

CERT-FI

TIETOTURVAKATSAUS 2/2009

3.7.2009

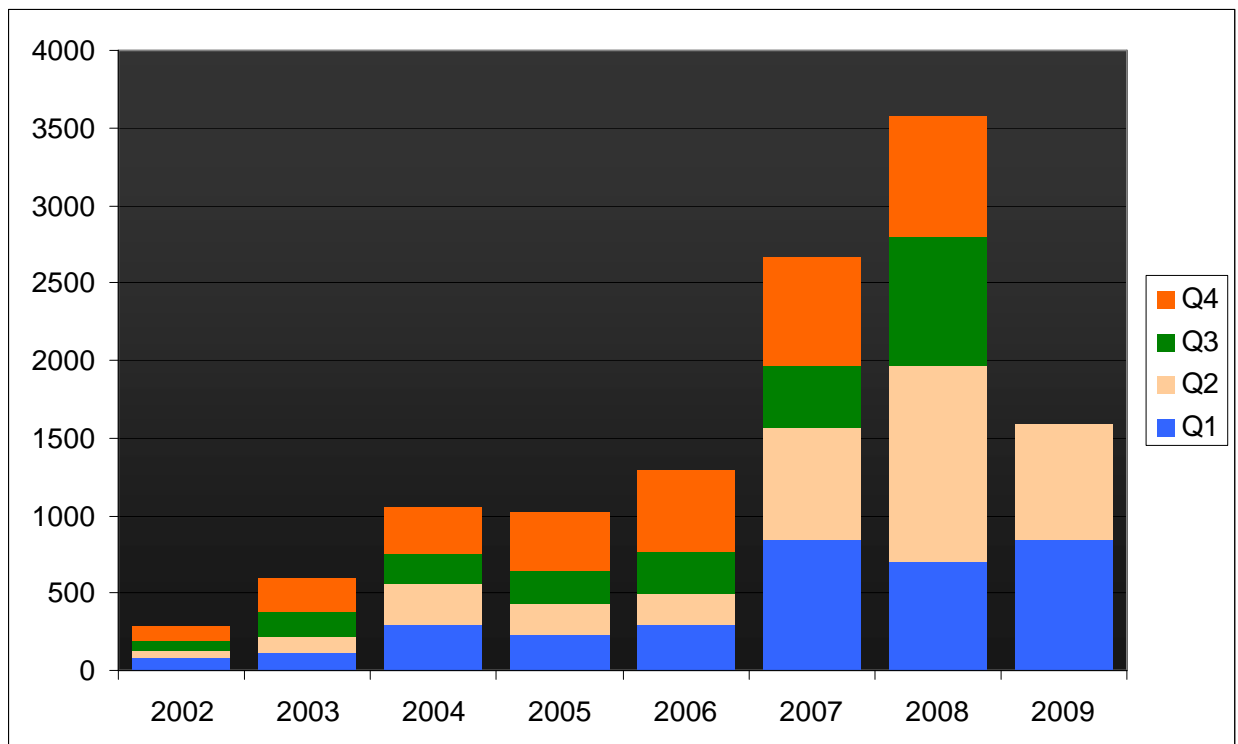
CERT-FI tietoturva- katsaus 2/2009

Johdanto

Haittaohjelmia levitetään myös www-sivuilla olevien mainosten välityksellä. Suomalaisen lehden internet-keskustelupalstalla olleen mainoskehiksen kautta on voinut saada koneelleen haittaohjelman. *Malvertising*-ilmiön torjuminen voi olla vaikeaa, sillä mainosten sisältö ei yleensä ole sivuston ylläpitäjän hallinnassa.

CERT-FI:n tietoon tulee edelleen tietokoneita, joihin on tarttunut Conficker-verkkomato. Mato levisi hetken jopa operaattorin myymän laitteen mukana.

TCP-protokollan toteutuksiin liittyvien haavoittuvuuksien korjausten koordinointi on ollut haastava tehtävä. Kymmenien eri valmistajien ohjelmistoihin tullaan julkaisemaan haavoittuvuuksiin liittyviä korjauksia.



CERT-FI:n käsittelemien tapausten määrä on laskenut viime vuodesta ja on nyt vuoden 2007 tasolla.

Haittaohjelmia on jaettu www-sivujen mainosten kautta

Suomessa on vahvistettu tapaus, jossa haittaohjelmia on jaettu www-sivustolla olleen mainoksen välityksellä. Suomalaisen lehden internet-keskustelupalstalla olleen mainoskehityksen kautta saattoi saada koneelleen haittaohjelman. Haittaohjelma ei latautunut jokaisella mainoksen näyttökerralla, vaan sitä jaettiin satunnaisesti. Siten pyritään tietoisesti vaikeuttamaan tietoturvaloukkausten selvittämistä.

Ulkoistetun mainosisällön mukana voi muuten turvalliselle sivustolle tulla myös haitallista sisältöä. Toistaiseksi tämä myös *malvertising*-nimellä tunnettu ilmiö on ollut harvinainen suomalaisilla sivustoilla. Haittaohjelmien levittäjien kannalta menetelmä on tehokas ja sivustojen ylläpitäjien on vaikea suojautua sitä vastaan.

Sivustojen ylläpitäjät eivät yleensä voi suoraan vaikuttaa mainosten sisältöön, vaan he tarjoavat sivulta tilaa ja tekevät sopimuksen mainoksia välittävän palveluyrityksen kanssa. Mainokset ladataan ulkoiselta palvelimelta ja niiden sisältö voi vaihdella eri latauskertojen välillä tai sen mukaan mistä maasta sivuilla vierailevan käyttäjän IP-osoite näyttää olevan.

Haitallista sisältöä murretuilla www-palvelimilla

Haittaohjelmat eivät ole pelkästään mainossivustojen ongelma. CERT-FI:lle tulee viikoittain ilmoituksia useista suomalaisista sivustoista, joille on onnistuttu syöttämään haitallista sisältöä.

Haittaohjelmia tarjotaan ladattavaksi murretuilta palvelimilta, joille sisältöä voidaan ujuttaa SQL-injektion avulla eli käyttämällä suojaamatonta tai virheellisesti ohjelmoitua syötteen käsittelyä palvelimella. Sivujen muokkaamiseen voidaan käyttää myös tietoja varastavalla haittaohjelmalla urkittuja sivuston ylläpitoon tarkoitettuja tunnuksia ja salasanoja.

Haittaohjelmia tarjotaan sivustolta käyttäjälle useimmiten siten, että että sivun

lähdekoodiin on lisätty iframe-elementti, jonka näkyvyys selaimessa on estetty CSS-tyylitiedoston määrittämiä muokkaamalla. Piilotettu iframe sisältää naamioitua javascript-komentosarjan tai linkin, jonka avulla varsinainen haittaohjelma ladataan koneelle.

Käyttäjä ei välttämättä huomaa mitään tavallisuudesta poikkeavaa, ja haittaohjelma saattaa latautua ilman, että käyttäjä klikkaa sivustolla olevia linkkejä.

Haittaohjelmat, joita murretuilta sivustoilta jaetaan, pyrkivät usein käyttämään hyväkseen tunnettuja selainten ja selainten lisäosien, kuten Flashin ja Javan haavoittuvuuksia. Käyttäjä voi pienentää haittaohjelmatartunnan todennäköisyyttä pitämällä selaimen, käyttöjärjestelmän ja virustorjuntaohjelmiston päivitettyinä tuoreeseen versioon.

Jos haitallista sisältöä onnistutaan lisäämään suosituille sivustolle, haittaohjelma voi levitä sen kautta laajaltikin. Automaattisesti murrettavia www-sivustoja etsivät haittaohjelmat eivät kuitenkaan erottele sivustoja niiden suosion mukaan, vaan haitallista sisältöä voi ilmestyä kaikille haavoittuville sivustoille.

Sivuston ja www-palvelimen ylläpitäjän aktiivisuus, palvelinohjelmistojen päivittäminen ja sivuston sisältöön tehtyjen muutosten tarkkailu ovat ensiarvoisen tärkeitä sivustojen pitämiseksi haittaohjelmista puhtaina.

Huolimattomasti suojatulta palvelimelta vuosi tietoja

Toukokuussa tuli julkisuuteen tapaus, jossa www-palvelimelta oli mahdollista ladata tiedostoja, joita ei ollut tarkoitettu julkisiksi.

Tapauksessa oli kyse huolimattomuudesta sivuston suojauksia määritettäessä, jolloin palvelimen kansiot olivat selattavissa ja sen sisältämät tiedostot ladattavissa. Tämän kaltaiset tapaukset eivät ole erityisen harvinaisia ja niitä tuodaan myös CERT-FI:n tietoon aika ajoin.

Conficker-verkkomato on edelleen yleinen

Joulukuussa liikkeelle laskettu Conficker-verkkomato, joka tunnetaan myös nimellä Downadup, on edelleen yleinen. CERT-FI:n tietoon tulee päivittäin tietoja tartunnan saaneista tietokoneista.

Toisen vuosineljänneksen aikana nähtiin myös ensimmäisiä merkkejä Confickerin saastuttamien tietokoneiden käyttämisestä edelleen hyväksi rikollisessa toiminnassa. Verkkomadon luoman vertaisverkon välityksellä ladattiin tartunnan saaneisiin tietokoneisiin roskapostitukseen tarkoitettu haittaohjelma, ja sitä käytettiin roskapostikampanjan toteuttamiseen. Vielä tuntemattomasta syystä roskapostitukseen tarkoitettu haittaohjelma kuitenkin oli ohjelmoitu tuhoutumaan kuukauden päästä asennuksesta. Tapaus on jäänyt yksittäiseksi eikä Conficker-tartunnan saaneita koneita ole tämän tapauksen lisäksi käytetty järjestelmällisesti hyväksi muuhun rikolliseen toimintaan.

CERT-FI lähetti toisen vuosineljänneksen aikana käyttäjille 22 000 Conficker-verkkomatoon liittyvää ilmoitusta. Suomalaisissa verkoissa verkkomadon saastuttamia koneita on havaittu noin 5 300 eri IP-osoitteesta. Ensimmäisellä vuosineljänneksellä lähetettiin vastaavasti noin 14 000 ilmoitusta, jotka koskivat 3 600 eri osoitetta.

Conficker pääsi hetkeksi myös kaupan hyllylle

Yksi Conficker-madon leviämistavoista on sen kopioituminen USB-muistikorteille. Toukokuussa tuli tietoon tapaus, jossa matkapuhelinoperaattorin myymän, data-liikenteeseen käytettävän USB-nettitikun mukana toimitetulla muistikortilla oli operaattorin tarjoaman tietoturvaohjelmiston lisäksi myös Conficker-haittaohjelma.

Madon sisältäneitä muistikortteja ehdittiin myydä joitakin kymmeniä. Operaattori on ottanut yhteyttä niihin asiakkaisiin, joiden ostaman laitteen mukana on voinut olla haittaohjelma. Tartunnan sisältäneiden nettitikkujen myynnin aikaan kaikki ylei-

simmät virustorjuntaohjelmat tunnistivat jo kyseisen haittaohjelmaversion, joten tapauksen vaikutukset jäivät todennäköisesti vähäisiksi.

Ghostnet koski myös suomalaisia

Edellisessä tietoturvakatsauksessa kerrottiin laajasta kohdistettujen hyökkäysten avulla tehdystä tietomurtojen sarjasta. Etähallittavan Ghost-haittaohjelman avulla pyrittiin hankkimaan tietoja kohdeorganisaatioista. CERT-FI:n tietojen mukaan haittaohjelmien levittäjien joukossa ei ollut suomalaisia tahoja.

CERT-FI sai ilmoituksen kahdesta suomalaisessa verkossa olleesta kaapatusta tietokoneesta, joskin vasta huomattavan kauan sen jälkeen kun asia oli tullut julkisuuteen. Tiedot välitettiin edelleen asianosaisille.

TCP-protokollaan liittyvien haavoittuvuuksien tietojen julkaisu lähestyy

TCP-protokollapinon toteutuksiin liittyvien haavoittuvuuksien korjausten julkaisuun tähtäävä koordinoitiprosessi on edennyt asian monitahoisuuteen nähden hyvin. Korjausten julkaisun ajankohtaa on tähän mennessä jouduttu lykkäämään suunnitellusta. Aikataulun viivästyminen on yleistä kun haavoittuvuus koskee useita ohjelmisto- ja laitevalmistajia.

CERT-FI on ottanut haavoittuvuuksiin liittyen yhteyttä 65 valmistajaan, joista 38:n kanssa on sittemmin työskennelty aktiivisesti. Suurin osa valmistajista on jo saanut korjattua haavoittuvuudet, mutta osalla luotettavan korjausmenetelmän luominen on yhä kesken. CERT-FI:n tarkoituksena on julkaista korjaukset koordinoitusti, minkä vuoksi lopullisesta julkaisupäivämäärästä ei ole vielä täyttä varmuutta.

Ohjelmistovalmistajien piirissä on myös esitetty erilaisia arvioita haavoittuvuuksien vakavuudesta. On osoitettu, että niitä hyödyntämällä voidaan vakavasti haitata monien ohjelmistojen, käyttöjärjestelmien ja verkon aktiivilaitteiden toimintaa.

CERT-FI on julkaissut haavoittuvuuksia koskevan lausunnon, jota on viimeksi päivitetty kesäkuussa. Linkki lausuntoon löytyy sivulta www.cert.fi.

Viime aikoina esiin tulleet vakavat ohjelmistohaavoittuvuudet ovat saaneet huomiota myös Euroopan unionin tasolla. EU:n komissio järjesti maaliskuun lopussa haavoittuvuuksien hallintaa käsitelleen työpajaseminaarin¹, johon osallistui CERT-FI:n asiantuntijoiden lisäksi myös muita suomalaisia alustajia.

Älypuheliiniin kohdistuvat tietoturva-uhat nousemassa tietoisuuteen

Tietoturvan parissa toimivat ovat jo pitkään esittäneet arvioita älypuheliiniin kohdistuvien tietoturva-uhkien, kuten haavoittuvuuksien ja haittaohjelmien lisääntymisestä. Siinä missä tietokoneet ovat olleet houkuttelevia kohteita tietoverkkojen toiminnan haittaajille ja tietoverkkorikollisuudelle, älypuhelimet ovat toistaiseksi enimmäkseen säästyneet tietoverkkojen haitallisilta lieveilmiöiltä.

Älypuhelimet alkavat muistuttaa ominaisuuksiltaan ja käyttötarkoituksiltaan tietokoneita ja niiden houkuttelevuus hyökkääjien silmissä kasvaa. Viime aikoina on julkisuuteen tuotu aiempaa enemmän älypuheliiniin liittyviä tietoturva-uhkia. Ilmiön taustalla on älypuheliiniin liittyvän tietoturvatutkimuksen lisääntyminen.

Vuoden 2009 toisen vuosineljänneksen aikana julkisuudessa on esitetty muun muassa älypuhelimien asetusviesteihin ja WAP push -viesteihin liittyviä tietoturva-ongelmia. Ne liittyvät puhelinten asetusten etähallintaan ja WAP-protokollan toteutukseen sekä käyttäjien tietämättömyyteen haitallisessa tarkoituksessa laadittujen asetustekstiviestien hyväksymiseen mahdollisesti liittyvistä riskeistä.

Asetustekstiviestit ovat tavallisesti operaattorin lähettämiä tekstiviestejä,

1

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/vulnerabilities_workshop/index_en.htm

joiden avulla voidaan välittää puhelimeen muun muassa internetin käyttöön liittyviä asetuksia, kuten nimipalveluasetukset. Viestejä voi kuitenkin lähettää myös harhauttamistarkoituksessa ja vaihtamalla puhelimen käyttämät nimipalvelimet erehdyttää käyttäjä haitallisille [www-sivustoille](http://www.sivustoille). Joissakin matkapuhelinmalleissa asetusviestien välityksellä on myös mahdollista etähallita puhelimen toimintoja.

Pääosa markkinoilla olevista matkapuhelinlaitteista tarkistaa vastaanottamansa asetusviestin alkuperän ja lisäksi kysyy käyttäjältä vahvistuksen ennen asetustekstiviestin hyväksymistä. Varovaisen käyttäjän on syytä hyväksyä vastaanottamansa asetustekstiviestit vain silloin kun matkapuhelin on ensimmäistä kertaa uuden operaattorin verkossa tai hän on itse pyytänyt operaattoria lähettämään asetukset puhelimeen.

Tietoverkkojen käyttö poliittisessa liikehdinnässä yleisty

Vuosina 2007 ja 2008 Viron ja Georgian poliittiset levottomuudet näkyivät myös tietoverkoissa. Verkkojen ja tietoyhteiskunnan palveluiden toimintaa häirittiin muun muassa palvelunestohyökkäyksin. Murrettuja [www-sivustoja](http://www.sivustoja) käytettiin poliittisten sanomien julkaisemiseen. Toiminnan taustalla ei kuitenkaan välttämättä ollut valtiollisia toimijoita.

Toukokuussa 2009 pidetyt Iranin presidentinvaalit toivat esiin uudenlaista tietoverkkoaktivismia. Yhteisö- ja julkaisupalveluista tuli kanava, jonka kautta yksityishenkilöt välittivät tietoja ja näkemyksiä Iranin tapahtumista vallinneissa poikkeusolosuhteissa.

Keskustelupalstoja ja blogisivustoja käytettiin myös vastakkaisten näkemysten levittämisen häirintään. Sivustoilla jaettiin tavallisille tietokoneiden käyttäjille ohjeita siitä miten he voivat valjastaa työasemansa ja internet-yhteytensä palvelunestohyökkäyksiin. Toteutetuissa hyökkäyksissä käytettiin varsin vähän bottiverkkoja, ja ne toteutettiin esimerkiksi HTTP-pyyntöjä generoimaan suunniteltujen [www-sivustojen](http://www.sivustojen) avulla.

Latvialainen haittaohjelmien levittäjä irti verkosta

CERT-FI avusti ulkomaisia viranomaisia selvittämään tapausta, johon liittyi pankkitietoja varastava haittaohjelma. Ohjelmaa levitettiin latvialaisen palveluntarjoajan verkko-osoitteiden kautta.

Selvitystyön yhteydessä ilmeni, että samaa verkkoa käytettiin useiden eri haittaohjelmien jakelualustana. CERT-FI otti yhteyttä latvialaiseen CERT-ryhmään ja palveluntarjoajan verkko-operaattoriin. Selvisi, että kyseisestä palveluntarjoajasta oli tehty useita ilmoituksia aktiivisesta verkon tietoturvaa vaarantavasta toiminnasta.

Tapahtumaketjun lopputuloksena palveluntarjoajan verkko-operaattori katkaisi sen verkkoyhteydet käyttöehtorikkomuksen perusteella.

Autoreporter palkittiin

CERT-FI:n tuottama Autoreporter-palvelu on palkittu FIRST:n (Forum of Incident Response and Security Teams) ja CERT/CC:n (CERT Coordination Center) järjestämässä kilpailussa². Kilpailussa etsittiin parhaita käytäntöjä tietoturvaloukkausten havaitsemiseksi ja estämiseksi.

Tulevaisuuden näkymiä

Internetissä liikkuvan roskapostin määrä putosi viime vuoden loppupuolella tilapäisesti noin puoleen kun haitallista sisältöä jakavia operaattoreita suljettiin verkosta. Sittemmin roskapostin määrä on noussut takaisin entiselle tasolle ja suunnilleen yhdeksän viestiä kymmenestä on tilaamatonta mainospostia, haittaohjelmien levittämiseen pyrkiviä viestejä tai rikolliseen toimintaan houkuttelevia viestejä.

Kansainvälisissä yhteistyöelimissä on merkkejä siitä, että halu löytää ratkaisuja ongelmaan on lisääntymässä. Yhteisesti sovitut menetelmät väärinkäyttöihin puuttumiseksi ovat kuitenkin vielä kehit-

tymättömiä. Internetin osoite- ja verkkotunnushallintoa koordinoiva ICANN sekä tietojen varastelutoiminnan torjumiseen keskittyvä APWG (Anti-phishing Working Group) ovat terävöittämässä toimintaansa.

APWG on käynnistämässä hanketta, jossa phishing-toimintaan käytettävät, virheellisillä tiedoilla rekisteröidyt verkkotunnukset saataisiin suljettua jo muutamman tunnin kuluessa huijausten havaitsemisesta ja raportoinnista. ICANN on tarkentamassa verkkotunnusten rekisteröintipalvelujen tarjoajien valvontaa ja ohjeistusta. Molemmat tahot korostavat tarvetta tiiviiseen yhteistyöhön erityisesti CERT-FI:n kaltaisten kansallisten CERT-yksiköiden kanssa.

2

<http://www.cert.fi/tietoturvanyt/2009/06/ttn200906301435.html>

| CERT-FI-yhteydenotot nimikkeittäin | 1-6/2009 | 1-6/2008 | Muutos |
|---|-----------------|-----------------|---------------|
| Haastattelu | 61 | 46 | +33% |
| Haavoittuvuus tai uhka | 65 | 271 | -76% |
| Haittaohjelma | 1055 | 1187 | -11% |
| Neuvonta | 178 | 151 | -59% |
| Hyökkäyksen valmistelu | 24 | 59 | -69% |
| Tietomurto | 65 | 102 | -32% |
| Palvelunestohyökkäys | 40 | 41 | -2% |
| Muu tietoturvaongelma | 46 | 21 | +119% |
| Social Engineering | 59 | 83 | -29% |
| Yhteensä | 1593 | 1961 | -19% |

Ilmoitukset haittaohjelmista muodostivat edelleen valtaosan CERT-FI:n käsittelemistä tietoturvatapauksista alkuvuoden 2009 aikana. Lisää tilastotietoja löytyy osoitteesta www.cert.fi.