Ajankohtaista kyberturvallisuudesta

Johtaja Jarkko Saarimäki

Viestintävirasto
Kyberturvallisuuskeskus

Vuoden 2017 DESI-indeksissä Suomi sijoittuu kakkoseksi. Suomi on yksi maailman digitaalisesti edistyneimpiä maita. Sen tulokset ovat erittäin hyviä neljällä yhteensä viidestä osa-alueesta. Vahvuus näkyy erityisesti digitaalisissa taidoissa, joissa Suomi on selvästi edellä kaikkia muita jäsenvaltioita. Sillä on erittäin hyvät vahvuudet myös digitaalisissa julkisissa palveluissa.

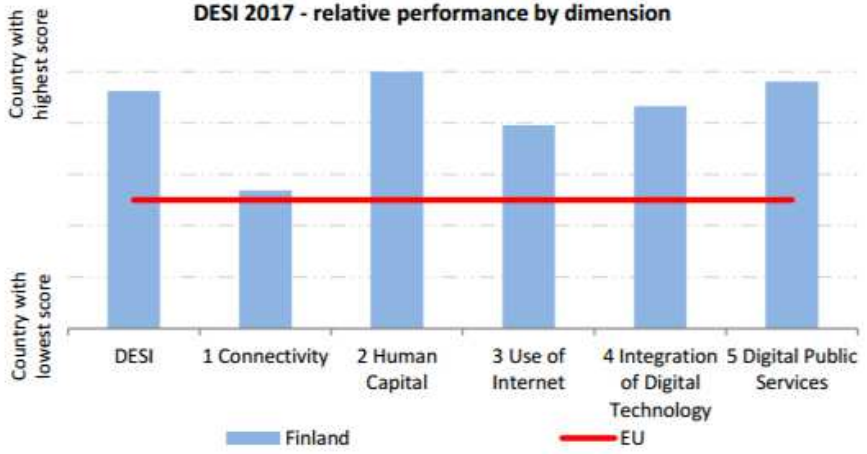
	Finland		Cluster	EU
	rank	score	score	score
DESI 2017	**2**	**0.68**	**0.63**	**0.52**
DESI 2016[1]	2	0.66	0.60	0.49

DESI (Digital Economy and Society Index) on yhdistetty indeksi, joka mittaa digitaalista kehitystä viidellä osa-alueella:

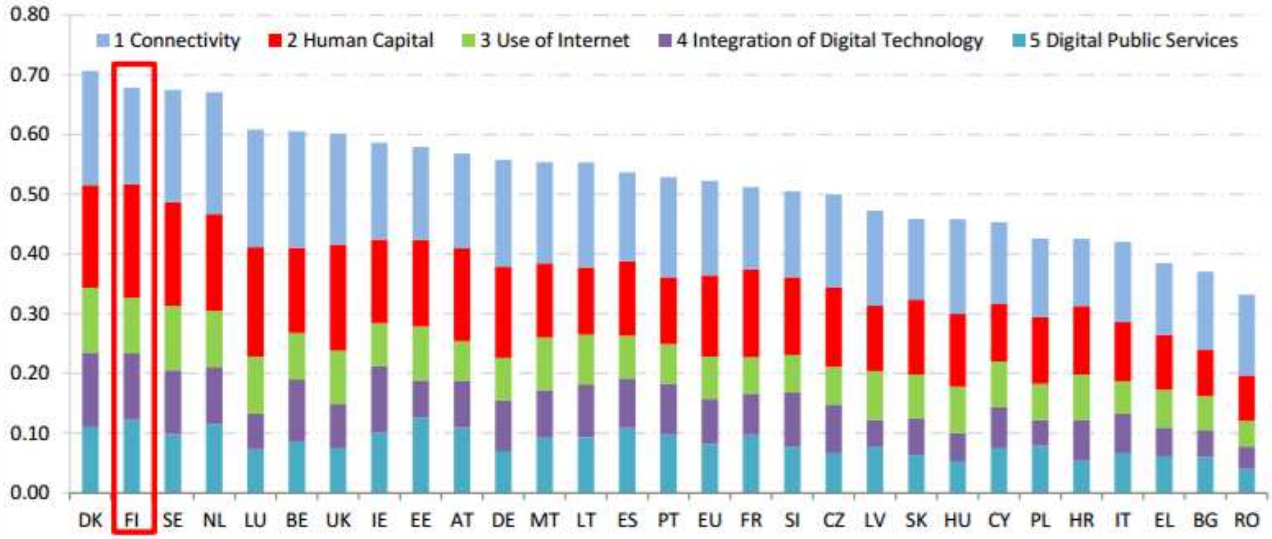
1 Siirtoyhteydet	Kiinteä laajakaista, mobiililaajakaista, laajakaistan nopeus ja hinnat
2 Inhimillinen pääoma	Internetin käyttö, digitaaliset perustaidot ja pitkälle viety digitaalinen osaaminen
3 Internetin käyttö	Sisällön, viestinnän ja verkkotoimintojen käyttö kansalaisten keskuudessa
4 Digitaaliteknologian integraatio	Yritysten digitalisointi ja sähköinen kaupankäynti
5 Julkishallinnon digitaaliset palvelut	Sähköiset viranomaispalvelut

Maaryhmitys: Suomi kuuluu huippusuoriutujien ryhmään.

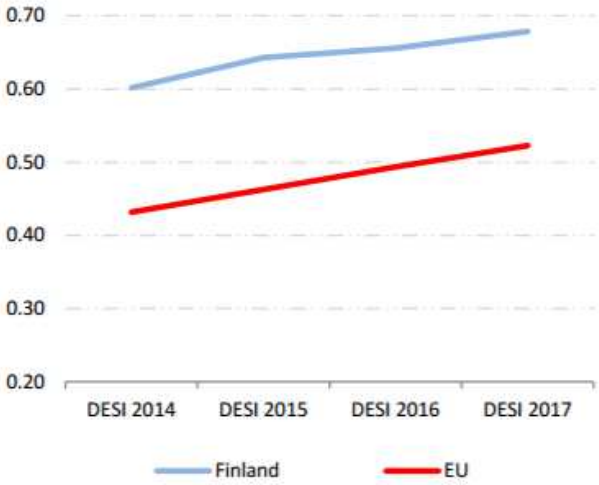
DESI 2017 - relative performance by dimension



Digital Economy and Society Index (DESI) 2017 ranking



DESI - evolution over time




BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

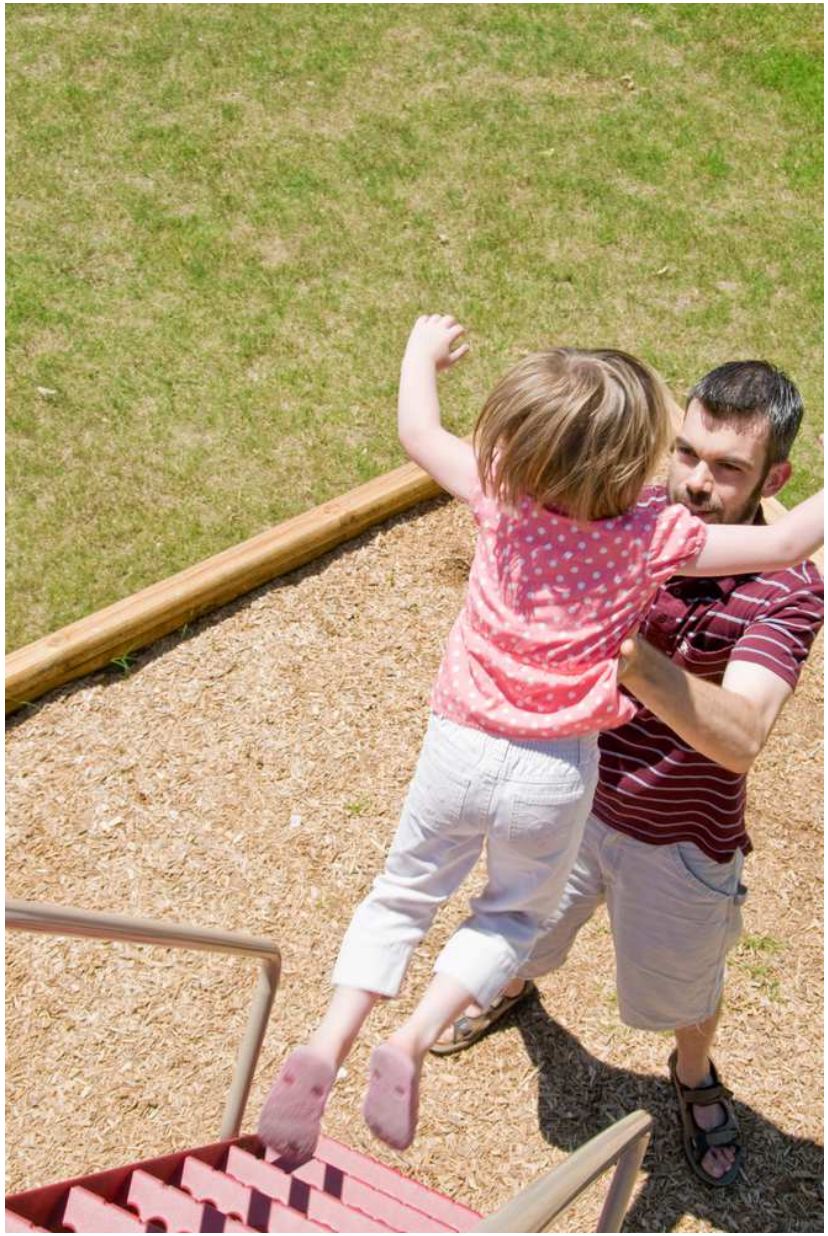
Jokaisen palasen tietoturvasta on huolehdittava

European Commission

http://ec.europa.eu/digital-agenda/en/towards-5g

Useita limittäisiä verkkoja, erilaisia laitteita ja uusia palveluita


OPPORTUNITY
JUST AHEAD



Turun Sanomat

SÄÄ Turku +2 °

Lue näköislehteä
Lähetä kuva
Jätä uutisvinkki

UUTISET PAIKALLISET URHEILU TSTV TS UUSIMMAT 24h PÄÄSIÄISMAKASIINI Hae

Juuri nyt Kahden rekan ja henkilöauton onnettomuus sulkee ajokaistan Säkylässä

Kaarinalaisvanhemmat vastustavat tablettiopetusta heikkotasoisena

Kaarinalaisvanhempien mielestä teknologiaharppaus kouluissa on mahalasku. E-kirjat ovat tylsiä ja lapset keskittyvät tableteilla mieluiten pelaamiseen.

Pirtta Salmi

Kaarinaan Piispanlähteen koulun ala-asteen matematiikan tunneilla ei käytetä enää kirjoja.

Uusimmat

9:57 Kahden rekan ja henkilöauton onnettomuus sulkee ajokaistan Säkylässä

9:57 Itsepäinen Suomi esittäytyy Vanhan kirjallisuuden päivillä

9:46 Kuluttajahinnat nousivat maaliskuussa 0,8 prosenttia, eniten kallistuivat polttonesteet ja sähkö

9:33 TS Vegebuumin konkarit

9:30 TS Vinttiteatteri valmistautuu Siniveriseen strategiaan

9:20 Kela muistuttaa opiskelijoita opintotukien palautuksista

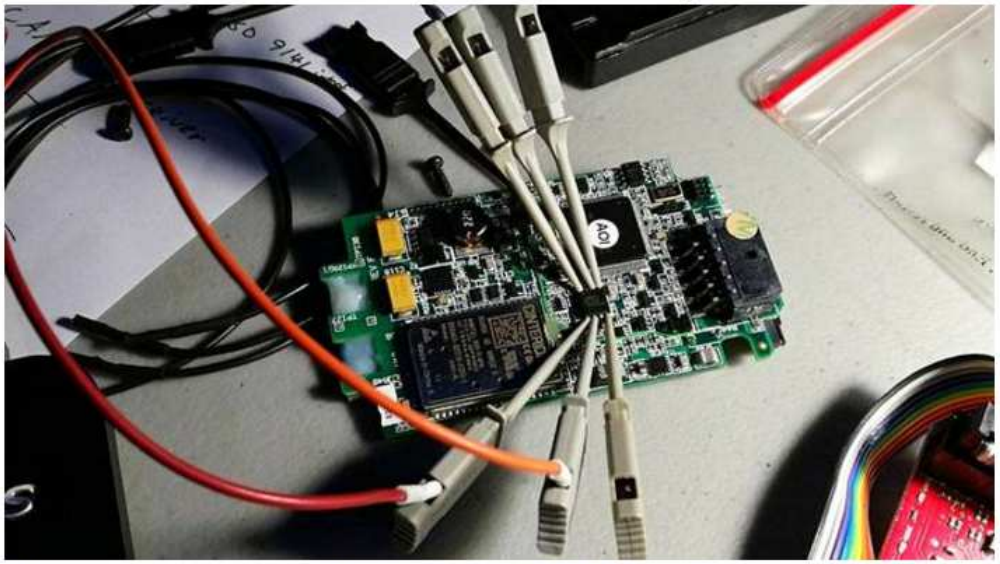
Lisää »

Luetuimmat

ILTA-SANOMAT TIETOTURVA

IS ETUSIVU | DIGITODAY | MOBIILI | TESTIT

Hakkerit mursivat autojen mustan laatikon – ”Asentaminen on tyhmä idea”



Mustan laatikon salaisuudet murrettiin piirikortin sisäistä tiedonsiirtoa kuuntelemalla.

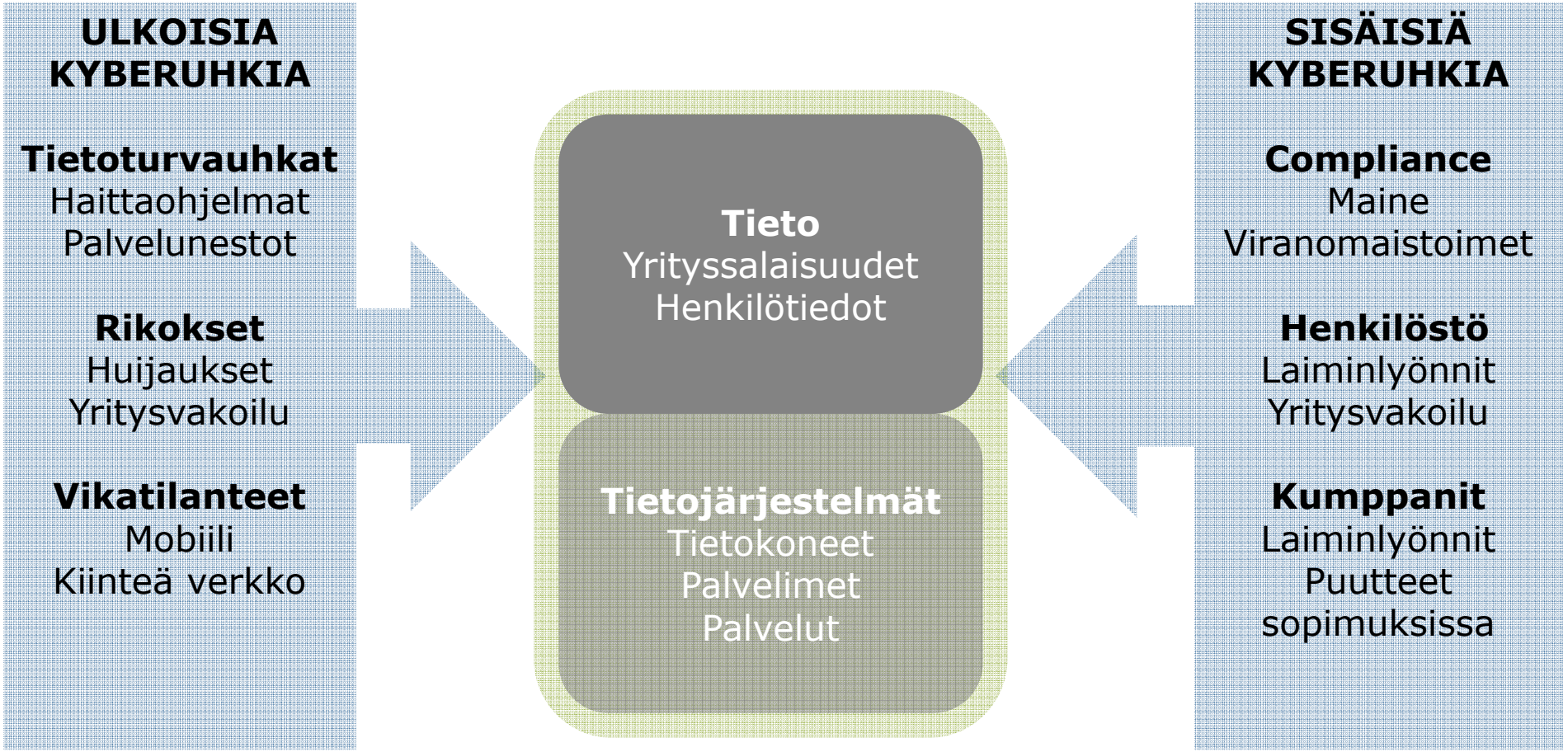
Julkaistu: 16.1. 7:26

Jaa | Twiittaa | Sähköposti

Autojen seurannassa käytetyn mustan laatikon salat paljastuivat hakkereille Disobey-hakkeritapahtumassa viime viikolla.

Digitaalinen maailma voi olla uhka fyysiselle maailmalle

Kyberuhkat


ULKOISIA KYBERUHKIA
Tietoturvauhkat
Haittaohjelmat
Palvelunestot
Rikokset
Huijaukset
Yritysvakoilu
Vikatilanteet
Mobiili
Kiinteä verkko
Tieto
Yrityssalaisuudet
Henkilötiedot
Tietojärjestelmät
Tietokoneet
Palvelimet
Palvelut
SISÄISIÄ KYBERUHKIA
Compliance
Maine
Viranomaistoimet
Henkilöstö
Laiminlyönnit
Yritysvakoilu
Kumppanit
Laiminlyönnit
Puutteet
sopimuksissa

HAKTIVISTIT

VERKKORIKOLLISET

VAKOOJAT

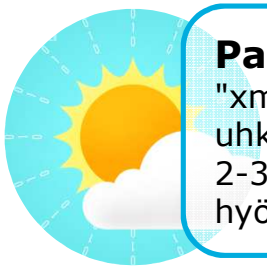
?

TERRORISTIT

#kybersää

Aktiivista huijausta ja runsaasti kalastelua

Vakoilu
APT28-ryhmä aktiivinen.
Sekä Suojelupoliisin että Viron CERT:n vuosiraporteissa uusia tietoja APT-toimijoista.



Palvelunestot
"xmr-squad" –niminen ryhmittymä uhkaili suomalaisia yrityksiä vaatien 2-3 bitcoinia, jotta he eivät toteuta hyökkäystä.

Huijaukset & kalastelut
Eri pankkien ja Applen nimissä runsasta kalastelua joka viikko.
Tilausansat yleistyneet.

Haittaohjelmat & haavoittuvuudet
Kyberrikolliset hyödyntävät valtiolliselta taholta vuotanutta DoublePulsar-haavoittuvuutta haittaohjelmien levityksessä.

Verkkojen toimivuus
Ei merkittäviä viestintäpalveluiden häiriöitä vuonna 2017.
Satunnaisia ja lyhyitä televisio- ja radioverkon häiriöitä.

IoT
BrickerBot-haittaohjelma tuhoaa haavoittuvien IoT-laitteiden ohjelmistot tehden ne käyttökelvottomiksi.

Vika- ja häiriötilanteet

Viestintävirasto
Kyberturvallisuuskeskus

Viestintäpalveluiden toimintavarmuus

Etusivu › Kyberturvallisuus › Tietoturva nyt! ›
Soneran 2G-verkossa koko maan kattava häiriö - vika korjattu

Tietoturva nyt!

Soneran 2G-verkossa koko maan kattava häiriö - vika korjattu

28.11.2016 klo 15:12 - *Päivitetty 28.11.2016 klo 23:40*

Soneran 2G-verkon häiriö vaikuttaa palveluihin koko maassa. Häiriö on alkanut kello 12:14 ja sen korjauksen arvioidaan valmistuvan klo 16:00 mennessä. Vika on korjattu.

Päivitys 28.11.2016 klo 22:40: Vika on korjattu n. klo 22:45.

Katkoksia Digitan TV- ja radiojakelussa

09.11.2016 klo 19:08

Digitan jakelemissa TV-ja radiolähetyksissä on katkoksia Pohjois-Suomessa Lapissa ja Itä-Suomessa Kuopion alueella.

Digitan jakelemissa TV- ja radiopalveluissa on häiriöitä isossa osassa Pohjois- ja Itä-Suomea. Syynä on siirtotien kaapelivika. Osa palveluista on saatu palautettua. Korjaustyöt ovat käynnissä.

Kotimaa 27.11.2014 klo 17:04 | päivitetty 28.11.2014 klo 9:32

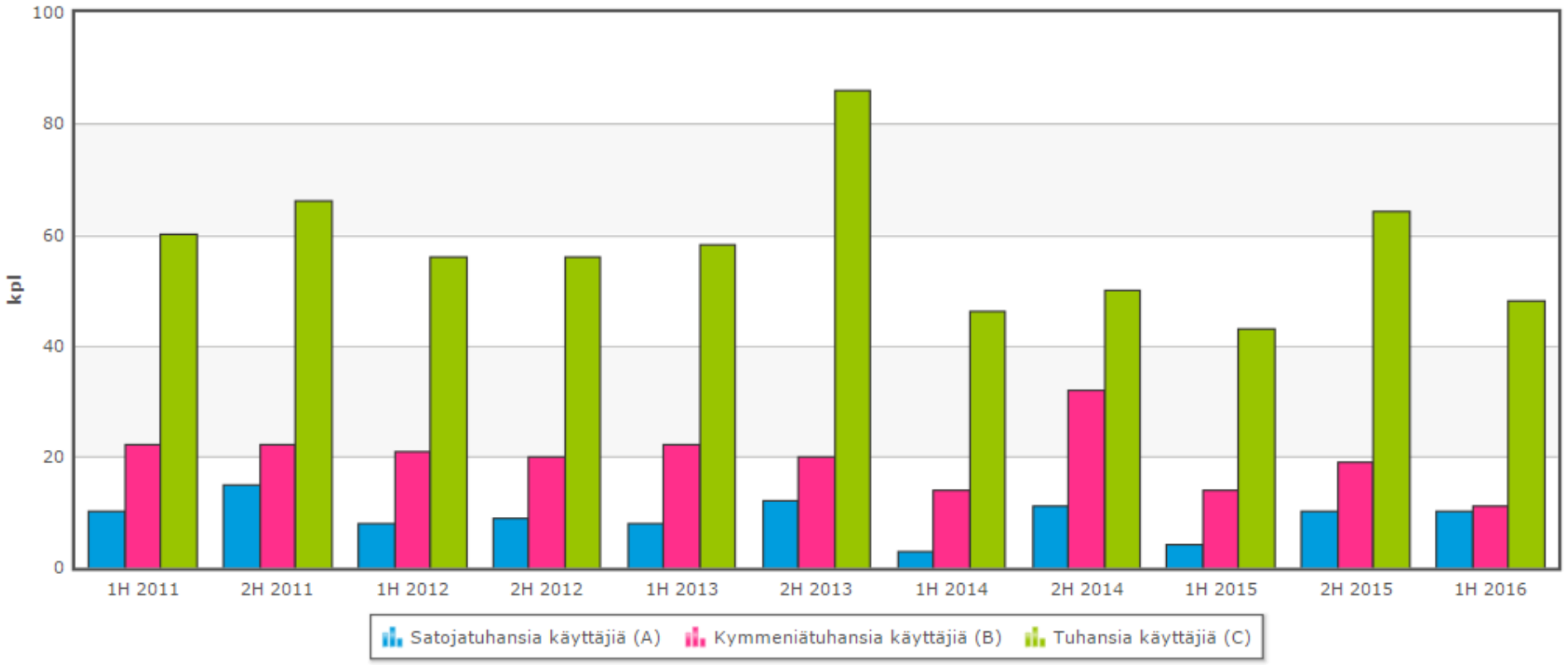
Kaivuri katkaisi sekä Elisan tietoverkkokaapelin että varayhteyden

Viestintäviraston mukaan Elisan eilisen tietoverkkoyhteyden häiriön aiheutti sekä varsinaisen kuitukaapelin että varakaapelin katkeaminen kaivinkoneen kauhaisussa samanaikaisesti. Kaapelit oli vedetty liian lähelle toisiaan.

Suosittele 696 henkilöä suosittelee tätä. Rekisteröidy ja näe, mitä kaverisi suosittelevat.

johtokeskuksessa. Kuva: Sami Halinen / Lehtikuva

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokan toimivuushäiriöt. Niitä on vuosittain 150–200. Pienempiä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 245 000–350 000 kappaletta vuodessa.

yle UUTISET

Etusivu Tuoreimmat Urheilu Sää | Kotimaa Ulkomaat Talous Politiikka Kulttuuri Kolumnit

Sydänpotilas hengenvaarassa teho-osastolla – kirurgia ei voitu Soneran heikon mobiiliverkon takia tavoittaa HUS:ssa

Helsingin ja Uudenmaan sairaanhoitopiiri vaihtoi mobiililiittymänsä keväällä Soneraan. Vanhan 2G-verkon heikon signaalin takia sairaalassa on toistuvasti oltu potilasturvallisuutta vaarantavissa tilanteissa, koska yhteydenotot eivät ole menneet läpi.

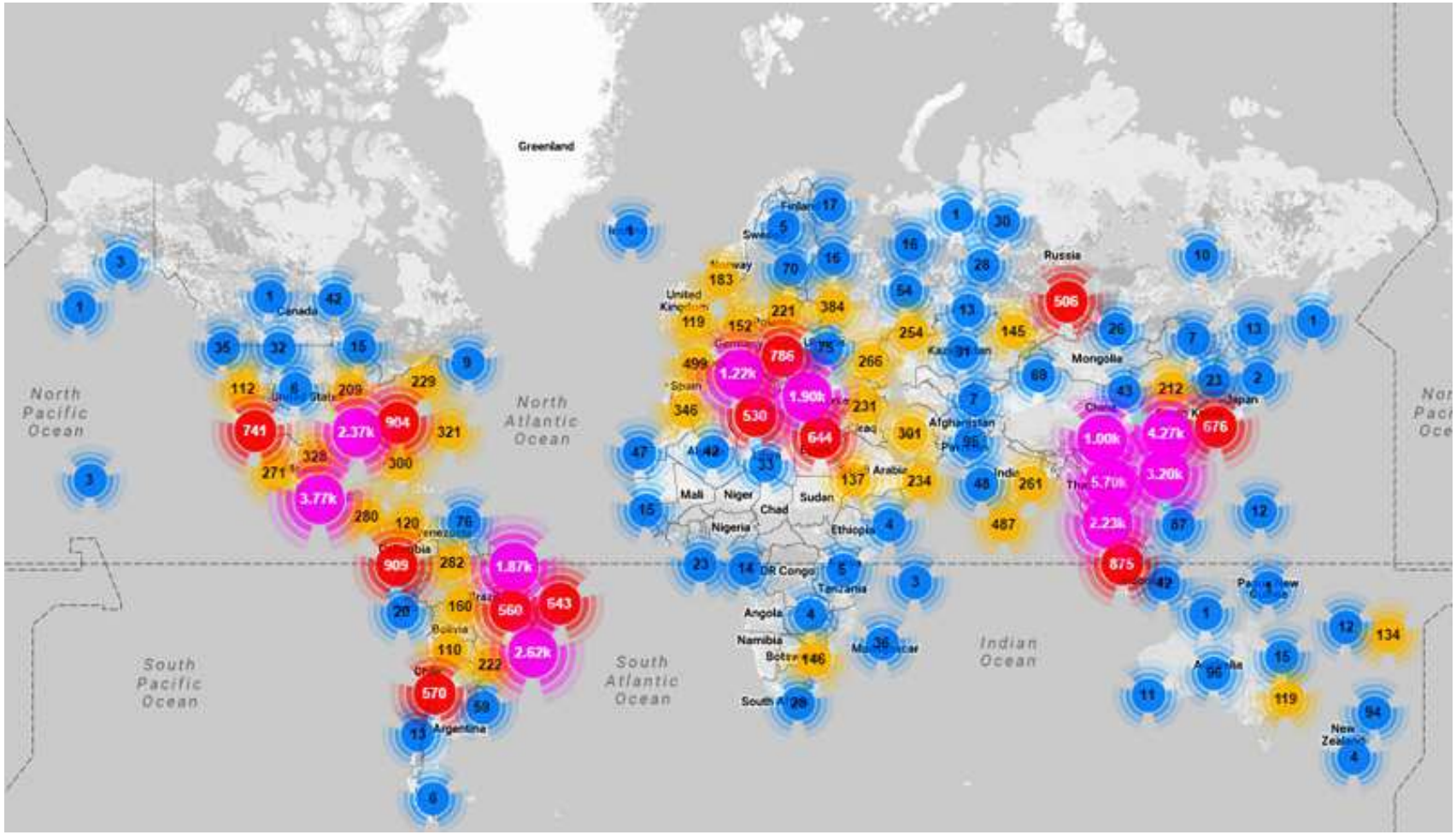
Kotimaa 8.6.2016 klo 08:05 | päivitetty 3.2.2017 klo 14:38

Kyberuhkat

Viestintävirasto
Kyberturvallisuuskeskus

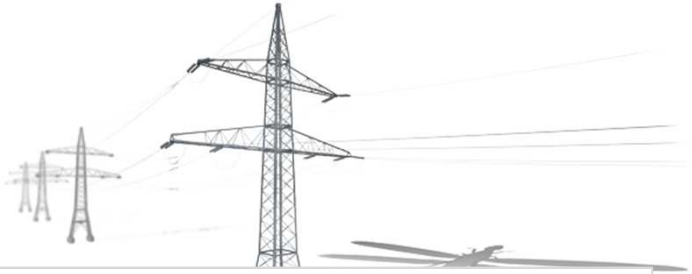
IoT-laitteet tulivat koteihin, tietoisuus riskeistä ei tullut samassa paketissa

Palvelunestohyökkäys yli 600 Gbit/s! IoT-bottiverkko MIRAI



Verkkovakoilun anatomia

Case Ukraina APT 2015



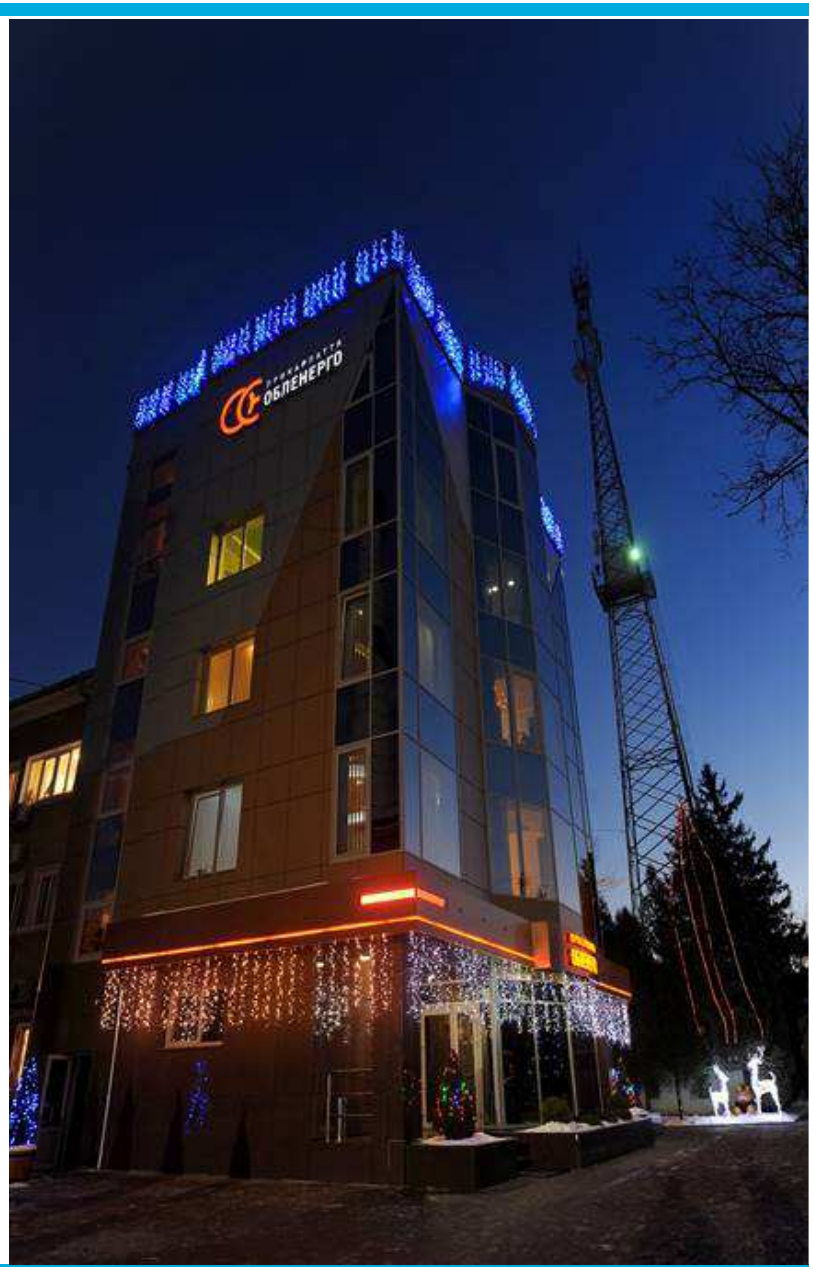
- Kohteena ukrainalaiset energiayhtiöt
  - *Kohdistettu hyökkäys energiayhtiöihin 23.12.2015, valmistelut alkaneet keväällä 2015*
- Kyseessä on ensimmäinen julkisuuteen tullut kyberhyökkäys, joka aiheutti sähkökatkoksia.
- Tunkeutumisissa käytettiin kyberrikollistenkin käyttämiä tavanomaisia keinoja
  - Haitallisen makron sisältämä Microsoft Office–tiedosto lähetettiin verkon ylläpitäjille.
    - Liitteen avaaminen latasi käyttäjän koneelle BlackEnergy 3 -haittaohjelman
- Hyökkääjällä ollut suuret resurssit ja paljon aikaa hyökkäyksen huolelliseen valmisteluun.
    - Hyökkäykseen valmistauduttu ainakin yli 6kk
    - Epäilyttävästä liikenteestä ilmoituksia ko. yrityksille, mutta ei ole reagoitu.

Ukrainalaisiin energiayhtiöihin kohdistettu hyökkäys katkaisi sähköt sadoiltatuhansilta asiakkailta joulukuussa. Katkokset kestivät useita tunteja. Palauttavat toimenpiteet tehtiin manuaalisesti. Lopullinen palautuminen kesti kuukausia mm. epäkuntoon saatettujen laitteiden uusimisen vuoksi.

Lähde:
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Vaikutukset:

- Kohdistui onnistuneesti kolmeen energiayhtiöön
- 30 sähköasemaa pimentyi (7kpl 110kV, 23kpl 35kV)
- 230 000 taloutta ilman sähköjä
- Sähkökatkos ~3h
- Laitteiden palautus ja korjaus vei kokonaisuudessaan kuukausia



Kohdistetun hyökkäyksen vaiheet

Macronin kampanjaa vastaan laaja tietomurto - Sähköposteja ja kirjanpitoa vuodettu nettiin

Tiedostot vuodettiin perjantaina ennen puoltayötä, vain hetkeä ennen presidentinvaalien huipennusta.

ULKOMAAT 06.05. 08.06

CAROLINE BLUMBERG

Emmanuel Macron on joutunut tietomurron kohteeksi.

LUETUIMMAT

NYT | Päivä | Viikko

1. Mies eli 10 vuotta salaa kahden naisen kanssa – Kun kaksoiselämä paljastui naisille, tapahtui rikos
2. Kun Armi sai siivet: Lue itkemättä Matti Kuuselan kertomus oman koiran kauniista kuolemasta
3. Tamperelaismies meni ulos aamukahville – käsittämätön näky odotti naapuritalon päädyssä
4. 52-vuotias nainen ikuisti hätkähdyttävän näyn autotien laidalla – harva pääsee näkemään koskaan
5. Harva tuntee erityislapsen äidin huolen: Jussin, 18, lapsuus ei lopu, vaikka Taina-äitikin vanhenee
6. Presidentti Niinistöltä poikkeuksellinen ulostulo – hermostui Iltalehden toimittajalle
7. Omistajan kesämökki katosi mystisesti talven jälkeen: Vain lautakasa jäi jäljelle
8. Pariskunta teki nurmikolta järkyttävän löydön: Luultiin ensin krokotiiliksi, totuus löi ällikällä
9. Kommentti: Leijonien pelissä ei päätä eikä häntää – kaikkien aikojen mahalasku uhkaa
10. Kaksi lasta ja molemmat vanhemmat vuorotöissä: Näin Keräset selviävät arjen rumbasta

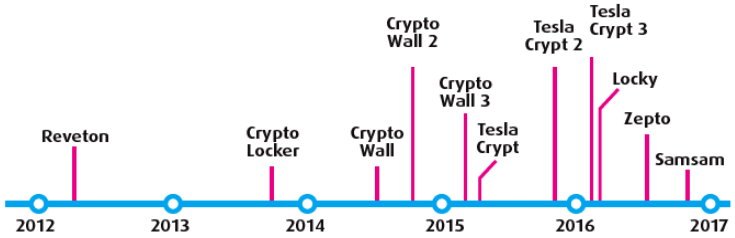
Kiristyshaittaohjelmat monipuolistuvat

Kiristyshaittaohjelma iskee organisaatioihin uusin keinoin

13.12.2016 klo 09:42

Verkkorikolliset valitsevat uusien kiristyshaittaohjelmien uhrit entistä tarkemmin. Nyt kohteena on yrityksiä ja organisaatioita, joiden verkosta etsitään haavoittuvuuksia. Kohdennettu haittaohjelma aiheuttaa yrityksille vakavaa haittaa ja jälkien korjaaminen on kallista. Keväällä Yhdysvaltoja ja Kanadaa vaivanneella Samsam-haittaohjelmalla on yritetty kiristää myös Suomessa.

Kiristyshaittaohjelmat salaavat tiedostoja ja järjestelmiä uhriin katsomatta niiden yksityisten kuin yritystenkin laitteissa. Lunnastroijalaisten saaliiksi on jäänyt työasemia, tietokoneita, tabletteja ja älypuhelimia. Normaaleja kiristyshaittaohjelmia lähetellään massasähköpostikampanjoilla tuhansittain eri vastaanottajille tai piilotetaan suositulle verkkosivustolle. Massatartutus kannattaa, jos riittävän moni maksaa lunnaat. Uusimmat kiristäjät valikoivat uhrinsa tarkemmin, etsivät verkosta heikon kohdan ja yrittävät siitä sisään



Suomessa havaittuja kiristyshaittaohjelmia ja niiden muunnoksia.

[Teema] Vieraskynä: Kiristyshaittaohjelmia HUS:n työasemissa

19.07.2016 klo 12:48

Viestintäviraston Kyberturvallisuuskeskuksen heinäkuun kiristyshaittaohjelma-teema jatkuu HUS:n tietohallinnon kirjoittamalla vieraskynä-artikkelilla. Kiristyshaittatapaukset ovat vuonna 2016 yleistyneet sairaaloissa ympäri maailmaa eikä Suomikaan ole tässä asiassa poikkeus. Mediassa on uutisoitu kevään aikana lunnastroijalaisten hyökkäyksistä mm. Helsingin ja Uudenmaan sairaanhoitopiirin tietoverkossa.

Keväällä 2016 muutama kiristyshaittaohjelma läpäisi HUS:n virustorjunnan ja sähköpostisuodatuksen. Kevään aikana työasemia on saastunut yhteensä neljä. Haittaohjelmat tulivat normaalin nettiselailun tai sähköpostin liitetiedoston mukana. Haittaohjelma saattoi piileksiä esimerkiksi sähköpostiviestiin liitettynä tekaistuna lähetyslistana.

Levyjä salakirjoittava kiristyshaittaohjelma havaitaan yleensä hyvin nopeasti. Käyttäjät ottavat herkästi yhteyttä palvelupisteeseen ja tapauksen selvitys alkaa usein jo ennen valvontajärjestelmän hälytystä.

Haittaohjelmat voivat aiheuttaa hengenvaaraa

- Tunnettuja tapauksia sairaaloissa Saksassa, USA:ssa, Israelissa...
  - » Röntgenlaite jäi kiristyshaittaohjelman panttivangiksi
  - » Verkon koneet jouduttiin sammuttamaan, "sisäinen hälytystila", $17 000 lunnaita maksettu, jne.
- Sairaaloissa kiristyshaittatapaukset lisääntyneet myös Suomessa
  - » Sairaalat ottavat varhain käyttöön uutta tekniikkaa, jonka verkkoturvallisuutta ei ole ehditty varmistaa → altis hyökkäyksille

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

> SC US
SC UK

RSA 2016: Enterprises, bad guys all turning to cloud

DA: San Bernardino shooter could have introduced 'dormant cyber pathogen'

NEWS | PRODUCT REVIEWS | BLOGS | SC CONGRESS | SC EXTRAS

SC Magazine > News > Ransomware holds data hostage in two German hospitals

Rene Millman

February 29, 2016

Ransomware holds data hostage in two German hospitals

Share this article:

A ransomware campaign has hit two German hospitals, soon after another ransomware campaign hit a Los Angeles medical centre, and the clean up is set to take weeks.

Two German hospitals have fallen victim to a ransomware attack that has left them unable to access their systems. It is thought the clean-up operation to remove all traces of the malware could take weeks.

According to a report by German broadcaster Deutsche Welle, the attack took place two weeks ago at the Lukas Hospital in the city of Neuss. Another attack took place at the Klinikum Arnsberg hospital which is located in North Rhine-Westphalia. It is not known if the two attacks are related.

Two more German hospitals have been hit with ransomware

According to Lukas Hospital spokesman Dr. Andreas Kremer, once it was realised that an attack was taking place, the hospital "pulled the plug on everything."

Tietomurrot


yle UUTISET

Etusivu Tuoreimmat Urheilu Sää | Kotimaa Ulkomaat Talous Politiikka Kulttuuri

Liikenneministeriön testaama autojen musta laatikko vuotaa - Hakkerit löysivät haavoittuvuuden

Helsingissä viikonloppuna pidetyssä hakkeritapahtumassa löydettiin vakava haavoittuvuus Suomessa koekäytössä olleesta autojen ajotietoja keräävästä laitteesta. Laitteeseen käsiksi pääsevä vosi hakkereiden mukaan vaarantaa muun muassa auton ohjauslaitteiden hallinnan.

Kotimaa 16.1.2017 klo 07:00

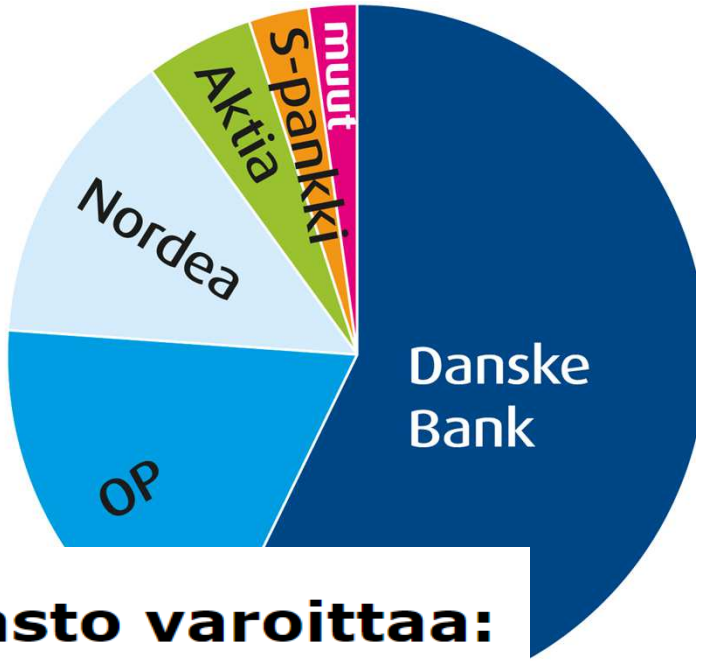
Uhkat ja haitat

- **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

Nettihuijaus- ja kalastelubisnes kukoistaa



TALOUSSANOMAT | OMX HELSINKI -0,03 % 18:35 8 989,20 | AFARAK 18:30

IS ETUSIVU | UUTISET | PÖRSSI | YRITYSTIEDOT

Viranomainen varoittaa huijauksesta: Näistä merkeistä tunnistat

Apple ID -, veronpalautus - ja pankkiteemaisilla tietojenkalasteluilla pyritää varastamaan luottokortti- j pankkitietoja

01.11.2016 klo 15:10 - *Päivitetty 20.12.2016 klo 13:47*

Viestintävirasto on vastaanottanut ilmoituksia suoma suunnatuista tietojenkalasteluviesteistä, joissa pyyde vahvistamaan vaihtunut Apple ID. Taitavasti väärenn kalastelusivulla erehdytetään käyttäjä luovuttamaan luottokorttitietonsa ja verkkopankkitunnukset. Nyt m veronpalautusten ja pankkien tietoturvapäivitysten v kalastetaan luottokorttitietoja ja verkkopankkitunnul

Viestintävirasto varoittaa: pankin nimissä leviää tilausansa

ına 2016

Keskiviikko 5.10.2016 klo 10.42

Viestintäviraston Kyberturvallisuuskeskus on saanut viimeaikoina useita ilmoituksia huijausviesteistä, joita on lähetetty Nordean tai Gigantin nimissä.

- **Viestintävirasto varoittaa liikkeellä olevista tilausansoista.**
- **Viestejä on lähetetty muun muassa Nordean ja Gigantin nimissä.**
- **Jos astuit tilausansaan, voit reklamoida ja kiistää maksuvelvollisuutesi.**

Kyberturvallisuuden näkymät

Vakoilu jatkuu

Palvelunestohyökkäyksien voima kasvaa

Kiristyshaittaohjelmat kehittyvät

Esineiden internet

Digitalisaation pelikenttä: Keinoäly, robotiikka, pilvipalvelut, Big Data

Mobiliteetti

Yhteystiedot

jarkko.saarimaki@ficora.fi

+358408360397

www.viestintavirasto.fi

@saarimaki

https://fi.linkedin.com/in/jarkko-saarimäki-5a13b7

200 000 syytä kertoa Viestintävirastolle tietoturvaloukkauksesta

Lähetä tieto tietoturvaloukkauksesta tai -epäilystä 24/7-palveluumme: cert@ficora.fi

Viestintävirasto