- APT-ryhmä Fancy Bear on pitkin vuotta pyrkinyt saamaan teknisin menetelmin käsiinsä Office 365 -salasanoja lukuisista organisaatioista. Ryhmä tunnetaan myös nimillä APT28 ja STRONTIUM.
  - Asiasta kertoneen Microsoftin mukaan salasanojen keräys (engl. credential harvesting) on kohdistunut viime vuoden syyskuun ja kuluvan vuoden kesäkuun välillä kymmeniin tuhansiin käyttäjätileihin ja yli 200 organisaatioon maailmalla. Vastaavasti alkusyksystä kohteena lähes 7 000 käyttäjätiliä 28 organisaatiossa.
  - Microsoft varoittaa toiminnan voivan onnistuessaan vaikuttaa esimerkiksi Yhdysvaltojen vaaleihin. Microsoftin mukaan havaintoja onnistuneista tunkeutumisista käyttäjätileille ei kuitenkaan ole ollut.
  - Microsoft on myös aiemmin tiedottanut sekä Trumpin että Bidenin kampanjoihin kohdistuneista vakoiluyrityksistä, joiden taustalla se on arvioinut olevan useita eri valtiolliseen toimintaan liitettyjä ryhmiä.

ANALYYSI

- Salasanojen arvaamista teknisin menetelmin esiintyy yleisesti, ja organisaatioiden olisi hyvä pyrkiä havainnoimaan erilaisiin järjestelmiin kohdistuvia salasanojen arvausyrityksiä.
- Organisaatioiden kannattaa pohtia, miten voidaan estää liian yksinkertaisten tai arvattavien salasanojen valinta, sekä huolehtia siitä, että työntekijöiden käyttäjätilit suojataan siten, että yksittäisen salasanan arvaaminen ei vielä mahdollista hyökkääjälle pääsyä organisaation tietoihin.

Vakoilu

- Kybervakoilussa voidaan hyödyntää avoimia tai ilmaisia pilvipalveluita tai niiden ilmaisia kokeilujaksoja esimerkiksi komentojen antamiseksi niille laitteille, joihin hyökkääjä on onnistunut tunkeutumaan.
  - Microsoft kertoi syyskuussa, että sen GADOLINIUM-nimellä kutsuma ryhmittymä oli hyödyntänyt Microsoftin pilvipalveluita komentopalvelimena. Ryhmä tunnetaan myös esimerkiksi nimellä APT40.
  - Operaatiossa oli hyödynnetty useita eri Microsoftin tarjoamia ratkaisuja komentojen välittämiseen. Esimerkkejä tästä olivat esimerkiksi kuvatiedostoksi naamioidun PowerShellin jakelu Microsoft Graph API:n kautta ja Outlook Task API:n käyttäminen komentojen antamiseen tai suorittamiseen.

ANALYYSI

- Tämän tyyppisen hyökkäyksen havaitseminen pelkästään verkkoliikennepohjaisella havainnoinnilla on vaikeaa, minkä vuoksi havainnointikykyä on tärkeää täydentää perinteisen viruksentorjuntaohjelmiston lisäksi myös muulla päätelaitteilla tehtävällä havainnoinnilla.
- Lisäksi ei-toivottua ohjelmakoodin suorittamista päätelaitteilla on hyvä pyrkiä estämään mahdollisimman kattavasti esimerkiksi sallittujen ohjelmien ja suoritussijaintien määrittelyllä (whitelist).

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

- HE-luonnos sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muutoksista lausuntokierroksella
- Hallituksen esityksen luonnos on lausuttavana 30.10. saakka.

ANALYYSI

- Ensitunnistamisen ketjuttamisen enimmäishintasääntelyä jatkettaisiin kahdella vuodella, 31.3.2023 asti.
- Enimmäishintaa ei muutettaisi, vaan se olisi jatkossakin 0,03 euroa, kuten muillakin tunnistustapahtumilla.
- Liikenne- ja viestintävirastolle tulisi uusi tehtävä kerätä ja muodostaa tilastotietoa vahvan sähköisen tunnistamisen markkinasta ja tarjonnasta sääntelyn vaikutusten seuraamista, sähköisen tunnistamisen markkinoiden ohjaamista ja lainsäädännön kehittämistä varten.
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ff740d82-a3b8-44c3-a578-6c6a5876c329

Oikeudelliset asiat

- EU:n tuomioistuin (EUTI) tulkitsi ensimmäisen kerran verkkoneutraliteettiasetusta 15.9. annetussa ratkaisussa.

ANALYYSI

- EUTI tulkitsi 15.9.2020 annetussa tuomiossa ensimmäistä kertaa asetusta 2015/2120, jossa vahvistetaan internetin avoimuuden keskeinen periaate (verkkoneutraliteetti).
- Telenor-yhtiö tarjosi asiakkailleen palvelupakettia, jossa oli ns. nollatariffipääsy tiettyihin palveluihin ja sovelluksiin riippumatta asiakkaan käytettävissä olevasta datakiintiöstä. Datakiintiön täytyttyä muihin palveluihin ja sovelluksiin sovellettiin liikenteen estämistä tai hidastamista koskevia toimenpiteitä.
- EUTI katsoi Telenorin menettelyn olevan vastoin internetin käyttäjien oikeuksien turvaamista ja liikenteen syrjimättömän kohtelun vaatimuksia.
- Tuomio yhdistetyissä asioissa C-807/18 ja C-39/19.

Oikeudelliset asiat

- Tiedonhallintalautakunnan suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta julkaistu
  - Valtiovarainministeriö on julkaissut viranomaisille tarkoitetun tiedonhallintalautakunnan suosituskokoelman, jonka tarkoituksena on opastaa tiedonhallintalain asettamien erinäisten tietoturvaan liittyvien vaatimusten täyttämisessä.
  - 21.9.2020 julkaistu suosituskokoelma korvaa 1.4.2020 julkaistun version.
  - http://urn.fi/URN:ISBN:978-952-367-295-6

Arjen kyberturvallisuus – syyskuu

Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus

- Postin nimissä liikkuu nyt tietojenkalastelua ja tilausansahuijauksia tekstiviestien välityksellä.
- Ethän avaa mitään linkkejä harkitsematta, koska vastaan voi tulla haittaohjelmia, kalastelua ja muita huijauksia - välittömästi.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

Polar Vantage M -kellolle Tietoturvamerkki

- Polar Vantage M -GPS-multisportkello on saanut Traficomin myöntämän Tietoturvamerkin
- Tietoturvamerkki kertoo siitä, että merkillä varustettu tuote tai palvelu on suunniteltu tietoturvalliseksi.
- Merkkiä käytetään internetiin yhdistettävissä olevissa älykkäissä kuluttajalaitteissa, eli ns. IoT-laitteissa.
- https://tietoturvamerkki.fi/fi/tuote-polar-vantage-m-gps-multisportkello/

#tietoturvatorstai - Ota arjen tietoturva haltuun asiantuntijoidemme kanssa

- Kyberturvallisuuskeskuksen asiantuntijat vastaavat moniin tietoturva-aiheisiin kysymyksiin #tietoturvatorstai-videoissa.
- Jatkossa löydät videot torstaisin somekanavistamme - ota seurantaan #tietoturvatorstai.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvatorstai-ota-arjen-tietoturva-haltuun-asiantuntijoidemme-kanssa

Euroopan kyberturvallisuuskuukausi

- Lokakuussa laitetaan kyberturvallisuuden ja tietoturvan perustaitoja kuntoon Euroopan kyberturvallisuuskuukauden merkeissä!
- Tämän vuoden kyberturvallisuuskuukauden pääteemat ovat kyberhuijaukset ja kybertaidot.
- Tutustu kampanjaan tältä sivulta:
- https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ajankohtaista Kyberturvallisuuskeskuksesta

Uusi oppaamme auttaa vahvistamaan pienyritysten kyberturvallisuutta

- Pienyrityksiin kohdistuvat tietoturvaloukkaukset voivat aiheuttaa merkittävää haittaa yrityksen taloudelle ja maineelle.
- Uusi oppaamme auttaa pienyrittäjiä suojautumaan yleisimpiä kyberuhkia vastaan.
- Oppaassa käsitellään muun muassa tietojenkalastelua, haittaohjelmia, päivityksiä ja käyttöoikeuksien hallintaa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-oppaamme-auttaa-vahvistamaan-pienyritysten-kyberturvallisuutta

Turun seudun puhdistamo näyttää esimerkkiä pitkäjänteisestä häiriönhallinnasta

- Kyberturvallisuuskeskus tukee säännöllisesti organisaatioiden harjoittelua.
- Olemme pyytäneet muutamia harjoitelleita tahoja kirjoittamaan kokemuksistaan. Tällä kertaa kyberharjoittelustaan kertoo Turun seudun puhdistamo.
- Noin päivän mittaisessa työpajassa parannettiin puhdistamon henkilöstön yleistä tietoisuutta kyberturvallisuutta uhkaavista riskeistä.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turun-seudun-puhdistamo-nayttaa-esimerkkia-pitkajanteisesta-hairionhallinnasta

Kyberharjoitusohje julkaistu ruotsiksi ja englanniksi

- Harjoitusohje soveltuu niin ensimmäistä harjoitustaan järjestävälle organisaatiolle kuin kokeneellekin harjoituskonkarille uusien menetelmien ja näkökulmien etsimiseen.
- Se on kirjoitettu ensisijaisesti käytännön ohjeeksi heille, joille kyberharjoituksen järjestäminen on ajankohtaista.
- Ruotsin- ja englanninkielisiin ohjeisiin pääset tutustumaan Harjoitustoimintamme sivuilla. Huomaa että sivun kieli pitää muuttaa sivun ylälaidasta joko ruotsiksi taikka englanniksi.
- https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

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