Huhtikuu | 2019

#KYBERSÄÄ

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

TRAFICOM

Varoitus 02/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä varastetaan edelleen. Varoitus aiheesta on ollut voimassa kesästä 2018. Kyberturvallisuuskeskus julkaisi huhtikuun alussa oppaan Office 365 -tuotteiden tietoturvaominaisuuksista, joiden käyttöä suositellaan.

Hyökkääjät kirjautuvat käyttäjätileille ja seuraavat yritysten sähköpostiliikennettä. He pyrkivät saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia. Varastettuja tunnuksia käytetään erilaisiin laskutuspetoksiin.

Käyttäjätunnuksia ja salasanoja kalastellaan sähköpostitse ja huijaussivujen avulla. Yksi viimeaikainen menetelmä on ollut toimittaa kalastelulinkki pdf-liitetiedoston sisällä. Monivaiheinen tunnistaminen (MFA) voidaan myös ohittaa, jos Office 365 on asetettu tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).

Ajantasaisimmat tiedot varoituksesta: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Julkaisimme oppaan uhkan torjumiseksi: https://www.kyberturvallisuuskeskus.fi/fi/node/2532

TRAFICOM

Top 5 -kyberuhat

1

Edistyneemmät rikollisryhmät etsivät kohteikseen isoja organisaatioita, joiden toimintaa haittaamalla voidaan yrittää kiristää huomattavia summia rahaa.

2

Verkkoon liitetään laitteita ja palveluita, joiden tietoturvaa tai päivittämistä ei ole huomioitu ja suojaustoimet ovat puutteellisia.

3

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

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Tietoturvan laiminlyönnit altistavat esimerkiksi häiriöille.

5

Puutteellinen elinkaaren- ja lokienhallinta heikentää organisaatioiden kykyä havaita ja reagoida poikkeamiin.

Top 5 -kyberuhkiin nostetaan Kyberturvallisuuskeskuksen näkökulmasta merkittävimpiä pidemmän aikavälin ilmiöitä.

TRAFICOM

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Julkaistut Office 365-kovennus sekä Turvallisesti netissä -ohjeet ovat saaneet myönteisen vastaanoton.

2. Vaikka palvelunestohyökkäysten voimakkuudet ovat kasvaneet, niiden käytännön vaikuttavuus ei ole lisääntynyt.

3. Kansalaisten tietämys yksinkertaisista huijauksista ja kiristysviesteistä on parantunut, ja ne tunnistetaan aiempaa paremmin.

Tietoturvan kehitystarpeet

1. Tietomurtoja ja –vuotoja tehdään paljon päivittämättömien järjestelmien kautta. Niiden tietoturvasta ei huolehdita.

2. Vakavista tietomurroista toipuminen vaatii ennakkosuunnittelua ja harjoittelua. Esimerkkinä varmuuskopioiden käyttö.

3. Järjestelmien ylläpitovastuut ja ylläpitosuunnitelmat ovat usein puutteellisia, joka johtaa pitkällä aikavälillä tietoturvaongelmiin.

TRAFICOM

Kybersää, huhtikuu 2019

Verkkojen toimivuus

- Toimivuushäiriöitä oli erityisesti TV- ja radiopalveluissa.
- Telia korjasi Dot-liittymiensä tilausprosessin haavoittuvuuden.
- Eduskuntavaalien tuloksesta viestimiseen tarkoitettuun verkkopalveluun tehtiin palvelunestohyökkäys

Tietomurrot & -vuodot

- Vilkas tietomurtojen kuukausi.
- Julkiseen verkkoon kytketyt päivittämättömät sovelluspalvelimet ovat usein tietomurtojen kohteena.

Haittaohjelmat & haavoittuvuudet

- Paljon kriittisiä haavoittuvuuksia päivitettäväksi.
- Yritysten web-alustat kohteena.
- Ransomware-toiminta kehittyy edelleen.

Vakoilu

- Yhdysvaltojen NSA:n verkkovakoilutyökaluja epäillään päätyneen kiinalaisryhmän haltuun.
- Lääkeyhtiö Bayer kertoi olleensa vakoilun kohteena.
- Venäläisen Turla-ryhmän vakoilutyökalu mahdollistaa sähköpostipalvelimen vakoilun.

Huijaukset ja kalastelut

- Julkaisimme oppaan Office 365 -kalastelulta suojautumiseen.
- Tekstiviestejä käytetään entistä enemmän huijausten ja tilausansojen levittämiseen.

IoT ja automaatio

- Uusi menetelmä haittaohjelmien havaitsemiseen sulautetuissa järjestelmistä perustuu virrankulutuksen vertailuun.

TRAFICOM


Verkkojen
toimivuus
TRAFICOM

Verkkojen toimivuus

Huhtikuussa toimivuushäiriöitä oli erityisesti TV- ja radiopalveluissa

- Huhtikuussa oli 8 merkittävää toimivuushäiriötä.
- Niistä viisi koski antenni-, kaapeli- tai IP-TV-palvelua tai radiopalvelua.

Alkuvuoden aikana on ollut keskimäärin enemmän toimivuushäiriöitä kuin vuonna 2018

Telia korjasi Dot-liittymiensä tilausprosessissa olleen haavoittuvuuden

- Kun Dot-liittymä otetaan käyttöön, muualla käytössä oleva kännykkänumero siirretään uuteen liittymään.
- Liittymän pystyi tilaamaan, jos tiesi tiettyjä henkilötietoja puhelinnumeron aiemmasta haltijasta. Haavoittuvuuden löysi tietoturvatutkija, eikä sitä tiedetä hyödynnetyn.
- Nyt tilaajat todennetaan vahvaa sähköistä tunnistamista käyttäen.
- https://www.is.fi/digitoday/tietoturva/art-2000006075402.html

Eduskuntavaalien tuloksesta viestimiseen tarkoitettuun verkkopalveluun tehtiin palvelunestohyökkäys

- Palvelunestohyökkäyksen kohteena oleva palvelu ei liity äänestämiseen eikä ääntenlaskentaan, vaan tuloksesta raportoimiseen. Hyökkäyksen avulla ei voitu vaikuttaa vaalien tulokseen.
- Viranomaiset ovat varautuneet tämänkaltaisiin epäiltyihin kyberrikoksiin vaalien yhteydessä.

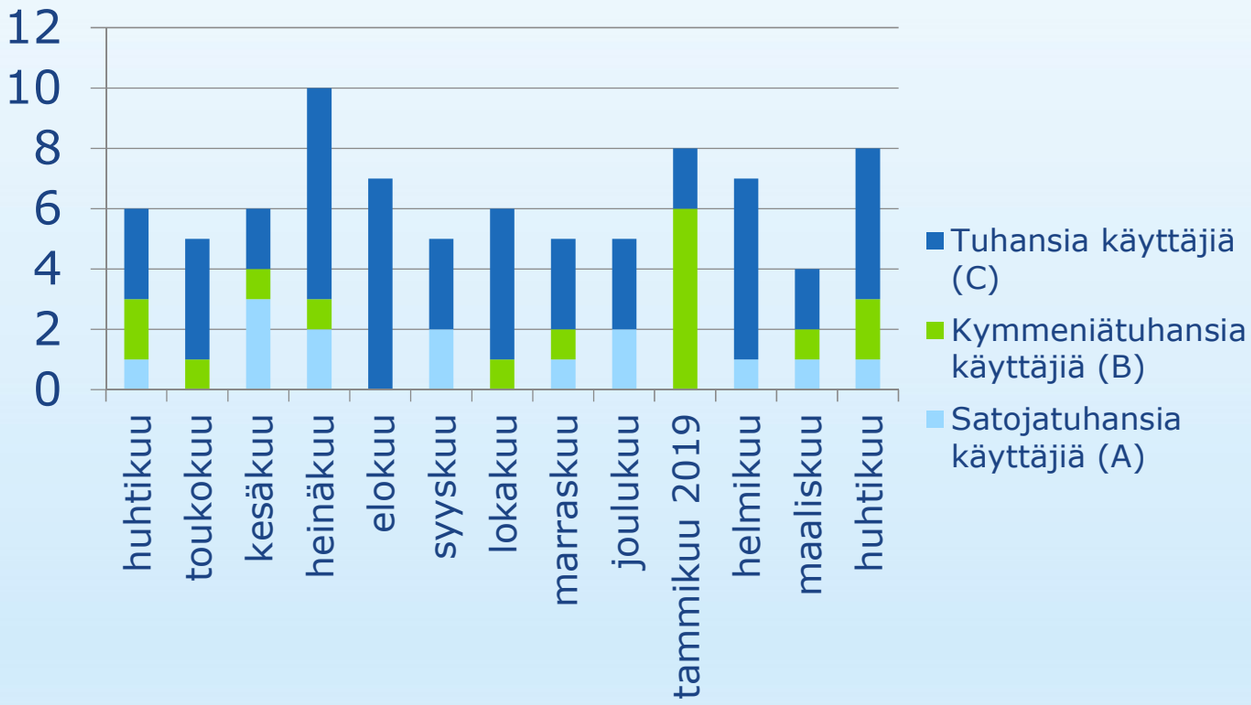
Haavoittuvia palvelimia on murrettu ja sinne asetettu haittaohjelma, jolla voi tehdä muun muassa palvelunestohyökkäyksiä

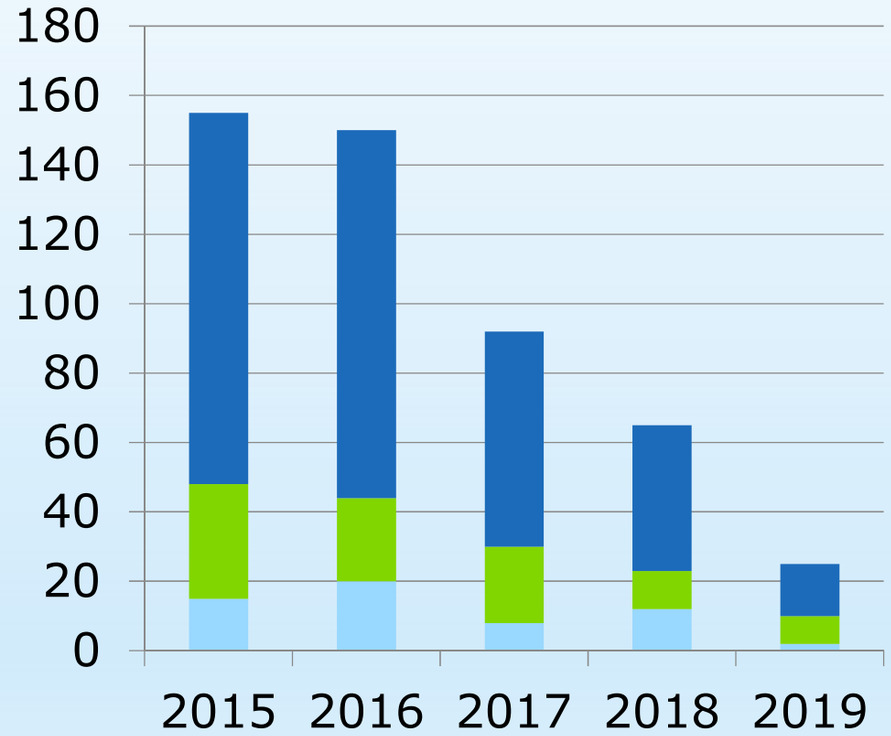
- Verkkopalvelimelle asennetun haittaohjelman avulla voidaan saada aikaiseksi merkittäviä liikennevolyymejä.

Palvelunestohyökkäysten voimakkuudet ovat kasvaneet, ja yli 10 Gbit/s:n hyökkäyksiä nähdään Suomessa jo päivittäin

- Hyökkäysten aiheuttamista häiriöistä ei kuitenkaan ole raportoitu Kyberturvallisuuskeskukselle tavanomaista enempää. Tämä saattaa johtua parantuneista suojautumiskeinoista.

Merkittävien toimivuushäiriöiden määrä





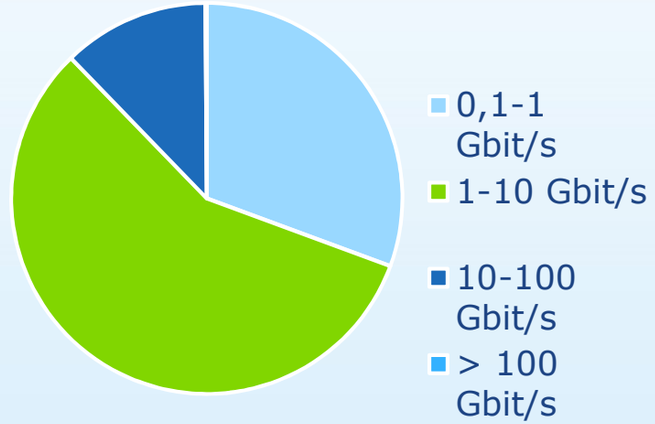
Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200, ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

Palvelunestohyökkäykset ja niillä uhkailu

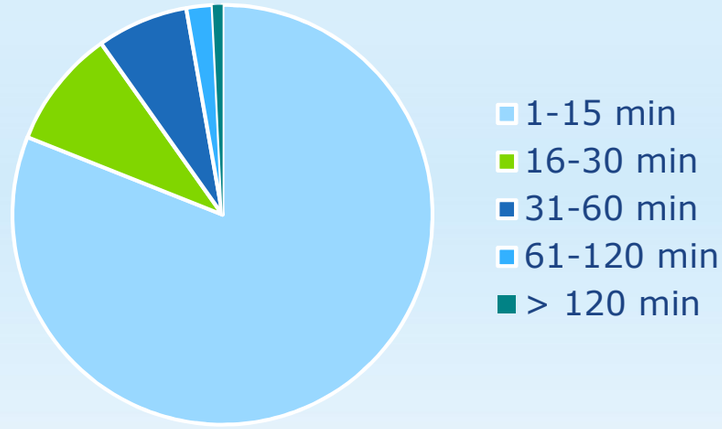
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (80 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 10 Gbit/s hyökkäysten osuus on kasvanut vuoden 2018 puolivälistä alkaen, ja niitä nähdään Suomessa jo päivittäin.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska saamme ilmoituksia vain murto-osasta tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q1:	2018/Q4:	2018/Q3:
n. 162 Gbit/s (kesto 9 min)	n. 45 Gbit/s (kesto 6 min)	n. 89 Gbit/s (kesto 30 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.


Tietomurrot & -vuodot
TRAFICOM

Tietomurrot & -vuodot

- **Selvitimme laajaa kansainvälistä tietomurtokampanjaa, joiden uhrien joukossa myös suomalaisia**
  - Selvitystyössä olemme olleet yhteydessä yli kahdeksaankymmeneen maahan.
- **Atlassian Confluence –ohjelmistossa haavoittuvuus, jota käytettiin hyväksi tietomurroissa**
  - Tiedossamme on useita suomalaisuhreja, joiden palvelimia on käytetty kryptovaluutan louhimiseen. Ulkomailla haltuun saatuja palvelimia on käytetty myös palvelunestohyökkäysten toteuttamiseen.
- **Microsoft Office 365 –tietomurtoja tapahtuu yhä säännöllisesti**
  - Tietomurroissa ja –vuodoissa käytetään hyväksi tietojenkalastelulla saatuja tunnuksia.
  - Murtojen tavoitteena on taloudellisen edun saamiseen esimerkiksi valelaskujen avulla.
- **Suuri eurooppalainen IT-palvelutalo joutui tietomurron ja kiristyksen kohteeksi**
  - Hyökkääjä kiristi palvelutaloa haltuunsa saamien asiakastietojen paljastuksella ja julkaisi ainakin osan haltuunsa saamista tiedoista, koska kiristykseen ei suostuttu.

- **Vilkas kuukausi tietomurto ja –vuototapausten tutkinnassa**
  - Yhden tietomurron yhteydessä joitakin luottokorttitietoja joutui hyökkääjään haltuun.

Big Game Hunting

Maailmalla on yleistynyt ilmiö, jota kutsutaan nimellä *Big Game Hunting* (suom. kirj. ”suurriistan metsästys”). Toiminnalle ominaista on, että rikollinen toimija tunkeutuu organisaation järjestelmiin, levittäytyy organisaation verkossa ja käynnistää kiristyshaittaohjelman siten, että tiedostojen salaus haittaa organisaation toimintaa vakavasti tai jopa lamauttaa sen.

Salauksen jälkeen organisaatiolta kiristetään lunnaita salauksen purkamiseksi. Kohteita yhdistää perinteisesti hyvä maksukyky tai toiminnan jatkumisen aikakriittisyys. Esimerkiksi tammikuussa kohteiksi joutui ranskalainen Altran ja maaliskuussa norjalainen Norsk Hydro. Yhdysvalloissa useat kunnat ja aluehallinnot ovat myös olleet kohteina.

Samaan ilmiöön liittyy useita eri kiristyshaittaohjelmia, kuten LockerGoga, SamSam, Ryuk ja MegaCortex. Organisaation järjestelmiin tunkeutuminen puolestaan voi alun perin tapahtua käyttäen hyväksi haavoittuvia verkkoon avoimia palveluita, haitallisilla sähköpostien liitetiedostoilla tai esimerkiksi onnistuneen tietojenkalastelun avulla.

Ilmiö on hyvä huomioida riskiarvioissa. Muun muassa murtautumisen ja levittäytymisen havaitsemiseksi on hyvä varmistua siitä, että jo hankittujen ratkaisujen tietoturvaominaisuuksia hyödynnetään kattavasti. Varautumista suunnitellessa on syytä huomioida myös, että rikolliset voivat pyrkiä vaikeuttamaan toipumista salaamalla myös esimerkiksi varmuuskopiot ja käyttövaltuushallinnan.

Suojautumisohjeita tietomurtojen varalta

- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.

Haittaohjelmat & haavoittuvuudet

TRAFICOM

Kyberturvallisuuskeskuksen haittaohjelmahavainnot

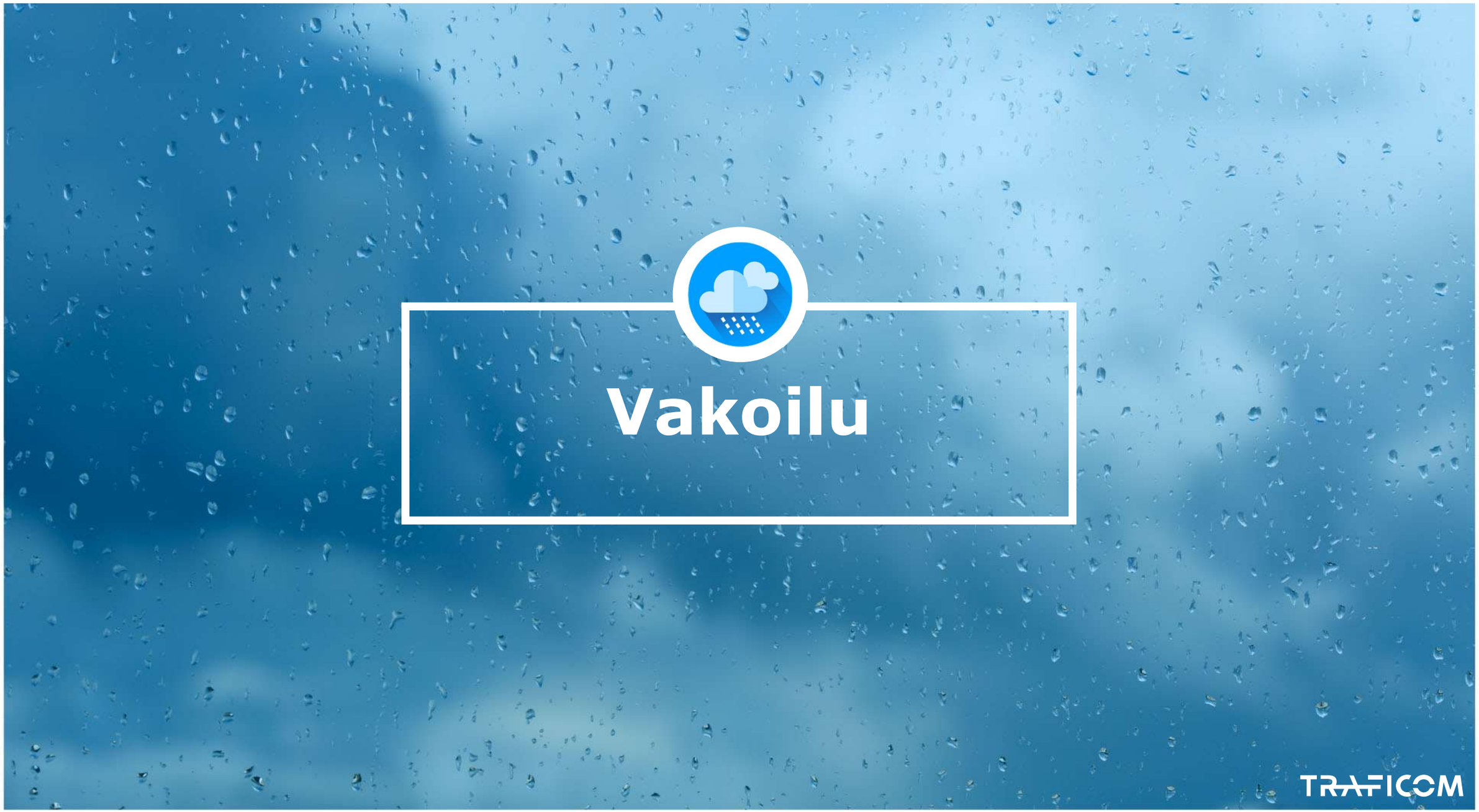
Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista.	
Kiristyshaittaohjelmat	Kiristyshaittaohjelmista on muutamia havaintoja.	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia on raportoitu muutamia tapauksia.	
Louhijat	Louhijoita levitetty haavoittuvuuksien avulla palvelimille.	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista on joitain havaintoja.	

Haittaohjelmat

- Edelleen runsaasti haitallista sisältöä sähköpostiliitteissä ja jaetuissa linkeissä. Kasvavana ilmiönä haitallista sisältöä sisältävät roskapostiviestit.
- Yrityskäytössä olevia web-alustoja, jotka ovat usein avoinna internetiin, on haavoittuvuuksia hyödyntämällä käytetty mm. kryptominingiin, palvelunestohyökkäyksiin sekä kiristyksiin (ks. haavoittuvuudet).

Haavoittuvuudet

- Microsoftin Edge- ja Internet Explorer -selaimissa korjaamaton XSS-haavoittuvuus (Haavoittuvuus 7/2019).
- Huhtikuun aikana on jälleen julkaistu paljon päivityksiä kriittisiin haavoittuvuuksiin eri ohjelmistoissa.
- WPA3-protokollasta löydettyjen haavoittuvuuksien vuoksi hyökkääjä voi saada haltuunsa salatuiksi tarkoitettuja tietoja (DragonBlood).
- VPN-istuntokohteiset evästeet ovat usein suojaamattomina järjestelmässä. Evästeiden avulla hyökkääjä voisi kaapata VPN-istunnon.
- Oraclelta ylimääräinen päivitys Weblogic-ohjelmiston haavaan.
- Atlassian Confluencen haavoittuvuutta käytetään aktiivisesti hyväksi usein samalla toimintamallilla kuin Weblogic-haavoittuvuutta (TTN-artikkeli 13.04.2019).
- Broadcom WiFi –piirisarjan ajureissa useita haavoittuvuuksia, joita hyödyntämällä voidaan pahimmillaan suorittaa koodia kohdejärjestelmässä.


Vakoilu
TRAFICOM

Vakoilutilanteessa ajankohtaista

NSA:n työkaluja päätyi kiinalaisten haltuun

Yhdysvaltojen NSA:n verkkovakoilutyökaluja epäillään päätyneen ulkopuolisten haltuun jo ennen niin kutsutun Shadow Broker -ryhmän tekemiä paljastuksia. Tietoturvayhtiö Symantecin mukaan on todennäköistä, että kiinalaiset saivat työkaluja haltuunsa NSA:n hyökättyä kiinalaisten järjestelmiin ja hyödynsivät niitä itse.

Lääkeyhtiö Bayer vakoilun kohteena

Saksalainen lääkeyhtiö Bayer kertoi huhtikuun alussa tunkeutumisesta järjestelmiinsä. Perusteellisen tutkinnan päätteeksi yhtiö oli poistanut hyökkääjän järjestelmistään maaliskuun lopussa. Yhtiön mukaan hyökkäystyyppi viittaa kiinalaisryhmä Wicked Pandaan. Hyökkäyksessä käytettiin kehittynyttä WINNTI-haittaohjelmaa.

Venäläinen Turla-ryhmä vakoili sähköpostipalvelimia

Vakoilukampanjassa hyödynnettiin erityisesti Microsoft Exchange -sähköpostipalvelimia varten räätälöityä LightNeuron-vakoilutyökalua, joka mahdollisti Exchange-palvelimen hallinnan takaoven avulla ja mm. sähköpostien muuntamisen.


Huijaukset ja kalastelut
TRAFICOM

Huijaukset ja kalastelut

- **Varoitus Office 365 -palvelun tietomurroista tietojenkalastelun avulla on yhä voimassa**
  - Käyttäjätunnusten kalastelu on jälleen kasvussa ja sen avulla tehdään uusia tietomurtoja lähes päivittäin.
  - Kyberturvallisuuskeskus julkisti kattavan ohjeen Office 365 -ympäristön suojaamiseen: https://www.kyberturvallisuuskeskus.fi/fi/node/2532
  - Tiedostonjakopalveluita käytetään levittämään vilpillisiä PDF-tiedostoja ja linkkejä kalastelusivuille.
- **Tekstiviestejä käytetään entistä enemmän myös pankkihuijauksiin**
  - Pankkitunnuksia kalastellaan tekstiviesteillä ja yritetään ohittaa vahva tunnistautuminen.
- **Huhtikuussa erityisesti postin nimissä lähetetyt saapumisilmoitukset ovat johtaneet tilausansoihin**
  - Myös Lidlin, Prisman ja Yliopiston apteekin nimillä lähetettiin tilausansoihin johtavia tekstiviestejä.
- **Pornokiristyshuijaukset ovat jälleen lisääntyneet**
  - Huijausviestejä on lähetetty niin yksityisiin kuin organisaatioiden sähköposteihin, ja niissä huijari väittää saaneensa uhrin koneen haltuunsa ja kiristää lunnaita muka tallentamastaan arkaluonteisesta materiaalista.
  - Lähettäjänä voi näkyä viestin vastaanottaja itse. Lähettäjäkenttä on helppo väärentää.
  - Kiristysviesti on liitetty mukaan kuvana, jotta tekstipohjainen suodatin ei huomaa sitä.
  - Kaikki kiristysviestissä väitetty on huijausta. Mitään lunnaita ei ole syytä maksaa.

Office 365-huijauksen vaiheet

1. Rikollinen lähettää tietojenkalastelu-viestin sähköpostitse.

2. Vastaanottaja lukee viestin ja klikkaa siinä olevaa linkkiä.

3. Linkin päässä onkin tietojen kalastelusivu, joka pyytää syöttämään käyttäjätunnuksen ja salasanan.

4. Kalastelusivulle syötetyt tunnukset menevätkin rikollisen tietoon.

5. Haltuunsa saamilla tunnuksilla rikollinen pääsee seuraamaan yrityksen sisäistä liikennettä.

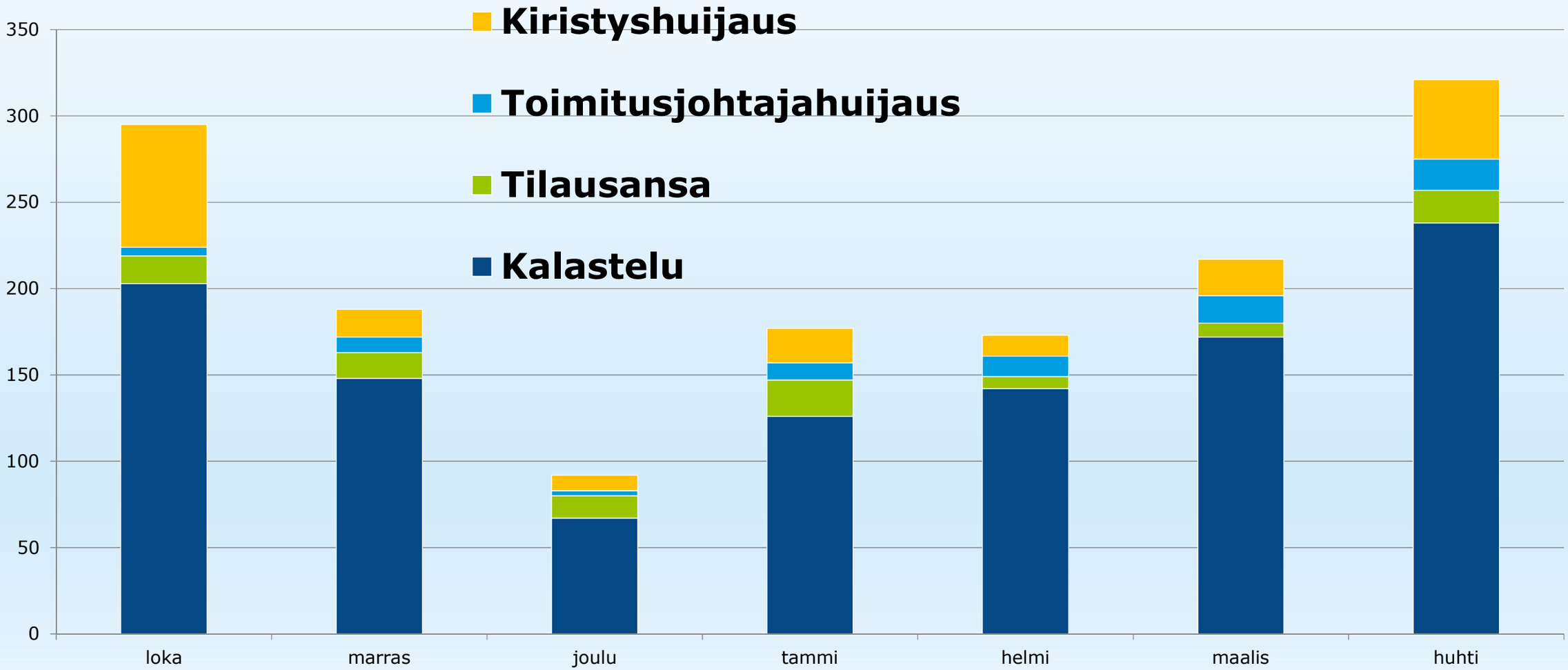
6. Nyt rikollinen pääsee lukemaan esim. laskutusliikennettä.

ASIAKAS

7. ”Anteeksi, edellinen lasku oli väärä. TÄSSÄ on oikea lasku.”, kirjoittaa rikollinen ja korjaa potin taskuunsa.

TRAFICOM

Käsiteltyjä huijaustapauksia 2018/10–2019/04



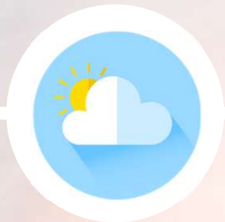
IoT ja automaatio

TRAFICOM

IoT ja automaatio

- Tutkijat ovat kehittäneet uuden tekniikan tunnistaa sulautetuissa järjestelmissä olevia haittaohjelmia. Uusi menetelmä vertaa järjestelmän virrankulutusta tunnettuun, puhtaan järjestelmän virran kulutukseen.

- On löydetty vähintään kaksi miljoonaa IoT-laitetta, joissa on käytössä tietty P2P-teknologia iLnkP2P ja jotka ovat haavoittuvuuksia hyödyntämällä otettavissa hallintaan. Korjausta ei ole saatavilla, siksi esimerkiksi haavoittuvia kameroita voidaan käyttää käyttäjien vakoiluun.



Tietoturva-alan kehitys

TRAFICOM

Kyberasioihin liittyvää uutisointia maailmalta

Virossa järjestettiin huhtikuussa laaja kyberharjoitus

- Virossa järjestettiin laaja kolmepäiväinen 'Locked Shields’ -kyberturvallisuusharjoitus.
- Kyseessä on vuosittainen harjoitus, jonka järjestäjänä toimii NATOn kyberpuolustuskeskus. Harjoituksessa oli pelaavia organisaatioita 23 eri maasta.
- Harjoitusympäristöön kuuluu noin 4000 virtualisoitua järjestelmää ja yli 2500 tietoturvapoikkeamaa.
- Harjoitukseen osallistui arviolta yli tuhat asiantuntijaa.

Kiinaa epäillään teollisuusvakoilusta Ruotsissa

- Ruotsin kokonaismaanpuolustuksen tutkimuslaitos yhdistää raportissaan Ruotsiin kohdistuvan teollisuusvakoiluun Kiinaan.
- Kyseessä on Dagens Nyheterin mukaan ensimmäinen kerta, kun ruotsalaisviranomaiset yhdistävät julkisesti Kiinan valtionhallinnon teollisuusvakoiluun.
- Raportin mukaan Ruotsi on erityisen haavoittuvainen teollisuusvakoilulle mm. avoimen talouden ja digitalisaation korkean asteen vuoksi.

Kyberpoikkeamien trendeissä muutoksia aiempaan verrattuna

- Maailmalla kybertapahtumien määrä on laskenut viime vuonna toissavuoteen nähden, mutta viime vuonna nähdyt hyökkäykset ovat olleet kehittyneempiä.
- Hyökkäyksiä myös kohdennetaan paremmin. Esimerkiksi kriittisiä toimijoita vastaan tehdyissä kyberhyökkäyksissä nähtiin merkittävä nousu edellisvuoteen verrattuna.
- Lähitulevaisuudessa 5G:n mahdollistama kehitys kasvattaa myös hyökkäyspinta-alaa, ja lisää yhteiskunnan haavoittuvuutta.

TRAFICOM

TRAFICOM

Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi

TRAFICOM