



11.10.2007



TIETOTURVAKATSAUS 3/2007

Botnet-hyökkäysverkkojen muodostamiseen käytettäviä haittaohjelmia on pyritty levittämään laajamittaisesti sähköpostin kautta. Storm Worm -haittaohjelman aktiivinen levittäminen roskapostiviestien avulla on tehnyt siitä yhden laajimmalle levinneistä haittaohjelmista.

CERT-FI:n tietoon on tullut yrityksiin kohdistettuja täsmähyökkäyksiä, joissa virustorjuntaohjelmistoille tuntemattomia haittaohjelmia on tartutettu yrityksen sisäverkon tietojärjestelmiin. Haittaohjelmia voidaan käyttää esimerkiksi yrityksen liiketoimintaan liittyvien tietojen urkkimiseen järjestelmistä. Kohdennettuja hyökkäyksiä on vaikeampaa havaita kuin yleisesti roskapostiviestien mukana levitettäviä haittaohjelmia.

Ohjelmistoista löytyi edelleen runsaasti haavoittuvuuksia. CERT-FI julkaisi kolmannen vuosineljänneksen aikana 60 tiedotetta vakavista ohjelmistohaavoittuvuuksista ja 26 Tietoturva nyt! -artikkelia. Varoituksia ei julkaistu.

Storm Worm leviää roskapostin mukana

Storm Worm on tammikuussa 2007 ensimmäisen kerran tavattu haittaohjelma, jota levitetään sähköpostin liitetiedostojen ja www-sivustojen kautta. Kesän ja syksyn aikana on ollut liikkeellä paljon roskapostiviestejä, jotka ovat sisältäneet linkin Storm Worm -haittaohjelmaa levittäville www-sivustoille. Storm Worm on tällä hetkellä yksi laajimmin levinneistä haittaohjelmista. CERT-FI:n tietoon ei kuitenkaan ole tullut merkittäviä määriä suomalaisissa verkoissa tavattuja tartunnan saaneita tietokoneita.

Storm Worm -tartunnan saaneet tietokoneet liittyvät osaksi hyvin laajaa Storm Worm -bottiverkkoa. Verkkoon kaapattujen tietokoneiden verkkoa komennetaan tehokkaasti hajautetulla ja vertaisverkkomaisella mekanismilla, ilman yhtä keskitettyä komentopalvelinta. CERT-FI:n saamien tietojen mukaan Storm Worm -bottiverkkoja käytetään aktiivisesti muun muassa palvelunestohyökkäyksiin ja roskapostitukseen.

Storm Wormin leviäminen perustuu pääasiassa englanninkielisiin, ajankohtaisista tapahtumista kertoviin tai muuten ihmisten mielenkiinnon herättäviin aiheisiin, joihin sähköpostiviesteissä viitataan. Niiden avulla lukijat saadaan seuraamaan viesteissä olevia linkkejä tai avaamaan haittaohjelman sisältäviä liitetiedostoja. Tietokoneeseen tarttuessaan Storm Worm asentaa siihen myös rootkit-toiminnallisuuden, minkä vuoksi sen havaitseminen on vaikeaa.

Storm Worm ei itse hyödynnä mitään erityistä ohjelmistohaavoittuvuutta, vaan viestien lukijat houkutellessaan asentamaan se itse työasemilleen klikkaamalla haittaohjelman sisältäviä linkkejä. Haittaohjelmaa levittävät www-sivustot pyrkivät kuitenkin hyödyntämään myös tunnettuja www-selainten haavoittuvuuksia, jolloin haittaohjelma voi asentua tietokoneeseen käyttäjän sitä huomaamatta. Säännöllisillä ohjelmistopäivityksillä huomaamattoman tartunnan todennäköisyyttä voi pienentää.

Microsoft Windows-käyttöjärjestelmän haittaohjelmanpoistaja (Malicious Software Removal Tool) osaa tunnistaa Storm Worm -haittaohjelman ja poistaa useimmat sen versioista.



11.10.2007



Yrityksiin kohdennettuja hyökkäyksiä

Yritysten www-sivustoja kohtaan tehdyt palvelunestohyökkäykset ovat saaneet paljon julkisuutta tiedotusvälineissä. Palvelunestohyökkäysten lisäksi yritysten tietoturvallisuutta voivat vaarantaa myös kohdennetut hyökkäykset, joissa haittaohjelmia pyritään tartuttamaan yrityksen tietojärjestelmiin. Tavoitteena voi olla esimerkiksi yrityksen liiketoimintaan liittyvien tietojen hankkiminen vakoiluohjelmien avulla. CERT-FI:n tietoon on tullut sellaisia tapauksia, joissa kohteena on ollut myös suomalaisia yrityksiä.

Kohdennetun hyökkäyksen tavoitteena on päästä käsiksi jonkin tietyn yrityksen tai organisaation järjestelmiin. Hyökkäyksessä voidaan käyttää varta vasten tätä tarkoitusta varten ohjelmoitua haittaohjelmaa, jota virustorjuntaohjelmistot eivät tunne. Tällaisia haittaohjelmien muunnoksia voi myös ostaa internetin kautta. Sen sijaan, että haittaohjelmaa levitettäisiin laajalla jakelulla helposti roskapostiksi tunnistettavien sähköpostiviestien mukana, niitä lähetetään vain pieniä määriä tarkoin valituille vastaanottajille. Hyökkääjä pyrkii siihen, ettei sen toimintaa havaittaisi ja vastatoimiin osattaisi ryhtyä.

Hyökkäykseen käytettävät haittaohjelmat lähetetään tavallisesti sähköpostiviestien liitteenä olevassa dokumentissa, joka käyttää hyväkseen jotain toimisto-ohjelmistojen tunnettua haavoittuvuutta. Massajakeluna levitettävistä roskapostiviesteistä poiketen itse viestin sisältö ja jakeluosoitteet on valittu huolellisesti niin, että jopa yrityksen omien työntekijöiden voi olla vaikeata huomata sisällössä mitään epäilyttävää. Viesti voi käsitellä yrityksen liiketoimintaan liittyviä todellisia asioita ja se voi myös olla lähetetty yrityksen sisäisellä sähköpostijakelulla.

Kohdennettujen hyökkäysten havaitseminen ja torjunta voi olla haastavaa, sillä automaattiset torjuntajärjestelmät eivät välttämättä niitä havaitse. Sekä käytettävät haittaohjelmat, että niiden tartuttamiseksi käytetyt menetelmät ovat yleensä taitavasti valittuja. Tunnettujen ohjelmistohaavoittuvuuksien paikkaaminen asentamalla valmistajan tarjoamat päivitykset pienentää tartunnan riskiä. Viestien sähköinen allekirjoittaminen yrityksen sisäisessä viestinnässä auttaisi viestin lähettäjän henkilöllisyyden varmentamisessa, mutta sitä käytetään harvoin.

Ohjelmistohaavoittuvuuksia löytyy edelleen paljon

Käyttäjärjestelmän komponentteihin, toimisto-ohjelmistoihin sekä selainohjelmistoihin liittyvät ohjelmistohaavoittuvuudet koskevat suurta osaa työasemien käyttäjistä. Niitä myös käytetään tavallisimmin hyväksi haittaohjelmien levittämiseen ja tietokoneiden kaappaamiseen esimerkiksi bottiverkkojen orjakoneiksi. Haavoittuvuuksia löytyi myös muun muassa pikaviestisovelluksista ja mediasoittimista.

Osa www-selaimiin liittyvistä haavoittuvuuksista liittyy selainten plugin-laajennuksiin, jolloin sama haavoittuvuus voi koskea useita eri ohjelmistoja.

Palvelinten haavoittuvuuksista kannattaa huomioida erityisesti PHP-ohjelmointikielen ja sillä toteutettujen julkaisujärjestelmien haavoittuvuudet, jotka voivat mahdollistaa verkkosivustojen sisällön luvattoman muokkaamisen. Murrettuja www-palvelimia käytetään yleisesti esimerkiksi haittaohjelmien levittämiseen ja huijaussivustoihin palvelimen ylläpitäjän sitä huomaamatta. Myös useista tietoturvatuotteista, esimerkiksi virustorjuntaohjelmistoista, löytyi jälleen haavoittuvuuksia.



11.10.2007



Ukkonen aiheutti häiriötä viestintäverkoille

Suomen yli kulki 22.8.2007 ukkosrintama, joka aiheutti merkittäviä ongelmia viestintäpalveluille. Matkapuhelintukiasemien toiminnassa ilmeni ukkosrintama-alueella melko runsaasti häiriötä. Ukkonen aiheutti ongelmia myös kiinteän puhelinverkon ja laajakaistayhteyksien toimintaan. Joukkoviestintäverkkojen osalta Radio Suomen lähetykatko Uudellamaalla katkaisi joksikin aikaa jopa viranomais- ja hätätiedotteiden lähetyksmahdollisuuden pääkaupunkiseudulla. Häiriöt saatiin poistetuksi kuitenkin melko nopeasti.

Roskaposti ruuhkautti postipalvelimia

CERT-FI:n tietojen mukaan suomalaisten operaattorien sähköpostipalvelimet ovat ajoittain olleet ylikuormittuneita roskapostiviestien suuren määrän vuoksi. Kuormitus on ajoittain aiheuttanut viestien välityksen viivästymistä. Kuormitustilanne on kuitenkin saatu hallintaan. Muut lyhytaikaiset ongelmat sähköpostipalveluissa ovat johtuneet muun muassa laitevioista ja reititysmuutoksista.

Skype-palvelussa laaja häiriö

Skype on vertaisverkkotekniikkaan perustuva internetpuheluohjelmisto, jonka käyttäjät voivat puhua ja viestiä toisilleen internetissä ilman puhelumaksuja. Skype-palvelussa oli laaja häiriö elokuun puolessa välissä. Häiriö alkoi Microsoftin julkaistua kuukausittaiset ohjelmistopäivityksensä. Skypen mukaan häiriö johtui ohjelmistovirheestä, joka aiheutti järjestelmän ylikuormittumisen lukuisten Windows-käyttöjärjestelmää käyttävien tietokoneiden pyrkiessä kirjautumaan uudelleen verkkoon uudelleenkäynnistyksensä jälkeen. Skype-verkkoon kirjautumisessa oli häiriötä useiden päivien ajan.

Palvelunestohyökkäys myös CERT-FI:n www-palvelinta vastaan

Viestintäviraston www-sivuja vastaan tehtiin palvelunestohyökkäys syyskuun viimeisenä viikonloppuna. Hyökkäyksen johdosta Viestintäviraston sivustot, kuten www.cert.fi ja www.ficora.fi olivat jonkin aikaa tavoittamattomissa.

Tulevaisuuden näkymiä

On todennäköistä, että jatkossa voidaan nähdä lisää bottiverkkojen avulla tehtäviä palvelunestohyökkäyksiä. Näyttää siltä, että hyökkäysverkkoja hallitsevat tahot myös puolustautuvat aktiivisesti heidän toimintansa tutkijoita vastaan. Joissakin tapahtuneissa hyökkäyksissä on nähtävissä piirteitä, joiden perusteella niitä voidaan pitää koston verkkojen toimintaa tai rakennetta selvittämään pyrkineille.

CERT-FI:n tietoon on edelleen tullut vain harvoja suomalaisissa verkoissa olevia bottiverkkojen ohjaustietokoneita. Murrettuja ja bottiverkkoihin liitettyjä suomalaisten käyttäjien tietokoneita on löydetty jonkin verran enemmän, ja niitä on poistettu verkosta yhteistyössä internetpalveluntarjoajien kanssa.

Erilaiset, myös maksulliset verkkopelit ovat kasvattaneet suosiotaan ja peleihin liittyvät haavoittuvuudet ja väärinkäytökset kannattaa myös huomioida. Tavallisimmin niissä on kyse peliin liittyvien käyttäjätunnusten ja salasanojen hankkimisesta.