

3.7.2007

CERT-FI

TIETOTURVAKATSAUS 2/2007

Alkuvuonna esiin tulleet palvelunestohyökkäykset jatkuivat myös loppukevään aikana. Toukokuussa ne nousivat otsikoihin varsinkin Viron valtionhallinnon ja Yleisradion palveluihin tehtyjen hyökkäysten johdosta. Tutkittujen palvelunestohyökkäysten toteuttamistavat ja -kohteet poikkesivat toisistaan, eikä CERT-FI:n käytettävissä olevien tietojen perusteella tapausten välillä ollut suoraa yhteyttä.

CERT-FI julkaisi toisen vuosineljänneksen aikana 39 tiedotetta ohjelmistohaavoittuvuuksista ja 35 Tietoturva nyt! -artikkelia. Yhtään varoitusta ei julkaistu.

Itsenäisesti toimivan ja leviävän Allaple-haittaohjelman tartuttamien tietokoneiden aiheuttama liikenne on häirinyt suomalaisen www-palvelimen toimintaa jo lähes vuoden ajan. Hyökkäyksen vaikutuksia pyritään nyt torjumaan Windows-käyttöjärjestelmän päivitysten mukana jaettavalla torjuntaohjelmalla.

Virossa hyökättiin valtionhallinnon ja pankkien järjestelmiä vastaan

Palvelunestohyökkäykset nousivat otsikoihin, kun hyökkääjät pyrkivät lamauttamaan Viron valtionhallinnon verkkopalveluja, erityisesti www-sivustoja. Lisäksi hyökättiin ainakin pankkien ja uutispalvelujen palvelimia vastaan. Hyökkäykset alkoivat Tallinnan ns. patsaskiistan puhjettua huhtikuun lopulla ja jatkuivat useiden viikkojen ajan.

Virolaiset torjuivat hyökkäyksiä aluksi rajoittamalla kaikkea Viron ulkopuolelta saapuvaa liikennettä, jolloin suurin osa kuormittavasta liikenteestä estyi. Myöhemmin liikennettä suodatettiin sekä IP-osoitteiden että yhteyksien sisällön perusteella.

Myös Suomessa näkyviä palvelunestohyökkäyksiä

Toukokuussa CERT-FI:n tietoon tuli myös suomalaisiin palveluihin kohdistuneita hyökkäyksiä. Maanantaina 14.5. kohdistettiin Yleisradion www-palvelimeen palvelunestohyökkäys, joka toistui samana iltana. Hyökkäys jatkui myös seuraavana päivänä ja sen aikana www.yle.fi-sivusto toimi hitaasti tai ajoittain ei lainkaan. Hyökkäystä torjuttiin aluksi estämällä pääsy palveluun ulkomailta. Myöhemmin häirintäliikennettä alettiin erottaa normaalien käyttäjien yhteyksistä analysoimalla sisään tulevien pakettien sisältöä. Yleisradiota vastaan tehdyssä hyökkäyksessä ohjattiin vertaisverkkoperiaatteella toimivan tiedostonjako-ohjelman yhteyspyyntöjä yli sadasta tuhannesta eri IP-osoitteesta kuormittamaan palvelinta.

Maanantaina 14.5. ilmoitettiin myös Eniron suomi24.fi-sivuihin kohdistuneesta hyökkäyksestä, joka näkyi palvelun ajoittaisina katkoksina ja hidastumisena. CERT-FI:n tietojen mukaan hyökkäys toteutettiin Yleisradion hyökkäyksestä poikkeavalla tavalla. Kohteena olleet palvelimet sijaitsevat Ruotsissa. Hyökkäys toistui myös maanantaina 21.5.

Palvelunestohyökkäyksissä pyritään ylikuormittamaan kohteena olevaa palvelua niin, ettei sen normaali käyttö ole mahdollista. Hyökkäykset toteutetaan useimmiten joko itsestään leviävien ja toimivien haittaohjelmien tai bot-verkkojen avulla. Yleisradiota vastaan tehdyssä hyökkäyksessä käytettiin kuitenkin hyväksi vertaisverkossa toimivien tiedostonjako-ohjelmien turvallisuuden puutteita.

3.7.2007

CERT-FI

Hyökkäysten julkisuus toi myös turhia ilmoituksia

Uutiset samanaikaisista palvelunestohyökkäyksistä johtivat väärin johtopäätöksiin tavanomaistenkin käyttökatkosten syistä, kun palvelujen toimivuutta seurattiin poikkeuksellisen tarkasti. CERT-FI:n tietoon ei tullut erityisen paljon palvelunestohyökkäyksiksi luokiteltavia tapahtumia.

CERT-FI julkaisi verkkosivuillaan toukokuun lopussa kaksi tiedotetta palvelunestohyökkäyksistä ja niihin varautumisesta. Lisäksi CERT-FI järjesti 22.5. palvelunestohyökkäyksiä käsittelevän lehdistötilaisuuden ja julkaisi samalla aihetta käsittelevän ylimääräisen tietoturvakatsauksen 1B/2007.

Allaple-verkkomadon torjunnassa edistysaskel

Heinäkuusta 2006 lähtien tietoverkoissa on levinnyt *Allaplesi* nimetty haittaohjelma, jonka ainoa tarkoitus on estää tiettyjen verkkopalvelujen toiminta. Yksi kohteista sijaitsee suomalaisessa verkossa. Liikkeelle laskemisensa jälkeen Allaple pyrkii tarttumaan yhä uusiin tietokoneisiin ja häiritsee kohteitaan itsenäisesti ilman 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 haittavaikutuksien lievittämiseksi Microsoft on lisännyt Allaple-verkkomadon tuntomerkit haittaohjelmien poistotyökaluun. Windows-automaattipäivitysten mukana jaettava *Malicious Software Removal Tool* tunnistaa ja poistaa tietokoneeseen tarttuneen Allaple-haittaohjelman. CERT-FI seuraa torjuntatoimien vaikutuksia - toistaiseksi haittaliikenteen määrä ei ole merkittävästi vähentynyt.

Vakoiluohjelmat tuntevat jo tuhansia verkkopankkeja

Varsinkin pankkien verkkopalvelujen käyttäjiin kohdistuu huijausyrityksiä, joissa palvelua käyttävän asiakkaan tietokoneeseen pyritään tartuttamaan vakoiluohjelma. Sen avulla voidaan kaapata palvelussa käytettäviä tunnuksia, salasanoja ja muita tietoja. On myös ohjelmia, joiden avulla voidaan kaapata käyttäjän verkkopankkiyhteys niin, että hyökkääjä syöttää pankkipalveluun tietoja käyttäjän sitä huomaamatta.

Haittaohjelmien tuntemien pankkipalvelujen määrä kasvaa koko ajan. Yleisesti käytetyt vakoiluohjelmat toimivat jo tuhansien eri verkkopankkipalvelujen kanssa, ja niiden joukossa on myös suomalaisia pankkeja. Suomalaisten pankkien palveluihin ei CERT-FI:n tietojen mukaan ole toistaiseksi kohdistunut sellaisia väärinkäytöksiä, jotka edellyttäisivät palvelujen käyttäjiltä tavanomaista varovaisuutta enempiä toimenpiteitä.

Vakoiluohjelmia levitetään järjestelmällisesti joko roskapostiviestien liitetiedostoina tai liittämällä viesteihin linkki, joka osoittaa haittaohjelman sisältävälle www-sivulle. Tavallisesti haittaohjelma tarttuu, kun käyttäjä klikkaa siihen osoittavaa linkkiä selaimella. Haittaohjelmien tartuttamiseksi käytetään kuitenkin hyväksi myös sellaisia käyttöjärjestelmän tai sovellusten korjaamattomia ohjelmistohaavoittuvuuksia, jotka mahdollistavat huomaamattoman tartunnan ilman käyttäjän toimia.

Viime aikoina on saatu tietoja erityisesti haittaohjelmien levittämiseen tarkoitettua ohjelmasta, joka on kaupan internetissä. *MPack*-ohjelman avulla voidaan helposti käyttää hyväksi lukuisia eri

3.7.2007

CERT-FI

haavoittuvuuksia haittaohjelmien levittämiseksi viattomilta näyttävien www-sivujen kautta. Haittaohjelman levittäjä asentaa ohjelman murretulle www-palvelimelle, ja se käynnistyy sivuja selailtaessa. Ohjelma pyrkii tartuttamaan käyttäjän tietokoneen käyttämällä hyväksi useita eri haavoittuvuuksia. Yksikin korjaamaton haavoittuvuus riittää haittaohjelmatarjunnan saamiseksi.

Haavoittuvuuksia löytyi tavanomaisen runsaasti

Suurin osa löydetyistä ohjelmistohaavoittuvuuksista koski työasemissa käytettäviä ohjelmistoja. Maaliskuun lopussa tuli julkisuuteen Windowsin ns. animoitujen kursorien (hiiren osoittimien) käsittelyyn liittyvä haavoittuvuus, johon ei ollut heti 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. Myös useita muita Windowsin ja Office-ohjelmistojen haavoittuvuuksia korjattiin.

Tietoturvallisuuteen liittyvistä tuotteista, kuten virustorjuntaohjelmistoista ja palomuurilaitteista, löytyi lukuisia haavoittuvuuksia. Korjauksia julkaistiin myös Mozilla Seamonkey-, Firefox- ja Thunderbird-ohjelmistoihin.

CERT-FI:n tietoon tuli useita www-sivustoja, joille oli murtauduttu käyttämällä hyväksi PHP-ohjelmointikielen haavoittuvuuksia.

Vika- ja häiriötilanteet

TeliaSoneran sähköpostipalvelussa oli pääsiäisen aikaan 6.-8.4.2007 toimintakatkos, joka johtui teknisestä viasta. Laajimmillaan vika vaikutti noin 400 000 sähköpostiasiakkaaseen, ja koko vikatilanteen ajan noin 200 000 asiakkaan yhteyksiin.

Runkoverkon siirtojärjestelmissä esiintyi jonkin verran laitevikoja, jotka aiheuttivat lyhyehköjä katkoksia laajakaistapalveluihin sekä kiinteän puhelinverkon ja matkaviestinverkon palveluihin. Maanrakennustyöt aiheuttivat runkoverkossa muutaman kaapelikatkoksen, jotka alueellisesti estivät puhelin- ja dataliikennettä.

Maanpäällisen Digi-TV:n ja analogisen television lähetyksissä on ollut alueellisia katkoksia, jotka ovat aiheutuneet TV-lähettimissä olleista häiriöistä. Mainittavin häiriö oli 26.-27.5.2007 Joutsenossa ollut lähetinvika, joka aiheutui salamaniskusta lähetinmastoon.

Tulevaisuuden näkymät

Sähköiset asiointipalvelut ovat osoittautuneet helpoiksi kohteiksi, ja niihin kohdistuvia palvelunestohyökkäyksiä tai murtautumisyrittäjiä järjestelmiin nähtäneen jatkossakin. Internetissä tarjottavien palvelujen häiriöitä seurataan entistä tarkemmin myös tiedotusvälineissä, mikä tekee niistä houkuttelevia kohteita julkisuuden tavoittelemiseksi.

Murrettujen ja hyökkäyksiin valjastettujen tietokoneiden lisäksi Suomesta on löydetty myös hyökkäyksissä käytettävien bot-verkkojen ohjaamiseen käytettäviä komentopalvelimia. Näyttää siltä, että Suomessa hyökkäysten valmisteleminen ei toistaiseksi ole ollut ammattimaista toimintaa, vaan niiden takana on ollut esimerkiksi julkisuutta tavoittelevia nuoria, joilla on käytettävissään joukko murrettuja tietokoneita. Bot-verkkoja voidaan kuitenkin käyttää rikollisessa toiminnassa myös järjestelmällisesti taloudellisen hyödyn tavoittelemiseksi tai aatteellisen propagandan levittämiseksi.