



# Mitä tiedämme vakoilusta nyt?

- Paljon uusia paljastuksia
  - mutta vain USA:sta, muista valtioista tiedämme vakoiluohjelmat mutta ei muuta
- Emme tiedä vieläkään totuutta PRISM-urkinnasta
  - https yleistynyt (Google & muut), mutta auttaako se?
- Tietoisuus urkinnasta lisääntynyt, mutta kanavoituuko se teoiksi?
  - salatun sähköpostin tai kotimaisen pilven kysyntä lisääntynyt vain vähän
  - vielä suurempi herätys oli UM:n vakoilupaljastus 30.10.2013
- EU aivan hajallaan
  - tapaus Belgacom, Saksa yhteistyössä NSA:n kanssa, Gemalto SIM-murto 2010-2011 ym.
- Antaudummeko urkinnan edessä?
  - matkalla kaapattuja läppäreitä, kiintolevyn firmwareen upotettua urkintaa...
  - jos kohde on riittävän arvokas, USA:lla on keinonsa - onko urkinta vain pakko hyväksyä?

@petterij

29.8.2016

## Researchers discover advanced cyber-espionage malware

Both Kaspersky and Symantec have unearthed a new type of malware so advanced, they believe it could have links to a country's intelligence agency. They're calling it "Remsec"...

According to Symantec, it has been used for what could be [state-sponsored attacks to infiltrate 36 computers across at least seven organizations around the world since 2011](#). Its targets include several individuals in Russia, a Chinese airline, an unnamed organization in Sweden and an embassy in Belgium. Kaspersky says you can add [various scientific research centers, military installations, telecommunications companies and financial institutions to that list](#).

ProjectSauron has been active since at least 2011, but it was only unearthed recently because [it was designed not to use patterns security experts usually look for when hunting for malware](#). Kaspersky only discovered its existence when it was asked by an unnamed government organization to investigate something weird going on with its network traffic.

The malware can move across a network -- [across even air gapped computers](#) that are supposed to be more secure than typical setups -- to siphon passwords, cryptographic keys, IP addresses, configuration files, among other data off computers. [It then stores all those information in a USB drive](#) that Windows recognizes as an approved device. Both security companies believe its development required the involvement of specialist teams and [that it costs millions of dollars to operate](#).

They didn't name a government in particular, but they noted that the malware took cues from older tools used for state-sponsored attacks, including Flamer that's been linked to Stuxnet in the past. As you might know, the Stuxnet worm, widely believed to be the joint creation of the US and Israel, infected Iran's nuclear program computers in the mid-2000s. <https://www.engadget.com/2016/08/09/projectsauron-malware>

# Muuta tapahtunutta

- Younited myytiin USA:han 2/2015
  - avattiin 2013, miksi lopetettiin jo nyt -- mitä Synchronoss varsinaisesti osti 52 milj. eurolla?
- TrueCryptin kehitys lopetettiin 5/2014
  - auditointi OK 4/2015, turva-aukko 9/2015; nyt Veracrypt ja Ciphershed
- Kanervan ja Haglundin salakuuntelukohu 9/2015?
  - vai tekninen häiriö?
- Suomesta merikaapeli Saksaan 2016
  - Ruotsin FRA:n piuhat hiljenevät?
- Jolla ja SSH yhteistyöhön
  - Kaspersky Lab yhteistyössä FSB:n kanssa?
- Näissä hommissa ei ole sijaa idealismille
  - jokainen huolehtikoon itsestään

## Jolla myöntää: Saifishistä Venäjän virallinen järjestelmä



18.8.2015 10:14 Venäjä suunnittelee kehittämänsä Jollan Saifish-käyttöjärjestelmästä oman kansallisen puhelimen käyttöjärjestelmän.

Venäjä haluaa kehittää Jollan saifish-käyttöjärjestelmän perustalle oman matkapuhelmeille tarkoitettun käyttöjärjestelmänsä, kertoo venäläinen [BBC-suomenkielinen](#).

Lehden mukaan Venäjän viestintäministeriö on päättänyt, että maa tarvitsee oman kansallisen puhelimen käyttöjärjestelmän.

Käyttöjärjestelmän perustana olisi kuitenkin Jollan kehittämä Saifish-käyttöjärjestelmä, sillä uuden käyttöjärjestelmän luominen täysin tyhjiästä olisi aikaa.

Jollan hallituksen puheenjohtaja [Antti Saarijo](#) kävi viime viikolla neuvottelemassa Venäjän viestintäministerin sekä maan il-yrittäjien edustajien kanssa.

@petterij

HS 22.11.2015

**Krimille julistettiin hätätila laajan sähkökatkon takia – Tass: Sähköpylväät räjäytettiin**

Krimin niemimaalla on edelleen rajoitettu Ukrainan kontrolloimissa läänneissä toimivien viestintäverkkojen toimintaa. Kukaan ei kuitenkaan ole saanut enää yhtäkään tekstiviestintää.

**Kasvokkain: Tilastonkari vertaa nykytyötä 1970-luvun duunielämään – "Pajon kivempää"**

Työväkijälästä on tullut entistä vaikeampaa työtä. 1970-luvun duunin aikana ihmisillä ei ollut vielä sähköä kotonaan, ja heidän piti tehdä töitänsä kassalla. Tällä hetkellä ihmisillä on sähköä kotonaan, ja heidän piti tehdä töitänsä kassalla.

**Katut valaistuslajit sulkevat katon parlamentin**

Parlamentin katon valaistuslajit sulkevat katon parlamentin. Tämä johtuu siitä, että valaistuslajit ovat sulkeutuneet.

**Merkivalit edustajat kostonväkivallan uhkana Suomessa – ministeri Toivola?**

Edustajat ovat kostonväkivallan uhkana Suomessa. Ministeri Toivola on kommentoinut tilannetta.

**Prosessi samppanjin öljy - tapauksessa Suomessa yhä ratkaisemattomat**

Prosessi samppanjin öljy - tapauksessa Suomessa yhä ratkaisemattomat. Tämä johtuu siitä, että tapaus on vielä ratkaisemattomana.

**Joko miehen ja naisen läheinen suhde on "shelvi" -shelvi ei ole helppo "shelvitä"**

Joko miehen ja naisen läheinen suhde on "shelvi". Shelvi ei ole helppo "shelvitä". Tämä johtuu siitä, että shelvi on vaikea käsitellä.

**Luottamus**

Luottamus on tärkeä asia. Tämä johtuu siitä, että luottamus on vaikea rakentaa.

**Suosittelemme**

Suosittelemme seuraavia artikkeleita. Tämä johtuu siitä, että ne ovat kiinnostavia.

HS 6.1.2016



“LÄNTISESSÄ Ukrainassa sijaitsevan 1,4 miljoonan asukkaan Ivano-Frankivskin kodeista noin puolet jäi joulun alla ilman sähköä. Ukrainalaisten sähköt vei kyberhyökkäys.

Tapahtuma muistuttaa Ilka Remeksen hittikirjan juonta. Nyt kyse ei kuitenkaan ole enää pelottavasta mielikuvituksesta, sillä **joulunaaton aattona sattunut sähkökatko on ensimmäinen kerta, kun tietoturvatutkijat ovat pystyneet osoittamaan suoran yhteyden todellisen sähkökatkon ja tietojärjestelmiin tunkeutuneen haittaohjelman toiminnan välillä.**

Vaikka sähkökatko jäi tällä kertaa vain muutaman tunnin mittaiseksi, se on huolestuttava merkki. Kun tietoverkkojen toimintaa saadaan häirittyä riittävän tehokkaasti, digitaaliseksi kuviteltu uhka muuttuu fyysiseksi. Kansalaisille tulee kylmä. Pitkittyessään se voi vaatia ihmishenkiä.

OLI kyseessä sitten rosvo, vakooja, valtio tai mikä hyvänsä niiden yhdistelmistä, tapaus on huolestuttava. Tietoturva-alalla valtioiden kriittiseen infrastruktuuriin kuten sähkölaitoksiin ja sairaaloihin sekä teollisuuteen kohdistuvia verkkosabotaaseja on osattu odottaa jo vuosia.” -- HS 6.1.2016




HS 14.4.2016 klo 10:00

Sano ihminen kirjoksi. Mäntä sai lakinsa Helsingissä

### Ruotsin lentoliikenteen pysäyttäneen häiriön on uusi löytö avaruussäätä – aiemmin syyskuu epäiltiin Venäjän kyberhyökkäystä

Vuosisikuryhtiönä Ruotsin epäily perustettiin Ruotsin lentoliikenteen viikon väden lopulla. Onnalle-työryhmä luokittelee rikkaita lauvastaan selvi- kento luokan sen luokitus tutkimusprosessin.

Kuusi vuotta sitten...  
 DIGITAALISET ARAKASLEHDIT HESARIN TILAAJILLE ESRIN TILAAJILLE 5,11 €




**14.4.2016**

HS 14.4.2016 klo 10:00

### Epäily: Ruotsin lentoliikenteen seisauttanut aurinkomyrsky olikin Venäjän kyberhyökkäys?

Yksi avarus tutkijat luokittelee häiriön...  
 Ruotsin lentoliikenteen häiriön syy on aurinkomyrsky, ei Venäjän kyberhyökkäys.



**14.4.2016**

HS 20.5.2016 klo 14:11

### Ruotsissa epäillään lähetysmastojen sabotaasia – yhteydessä torstain lentokaaokseen?

Tutkimusryhmä epäilee torstain viikonloppuun...  
 Ruotsin lentoliikenteen häiriön syy on lähetysmastojen sabotaasi.



**20.5.2016**

HS 20.5.2016 klo 14:11

### Ruotsin uusi mastovahinko ei ollut sabotaasi

Kirkkokokouksen todettiin, että Ruotsin ei ole tehnyt...  
 Ruotsin lentoliikenteen häiriön syy on mastovahinko, ei sabotaasi.



**20.5.2016**

**Nyt**

**Hakkerit sulattivat terästehtaan – jep, sulattivat terästehtaan – ja ovat pian sinun jääkaapillasi**

Yhteistyössä, jotta et olisi vielä väkisin. Yhteistyössä, että saisi James Bond -titaan joutua. Niitä on ollut viime aikoina aiti helppo ajella. Nyt se kannattaa lopettaa.

**Ostospaikka pari viikoksi keskeytyksissä**

Itämaassa ja lounaissa on joutunut jättämään työt väliin. Terveystieteiden tutkimuskeskus on joutunut jättämään työt väliin. Jokaista edes harkittava.

Samaan päivään samaan aikaan Helsingin joutui myös sulattamaan Yhdysvaltojen läheisyydessä hyökkäykseen. Terveystieteiden tutkimuskeskus on joutunut jättämään työt väliin.

Viime viikolla saatiin tietää, että joku on tullut sulattamaan terästehtaan.

**Kyberhyökkäys saksalaiselle terästehtaalte aiheutti suuret vahingot**

Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot. Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot.

**Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot**

Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot. Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot.

**Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot**

Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot. Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot.

**Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot**

Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot. Teollisuuslaitos saksalaiselle terästehtaalte aiheutti suuret vahingot.

I'm referring to the revelation, in a [German report released just before Christmas](#) (.pdf), that hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

"Failures accumulated in individual control components or entire systems," the report notes. As a result, the plant was "unable to shut down a blast furnace in a regulated manner" which resulted in "massive damage to the system."

U.S. congressional source said there was a suspicion that it was a "corrupt employee in the pay of a foreign government" could have been the source of the German steel mill breach, adding "so far, we have no conclusive proof of that."

[Ilmeisesti Havex-haittaohjelma. Kukaan ei tunnu tietävän yksityiskohtia?](#)

# Tiedustelulaki on tarpeen

- Mutta minkälainen?
- Ovatko salaukset ja liian Big Data jo syöneet suurimman hyödyn?
- FBI, Britannia ym. haluaisivat kieltää salaukset tai vaativat takaportteja puhelimiin – it's 90's once more...
- Kannattaa lukea G. Tenetin muistelmat – At the center of Storm
- Kuka valvoo valvoja? – Suomen poliisi on maailman luotettavin, mutta riittääkö sekään?



@petterij

## Älylamppu teki palvelunestohyökkäyksen - koko talo meni jumiin

Tietojenkäsittelytieteen professori Rauli Rojas osoitti talonsa toimivien älylaitteiden älyä – lähes kaikki osat oli yhdistetty internetiin. Käipyä seurauksia olivat lastatsofonia, kun yksi älylamppu teki palvelunestohyökkäyksen sisäiseen järjestelmään, Finbox.net [lue lisää](#).

Koko koti jumitti eikä voinut saast päälle. Älylaitteet löytyi epätoivosta nimenomaan älylamppu, joka yritti viestiä lähteestään. Vain tämä lamppu ei heilittänyt, vaan lähetti signaalia jatkuvasti.

"Älykotien turvallisuus on valitsemalla se, jota turvot vain laittaisi päälle. Normaaliäly henkilöille tilanne olisi ollut lause. He olisivat epäusmi tiri kaikki kodin järkeä", Rojas kommentoi.

Hiljain talossa on yksi Raksan automaattisesti tarkoitettu älykoti. Eri laitteita varten on suunniteltu erillisiä...

Älykotien turvallisuus on valitsemalla se, jota turvot vain laittaisi päälle. Normaaliäly henkilöille tilanne olisi ollut lause. He olisivat epäusmi tiri kaikki kodin järkeä", Rojas kommentoi.

**Hyökkäys**

Älykotiin hyökkäys jatkui lähes...

Hyökkäys alkoi tarkasti silloin...

Facebookin kaltaisia palveluita...

Uuden kodin...

Facebookin...

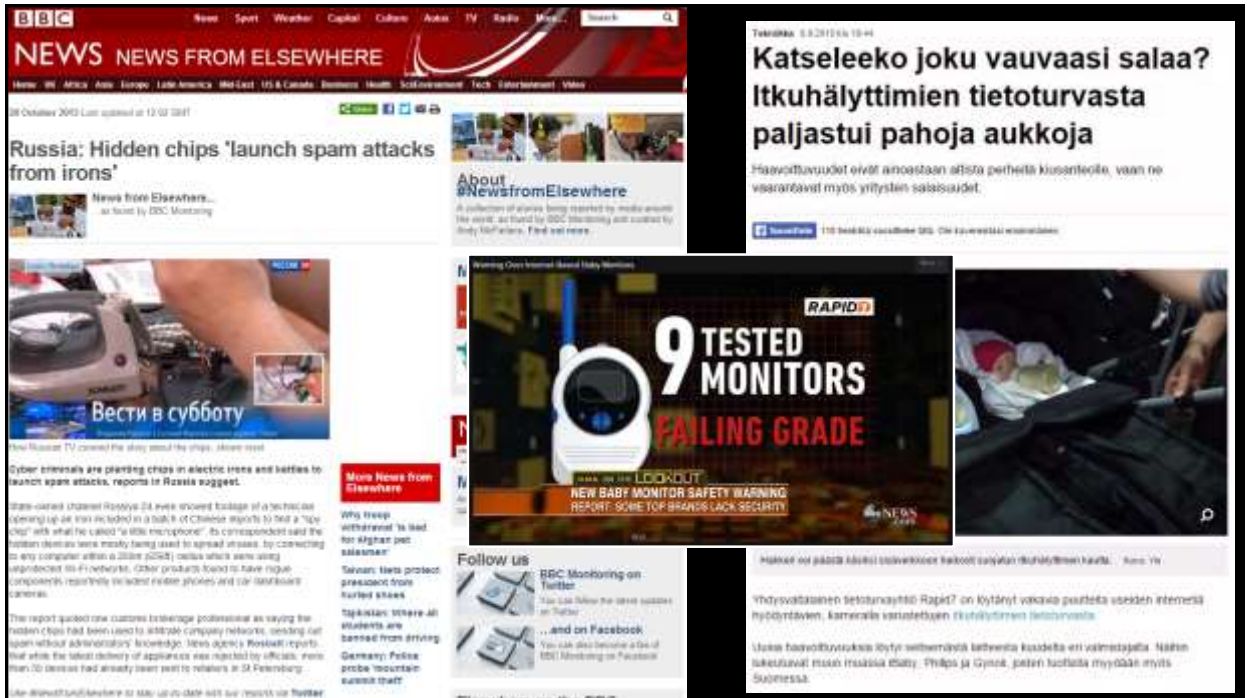
Älykotien...

Kuinka turvallisia ovat älykotien etäohjauksratkaisut?

IT:tä saa tehdä kuka tahansa, kylppäreihin vaaditaan sertifikaatti

IT:n elinkaari paljon lyhyempi kuin rakennuksen elinkaari





## Wilma kaatui – ”Ihmiset eivät tiedä, minne mennä tai mitä tehdä”

8.10.2013 – Uusi Suomi: ”Koulujen tiedonvälitykseen käytettävän Wilma-järjestelmän käyttökatko aiheutti tiistaina hämmennystä vantaalaisissa lukiissa.

– Tämä aamu on ollut komediaa. **Ihmiset eivät tiedä, minne mennä tai mitä tehdä. He haahuilevat kummituksina pitkin käytäviä tuskaisesti kirkuen yrittäessään löytää oikeaan luokkaan**, Uronen kuvaa blogissaan kärjistäen.

Uronen mukaan monella oppilaalla lukujärjestykset, opettajien viestit ja lähes kaikki muu koulunkäyntiin tarvittava tieto on Wilmassa.

Koiviston mukaan katkos sattui uuden opintojakson ensimmäisenä päivänä. Opintojakson vaihtuminen tarkoittaa uusien kurssien alkamista ja muutoksia lukiolaisten lukujärjestyksiin. Moni opiskelija ei muistanut uutta lukujärjestystä ulkoa.

– Jakson ensimmäinen päivä oli mahdollisimman kriittinen aika, joten huonona päivänä tämä tapahtui, Koivisto sanoo.

Opettajat olivat Koiviston mukaan teknisestä ongelmasta huolimatta selvillä omista aikatauluistaan.

Aamun sekaannuksen jälkeen tilanne selkiintyi Koiviston mukaan melko pian. Koiviston mukaan osa oppilaista oli ottanut älypuhelimella lukujärjestyksestään kuvan, jota sitten näytettiin kavereille tarvittaessa.


Myös Emma Uronen kirjoittaa blogissaan, että hyvin harvat oppilaat olivat kirjoittaneet lukujärjestyksen ylös, koska **tapana on tarkistaa se älypuhelimella Wilmasta.**”

## ”Anarkia on kolmen saamatta jääneen aterian päässä”



## Yhteinen asiamme

- Aluksi **yrityksen** sitten **jokaisen kansalaisen** nyt **koko Suomen** asia
- Kukaan ei halua joutua tietämättään desantiksi tai informaatio sodan hyväksikäyttämäksi – propaganda on uusi aselaji
- Kyberturvallisuudessa Suomen etulinja kulkee jokaisen kodin ja yrityksen kautta
- Suomi katsoo taaksepäin, ei tulevaisuuteen – **siihen ei ole varaa**
- Nyt ei kaivata talvisodan henkeä



**British Army** British army creates team of Facebook warriors

Soldiers familiar with social media sought for 7th Brigade, which will be responsible for 'non-lethal warfare'

**Down MacAskill**, defence correspondent

Saturday 17 January 2015 3:40 GMT


23k 505

The British army is creating a special force of Facebook warriors, skilled in psychological operations and use of social media to engage in unconventional warfare in the information age.

The 7th Brigade, to be based in Hermitage, near Newbury, in Berkshire, will be about 1,500 strong and formed of units drawn from across the army. It will formally come into being in April.

The brigade will be responsible for what is described as non-lethal warfare. Both the Israeli and US army already engage heavily in psychological operations.

Against a background of 24-hour news, smartphones and social media, such as Facebook and Twitter, the force will attempt to control the narrative.



**Armeija 2.0: Iso-Britannia värvää pataljoonallisen Facebook-sotilaita**

(Ilm. Tuomari Anttilä)

Iso-Britannian armeija on perustanut uuden aikalaisen Facebook-sotilait. Finnsal Timesin mukaan Facebook-sotilait kutsutaan nimellä "Information Warfare" ja prosessitiedotus.

Uusi yksikkö nimetään 77. pataljoonaksi ja siihen kuuluu 1500 sotilasta. Yksikkö on tarkoitettu psykologiseen sotaan ja informaation sotaan. Yksikkö on tarkoitettu psykologiseen sotaan ja informaation sotaan.

Iso-Britannia ei ole vielä julkistanut yksikköä koskevia tietoja sotilaitaan. Suomessa keuhkotautia on harvinaisesti esiintynyt Venäjän miekkovalvottuina sotilaina "trollit". Niitä on odotettavissa terrorismitapahtuihin ja tällä hetkellä aktiivisena osana median käyttöä ennen julkista lehti- ja televisioita.

Informaatiosota ei ole trollausta vaan huomaamaton vaikuttamista.

Homer Simpson: "Faktoilla voi perustella mitä tahansa, joka on vähänkin totta"

<https://www.youtube.com/watch?v=KF6SNxNIV08>

## Mitä minä voin tehdä?

- Kaikkien laitteiden päivitykset ajan tasalle
  - äly-tv, wlan-reititin, itkuhälyttimet, älypuhelimet ym.
- Wlan-verkkojen salasana
  - ei avoimia verkkoja, ei kaikkein yleisimpiä salasanoja
- Henkilökohtainen resilienssi
  - varautuminen sähkö- ja nettikatkoihin
- Yleinen tietoturvaosaaminen
  - usb-laitteet, toiminta ulkomailla, click-to-run-asetus...
  - APT-hyökkäysten torjunta organisaatioissa
- Kansalaisten koulutus tietoturvaan
  - etulinjassa virheet voivat olla kohtalokkaita



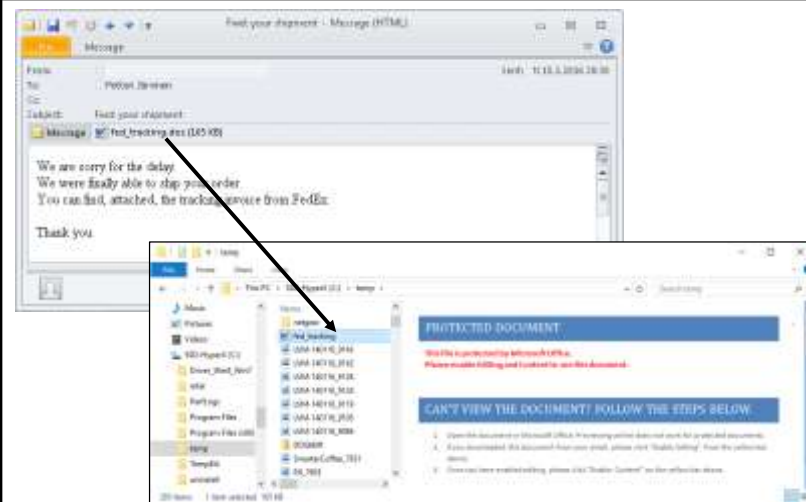
<http://tiedostot.spek.fi/kotivara/desktop/index.html>



@petterij

29.8.2016

# Varo word-liitetiedostoja



- Virustorjunta voi havaita vasta kun haittaohjelma yrittää aktivoitua



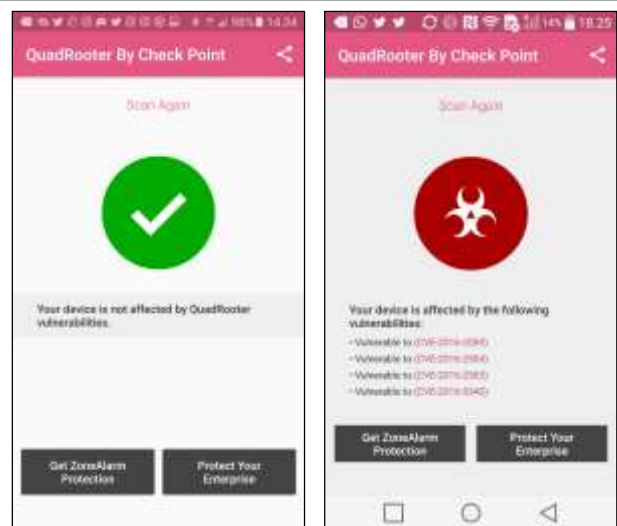
- Esikatselu paljastaa
- Älä aktivoi makroja, vaikka liite kehottaa!
- Avaa Google Docsissa tai älypuhelimella

@petterij

29.8.2016

# Älypuhelimien haavoittuvuudet

- QuadRooter Androidissa
  - käyttöjärjestelmän suojausten ohittaminen sovelluksesta
  - haavoittuvuusia etsittiin vain Qualcomm piireistä – ja löytyi
- 3 haavoittuvuutta iPhoneissa
  - israelilainen NSO myynyt ohjelman UAE:n viranomaisille
  - kohteena Ahmed Mansoor: viestin avaaminen olisi avannut pääsyn puhelimeen
  - ei varmasti ainoat NSO:n tuntemat
- Mitä Snowden sanoikaan?
  - ”brittikavoojat kykenevät hakkeroimaan älypuhelimien yhdellä tekstiviestillä. Tämän jälkeen puhelimella voidaan tehdä äänityksiä ja ottaa kuvia omistajan tietämättä”



@petterij

29.8.2016

Mukavuus \* turvallisuus =  
vakio

Turvallisuus vaatii **työtä**