Yhteystietoja

dipl. ins.
Petteri Järvinen

@petterij

pjarvinen.blogspot.com
bittimittari.blogspot.com

www.facebook.com/petterijj

fi.linkedin.com/in/petterij

instagram.com/petterijj

Tekniikantie 12, Espoo

BTC: 18XdRN46UvrHtteFyMejND7af5CBUe5A1o
PGP: 0809 2085 308E 0DF1 4173 EADD 8231 7135 9F31 FC66

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

@petterij

HS 22.11.2015

HS 6.1.2016

Poikkeuksellinen kyberhyökkäys onnistui sammuttamaan ukrainalaisten sähköt

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

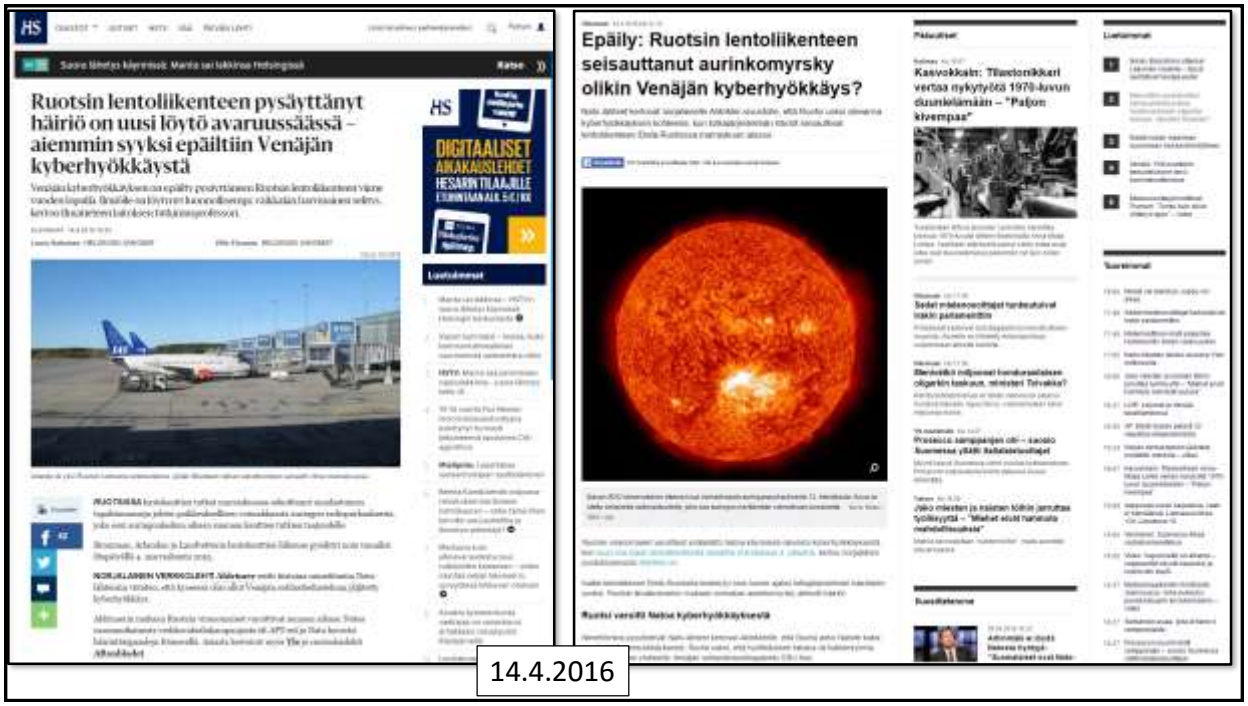
Tapahtuma muistuttaa Ilkka Remeksen hittikirjan juonta. Nyt kyse ei kuitenkaan ole enää pelottavasta mielikuvituksesta, sillä joulunaaton aattona sattunut sähkökatko on ensimmäinen kerta, kun tietoturvatutkijat ovat pystyneet osoittamaan suoran yhteyden todellisen sähkökatkon ja tietojärjestelmiin tunkeutuneen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

Yle 4.11.2015

Yle 6.11.2015


Ruotsin lentoliikenteen pysäyttänyt häiriö on uusi löytö avaruussäässä – aiemmin syyksi epäiltiin Venäjän kyberhyökkäystä
Epäily: Ruotsin lentoliikenteen seisauttanut aurinkomyrsky olikin Venäjän kyberhyökkäys?
14.4.2016


Ruotsissa epäillään lähetysmastojen sabotaasia – yhteydessä torstain lentokaaokseen?
Ruotsin uusin mastovahinko ei ollut sabotaasi
20.5.2016

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 valvojia?
  - Suomen poliisi on maailman luotettavin, mutta riittääkö sekään?

@petterij

Kuinka turvallisia ovat älykotien etäohjausratkaisut?

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 vantaalaisessa lukiossa.

– 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.

Urosen 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.”

@petterij 29.8.2016

”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 informaatiosodan 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 creates team of Facebook warriors

Soldiers familiar with social media sought for 77th Brigade, which will be responsible for 'non lethal warfare'

Dawn MacAskill, defence correspondent

21k 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 77th 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

Informaatiosota ei ole trollausta vaan huomaamatonta vaikuttamista.

Homer Simpson: ”Faktoilla voi perustella mitä tahansa, joka on vähänkin totta”
https://www.youtube.com/watch?v=KF6SNxNIV08

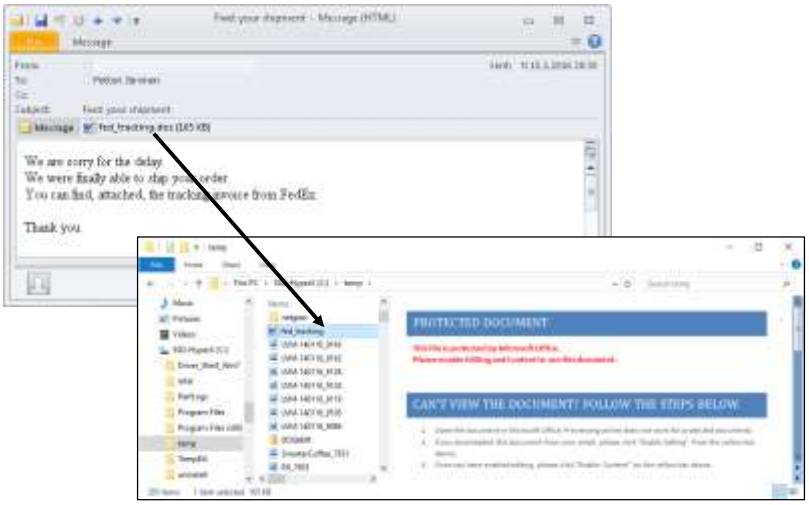
Mitä minä voin tehdä?

- Kaikkien laitteiden päivitykset ajan tasalle
  - äly-tv, wlan-reititin, itkuhälyttimet, älypuhelimet ym.
- Wlan-verkkojen salasanat
  - 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



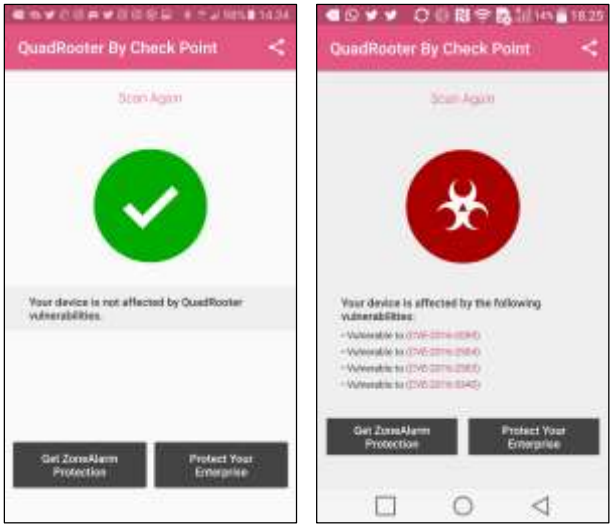
- Virustorjunta voi havaita vasta kun haittaohjelma yrittää aktivoitua

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

@petterij 29.8.2016

Älypuhelinten haavoittuvuudet

- QuadRooter Androidissa
  - käyttöjärjestelmän suojausten ohittaminen sovelluksesta
  - haavoittuvuuksia etsittiin vain Qualcomin 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?
  - ”brittivakoojat kykenevät hakkeroimaan älypuhelimen yhdellä tekstiviestillä. Tämän jälkeen puhelimella voidaan tehdä äänityksiä ja ottaa kuvia omistajan tietämättä”



@petterij 29.8.2016

Mukavuus * turvallisuus = vakio

Turvallisuus vaatii **työtä**