



CERT-FI TILANNEKATSAUS 1/2005

Ensimmäisellä vuosineljänneksellä 2005 hyväksikäytettiin laajamittaisesti phpBB-ohjelmistosta löydettyjä haavoittuvuuksia mm. Santy-nimisen haittaohjelman avulla. Mobiililaitteille kohdistettujen haittaohjelmien leviämismekanismieissa nähtiin myös kehitystä. Ensimmäinen multimediasivustojen välityksellä leviävä haittaohjelma ilmestyi.

Teleyritykset ovat tehneet merkittäviä toimia roskapostiongelman hallitsemiseksi rajoittamalla kuluttajaliittymistä lähtevää sähköpostiliikennettä Viestintäviraston antaman määräyksen sähköpostipalveluiden tietoturvesta ja toimivuudesta mukaisesti.

Tarkastelujaksolla julkaistiin jälleen joukko merkittäviä ohjelmistohaavoittuvuuksia. Uutena trendinä nousi esiin eri ohjelmistovalmistajien virustorjuntatuotteista löydetyt haavoittuvuudet.

Haittaohjelmat

Ensimmäisellä vuosineljänneksellä 2005 Suomessa ongelmia aiheuttivat edelleen ns. bot-haittaohjelmat. Osaa näistä haittaohjelmista levitettiin hyökkääjien toimesta www-sivustojen välityksellä. Viime vuoden loppupuolella leviämisensä aloittanut phpBB-ohjelmiston haavoittuvuutta hyväksikäyttävä Santy-haittaohjelma jatkoi leviämistään myös vuoden 2005 ensimmäisellä neljänneksellä saastuttaen useita www-palvelimia, jotka oli varustettu haavoittuvalla phpBB-ohjelmistoversiolla.

Mobiililaitteille suunnattujen haittaohjelmien ominaisuudet kehittyivät ensimmäisen vuosineljänneksen aikana. Maailmalla älypuhelimia saastuttivat jonkin verran Cabir-haittaohjelman eri versiot sekä CommWarrior, joka leviää Bluetooth-tietoliikenneyhteyden lisäksi multimediasivustojen välityksellä. Mobiili-haittaohjelmat eivät kyenneet leviämään älypuhelimesta toiseen itsenäisesti. Mobiili-haittaohjelmien saaminen matkapuhelimeen on edelleen epätodennäköistä.

Tarkkailujaksolla levisi myös ensimmäinen selainohjelmariippumaton java-ohjelmointirajapintaa hyödyntävä haittaohjelma nimeltään Java.OpenStream.T. Haittaohjelma ei kuitenkaan CERT-FI:n tietojen mukaan saastuttanut merkittävästi suomalaisia tietojärjestelmiä.

Ensimmäisellä vuosineljänneksellä merkittävimmäksi sähköpostimadoksi nousi Mydoom.BB, joka on tyypillinen sähköpostin liitetiedoston välityksellä leviävä haittaohjelma. Mato sisältää takaportt ominaisuuden, jonka välityksellä hyökkääjän on mahdollista suorittaa saastuneessa kohdejärjestelmässä omia komentojaan.

Roskaposti

Suomalaiset teleyritykset ovat tehneet Viestintäviraston sähköpostipalveluiden tietoturvesta ja toimivuudesta antaman määräyksen mukaisia toimenpiteitä yleisen roskapostiongelman rajoittamiseksi. Vastaavia toimenpiteitä on laajasti käytössä myös ulkomaisilla Internet- ja sähköpostipalveluntarjoajilla roskapostiongelman hallitsemiseksi. Internet-palveluntarjoajat rajoittavat mm. suomalaisten teleyritysten tavoin kuluttaja-asiakkaiden suoraa sähköpostiliikennöintiä kuluttajaliittymästä Internetiin ohjaamalla sähköpostiliikenteen teleyrityksen tai sähköpostipalveluntarjoajan sähköpostipalvelimen kautta niin saapuvan kuin lähtevän sähköpostiliikenteen osalta.

Roskapostituksen rajoittamisessa kyseisen tarkastelujakson aikana on todettu myös varsin tiukkoja toimenpiteitä, kun suuri yhdysvaltalainen palveluntarjoaja on estänyt sähköpostin vastaanottamisen



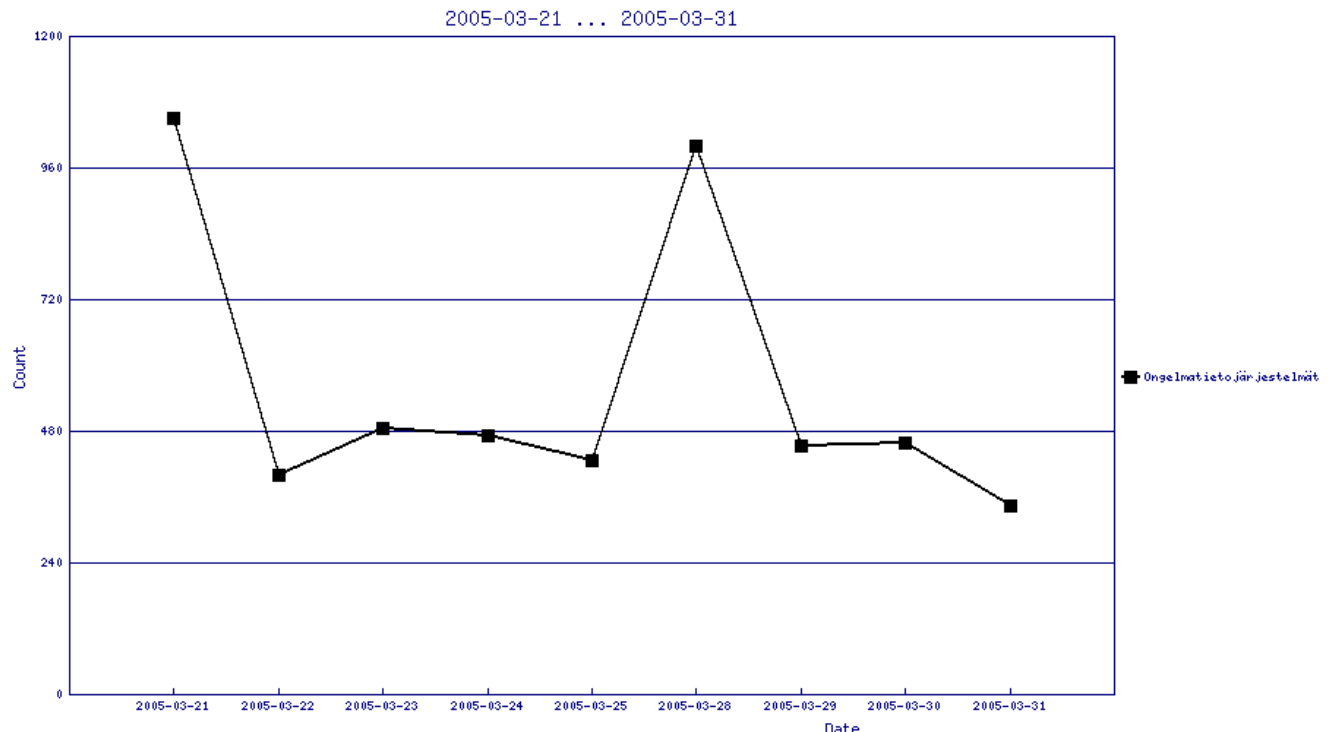
Euroopasta vedoten roskapostiliikenteen vähentämiseen.

Roskapostin määrä pysytteli tarkastelujakson aikana Suomessa CERT-FI:n arvioin mukaan noin 35 - 40 prosentissa kaikista sähköpostiviesteistä, edelleen yksittäisten liikennehuippujen kohotessa jopa 80 prosenttiin kaikista sähköpostiviesteistä. Roskapostin määrä vaihteli merkittävästi eri kohdeorganisaatioiden välillä.

Kansainvälisten tietojen mukaan roskapostin kokonaismäärissä ei ole tapahtunut merkittävää muutosta, mutta roskapostilähteiden kokonaismäärä on vähentynyt.

Ongelmatietojärjestelmien lukumäärä Suomessa

Ensimmäisellä vuosineljänneksellä 2005 CERT-FI:n päivittäin käsittelemä ongelmatietojärjestelmien lukumäärä vaihteli 300 tietojärjestelmästä aina yli 1000 tietojärjestelmään. Suurin osa ongelmatietojärjestelmistä oli saanut bot-haittaohjelmatartunnan tai oli joutunut roskapostin lähetykskanavaksi. Päivittäinen vaihtelu ongelmatietojärjestelmien lukumäärässä oli merkittävä.



Kuva 1. Ote CERT-FI:n päivittäin käsittelemästä ongelmatietojärjestelmien lukumäärästä ensimmäisellä vuosineljänneksellä 2005.

Hyväksikäytetyimmät haavoittuvuudet

CERT-FI:n saamien tietojen mukaan ensimmäisellä vuosineljänneksellä Suomessa hyväksikäytettiin laajasti phpBB-ohjelmistossa olleita haavoittuvuuksia. CERT-FI sai myös lukuisia yhteydenottoja www-palvelimien tietomurroista, joissa hyväksikäytettiin AWStats-ohjelmiston haavoittuvuutta.



Vuoden ensimmäisellä tarkastelujaksolla löydettiin vakavia ohjelmistohaavoittuvuuksia Mozilla Firefox -selainohjelmasta sekä RealPlayer-mediaohjelmistosta. Vaikka haavoittuvuuksille on olemassa julkisesti saatavilla olevia haavoittuvuuksien hyödyntämismenetelmiä, haavoittuvuuksia ei CERT-FI:n tietojen mukaan hyväksikäytetty tarkastelujaksolla laajamittaisesti suomalaisia tietojärjestelmiä vastaan.

Samoin ensimmäisellä vuosineljänneksellä merkittäviksi ohjelmistohaavoittuvuuksiksi nousivat virustorjuntaohjelmistoista löytyneet haavoittuvuudet, jotka koskivat mm. F-Securen Anti-Virus - tuotteita sekä TrendMicro- ja McAfee-virustorjuntaohjelmistoja. Virustorjuntaohjelmistoja päivitetään kuitenkin pääosin automaattisesti. Merkittäviä ohjelmistohaavoittuvuuksia löydettiin myös Microsoft-ohjelmistotuotteista, joista osaa voi olla mahdollista hyväksikäyttää esimerkiksi verkkomadon avulla.

Vuoden 2005 ensimmäisellä tarkastelujaksolla hyväksikäytettiin kansainvälisesti myös Symantec Gateway Security -tuotteista löydettyä haavoittuvuutta, joka löydettiin kesällä 2004. Haavoittuvuutta hyväksikäytettiin ohjaamalla käyttäjiä haitallista ohjelmakoodia jakeleville sivustoille manipuloimalla välimuistissa olleita nimipalvelutietoja. Tarkastelujaksolla julkaistiin myös merkittäviä reitittimiin liittyviä haavoittuvuuksia, joiden hyväksikäytöllä olisi voinut olla vakava uhka koko viestintäverkkojen toimivuudelle. Suomessa teleyritykset ja Internet-palveluntarjoajat päivittivät kuitenkin verkkolaitteensa välittömästi ohjelmistopäivityksen julkaisemisen jälkeen.

Sun Java -ohjelmistosta löydettiin myös vakava haavoittuvuus, jota voidaan hyväksikäyttää mm. www-sivuston välityksellä. Erityisenä huomiona tämän haavoittuvuuden osalta on pidettävä sitä, että selainohjelmien käyttäjät eivät välttämättä ymmärrä päivittää haavoittuvaa Sun Java -ohjelmistoversiota.

Tarkastelujaksolla nähtiin edelleen viime vuoden viimeisen vuosineljänneksen tapaan SSHD-palvelua vastaan kohdistettuja sanakirjahyökkäyksiä, joilla pyrittiin selvittämään kohdejärjestelmän käyttäjätunnuksia ja salasanoja. Hyökkäykset SSHD-palvelua vastaan eivät liittyneet ohjelmistohaavoittuvuuksiin.

Tulevaisuuden näkymät

Seuraavalla vuosineljänneksellä voi olla mahdollista, että hyväksikäyttöyritykset Internet Explorer -selainohjelmasta ja Outlook-sähköpostiohjelmistosta maaliskuussa 2005 löydettyjä haavoittuvuuksia vastaan lisääntyvät. Tiettyjen vuoden ensimmäisellä neljänneksellä julkaistujen vakavien ohjelmistohaavoittuvuuksien hyväksikäyttö tulee todennäköisesti lisääntymään. Haavoittuvuuksista merkittävimpana voidaan pitää Microsoft SMB -protokollaan liittyvää haavoittuvuutta.

Internet-palveluntarjoajien ja teleyritysten yleistyvät toimenpiteet lähtevän sähköpostiliikenteen rajoittamiseksi vaikuttavat haittaohjelmien kehitykseen. Roskapostin lähestyskanaviksi valjastetut tietojärjestelmät joutuvat jatkossa välittämään lähtevän roskapostiliikenteen Internet-palveluntarjoajien tai teleyritysten sähköpostipalvelimien välityksellä.

Mobiili-haittaohjelmien ominaisuudet kehittyvät edelleen, ja jo olemassa olevista haittaohjelmista tullaan julkaisemaan uusia variantteja. Jatkossa haittaohjelmien levittämismekanismina tullaan edelleen käyttämään Bluetooth-yhteyttä sekä multimediatekstejä. Seuraavan kahden vuosineljänneksen aikana voi olla mahdollista, että mobiililaitteille ilmestyy ensimmäinen itsenäisesti leviävä haittaohjelma, jonka toteuttaminen tosin vaatii edelleen teknisesti monimutkaisempia sekä haasteellisempia toimia.

Virustorjuntaohjelmistoista löydettyjen haavoittuvuuksien laajamittainen hyödyntäminen on epätodennäköistä virustorjuntaohjelmistojen automaattisten päivitysominaisuuksien vuoksi.