

27.12.2007

CERT-FI

CERT-FI VUOSIKATSAUS 2007

Identiteettivargaat ovat kiinnostuneita sähköisten asiointipalvelujen käyttäjien tiedoista. Haittaohjelmia ja väärinkäytöksiä tutkittaessa on löydetty varastoituna suuria määriä käyttäjätietoja. CERT-FI:n tietoon ei kuitenkaan ole tullut hälyttäviä määriä suomalaisten käyttäjien tietoja.

Verkossa tarjottavat sähköiset asiointipalvelut voivat olla monella tavoin haavoittuvia väärinkäytöksille. Itse tarjottava palvelu saattaa olla helposti lamautettavissa ohjaamalla palvelimelle tarpeeksi verkkoliikennettä. Haavoittuvaa palvelinta voidaan käyttää haittaohjelmien levittämiseen, huijaussivustojen ylläpitämiseen tai palvelimelle talletettujen käyttäjätietojen urkkimiseen.

Haittaohjelmahavainnot suomalaisissa verkoissa ovat jonkin verran vähentyneet, vaikka laajakaistaliittymien määrä jatkaa kasvuaan. Yhteistyössä kotimaisten palveluntarjoajien kanssa havaittuihin ongelmiin on pystytty reagoimaan nopeasti.

Palvelunestohyökkäykset herättivät paljon huomiota

Internetin juurinimipalvelimia vastaan kohdistettiin palvelunestohyökkäys helmikuussa. Hyökkäys toteutettiin kaapattujen tietokoneiden muodostaman bottiverkon avulla ja se kesti noin vuorokauden. Hyökkäyksen volyymi oli huomattava, mutta sen käytännön vaikutukset jäivät vähäisiksi, sillä suurin osa loogisista juurinimipalvelimista säilyi toimintakykyisenä. Suomalaisille käyttäjille hyökkäys näkyi ainoastaan ajoittaisena internetin käytön hidastumisena. Osa hyökkäyksen kohteena olevista palvelimista vastaa myös joidenkin kansallisten verkkotunnusten nimipalveluista ja niidenkin toiminnassa oli häiriöitä. Fi-verkkotunnusten toimintaan hyökkäykset eivät vaikuttaneet.

CERT-FI sai samoihin aikoihin tiedon kahdesta laajasta palvelunestohyökkäyksestä, joissa asetuksiltaan liian avoimia nimipalvelimia käytettiin hyökkäysliikenteen vahvistajana. Hyökkäyksissä käytettiin hyväksi myös suomalaisia nimipalvelimia. Palvelinten ylläpitäjiin otettiin yhteyttä ja näitä neuvottiin muuttamaan palvelinten asetukset sellaisiksi, ettei niiden hyödyntäminen hyökkäyksessä olisi enää mahdollista.

Tallinnan ns. patsaskiistan puhjettua huhtikuun lopulla Viron valtionhallinnon verkkopalvelut lamautettiin liikennemäärältään jatkuvasti voimistuvilla palvelunestohyökkäyksillä. Lisäksi hyökättiin ainakin maksunvälitysjärjestelmiä ja uutispalveluita vastaan. Hyökkäykset jatkuivat useiden viikkojen ajan.

Viron hyökkäysten laannuttua CERT-FI:lle raportoitiin myös suomalaisiin palveluihin kohdistuneista hyökkäyksistä. Yleisradion www-palvelimeen tehdyn hyökkäyksen aikana sivustot toimivat hitaasti tai ajoittain eivät lainkaan. Hyökkäyksessä ohjattiin vertaisverkkoperiaatteella toimivan tiedostonjako-ohjelman yhteyspyyntöjä kuormittamaan palvelinta. Hyökkäyksellä ei CERT-FI:n tietojen mukaan ollut yhteyttä Viron tapahtumiin. Vaikutuksiltaan vähäisemmäksi jääneitä hyökkäyksiä tehtiin myös muita www-palvelimia ja sähköpostipalvelimia vastaan. Viestintäviraston ja CERT-FI:n www-sivustoja vastaan hyökättiin syyskuussa. Myös roskapostiviestien suuri määrä on aiheuttanut ajoittain viestinvälityksen hidastumista.

27.12.2007

CERT-FI

Paljon julkisuutta saaneet hyökkäykset johtivat osittain vääriin johtopäätöksiin tavanomaistenkin käyttökatkosten syistä, kun palvelujen toimivuutta seurattiin poikkeuksellisen tarkasti. Suuri osa CERT-FI:lle raportoiduista tapauksista ei kuitenkaan osoittautunut palvelunestohyökkäyksiksi. Hyökkäykset käynnistivät vilkkaan keskustelun sähköisten asiointipalvelujen toimintavarmuudesta hyökkäystilanteessa.

Käyttäjien tietoja keräillään monin keinoin

Sähköisten asiointipalvelujen käyttäjätiedot kiinnostavat haittaohjelmien ja verkkourkintasivustojen tekijöitä. Huijaussivustojen kautta tapahtuvan tietojen keräilyn lisäksi selainyhteyksiä tarkkailevat haittaohjelmat voivat lähettää www-lomakkeille syötettyjä tietoja keräilypalvelimille, joilta ne myöhemmin noudetaan mahdollista hyödyntämistä varten. CERT-FI on vuoden mittaan saanut ilmoituksia myös suomalaisten käyttäjien tiedoista, jotka ovat tällä tavoin joutuneet sivullisten tietoon. Suomalaisten osuus kaikista löytyneistä tiedoista on toistaiseksi ollut vähäinen, joitakin kymmeniä tapauksia.

Tunnusten, salasanojen ja muiden tunnistetietojen keräämisen lisäksi haittaohjelmat voivat myös muuttaa käyttäjän www-selaimella syöttämiä ja näkemiä tietoja yhteyden aikana. Ohjelma voi esimerkiksi tehdä verkkopankkiyhteyden aikana tilisiirron ennalta määrätylle tilille käyttäjän sitä havaitsematta. Toistaiseksi CERT-FI:n tietoon ei ole tullut sellaisia istuntoja kaappaavia haittaohjelmia, jotka toimisivat suomalaisissa palveluissa. Eräästä CERT-FI:n analysoimasta näytteestä on kuitenkin löydetty Suomeen viittaavia tietoja. Esimerkiksi verkkopankki-istunnon kaappaava haittaohjelma siirtää tartunnan saaneen tietokoneen käyttäjän tililtä huomaamattomasti rahaa. Tämän jälkeen rahavirtojen jäljet pyritään hävittämään talousrikollisuudesta tuttujen muulien eli bulvaanien avulla.

Lokakuussa www-sivustoilla ja vertaisverkkopalveluissa levitettiin tiedostoa, jonka sisältönä oli noin 80 000 suomalaisen internet-verkkopalvelun käyttäjän käyttäjätunnusta ja salasanaa tai salasanatiivistettä. Salasanat oli hankittu hyödyntämällä eri www-yhteisöpalvelujen ylläpitäjien itse kehittämässä tai kolmannen osapuolen tuottamissa ohjelmistokomponenteissa olevia haavoittuvuuksia.

Tapaus toi esiin puutteita monien verkon yhteisöpalvelujen tietoturvallisuudessa. Osassa palveluista salasanat oli talletettu palvelimelle selväkielisinä tai heikosti suojattuina. Yritysten lisäksi yhteisöpalveluja tarjoavat verkossa myös yksityiset harrastajat, joiden tietämys järjestelmän ja ohjelmistojen tietoturvallisesta ylläpidosta ei ole aina riittävä. Palveluissa käytettävistä ohjelmistoista löydetään jatkuvasti haavoittuvuuksia. Puutteita nähtiin myös palvelujen käyttäjien toimintatavoissa. Esimerkiksi saman salasanan käyttäminen eri palveluissa aiheuttaa sen, että yhden palvelun salasanan paljastuessa käyttäjän tietoja voidaan keräillä sellaisista palveluista, joissa on käytetty samaa salasanaa. Eri palveluista saatavia tietoja yhdistelemällä käyttäjän yksityisyyden suoja voi vaarantua ja niiden avulla voi esimerkiksi esiintyä toisen nimissä eri palveluissa.

Bottiverkot ovat yhä haitallisen toiminnan perustyökalu

Murrettujen tietokoneiden muodostamia bottiverkkoja käytetään edelleen monenlaiseen haitalliseen toimintaan. Niiden avulla voidaan esimerkiksi lähettää roskapostia tai toteuttaa palvelunestohyökkäyksiä.

27.12.2007

CERT-FI

Storm Worm on tammikuussa 2007 ensimmäisen kerran tavattu haittaohjelma, jota levitetään sähköpostin liitetiedostojen ja www-sivustojen kautta. Kesän ja syksyn aikana levitettiin paljon roskapostiviestejä, jotka sisälsivät linkin Storm Worm -haittaohjelmaa levittäville www-sivustoille. Tietokoneeseen tarttuessaan ohjelma asentaa siihen myös rootkit-toiminnallisuuden, eli pyrkii piilottamaan itsensä käyttäjältä ja virustorjuntaohjelmilta. Tämän vuoksi sen havaitseminen ja poistaminen tietokoneesta on vaikeaa. Storm Worm on tällä hetkellä yksi laajimmin levinneistä haittaohjelmista.

Storm Worm -tartunnan saaneet tietokoneet liittyvät osaksi hyvin laajaa bottiverkkoa. Verkkoon kaapattujen tietokoneiden verkkoa komennetaan tehokkaasti hajautetulla ja vertaisverkkomaisella mekanismilla, ilman yhtä keskitettyä komentopalvelinta. Tämä vaikeuttaa verkon toiminnan ja rakenteen selvittämistä. Bottiverkko voi myös käynnistää vastatoimena palvelunestohyökkäyksen suojautuakseen sen toiminnan tutkimiselta. Storm Worm -haittaohjelman merkittävyyttä suomalaisten käyttäjien kannalta ei täysin nähty vielä alkuvuodesta, eikä CERT-FI:n tietoon ole senkään jälkeen tullut merkittäviä määriä suomalaisissa verkoissa tavattuja tartunnan saaneita tietokoneita. Bottiverkkoa on kuitenkin sittemmin voitu käyttää myös hyökkäyksissä suomalaisia kohteita vastaan.

Ohjelmistohaavoittuvuudet helpottavat väärinkäytöksiä

Viime vuoden lopulla ja vuoden alussa esiintyneet haavoittuvuuksien julkaisukampanjat hiipuivat, eikä niitä nähty lisää. Ohjelmistoista löytyi kuitenkin edelleen paljon haavoittuvuuksia. 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.

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 huijaussivustojen tarjoamiseen palvelimen ylläpitäjän sitä itse huomaamatta. Internet-operaattorien käyttämien reititinten ohjelmistoista löydettiin myös haavoittuvuuksia, joita hyödyntämällä verkon toimintaa olisi voitu häiritä. Haavoittuvuuksia ei CERT-FI:n tietojen mukaan kuitenkaan ole käytetty hyväksi. Laittevalmistaja on toimittanut korjaavat ohjelmistopäivitykset rekisteröityneille asiakkailleen.

Ohjelmistohaavoittuvuuksista pyritään usein hyötymään myös kaupallisesti. Tietoja haavoittuvuuksista on kaupattu julkisesti ainakin jo vuodesta 2002, mutta viimeksi kuluneen vuoden aikana kaupankäynti haavoittuvuuksilla on vilkastunut sveitsiläisen haavoittuvuuksia huutokauppaavan WabiSabiLabi-sivuston myötä. Haavoittuvuustietoja ostavat esimerkiksi tietoturvatuotteiden valmistajat, jotka käyttävät niitä hyväksi tuotteissaan ja saavat siitä markkinointihyötyä omille tuotteilleen. Tavallisesti haavoittuvuudet julkaistaan jonkin ajan kuluttua yhteistyössä haavoittuvien ohjelmistojen valmistajien kanssa.

Haavoittuvuuksien kauppaamiseen liittyy myös ongelmia. Haittaohjelmien tekijät voivat saada tietoja haavoittuvuuksista analysoimalla tietoturvatuotteita, joissa ostettuja tietoja on käytetty. Haavoittuvuuksien kauppaajien luotettavuudesta ei ole takeita ja tiedot haavoittuvuuksista ovat haluttua ja arvokasta tietoa verkkorikollisten piirissä. Vielä julkaisemattomia haavoittuvuuksia voidaan käyttää hyväksi erityisesti kohdennetuissa hyökkäyksissä.



27.12.2007

CERT-FI

Haittaohjelmia levittävät sivustot keskittyneet tiettyihin ulkomaisiin verkkoihin

Haitallista sisältöä levittävät palvelimet näyttävät keskittyneen samojen verkko-operaattorien tai palvelinhotellien asiakkaisiksi. Osa internet-operaattoreista näyttää estäneen liikennöinnin joihinkin pahamaineisimmista verkko-osoitteista. Erityisesti Russian Business Network -nimisen ryhmittymän toiminnasta on esitetty julkisesti vastalauseita. Näyttää siltä, että se on loppuvuodesta pyrkinyt vaihtamaan käyttämiään IP-osoiteavaruuksia.

Tulevaisuuden näkymiä

CERT-FI julkaisi lähes 200 ilmoitusta ohjelmistohaavoittuvuuksista ja seitsemän varoitusta. Haavoittuvuusilmoitukset ja varoitukset on tämän vuoden alusta julkaistu erikseen, ja niiden julkaisuperusteita on tarkistettu. Lisäksi CERT-FI julkaisi yli sata Tietoturva Nyt! -artikkelia ajankohtaisista tietoturva-aiheista.

Ohjelmistohaavoittuvuuksien merkitys on edelleen suuri. Haavoittuvuuksia löydetään myös suljetummista ympäristöistä, kuten teollisuudessa käytettävistä sovelluksista. Järjestelmät, joiden suunnittelussa ei ole otettu huomioon haittaohjelmien leviämisen mahdollisuutta, voivat olla hyvinkin haavoittuvia.

Useamman pienemmän tapauksen lisäksi CERT-FI on työskennellyt viime vuonna suuren, lukuisten valmistajien tuotteisiin vaikuttavan haavoittuvuuskoordinointihankkeen parissa. Tulosten toivotaan olevan julkaistavissa alkuvuonna 2008.

Korjaamattomia ja julkistamattomia haavoittuvuuksia voidaan käyttää hyväksi kohdistetuissa hyökkäyksissä, joissa tätä tarkoitusta varten räätälöityä haittaohjelmaa pyritään levittämään vain valittuun kohteeseen. Tavoitteena voi olla esimerkiksi tietojen hankkiminen kohdeorganisaatiosta.

Sähköpostia käytetään edelleen haittaohjelmien levittämiseen joko lähettämällä roskapostiviestien mukana haittaohjelmia sisältäviä liitetiedostoja tai sisällyttämällä viesteihin linkkejä, jotka houkuttelevat varomattomia käyttäjiä tunnettuja haavoittuvuuksia hyväksikäyttävälle www-sivuille.

Haittaohjelmien tekninen kehitys tuo mukanaan uusia haasteita, uudenlaisten bottiverkkojen toiminnan selvittäminen on niiden hajautetun ohjausjärjestelmän vuoksi vaikeampaa. Sähköiset asiointipalvelut ovat edelleen varsin haavoittuvia palvelunestohyökkäyksille, jotka voidaan toteuttaa joko bottiverkkojen tai vertaisverkkojen avulla. Ei ole lainkaan mahdotonta, että selainyhteyksiä tarkkailevat tai kaappaavat haittaohjelmat laajentavat tuntemiensa palvelujen joukkoa myös suomalaisiin sivustoihin. Tietokoneista tutut tietoturvanäkökulmat täytyy huomioida myös matkaviestimien käytössä.

Samaan aikaan kun laajakaistaliittymien määrä jatkaa kasvuaan, haittaohjelmahavaintojen määrä suomalaisissa verkoissa näyttäisi pienentyvän. Suotuisaan kehitykseen ovat vaikuttaneet teleyritysten, tietoturvayhtiöiden ja tietoturvaviranomaisten sujuva yhteistyö sekä kansallinen lainsäädäntö ja tietoturvamääräykset. Suomalainen malli toimii esikuvana kansainvälisissä yhteyksissä kuten EU:n piirissä.