

**CERT-FI**

**TIETOTURVAKATSAUS 1/2010**

9.4.2010

# CERT-FI tietoturva- katsaus 1 / 2010

## Johdanto

Älypää-pelisivustolta maaliskuussa varastettujen käyttäjätietojen julkaiseminen vaaransi palveluun rekisteröityneiden käyttäjien tietoturvallisuuden. Yli 125 000 käyttäjätunnusta, salasanaa ja sähköpostiosoitetta julkaistiin internetissä.

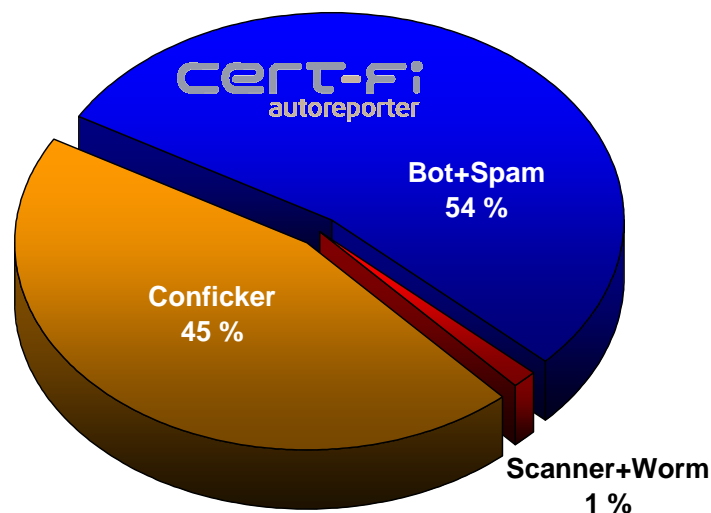
Helmikuussa kävi ilmi, että helsinkiläisen kahvilan murretusta tietokoneesta oli viety yli 100 000 luottokortin tiedot.

Palvelujen tietoturvalliseen toteuttamiseen tulisi kiinnittää enemmän huomiota. Turvattomasti toteutettujen palvelujen kautta voidaan varastaa käyttäjien salasanoja ja syötetty luvattomasti sisältöä www-sivustoille. Myös käyttäjien salasanakäytännöissä on toivomisen varaa. Liian helpot ja monissa eri palveluissa käytetyt salasanat lisäävät väärinkäytösten riskiä.

Verkkopankkiyhteyksiä häiritsevät haittaohjelmat toimivat jo suomalaistenkin verkkopankeissa. Pankit ovat ottamassa käyttöön lisävarmistuksia luvattomien tili-siirtojen torjumiseksi. Toistaiseksi verkkopankkiyhteyksiä kaappaavien haittaohjelmien määrä Suomessa on vähäinen.

CERT-FI:n Autoreporter-järjestelmän tilastotiedoista käy ilmi, että haittaohjelmahavaintojen määrä kasvoi vuonna 2009 selvästi edellisvuodesta. Lähes puolet kaikista haittaohjelmiin liittyvistä ilmoituksista johtui Conficker-verkkomadosta. Vuoden 2009 aikana CERT-FI lähetti lähes 100 000 ilmoitusta Conficker-haittaohjelmatartunnoista.

## Haittaohjelmahavainnot tyypeittäin 2009



Conficker vastasi yksin lähes puolesta kaikista vuoden 2009 haittaohjelmailmoituksista.

## **Älypää-pelisivuston salasanoja levitettiin julkisesti**

Maaliskuun lopulla tuli ilmi tapaus, jossa alypaa.com-pelisivustolta oli onnistuttu varastamaan käyttäjätunnukset, salasanat ja palveluun rekisteröityessä käytetyt sähköpostiosoitteet.

Yli 125 000 käyttäjän tiedot sisältävä tiedosto oli saatavilla useiden tiedostonjakopalvelujen kautta, ja tieto siitä levisi nopeasti internetissä.

Älypää-sivustolle kirjautuminen estettiin nopeasti, mutta käyttäjien tietoturvasuus vaarantui myös sen vuoksi, että monet olivat käyttäneet samaa salasanaa muissakin verkkopalveluissa. Sähköpostiosoitteen perusteella saattoi useissa tapauksissa päätellä käyttäjätunnuksen ja kokeilla sen jälkeen Älypää-palvelusta varastettua salasanaa.

CERT-FI:n tietoon on tullut esimerkiksi käyttäjän Gmail-sähköpostitilin tai Facebook-tunnusten luvattonta käyttöä.

### **Salasanoissa toivomisen varaa**

Käyttäjätunnus ja salasana ovat yleisin tapa varmistua käyttäjän henkilöllisyydestä verkkopalveluissa. Salasanojen valintaan ja säilyttämiseen tulisikin kiinnittää nykyistä enemmän huomiota.

Älypää-palvelusta varastettujen salasanojen tarkastelu osoittaa, että joukossa on aivan liian helposti arvattavia tai lyhyitä salasanoja. Saman salasanan käyttämistä eri palveluissa tulisi välttää ja varautua siihen, että minkä tahansa palvelun salasana voidaan murtaa tai se voi muulla tavoin joutua väärin käsiin.

### **Palvelun toteutuksessa puutteita**

CERT-FI:n tietojen mukaan Älypää-palvelun salasanojen urkkimisessa on voitu käyttää hyväksi palvelun vanhentunutta ja tietoturvasuudeltaan puutteellista toteutusta.

Salasanat ovat ilmeisesti olleet selväkielisinä palvelun taustajärjestelmän tietokannassa. Tietokantaan on voitu päästä käsiksi ns. *SQL injection* -tyyppisen puutteelliseen syötteentarkistukseen perustuvan haavoittuvuuden kautta.

## **Poliitikkojen verkkosivuja töhritty**

Maaliskuussa tuli tietoon joitakin tapauksia, joissa julkisuuden henkilöiden www-sivustoille oli syötetty luvattomasti sisältöä.

CERT-FI:n tietojen mukaan tapauksissa käytettiin sivujen ylläpitäjän salasanaa, joka oli joko pystytty arvaamaan tai hankittu tietoon muulla tavoin. Sivuja oli muokattu niiden normaalin ylläpitökäyttöliittymän avulla.

### **Puutteellinen syötteentarkastus voi mahdollistaa tietovuodot tai töhrimisen**

Yhä useamman www-palvelun taustalla on tietokanta, jota hallitaan SQL-kielillä komentolauseilla. Niiden avulla tietokannasta voidaan hakea tietoja tai muokata niitä.

Tietokanta voi sisältää sivujen sisällön, palveluun liittyvät käyttäjätunnukset ja salasanat tai tietoja, joiden avulla käyttäjille näkyvät sivut muodostetaan. Tietokantaan voi päästä käsiksi esimerkiksi sivustolla olevan www-lomakkeen tai sivun URL-osoitteen kautta.

Jos käyttäjältä tulevaa syötettä ei tarkasteta riittävän huolellisesti, voidaan tietokannalle syöttää komentoja, jotka mahdollistavat tietojen etsimisen tai sivujen luvattoman muokkaamisen. Salasanoja ei pitäisi koskaan säilyttää järjestelmässä selväkielisinä.

CERT-FI:n tietoon tulee jatkuvasti tietoja eri sivustoihin liittyvistä SQL injection -tyyppisistä haavoittuvuuksista. Haavoittuvuuksien etsimistä ja niiden toimivuuden kokeilemistä varten on yleisesti saatavilla valmiita ohjelmia eikä niiden käyttäminen vaadi erityisen suurta asiantuntemusta.

### **Tietoja varastetaan myös haittaohjelmien avulla**

Helsinkiläisen kahvilan palvelimelta vietiin helmikuussa yli 100 000 asiakkaan luottokorttinumerot. Luottokorttinumerot ovat tietoja varastavien haittaohjelmien tavalisinta saalista. Korttinumeroita voidaan käyttää ostoksiin tai kaupata edelleen rikollisiin tarkoituksiin.

## Haittaohjelmahavainnot entistä enemmän vuonna 2009

CERT-FI:n julkaisemat Autoreporter-järjestelmän tilastotiedot<sup>1</sup> vuoden 2009 haittaohjelmahavainnoista osoittavat, että niistä tehtyjen ilmoitusten määrä on kasvanut selvästi edellisvuodesta.

Havaintojen määrän kasvuun on vaikuttanut erityisesti Conficker-nimellä tunnettu verkkomato, joka levisi voimakkaasti erityisesti vuoden 2009 ensimmäisellä puoliskolla.

Vuoden aikana tehdyistä haittaohjelmahavainnoista peräti 45 % johtui pelkästään Conficker-haittaohjelmasta. Yksi prosentti liittyi tietomurron valmisteluun ja loput 54 % tarkemmin erittelemättömiin botnet-tyyppisiin haittaohjelmiin, joita käytettiin esimerkiksi roskapostin lähettämiseen.

Koska myös Confickeria voidaan pitää botnet-tyyppisenä haittaohjelmana, on helppo todeta, että bottiverkkoihin liittyvät haittaohjelmahavainnot ovat vienneet lähes kaiken huomion.

Vuoden 2009 aikana CERT-FI on lähettänyt lähes 100 000 ilmoitusta Conficker-haittaohjelmahavainnoista. Vuoden aikana on havaittu haittaohjelmataruntoja yli 25 000 suomalaisessa IP-osoitteessa.

## CERT-FI pyrkii tavoittamaan haittaohjelmakroonikkoja

CERT-FI:n havaintojen mukaan samat osoitteet esiintyvät usein haittaohjelmatarunnasta kertovissa ilmoituksissa toistuvasti.

Muun muassa Conficker-haittaohjelman levinneisyyden vuoksi CERT-FI on loppuvuodesta 2009 lähtien pyrkinyt ottamaan aktiivisesti yhteyttä niiden koneiden haltijoihin, joiden osoitteet esiintyvät haittaohjelmatarporteissa jatkuvasti. Kuluvaan vuoden aikana pyritään edelleen aktiivisesti tavoittamaan jatkuvasti haittaohjelmista kärsiviä käyttäjiä.

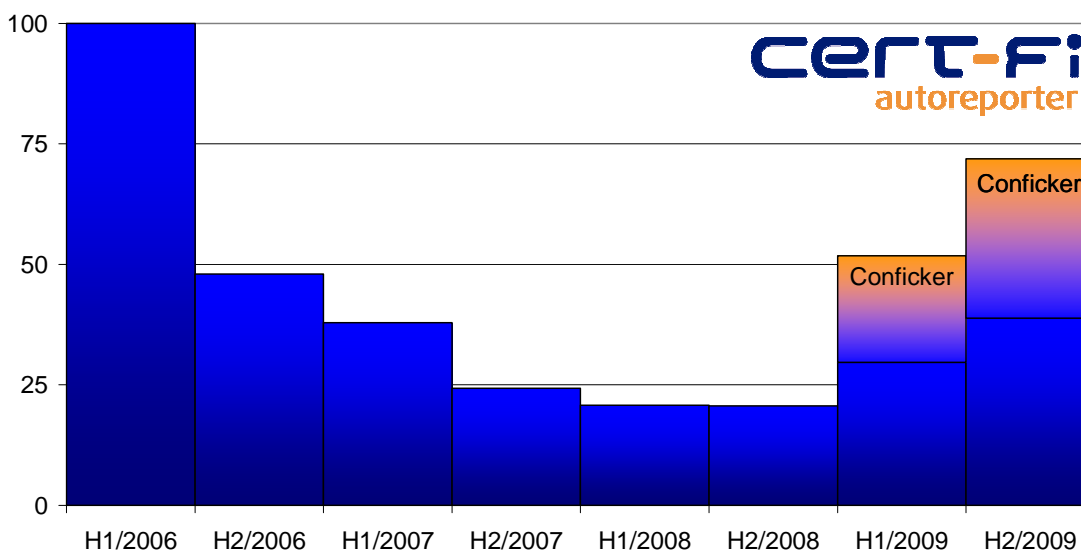
## Conficker on edelleen uhka

Conficker-haittaohjelma on saastuttanut miljoonia tietokoneita eri puolilla maailmaa. Haittaohjelmatarunnan saaneet koneet odottavat edelleen ohjelmistopäivitystä ja toimintaohjeita. Toistaiseksi Conficker-koneiden muodostamaa bottiverkkoa ei kuitenkaan ole käytetty laajemmin hyväksi.

On huomattava, että Confickerin saastuttamat koneet ovat haavoittuvia myös muille haittaohjelmatarunnoille, sillä Conficker kytkee käyttöjärjestelmän turvatoimintoja pois käytöstä.

## Haittaohjelmahavainnot laajakaista-asiakasta kohti

(H1/2006=100)



<sup>1</sup> <http://cert.fi/katsaukset/tilastot/autoreporter.html>

## **Haittaohjelmilla tavoitellaan suomalaisten verkkopankki-käyttäjien rahoja**

Haittaohjelmat, joiden avulla pyritään verkkopankki-istunnon aikana tekemään luvattomia rahansiirtoja käyttäjän tililtä, toimivat jo myös suomalaisissa verkkopankeissa.

CERT-FI:n havaintojen mukaan verkkopankkikäyttäjiin kohdistuvien haittaohjelmien määrä Suomessa on edelleen varsin pieni, mutta ilmiö näyttää muuttuneen pysyväksi.

Kansainvälisen yhteistyön avulla on onnistuttu poistamaan internetistä useita sellaisia internetpalveluntarjoajia, joiden palveluita on käytetty haittaohjelmien levittämiseen ja pankkiyhteyksien kaappamiseen.

Pankit harkitsevat vastatoimia haittaohjelmien avulla tehtävien luvattomien rahansiirtojen estämiseksi. Tavallisuudesta poikkeava siirto voidaan pyytää varmistamaan esimerkiksi tekstiviestin tai tarkistuspuhelun avulla.

Verkkopankkiyhteyteen käytettävästä ympäristöstä riippumattomalla vahvistusmenettelyllä pyritään varmistamaan siitä, että siirto on käyttäjän tahdon mukainen.

## **Tekstiviestien väärinkäytökset lisääntyneet**

Tekstiviesteihin pohjautuvan "roskapostin" määrä on ollut viime vuosina kasvussa. Trendi on alkanut näkyä myös suomalaisille matkapuhelinkäyttäjille, sillä huijaus-tarkoituksessa lähetettyjen tekstiviestien kohteena on yhä useammin suomalainen matkapuhelinnumero ja kielenä suomi.

CERT-FI:n tietoon on tullut tapaus, jossa suomalainen matkapuhelinnumero väärennettiin lähettäjän numeroksi huijaus-tarkoituksessa lähetettyihin tekstiviesteihin. Tämän seurauksena huijausviesteihin vastaanottaneet henkilöt suuntasivat kyseiseen matkapuhelinnumeroon vastaukseksi suuria määriä vihaisia tekstiviestejä ja puheluita. Puhelimeen tulvineiden viestien ja puheluiden vuoksi matkapuhelinliit-

tymän normaali käyttö kävi mahdottomaksi.

Perinteiset puhelin- ja matkapuhelinverkot on usein suunniteltu siten, että niissä oletetaan muiden verkkojen ja verkkolaitteiden olevan luotettavia. Tämän vuoksi puhelinverkkoja hyödyntävien väärinkäytöksen tutkiminen ja estäminen on osoittautunut joissain tilanteissa vaikeaksi.

Häiritsijän jäljittäminen on vaikeaa erityisesti tilanteissa, joissa hän voi käyttää suoraan hallinnassaan olevaa matkapuhelinverkon verkkolaitetta, kuten esimerkiksi tekstiviestikeskusta.

## **Haavoittuvuuskoordinoinnin alkuvuosi rauhallinen**

Viime vuosien aikana CERT-FI on käsitellyt useita laajavaikuttaisia ohjelmistokirjastoisiin, tiedostoformaatteihin ja protokolliin liittyviä haavoittuvuuksia. Kuluva vuosi on kuitenkin alkanut haavoittuvuuskoordinoinnin osalta tavanomaisemmissa merkeissä.

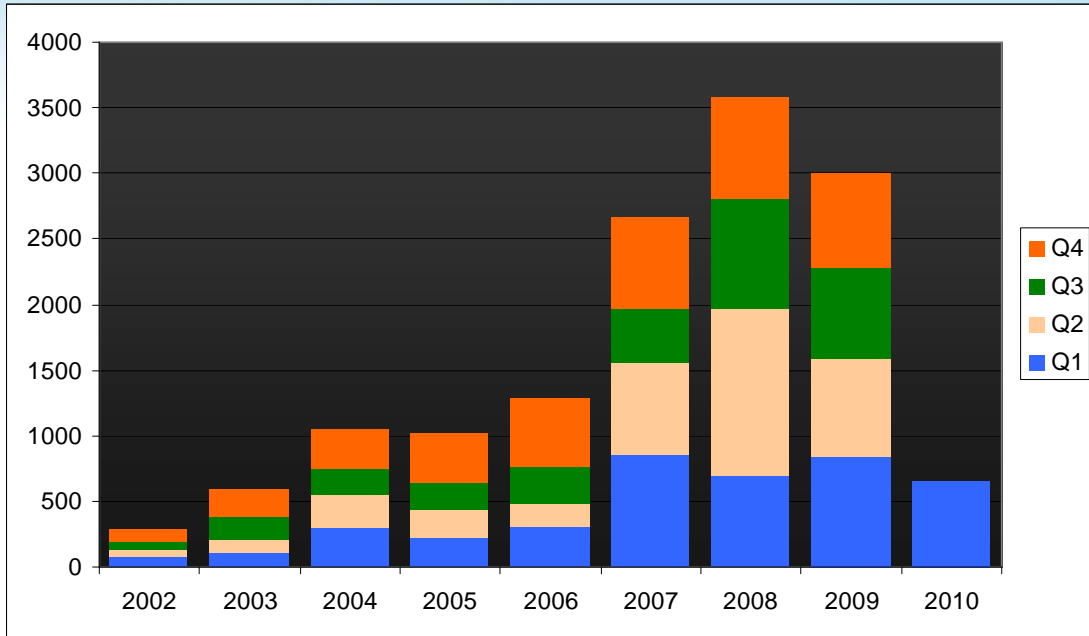
CERT-FI julkaisi tammikuussa 2010 kaksi haavoittuvuutta, joista toinen liittyi Linux-ytimen IPv6-toteutukseen ja toinen GNU Gzip -pakkausohjelmistoon.

Molemmissa tapauksissa ohjelmistovalmistaja tuotti korjatut ohjelmistoversiot ja useimmat käyttöjärjestelmäjakelut liittivät korjaukset nopeasti osaksi jakamiaan ohjelmistopaketteja, jolloin haavoittuvuusi- en käyttäjille aiheuttama uhka saatiin pidettyä jokaisessa koordinoitiprojektin vaiheessa varsin pienenä.

## **Tulevaisuuden näkymiä**

Lähitulevaisuudessa voi tulla esiin lisääkin äskettäin paljastuneisiin salasanoihin liittyviä väärinkäytöksiä. Arvaamalla käyttäjän tunnuksen ja salasanan on mahdollista kaapata esimerkiksi käyttäjän sähköpostitili ja esiintyä hänen nimissään.

CERT-FI seuraa jatkuvasti tietoja varastavien ja pankkiyhteyksiä kaappaavien haittaohjelmien kehitystä ja on mukana kansainvälisessä yhteistyössä niiden aiheuttamien haittojen minimoimiseksi.



CERT-FI-yhteydenotot nimikkeittäin	1/2010	1/2009	Muutos
Haastattelu	32	35	-9 %
Haavoittuvuus tai uhka	63	20	+215 %
Haittaohjelma	317	577	-45 %
Neuvonta	130	93	+40 %
Hyökkäyksen valmistelu	11	10	+10 %
Tietomurto	36	28	+29 %
Palvelunestohyökkäys	15	23	-35 %
Muu tietoturvaongelma	10	23	-56 %
Social Engineering	43	33	+30 %
<b>Yhteensä</b>	<b>657</b>	<b>842</b>	<b>-22 %</b>

CERT-FI:n käsittelemien yhteydenottojen määrä on suunnilleen viime vuosien tasolla. Haittaohjelmailmoitusten osuus on edelleen lähes puolet, vaikka niiden käsittelyä onkin pyritty automatisoimaan.