TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 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 Heinäkuu 2020

Tietomurrot ja -vuodot

- Havaintoja suomalaisista murretuista PulseSecure- ja Netscaler-palvelimista ja haavoittuvista BIG-IP-palvelimista.
- Office 365 –tietomurtojen määrä jälleen nousussa kesän hiljaisemman ajan jälkeen.

Huijaukset ja kalastelut

- Tietojenkalastelu on ammattirikollisten aktiivisesti käyttämä työkalu, jonka merkitys verkkohuijauksissa on korostunut.
- Puhelinhuijaukset ovat palanneet karanteenitauon jälkeen. Suomeen tulee satojatuhansia huijauspuheluita.

Haittaohjelmat ja haavoittuvuudet

- Ransomware-toimijat huutokauppaavat varastettuja tietoja tavoitteenaan rahastaa tiedoilla.
- Heinäkuussa julkaistiin kriittisiä haavoittuvuuksia ja verkkolaitteisiin kohdistuneita haavoja käytettiin aktiivisesti hyväksi.

Automaatio

- Yhdysvaltain viranomaiset varoittivat lisääntyneestä kyberhyökkäysten uhkasta automaatiojärjestelmiä vastaan.
- Automaatiojärjestelmiä koskevia haavoittuvuuksia löytyy entistä useammin.

Verkkojen toimivuus

- Vain kolme merkittävää yleisten viestintäpalveluiden häiriötä.
- DigiCert mitätöi useita varmenteita 11.7., mikä vaikutti myös useiden suomalaisten palveluiden toimintaan.
- Heinäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen.

Vakoilu

- EU on ryhtynyt ensimmäistä kertaa aktiivisiin vastatoimiin valtiollisia kyberhyökkäyksiä vastaan pakotteiden muodossa.
- Kohdistettujen hyökkäysten tavoitteena ei ole vain vakoilu, vaan myös vaikuttaminen ja ydinaseohjelman rahoittaminen.

Kuukauden tunnuslukuja

3

VALTIOTA, KIINA, VENÄJÄ JA POHJOIS-KOREA, ENSIMMÄISTÄ KERTAA EU:N PAKOTTEIDEN KOHTEENA KYBERHYÖKKÄYSTEN TAKIA

$10M

KIRISTYSHAITTAOHJELMAN LUNNASVAATIMUS GARMINILLE JA CWT:LLE. GARMININ KERROTAAN MAKSANEEN VAADITUT 10 MILJOONAA, CWT NEUVOTTELI MAKSUN 4,5 MILJOONAAN

6

KUUSINKERTAINEN MÄÄRÄ KYBERTURVALLISUUSKESKUKSELLE ILMOITETTUJA TILAUSANSOJA KESÄKUUHUN VERRATTUNA

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 UUSI

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

5 UUSI

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

UUSI

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

UUSI

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

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 UUSI

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 UUSI

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

- Havaintoja suomalaisista murretuista PulseSecure- ja Netscaler-palvelimista ja haavoittuvista BIG-IP-palvelimista.
  - Havaintoja on yli kolmekymmentä ja niistä on ilmoitettu palvelinten omistajille.
  - Haavoittuvat palvelimet ovat tyypillisesti kenen tahansa havaittavissa esim. Shodan-palvelulla.
- Office 365 –murrot ovat jälleen yleistyneet keskikesän suvantovaiheen jälkeen.

ANALYYSI

- Verkkojen omistajien kannattaa itse aktiivisesti havainnoida verkoistaan internetiin paljastuvaa hyökkäyspinta-alaa ja laatia suunnitelmat tietomurroista toipumiseen.
- Rikolliset kartoittavat uusia hyökkäysvektoreita jatkuvasti, joten organisaatioiden oma havainnointikyky on tärkeä osa hyökkäysten havaitsemisessa.

Tietomurrot ja -vuodot

- Twitterin taustajärjestelmään kohdistunut tietomurto herätti maailmanlaajuista huomiota
  - Useiden julkisuuden henkilöiden Twitter-tilit kaapattiin ja niiltä lähetettiin Bitcoin-huijausviestejä
  - Viesteissä kehotettiin lähettämään $1000 ja summa luvattiin maksaa kaksinkertaisena takaisin
- Garmin kyberhyökkäyksen kohteena - vaikutuksia lukuisiin palveluihin
  - Kiristyshaittaohjelma haittasi ja esti Garminin toimintaa
- CWT tietomurron kohteena, hyökkääjät uhkasivat vuotaa satoja gigatavuja varastettua dataa.

ANALYYSI

- Viestin lähettäjään ei tule luottaa sokeasti ja mikäli tilaisuus vaikuttaa liian helpolta, se tuskin on totta.
- Omien tietojen luovuttamista puhelimitse tai sähköpostitse tulee harkita tarkkaan. Huijarit voivat hyödyntää haltuunsa saatuja tietoja muissakin huijauksissa.

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

- WhatsApp-varmistuskoodeja on yritetty kalastella, jotta sillä voisi kiertää kaksivaiheisen tunnistautumisen.
- Tilausansoja on viritetty runsaasti mm. Postin ja Keskon nimissä.
- Pankkitunnusten ja henkilötietojen kalastelu jatkuu värikkäänä eri teemoilla, mm. Postin nimissä. Kalasteltuja tietoja on käytetty pikavippien nostamiseen uhrien kustannuksella.
- Kansainvälinen käyttäjätunnusten kalastelukampanja on saanut heinäkuussa tuhansia uhreja, joista Suomessakin kymmeniä.
  - Tietojenkalastelu on ammattirikollisten tyypillinen työväline.

ANALYYSI

- Kyberturvallisuuskeskus sai heinäkuun aikana ilmoituksia toimitusjohtajahuijausyrityksistä, mutta onnistuneita tapauksia ilmoitettiin vain muutama.
  - 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.
- On tärkeää, että tietoisuutta ilmiöstä pidetään yllä. Kesän aikana tulee huolehtia siitä, että työntekijät tietävät keneltä he voivat tarkistaa mahdollisen maksun oikeuden mikäli he epäilevät asiaa.

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.

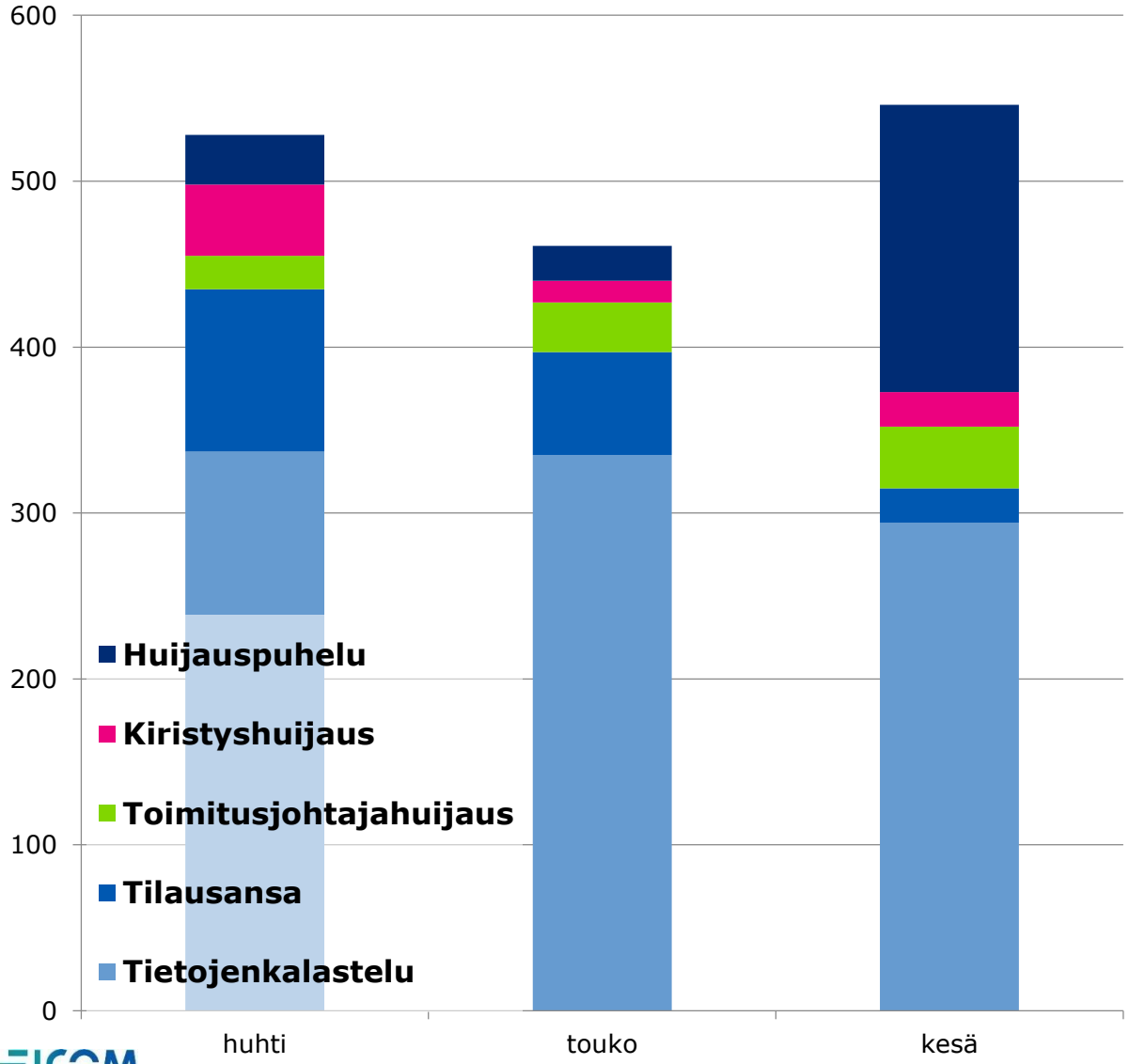
Office 365 tietojenkalastelu

- Office 365 tietojenkalastelu on edelleen yleistä. Alkuvuodesta tietojenkalastelu rauhoittui hieman, mutta vain hetkellisesti.
- Uutena havaintona on, että tietojenkalasteluviestit sisältävät liitteen, jonka lähdekoodi on sumutettu (muutettu symboliseen konekieliseen muotoon).
- Sähköpostin liitteenä olleita tiedostoja ei ole aluksi havaittu haitallisiksi erilaisten sähköpostisuodattimien avullakaan.

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

- Sähköpostin liitetiedostoina yritetään levittää haittaohjelmia
  - Emotet –yksi eniten kustannuksia aiheuttavista haittaohjelmista, jotka leviävät esim. liitetiedostojen makrojen ja haitallisten linkkien avulla
  - Emotet:n avulla levitetään myös muita haittaohjelmia, joista osa voi johtaa jopa kiristyshaittaohjelma tapauksiin
  - Suomalaisen logistiikkayrityksen nimissä lähetettiin huomattavia määriä sähköposteja, jotka sisälsivät haitallisen liitetiedoston
- Suomessakin havaintoja Wacatac-troijalaisesta
  - Tulee koneelle yleensä kalasteluviestien kautta, mahdollistaa etäkäytön ja varastaa tietoja

ANALYYSI

- Sijaisten ja henkilökunnan ohjeistus on tärkeää sähköpostien käsittelyssä sekä etenkin tilanteissa, joissa on avattu haitallinen liitetiedosto.
- Mikäli liitetiedosto vaikuttaa epäilyttävältä, ilmoita yrityksen käytäntöjen mukaisesti heti asiasta esim. tekniseen tukeen tai tee ilmoitus tietoturvapoikkeamasta.

Haittaohjelmat

- Big Game Hunting –kiristyshaittaohjelmien uhkaan on syytä varautua myös Suomessa
  - Kampanjat voivat kohdistua kaiken kokoisiin organisaatioihin. Onnistunut kampanja voi lamauttaa toiminnan ja siksi sen tuomiin haittoihin tulee varautua ennalta.
  - Hyökkääjät eivät ole levänneet lomakaudella, vaan haittaohjelmia on yritetty levittää aktiivisesti esimerkiksi sähköpostissa.
  - Organisaatioiden tulisi ymmärtää IT-toimintaympäristöänsä, tunnistaa kriittiset järjestelmät ja valvoa vähintään niitä poikkeamien varalta.
  - Kiristyshaittaohjelmille on tyypillistä aktivoitua viikonloppuisin tai sellaisina ajankohtina, jolloin työntekijöitä on vähemmän paikalla.
  - Julkaisimme aiheesta Tietoturva Nyt! –artikkelin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kiristyshaittaohjelmien-aktiivinen-toiminta-jatkuu

ANALYYSI

- Ajantasaisten varmuuskopioiden, dokumentoinnin ja lokienhallinnan olemassaolo tulee tarkistaa ja järjestelmien palauttamisprosessi harjoitella.
- Huolehti, että kriittiset varmuuskopiot ovat hyökkääjien ulottumattomissa.

Haavoittuvuudet

- Kriittinen SIGRed-haavoittuvuus Windows DNS-palvelimessa
  - Mahdollistaa etähyökkäyksellä ylläpitäjän käyttäjävaltuuksien saamisen
- Käyttöjärjestelmien Secure Boot -ominaisuudessa haavoittuvuus
  - Hyökkääjien mahdollista ohittaa Secure Boot –ominaisuuden tarjoama suoja
- SAP NetWeaver –kriittinen haavoittuvuus
  - Mahdollistaa järjestelmän haltuunoton verkon yli tunnistautumatta

ANALYYSI

- Kriittiset haavoittuvuudet aiheuttavat paineita ympäristöjen nopealle päivittämiselle.
- Päivitysten asentaminen on tärkeää myös loma-aikana.

Haavoittuvuudet

- Usean valmistajan verkkolaitteissa on tullut heinäkuussa ilmi kriittisiä haavoittuvuuksia
- F5 BIG-IP hallintakäyttöliittymässä on kriittinen haavoittuvuus, jota hyväksikäytetään aktiviisesti laitteiden kaappaamiseksi
- Citrix haavoittuvuuden avulla voi ohittaa palvelun hallintakäyttöliittymän kirjautumisen
- Cisco ASA ja Firepower –verkkolaitteissa vakava haavoittuvuus
  - Haavoittuvuuden avulla hyökkääjä voi yhdistää VPN-palveluun tunnistautumatta
- Palo Alto PAN-OS
  - Haavoittuvuuden avulla hyökkääjä voi pahimmillaan yhdistää VPN-palveluun tunnistautumatta

ANALYYSI

- Etäyhteyspalveluiden haavoittuvuudet ovat olleet hyökkääjien suosimia jo pidemmän aikaa.
- Hyökkäykset alkavat usein nopeasti haavoittuvuuden julkaisun jälkeen, joten nopea päivittäminen on 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

- Yhdysvaltain turvallisuusviranomaiset varoittivat kyberhyökkääjien kasvaneesta mielenkiinnosta automaatiojärjestelmiä kohtaan.
  - Internetin kautta automaatiojärjestelmiin hyökkäämisestä on tullut entistä helpompaa.
  - Varoituksessa on kuvattu hyökkääjien toimintaa sekä tehokkaita keinoja hyökkäysten torjumiseksi.
  - https://us-cert.cisa.gov/ncas/alerts/aa20-205a

ANALYYSI

- Kyberhyökkääjät ovat edelleen kiinnostuneita automaatiojärjestelmistä. Järjestelmät kiinnostavat sekä nopean rahanteon motivoimia rikollisia että strategiseen vaikuttamiseen pyrkiviä toimijoita.
- Toiminnan keskeytyminen on yleensä suurin riski.
- Torjuntakeinot ovat tuttuja ja pääosin teknisesti yksinkertaisia, mutta valitettavan usein niiden huolelliseen toteuttamiseen ei ole riittäviä resursseja.

Automaatio

- Automaatiojärjestelmien VPN-tuotteista paljastui kriittisiä haavoittuvuuksia.
  - Haavoittuvuuksien hyväksikäytäjä voi ottaa hallintaansa useita osia internetiin kytketyistä automaatiojärjestelmistä.
  - https://www.claroty.com/2020/07/28/vpn-security-flaws/
- USB-muistitikut ovat edelleen keskeisiä haittaohjelmien leviämisessä automaatiojärjestelmiin.
  - Honeywellin tekemä tutkimus osoitti, että 45 %:iin automaatiojärjestelmistä on vuoden aikana yritetty hyökätä USB-muistitikun välityksellä.
  - https://www.scmagazine.com/home/security-news/vulnerabilities/usb-prevalent-industrial-vector-vulnerability-for-ot-systems/

ANALYYSI

- Haavoittuvuuksia löytyy enemmän paitsi lisääntyneiden hyökkäysten myötä myös siksi, että tietoturvatutkijat käyttävät entistä enemmän aikaa automaatiotuotteiden tutkimiseen. Myös IT-järjestelmien VPN-tuotteiden haavoittuvuuksia on tutkittu runsaasti viimeisten 12 kk aikana.
- Järjestelmien omistajien täytyy nopeuttaa korjaavien ohjelmistopäivitysten käyttöönottoa.

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

- Heinäkuussa yleisissä viestintäpalveluissa oli kolme merkittävää toimivuushäiriötä
  - Määrä oli keskimääräistä kuukautta pienempi ja vaikutukset olivat suhteellisen vähäisiä.
- Cloudflaren palveluissa oli häiriöitä ympäri maailmaa 17.7.
  - Häiriöt alkoivat alkuyöstä Suomen aikaa. Selvimmin ne näkyivät Yhdysvalloissa ja ne vaikuttivat useisiin suosittuihin verkkopalveluihin.
  - Häiriö johtui Cloudflaren huoltotyössä tekemästä konfigurointivirheestä. https://blog.cloudflare.com/cloudflare-outage-on-july-17-2020/

ANALYYSI

- Yleisten viestintäpalveluiden häiriöiden juurisyissä korostuivat huolellisuuden tarpeellisuus viestintäpalveluiden huolto- ja muutostöiden toteuttamisessa sekä varajärjestelmien toimintakunnon valvonnan tärkeys.
- Sama näkyi myös Cloudflaren palveluiden häiriössä.

Verkkojen toimivuus

- Merkittävä TLS-varmenteiden myöntäjä DigiCert mitätöi lyhyellä varoitusajalla suuren määrän varmenteita 11.7.2020.
  - Mitätöinti johtui auditointiprosessissa tehdyistä virheistä. Varmenteiden myöntäjien yhteiset toimintasäännöt edellyttävät, että väärin auditoidun toiminnon tuottamat varmenteet mitätöidään.
  - Varmenteiden mitätöinti vaikutti Suomessa myös julkisen hallinnon sähköisten palveluiden saatavuuteen.
  - https://knowledge.digicert.com/alerts/DigiCert-ICA-Replacement

ANALYYSI

- Varmenteiden voimassaolon päättyminen haittaa päivittäin yksittäisten verkkopalveluiden toimintaa. Joitakin kertoja vuodessa varmenteiden myöntäjille tapahtuu virheitä, joiden vuoksi suuri määrä varmenteita täytyy mitätöidä kerralla. Seuraukset ovat yksittäisten verkkopalveluiden kannalta samat.
- Organisaatioiden kannattaa seurata aktiivisesti verkkopalveluidensa varmenteiden kelpoisuutta ja suunnitella käytännöt, joilla varmenteita saadaan uusittua ripeästi.

Palvelunestohyökkäykset

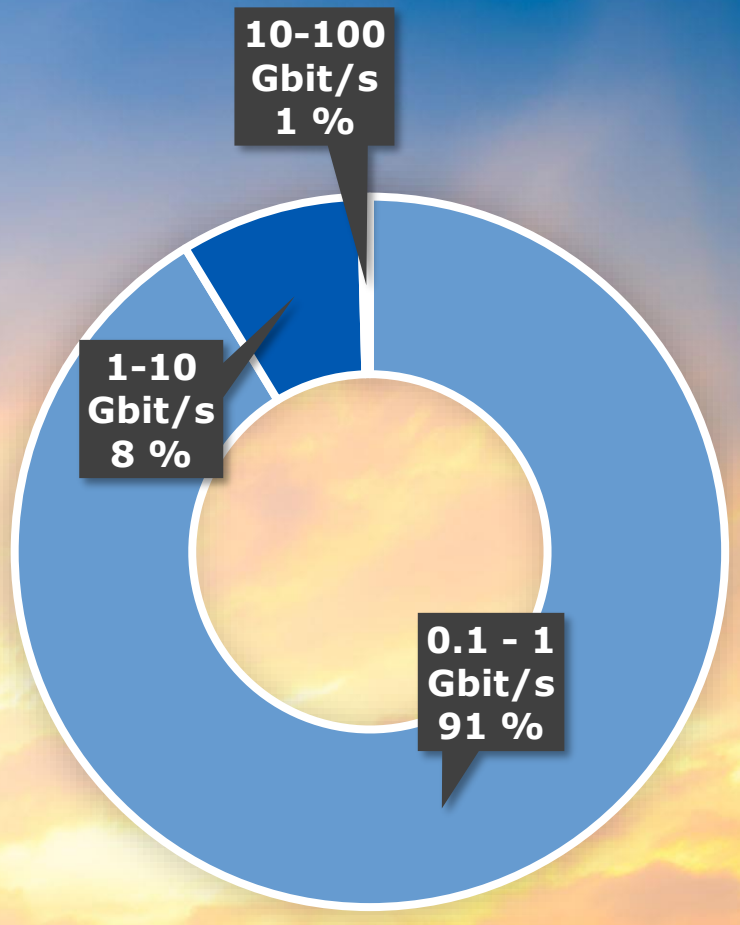
- Heinäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
- Suomeen kohdistuneiden palvelunestohyökkäysten määrä ja volyymit ovat kuitenkin olleet lievässä nousussa, mutta hyökkäystavoissa ei ole tapahtunut mitään erityistä muutosta.
- 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

- EU asetti ensimmäistä kertaa pakotteita kyberhyökkäysten takia
  - Pakotteiden kohteena oli kuusi henkilöä ja kolme organisaatiota Kiinasta, Venäjältä ja Pohjois-Koreasta.
  - Pakotteisiin kuuluu matkustuskielto ja varojen jäädyttäminen
  - Pakotteiden syynä olevat kyberhyökkäykset ovat:
    - Cloud Hopper –tietomurtokampanja (Kiina)
    - Hyökkäys OPCW-organisaatioita vastaan ja NotPetya-haittaohjelman levittäminen (Venäjä)
    - WannaCry-haittaohjelman levittäminen (Pohjois-Korea)

ANALYYSI

- Aikaisemmin vastaavia sanktioita ovat asettaneet lähinnä Yhdysvallat ja Iso-Britannia
- EU:ta on aikaisemmin moitittu passiivisuudesta valtioiden tukemien kyberhyökkäysten torjunnassa. Pakotteet mahdollistanut ”Kyberdiplomatian työkalupakki” on ollut voimassa vuodesta 2017 lähtien

Vakoilu

- Sekä Kiinaa että Venäjää syytetään COVID-19 –tutkimusta tekeviin organisaatioihin kohdistuneesta vakoilusta
  - Yhdysvaltain oikeusministeriö asetti kaksi kiinalaista syytteeseen tutkimustiedon kybervakoilusta
  - Yhdysvaltain NSA ja DHS CISA, Kanadan CSE sekä Iso-Britannian NCSC syyttävän Venäjän tiedustelupalveluun liitettyä APT29-ryhmää COVID-19 rokotetutkimuksen vakoilusta
  - Lisätietoja: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

ANALYYSI

- COVID-19 tutkimustiedon vakoilu nousi esiin jo keväällä eikä pandemian jatkuessa tule vähenemään

Vakoilu

- Pohjois-Korean uskotaan rahoittavan ydinaseohjelmaansa kyberhyökkäysten avulla
  - Uuden kiristyshyökkäyksissä käytetyn haittaohjelman uskotaan olevan vain pohjois-korealaisten hyökkääjien käytössä
  - Myös laajan verkkokauppoihin ja niiden asiakkaisiin kohdistuneen hyökkäyskampanjan uskotaan olevan Pohjois-Korean tiedustelupalvelun tekosia
  - Jo aikaisemmin sekä WannaCry-kiristyshaittaohjelma että digitaalisia pankkiryöstöjä tekevä Lazarus-ryhmä on liitetty Pohjois-Korean hallintoon

ANALYYSI

- Jo aikaisemmin sekä rikolliset että valtiolliset toimijat ovat käyttäneet kyberhyökkäyksiä samoja menetelmiä ja työkaluja. Nyt rajanveto myös motiivin suhteen hämärtyy entisestään
- Mahdolliset EU:n alueella olevat kiristyshyökkäysten uhrit joutuvat entistä vaikeampaan asemaan, sillä uudet EU:n Pohjois-Korealle asettamat sanktiot kyberhyökkäyksistä kieltävät myös varojen luovuttamisen sanktioiden kohteille

Vakoilu

- Kohdistettujen hyökkäysten tavoitteena ei ole pelkästään vakoilu, vaan lisääntymässä määrin myös vaikuttaminen
  - Yhdysvaltain CIA väitetään tehneen lukuisia kyberoperaatioita, joiden tarkoituksena on ollut tietojärjestelmien lamauttaminen tai arkaluonteisen tiedon vuotaminen julkisuuteen
  - Israelilaiset vesiyhtiöt ovat olleet jälleen kyberhyökkäysten kohteena. Aikaisemmin keväällä iranilaiset sataman toiminta lamaantui kyberhyökkäyksen takia
  - Venäjän sotilastiedusteluun liitetyn Fancy Bear / APT28 –ryhmän väitetään kohdistaneen hyökkäyksiin jälleen myös Yhdysvaltain energia-alan yrityksiin

ANALYYSI

- Vaikuttamisen kohteena on myös yksilöiden poliittinen päätöksenteko vaalien aikana. Erityisesti Yhdysvalloissa pelätään syksyn presidentinvaaleihin vaikuttavia vieraiden valtioiden tekemiä informaatiovaikuttamisoperaatiota siinä määrin, että lupaavat jopa 10 miljoonan dollarin palkkion kyseisten tahojen tunnistamiseen johtavista tiedoista.
- Iso-Britannian parlamentin raportin mukaan Venäjä yritti vaikuttaa Skotlannin itsenäisyysäänestykseen vuonna 2014 ja mahdollisesti myös Brexit-äänestykseen

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

- Hallituksen esitys laiksi tartuntatautilain väliaikaisesta muuttamisesta (HE 101/2020 vp) ja mobiilisovellus tartuntaketjujen jäljittämiseksi

ANALYYSI

- Eduskunnassa on käsitelty tartuntatautilakiin ehdotettua väliaikaista muutosta, jossa Liikenne- ja viestintävirastolle säädetään tehtäväksi arvioida THL:n korona-sovelluksen tietojärjestelmän tietoturvallisuus ennen sen käyttöönottoa.
- Sovelluskehityksestä vastaavat sosiaali- ja terveysministeriö sekä Terveyden ja hyvinvoinnin laitos. Kyberturvallisuuskeskuksen tehtävänä on arvioida sovellus.
- Lue lisää:
  https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_101+2020.aspx
  https://www.eduskunta.fi/valtiopaivaasiakirjat/StVM+17/2020
  https://www.eduskunta.fi/valtiopaivaasiakirjat/LiVL+3/2020

Oikeudelliset asiat

- EU-tuomioistuin tuomitsi 16.7.2020 laittomaksi Privacy Shield -sopimuksen, joka salli yhtiöiden luovuttaa käyttäjien henkilötietoja EU-alueelta Yhdysvaltoihin.

ANALYYSI

- Henkilötietoja kerätään muun muassa silloin, kun kuluttaja ostaa tavaroita tai palveluita verkossa, asioi sosiaalisessa mediassa tai tallentaa tietoja pilvipalveluun.
- EU:n ja Yhdysvaltojen Privacy Shield –järjestelyssä oli sallittu henkilötietojen siirto EU:sta yhdysvaltalaiselle yritykselle, jos kyseinen yritys käsittelee henkilötietoja siten, että se noudattaa lukuisia tietosuojasäännöksiä ja soveltaa lukuisia suojatoimia.
  - Nyt suojatoimet ja Privacy Shieldin tarjoama suoja on katsottu riittämättömäksi EU-tuomioistuimessa. EU:n ulkopuolelle, tässä tapauksessa Yhdysvaltoihin, luovutettavan tiedon tulee täyttää samanlainen suojaus kuin EU:ssa.
  - Päätös on merkittävä erityisesti sen takia, että Privacy Shieldiin perustuneelle henkilötietojen siirrolle Yhdysvaltoihin on osoitettava muu peruste, jos siirtoa halutaan jatkaa.
    - EU-tuomioistuimen päätös: http://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=FI&part=1&occ=first&mode=DOC&pageIndex=0&cid=13547852,
      EU-tuomioistuimen lehdistötiedote: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fi.pdf
      ja Euroopan tietosuojaneuvostona vastauksia yleisimpiin kysymyksiin tuomiosta: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

Oikeudelliset asiat

- Laki kuluttajansuojaviranomaisten eräistä toimivaltuuksista (566/2020) hyväksyttiin heinäkuussa
  - Lisätietoja: https://www.finlex.fi/fi/laki/alkup/2020/20200566
- Kuluttaja-asiamiehellä, tietosuojavaltuutetulla, Liikenne- ja viestintävirastolla sekä Kilpailu- ja kuluttajavirastolla on tässä laissa säädetyt toimivaltuudet yhteistyöasetuksen soveltamisalaan kuuluvissa asioissa

ANALYYSI

- Moni tekee nykyään ostoksia verkossa. Tämä on saanut myös rikolliset liikkeelle. Erilaisia valeverkkokauppoja ja sivuja, joiden tarkoitus on tietojenkalastelu, havaitaan yhä enenevissä määrin.
- Uusi lainsäädäntö antaa eri viranomaisille parempia mahdollisuuksia puuttua verkkosivuihin, joiden tarkoitusperä ei ole todellinen.

Arjen kyberturvallisuus – huiputuksia myös heinäkuussa

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

Neuvoja salasanan hallintasovelluksen käyttöönottoon

- Niin kutsutuissa salasanamanageri-sovelluksissa kaikki käyttäjän salasanat ovat tallessa hallintasovelluksen pääsalasanan takana. Tämä mahdollistaa yksilöllisten ja vahvojen salasanojen luomisen eri palveluihin.
- Käyttäjän on hyvä vertailla erilaisia hallintasovelluksia ja valita niistä itselleen sopivin.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Office 365 –kalastelu taas aktivoitunut

- Office 365 –teemainen tietojenkalastelu jatkuu taas aktiivisena rauhallisemman vaiheen jälkeen.
- Huijauksessa uhri menee linkin kautta tietojenkalastelusivulle ja syöttää sinne O365-tunnuksensa, jotka menevätkin rikollisen tietoon.
- Kaksivaiheinen tunnistautuminen on tärkein keino suojautua tietomurroilta. Varmista myös, että syötät tunnuksesi vain luotettaville sivuille.

Turvallisuusopas poikkeusolojen jälkeiseen aikaan

- Koronapandemia ei ole ohi, ja etäyhteydenpito ja –palaverit jatkuvat. Koronakevät ja –kesä ovat jättäneet jäljen nettiarkeemme, ja uusi aika vaatii uudistettuja ajattelu- ja toimintatapoja.
- Tutustu Kyberturvallisuuskeskuksen oppaan tietoturva- ja kyberturvallisuusneuvoihin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallisuusopas-poikkeusolojen-jalkeiseen-aikaan

Vietä #KyberturvallinenKesä

Toimitusjohtajahuijauksessa rikollinen lähettää organisaatiolle valelaskun.
Palkanmaksuhuijauksessa rikollinen pyrkii ohjaamaan organisaation työntekijän palkan itselleen.

Vahvistusprosessi

Organisaation olisi hyvä suunnitella erillinen vahvistusprosessi tilitietojen muutoksia varten.

Edelleenlähetys

Organisaation kannattaa rajoittaa sähköpostiviestien edelleenlähetyssääntöjä ja tarkastaa niitä säännöllisesti.

Varmista

Laskun maksaminen kannattaa varmistaa aina erikseen esimieheltä tai kollegalta.

Perehdytä

Kesäsijaiset tulee perehdyttää organisaation laskutuskäytäntöihin perusteellisesti.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

POLIISI
KESKUSRIKOSPOLIISI

Ajankohtaista Kyberturvallisuuskeskuksesta

Ohjeet kiristyshaittaohjelmiin varautumiseen

- Kiristyshaittaohjelmien aktiivinen levittäminen jatkuu myös Suomessa. Onnistunut kiristyshaittaohjelma-kampanja voi lamauttaa organisaation toiminnan jos tilanteeseen ei ole varauduttu ennalta.
- Organisaation tulee huolehtia lokienhallinnasta, verkkoliikenteen tarkkailusta ja varmuuskopioista. Kiristyshaittaohjelmasta tulee ilmoittaa Kyberturvallisuus-keskukselle, eikä lunnaita pidä maksaa.
- Tietoturva nyt! –julkaisu aiheesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kiristyshaittaohjelmien-aktiivinen-toiminta-jatkuu

Älä anna päivitysprosessin lomailla

- Kriittisten haavoittuvuuksien päivittäminen nopeasti on tärkeää, myös kesällä.
- Haavoittuvuuksien hyväksikäyttö tapahtuu nopeasti, joten organisaatioiden on tärkeää varmistaa prosessien toimivuus ja sijaisjärjestelyt myös lomien aikana.
- Haavoittuvuuden hyväksikäyttö voi johtaa esimerkiksi laitteen haltuunottoon tai tunnistautumisen ohittamiseen. Tietoturvapäivitys korjaa ohjelmiston haavoittuvuuden.
- Lue lisää Tietoturva nyt! -julkaisustamme: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ala-anna-paivitysprosessin-lomailla-suvena

Kyberharjoittelu paransi Kevan valmiuksia kohdata tosielämän uhkatilanteita

- Kyberturvallisuuskeskuksen uudessa julkaisusarjassa organisaatiot kertovat kyberharjoituskokemuksistaan.
- ”Harjoituksen avulla pystyimme tarkentamaan omia toimintatapojamme sekä sisäistä että ulkoista viestintää”, Kevasta kerrotaan.
- Kyberturvallisuuskeskus voi antaa tukea kyberharjoituksien suunnitteluun ja toteuttamiseen.
- Tutustu: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberharjoittelu-paransi-kevan-valmiuksia-kohdata-tosielaman-uhkatilanteita

Sinustako arjen kybersankari? – Spoofy-mobiilipeli koululaisille

- Spoofy-mobiilipeli opettaa alakoululaisille hauskalla tavalla salasanoihin, yksityisyyteen ja netin käytöstapoihin liittyviä digitaalisen turvallisuuden perustaitoja sekä huijauksilta ja nettikiusaamiselta suojautumista

- CGI:n yhdessä Traficomin ja Valtion kehitysyhtiö Vaken toteuttaman Spoofy-pelin voi ladata ilmaiseksi Google Play -kaupasta ja Applen App Storesta
- **Hyvää kyberturvallista loppukesää!**

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)