

CERT-FI
TIETOTURVAKATSAUS 1/2009

3.4.2009

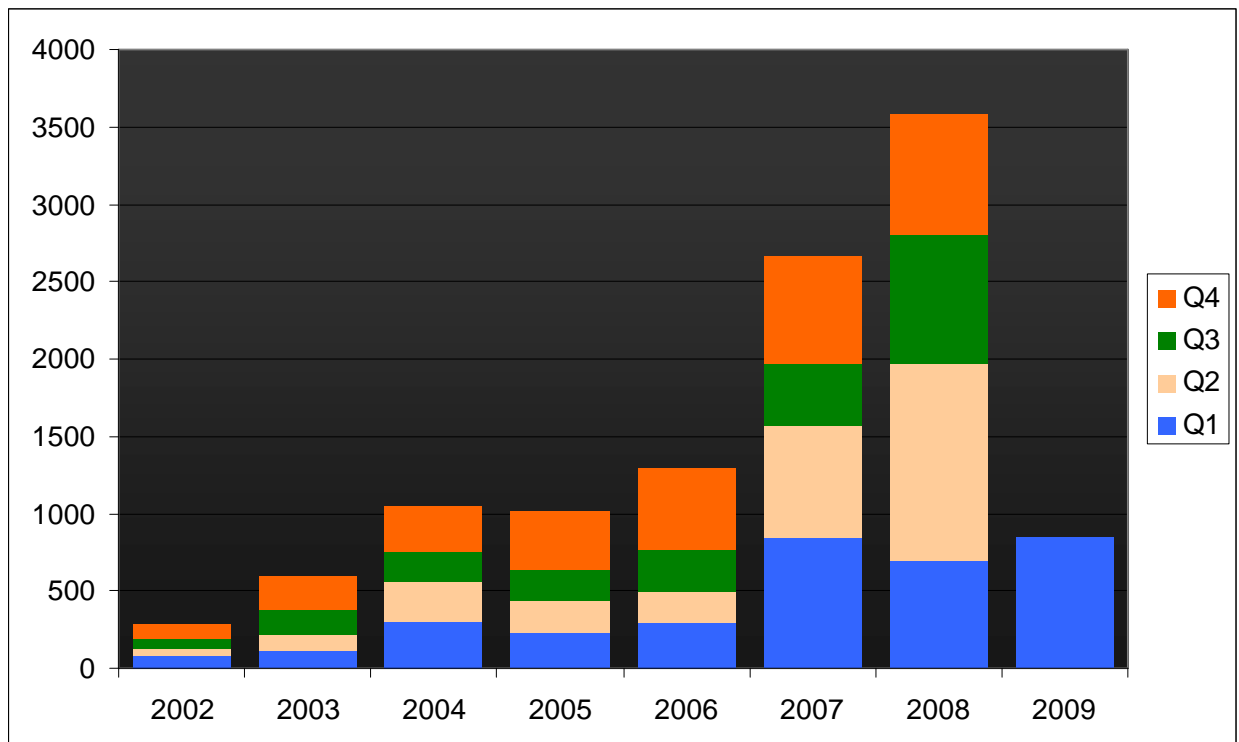
CERT-FI tietoturva- katsaus 1/2009

Johdanto

Vuodenvaihteen jälkeen on tietoturvauutisia hallinnut Conficker- tai Downadup-nimellä tunnettu haittaohjelma. Conficker on levinnyt miljooniin tietokoneisiin ympäri maailman käyttämällä hyväkseen kolmea eri leviämistapaa. Verkkomato leviää Windows-käyttöjärjestelmän jo paikatuun haavoittuvuuden kautta tai kopioimalla itsensä verkkolevyille, jotka on suojattu heikolla salasanalla. Lisäksi mato kopioi itsensä tietokoneessa käytettäville USB-muistitikuille, joiden kautta se siirtyy uuteen koneeseen Windows-käyttöjärjestelmän AutoRun-ominaisuutta hyödyntämällä. Suomessa Conficker-tartuntoja on havaittu suhteellisen vähän.

Haittaohjelmat voivat tarttua muihinkin laitteisiin kuin tietokoneisiin. Suomessakin on havaittu ADSL-päätelaitteita, joihin on tartutettu botnet-haittaohjelma. Verkon aktiivilaitteissa olevan tartunnan havaitseminen voi olla vaikeaa ja laitteen suojaaminen ja ohjelmistojen päivittäminen vaikeampaa kuin työaseman ohjelmistopäivitysten pitäminen ajan tasalla.

Kohdistettuja haittaohjelmajakelua käytetään tietojen vakoilemiseen kohteena olevasta organisaatiosta. Tietoja varastavat haittaohjelmat voivat olla etähallittuja tai itsenäisesti toimivia, ja niitä pyritään tartuttamaan jakamalla niitä sähköpostiviestien liitetiedostoina tai linkkeinä tarkkaan rajatulle joukolla vastaanottajia. Viestien lähettäjäksi on väärennetty tunnettu taho, ja viestien aiheet ovat uskottavia ja organisaation normaaliin toimintaan liittyviä. Tyypillinen haittaohjelman sisältävä liitetiedosto voi olla esimerkiksi kutsu kokoukseen tai konferenssiin.



CERT-FI:n käsittelemien tapausten määrä oli alkuvuonna suunnilleen kahden edellisvuoden tasolla.

Laajalle levinnyt verkkomato muistuttaa tietoturvallisuuden perusasioista

Vuodenvaihteen jälkeen miljooniin tietokoneisiin ympäri maailman levinnyt *Conficker*- ja *Downadup*-nimillä tunnettu haittaohjelma muistuttaa haittaohjelmilta suojautumisen perusasioista. Haavoittuvien ohjelmien päivittäminen, hyvät salasana-käytännöt ja varovaisuus koneesta toiseen siirrettäviä muistilaitteita (esim. USB-muistitikut) käytettäessä ovat hyviä suo-jakeinoja.

Conficker-haittaohjelmassa tai sen tavasa levitä ei ole varsinaisesti uutta, mutta siihen kerätyt ominaisuudet ovat osoittautuneet varsin tehokkaaksi yhdistelmäksi madon leviämisen kannalta. Muistitikujen käyttäminen leviämismenetelmänä tuo mieleen jo 1980-luvulla levykkeiden kautta levinneet virukset.

Verkkomadolla on monta tapaa levitä

Conficker-haittaohjelman ensimmäiset versiot käyttävät useita eri leviämistapoja. Haittaohjelmasta on liikkeellä useita toisistaan hiukan poikkeavia versioita.

Verkkomato käyttää leviämisessään verkon kautta Microsoft Windows -käyttäjärjestelmän tiedostojen ja kirjoitimien jakamiseen liittyvää haavoittuvuutta, johon julkaistiin korjaava ohjelmistopäivitys lokakuussa 2008. Haittaohjelma voi kuitenkin levitä sellaisiin tietokoneisiin, joiden käyttäjärjestelmää ei ole päivitetty ja joiden haavoittuviin palveluihin saa yhteyden verkon kautta.

Tartuttuaan tietokoneeseen mato pyrkii kopiaimaan itsensä tietokoneessa käytettäville siirrettäville tallennusvälineille, kuten USB-muistitikuille. Kun Confickerin saastuttama muistitikku siirretään toiseen tietokoneeseen, käynnistyy haittaohjelma Windowsin Autorun-toiminnon avulla, jolloin toinen tietokone saa tartunnan.

Conficker yrittää myös kopioida itsensä lähiverkosta löytyville verkkolevyille. Tämän onnistumiseksi ohjelma yrittää arvaila verkkolevyjen käyttämiseksi tarvittavia salasanoja toimialueen hallintapalvelimelta. Jos käytössä on heikkoja salasanoja,

ohjelma saattaa onnistua yrityksessään. Salasanojen arvaaminen kuormittaa hallintapalvelinta, ja epäonnistuneet arvaukset johtavat usein myös arvauksissa käytettyjen käyttäjätunnusten sulkemiseen, mikä voi paljastaa lähiverkossa olevan tartunnan.

Maaliskuun loppupuolella havaitusta Conficker.C-nimellä tunnetusta haittaohjelman versiosta on kokonaan poistettu leviämismekanismit. Se ei siis pyri leviämään uusiin tietokoneisiin, vaan ainoastaan pyrkii päivittämään itsensä uuteen haittaohjelmaversioon.

Madon päivitysmekanismi perustuu verkkotunnuksiin ja vertaisverkko-yhteyksiin

Conficker pyrkii päivittämään itsensä tartunnan jälkeen ottamalla yhteyden päivämäärän ja kellonajan perusteella laskemaansa verkkotunnukseen uuden haittaohjelmätiedoston lataamista varten.

Tietoturvatutkijat ovat pystyneet selvittämään tavan, jolla haittaohjelma muodostaa käyttämänsä verkkotunnukset. Rekisteröimällä päivitykseen käytettäviä verkkotunnuksia ennalta on madon ensimmäisten versioiden päivittymistä pystytty haittaamaan.

Myöhemmät Conficker-versiot eivät enää välttämättä tarvitse tiettyä verkkoosoitetta, josta ne yrittävät ladata päivitystä, vaan ne käyttävät vertaisverkko-tekniikkaa päivitystiedoston löytämiseksi ja lataamiseksi.

Huhtikuun alusta lähtien yksi haittohjelman versio käyttää päivittymispyrkimyksissään aikaisempaa huomattavasti useampia verkkotunnuksia, mikä vaikeuttaa päivitysten estämistä.

Confickerin tarkoitus on arvoitus

Tartuttuaan tietokoneeseen Conficker pyrkii haittaohjelmille tyypilliseen tapaan piilottamaan itsensä niin, että sen havaitseminen tai poistaminen on mahdollisimman vaikeaa. Ohjelman poistamista varten on julkaistu työkalu, mutta usein haittaohjelmien saastuttamaan tietokoneeseen on varminta asentaa käyttäjärjestelmä kokonaan uudestaan.

Toistaiseksi Confickerin levittämiselle ei ole tullut esiin varsinaista tarkoitusta. Tähän saakka tavattujen versioiden ei ole todettu tekevän muuta kuin leviävän tietokoneesta toiseen ja yrittävän päivittää itsensä uudempaan versioon.

Jos haittaohjelma päivittyy onnistuneesti, uusi ohjelmatiedosto voi sisältää uusia ominaisuuksia ja haitallisia toimintoja.

Suomessa madon leviämistä on torjuttu melko tuloksetta

Conficker-haittaohjelman leviämisen laajuutta on voitu arvioida kohtalaisen luotettavasti, koska sen tapa päivittää itsensä on onnistuttu selvittämään. Haittaohjelman lähettämien päivityspyyntöjen perusteella on arvioitu, että mato on levinnyt yli viiteentoista miljoonaan tietokoneeseen maailmanlaajuisesti.

Suomessa tartuntoja on arvioitu olevan joitakin tuhansia, mitä voidaan pitää kohtalaisen pienenä määränä. Madon leviämistä Suomessa on hidastanut se, että madon hyödyntämän Windows-käyttäjärjestelmän haavoittuvan palvelun käyttämät portit on suljettu kuluttajille tarjottavista internetliittymistä. Yritysverkkoja suojaavat palomuurit estävät myös tartunnan aiheuttavan liikenteen internetistä. Sisäverkoissa mato voi kuitenkin usein levitä myös verkon kautta koneesta toiseen.

Verkkomato on kaikesta huolimatta Suomessakin päässyt leviämään joidenkin suurehkojen organisaatioiden verkkoihin. Mato pääsee todennäköisimmin sisäverkkoon koneiden välillä siirrettävien USB-muistitikkujen välityksellä.

Haittaohjelmat voivat tarttua muihinkin laitteisiin kuin henkilökohtaisiin tietokoneisiin

CERT-FI:n tietoon on tullut tapauksia, joissa käyttäjän laajakaistamodeemi tai reititin on murrettu ja liitetty botnet-verkkoon. PsyBot-nimisellä haittaohjelmalla on tartutettu Linux-käyttäjärjestelmällä varustettuja laitteita, joissa on käytössä BusyBox-komentokäyttöliittymä.

Kyseisessä tapauksessa murtautumiseen ei ole käytetty hyväksi varsinaista ohjelmistohaavoittuvuutta. Haittaohjelma on asennettu sellaisiin laitteisiin, joiden etähallintakäyttöliittymässä on käytetty tehdasasennuksen jäljiltä olevaa hallintatunnusta ja heikkoa salasanaa eikä niitä ole muutettu turvallisemmiksi otettaessa laite käyttöön.

Operaattorien toimittamissa laitteissa tunnukset ja salasanat on yleensä muutettu turvallisemmiksi, mutta kaupan hyllyltä saatavilla olevissa ADSL-päätelaitteissa, WLAN-tukiasemissa ja muissa aktiivilaitteissa on käytössä oletustunnukset ja salasanat jos käyttäjä ei niitä itse muuta.

Yleistyessään verkkolaitteiden haavoittuvuudet ja niihin kohdistuvat haittaohjelmahyökkäykset voivat olla haastavia. Verkon aktiivilaitteeseen tarttunut haittaohjelma voi jäädä helpommin kokonaan huomaamatta kuin työaseman haittaohjelmatartunta. Laitteissa ei ole käytössä virustorjuntaohjelmia eikä niiden ja internetin välissä ole erillistä palomuuria suodattamassa yhteyksiä. Laitteet ovat yleensä päällä jatkuvasti, joten haittaohjelmakoodia ei tarvitse välttämättä tallentaa laitteeseen pysyvästi.

Työasemat on totuttu päivittämään säännöllisesti ja asentamaan käyttäjärjestelmään ja ohjelmistoihin valmistajan tarjoamat tietoturvapäivitykset. Verkkolaitteiden ohjelmistopäivityksiä varten ei ole samanlaisia menetelmiä ja käytäntöjä, joten haavoittuvuuksien korjaaminen kestää usein kauemmin kuin työasemissa.

Kohdistettuja haittaohjelmahyökkäyksiä eri organisaatioihin

Maaliskuun lopussa julkaistiin Kanadassa raportti¹, jossa kerrottiin laajasta kohdistettujen haittaohjelmajakelujen avulla tehdystä tietomurtojen sarjasta. Raportin mukaan Gh0st-haittaohjelman avulla muodostettua etähallintayhteyttä on käytetty tietojen vakoilemiseen eri organisaatioiden tietokoneista.

¹ <http://www.f-secure.com/weblog/archives/ghostnet.pdf>

CERT-FI on jo aikaisemmin kertonut tieto- ja varastavista haittaohjelmista, joita on pyritty levittämään myös suomalaisiin organisaatioihin. Haittaohjelmia on levitetty sähköpostiviestien liitetiedostoina rajatulle ja tarkkaan valitulle vastaanottajien joukolle. Viestien lähettäjäksi on väärennetty tunnettu taho, ja viestien aiheet ovat olleet uskottavia ja organisaation normaaliin toimintaan liittyviä. Tyypillinen haittaohjelman sisältävä liitetiedosto voi olla esimerkiksi kutsu kokoukseen tai konferenssiin.

Kohdistetuissa hyökkäyksissä käytetyt haittaohjelmat ovat yleensä olleet sellaisia versioita, joita virustorjuntaohjelmat eivät ole hyökkäyksen toteuttamisvaiheessa tunnistanee. Ohjelmien tarkoituksena on ollut saada käyttäjän tietokone etähallittavaksi, jolloin sen kautta voidaan hankkia tietoja organisaation toiminnasta.

Haittaohjelmatilastot eivät näytä kasvua vielä vuonna 2008

CERT-FI on julkaissut tilastotietoja vuoden 2008 haittaohjelmahavainnoista. Tilastoista nähdään, että haittaohjelmahavaintojen määrä suomalaisissa verkoissa on pysynyt lähes ennallaan sitten kesän 2007.

Haittaohjelmahavaintojen lukumäärä laajakaista-asiakasta kohti laskettuna on laskenut viime vuosina, vaikka laajakaistaliittymien määrä kasvaa edelleen. Vuoden 2008 loppupuolella laajakaistaliittymien määrä Suomessa ylitti kahden miljoonan rajan. Edellisvuoteen verrattuna kasvua on lähes 20 prosenttia.

Conficker-verkkomato tulee näkymään tilastoissa ainakin vuoden 2009 alkupuoliskon osalta. CERT-FI on ensimmäisen vuosineljänneksen aikana lähettänyt yli 14000 raporttia pelkästään kyseiseen verkkomatoon liittyen. Suomalaisissa verkoissa verkkomadon saastuttamia koneita on havaittu yli 3600 eri IP-osoitteesta.

Suomalaistenkin toimijoiden tietoja julkaistu epähuomiossa web-sivustoilla

CERT-FI:n tietoon on tullut joitakin tapauksia, joissa suomalaisen organisaation suojattavia tietoja, kuten käyttäjätunnus- ja salasana-tietoja on epähuomiossa ollut saatavilla web-sivustoilla. Asianosaisille ei ole aiheutunut suurta vahinkoa, mutta joissain tapauksissa on ollut edellytyksiä suurempienkin vahinkojen syntymiselle.

Suojattavien tietojen joutuminen erehdyksessä tai huolimattomuudesta johtuen julkisesti saataville näyttää niitä koskevien uutisten perusteella olevan melko yleistä eri puolilla maailmaa.

Nimipalvelua hyödyntävissä palvelunestohyökkäyksissä uusia mausteita

CERT-FI on kertonut viime vuosina useista tapauksista, joissa avoimia rekursiivisia nimipalvelimia on hyödynnetty palvelunestohyökkäyksissä.

Viime aikoina on havaittu yhä enemmän sellaisia hyökkäyksiä, joissa käytetään hyväksi nimipalvelimia, jotka vastaavat nimipalvelimen omasta välimuistista tai tiedostojärjestelmästä löytyviä tietoja koskeviin kyselyihin. Kyselyt voivat kohdistua esimerkiksi juurinimipalvelinten osoitteisiin, jotka löytyvät jokaiselta nimipalvelimelta.

CERT-FI on elokuussa 2008 ja helmikuussa 2009 tutkinut fi-verkkotunnuksia palvelevien nimipalvelinten tilaa ja todennut, että niiden joukossa on paljon sellaisia palvelimia, joita voi eri tavoin käyttää hyväksi palvelunestohyökkäyksissä. Näiden tutkimuskierrosten perusteella on todettu, että nimenomaan nimipalvelimen välimuistitietoja koskeviin kyselyihin vastavia nimipalvelimia löytyy verkosta vielä avoimia rekursiivisia palvelimia enemmän.

Tulevaisuuden näkymiä

Lähitulevaisuudessa kiinnostaa erityisesti mitä tapahtuu Conficker-haittaohjelmilla saastuneille tietokoneille. Mato on toistaiseksi vain levittänyt itseään ja pyrkinyt päivittämään itsensä uudempaan versioon.

Pitemmällä aikavälillä on odotettavissa, että haittaohjelmien kehitys siirtyy myös muihin ympäristöihin kuin varsinaisiin tietokoneisiin. Yhä useammat kotien sähköiset laitteet kytketään myös internetiin, eikä niissä käytettävien ohjelmistojen mahdollisia haavoittuvuuksia ole tutkittu läheskään siinä määrin kuin tietokoneiden käyttöjärjestelmiä ja ohjelmistoja.

CERT-FI-yhteydenotot nimikkeittäin	1-3/2009	1-3/2008	Muutos
Haastattelu	35	17	+106%
Haavoittuvuus tai uhka	20	39	-49%
Haittaohjelma	577	460	+25%
Neuvonta	93	64	+45%
Hyökkäyksen valmistelu	10	32	-69%
Tietomurto	28	14	+100%
Palvelunestohyökkäys	23	15	+53%
Muu tietoturvaongelma	23	10	+130%
Social Engineering	33	47	-30%
Yhteensä	842	698	+21%

Ilmoitukset haittaohjelmista muodostivat suurimman osan CERT-FI:n käsittelemistä tietoturvatapauksista alkuvuoden 2009 aikana. Lisää tilastotietoja löytyy osoitteesta www.cert.fi.