

CERT-FI

TIETOTURVAKATSAUS 3/2009

21.10.2009

CERT-FI tietoturva- katsaus 3/2009

Johdanto

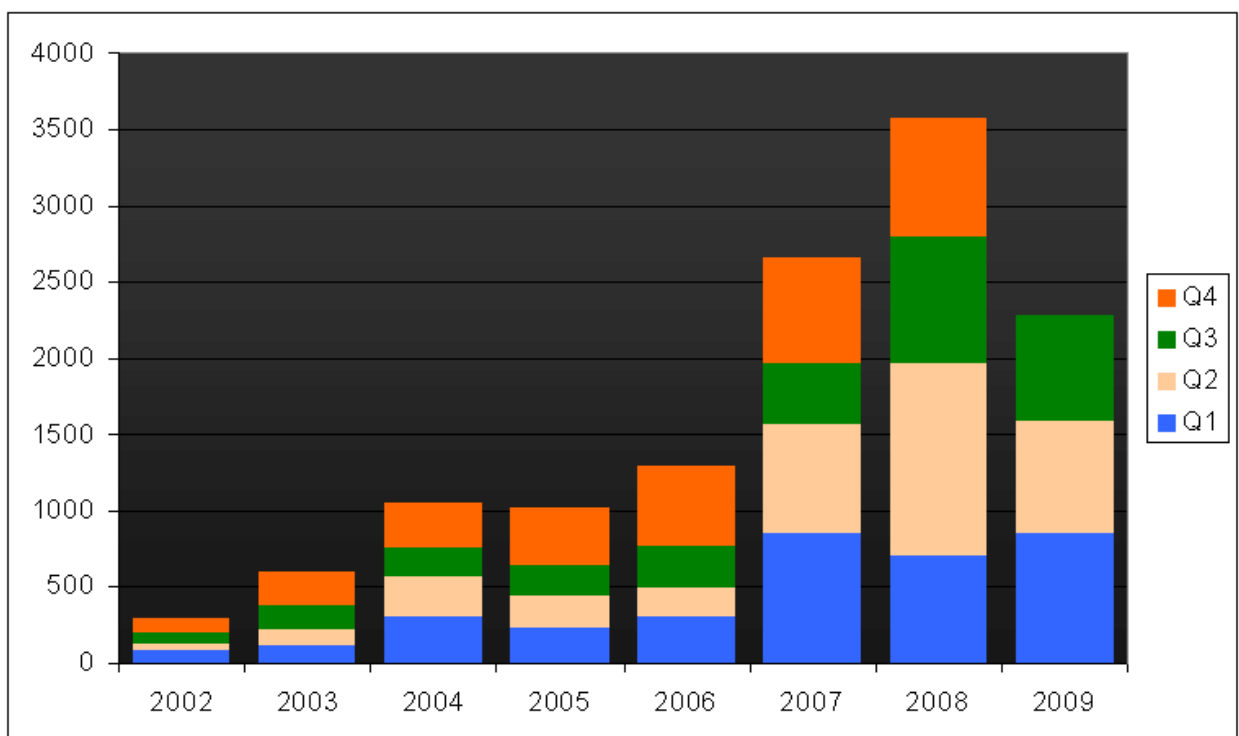
CERT-FI on käsitellyt vuoden 2008 alusta kuluvan vuoden elokuun loppuun mennessä noin 1800 sellaista tapausta, joissa tietoja varastava haittaohjelma on välittänyt käyttäjän tietoja sivullisille. Myös suomalaisia käyttäjiä on joutunut tietoja varastavien haittaohjelmien kohteeksi.

Kahden tavallista laajemman haavoittuvuuskoordinoitiprojektin tulokset on julkaistu. Elokuussa julkaistiin XML-kirjastoihin liittyvä koordinoitiprojekti. XML-kirjastoja käytetään tiedon ja dokumenttien käsittelyyn hyvin monenlaisissa tietojärjestelmissä.

Syyskuussa julkaistiin TCP-protokollan palvelintoteutuksiin liittyvän, pitkään kestäneen haavoittuvuuskoordinoitiprojektin tulokset. TCP on verkon yhteysmenettely, jota käytetään tiedonsiirtoon useimmissa verkon sovelluksissa ja tästä syystä tämä tapaus kosketi monia ohjelmistovalmistajia.

Haavoittuvuuskoordinoinnin tavoitteena on saada valmistajat testaamaan tuotteensa ja korjaamaan niistä mahdollisesti löytyvät haavoittuvuudet. Ohjelmistovalmistajien ja CERT-FI:n välisen hyvän yhteistyön ansiosta koordinoitiprojektit onnistuivat hyvin.

Suomalainen verkkosivusto on ollut useiden ulkomaisten palvelujen ohella palvelunestohyökkäyksen kohteena. CERT-FI on koordinoitunut tapauksen selvittämistä. Kansainvälisen yhteistyön avulla selvitystyössä on edistytty hyvin.



CERT-FI:n käsittelemät yhteydenotot ovat vähentyneet edellisvuodesta jonkin verran.

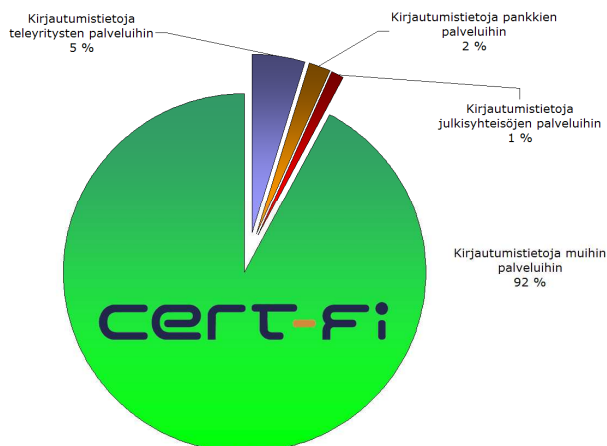
Haittaohjelmat varastavat suomalaistenkin käyttäjien tunnuksia

CERT-FI saa satunnaisesti ilmoituksia tapauksista, joissa suomalaisten sähköisten asiointipalveluiden käyttäjät ovat joutuneet tietoja varastavien haittaohjelmien uhreiksi. Ilmoitukset voivat sisältää myös haittaohjelmien keräämiä tietoja. Haittaohjelmien keräämät tiedot ovat tavallisesti sähköisten palveluiden kirjautumistietoja, kuten käyttäjätunnuksia ja salasanoja. Haittaohjelmat keräävät kuitenkin myös selaimella käytettävien lomakkeiden, kuten sähköpostiviestien, verkkokauppatilauksen sekä verkkopankkilomakkeiden sisältöjä.

CERT-FI on käsitellyt vuoden 2008 alusta kuluvan vuoden elokuun loppuun mennessä noin 1800 sellaista tapausta, joissa on ollut kyse käyttäjän tietoja varastavasta haittaohjelmasta. Suurin osa kohteena olevista palveluista on ollut erilaisia internetin yhteisöpalveluja. Merkittävä osa kaikista CERT-FI:n käsittelemistä tapauksista on kohdistunut yhden suomalaisen yrityksen tarjoamaan kansainväliseen palveluun. Valtaosan tapausten kokonaismäärästä muodostavat siten kyseisen palvelun ulkomaalaiset käyttäjät.

Tapauksia tarkasteltaessa on huomattava, että pankkipalvelujen kirjautumistietojen osuus kaikista varastetuista tiedoista on pieni. Luottokorttitiedot puuttuvat CERT-FI:n vastaanottamista tiedoista kokonaan, sillä niille on olemassa muita vakiintuneita raportointikanavia.

Tapauksen jakautuminen palveluntarjoajittain



Haittaohjelmien saastuttamat www-sivustot yleisiä

Haittaohjelmatartunnan saa yhä useammin vieraillemalla haittaohjelmia jakavalla, murretulla www-sivustolla. Sivuston koodiin upotetaan haittaohjelman varastamisen ftp-tunnusten avulla esimerkiksi haittaohjelman lataava Javascript-koodi tai haittaohjelman lataava linkki piilotettuun iframe-tagtiin. Tartunta voi tapahtua, jos satunnaisen sivustolla kävijän selaimen lisäosat tai sisällön näyttämiseen tarkoitettut ohjelmat, kuten Adobe Acrobat tai Adobe Flash Player, ovat haavoittuvia eikä virustorjuntaohjelmisto ole ajan tasalla.

Haittaohjelman tartuttua koneelle se voi tarkkailla työaseman verkkoliikennettä varastaakseen käyttäjän ftp-tunnuksia ja salasanoja. Se voi myös lähettää työasemasta roskapostia, asentaa tietoturvaohjelmaa muistuttavan haittaohjelman tai väärentää internetin hakukoneilla tehtyjen hakujen tuloksia ohjatakseen käyttäjän huijaussivustoille. Haittaohjelmien toimintamekanismit vaihtelevat sen mukaan mikä ohjelma on kyseessä.

Zeus-haittaohjelmaperheen ohjelmistot osaavat myös kerätä tunnuksia ja salasanoja tallentamalla näppäinten painallukset ja lähettämällä ne komentopalvelimelle myöhempää hyväksikäyttöä varten. Varastettuja tunnuksia voidaan käyttää edelleen hyökkäystarkoituksessa tehdyn sisällön lisäämiseen uusille sivustoille.

Hakukoneiden tulosten optimointia käytetään haittaohjelmien levityksessä

Hakukoneiden käyttäjille palauttamia hakutuloksia on käytetty haittaohjelmien levittämiseen jo joidenkin vuosien ajan. Kuluvana vuonna ilmiö on yleistynyt ja saanut myös uusia muotoja. Haittaohjelmien levitys tapahtuu murrettujen tai tarkoitusta varten erityisesti perustetuille palvelimille luotujen www-sivustojen välityksellä. Haittaohjelmien levittäjät pyrkivät nostamaan näitä sivustoja hakutulosten kärkipäähän hakukoneoptimoinnin keinoin.

Hakukoneoptimoinnissa haitallisille sivuille syötetään hakusanoja ajankohtaisista tapahtumista. Tällöin lisätietoa ajankohtaisesta aiheesta etsivät käyttäjät päätyvät

joitakin hakukoneen palauttamia tuloksia seurattessaan www-sivustoille, jotka pyrkivät selainhaavoittuvuuksia hyväksikäyttämällä saastuttamaan kävijän työaseman tai erehdyttämään käyttäjän asentamaan haittaohjelman itse.

Selaimet ja hakukoneet tunnistavat osan huijaussivustoista

Haittaohjelmien saastuttamat verkkosivut voivat olla vaikeita havaita. Sivusto ei välttämättä eroa ulkoisesti mitenkään normaalista, puhtaasta sivusta. Ilmiötä kutsutaan myös nimellä *drive-by-download*.

On kuitenkin hyvä huomata, että hakukoneyhtiöt ovat kuluneen vuoden aikana myös huomattavasti panostaneet siihen, että hakutuloksien palauttamia sivustoja tarkastetaan haittaohjelmien tai haittaohjelmia tartuttavien hyväksikäyttämismenetelmien varalta. Tällä hetkellä yleisimmät hakukoneet varoittavat käyttäjää jos hakutuloksien yhteydessä on sivu, jonka sisältö on tunnistettu haitalliseksi. Myös selain voi varoittaa haitallisesta sisällöstä.

Joissakin tapauksissa hakukoneiden turvatarkistusmekanismit pyritään ohittamaan. Tämä tapahtuu siten, että hakukoneen tuloksissa näkyvät haittaohjelmien levittämiseen käytettävät linkit johtavat sivustolle, jotka ainoastaan uudelleenohjaavat käyttäjän vielä uudelle sivustolle, jolta haittaohjelmatartunta tulee. Ketjun viimeisestä sivustosta vastaava palvelin tarkistaa HTTP-pyyntöön Referrer-kentän arvon. Tämän perusteella ainoastaan tietyiltä sivuilta uudelleenohjatuille kävijöille tarjotaan sivusto, joka levittää haittaohjelmia.

Sivuston puhdistaminen ei riitä, uudelleen saastuminen täytyy myös estää

Pelkkä haittaohjelman tartuttaman sivuston sisällön puhdistaminen ei välttämättä riitä. Www-sivujen ylläpitäjälle tulee välittää tieto sivujen päivittämiseen käytettävien tunnusten ja salasanojen joutumisesta väärin käsiin ja koneen saastumisesta. Näin voidaan estää sivuston saastuttaminen uudelleen. Sivuston ylläpitoon käytettyyn ftp-tunnukseen liittyvä salasana tulee vaihtaa.

Viranomaiset reagoivat haitallisen sisällön tarjoamiseen

Kesäkuun alussa yhdysvaltalainen hosting-palveluntarjoaja 3FN poistettiin verkosta viranomaismääräyksellä FTC:n eli Yhdysvaltain kauppakomission aloitteesta. FTC:n mukaan palveluntarjoaja oli suojannut aktiivisesti rikollisia olemalla reagoimatta niin sanottuihin takedown-pyyntöihin. Palveluntarjoajaa syytettiin FTC:n tekemässä valituksessa muun muassa haittaohjelmien, lapsipornon, sekä roskapostin levityksestä. Yritystä syytettiin tietoisesta kaapattujen koneiden verkon, eli botnetin, sekä botnetin komento- palvelinten ylläpidosta.

Operaattorin yhteydet katkaistiin oikeuden päätöksellä. Yhteyksien katkaisulla oli välitön vaikutus Cutwail-botnetin lähettämään roskapostin määrään. Vaikutus ei ollut kuitenkaan yhtä suuri kuin marraskuussa 2008 irtikytetyssä McColo-palveluntarjoajan tapauksessa. Sen verkossa oli useampi roskapostia lähettävä botnet-verkko, ja sen poistuttua roskapostin määrä tippui hetkellisesti jopa kolmannekseen.

Poikkeuksellista 3FN-operaattorin irtikytkenässä on, että palveluntarjoaja kytkettiin irti verkosta viranomaismääräyksellä. Aikaisemmin McColon ja toisen yhdysvaltalaisen palveluntarjoajan, Intercagen, tapauksessa irtikytettäisiin vaikuttivat kansainvälisen tietoturvyhteisön tietoliikenneoperaattoreille lähettämät jatkuvat ilmoitukset haitallisesta liikenteestä ja rikollisesta toiminnasta.

CERT-FI julkaisi laajojen haavoittuvuuskoordinoitiprojektien tuloksia

CERT-FI julkaisi elokuussa XML-kirjastoihin liittyvän tavallista laajemman haavoittuvuuskoordinoitiprojektin tulokset. Tapauksen laajuus johtuu siitä, että XML-kieltä käytetään tiedon ja dokumenttien käsittelyyn hyvin monenlaisissa tietojärjestelmissä. Lisäksi ohjelmistokirjastojen haavoittuvuudet ovat yleisesti luonteeltaan laajavaikutteisia, sillä haavoittuvat kirjastot ovat usein käytössä kymmenissä tai sadoissa sovellusohjelmissä.

Syyskuussa julkaistiin TCP-protokollan palvelintoteutukseen liittyvän, pitkään kestäneen haavoittuvuuskoordinointiprojektin tulokset. TCP on verkon yhteysmenettely, jota käytetään tiedonsiirtoon useimmissa verkon sovelluksissa ja tästä syystä myös tämä tapaus kosketti hyvin monia ohjelmistovalmistajia.

Haavoittuvuuskoordinoinnin tavoitteena on saada valmistajat testaamaan tuotteensa ja korjaamaan niistä mahdollisesti löytyvät haavoittuvuudet. CERT-FI on ollut yhteydessä sataan ohjelmistovalmistajaan TCP-haavoittuvuuden koordinointityön aikana. Tähän mennessä 13 ohjelmistovalmistajaa on julkaissut lausunnon tai ohjelmistokorjauksia heille tarjottujen tietojen pohjalta.

Laajoissa haavoittuvuuskoordinointiprojekteissa myös epäonnistumisen riski kasvaa. Epäonnistumisella tarkoitetaan tavallisesti haavoittuvuutta koskevien yksityiskohtaisten tietojen ennenaikaista paljastumista osittain tai kokonaan. Yksityiskohtien liian aikainen julkaiseminen voi johtaa haavoittuvuuden käyttämiseen hyväksi hyökkäyksissä.

Molemmat nyt julkaistuista projekteista onnistuivat tavoitteessaan. Kummassakaan tapauksessa haavoittuvuuksien kaikkia yksityiskohtia ei vielä ole julkaistu. TCP-protokollaan liittyvien haavoittuvuuksien koordinointityö ja työ haavoittuvien valmistajien löytämiseksi jatkuu edelleen. Projektista julkaistu haavoittuvuustiedote löytyy sivulta www.cert.fi.

Palvelunestohyökkäys suomalaista verkkosivustoa kohtaan

CERT-FI on osallistunut aktiivisesti suomalaisen yritykseen kohdistuneen palvelunestohyökkäyksen selvittelyyn. Hyökkäys ei kohdistunut pelkästään suomalaiseen palveluun, vaan kohteena oli myös useita ulkomaisia sivustoja.

Tapaukseen liittyvä koordinointityö jatkuu yhä. Työ käynnistyi hyvin - palvelua vastaan hyökkäävä botnet-verkko pystyttiin tunnistamaan kansainvälisellä yhteistyön avulla erittäin nopeasti.

Palvelunestohyökkäystilanteessa nopealla yhteistyöllä oman internetpalveluntarjoajan sekä CERT-FI:n kanssa on mahdollista rajoittaa tehokkaasti hyökkäyksen vaikutuksia.

Jos organisaation toiminta on merkittävästi riippuvaista kaikissa olosuhteissa toimivista verkkopalveluista, tarvittavista varautumistoimenpiteistä on syytä keskustella palveluntarjoajan kanssa jo etukäteen.

Suomeen kohdistuvat palvelunestohyökkäykset ovat melko harvinaisia.

Viestintävirasto mukana Tieto 2009 -valmiusharjoituksessa

Viestintävirasto oli mukana lokakuun alkupuolella pidetyssä Tieto-harjoituksessa¹.

Harjoituksen päämääränä on tehostaa viranomaisien ja hallinnon yhteistyökykyä tietojärjestelmiin kohdistuvien ongelmien hoitamisessa. Kahden vuoden välein järjestettävä harjoitus pidettiin viime viikolla.

Harjoituksessa oli mukana puolustusvoimien, valtion tietohallinnon ja ministeriöiden lisäksi tietotekniikka-alan yrityksiä, kuten teleoperaattoreita ja ICT-palveluntarjoajia.

Tulevaisuuden näkymiä

Tietoja varastavat haittaohjelmat ja niiden levityskampanjat roskapostiviestien ja www-sivujen avulla ovat todennäköisesti yleisiä myös loppuvuoden aikana. Joulutervehdyksiksi tai yritysten joulutarjouksiksi naamioidut viestit ovat tavallisia tapoja levittää haitallista sisältöä. Haittaohjelmia voidaan levittää myös viesteissä olevien linkkien kautta.

Jos jostakin yleisesti käytettävästä ohjelmistosta, kuten selaimesta, sen lisäosista tai dokumenttien katseluun käytettävistä ohjelmista löytyy paikkaamaton haavoittuvuus, voivat haittaohjelmat käyttää sitä hyväksi ja levitä laajaltikin.

Myös matkapuhelimiin voidaan lähettää haitalliseen sisältöön johtavia linkkejä tekstiviesteinä.

¹ <http://www.mil.fi/paaesikunta/artikkelit/5544.dsp>

CERT-FI-yhteydenotot nimikkeittäin	1-9/2009	1-9/2008	Muutos
Haastattelu	78	67	+16%
Haavoittuvuus tai uhka	107	323	-67%
Haittaohjelma	1451	1719	-16%
Neuvonta	250	243	+3%
Hyökkäyksen valmistelu	29	71	-59%
Tietomurto	101	147	-31%
Palvelunestohyökkäys	63	72	-13%
Muu tietoturvaongelma	82	33	+148%
Social Engineering	118	127	-7%
Yhteensä	2279	2802	-19%

Ilmoitukset haittaohjelmista muodostavat edelleen valtaosan CERT-FI:n käsittelemistä yhteydenotoista.