Missä Suomen kyberturvallisuudessa mennään - Kyberturvallisuuskeskuksen näkökulma

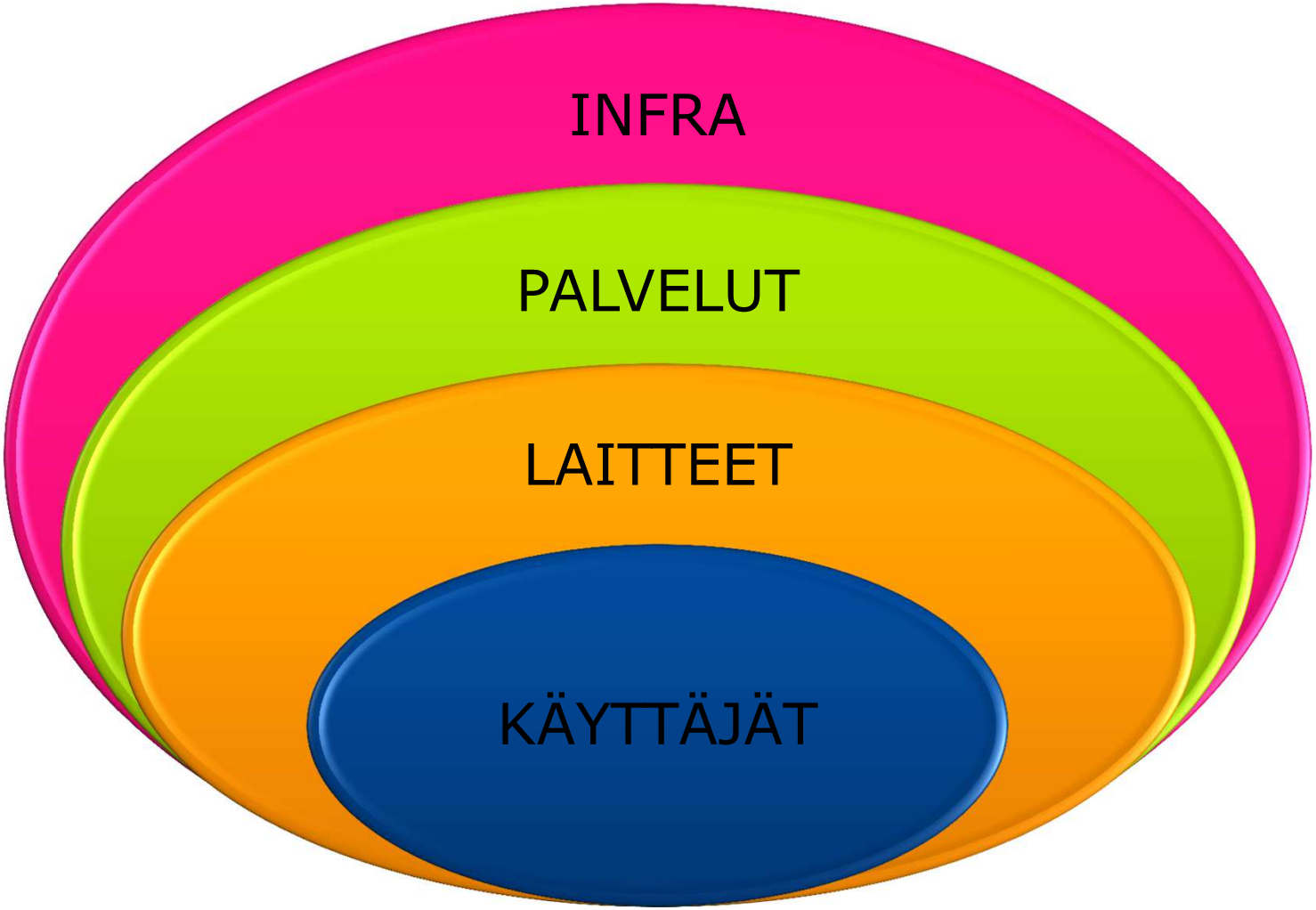
Viestintävirasto
Kyberturvallisuuskeskus

Apulaisjohtaja Jarkko Saarimäki

20.11.2015


Jatkuva tavoitettavuus ja läsnäolo verkossa
Tieto digitalisoituu
Langattomuuden merkitys kasvaa
Kyberuhkat kehittyvät
Häiriöiden merkitys kasvaa
Riippuvuus muista lisääntyy
Tilanne-kuvan tarve korostuu
Yhteistyö on elinehto
Verkottunut maail
ttajatottumusten
utos
Kyberturvallisuuden merkitys kasvaa

Luottamus sähköisten palveluiden edellytyksenä



Viestintäpalveluiden toimintavarmuus

Viestintäverkkojen toimivuus

Vuosi 2014

A-luokka: 14 kpl

B-luokka: 43 kpl

C-luokka: 97 kpl

D-luokka: 104 905 kpl (1H)

Vuosi 2015

(tammi–lokakuu)

A-luokka: 10 kpl

B-luokka: 27 kpl

C-luokka: 91 kpl

D-luokka: (alkuvuoden 2015 tilannetta ei määräysten siirtymäajan vuoksi tilastoida)

Viestintäverkot ovat toimineet hyvin. Lokakuussa Valio-myrskyn aiheuttamista merkittävistä häiriöistä toivuttiin nopeasti.

Puhelimien salakuuntelu

TV & RADIO | POSTI | KYBERTURVALLISUUS | TAAJUU

Etusivu › Kyberturvallisuus › Tietoturva nyt! ›
Puheluiden yhteydessä kuuluvat häiriöäänet ovat tavallisia

Tietoturva nyt!

Puheluiden yhteydessä kuuluvat häiriöäänet ovat tavallisia

25.09.2015 klo 10:50

Matkapuhelimen salakuunteluun ja sijainnin seuraamiseen on useita menetelmiä. Viestintäviraston Kyberturvallisuuskeskus muistuttaa ettei matkapuhelimessa pidä käsitellä arkaluonteisia asioita.

Uutisoinnissa esiin nostetut matkapuhelinverkkoon liittyvät tietoturvauhat ovat olleet tiedossa jo vuosia. Matkapuhelimen salakuuntelun ja sijainnin seuraamiseen on useita menetelmiä kuten valetukiasemat ja haittaohjelmat. Puheluita voi yrittää salakuunnella muun muassa matkapuhelimen ja tukiaseman välisestä radioliikenteestä, operaattorien välisestä liikenteestä tai päätelaitteelle ujutetun haittaohjelman avulla. Tunnetut radiotiehen liittyvät turvallisuusuhat liittyvät kuitenkin vain vanhempaan 2G-verkkoon. 3G- ja 4G-yhteyksien turvaamisessa käytetään uudempia salausmenetelmiä.

Viestintävirasto ohjaa ja valvoo teleyritysten toimintaa muun muassa määräyksin ja tarkastuksin. Matkapuhelinoperaattorien on huolehdittava verkkojensa ja palveluidensa tietoturvasta. Kyberturvallisuuskeskus seuraa aktiivisesti matkapuhelintekniikkaan liittyvien uhkien ja riskien kehitystä.

1. käyttäjän sijainnin selvittäminen ja seuraaminen
2. puheluiden salakuuntelu ja nauhoittaminen
3. radioliikenteessä käytetyn salauksen purkaminen
4. liittymän irtikytkeminen matkapuhelinverkosta eli viestinnän estäminen ja
5. liittymän laskutuksen manipuloiminen petoksellisesti.

Käyttäjällä ei ole mahdollisuutta havaita väärinkäytöksiä omasta päätelaitteestaan.

toteuttaa laaja-alaisesti, vaan se rajoittuu tarkasti valittuihin kohteisiin.

Matkapuhelinta voi käyttää normaaliin viestintään

Matkaviestinpalveluita voi käyttää turvallisesti tavalliseen viestintään. Kannattaa kuitenkin miettiä, vaatiiko viestin sisältö suojausta. On syytä esimerkiksi pohtia, kuka voisi hyötyä sisällöstä tai onko oman sijainnin paljastuminen kriittistä. Matkaviestinverkko ei sovellu arkaluontoisten asioiden

Kanerva ja Haglund epäilevät joutuneensa salakuuntelun kohteiksi – "Emme elä lintukodossa"

POLITIIKKA 24.9.2015 19:23 Päivitetty: 24.9.2015 21:16

Kalle Koponen HELSINGIN SANOMAT
Juho-Pekka Pekonen HELSINGIN SANOMAT
Tommi Hannula HELSINGIN SANOMAT

MARKUS JOKELA / HS JA VESA MOILANEN / LEHTIKUVA

ntinen ulkoministeri Ilkka Kanerva ja entinen puolustusministeri Carl Haglund.

443
13

Kansanedustaja **Ilkka Kanerva** (kok) ja Rkp:n puheenjohtaja **Carl Haglund** epäilevät, että heidän puhelimiaan on salakuunneltu. Asiasta kertoi ensimmäisenä **Hufvudstadsbladet verkkosivuillaan**.

Euroopan turvallisuus- ja yhteistyöjärjestön Etyjin parlamentaarisen yleiskokouksen

Matkaviestin ei sovellu arkaluontoisen tiedon käsittelyyn ilman asianmukaisia suojauksia

UHKIA

- Salakuuntelu
- Sijainnin selvitys
- Puhelun/yhteyden estäminen
- Tietojen urkinta/muutos

KEINOJA

- Älypuhelinten haittaohjelmat
- Valetukiasemat
- SIM-korttien väärinkäytökset
- Verkon merkinantoliikenteen väärinkäytökset (SS7)

- Kyberturvallisuuskeskus ylläpitää tilannekuvaa uhkista yhteistyössä viranomaisten ja teleyritysten kanssa
- **Arkaluonteisia tietoja suositellaan viestittäväksi salattuna lähettäjältä vastaanottajalle**

Palvelunestohyökkäyksiä riittää

VERKKOHYÖKKÄYKSET

"Tilannetta verkossa seurataan" - Laaja hyökkäys saatiin taltutettua

Talouselämä | 18.11. 11:53

JAA ARTIKKELI

Häiriöt useiden valtionhallinnon viranomaisten verkkopalveluissa saatu hallintaan. Häiriöt aiheutti palveluntarjoajalla havaittu palvelunestohyökkäys.

Nyt tilannetta seurataan. Häiriöt konesalista tuotetuissa palveluissa alkoivat maanantaina ja niitä oli vielä keskiviikkona kello 9.15–9.30. Sen jälkeen tilanne saatiin rauhoittumaan.

Hyökkäys ei kohdistunut konesalista tuotettuihin viranomaispalveluihin, mutta se vaikutti palveluntoimittajan palvelukykyyn ja siten myös alla lueteltuihin viranomaispalveluihin, jotka tuotetaan samasta konesalista.

Häiriö aiheutti hetkittäisiä katkoksia seuraavien verkkopalvelujen käyttöön:

- Aluehallintovirastot: www.avi.fi
- ELY-keskukset: www.ely-keskus.fi
- rakennerahastot.fi
- Yritys-suomi
- Oma Yritys-suomi

Taloussanomat 18.11.2015

Yritysvakoilu

Kohdistetut hyökkäykset ovat pitkäkestoisia ja niiden kehitys on jatkuvaa

17.09.2015 klo 09:39 - *Päivitetty 17.09.2015 klo 15:24*

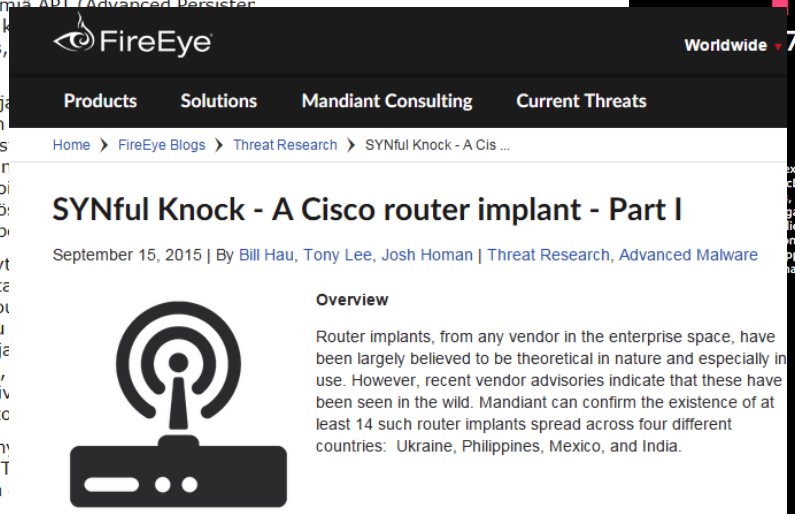
Kohdistettuihin hyökkäyksiin käytettäviä työkaluja kehitetään pitkäjänteisesti ja ammattimaisesti. Hyökkäyksissä käytettyjä työkaluja ja menetelmiä tiedetään ylläpidetyn useita vuosia. Kampanjoissa käytetyt työkalut myös päivittyvät havaitsemisen vaikeuttamiseksi ja mahdollistaen uusimpien haavoittuvuuksien hyväksikäyttämisen.

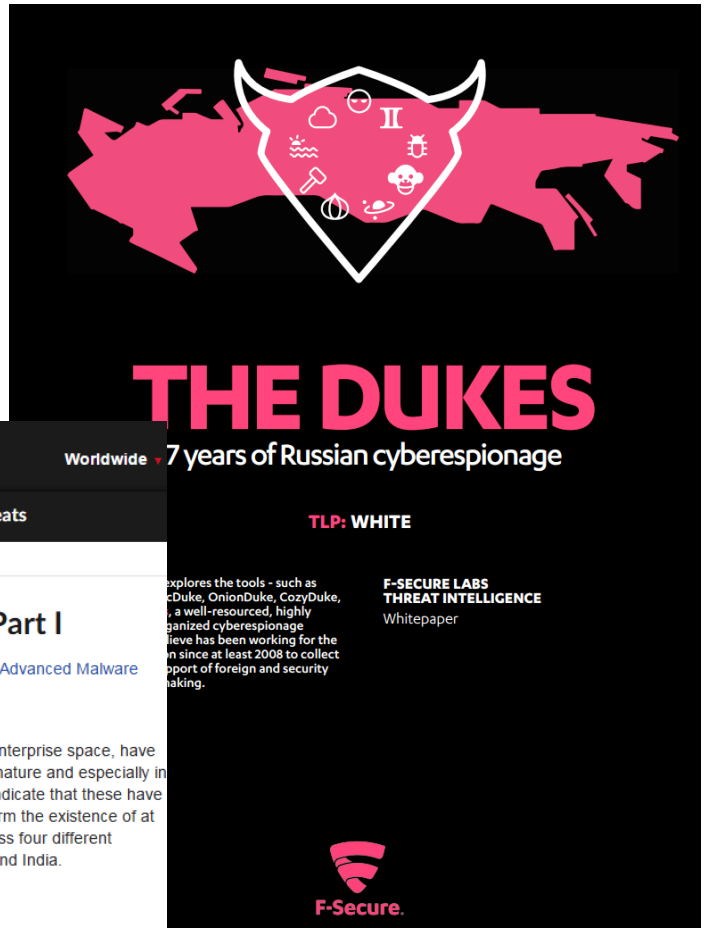
Kohdistettuja haittaohjelmahyökkäyksiä on tunnistettu jo noin vuosikymmene
ajan. Kohdistetuista hyökkäyksistä käytetään termiä APT (Advanced Persister
Threat). Kohdistettu hyökkäys tai APT-kampanja k
tiettyyn rajattuun kohteeseen, joka voi olla yritys,
valtionhallinnon organisaatio.

Hyökkääjällä on usein kohdeorganisaatiosta tietoj
haittaohjelma on mahdollista saada organisaation
käytettyjä menetelmiä ovat esimerkiksi sähköpos
lähetetty saastutettu dokumentti, joka sisällöltään
epäilyksiä. Sähköpostin aihe voi liittyä juuri uutisoi
olevaan konferenssiin. Lähettäjätiedot voivat myös
Tällaisesta hyökkäyksestä käytetään nimitystä sp

Hyökkääjä voi myös houkutella organisaation käyt
saastutetulla verkkosivustolla, joka tarjoilee haitta
organisaatiosta saapuville käyttäjille. Tällainen hou
hole) voi olla esimerkiksi konferenssin verkkosivu
kohdistuvissa hyökkäyksissä tietyn laitevalmistaja
kohdistuvissa hyökkäyksissä tiedetään tapauksia,
laitteistolle valmistajan verkkosivuilla tarjottu päiv
saastutettu ja saatu näin järjestelmään ohjelmisto

Hyökkäävän tahon tarkoituksena kohdistetuissa hy
organisaation kriittisen tiedon haltuun saaminen. T
organisaatiosta huomaamattomasti ja operaation





Tietojen kalastelu

Kyberturvallisuus

Varoitukset
Tietoturva nyt!
Haavoittuvuudet
Palveluiden turvallinen käyttö
Laitteen turvallinen käyttö
Sähköinen tunnistaminen ja allekirjoitus
Tietoturvallisuuden arviointilaitokset
Teleyritysten oikeudet ja velvollisuudet
Yhteisötilaajien oikeudet ja velvollisuudet
Kyberturvallisuuskeskuksen palvelut
Tietoturvaohjeet

Yhteystiedot

Viestintävirasto
Kyberturvallisuuskeskus

Viestintävirasto
Kyberturvallisuuskeskus
PL 313, 00181 Helsinki

- CERT-toiminto ›
- Haavoittuvuuskoordinointi ›
- NCSA-toiminto ›
- PRS-toiminto ›

- Salausavaimet ›
- Liity postituslistallemme! ›

Mediayhteydenotot puhelimitse:
0295 390 248

Etusivu › Kyberturvallisuus › Tietoturva nyt! ›
Pankkitunnusten kalastelukampanja jälleen aktiivinen
Tietoturva nyt!

Pankkitunnusten kalastelukampanj jälleen aktiivinen

14.09.2015 klo 10:27 - *Päivitetty 14.09.2015 klo 16:42*

Viime päivien aikana Kyberturvallisuuskeskuksen tietoon on tullut y kymmenen tietojenkalastelusivua Osuuspankin, Nordean ja Aktian nimissä.

Nordean, Osuuspankin ja Aktian nimissä lähetetyissä tietojenkalasteluviestei ilmoitetaan "verkkopankin päättymisestä" ja pyydetään vastaanottajia kirjautumaan sähköpostiviestissä olevan linkin kautta verkkopankkiin. Linkki ohjaa väärennetylle sivustolle, jossa pyritään varastamaan pankkitunnukset.

Erään ilmoituksen mukaan tietojenkalasteluviestin lähettämisen jälkeen vastaanottajalle on myös soitettu ja kysytty tunnuslukulistalta tiettyä tunnuslukua.

Päivitetty 14.9.2015 klo 16:30:

Tietojenkalastelua havaittu myös Danske Bankin nimissä.

Esimerkki tietojenkalasteluviestistä:

Hyvä asiakas,

Huomaa, että verkkopankin on päättymässä. Tämän palvelun jatkuvan keskeytyksettä napsauttamalla alla olevaa kuvaketta manuaalisesti päivittää tilisi.

klikkaa tästä <http://[huijaussivuston osoite]/Nordeaupdate/nordea.fi.html>

Suoritettuanne tilinne päivitystä varten annetut ohjeet, asiointitilinne sähköinen käyttöönotto palautuu automaattisesti eikä teidän tarvitse tehdä muita lisätoimenpiteitä.
Kun automaattinen päivitys on valmis saatte puhelun verkkopankin palveluist vastaavalta osastolta joka antaa teille lisätietoja päivityksestä.

Etusivu › Kyberturvallisuus › Tietoturva nyt! › Huijausviestejä Iltalehden nimissä

Tietoturva nyt!

Huijausviestejä Iltalehden nimissä

18.09.2015 klo 09:48

Iltalehden nimissä houkutellaan käyttäjiä ostamaan Apple Watch yhdellä eurolla. Kyseessä on huijaussivusto, jonka tarkoituksena on kerätä käyttäjien tietoja.

OP

» Tekstiversio » På svenska » In English

Hae

Henkilöasiakkaat | Yritysasiakkaat | OP Ryhmä

Etusivu | Edut | Tilit ja maksut | Kortit | Lainat | Säästöt ja sijoitukset | Vakuutukset ja vahingot | Asunnot

Henkilöasiakkaat > Tietoturva > Verkkopankkitunnuksia kalastellaan huijaussähköpostilla

- Verkkorikollisuus
- Huolehdi laitteesi turvallisuudesta
- OP-verkkopalveluiden turvaominaisuudet
- Apua ongelmatilanteissa

Verkkopankkitunnuksia kalastellaan huijaussähköpostilla

23.7.2015

Liikkeellä on OPn nimissä lähetetty huijaussähköposti, jonka avulla kalastellaan yritysasiakkaiden verkkopankkitunnuksia. Mikäli saat huijausviestin, älä vastaa viestiin tai klikkaa viestissä olevia linkkejä äläkä luovuta verkkopankkitunnuksiasi. Poista kaikki epäilyttävät viestit niitä avaamatta.

Huijausviestissä kerrotaan, että "Ilmoitamme teille, että haavoittuvuus on havaittu omassa verkkopankissa.
Jos haluat jatkaa käyttämällä palveluita, sinun tulee suorittaa päivityksen." ja ohjataan kirjautumaan sisään linkin kautta avautuvalla huijaussivustolla. Huijaussivusto muistuttaa Kassanhallintapalvelun sisäänkirjautumisnäkymää ja siinä pyydetään kirjautumaan verkkopalveluun käyttäjätunnuksella ja salasanalla.

Muistathan, että OP ei koskaan pyydä kirjautumaan verkkopalveluihin sähköpostissa tai tekstiviestissä olevan linkin kautta tai lähettämään henkilökohtaisia verkkopalvelutunnuksiasi, luottokortin tietoja tai henkilötunnusta sähköpostitse tai tekstiviestillä. Mikäli saat huijausviestin, älä vastaa viestiin tai klikkaa viestissä olevaa linkkiä.

Mikäli olet luovuttanut verkkopankkitunnuksesi huijaussivustolla, sulje välittömästi tunnuksesi soittamalla OP Yritys- ja maksuliikepalvelut 0100 05151 (arkisin kello 8-16:30, pvm/mpm) puhelinpalveluun. Puhelinpalvelun palvelualan ulkopuolella sulje tunnuksesi soittamalla verkkopalvelutunnusten sulkupalveluun +358 20 333 (24 h/vrk). Ilmoita tapahtuneesta myös puhelinpalveluun sen avauduttua.

Esimerkki huijaussähköpostista:

Lähettäjä: Osuuspankki Yritysasiakkaat <osuuinfo@bussinesosu.fi>
Päiväys: 23. heinäkuuta 2015 15.09.19 UTC+3
Vastaanottaja: [redacted]
Aihe: Paivitys - 009366

Lataa kuvat napsautt...

Hyvä Yritysasiakkaat,

Ilmoitamme teille, että haavoittuvuus on havaittu omassa verkkopankissa.
Jos haluat jatkaa käyttämällä palveluita, sinun tulee suorittaa päivityksen.

Kirjaudu Kassanhallintapalvelu .

Tietomurrot

Uhkat ja haitat

- **Laajentuminen muihin palveluihin ja vuosia kestävät vaikutukset**
  Yhdestä palvelusta varastettua ja kertaalleen vuodettua salasanaa voi hyödyntää myös muihin palveluihin murtautumisessa. Paljastunutta ja päivittämätöntä salasanaa voi hyödyntää vuosienkin kuluttua

- **Henkilötietojen hyödyntäminen verkon ulkopuolella**
  Päästään käsiksi sähköisen palvelun käytössä tarvittaviin tietoihin, kuten henkilötunnukseen, yhteystietoihin ja luottokorttinumeroihin. Tietoja voidaan hyödyntää esimerkiksi henkilöksi tekeytymisessä tai maksamisessa

Kyberturvallisuuskeskuksen toimet

Ennaltaehkäisy	•Tiedotus uusista murtomenetelmistä •Riskien selvittäminen ja ennakoiminen
Tekninen selvitys	• Uusi murto: Milloin, miten ja mitä tietoja? • Toteutustapa: ohjelmistot, haavoittuvuudet
Tiedottaminen	•Tieto murrosta tai sen uhasta ylläpitäjälle •Tarvittaessa käyttäjien toimenpideohjeet
Toipuminen	•Neuvonta ylläpitäjille korjaavista toimista •Yleistiedottaminen uhasta

Tietoturvapoikkeamat suomalaisissa verkoissa

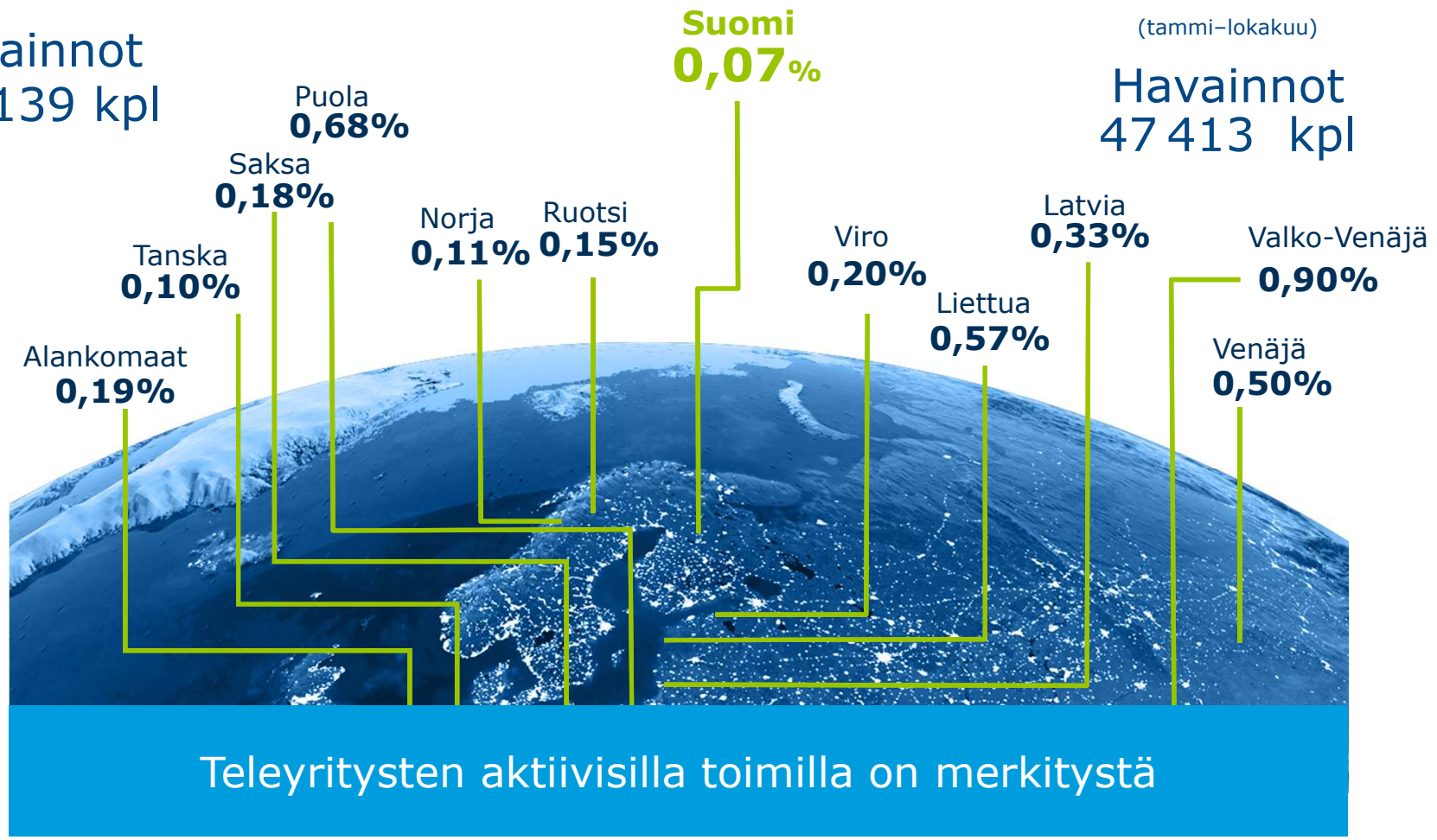
2014

Havainnot
204 139 kpl

2015

(tammi–lokakuu)

Havainnot
47 413 kpl



Teleyritysten aktiivisilla toimilla on merkitystä

TALOUS SANOMAT | Taloussanomat | It-viikko | Digitoday | Mobiiliversio

digitoday

Ohje | Hae

Etusivu | Uutiskirjeet | Toimitus | Pörssi | Mediakortti | RSS

UUTISLISTA | data | bisnes | mobiili | työ ja ura | tietoturva | tiede ja teknologia | viimpaimet | yhteiskunta | viihde | mielipide

Lue uutinen mobiilisivustolla

Tässä Suomen 10 yleisintä haittaohjelmaa

Kuva: © Kacper Pempel / Reuters

16.11.2015 13:50 Tietoturvayhtiö Check Point Software sijoittaa Suomen 12:nneksi verkkojen turvallisuudessa.

Tietoturvayhtiö Check Pointin mukaan maailman yleisin haittaohjelma lokakuussa oli *Conficker*-virus, joka edustaa noin viidennestä haittaohjelmahavainnoista. Haitakkeen tarkoitus on siirtää saastunut kone osaksi bottiverkkoa ja verkkorikollisten komentoon.

Rekisteröinti

Rekisteröidy Taloussanomiin. Saat käyttöösi uuden Oman seurannan ja räätälöitävän pörssinäkymän. Lue lisää ja rekisteröidy

Kirjaudu Taloussanomiin

Sähköpostiosoite | Salasana

Kirjaudu

Uusimmat uutiset

tietoturva | kaikki

Näihin kysymyksiin Isisin "mikrotuki" vastaa 19:59

Vaara Applen Sirissä: 30 sekuntia ja tietosi on viety 16:02

Nyt se alkaa: "Puhelimiin takaovet viranomaisille" 13:38

Uudenlainen bottiverkko leviää – ja tahkoaa 230 000 000 euroa kuukaudessa 12:51

Ministerin varoitus Britanniassa: Isis haluaa tappaa kyberiskuilla 17:17

10 faktaa Googlen Kuvat-sovelluksesta + 2, joita Google ei kertonut 16:16

Homokohun runtelema selainpomo: Nyt startupin ruorissa 16:00

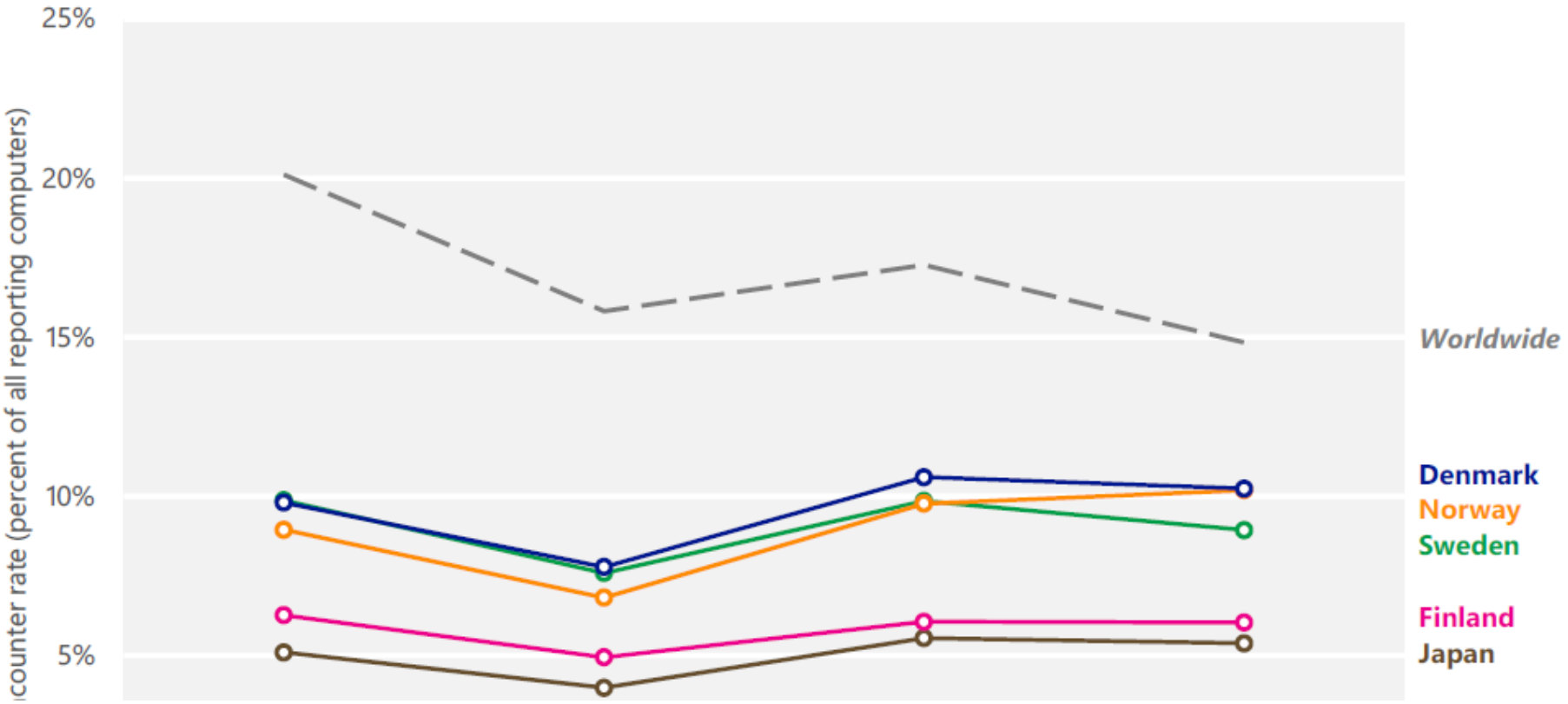
Facebookin kiistelty tekniikka: Pelastaa kohta lapsia? 14:40

Lisää

Microsoft Security Intelligence Report

Volume 19 | January through June, 2015

Figure 46. Trends for locations with low encounter rates in 1H15 (100,000 reporting computers minimum)



Yksityisyydensuojan merkitys ei ole vähenemässä

- Euroopan unionin tuomioistuin on antanut päätöksen ns. Schrems -asiassa ja todennut EU:n ja USA:n välisen Safe Harbor -järjestelyn pätemättömäksi.
- Artikla 29:n mukainen tietosuojavaltuutettujen työryhmä piti ylimääräisen kokouksen
  - » Yhdysvaltojen tiedustelutoiminta on EU-oikeuden vastaista
  - » Safe Harbourilla ei voida perustella tietojen siirtoa valvonnan piiriin
- Henkilötietojen siirto ei voi enää perustua Safe Harbouriin
  - » Mitä tarkoittaa viestinnän näkökulmasta?

Viestintävirasto
Kyberturvallisuuskeskus
Luottamusta lisäämässä