Verkkorikollisuuden uudet uhkat

kiristysohjelmat, kryptovaluutat ja IoT

Mikä verkossa vaanii? – Apua ja oikeutta verkkorikosten uhreille
Oulu 20.4.2018

@petterij
Petteri Järvinen

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: 1PetterieJAPNAbcWjwWU3GtWuzMLnq6SM
PGP: 0809 2085 308E 0DF1 4173 EADD 8231 7135 9F31 FC66

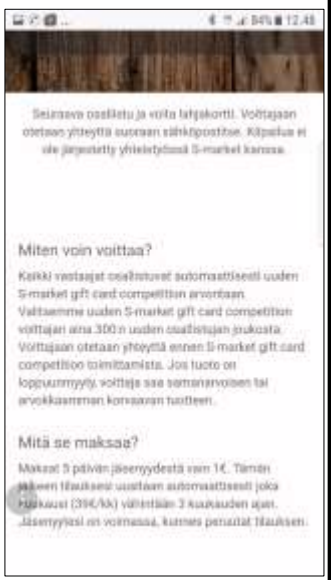
TIETOTURVA/TIETOSUOJA TULEE IHOLLE

Tekniikka tulee iholle - kirjaimellisesti

Data on uusi öljy, kaikki palvelut perustuvat sen käyttöön.

EU tietosuoja-asetus (GDPR) 25.5.2018 antaa kuluttajalle oikeuksia omiin tietoihinsa: tarkistus, poisto, siirto ym.

@petterij 20.4.2018



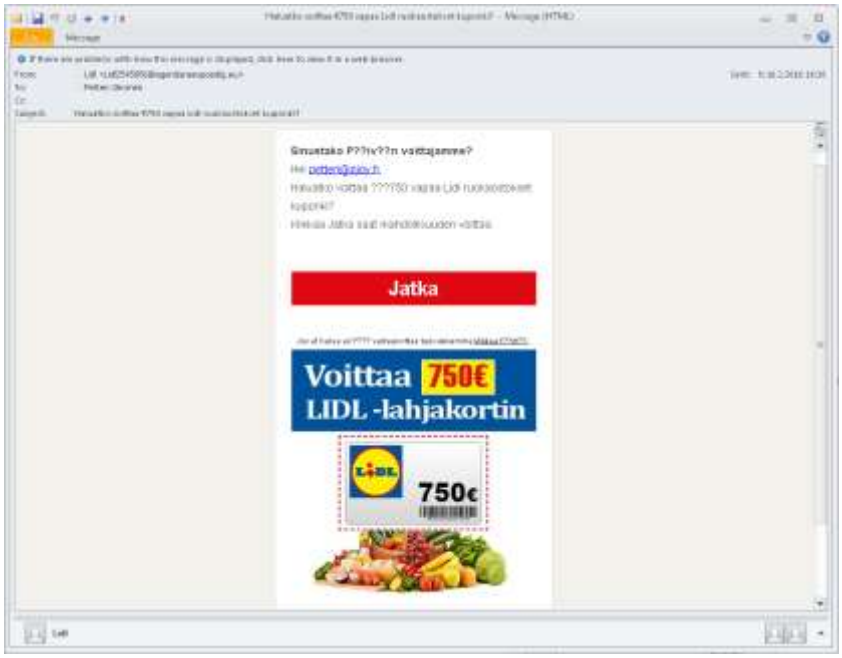
Houkutteluviesti sähköpostilla.

"Read the fine print!"

Linkki vie lomakkeeseen ja kysyy luottokortin tiedot.

Maksaa 1+3*39 eur = 118 euroa. Kulu rikollisille 600 eur/300 osallistujaa = 2 euroa, voitto 116 euroa/uhri.

@petterij 20.4.2018



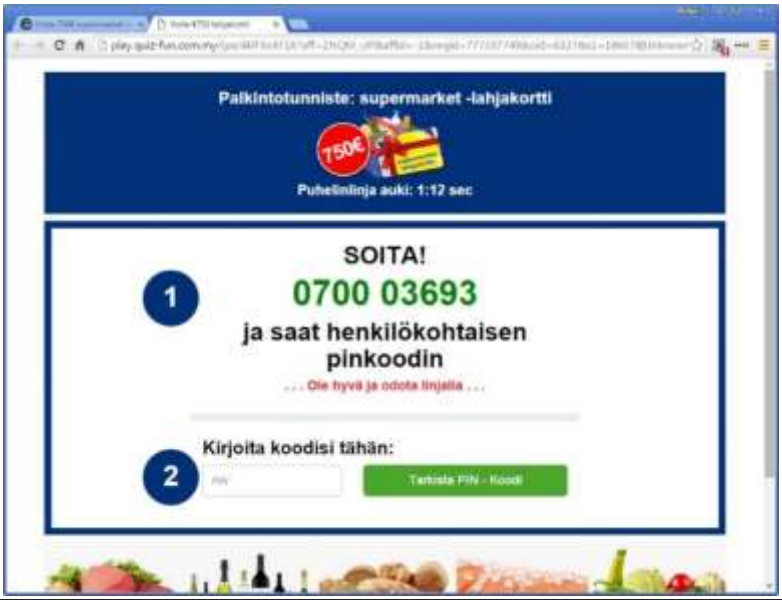
@petterij 20.4.2018

@petterij 20.4.2018

VAIN KOLME LAHJAKORTTIA ARVOTAAN

@petterij 20.4.2018

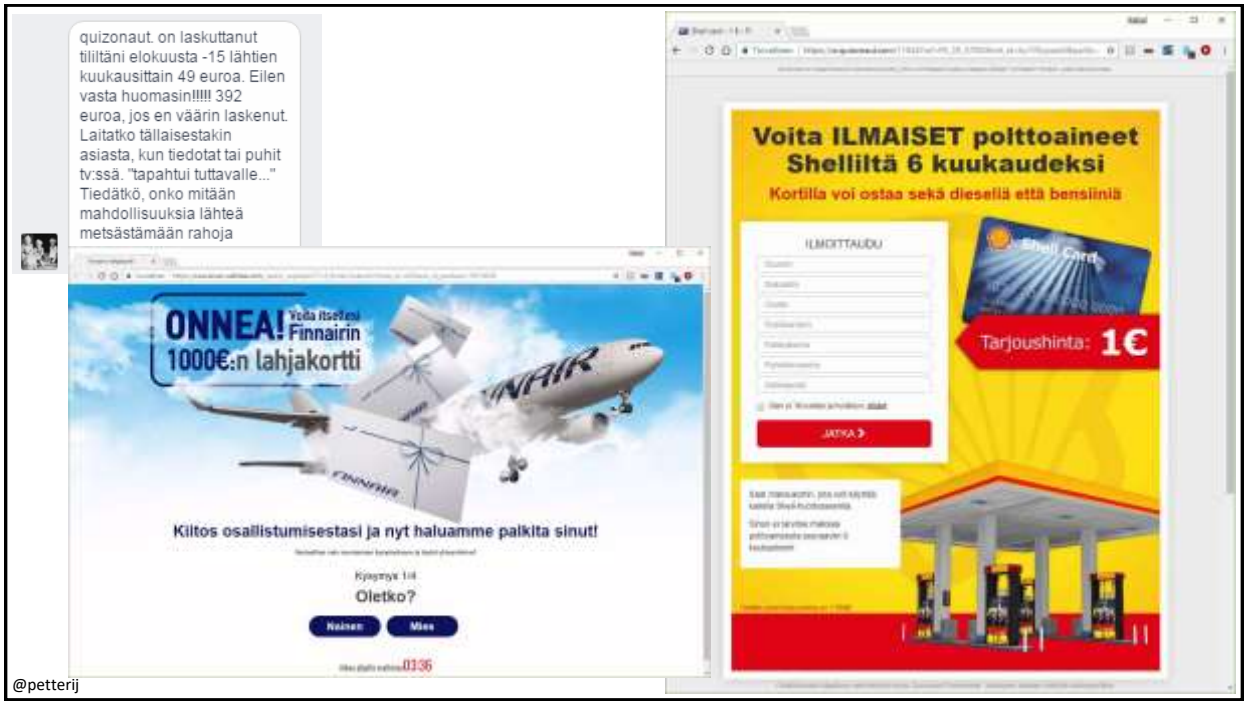
SOITTO 0700-NUMEROON



@petterij 20.4.2018

TARKOITUS KULUTTAA MAX. 30 MIN

@petterij 20.4.2018



@petterij

SUOMALAINEN METODI

"Suomalainen Metodi on 100% ILMAINEN ohjelma joka tekee vaihtoja binäärioptiomarkkinoilla vain 1 klikkauksella! Se paikantaa voittavat vaihdot sinulle täysin automaattisesti"

@petterij 20.4.2018

RUOTSALAINEN METODI

@petterij 20.4.2018

TANSKALAINEN METODI

@petterij 20.4.2018

ITALIALAINEN METODO

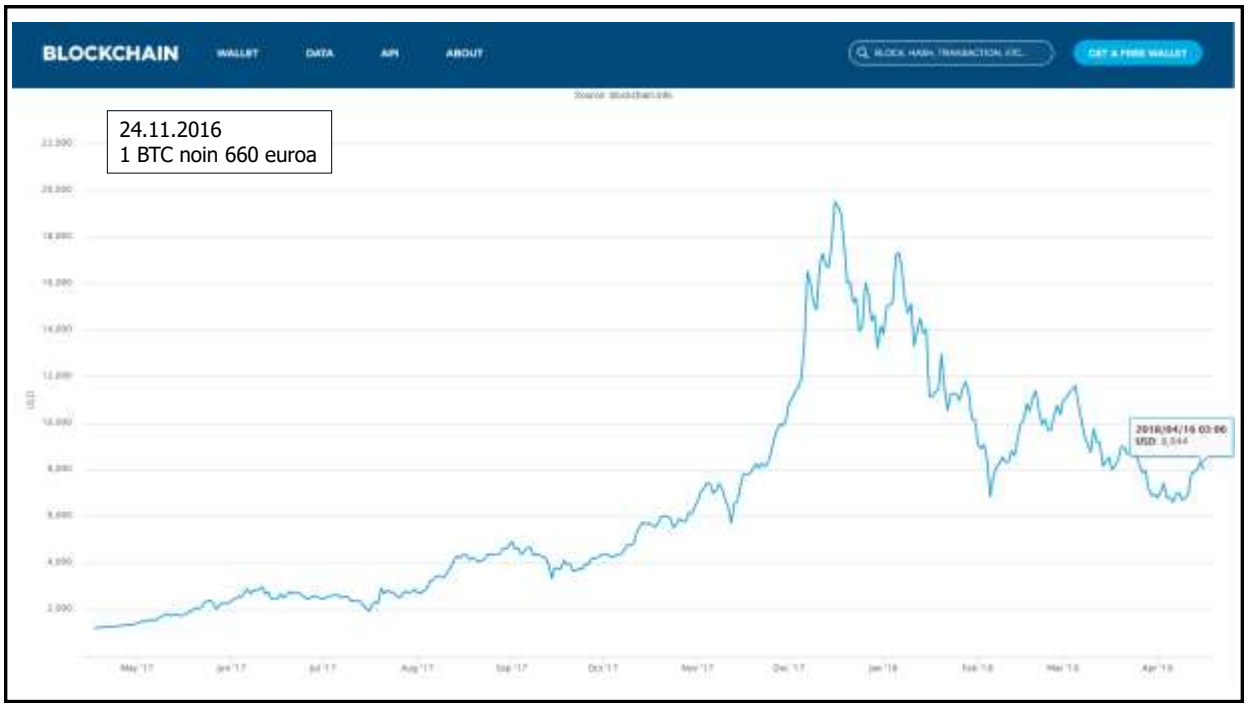
@petterij 20.4.2018

KRYPTOVALUUTAT

- Digitaalinen käteinen
  - (lähes) anonyymi, pienet välityspalkkiot kv-siirroissa (remittance-toiminta)
  - rahaa voi tehdä tyhjästä ”louhimalla” tai ostaa/myydä pörsseissä
  - taustalla lohkoketju tai vastaava teknologia joka ei vaadi luottamusta osapuolten välillä
  - krypto viittaa salaustekniikoihin (cryptography), jolla varmistetaan valuutan aitous, lohkoketjun muuttumattomuus ja estetään double spending
- Ei keskuspankkia
  - arvo määräytyy puhtaasti kysynnän ja tarjonnan perusteella
  - voimakkaat arvonmuutokset, voi mennä nollaan asti
  - käyttäjät toivovat, että säilyttää arvonsa verrattuna FIAT-valuuttoihin
- Houkuttelevat huijareita
  - rahansiirtoja ei voi jäljittää, sopii huumekauppaan ym.
  - osa kryptovaluutoista ja ns. kolikkoanneista (ICO) itsessään huijauksia
  - haittaohjelmat louhivat salaa (case Lahti 2018)

BITCOIN

- Raha ilman pankkeja ja valtioita
  - käyttöön 3.1.2009 nimellisarvo 0,10 dollaria
  - keksijä Satoshi Nakamoto
  - max 21 miljoonaa kappaletta, määrä kasvaa logaritmisesti
  - rahan syntyvauhti puolittuu n. 4 vuoden välein
  - kaikki kurssitasot yhtä perusteltuja, treidaus 24/7
- Todellinen keksintö lohkoketju (blockchain)
  - tiedot rahansiirroista tallennetaan pysyvästi lohkoketjuun
  - proof-of-work estää huijaukset mutta tuhlaa sähköä
  - pankkien väliset rahansiirrot, Teoston muusikkotilitykset
  - koneet voivat maksaa toisilleen automaattisesti, ilman ihmisen tai pankin apua (esim. ylijäämäsähkön myynti omasta tuuli/aurinkovoimalasta)
  - älykkäät ohjelmalliset sopimukset ja prosessit eri osapuolten välillä
  - esim. automaattinen Uber-vastine Arcade (www.arcade.city), jossa palvelun omistavat kuljettajat itse
  - Ethereum, Monero, Litecoin, Zcash…

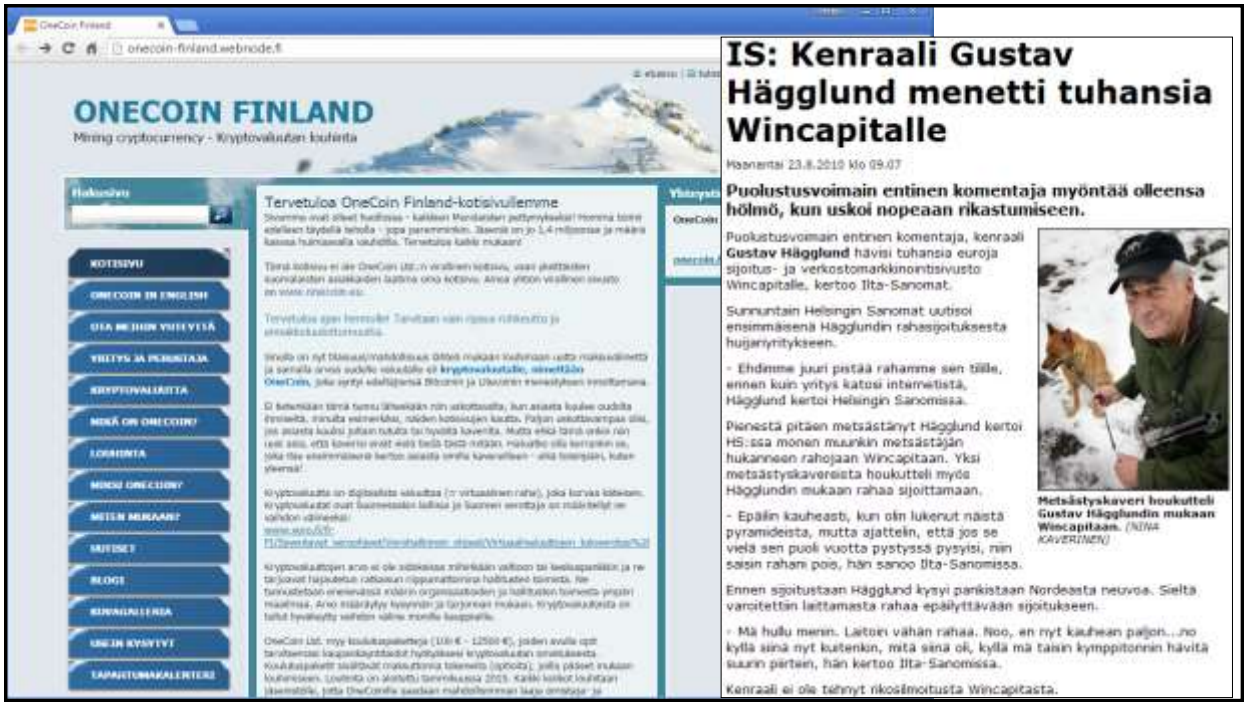


ONECOIN

- Perustaja Ruja Ignatova Bulgariasta
  - suomalaiset verkoston avainpaikoilla
  - maailman ensimmäinen MLM-tilaisuus Suomessa 7.2.2015
- Onecoin-valuutta
  - louhitaan supertietokoneilla salaisissa konesaleissa
  - arvo nousee yhtiön ilmoittamalla tavalla
  - ostetaan ”koulutuspaketteja” 100-5000 euroa, ilmaisilla tokeneilla voi sitten louhia valuuttaa
  - yksityinen (private) lohkoketju
  - kaikkien kolikkomäärät kaksinkertaistettiin 1.10.2016
  - Ruja Ignatova kateissa viime lokakuusta lähtien
  - moni jäsen uskoo yhä olevansa miljonääri
- Ilmoitettu jäsenmäärä nyt 3,3 miljoonaa
  - vetoaminen Bitcoinin esimerkkiin
  - harva edes yrittää ymmärtää kryptovaluutan olemusta, louhintaa tai lohkoketjua
  - suomalaisia n. 30 000?

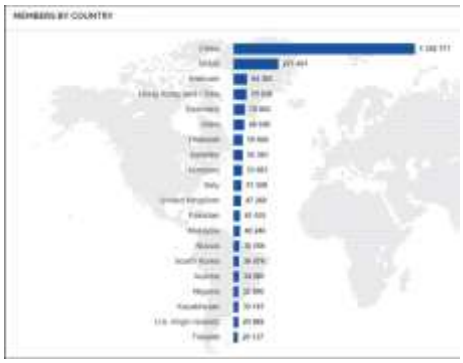
Ruja Ignatova Suomessa, Ylen uutinen 17.2.2015

@petterij



VERKOSTON VOIMA ON PELOTTAVA

- KRP tutki laitonta rahankeräystä syksyllä 2015 ja jäi odottamaan ”lähdekoodin vapauttamista”
- Vaikea todistaa huijaukseksi, kun lupaukset ovat tulevaisuudessa
- Kansainvälinen yhteistyö hankalaa, Bulgaria Euroopan korruptoitunein maa
- Jäsenet markkinoivat omilla sivuillaan ja Facebookissa
- Vetoaa erityisesti helpon rahan etsijöihin
  - mm. ”Kukkaron herraksi” Atte Virtanen
- Jäsenet eivät halua myöntää tulleensa petetyiksi
  - kaveritkin pulassa
- Kuka tekisi rikosilmoituksen… itsestään?



Uhreja etenkin Afrikasta, Kiinasta, Vietnamista…

Osa Wincapitan jäsenistä uskoo yhä valtion kaataneen tarkoituksella liian tuottoisan bisneksen ja jatkaa oikeudellista taistelua. http://pjarvinen.blogspot.fi/2017/04/wincapita-puolustuksen-puheenvuoro.html

@petterij 20.4.2018

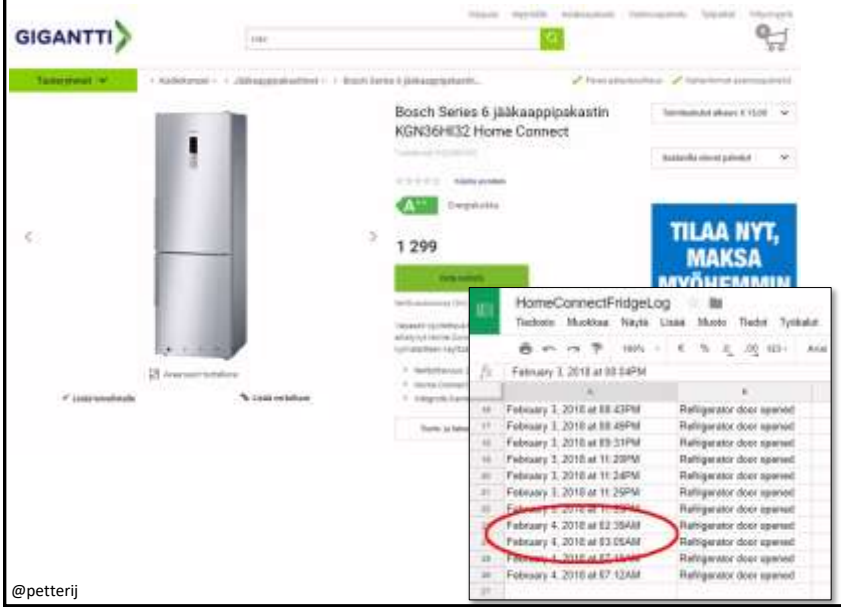
JOHTOPÄÄTÖKSET

- Ihmisten toive helposta rikastumisesta on loputon
- Suomessa saa vapaasti huijata ihmisiä
- Huijareita riittää jatkossakin
- Mitä teknisempi ja vaikeampi systeemi, sitä helpommin se uppoaa ihmisiin
- Osaa ei edes kiinnosta, onko touhu laillista vai ei – kunhan itse ehdin hyötyä siitä
- Katse kohti 8.10.2018 – valuutan pitäisi vihdoin vapautua


Virtuaalikolikkohuijarit keräsivät yli 500 miljoonaa euroa – uhrit rynnistivät toimistoon

@petterij 20.4.2018

ÄLYKOTI JA IOT-LAITTEET



@petterij

Sisällä kaksi kameraa, voi katsoa älypuhelimella

PUHEOHJAUS JA DIGITAALISET AVUSTAJAT

puhekäyttöliittymä inhimillistää tekniikkaa (tai teknistää inhimillisyyttä)
alamme kohdella laitteita ihmisinä (”thank you”) ja ihmisiä laitteina

- Seinilläkin on korvat, jatkossa myös laitteilla
  - Apple Siri, Google Now, Microsoft Cortana
  - tietoturva ja tietosuoja??
- Amazon Echo, Google Home
  - ajureilla (skills) uusia ominaisuuksia
- Mitä nämä osaavat?
  - kysy uutisia tai trivia-tietoja, sääennuste
  - tilaa tuotteita kaupasta, Uber, pizza
  - aseta hälytykset ja muistutukset, kalenteri
  - älykodin puheohjaus (”bedroom lights on”, ”turn small lamp on”)
  - etsi puhelin (”Hey Google, where is my phone”)
  - kysy askeleita, unta tai ilman lämpötilaa
  - käännökset (”how do you say… in Finnish”)
  - soita musiikkia, näytä videoita Chromecastilla

@petterij 20.4.2018

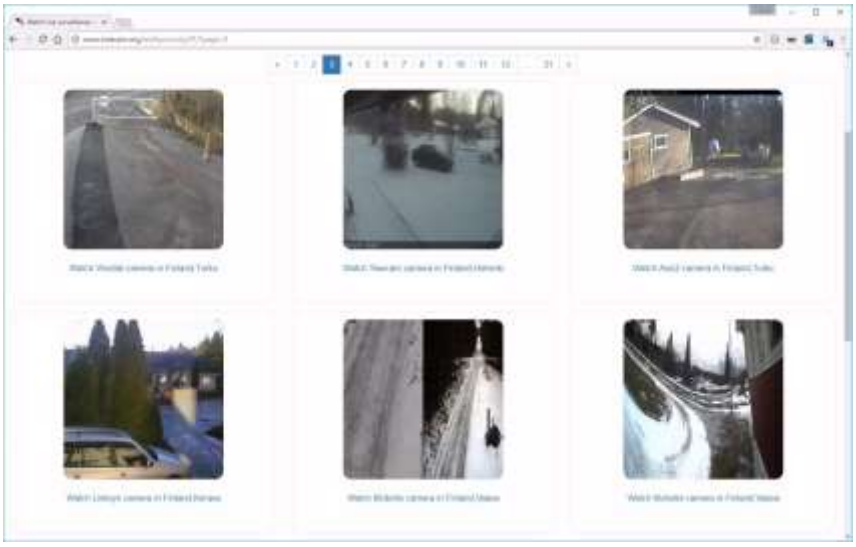
ÄLYKKÄÄT KODINKONEET

- Kodin IoT (Internet of Things)
  - wlan, Bluetooth, Zigbee, Z-Wave, 433…
- Smart == vulnerable
  - aivan uudenlaisia tietoturvaongelmia, kun virus tarttuu kahvinkeittimeen
- Tavallisen perheen hyödyt vs vaiva?
  - älykäs jääkaappi tilaamassa itse ruokaa??
  - päivitykset, tietoturva, tietoliikenneongelmat…
  - onko visio sadoista antureista realistinen?
- Aitoa hyötyä vammaisille ja ikääntyneille
  - myös energiansäästö, ilmanlaadun seuranta, vesi- ja palovahinkojen ehkäisy…
  - graafinen näyttö mahdollistaa havainnollisen käyttöliittymän (esim. Samsung pesukone)

Älyn lisääminen ei ole kustannuskysymys. Jonain päivänä äly lisätään joka tapauksessa käytettiin sitä tai ei.

@petterij 20.4.2018

EIHÄN KOTISI KAMERA OLE TÄSSÄ JOUKOSSA?



http://www.insecam.org/en/bycountry/FI/?page=1

@petterij 20.4.2018

MIRAI-MATO JA IOT-TURVA

- Linux/Mirai-haittaohjelma haittasi DDoSilla nettipalveluita 21.10.2016
  - hyökkäys kohdistui nimipalveluita tarjoavaa Dyn-yhtiötä vastaan
  - mm. Twitter, Spotify, Paypal, Pinterest, Netflix, Airbnb hidastelivat
- Pommituksessa 493 000 IP-osoitetta
  - Webcam-kameroita, DVR-laitteita, itkuhälyttimiä, Wlan-reitittimiä ym.
- Seksilelu paljasti liikaa verkkoon
  - ”Saksalaisen Amor Gummiwaren Vibratissimo Panty Buster -seksilelu naisille osoittautui testissä erittäin reikäiseksi, omistajat joutuvat lähettämään lelunsa valmistajalle korjauksia varten” (IS 20.2.2018)
  - tietokantavirhe mahdollisti käyttäjän tililleen lataamien kuvien varastamisen, ohjaus etäyhteydellä ilman omistajan lupaa ym.
- Tulevaisuuden kiristysohjelmat laitteissa?
  - autot, sähkölukot, kahvinkeittimet…

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345

admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker

Tässä tapauksessa suomalainen *salasana* riittää


HS

Verkkohyökkäys katkaisi kahdesta kerrostalosta lämmöt Lappeenrannassa – "Laajuus ja voima on aika poikkeuksellinen"

Kylmentyneitä kerrostaloja paljastui lisää – hakkerit iskevät lämmitykseen

9.11.2016 Viime viikolla hakkerit häiritsivät kahden kerrostalon lämmitysjärjestelmää palvelunestohyökkäyksellä. Tapauksia on kuitenkin merkittävästi lisää, ja vain osa on havaittu.

Lappeenrannassa hyökkäyksestä kärsivät järjestelmätoimittaja Fidelixin laitteistot. Fidelixin laitteet eivät olleet hyökkäyksen varsinainen kohde vaan välikäsi, jonka kautta pyrittiin ohjaamaan liikennettä hyökkäyksen todelliseen kohteeseen bottiverkon tyypilliseen tapaan.

Iskun vuoksi kiinteistöjen tietokoneet jumittuivat uudelleenkäynnistyskierteeseen, jonka vuoksi niiden takana olleet prosessit pysähtyivät. Tämä johti lämmityksen katkeamiseen.

Fidelixin osastopäällikkö Antti Koskinen tietää, että tapaukset eivät ole ainoita lajissaan.

”Voidaan puhua kymmenistä tapauksista,” Koskinen aloittaa. ”**Osassa tapauksista ei ole ymmärretty miksi laitteet oikuttelevat**. Toisissa taas **hyökkäys on ohi ennen kuin siitä on suoraa haittaa**, koska järjestelmien takana olevat prosessit eivät ole ehtineet kärsiä, jolloin huoltajien huomiokynnys ei ole ylittynyt.”

”Suomessa on kuitenkin **satoja potentiaalisia kohteita** joihin tämänkaltaisia hyökkäyksiä voidaan tehdä.”

”Talotekniikka on hyvästä syystä verkottunut, koska se helpottaa kiinteistöjen ylläpitoa ja esimerkiksi mahdollistaa nopean reagoinnin yllättäviin ongelmiin. Valitettavasti tietoturva ja sen merkityksen hahmottaminen raahaavat perässä,” Koskinen luonnehtii.

”Ongelmana on, että yhteyden saisi turvalliseksi vpn:n avulla, mutta koska se on yksi mutka lisää huoltoprosessiin, usein valitaan se suorempi reitti ja jätetään tahallaan huomioimatta se tietoturvapuoli. Sitä ei pidetä niin merkittävänä, ja nyt se helpon tien valitseminen kostautuu,” Koskinen selventää.

”Tilanne on kuitenkin selkeästi paranemassa. Kiinteistöalalla on ryhdytty toimenpiteisiin jo vuosia sitten, ja nykyisin myydään vain suojattuja yhteyksiä, ellei asiakas syystä tai toisesta erikseen toisin halua. Viestintäviraston Kyberturvallisuuskeskuksen kanssa ollaan luotu ohjeistusta siihen, miten kiinteistöjen tietoturva pidetään mielessä heti alusta asti,” Koskinen kertoo.

www.tivi.fi/Kaikki_uutiset/kylmentyneineita-kerrostaloja-paljastui-lisaa-hakkerit-iskevat-lammitykseen-6598148

KOTILAITTEIDEN TIETOTURVA

- Älä osta halvinta kiinalaismerkkiä
- Tee asennus loppuun asti - se, että laite toimii, ei vielä riitä!
- Määritä oma käyttäjätunnus ja salasana
- Sammuta laitteet säännöllisesti (tyhjentää muistin)
- Älä kytke nettiin, jos ei tarvitse (esim. äly-tv)
- Tarkista säännöllisesti firmware-päivitysten saatavuus
- Testaa verkon ulkopuolelta
- Tiedätkö mitä laitteita kotiverkossasi on ja miten paljon dataa ne lähettävät ulos?
- Hanki kodin IoT-palomuuri (F-Secure Sense, Bitdefender Box)

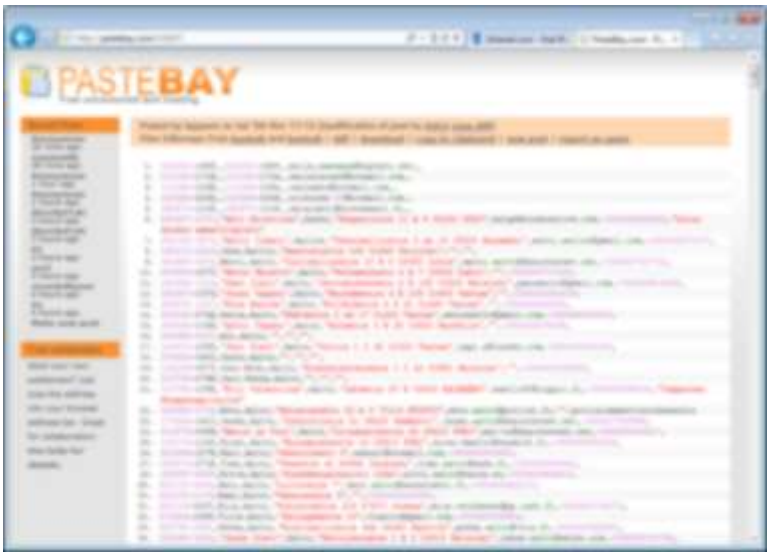
Fing-verkkoanalysaattori

SMARTER COFFEE

- Kahvimylly ja kahvinkeitin yhdessä
  - ohjaus painikkeilla tai älypuhelimella
  - kolme vahvuutta
- Kiva idea mutta…
  - suodatinpaperi pitää kuitenkin vaihtaa etukäteen, tämä ei ole kahviautomaatti
  - vesisäiliö pitää muistaa täyttää
  - carafe detection pakko kytkeä pois toiminnasta
  - verkkoasennus hankala

NÄIN PÄIVITÄN KAHVINKEITTIMENI…

20.4.2018



"Tässä vaiheessa on vaikea sanoa, miten vakava tästä tietovuodosta tulee. Se riippuu siitä, miten useiden tuhansien ihmisten henkilötietoja käytetään väärin – vai käytetäänkö ollenkaan", rikoskomisario XX Keskusrikospoliisista sanoo. Hänen mukaansa vuoto voi myös mennä ohi ilman mitään väärinkäytösrypästä. "Henkilökohtaisesti en huolestuisi nimen listallaolosta mahdottomasti". (HS 5.11.2011) – uhreille ei ilmoitettu asiasta.

HETUDUMP

- Hetudump.txt vuodettiin nettiin 5.11.2011: 16 103 ihmisen hetu, koko nimi, osoite, sähköposti, puhelin
- Tietoja mm. Itä-Suomen yliopiston ja Työtehoseuran järjestelmistä
- Päivitysten puuttuminen ainakin osasyy tietomurtoon
- Hakkeri- ja aktivistiryhmä Anonymous Finland ilmoitti olevansa tietovuodon taustalla
- Syyteoikeus vanheni 2016, epäilty suomalainen tekijä asui ulkomailla eikä riittävän vahvoja todisteita luovutuspyyntöön ollut
- **Tiedoilla tehdään identiteettivarkauksia vielä nykin**
- Ilmeisesti paransi tietoturvaa, koska yhtä isoja vuotoja ei sen jälkeen enää ollut

20.4.2018


asiakastieto.fi

TODISTUS

SUOMEN ASIAKASTIETO OY

SUOMEN ASIAKASTIETO OY

OMA LUOTTOKIELTO

http://pjarvinen.blogspot.fi/2017/11/oma-luottokielto-tuo-lisasuojaa.html

Pidä hyvää huolta ajokortista ja kela-kortista!

Asiakastieto 20 eur, Bisnode ilmainen


omatieto.fi

20.4.2018

KIRISTYSOHJELMAT 2017

- WannaCry (Wannacrypt0r)
  - 12.5.2017 uhreina n. 200 000 konetta: Telefonica, FedEx, erit. National Health Service
  - uutta: matomainen leviäminen sisäverkossa yhdistettynä kiristysohjelmaan
  - tappokytkimen löytyminen pysäytti epidemian
  - käytti NSA:n löytämää EternalBlue-haavoittuvuutta (SMB), jonka Microsoft korjasi 14.3.2017 julkaistulla päivityksellä MS17-010 (Windows Vista, 7, 8, 10, Server 2008-2016)
  - Shadow Brokers paljasti haavoittuvuuden 14.4.2017
  - XP- ja Server 2003-korjaukset oli tehty, mutta ei aluksi jaettu; osuus epidemiassa pieni
  - lunnasvaatimus 300-600 dollaria, uhreja erityisesti Intia, Venäjä, Ukraina, Taiwan
  - Suomessa noin sata uhria
- Petya
  - alkuperäinen Petya maaliskuussa 2016 (James Bondin Golden Eyen mukaan?)
  - NotPetya-isku 27.6.2017 Ukrainan perustuslain päivän aattona M. E. Doc talousohjelman mukana
  - sama EternalBlue + salasanojen kerääminen sisäverkosta ym. tekniikoita
  - lunnaat 300 dollaria kiinteään Bitcoin-osoitteeseen – ei voida erotella maksajia
  - yhteystietona ilmaispalvelun sähköpostiosoite, joka ei ollut käytössä
  - salaus vain hämäystä, ei voida palauttaa edes avaimella
  - uhreina Ukrainan valtionpankki, Tsernobylin säteilynvalvontajärjestelmä ym.
  - samana aamuna surmattiin autopommilla Ukrainan tiedustelun eversti Maksim Šapoval

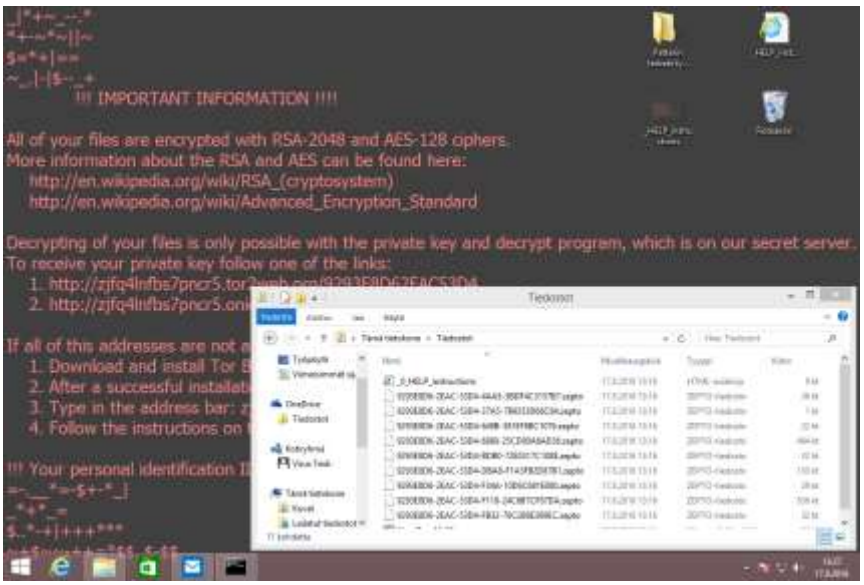
@petterij 20.4.2018

KIRISTYSOHJELMAT

- Salakirjoittavat työtiedostot ja vaativat rahaa
  - CryptoWall, CryptoLocker, TeslaCrypt, KeRanger (OS X), WannaCry, Locky (ei iske venäläisiin koneisiin), Zepto, Odin -- yli 100 haittaohjelmaperhettä
  - salaus todellinen (AES), ei voi yleensä murtaa ilman avainta
  - selaimissa myös vaarattomia lukitussivuja, syyttävät rikoksesta ja vaativat maksamaan sakon (”poliisivirus”)
  - maksuvaluuttana yleensä Bitcoin
- Kiristys on hyvä bisnes
  - www.nomoreransom.org
- CyberEdgen selvityksessä 55 % kertoi organisaationsa joutuneen kiristyshaittaohjelman uhriksi vuonna 2017
- 61 % päätti olla antamatta periksi, heistä 8 % menetti tietonsa pysyvästi, 53 % onnistui palauttamaan datan
- Lunnaat maksoi 39 % vastaajista, 19 % heistä onnistui palauttamaan tietonsa, loput 20 % menettivät tiedostonsa (ei purkuavainta tai se ei toiminut)
- CyberEdgen selvityksestä käy ilmi, että 28 % menetti tietonsa pysyvästi, joko maksamalla vaaditut lunnaat tai pidättäytymällä niiden suorittamisesta
- Siis vähän alle puolet maksaneista sai tiedot takaisin
- 2-12/2017 kiristysohjelmia havaittiin vähiten Suomessa, Japanissa ja USA:ssa, keskimäärin vain 0,03 % Windows-työasemista

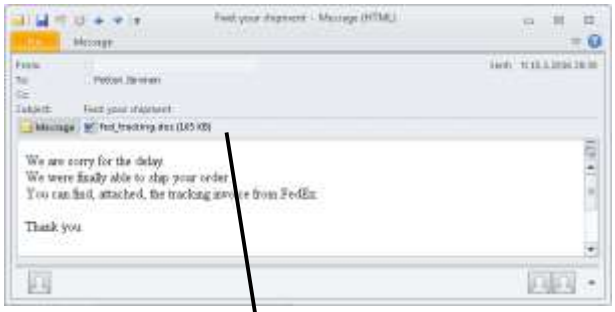
@petterij 20.4.2018

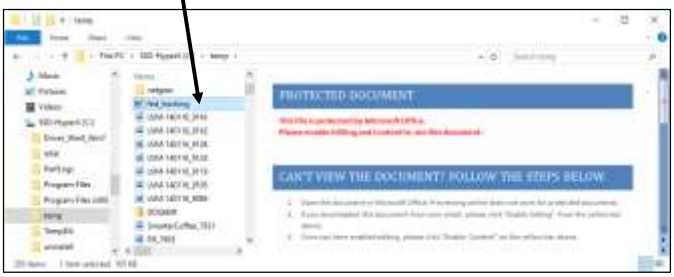
NÄYTÖN TAUSTAKUVA VAIHTUU



@petterij 20.4.2018

VARO WORD/EXCEL-LIITETIEDOSTOJA





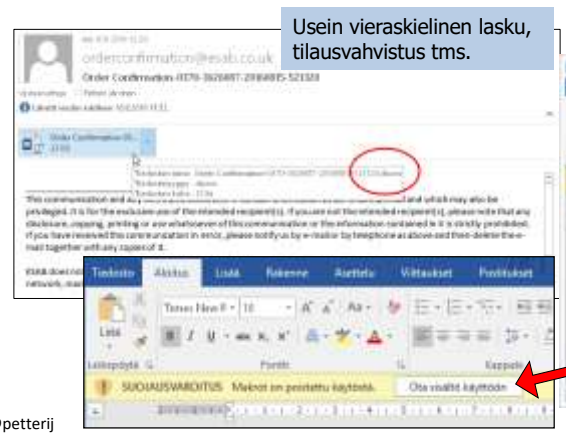
- Avaa Google Docsissa tai älypuhelimella
- Älypuhelin ei aja makroja eikä avaa vaarallisia liitteitä

@petterij

DOKUMENTTIEN MAKROT VAARALLISIA

Tiedostopääte	Sovellus	Makroja
.DOC	vanha Word	voi sisältää makroja
.DOCM	Word 2007 ja uudemmat	sisältää makroja
.DOCX	Word 2007 ja uudemmat	ei sisällä makroja

Vastaavasti Excel .XLS, .XLSM, .XLSX ja Powerpoint (.PPT, .PPTM, .PPTX)



”Enable Content = Infect my computer”

@petterij 20.4.2018


Kiitos!