

**Parhaan käytännön nimi:** Teknisten “alustavikojen” ennaltaehkäiseminen ja “ehkäisyvälineiden” toimittaminen koko kansalle.

**Yrityksen/yhteisön nimi:** Jussi & Petri

**Yhteyshenkilö:** Petri Kuivala tai Jussi Jaakonaho

**Osoite:**

**Sähköpostiosoite:** [petri.kuivala@iki.fi](mailto:petri.kuivala@iki.fi) tai [jussij@gmail.com](mailto:jussij@gmail.com)

**Puhelin:** 050-487 6723 (Jussi)

**Osallistuminen:** Osallistumme Parhaat käytännöt -kilpailuun ja haluamme, että käytäntöämme esitellään tietoyhteiskuntaohjelma.fi-sivuilla

**Ilmoitamme käytäntömme kilpailusarjaan:** Tietoturvan edistäminen ja soveltaminen

### ***Haaste:***

Tietoturvallisuusohjelmistojen toimittajat korjaavat ohjelmistoissa olevia teknisiä (yleensä käyttöjärjestelmissä, mutta myös muissa ohjelmistoissa) ongelmia retroaktiivisesti. Käytännössä tämä tarkoittaa sitä, että uusin ”reikä” eli haavoittuvuus on aina jonkin aikaa matojen tms. käytettävissä. Kyseinen ongelma on kasvanut viimeisten vuosien aikana, kun haavoittuvuuksia hyväksi käyttävät haittaohjelmat ilmestyvät ”markkinoille” todella nopeasti haavoittuvuuden löytymisen jälkeen ja siten tietoturvallisuusohjelmistot eivät välttämättä ehdi kaikkien koneille ennen kuin koneita jo käytetään hyväksi. Joskus nämä haavoittuvuudet ovat käytettävissä hyvinkin pitkän ajan rajoitetun (krakkeri) piirin käytössä. Jos ja kun krakkeripiiri käyttää haavoittuvuutta pienimittaisesti esim. vakoiluun tms. toimintaan, jonka kohteena on vain muutamia käyttäjiä tai yhteisöjä eivät tietoturvallisuusohjelmistojen / käyttöjärjestelmäpaikkausten toimittajat tule tietoiseksi ko. haavoittuvuudesta pitkään aikaan. Samoin haittaohjelmien teko on yllättävänkin nopeata vaikka sen teko perustuisi julkiseen informaatioon, eräiden otantojen mukaan julkisesta informaatiosta haittaohjelman tekeminen onnistuisi jopa tunnissa. Tämä tuo haasteita varsinkin suojautumispuolelle ennaltaehkäisevään toimintaan.

### ***Tekninen ratkaisu:***

Kyseistä ongelmaa ei voi poistaa kokonaan, mutta todennäköisyyttä joutua vahingon kärsijäksi voidaan merkittävästi pienentää tekemällä ns. käyttöjärjestelmän kovettaminen ”hardening”. (Kyseessä ei ole teknisesti uusi ratkaisu – uutuus selostetaan seuraavassa kappaleessa). Hardening tarkoittaa lyhyesti käyttöjärjestelmän/ohjelmistojen konfiguroimista siten, että uusi haavoittuvuus ei käytännössä toimi, tai sen hyödyntäminen vaikeutuu. Käytännössä haittaohjelmat tai krakkerit eivät pysty väärinkäyttämään hardenoidun koneen resursseja vaikka siihen ei olisi vielä asennettukaan uusimpia haavoittuvuuksien paikkauksia (Patchejä).

Tyypillinen haittaohjelma toimii siten, että poikkeamatilanteen<sup>1</sup> sattuessa se pyrkii käyttämään hyväkseen kohdesovelluksen/käyttöjärjestelmän omia toimintoja.

---

<sup>1</sup> Poikkeamatilanne = kun haittaohjelma saa aikaan tilanteen, jossa se suorittaa oman ohjelmansa normaalin ohjelman sijasta.

***Käytännön tekninen esimerkki helposti korjattavista teknisistä ongelmista:***

Tyypillisesti MS Windowsin tapauksessa suoritettavat ohjelmat kuten: cmd.exe, tftp.exe, ftp.exe jne, ja Unix-pohjaisissa komentotulkki<sup>2</sup> sallivat oletusarvoisesti ko. ohjelmien suorituksen tunnuksilta, joita tyypilliset haittaohjelmat käyttävät. Esim Windowsin tapauksessa tyypillisesti haittaohjelma ottaa ns. System – oikeudet.

***Käytännön tekninen esimerkkejä korjauksesta:***

Jos System tunnukselle asetettaisiin ns. Deny Access – oikeudet edellä mainittuihin tiedostoihin niin haittaohjelma ei pysty käynnistämään niitä, ja tämä estää haittaohjelman leviämisen.

Windowsin suojauslistoissa voidaan myös käyttää ryhmä-tunnuksia, joihin haittaohjelman suoritusvaiheen tunnuksen konteksti ei kuulu esim. ”INTERACTIVE”.

***Uutuus:***

1. Ficoran tietoturvaluusyksikkö julkaisee jo tänäpäivänä tietoja merkittävimmistä haavoittuvuuksista ja puolustuksesta niitä vastaan. Toiminta on mielestämme kuitenkin hyvin retroaktiivista ja teknologia ”nörtti” suuntautunutta.
2. Ficoran tietoturvaluusyksikkö kerää jo tietoja siitä miten koneita voitaisiin hardenoida, mutta jostakin syystä näitä ohjeita tai puhumattakaan automaattisista ”skripteistä” ei ole suuren yleisön / yritysten saatavilla.
3. Ehdotamme, että Ficoran tietoturvaluusyksikkö:
  - a. Pitäisi ainakin puolivuositaisissa päivän parin mittaisia seminaareja valtakunnan ykköstietoturvaluusietäjien kanssa, jossa he laatisivat eri käyttöjärjestelmille, sekä käyttöä varten valmiita helposti käytettäviä hardeningohjeistuksia ja -skriptejä.
  - b. Tekisivät analyysin siitä miten ko. skriptit voivat vaikuttaa tietokoneen tavalliseen käytettävyyteen (tavoite tulee olla, ettei mitenkään) ja tekevät lyhyen e.g. flash<sup>3</sup> videon, joka selittää ko. vaikutukset.
  - c. Levittää ko. skriptejä ja videoita tavallisille käyttäjille Suomalaisten ISP:iden kautta (ISP:iden help deskit pitäisi valjastaa auttamaan). Tämä voi aiheuttaa pieniä lisäkustannuksia ISP:ille, mutta he saavat taatusti ko. kustannukset takaisin säästyneinä tietoliikenne tms. kustannuksina kun näiden skriptien käyttämisestä tulee osa normaalia suomalaista yhteiskunnallista toimintaa.

---

<sup>2</sup> Komentotulkki = esim: /bin/sh

<sup>3</sup> Flash viedo = Jokaisessa tietokoneessa toimiva standardi video formaatti. Formaatin etu on siinä, ettei videon levittäjän tarvitse huolehtia siitä, että loppukäyttäjällä eli katselijalla on oikeanlainen katseluohjelmisto.

### ***Rahallinen hyöty yhteiskunnalle:***

Yllämainitu ongelma:

- a) Kuluttaa ISP:eiden verkkokapasiteettia
- b) Kuluttaa ISP:iden help desk - resursseja, koska ihmiset soittavat niihin ensimmäisenä kun ”koska verkko ei toimi”
- c) Hidastaa tai jopa estää yksiköiden ja yhteisöjen tietokoneiden toimintaa.
- d) Tuhoaa ja muuttaa yksilöiden ja yhteisöjen tietoja, vaikeuttaen päätöksentekoa.
- e) Aiheuttaa IRP omaisuuden ja yksityisyyden suojan piiriin kuuluvine tietojen vuotamista tahoille, joille ko. omaisuus / tiedot eivät kuulu.

Kuten alussa mainitsimme ongelmaa ei voida kokonaan poistaa, mutta laajamittaisesti käytetyn hardenoinnin on arvioitu vähentävän näitä ongelmia jopa 85 %<sup>4</sup>, tärkeintä kuitenkin on katsoa että mitä suojataan ja miltä suojaudutaan, eli olemassa olevia ohjeistuksia ei sinänsä pyrittäisi kopioimaan vaan muokkaamaan siten että toiminnallisuus säilyisi ja tietoturvan taso nousisi.

### ***Pari sanaa ideoijista:***

<b>Petri Kuivala</b>	<b>Jussi Jaakonaho</b>
Toimii Nokia Oyj:n yritysturvallisuusyksikön Kiinan vetäjänä. Ennen tätä hän on toiminut mm. Tietoturvallisuus teamin vetäjänä Nokia Oyj:ssä sekä aiemmassa työssään Helsingin poliisilaitoksella toiminut tietotekniikkarikostutkijana.	Toimii Nokia Oyj:n operatiivisessa tietoturvallisuusyksikössä johtavana asiantuntijana. Ennen tätä hän on toiminut mm. vanhempana tietoturvakonsulttina Defcom MSSP:ssä, sekä globaalina palvelinverkon ylläpitäjänä Digital Equipment Corporation:lla. Harrastuksena hänellä on luennoita suljetuissa, ja avoimissa tietoturvatapahtumissa ympäri maailmaa.

<sup>4</sup> NSA:n arvio vuodelta 2000. Löysimme vain ko. tutkimukseen viittaavia lähteitä:

<http://www.sans.org/onsite/description.php?tid=297> ja

<http://www.panurgvvt.com/pdf/outlines/microsoft/MSSecToolsTech.pdf>