Mitkä ovat vuoden 2017 keskeisimpiä tietoturvauhkia?

ja kuinka niiltä tulisi suojautua?

2.10.2017 Julkisen hallinnon digitaalisen turvallisuuden teemaviikko

Tietoturva- ja kyberturvallisuusluennot

Turvaamme digitaalisuutta

Koordinaattori

Päivystäjä

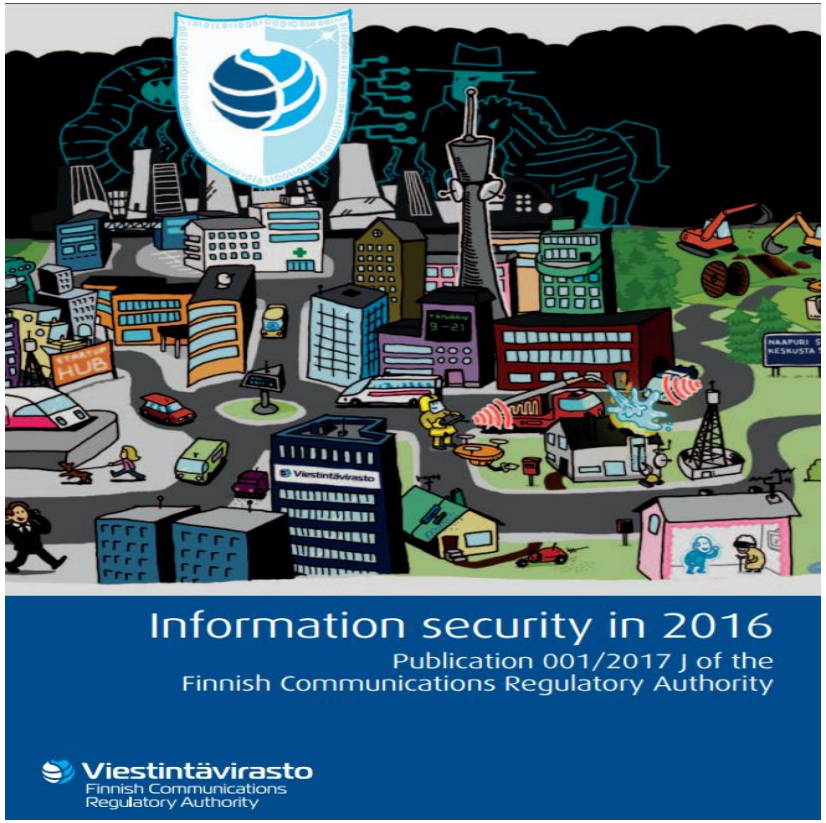
+60 kyber-turvallisuusalan asiantuntijaa

Tilannekeskus kerää tietoa

Ilmoitukset vuosittain	
Ilmoitukset	**Yli 1000**
Haavoittuvuus-koordinaatio	**Yli 10**
Omat järjestelmähavainnot	
Yleiset viestintäverkot (Autoreporter)	**50 - 410 000**
Organisaatioiden verkot (HAVARO)	**Yli 100**

Ja välittää tilannekuvaa

Julkiset tiedotteet	
Tietoturva nyt!	~100
Facebook & Twitter (+4500) (+6800)	Yli 250
CIP-jakeluille	
Viikkoraportit	52
Kuukausikoosteet	12
Päivittäiset uutiskoosteet	360
Haavoittuvuuskoosteet	99 (from june 2016)
CIP-infokirjeet	238



"CERT-massatiedotus" vuoden tietoturvailmiö 2016 by Mikrobitti

ALERTS

13.05.2017 time 13:09
Alert 02/2017
Updated 15.05.2017 time 15:50

Active ransomware campaign - install Windows updates immediately

Cases of the WanaCryptor ransomware have also been detected in Finland. The ransomware spreads very aggressively in the internal network of an organisation if the security patches for the vulnerabilities exploited by the ransomware have not been installed. To protect against this

[Teema] Kiire ja yllättävä rahantarve paljastaa verkkohuijarin

23.03.2017 klo 14:29

Nyt esittelyssä ovat yleisimmät sekä tuoreimmat huijaustyypit, jotka saapuvat sähköpostitse, tekstiviestitse, puhelimitse tai seuranhakupalvelun kautta. Usein verkkohuijarilla on kiire. Uhrin on toimitettava rahat pian, muuten ainutkertainen tilaisuus on ohi. Kaukorakkauskin voi katketa, jos varat eivät äkkiä kilahda armaan tilille. Pikavoittoja jaetaan kuitenkin vain harvoille, siksi niiden tarjoajiin ei pidä luottaa.

TOP5: käyttäjän tietoturvauhat ja -ratkaisut

Ongelmat	Ratkaisut
1. Huijaukset ja tilausansat	1. Mieti ennen kuin klikkaat
2. Kiristyshaittaohjelmien leviäminen älylaitteisiin	2. Salasanojen hallinta
3. IoT tuli joka kotiin	3. Päivitä verkossa olevat laitteet ja käyttämäsi ohjelmistot säännöllisesti
4. Yksityisyys somemaailmassa	4. Varmuuskopioi tärkeät tiedot
5. Salasanojen kierrätys	5. Käytä tietoturvaohjelmistoja

TOP5: työpaikan tietoturvauhat ja -ratkaisut

Ongelmat	Ratkaisut
1. Päivitysten laiminlyönti	1. Järjestelmien rutiininomainen päivitys
2. Kiristyshaittaohjelmat	2. Koulutettu henkilöstö
3. Huijausviestit ja tietojen kalastelu	3. Varmuuskopiot
4. Ulkoistusten ja laitehankintojen hallinta	4. Lokien hallinta
5. Palvelunestohyökkäykset	5. Tietoturvan hallittu johtaminen

#kybersää

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tarkoituksena on antaa lukijalle nopea kokonaiskuva siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

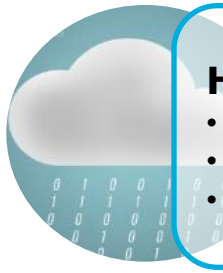
huolestuttava

vakava

#kybersää

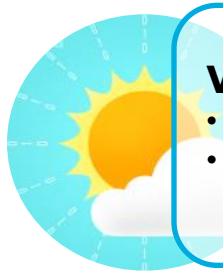
Palvelunestot
- Yksittäisiä hyökkäyksiä julkishallintoa ja yksityistä sektoria vastaan.
- 19-vuotias otettu kiinni epäiltynä palvelunestohyökkäyksistä.

Haittaohjelmat & haavoittuvuudet
- Sähköpostin .zip- ja .doc-liitetiedostojen avulla on levitetty kiristyshaittaohjelmia.
- Mirai havainnot lisääntyneet Netgear-laajakaistareitittimen oletussalasanojen takia.

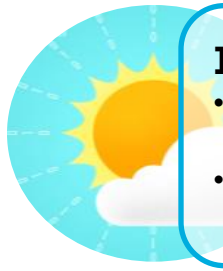


Huijaukset & kalastelut
- Pankkitunnusten kalastelu jatkuvaa.
- Toimitusjohtajahuijaukset piinaavat.
- Tilausansoja tunnettujen brändien nimissä.

Vakoilu
- Energiasektoriin ja teollisuusyrityksiin kohdistuneet vakoilukampanjat jatkuvat.
- ShadowPad-haittaohjelma osoittaa toimitusketjujen herkkyyden.



Verkkojen toimivuus
- Elokuussa merkittäviltä häiriöiltä vältyttiin.
- Kiira-myrskykään ei häirinnyt merkittävästi viestintäpalveluita.



IoT
- Lakiesitys: USA:n liittovaltion IoT-laitteiden on täytettävä tietoturvan minimivaatimukset.
- Suojaamattomaan IoT-laitteeseen murtaudutaan noin 2 minuutissa.

Elokuu 2017 on ollut pilvinen

"Internetissä huijauksia on käynnissä jatkuvasti.
Toimitusketjujen tietoturvallisuuden valvonta on haasteellista."

Palvelunestot

MONTHLY BRONZE

19.99$

- XyZ Public Network
- 250Gbps Network Capacity
- 27 Attack Methods
- 1800(s) Stress Time Per Attack
- 1 Months Membership
- 1 Concurrent attacks

REGISTER

MONTHLY SILVER

24.99$

- XyZ Public Network
- 250Gbps Network Capacity
- 27 Attack Methods
- 2400(s) Stress Time Per Attack
- 1 Months Membership
- 1 Concurrent attacks

REGISTER

MONTHLY DIAMOND

29.99$

- XyZ Public Network
- 250Gbps Network Capacity
- 27 Attack Methods
- 3600(s) Stress Time Per Attack
- 1 Months Membership
- 1 Concurrent attacks

REGISTER

V.I.P GOLD

BEST

149.99

$

- XyZ VIP Network
- 300-350Gbps Network Capacity
- 27 Attack Methods
- 8400(s) Stress Time Per Attack
- 1 Months Membership
- 2 Concurrent attacks

REGISTER

V.I.P DIAMOND

BEST

299.99

$

- XyZ VIP Network
- 350-400Gbps Network Capacity
- 27 Attack Methods
- 9600(s) Stress Time Per Attack
- 2 Months Membership
- 2 Concurrent attacks

REGISTER

V.I.P METAL

BEST

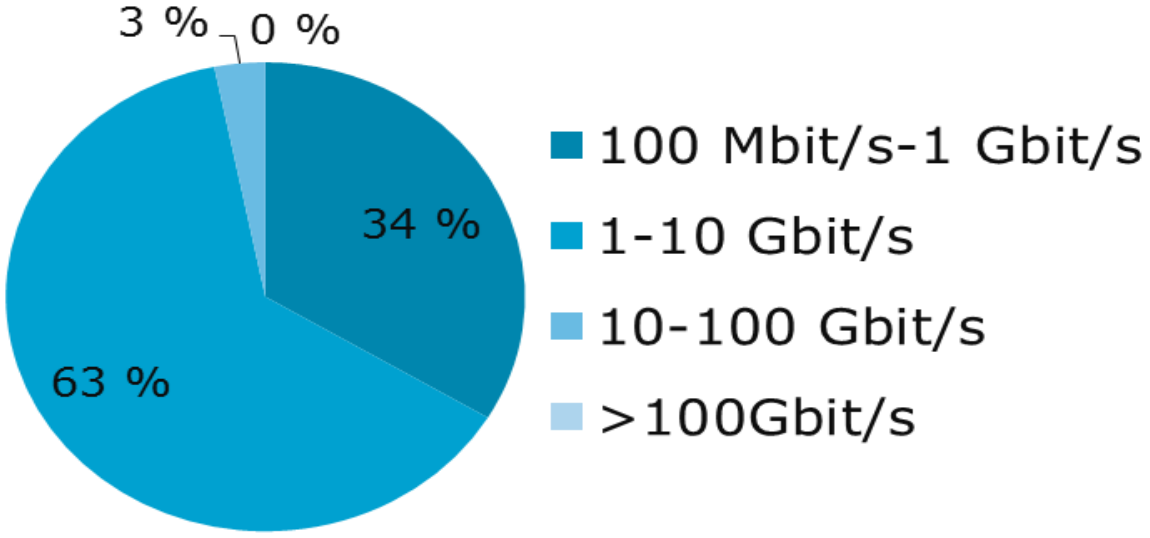
449.99

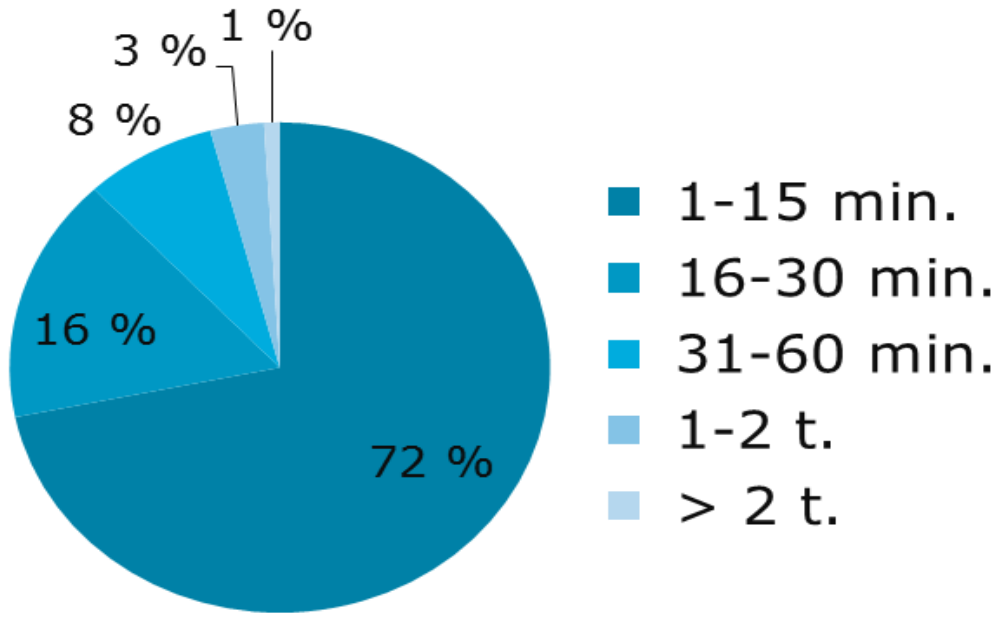
$

- XyZ VIP Network
- 350-400Gbps Network Capacity
- 27 Attack Methods
- 10800(s) Stress Time Per Attack
- 3 Months Membership
- 2 Concurrent attacks

REGISTER

Palvelunestohyökkäykset ja niillä uhkailu





Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2017/Q2. Lähde: Telia.
Seuraava tilasto: lokakuussa 2017

Palvelunesto: Miten suojaudun?

Käyttäjä

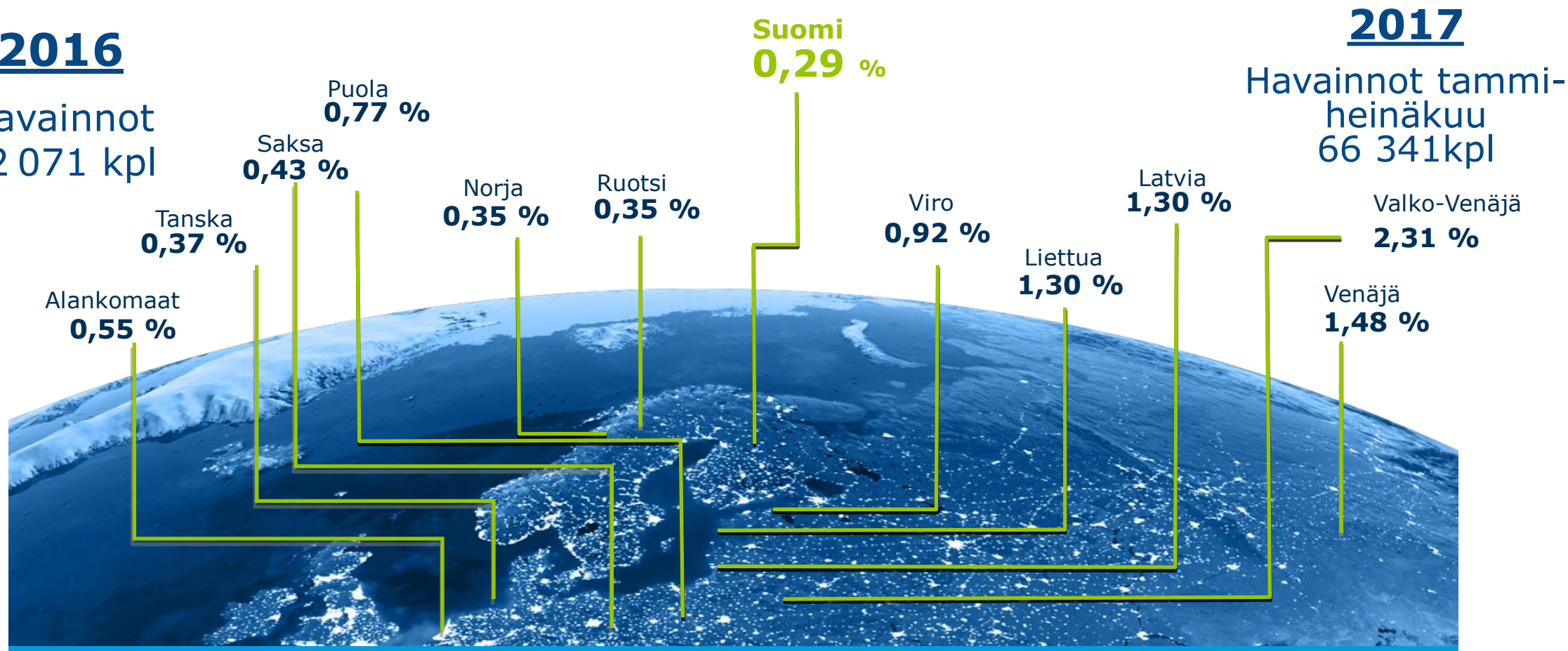
- Päivitä, päivitä, päivitä

Organisaatio

- Mieti riski+hinta ja suojaudu sen mukaan

Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa



Havaintojen määrä on keskimäärin vuoden 2015 tasolla. Mirai-botin leviäminen marras-joulukuussa 2016 nosti lukemaa selvästi.

Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

About bitcoin

How to buy bitcoins?

bitcoin ACCEPTED HERE

Send $600 worth of bitcoin to this address:

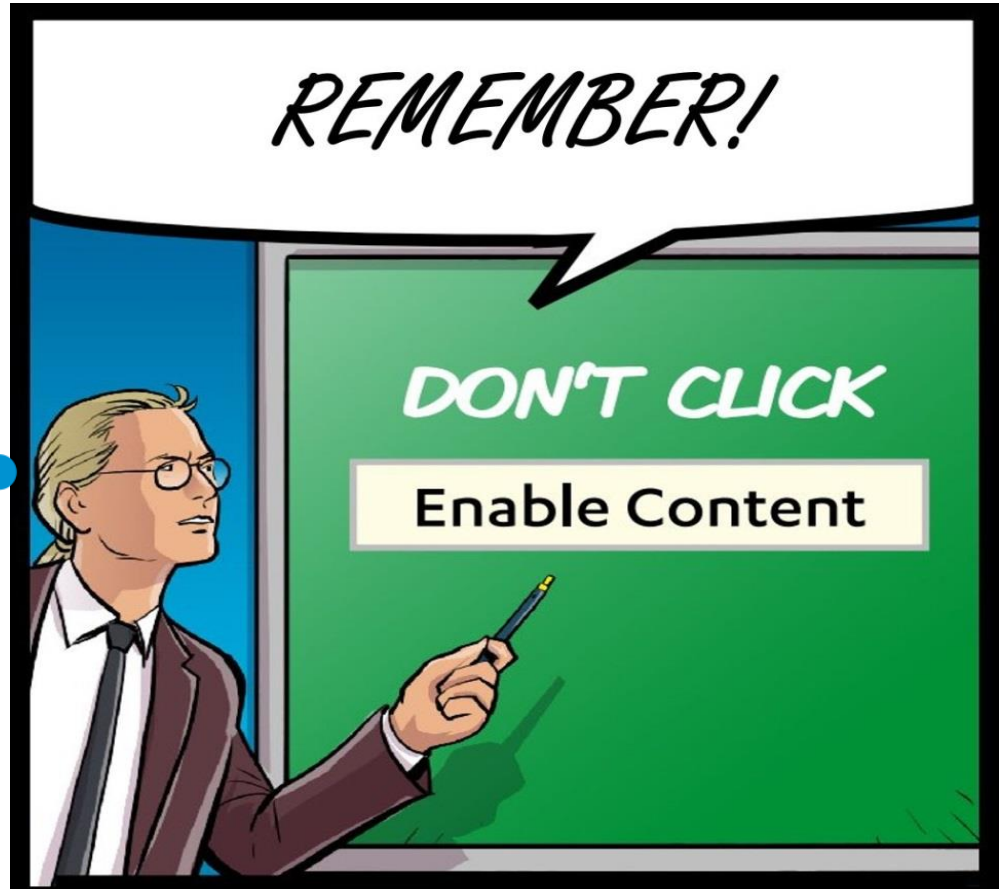
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Haittaohjelmat & haavat: Miten suojaudun?

- Käytä tietoturvaohjelmistoa
- Päivitä, päivitä, päivitä
- Varmuuskopioi, varmuuskopioi

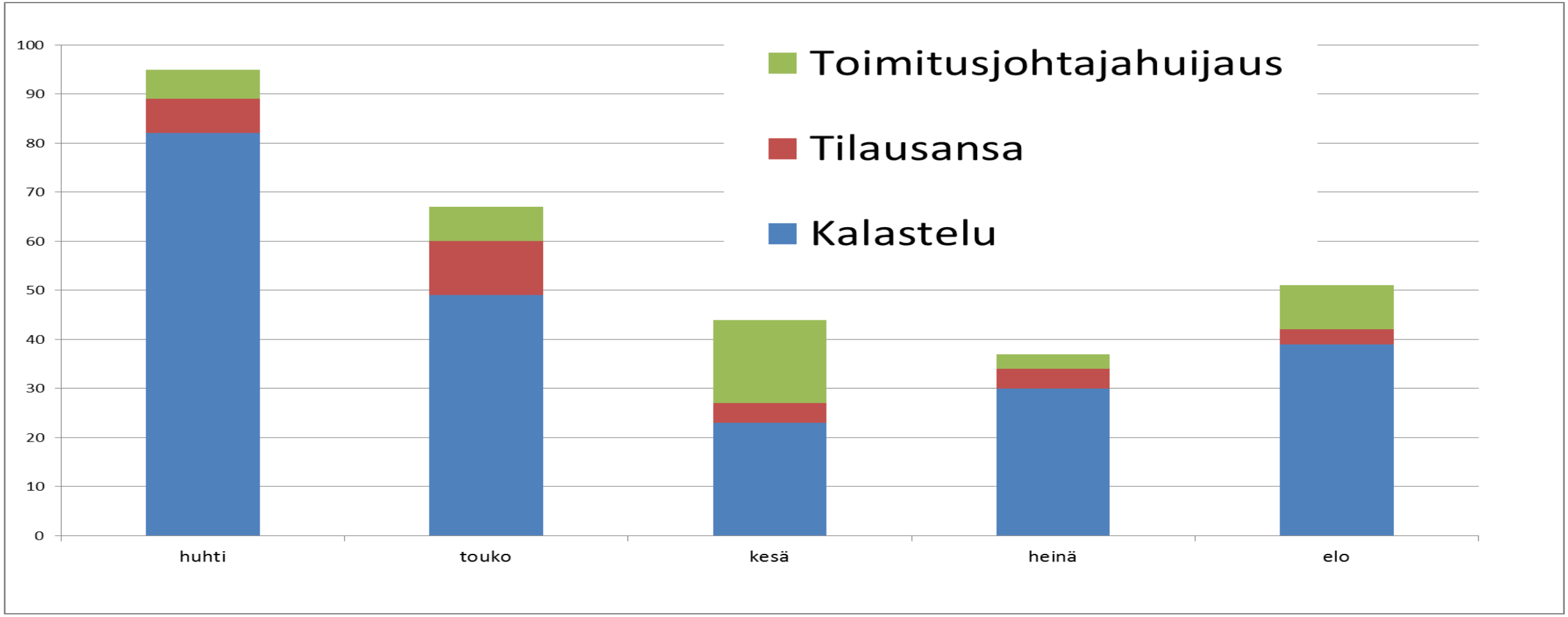
  &
- Mieti mitä klikkaat!



Twitter 18,11,2016: @mikko

Huijaukset & kalastelut

Huijausyritykset 2017/04-08



Huijaukset ja kalastelut: Miten suojaudun?

Käyttäjä

- Älä anna käyttäjätunnuksia ja –salasanoja ulkopuoliselle
- Liian hyvä tarjous on liian hyvä tarjous!

Organisaatio

- Laskujenmaksu ei ole kiireprosessi

Vakoilu


Verkkovakoilun anatomia
Hyökkääjän etumatka voi olla vaikka yli 9 kuukautta!
VALMISTELU
PÄIVÄ 1
Hyökkääjä päättää kohteen
HYÖKKÄÄJÄ PÄÄSEE VERKKOON
PÄIVÄ 7
Kerää tietoa ohjelmistoista ja henkilöstöstä
PÄIVÄ 70
Räätälöi haittaohjelman
PÄIVÄ 100
Tekee tarkentavan yhteydenoton
PÄIVÄ 140
Laatii sähköposti- ja phishing-viestit
PÄIVÄ 180
Saa jonkun avaamaan haittaohjelman
PÄIVÄ 181
Haittaohjelma lataa vakoiluohjelman komentopalvelimeen
PÄIVÄ 185
5 tartuttunutta konetta
PÄIVÄ 186
Useita käyttäjätunnuksia haltuun
PÄIVÄ 187
Admin-haltuun
Päivä 188
Siivoaa jäljet
ENSIMMÄINEN HAVAINTO VERKKO-VAKOILUSTA
PÄIVÄ 265
Havainto ulospäin lähtevästä ei-sallitusta liikenteestä
PÄIVÄ 268
Epäilys verkkovakoilusta
PÄIVÄ 270
Sisäinen tutkinta
Viestintävirasto
Päivä 280
Yhteydenotto Viestintävirastoon ja poliisiin

Verkkovakoilutilanteessa ajankohtaista

Energiasektori	Energiasektoriin ja teollisuusyrityksiin kohdistunut verkkovakoilukampanja aktiivinen läpi kesän.
Gazer/WhiteBear	Tietoturvayhtiöt paljastivat uuden edistyneen vakoiluohjelman. Haittaohjelma on yhdistetty Turla-vakoiluoperaatioon.
ShadowPad	Verkonhallintasovelluksen päivitykseen oli ujutettu haitallinen komponentti. Näin hyökkääjä voi päästä käsiksi ylläpitäjän työasemaan.

Vakoilu: Miten toimin?

Käyttäjä

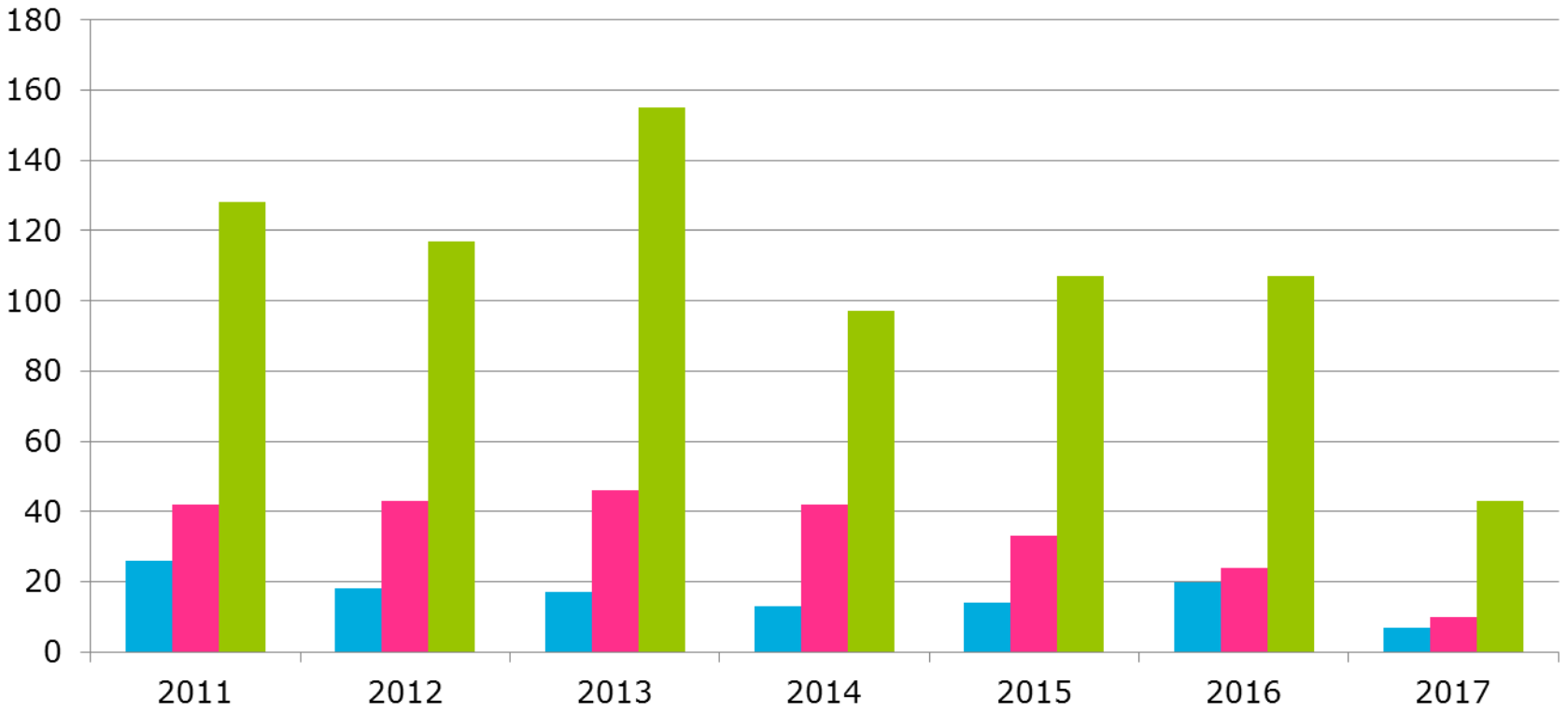
- Tutustu organisaation tietoturvaohjeisiin
- BYOD? Omia laitteita ja yhteyksiä käytettäessä riskistä ja suojauksesta vastaat itse

Organisaatio

- Harkitse riskit ja tunnista suojattavat tiedot/toiminnot
- Mieti sopiva keinovalikoima

Verkkojen toimivuus

Viestintäverkkojen toimivuus



Vakavia häiriöitä on 150-200/v.
Kaikkien häiriötilanteiden määrä on 200 000–350 000 vuodessa.

Elokuun loppuun mennessä vuonna 2017 on ollut selvästi vähemmän merkittäviä häiriöitä kuin edellisenä vuonna.

Käyttäjä: Miten toimin?

Käyttäjät

- Vältä verkon käyttöä häiriön aikaan, korjaukset ovat jo käynnissä

Organisaatio

- Varaudu verkon katkoksiin kriittisten toimien osalta

IoT

Viimeaikaisia uutisia

New IoT/Linux Malware Targets DVRs, Forms Botnet

By Claud Xiao, Cong Zheng and Yanhui Jia
April 6, 2017 at 1:00 PM
Category: Unit 42 Tags: Amnesia, botnet, DVR, IoT, Linux, malware, Tsunami

12,627

Unit 42 researchers have identified a new variant of the IoT/Linux botnet "Tsunami", which we are calling "Amnesia". The Amnesia botnet targets vulnerability that was publicly disclosed over a year ago in March 2016 in DVR (digital video recorder) devices made by TVT Digital and brande of which can be found on the original vulnerability report we've linked to). Based on our scan data shown below in Figure 1, this vulnerability aff around the world with Taiwan, the United States, Israel, Turkey, and India being the most exposed.

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

THE INTERNET OF HACKABLE THINGS

A Hackable Dishwasher Is Connecting Hospitals to the Internet of Shit

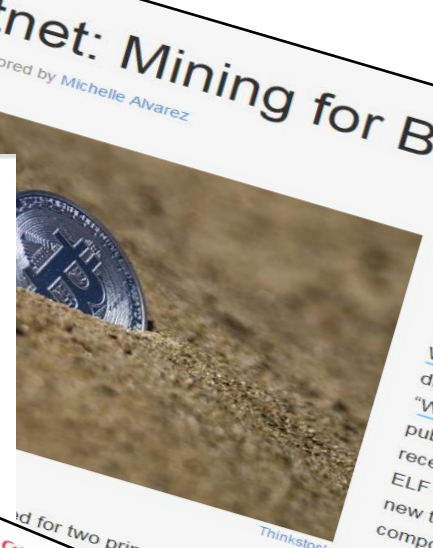
LORENZO FRANCESCHI-BICCHIERAI
Mar 27 2017, 5:59pm

Image: Andrey_Popov/Shutterstock

Despite all kinds of internet-connected things getting pwned, manufacturers insist of putting stuff on the internet without any security.

Mirai IoT Botnet: Mining for Bitcoins?

April 10, 2017 | By Dave McMillen Co-authored by Michelle Alvarez



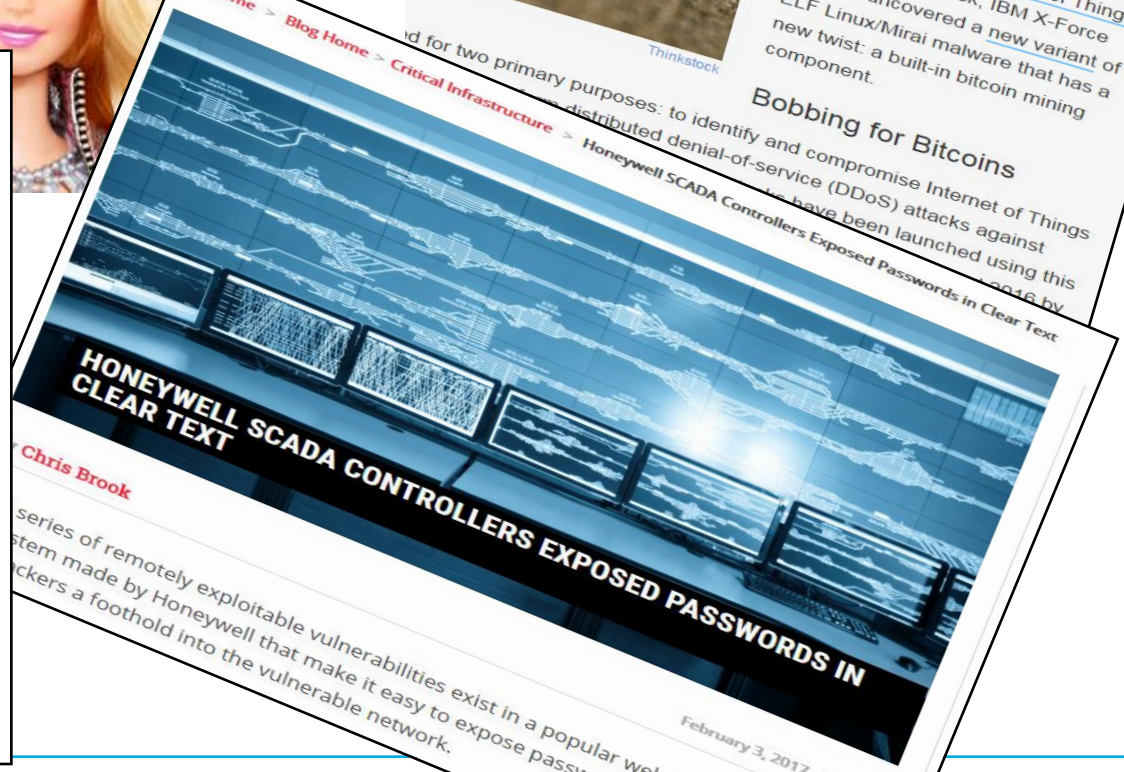
Thinkstock

Just in time for IoT Day, the Mirai botnet is launching attacks with a new trick up its sleeve. In February, the Mirai malware began leveraging a Windows Trojan to widen its distribution. On the heels of our paper "Weaponizing the Internet of Things," published last week, IBM X-Force recently uncovered a new variant of the ELF Linux/Mirai malware that has a new twist: a built-in bitcoin mining component.

Bobbing for Bitcoins

d for two primary purposes: to identify and compromise Internet of Things distributed denial-of-service (DDoS) attacks against have been launched using this

Welcome > Blog Home > Critical Infrastructure > Honeywell SCADA Controllers Exposed Passwords in Clear Text



Chris Brook

February 3, 2017, 3:03 pm

series of remotely exploitable vulnerabilities exist in a popular web-based SCADA tem made by Honeywell that make it easy to expose passwords and in turn, give ckers a foothold into the vulnerable network.

Käyttäjä: Miten toimin?

Käyttäjä

- Kaikki mikä on verkossa: päivitä, päivitä, päivitä
- Vaihda oletussalasana

Organisaatio

- Mitkä laitteet kuuluu olla verkossa?
- Päivitä verkossa olevat

Käyttäjä organisaatiossa: Mitä pitää muistaa?

1. Päivitä, päivitä, päivitä
2. Mietin mitä klikkaan
3. Huolehdin salasanoista
4. Noudatan organisaation ohjeita
5. Ilmoitan jos jotain epäilyttävää huomaan!

Ota Yhteyttä!

www.viestintavirasto.fi/
kyberturvallisuus

sähköpostitse: cert@ficora.fi

asiakaspalvelu: 0295 390 230

www.facebook.com/NCSC.FI

twitter.com/certfi

Viestintävirasto

Jarna.hartikainen@ficora.fi

www.viestintävirasto.fi

Suomi Finland 100