

## Tällainen on Microsoftin lahja Vantaan poliisille

13.5.2008 16:10 — Aleksis Moisio [aleksi.moisio@sanoma.fi](mailto:aleksi.moisio@sanoma.fi)

It-viikko tutustui todisteidenkeruuohjelmaan, jota Microsoft jakaa usb-tikuilla eri maiden poliiseille. Vantaan poliisin it-rikosryhmä on käyttänyt ohjelmaa jo vuoden päivät.

Rikollinen käyttää yhä useammin tietokonetta rikoksensa tekemiseen. Siksi myös todistusaineisto rikoksesta muodostuu monissa tapauksissa ykkösistä ja nolista.

Tämä on ongelma poliisille. Se painii alati paisuvien rikosteknisten todistemäärien kanssa.

Esimerkiksi Itä-Uusimaan aluetta palveleva Vantaan kihlakunnan poliisilaitoksen kolmihenkkinen it-rikosryhmä tutki viime vuonna 20 teratavua todistusaineistoa.

Käsiteltävän todistusaineiston määrä moninkertaistuu joka vuosi. Tänä vuonna todistusaineistoa on kertynyt jo 10,8 teratavun edestä.

Näin kertoo yksikköä johtava rikosylikonstaapeli **Jari Javanainen**. Hän kertoo, miten ohjelmistoyhtiö Microsoftin poliisilaitoksille lahjoittama Cofee-ohjelma (Computer Online Forensic Evidence Extractorin) toimii.

Hongkongin poliisille työskennelleen **Anthony Fungin** kehittämä [Cofee-ohjelmaa esiteltiin 350 poliisille](#) huhtikuun lopussa Microsoftin päämajassa Redmondissa.

Paikan päällä olleen Javanaisen mukaan kyseessä on Windows-sovellus, joka on tarkoitettu helpottamaan ja nopeuttamaan poliisien todisteiden keräämistä.

Graafinen ohjelma koostuu 150:stä komentokehotteen puolella suoritettavasta käskystä, jotka keräävät tietoa käynnissä olevan tietokoneen toiminnasta, prosesseista, verkkoyhteyksistä ja niin edelleen. Ohjelma voidaan asentaa esimerkiksi usb-tikulle tai cd-levylle.

### Todisteiden kerääminen kuluttaa it-poliisin resursseja

Kun tieto ohjelman olemassaolosta päätyi julkisuuteen, [tietokoneharrastajat heräsivät](#)

---

Moni pelkää Microsoftin luoneen salaovia suosittuun Windows-käyttöjärjestelmään. Monen mielikuvissa Cofee on vaarallinen tiirikka, joka väärin käsiin päätyessään saa aikaan valtavasti tuhoa.

Javanaisen mukaan pelot ovat kuitenkin ylimitoitettuja.

- Cofee itse ei tee mitään mullistavaa. Se vain nopeuttaa ja helpottaa todisteiden keräämistä, hän sanoo.

Juju on tämä. Alati yleistyvät tietomurrot, bottiverkot ja muu tietotekniikkarikollisuus työllistävät it-yksikköä. Nykyisellään rikospaikalle pitää lähettää tehtävään koulutettu poliisi. Tavoite on, että ainakin osa näistä tehtävistä voitaisiin antaa Poliisikoulusta valmistuneelle rivikonstaapelille.

Javanainen toivoo, että Cofeen ansiosta hänen ei tarvitse lähettää yhtä kolmesta miehestään kentälle.

Rikosylikonstaapeli istuu keskellä pöytäkoneiden, kannettavien, palvelinten ja johtojen täyttämää huonetta ja napauttaa auki MacBook Pro -kannettavan. Siinä hyrrää Windows XP.

Javanainen kirjautuu sisään, tökkää usb-tikun kiinni ja napsauttaa Cofeen konfigurointiin tarkoitetun ohjelman kuvaketta. "Process id=0x9ac"-virheilmoitus pomppaa esiin.

Paljon pelätty "vakoilulaite" toimii, kuten moni muu ohjelma: satunnaisesti.

### **Ohjelma ei murra salasanoja**

Vaikka Cofeen konfigurointityökalu kieltäytyy käynnistymästä, ohjelma kuitenkin todistettavasti toimii.

Javanainen sanoo yksikkönsä käyttäneen ohjelmaa kahdessa tapauksessa.

Ohjelma suorittaa poliisin määrittelemät käskyt ja kerää näiden tuottamat tiedot kollaboratiiviseen raporttiin.

Javanainen esittelee raporttia, johon Cofee on kerännyt tietoja muun muassa koneen verkkoliikenteestä, siihen asennetuista ohjelmista ja niiden asetuksista.

Toisin kuin verkkokeskusteluissa on huhuttu, ohjelma ei osaa Javanaisen mukaan murtaa yhtäkään salasanaa.

Jos rikollinen on jättänyt koneensa auki ja lukinnut Windows-käyttöjärjestelmän, Cofee on voimaton. Ainakin

---

tehdasasetuksilla.

Poliisilla on kuitenkin omat keinonsa päästä salasanojen ohitse joissain tapauksissa. Kun rikosepäily kohdistuu yrityksen työntekijään, poliisi saa salasanan yleensä järjestelmän ylläpitäjältä.

Se, mitä tietoja poliisi saa tutkinnassaan kerätä, määritellään laissa. Esimerkiksi ip-verkon ylitse välittyvien puheluiden salakuuntelemiseen poliisi tarvitsisi erilliset luvat.

Javanainen ei ole huolissaan siitä, että ohjelma saattaa päätyä väriin käsiin.

- En näe sitä, miten Cofee kääntyisi hakkerityökaluksi. Eihän se tee mitään uutta, Javanainen sanoo.

Kunhan Cofeen käyttökoulutus on aloitettu ja ohjelma on konfiguroitu suomalaiseen rikostutkintaan sopivaksi, it-rikosyksikkö toivoo sen käytön yleistyvän poliisissa.

- Yhteistyö väkivaltarikosyksikön kanssa on jo aloitettu, Javanainen sanoo.

<http://www.digitoday.fi/tietoturva/2008/05/13/tallinen-on-microsoftin-lahja-vantaan-poliisille/200813134/66>