

**CERT-FI**

**VUOSIKATSAUS 2008**

16.01.2009

# CERT-FI tietoturva- katsaus 4/2008

## Johdanto

Vuoden 2008 aikana tuli esiin laajavaikuttaisia internetin infrastruktuuria koskevia haavoittuvuuksia. Internetin nimipalvelua koskeva haavoittuvuus olisi korjaamattomana mahdollistanut käyttäjän harhautamisen tai sähköpostin ohjaamisen väärään osoitteeseen. CERT-FI julkaisi haavoittuvuuden johdosta varoituksen. Nimipalvelinohjelmistot päivitettiin turvallisempiin versioihin nopeasti eikä haavoittuvuutta ehditty käyttää laajamittaisesti hyväksi. Tapaus osoitti kuitenkin internetin nimipalvelun rakenteellisen haavoittuvuuden tietojen väärentämisyrietyksille. TCP-protokollatoteutuksista löydetty haavoittuvuus saattaa vaikuttaa moniin internet-verkkoon kytkettäviin laitteisiin ja ohjelmistoihin.

Haitallisen sisällön levittäminen verkossa on osoittautunut aikaisemmin oletettua keskittyneemmäksi. Suurten botnet-verkkojen komentopalvelimia sisältäneen palveluntarjoajan poistaminen verkosta marraskuussa vähensi verkossa liikkuvan roskapostin määrää hetkeksi hyvin merkittävästi.

Myös suomalaisten www-palvelinten sisältöä on toistuvasti muokattu luvottomasti käyttämällä hyväksi palvelinohjelmistojen haavoittuvuuksia. Palvelimille murtautumisella pyritään nykyisin tavallisesti valjastamaan sivustoja haittaohjelmien levittämiseen, ja uusien murrettujen koneiden liittämiseen sitä kautta botnet-verkkoihin. Aivan vuoden lopussa havaittiin lähiverkossa itsenäisesti leviävä verkkomato, joka saastutti työasemia ja tietoverkkoja niin Suomessa kuin maailmallakin.

CERT-FI julkaisi vuonna 2008 kaksi varoitusta, 156 haavoittuvuusilmoitusta ja 83 Tietoturva nyt! -artikkelia.

## **Internetin ikä näkyy laajavai- kutteisina haavoittuvuuksina**

Internetin perustana olevat yhteyskäytännöt ja ohjelmistot ovat osittain jo yli kolmenkymmenen vuoden takaa. Niitä kehitettäessä ovat lähtökohdat olleet aivan toisenlaiset kuin nykyisin tuntemassamme verkossa. Suunnittelua on ohjannut pyrkimys yksinkertaisuuteen ja sitä kautta mahdollisimman hyvään suorituskykyyn hitailla yhteyksillä ja laskentakyvyiltään rajallisilla tietokoneilla. Tietoturvasuoritus ei suunnitteluvaiheessa ole erityisesti huomioitu. Käyttöön otettuja protokollia ja sovelluksia on myöhemmin vaikea muuttaa tai niiden käytöstä luopua.

Verkon käytön laajennuttua ja toimintaympäristön muututtua siten vihamielisemmäksi, ovat monet aikanaan tehtyjen teknologisten ratkaisujen puutteet muodostuneet ongelmiksi, jotka vaikeuttavat toisaalta verkon turvallista käyttöä ja toisaalta sen väärinkäytösten torjumista.

### ***DNS-haavoittuvuus perustuu osapuolten puutteelliseen tunnistamiseen***

Kesällä 2008 tietoturvyhteisöä kohauttanut, *Dan Kaminskyn* julkaisema internetin nimipalvelua (DNS) koskeva haavoittuvuus johtuu pitkälti siitä, että nimipalvelu käyttää UDP-protokollaa. UDP ei edellytä kaksisuuntaista yhteydenmuodostusta, mikä mahdollistaa DNS-kyselyjen ja etenkin niihin liittyvien vastausten lähettämisen käyttämällä väärennettyä IP-osoitetta. UDP-protokollapakettien todellisen lähettäjän jäljittäminen on myös hyvin vaikeaa.

Nimipalvelukyselyihin ja -vastauksiin liittyy tunniste, jonka avulla pyritään yhdistämään nimipalvelimelle esitetty kysymys ja palvelimen siihen antama vastaus. Haavoittuvuus liittyi siihen, että sivullisen hyökkääjän oli joissakin tapauksissa liian helppo arvata seuraavaksi käytettävä tunniste, jolloin kysyjälle voi syöttää väärennettyjä vastauksia. Haavoittuvuuden korjaamiseksi nimipalveluohjelmistoja korjattiin niin, että tunnisteiden satunnaisuutta parannettiin.

Korjaukset eivät kuitenkaan riitä korjaamaan itse protokollan puutteita. Nimipalvelukyselyjä voi edelleen tehdä väärennetyillä osoitteilla ja näin käyttää nimipalve-

limia apuna palvelunestohyökkäyksissä. Vastaavan palvelimen oikeellisuutta ei voi varmistaa, mikä mahdollistaa käyttäjien harhauttamisen ohjaamalla käyttäjän tietokoneen tekemät nimipalvelukyselyt harhauttajan ylläpitämälle palvelimelle. Loppuvuodesta CERT-FI:n tietoon tuli havainnot haittaohjelmasta, joka pyrki DHCP-palvelimena esiintymällä muuttamaan lähiverkossa olevien tietokoneiden käyttämät nimipalvelimet haluamukseensa. Nämä palvelimet antoivat tiettyihin osoitekyselyihin väärennettyjä vastauksia, joiden avulla esimerkiksi pankin sivulle pyrkivä käyttäjä voitiin ohjata huijaussivustolle.

DNS-protokollaan on suunniteltu DNSSEC-niminen tietoturvalaajennus, jonka avulla voidaan varmistua siitä, että vastaukset nimipalvelukyselyihin tulevat oikealta palvelimelta. DNSSEC ei ole toistaiseksi yleistynyt, sillä sen käyttämiseen liittyy useita haasteita. Se kuormittaa nimipalvelimia nykyistä enemmän ja aiheuttaa myös nykyistä enemmän verkkoliikennettä. Erityisesti käytettävien salausavainten hallinta on ongelmallista ja myös jossain määrin poliittinen kysymys.

### ***TCP-protokollan toteutuksista löydettiin ongelmia***

TCP-protokollaa ja sen toteutuksia on vuosien varrella useaan kertaan paranneltu. TCP on suunniteltu luotettavaan tiedonsiirtoon, ja sen viat ovat pikemmin liittyneet sen huomattavaan monimutkaisuuteen kuin päinvastoin.

Ruotsalainen *Outpost24*-yhtiö ilmoitti syyskuussa löytäneensä TCP-protokollatoteutuksiin liittyviä haavoittuvuuksia. Tietoja haavoittuvuuksista esiteltiin julkisudessa ruotsalaisessa Sec-T- ja suomalaisessa T2-tietoturvakonferenssissa. Outpost24 otti sittemmin yhteyttä CERT-FI-yksikköön haavoittuvuuksien korjaamisen koordinoimiseksi eri valmistajien kanssa. Koordinointiprosessi on edennyt odotetusti. CERT-FI ja sen kansainväliset yhteistyökumppanit ovat ottaneet yhteyttä ohjelmistotuotteiden valmistajiin, jotta ne voivat arvioida haavoittuvuuksien vaikutuksia omiin tuotteisiinsa. Tarkempia yksityiskohtia haavoittuvuudesta julkais-taneen vuoden 2009 aikana.

### ***Matkaviestinten ohjelmistoissa haavoittuvuuksia***

Matkaviestinten haittaohjelmat tai merkittävät haavoittuvuudet ovat tähän saakka olleet harvinaisia. Aivan vuoden lopussa nousi esiin matkapuhelimissa käytetyn S60-käyttöjärjestelmän haavoittuvuus, joka mahdollistaa matkaviestinverkon päätelaitteeseen kohdistuvan palvelunestohyökkäyksen. Puhelimen ohjelmistosta löytyi tekstiviestien käsittelyyn liittyvä ohjelmistovirhe. Tietyllä tavalla muodostetun tekstiviestin vastaanottaminen haavoittuvalla ohjelmistolla varustetulla puhelimella sai aikaan sen, ettei puhelimella sen jälkeen voinut lähettää tai vastaanottaa viestejä ennen sen asetusten nollaamista tehdasasetuksiin. Kotimaiset matkapuhelinoperaattorit ovat ryhtyneet suodattamaan haitalliseksi tiedettyjä viestejä.

CERT-FI:n tietoon on tullut myös muita matkaviestimien tietoturvasuhteeseen vaikuttavia haavoittuvuuksia. Niiden julkaisuaikataulusta ei toistaiseksi ole tehty päätöksiä.

### ***Haavoittuvuuskoordinointi työllisti***

CERT-FI:n haavoittuvuuskoordinoitointitoiminta on muutenkin ollut vilkasta. Maaliskuussa julkaistiin Oulun yliopiston tietoturvaryhmä OUSPG:n koostama testimateriaali lukuisten pakkaus- ja arkistoformaattitoteutusten toimintavarmuuden testaamiseksi. Päivityksiä materiaalin avulla löydettiin haavoittuvuuksiin on julkaistu pitkin vuotta.

Toukokuussa julkaistiin Codenomicon Oy:n löytämät haavoittuvuudet yleisesti salaamattomuuteen käytetyistä avoimen lähdekoodin OpenSSL- ja GnuTLS-ohjelmistoista. Koordinoinnin yhteydessä otettiin yhteyttä muihinkin tätä koodia omista ohjelmistoissaan käyttäviin valmistajiin.

Syyskuussa julkaistiin myös Codenomicon Oy:n löytämä avoimen lähdekoodin IPv6-projekti KAME:n ICMPv6-protokollan toteutukseen liittyvä haavoittuvuus. Vuoden viimeisellä neljänneksellä CERT-FI:n koordinoitavaksi saatettiin useita tapauksia, joiden julkaisu lienee ajankohtainen vuoden 2009 aikana.

### ***Viestinnän luottamuksellisuus puntarissa***

Sähköisen viestinnän luottamuksellisuudesta on käyty keskustelua valmisteltaessa sähköisen viestinnän tietosuojalain uudistusta. Ruotsin puolustusvoimien signaalitiedustelu (FRA) on saanut vuoden 2009 alussa oikeuden tarkkailla Ruotsin kautta kiinteissä verkoissa kulkevaa tietoliikennettä. Suurin osa myös suomalaisten ulkomaille suuntautuvasta internet-liikenteestä kulkee Ruotsin kautta. Liikenteen tarkkailu voi kohdistua erityisesti salaamattomaan viestintään.

Sähköpostiviestit voivat kulkea postipalvelinten välillä salaamattomina, jolloin verkkoliikennettä salakuuntelemalla pääsee käsiksi myös niiden sisältöön. Luottamuksellisten viestien sisällön voi halutessaan salata ja sähköisesti allekirjoittaa. Tästä on kuitenkin erikseen sovittava vastaanottajan kanssa, sillä mikään sähköpostiviestien salaamistapa ei ole yleistynyt niin, että sen voisi ilman muuta olettaa olevan käytettävissä myös vastaanottajalla. Joka tapauksessa viestin tunnistetiedot, kuten vastaanottajan sähköpostiosoite, täytyy lähettää salaamattomina, jotta viestit voidaan välittää perille.

Sähköpostiviestien välittämisessä käytettävä SMTP-protokolla ei vaadi lainkaan viestin lähettäjän todentamista, mikä mahdollistaa sähköpostiviestien lähettämisen kenen tahansa nimissä. Sähköposti onkin suurin haitallisen sisällön, kuten ei-toivotun mainospostin ja haittaohjelmien levityskanava. Valtaosa roskapostista lähetetään yksittäisten käyttäjien murretuista tietokoneista muodostettujen botnet-verkkojen avulla. Ongelmaa pyritään lievittämään roskapostin suodattamiseen tarkoitettujen ohjelmien avulla.

### ***Botnet-verkkojen merkitys on edelleen suuri***

Botnet-verkot ovat viime vuosien aikana vakiintuneet kaikenlaisten tietoverkkokosten tärkeimmäksi välineeksi. Jopa palvelinten tietomurrot tehdään nykyisin lähes yksinomaan tavoitteena botnet-verkkojen kasvattaminen, eikä palvelimilla mahdollisesti olevan tiedon vuoksi.

Hakukoneiden avulla kerätään tietoa havoittuvista palvelimista, joita pyritään käyttämään haittaohjelmien jakamiseen.

Käyttäjät houkutellaan murretuille sivustoille, joilta heidän tietokoneeseensa asentuu botnet-haittaohjelma, joka ottaa yhteyttä botnetin hallintapalvelimeen. Hallintapalvelimelta käsin botnetin koneita voidaan komentaa keräämään ja luovuttamaan tietokoneen sisältämiä tietoja, leviättämään haittaohjelmaa edelleen uusille palvelimille, lähettämään roskapostia tai käynnistämään palvelunestohyökkäyksiä haluttuja kohteita vastaan. Haittaohjelmat voivat myös vakoilla ja välittää tietokoneeseen talletettuja tai www-yhteyden aikana sivuille syötettyjä tietoja ulkopuolisille.

Haittaohjelmista levitetään jatkuvasti uusia versioita, jotta virustorjuntaohjelmat eivät tunnista niitä. Ne osaavat myös päivittää itsensä automaattisesti.

### ***Roskapostin määrä romahti hetkeksi***

Verkkorikollisuuden torjunnan kannalta tärkeitä tekijöitä ovat toiminnalle myönteelliset tai välinpitämättömät palvelinhotellit, rikolliseen käyttöön rekisteröitävät verkkotunnukset ja operaattorien väliset yhdysliikennesopimukset. Tärkeitä tekijöitä ovat myös internetin käyttäjien murretuista tietokoneista muodostetut botnet-verkot, joiden kasvattamiseksi pyritään leviättämään haittaohjelmia yhä uusien käyttäjien tietokoneisiin.

Haitallisen sisällön jakamiseen keskittyvät palvelinhotellit ja niille tietoliikenneyhteyksiä tarjoavat verkko-operaattorit ovat osoittautuneet merkittäväksi tekijäksi. Näistä palveluntarjoajista käytetään joskus nimityksiä "bullet-proof hosting" tai "anti-abuse-resistant hosting".

Syyskuussa verkkoyhteytensä menettänyt *Intercage* sai seuraan marraskuun puolivälissä toisesta, Kalifornian San Josesta toimineesta *McColo*-nimisestä palveluntarjoajasta. Yhteyksien katkaisua edelsi tietoturvatutkijoiden ja lehdistön kirjoittelu kyseisten palveluntarjoajien verkosta havaitusta haitallisesta liikenteestä. McColon verkko-osoitteista oli havaittu roskapostin levitykseen erikoistuneiden botnet-verkkojen hallintapalvelimia. Palvelun-

tarjoajan verkkoyhteyksien katkaisun vaikutukset olivat kuitenkin yllätys: koko internetissä liikkuvan roskapostin määrä väheni eri arvioiden mukaan noin puoleen aikaisemmasta.

Parissa kuukaudessa roskapostin määrä kuitenkin palautui lähelle aikaisempaa tasoa. Haitallisiin palveluihin keskittyviä tai sellaisia asiakaskunnassaan sietäviä hosting-palveluntarjoajia on edelleen useita eri puolilla maailmaa.

Suomesta ei ole toistaiseksi löydetty järjestelmällisesti haitallisia palveluita suosivia palveluntarjoajia. Yhteistyö CERT-FI:n ja suomalaisten internet-palveluntarjoajien välillä toimii hyvin. Havaitut tietoturvaloukkaukset suomalaisten hosting-palvelujen tarjoajien verkoissa ovat tavallisesti johtuneet ohjelmistopäivitysten laiminlyönneistä ja muista yksittäisten www-palvelujen tietoturvapuutteista.

### ***Verkkotunnuksia rekisteröidään väärennetyillä tiedoilla väärinkäyttöksiä varten***

Haittaohjelmien leviättämiseen ja erilaisiin verkkohuijauksiin käytetään yleisesti väärennetyillä tiedoilla rekisteröityjä verkkotunnuksia. Verkkotunnuksen rekisteröijän henkilöllisyyttä tai yhteystietojen oikeellisuutta ei useinkaan varmisteta.

Haittaohjelmiin on usein etukäteen ohjelmoitu verkkotunnuksia, joiden avulla ne pyrkivät myöhemmin ottamaan yhteyttä hallintapalvelimeensa. Ohjelmat voivat myös ottaa yhteyttä satunnaisilta vaikuttaviin verkkotunnuksiin, jotka on muodostettu esimerkiksi päivämäärän ja kellonajan perusteella. Tämä vaikeuttaa hallintapalvelinten torjumista, sillä haittaohjelman käyttämä osoite voi vaihtua vaikkapa päivittäin, eikä niiden muodostamista välttämättä pystytä selvittämään.

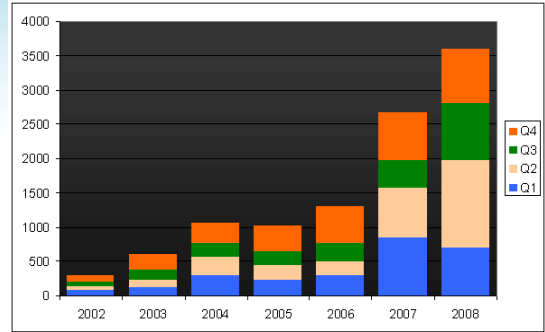
Suomeen tämänkaltaisia verkkotunnuksia ei ole rekisteröity, vaan haittaohjelmat ovat käyttäneet kansainvälisiä verkkotunnuksia. FI-verkkotunnus on osoitettu useissa tutkimuksissa turvallisimmaksi verkkotunnukseksi maailmassa.

## **Väärinkäyttöihin puuttuminen on usein hidasta**

"Bullet-proof hosting" -palveluntarjoajien toimintaan puuttuminen on toistaiseksi ollut melko satunnaista ja järjestäytymätöntä. Internet-palveluntarjoajien perusteet puuttua niiden toimintaan ovat liiketoiminnallisia, sillä rikolliselta vaikuttavassa toiminnassa mukana olevat asiakkaat voivat vaikeuttaa operaattorin toimintaa ja vahingoittaa sen mainetta. Viranomaisten osuus Intercagen ja McColon verkosta irrottamisessa näyttää olleen vähäinen. Tietoverkkoverkkorikosten torjunnan ilmeinen tehottomuus onkin saanut tietoturvatutkijat julkaisemaan raportteja kyseisten palveluntarjoajien verkkoihin liittyvästä haitallisesta liikenteestä, mikä näyttää ajaneen Intercagen ja McColon verkkoyhteydet tarjonneet operaattorit purkamaan heidän sopimuksensa. Suuret tietoliikenneoperaattorit liikennöintisopimuksineen ovat merkittävässä asemassa jos jokin yksittäinen toimija halutaan eristää pois internetistä. Voidaan kuitenkin sanoa, että tämä toimintamalli lähestyy jonkinlaista "oman käden oikeutta".

Internetin kansainvälinen koordinaatiojärjestö ICANN ja eurooppalainen IP-osoitteita hallinnoiva RIPE ovat reagoineet joihinkin väärinkäytöstapauksiin. ICANN peruutti *Estdomains*-nimiseltä verkkotunnusten tarjoajalta oikeuden verkkotunnusten rekisteröintiin. Yhtiön kautta rekisteröidyt verkkotunnukset on siirretty toiselle palveluntarjoajalle. RIPE on puolestaan perunut pahamaineisen *Russian Business Network* -palveluntarjoajan käyttöön annetut IP-osoitteet.

ICANN ja RIPE perustavat ratkaisunsa teknisten verkkoresurssien käyttöön liittyviin sopimusrikkomuksiin. Se ei kuitenkaan riitä tekijöiden saamiseksi rikosoikeudelliseen vastuuseen. Internet-palveluntarjoajien ja CERT-toimijoiden aktiivisen seurantatyön lisäksi olisi kansainvälisen poliisiyhteistyön tehostuttava merkittävästi, jotta rikollisjärjestöjen huomattavan monitahoiseen ja kansainväliseen toimintaan tietoverkoissa voitaisiin vaikuttaa tehokkaasti.



CERT-FI:n käsittelemien tapausten määrä kasvoi edellisvuodesta.

## **IP-osoitteet ovat loppumassa, iso haaste edessä**

Edelleen valtaosa internet-verkko-liikenteestä perustuu IP-protokollan versioon 4, jonka mukaisten IP-osoitteiden määrä on kuitenkin rajallinen. Ongelman kiertämiseksi tehdyistä järjestelyistä, kuten osoitemuunnoksista (NAT) huolimatta, käytettävissä olevat IP-osoitteet ovat loppumassa. Tämänhetkisen arvion mukaan osoitteita riittää vielä muutamaksi vuodeksi.

IP-protokollan versio 6 on suunniteltu nykyisen korvaajaksi, ja siinä osoitteita on käytettävissä valtavan paljon enemmän. Protokollaa käytetään jo jonkin verran, enimmäkseen kokeilumielessä, mutta sen osuus internetin tietoliikenteestä on toistaiseksi häviävän pieni.

IPv6:n ottaminen käyttöön tulee olemaan pitkäaikainen hanke, joka todennäköisesti vaikuttaa lähes kaikkiin internetiin kytkettyihin tietokoneisiin ja verkon aktiivilaitteisiin. Osa laitteista voi muuttua kokonaan käyttökelvottomiksi, ja valtaosaan niistä tulee joka tapauksessa asentaa ainakin ohjelmistopäivityksiä. Siirtymäajasta tulee varmasti myös pitkä.

Kokemuksia IPv6:n laajamittaisesta käytöstä on toistaiseksi varsin vähän. On odotettavissa, että itse protokollasta ja sen varaan toteutettujen ratkaisujen suunnittelusta tullaan löytämään uusia toiminnallisia ja myös tietoturvaan liittyviä puutteita.

IPv6:n käyttäjien pienestä osuudesta huolimatta tuli CERT-FI:n tietoon vuonna 2008 ensimmäinen IPv6-protokollaa käyttävä Suomesta löytnyt haittaohjelma.

## **Haittaohjelmia levitetään murrettujen www-sivustojen kautta**

Haittaohjelmien levittäminen perustuu usein siihen, että haittaohjelmat käyttävät hakukoneita etsiäkseen sivustoilta esimerkiksi SQL injection -tyyppisiä haavoittuvuuksia, jotka mahdollistavat sivujen sisällön muokkaamisen. Kun haavoittuva palvelin löytyy, sen sivuille lisätään pieni JavaScript-viittaus, jonka tarkoituksena on tarjota sivuilla vierailijalle ladattavaksi haittaohjelma. Sivuille lisätty ylimääräinen linkki voi helposti jäädä huomaamatta sivuston ylläpitäjältä.

Www-sivustojen ylläpitoon yleisesti käytettävistä julkaisujärjestelmistä löytyy jatkuvasti uusia haavoittuvuuksia, jotka mahdollistavat koodin lisäämisen sivustoille. Tämän vuoksi julkaisujärjestelmien ja niihin liittyvien oheisohjelmistojen tietoturvapäivityksistä huolehtiminen on tärkeää.

Haittaohjelman tartuttamiseksi käyttäjän tietokoneelle ei välttämättä käytetä hyväksi ohjelmistohaavoittuvuuksia, vaan haittaohjelma voidaan naamioida esimerkiksi videotiedostojen katselua varten tarjottavaksi ohjelmaksi tai jopa tietoturvaohjelmistoksi, kuten vakoiuohjelmien poistajaksi, palomuuriksi tai virustorjuntaohjelmaksi. Käyttäjä houkutellessaan asentamaan tällainen ohjelma itse tietokoneeseensa. Joissakin tapauksissa käyttäjä voi jopa ostaa ja maksaa tällaisen ohjelmiston asentamisen. Luvattomien ohjelmistokopioiden asennuspakettien tai niihin liittyvien lisenssiavainten murto-ohjelmien mukana on myös usein haittaohjelma.

Linkkejä haittaohjelmiin levitettiin www-sivujen ja sähköpostiviestien lisäksi jonkin verran myös pikaviestimillä.

## **Verkkomato levisi vuodenvaihteessa**

Vuoden lopulla havaittiin lähiverkossa itsenäisesti leviävä haittaohjelma, joka on saastuttanut tietokoneita sekä kotimaisissa että ulkomaisissa verkoissa. Mato pyrkii leviämään koneiden välillä monilla eri tavoilla ja ottamaan tartunnan jälkeen yhteyttä satunnaiselta näyttävään, päiväyksen ja kellonajan perusteella muodostettaviin verkko-osoitteisiin päivittääkseen itsensä.

## **Huijaussivustot ja -sähköpostiviestit eivät ole juuri kiusanneet suomalaisia käyttäjiä**

Kovin uskottavia suomenkielisiä sähköisiä asiointipalveluja jäljitteleviä huijaussivustoja ei vuoden aikana ole tavattu. Suurin osa varsinaisista huijaussivustoista näyttääkin keskittyneen ulkomaisten palvelujen asiakkaisiin. Murretuilta suomalaisilta www-palvelimilta on löydetty useita ulkomaisia palveluja jäljitteleviä huijaussivuja. Kevättalvella levitettiin sähköpostiviestejä, joiden mukana jaetun linkin kautta saattoi tietokoneeseensa tartuttaa haittaohjelman. Sen avulla pyrittiin kaappaamaan käyttäjän verkkopankkiyhteys. Tämä "Mikkelin ydinvoimalaonnettomuudesta" tai "seuraa etsivästä Tatjanasta" kertova viesti houkuttelikin monet asentamaan tietokoneeseensa haittaohjelman. Samaa viestiä ja haittaohjelmaa levitettiin myös useissa muissa Euroopan maissa.

## **Verkkoaktivismi oli melko hiljaista**

Vuoden aikana ei nähty merkittäviä kotimaisiin palveluihin kohdistuneita palvelunestohyökkäyksiä tai sivustojen töhrimisiä. Suomen isännöimän ETYJ-kokouksen järjestelyihin ei liittynyt erityisiä tietoturvasuustapauksia.

Georgian konfliktin yhteydessä murrettiin joitakin sikäläisiä www-palvelimia ja niiden sivuille lisättiin propagandasisältöä.

## Tulevaisuuden näkymiä

CERT-FI:n arvion mukaan etähallittavien ja päivitettävien haittaohjelmien levittäminen tietokoneisiin on merkittävä uhka käyttäjien tietoturvallisuudelle. Haittaohjelmat kehittyvät entistä monikäyttöisemmiksi, jolloin kerran tartunnan saanutta konetta voidaan käyttää monenlaiseen haitalliseen toimintaan päivittämällä haittaohjelman ominaisuuksia.

Haittaohjelmien levitystavat tulevat edelleen kehittymään. Murretuilla www-sivustoilla ja houkuttelevilla roskapostiviesteillä tulee edelleen olemaan merkittävä rooli. Ohjelmia pyritään tartuttamaan sekä laajoilla levityskampanjoilla että rajatumilla täsmäjakeluilla.

CERT-FI-yhteydenotot nimikkeittäin	1-3/2008	4-6/2008	7-9/2008	10-12/2008	2008	2007	Muutos
Haastattelu	17	29	21	21	<b>88</b>	80	+10%
Haavoittuvuus tai uhka	39	232	52	71	<b>375</b>	64	+485%
Haittaohjelma	460	727	532	437	<b>2156</b>	1678	+28%
Neuvonta	64	87	92	116	<b>359</b>	393	-9%
Hyökkäyksen valmistelu	32	27	12	16	<b>87</b>	3	+2800%
Tietomurto	14	88	45	40	<b>187</b>	119	+57%
Palvelunestohyökkäys	15	26	31	24	<b>96</b>	64	+50%
Muu tietoturvaongelma	10	11	12	10	<b>43</b>	48	-10%
Social Engineering	47	36	44	62	<b>189</b>	197	-4%
Roskaposti (ei tilastoitu 2008-)	-	-	-	-	-	18	-
<b>Yhteensä</b>	<b>698</b>	<b>1263</b>	<b>841</b>	<b>797</b>	<b>3580</b>	<b>2664</b>	<b>+34%</b>

Suurin osa CERT-FI:n käsittelemistä yhteydenotoista liittyi erilaisiin haittaohjelmiin ja niistä johtuviin tietoturvauxkiin. Ilmoitukset haittaohjelmista muodostivat yksinään kaksi kolmasosaa kaikista yhteydenotoista.