



CERT-FI TILANNEKATSAUS 3/2004

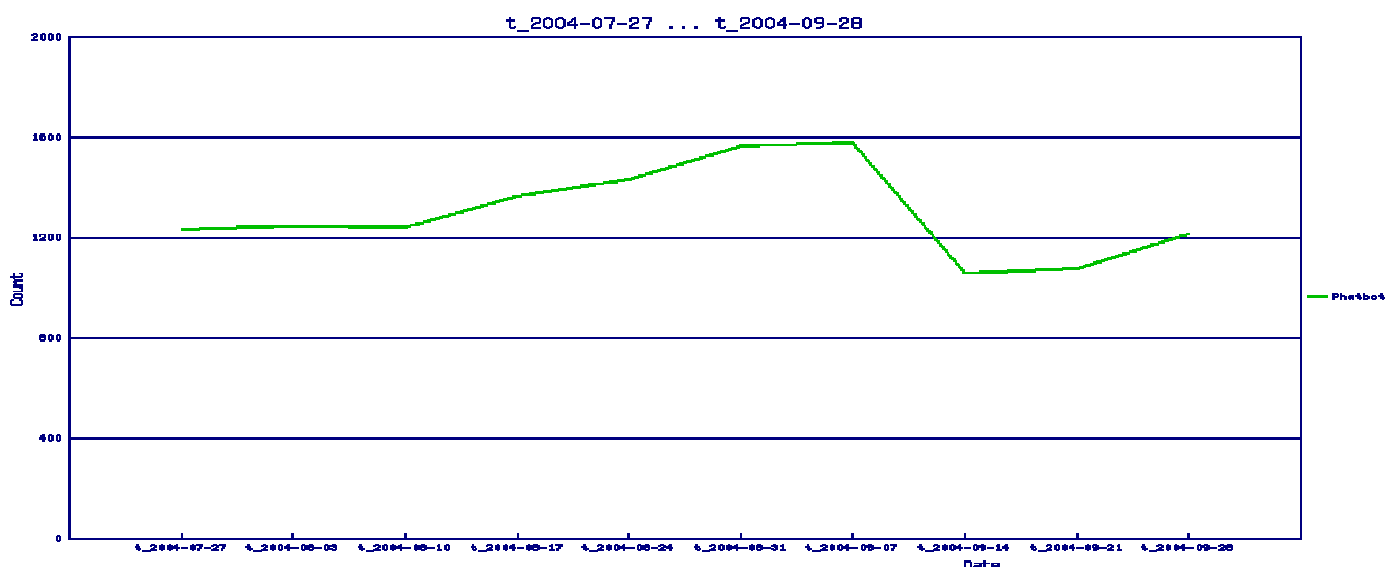
Tietoturvaongelmia aiheuttivat Suomessa kolmannen vuosineljänneksen aikana erityisesti erilaiset bot-haittaohjelmat. Bot-haittaohjelmien tunnistamista vaikeuttivat erittäin nopeaan tahtiin kirjoitetut uudet variantit, joita tarkasteluajanjaksolla ilmestyi tuhansia. Suomessa useat merkittävätkin organisaatiot kokivat bot-haittaohjelmatartunnan sisäverkossaan.

Maailmalla esille tulleista ilmiöistä korostui phishing-toiminta. Phishing-toiminnassa käyttäjä yritetään saada luovuttamaan tietoja aidolta näyttävään verkkopalveluun, joka onkin väärennetty ja jonka tarkoitus on kerätä luottokorttitietoja, verkkopalvelun kirjautumistietoja tai henkilötietoja rikollista toimintaa varten. Tarkastelujaksolla levisi myös haittaohjelmia, jotka keräsivät taloudellista tietoa suoraan saastuneesta järjestelmästä käyttäjän syötteitä tarkastelemalla. Haavoittuvat kotitietojärjestelmät ovat edelleen hyväksikäytetyimpiä tietojärjestelmiä.

Haittaohjelmat

Heinä–syyskuussa esille tulleista haittaohjelmista merkittävimpiä olivat erilaiset bot-haittaohjelmat (Phatbot, SDbot, Agobot). Bot-haittaohjelmien ominaisuuksiin kuuluu mm. yhteydenotto IRC (Internet Relay Chat) -komentokanavalle, jonka kautta hyökkääjä voi antaa saastuneelle tietojärjestelmälle komentoja. Saastuneet tietojärjestelmät päätyvät tyypillisesti roskapostin lähetyiskanaviksi ja palvelunestohyökkäyksiin osallistuviksi järjestelmiksi. Laajamittaisilla hajautetuilla palvelunestohyökkäyksillä uhkaamalla pyritään mm. kiristämään rahaa erilaista online-toimintaa harjoittavilta yrityksiltä. Kesän aikana ilmestyi nopeasti tuhansia varianteja bot-ohjelmista, mikä vaikeutti huomattavasti niiden nopeaa havaitsemista.

Tarkastelujaksolla useat merkittävät suomalaiset organisaatiot kokivatkin bot-tartunnan työasemaverkossaan. Tarkasteluajalla CERT-FI:n havaintojen ja saamien tietojen mukaan bot-haittaohjelmalla saastuneita suomalaisia järjestelmiä oli jatkuvasti 1500 – 2000. CERT-FI:n arvio saastuneiden tietojärjestelmien kokonaismäärästä on kuitenkin 2500 – 3500. Tarkasteluajanjakson aikana ei koettu erityisen pahoja sähköpostivirusepidemioita. Www-sivujen kautta levinneiden troijalaisten suhteellinen osuus saastumistapauksiin nähden kasvoi.



Kuva 1. CERT-FI:n tietoon tulleet Phatbot-haittaohjelmilla saastuneet järjestelmät viikottain



Roskaposti

Tarkasteltavan ajanjakson aikana roskapostin osalta ei tapahtunut merkittäviä muutoksia: roskapostin määrän lisääntyminen ja havaitsemisen vaikeus kehittyivät tasaisesti. Tarkasteluajankohtana roskaposti ei aiheuttanut merkittäviä ongelmia Suomessa sähköpostipalveluiden toimintaan. Roskapostitukseen liittyi voimakkaasti laittomien tietokoneohjelmistokopioiden kauppaaminen, perinteiset huijauskirjeet sekä phishing-toiminta.

Ongelmatietojärjestelmien lukumäärä Suomessa

CERT-FI:lle tulleiden tietojen mukaan suomalaisissa tietoverkoissa on jatkuvasti noin 3500 tietoturvaongelmista kärsivää tietojärjestelmää. Ongelmakoneiksi luetaan saastuneeksi tai murretuiksi havaitut järjestelmät sekä erilaiset avoimet välityspalvelimet.

Tietomurrot ja hyväksikäytetyimmät haavoittuvuudet

CERT-FI:n tietoon tulleiden tapausten perusteella tarkasteltavalla ajanjaksolla hyväksikäytetyin haavoittuvuus oli Microsoft Windows LSASS –haavoittuvuus, jota etupäässä hyväksikäytettiin automatisoiduilla hyökkäysohjelmilla ja jota hyväksikäytti myös monet bot-haittaohjelmat. CERT-FI julkaisi keväällä LSASS-haavoittuvuudesta varoituksen 25/2004. Eryyisen hyväksikäytetty haavoittuvuus oli myös Internet Explorer –selainohjelman ADODB.Stream-haavoittuvuus. CERT-FI julkaisi haavoittuvuudesta varoituksen 40/2004.

Tulevaisuuden näkymät

CERT-FI:n arvion mukaan bot-haittaohjelmiin liittyvä kehitys tulee jatkumaan. Lähitulevaisuudessa bot-haittaohjelmat käyttävät edelleen merkittävimpänä leviämisreittinä Windows-käyttöjärjestelmän LSASS–haavoittuvuutta.

Microsoft Windows JPEG –kuvatiedostojen käsittelyyn liittyvän haavoittuvuuden hyväksikäyttö tulee voimakkaasti lisääntymään. Hyväksikäyttö voi tapahtua sekä www-sivustojen että sähköpostin välityksellä. Mahdollisesti myös kesän ja alkusyksyn aikana julkaistuja kuvaformaattien käsittelyyn liittyviä haavoittuvuuksia tullaan hyväksikäyttämään erityisesti palomuurin läpäisemisessä.

Internet Explorer –selainohjelmasta on julkaistu lukuisia haavoittuvuuksia, joita osaa tullaan käyttämään laajamittaisesti hyväksi. Mahdollisesti myös syyskuussa julkaistuja Mozilla-selainohjelman haavoittuvuuksia hyväksikäytetään laajamittaisesti.

Tietoturvaloukkaustrendeissä taloudellista hyötyä tavoittelevat loukkaukset jatkanevat voimakasta lisääntymistä seuraavan vuosineljänneksen aikana.

Internetin uhiin varautumisessa on edelleen huomioitava palomuurin sekä turvallisten ohjelmistoversioiden käyttäminen. Eryyisesti tämä koskee Microsoft Windows -käyttöjärjestelmästä sekä Microsoft Internet Explorer –selainohjelmasta löydettyjä haavoittuvuuksia.