



13.4.2007



## TIETOTURVAKATSAUS 1/2007

Vuoden ensimmäisellä neljänneksellä CERT-FI:n tietoon tuli tavanomaista enemmän palvelunestohyökkäyksiä tai niiden yrityksiä. Mainittavimmat hyökkäykset kohdistuivat Internetin nimipalvelimiin sekä suomalaisen yrityksen verkkopalveluihin. Hyökkäys suomalaista kohdetta vastaan toteutettiin tavanomaisesta poiketen itsenäisesti toimivan haittaohjelman avulla.

Verkkopankkiasiakkaiden käyttäjätunnusten ja salasanojen huijaamiseen käytettäviä sivustoja mainostettiin laajasti levitetyissä roskapostiviesteissä. Osa huijauspalvelimista ja niihin johdettavista verkkotunnuksista pysyi aktiivisena jopa viikkojen ajan. Kaikki sijaitsivat ulkomaisissa verkoissa. Suomalaisiin palveluihin kohdistuneet vakoiluohjelmatapaukset ovat olleet toistaiseksi harvinaisia, joskin merkkejä muutoksesta on havaittavissa.

Ohjelmistohaavoittuvuuksia löydettiin työasemissa käytettävien ohjelmistojen lisäksi internet-reitittimistä ja teollisuuden prosessien ohjaukseen käytettävistä SCADA-järjestelmistä. Haavoittuvuuksien julkaiseminen erityisinä tiettyihin ohjelmistoihin tai käyttöjärjestelmiin keskittyvinä teemakampanjoina jatkuu.

### Palvelunestohyökkäys juurinimipalvelimia vastaan

Internetin juurinimipalvelimia vastaan kohdistettiin palvelunestohyökkäys helmikuun alussa. Hyökkäys toteutettiin kaapattujen tietokoneiden muodostaman botnet-verkon avulla ja se kesti noin vuorokauden. Vaikka hyökkäysvolyyymi oli huomattava, sen käytännön vaikutukset jäivät vähäisiksi kymmenen juuripalvelimen säilyessä toimintakykyisenä. Kolmen loogisen juuripalvelimen toiminnan estyminen näkyi suurimmalle osalle käyttäjistä ainoastaan ajoittaisena internetin käytön hidastumisena.

Hyökkäyksen yhteydessä havaittiin myös estoa joidenkin kansallisten verkkotunnusten nimipalveluissa. Osa häiriöistä johtui siitä, että kyseisten maatunnusten nimipalvelut tuotettiin samalla järjestelmällä kuin internetin juuren.

FI-verkkotunnuksen palvelutasoon hyökkäyksillä ei ollut vaikutusta, joskin valmiustasoa korotettiin joksikin aikaa yhdessä nimipalvelimia ylläpitävien tahojen kanssa. FI-nimipalvelinten toimintaa tarkkailevan järjestelmän käyttöönottoa päätettiin aikaistaa.

### Avointen nimipalvelinten käyttäminen palvelunestohyökkäystyökaluna

Koska nimipalvelujärjestelmässä ei tarkisteta osapuolten aitoutta, on palvelujärjestelmä altis osoiteväärennöksille. Tätä ominaisuutta väärinkäyttämällä niin sanotun rekursiivisen resolverinimipalvelimen voi saada toimimaan vahvistavana hyökkäyspeilinä ohjaamalla palvelimen tuottamat nimenselvityspyyntöjen vastaukset hyökkäyksen kohteena olevalle kolmannelle osapuolelle. Kun väärennettyjä kyselyjä lähetetään suuri määrä useisiin nimipalvelimiin, saadaan kohteessa aikaan hajautettu palvelunestohyökkäys. Liikenteen aiheuttajan selvittäminen on yleensä vaikeaa ja vaatii useiden osapuolten aktiivista yhteistyötä.

CERT-FI sai 9.2.2007 tiedon hyvin laajasta palvelunestohyökkäyksestä, jossa hyödynnettiin myös suomalaisia nimipalvelimia. Vastaava hyökkäys toistui 28.2.2007. Suomalaisten palvelinten ylläpitäjiin otettiin molemmilla kerroilla yhteyttä ja näitä neuvottiin muuttamaan palvelimien asetukset sellaisiksi, ettei niiden hyödyntäminen hyökkäykseen olisi enää mahdollista.



13.4.2007

CERT-FI

## Fire and forget -palvelunestohyökkäys

Heinäkuusta 2006 lähtien tietoverkoissa on levinnyt Allapleksi nimetty haittaohjelma, jonka ainoa tarkoitus on estää tiettyjen verkkopalvelujen toiminta. Tapauksesta tekee mielenkiintoisen se, että yksi kohteista sijaitsee suomalaisessa verkossa.

Palvelunestohyökkäyksissä käytetään tavallisesti etäohjattavaa botnet-verkkoa. Allaple-verkkomato toimii kuitenkin toisin. Haittaohjelma ainoastaan levittää itseään ja aiheuttaa häiritsevää verkkoliikennettä ohjelman laatijan määäämiin osoitteisiin. Liikkeelle laskemisen jälkeen ohjelma toimii täysin itsenäisesti, eikä siihen ole komento- tai ohjausyhteyttä.

Komentoyhteyden puuttuminen tarkoittaa myös sitä, ettei kerran leviämään päässeen madon aiheuttamaa liikennettä voi enää pysäyttää. Ongelma poistuu vasta kun kaikki saastuneet tietokoneet on poistettu verkosta ja haittaohjelman leviäminen pysähtyy. Ohjelman aiheuttaman haitallisen verkkoliikenteen suodattaminen on vaikeaa, sillä yhteyksiä tulee eri puolilta maailmaa ja liikenne näyttää samanlaiselta kuin palvelun oikeutettujen käyttäjien yhteydet.

Allaple on aiheuttanut kohteilleen suuria vaikeuksia teleoperaattorin toteuttamista raskaista verkkoliikenteen suodatustoimista huolimatta.

## Palvelunestohyökkäykset sähköpostipalvelimia vastaan

CERT-FI:n tietoon tuli myös suomalaisiin sähköpostipalvelimiin kohdistuneita palvelunestohyökkäyksiä.

Yksi hyökkäyksistä on ollut pitkäkestoinen, ja sen tarkoituksena on saattanut olla kohdejärjestelmän suorituskyvyn selvittäminen. Kasvanut yhteyksien määrä on näkynyt palvelinten kuormituksen kasvuna, mutta palvelu ei ole kuitenkaan kokonaan tukkeutunut. Hyökkäyksessä palvelinta on kuormitettu lähettämällä viestejä keksittyihin osoitteisiin.

Maaliskuun loppupuolella hyökättiin erään suomalaisen yrityksen sähköpostipalvelimia vastaan rajusti niin, että sähköpostin välittäminen palvelimia käyttäneisiin yrityksiin oli estyneenä useiden tuntien ajan. Hyökkääjä avasi suuren määrän yhteyksiä palvelimiin, mutta jätti yhteydet odottamaan aikakatkaisua.

Tällaisia hyökkäyksiä on vaikeaa torjua yhteyksiä rajoittamalla, sillä hyökkäysliikenne muistuttaa oikeutettuja sähköpostin välitysyhteyksiä. Hyökkäykseen käytettäviä tietokoneita voi olla satoja tai tuhansia eri verkoissa. Suomalaisten koneiden käyttäminen hyökkäystyökaluina on vaikeaa, sillä Viestintäviraston määräyksen 11/2004 M mukaisesti SMTP-liikenne kuluttajaliittymistä on pääsääntöisesti sallittu vain internet-operaattorin omaan sähköpostipalvelimeen.

## Internet-huijausten uusi aalto

Maaliskuussa havaittiin jälleen laaja phishing-operaatio, jossa pyrittiin urkkimaan muiden muassa Nordea-pankin asiakkaiden käyttäjätunnuksia ja tunnuslukuja. Miljoonien roskapostiviestien mukana lähetettiin linkkejä huijaussivustoille, joita oli perustettu useisiin eri maihin. Tällä kertaa sivustoille houkuteltiin myös suomalaisia asiakkaita.

Suurin osa huijaussivustoilla käytetyistä verkkotunnuksista oli rekisteröity Hong Kongiin ja palvelimia löytyi mm. Virosta, Romaniasta, Bulgariasta, Koreasta, Chilestä, Ranskasta ja Yhdysvalloista. Nordea ei suinkaan ollut ainoa huijausten kohde, vaan samoilla palvelimilla toimi yhtä aikaa kymmeniä tai jopa satoja eri palveluja jäljitteleviä huijaussivustoja.



13.4.2007

CERT-FI

Sivustojen toteutustapa viittaa siihen, että siinä on käytetty Rock Phish Kit -työkalupakettia, joka sisältää valmiit asetukset useiden verkkopankkeja matkivien sivustojen luomiseksi. Paketin avulla voi luoda nopeasti suuren joukon sivuja, joiden avulla voi kerätä käyttäjien käyttäjätunnuksia ja salasanoja.

## Vakoiluohjelmilla urkittuja tietoja löytyy lisää

Tietoa varastavien ja tietokoneen käyttäjiä tarkkailevien haittaohjelmien uuden sukupolven synty voidaan ajoittaa helmikuulle 2006, jolloin virustorjuntayhtiö F-Secure sai ensimmäiset raportit Haxdoor-nimisestä haittaohjelmasta. CERT-FI vastaanotti ensimmäiset suomalaisia vakoiluohjelmien uhreja koskevat raportit heinäkuussa 2006. Sitten Haxdoorin lisäksi tapauksiin on liittynyt myös BZub- ja Torpig-nimillä tunnettuja haittaohjelmia.

CERT-FI:n tietoon on alkuvuonna tullut huomattavasti aiempaa enemmän vakoiluohjelmien käyttöön valjastettuja lokipalvelimia, joihin haittaohjelmamatartunnan saaneiden tietokoneiden käyttäjiltä varastetut tiedot kerätään. Lokipalvelimet sijaitsevat lähes poikkeuksetta ulkomailla ja huomattavan usein samoissa verkoissa. Toistaiseksi on vielä aikaista sanoa, johtuuko raportoitujen lokipalvelinten määrän kasvu vakoiluohjelmien yleistymisestä vai haittaohjelmatilannetta seuraavien tahojen havainnointikyvyn paranemisesta.

CERT-FI:n havaintojen mukaan suomalaisten palvelujen käyttäjät eivät ole huijausten tai vakoiluohjelmien pääkohde, mutta phishing-sivustojen ja haittaohjelmien luomiseen käytettävät työkaluohjelmistot tuntevat jo myös suomalaisia palveluja. Näyttää siltä, että haittaohjelmien kehittyessä myös pienemmät ja paikalliset sähköiset asiointipalvelut voivat joutua verkkourkinnan kohteiksi.

## Työasemien ohjelmistojen haavoittuvuudet

Työasemissa käytettävistä ohjelmistoista löydettiin alkuvuoden aikana jälleen useita haavoittuvuuksia, joista osaan ei ole vielä saatavilla korjausta.

Maaliskuun lopussa tuli julkisuuteen Windowsin ns. animoitujen kursorien (hiiren osoittimien) käsittelyyn liittyvä haavoittuvuus, johon ei ollut saatavilla korjausta. Haavoittuvuus koski useita Windows-versioita, myös uutta Windows Vistaa, ja sen hyödyntäminen web-sivun tai sähköpostiviestin avulla oli helppoa. Microsoft julkaisi korjauksen haavoittuvuuteen tavanomaista nopeammalla aikataululla heti huhtikuun alussa.

## Teollisuusohjelmistoissakin haavoittuvuuksia

Maaliskuussa julkaistiin haavoittuvuuksia SCADA-tuotteissa, joita käytetään teollisuudessa ohjaamaan tehtaiden prosesseja ja välittämään niihin liittyviä mittaustietoja. SCADA-tuotteiden turvallisuuteen ei ole perinteisesti kiinnitetty erityistä huomiota, sillä ne ovat sijainneet tuotantolaitosten suljetuissa verkoissa.

SCADA-tuotteet asettavat verkko- ja tietojenkäsittely-ympäristön turvallisuudelle suuria vaatimuksia. Tavanomaisetkin verkon häiriötilanteet voivat aiheuttaa vakavia virhetilanteita. SCADA-järjestelmiin liittyvät tietoturvaloukkaukset ovat lisääntyneet viime vuosina.

CERT-FI:n arvion mukaan maaliskuussa julkaistut haavoittuvuudet saattoivat muodostaa uhan myös yhteiskunnalle elintärkeiden toimintojen kannalta tärkeille järjestelmille. Haavoittuvuuksista lähetettiin kohdennettuja tiedotteita ja analyysyjä järjestelmien haltijoille.



13.4.2007

CERT-FI

Nyt julkaistut haavoittuvuudet löydettiin riippumattoman toimijan luoman testimateriaalin avulla. Todennäköisesti vastaavalla tavalla löydetään jatkossa lisää haavoittuvuuksia muista SCADA-järjestelmistä.

### **Verkkolaitteiden haavoittuvuus johti liikenteen suodattamiseen**

Internet-reititinlaitteissa käytettävän Cisco IOS -käyttäjärjestelmän 25.1. julkaistua haavoittuvuutta ehdittiin käyttää hyväksi palvelunestohyökkäyksissä ennen kuin kaikkia laitteita ehdittiin päivittää haavoittuvuuden korjaamiseksi. Hyökkäysten estämiseksi osa operaattoreista päätyi suodattamaan verkkoliikennettä – tämä saattoi näkyä käyttäjille tiettyjen verkon palvelujen käytön estymisenä.

### **Haavoittuvuuksien julkaisukampanjat jatkuivat**

Viime vuonna alkanut haavoittuvuusjulkaisujen politisoituminen on jatkunut. Tammikuussa julkaistiin 30 Apple-ohjelmistoihin liittyvää, aiemmin julkaisematonta haavoittuvuutta. "The Month of Apple Bugs" -teemakuukauden taustahenkilöiden ilmoittamana tavoitteena oli saada Apple suhtautumaan vastuullisemmin tuotteissaan esiintyviin haavoittuvuuksiin.

Maaliskuussa julkaistiin 44 PHP-haavoittuvuutta. PHP on suosittu verkkosovelluksissa käytetty ohjelmointikieli. Myös "The Month of PHP Bugs" oli vastaus ohjelmistojen kehittäjien tapaan käsitellä niistä löydettyjä haavoittuvuuksia.

### **Vika- ja häiriötilanteet**

Vakavia vika- ja häiriötilanteita ei esiintynyt. Aamupäivällä 19.2. TeliaSonera Finlandin kuluttaja- ja yrityssähköpostipalvelussa oli vika, joka esti sähköpostiviestien lukemisen ja kuluttaja-asiakkaiden osalta myös viestien lähettämisen noin kolmen tunnin ajan.

### **Tulevaisuuden näkymät**

CERT-FI:n arvion mukaan on odotettavissa, että tulevaisuudessa myös suomalaisten sähköisten asiointipalvelujen käyttäjät joutuvat järjestelmällisten väärinkäytösyritysten kohteeksi. Haittaohjelmien ja huijaussivustojen luomiseen käytettävissä työkalukokoelmissa esiintyy jo suomalaisten palvelujen verkko-osoitteita, nimiä ja muita asiasanoja.

Monet sähköiset asiointipalvelut ovat osoittautuneet haavoittuviksi palvelunestohyökkäyksille ja niihin kohdistettuja hyökkäyksiä saatetaan nähdä lisää. Hyökkäykset voivat kohdistua esimerkiksi www-palvelimiin, sähköpostipalvelimiin tai nimipalvelimiin. Palvelujen tarjoajien tulisi varautua vihamielisten hyökkäysten mahdollisuuteen. Hyökkäykset voidaan toteuttaa joko itsestään leviävien ja toimivien haittaohjelmien tai botnet-verkkojen avulla.

Haavoittuvuuksien julkaisukampanjoita todennäköisesti nähdään myös tulevaisuudessa ja niissä julkaistujen haavoittuvuuksien korjaaminen tulee työllistämään ohjelmistovalmistajia. Kaikki tähän mennessä ilmoitetut kampanjat eivät kuitenkaan ole toteutuneet tai niiden vaikutukset ovat julkisuuteen tulleiden tietojen valossa jääneet melko vähäisiksi.



13.4.2007

CERT-FI

## Sanastoa:

**Palvelunestohyökkäys** = Hyökkäys, jonka tarkoituksena on estää kohteena olevan palvelun normaali toiminta ja käyttö.

**Juurinimipalvelimet (root name servers)** = Hierarkkisesti järjestetyn internetin nimipalvelujärjestelmän huipulla olevat kolmetoista nimipalvelinta, jotka toimivat lähtöpisteenä nimipalvelutietoja etsittäessä.

**Botnet** = Murrettujen tietokoneiden ja niihin yhteydessä olevien komentopalvelinten verkosto. Murretut tietokoneet ovat etähallittavissa ja käytettävissä esimerkiksi roskapostin lähettämiseen tai palvelunestohyökkäyksiin ilman, että niiden käyttäjä välttämättä edes tietää asiasta.

**Resolverinimipalvelin (resolver)** = Nimipalvelin, jota internet-verkkoon liittynyt tietokone käyttää tekemiinsä nimipalvelukyselyihin. Kysyjä saa vastauksen resolveripalvelimelta, joka hoitaa nimipalvelutietojen selvittämisen kysyjän puolelta siitä eteenpäin.

**Rekursiivinen nimipalvelukysely (recursive dns query)** = Nimipalvelukysely, jossa resolverinimipalvelin selvittää kysytyn nimipalvelutiedon sen sijaan, että kysyvän tietokoneen tarvitsisi ottaa suoraan yhteyttä kyselyn kohteen autoritäärisen nimipalvelimeen.

**Autoritäärinen nimipalvelin (authoritative name server)** = Nimipalvelin, jolla ylläpidetään verkkotunnukseen liittyviä tietoja kuten IP-osoitteita, tietoa sähköpostin ohjauksesta jne.

**SCADA (Supervisory Control And Data Acquisition)** = Teollisuuden prosessinohjaus- ja mittaustiedon keruujärjestelmä.

**PHP** = Web-sivujen sisällön tuottamiseen ja muokkaamiseen käytettävä ohjelmointikieli

**SMTP (Simple Mail Transfer Protocol)** = Yhteyskäytäntö sähköpostiviestien lähettämiseksi sähköpostipalvelimelle sekä viestien välittämiseksi sähköpostipalvelinten välillä.