

CERT-FI

VUOSIKATSAUS 2009

20.01.2010

CERT-FI vuosikatsaus 2009

Johdanto

Conficker levisi laajalti

Conficker-haittaohjelma levisi vuoden 2009 aikana miljooniin tietokoneisiin. Suomessakin tuhansiin koneisiin verkon tai liikuteltavien muistivälineiden kautta levinnyt Conficker on arvoituksellinen, sillä sen ei ole vielääkään todettu tekevän juuri muuta kuin leviävän koneesta toiseen.

Haittaohjelmien avulla voi luvattomasti etähallita käyttäjän tietokonetta tai urkkia käyttäjän tietoja. Suomessakin tuli tietoon tapauksia, joissa haittaohjelman avulla on puututtu verkkopankki-istunnon sisältöön ja tehty luvattomia tilisiirtoja käyttäjän tietämättä.

Kansainvälinen yhteistyö tiivistä

Kansainväliset tietoturvayhteisöt ja viranomaiset ovat vuoden mittaan tiivistäneet yhteistyötään. Conficker-haittaohjelman torjuntatoimien lisäksi on haitallista sisältöä tarjoavia yrityksiä suljettu verkosta. Haittaohjelmien käyttämien verkkotunusten käyttöä on myös estetty.

Vertaileva tutkimus eurooppalaisista CERT-toimijoista

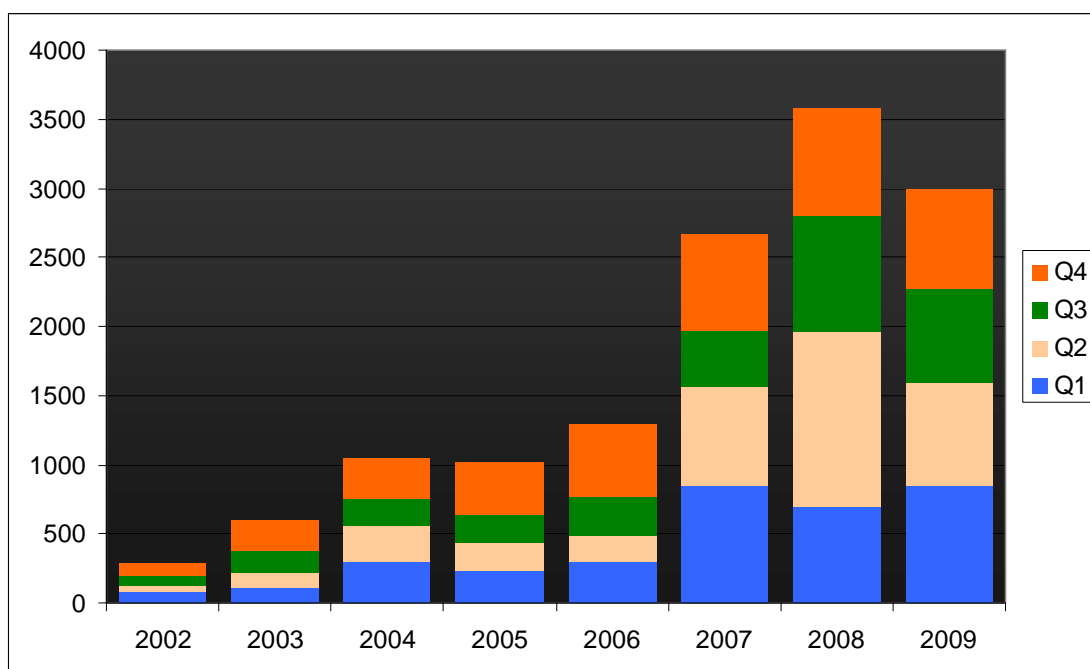
CERT-FI saattoi vuoden 2009 aikana päätökseen tutkimuksen eurooppalaisista CERT-toimijoista. Tutkimuksessa vertailtiin yhdentoista CERT-yksikön toimintaa. Tutkimus oli ensimmäinen laatuaan Euroopassa ja sen tulokset ovat herättäneet kansainvälistä kiinnostusta.

Sähköisen viestinnän tietosuojalaki uudistui

Sähköisen viestinnän tietosuojalain muutos tuli voimaan kesäkuussa. Viestintävirasto on lain voimaantulon jälkeen jo keran suosittanut teleyrityksiä ryhtymään uudistetun lain mukaisiin toimenpiteisiin suomalaisten verkkopankkien käyttäjien suojelemiseksi.

Ruotsin tiedustelutoiminta voi vaikuttaa myös suomalaisten tietoliikenneyhteyksiin

Uusi signaalitiedustelua koskeva laki tuli voimaan Ruotsissa 1.12.2009. Viestintäviraston määräyksen mukaan teleyrityksillä on velvollisuus tiedottaa asiakkailleen ulkomailta toteutettaviin, suomalaisille asiakkaille tarjottaviin palveluihin kohdistuvista tietoturvavauhkista.



CERT-FI:n vuosittain käsittelemien tapausten määrä näyttää tasaantuvan.

Conficker eniten levinnyt haittaohjelma

Conficker-haittaohjelman aggressiivinen leviäminen johti miljoonien tietokoneiden saastumiseen. Eräs vuoden 2009 lopulla esitetty arvio Confickerin saastuttamien tietokoneiden määrästä oli noin seitsemän miljoonaa tietokonetta ympäri maailmaa. Suomessakin kyseinen haittaohjelma on tarttunut tuhansiin tietokoneisiin.

CERT-FI:n Autoreporter-järjestelmä lähetti vuoden 2009 aikana lähes 100 000 Conficker-verkkomatoon liittyvää ilmoitusta. Lukumäärä ei suoraan kerro tartunnan saaneiden koneiden määrää, koska ilmoitusten joukossa on paljon toistuvia IP-osoitteita. Lähempi tarkastelu osoittaa, että suomalaisissa verkoissa havaittiin vuoden aikana runsaat 25 000 verkkomaton saastuttamaa konetta.

Yksi syy Confickerin tehokkaaseen leviämiseen on sen kyky levitä liikuteltavien tallennusvälineiden, kuten USB-muistitikkujen välityksellä. Lisäksi ohjelma leviää madoille tyypilliseen tapaan myös verkkoyhteyden välityksellä.

Conficker on arvoituksellinen haittaohjelma, sillä sen varsinaista tarkoitusta ei edelleenkään tiedetä. Yhden Conficker-muunnelman tiedetään tosin levittäneen myös Waledac-haittaohjelmaa sekä peloteluohjelmana tunnettua Spyware Guard-haittaohjelmaa. Waledacia on käytetty aiemmin roskapostin lähettämiseen, sekä erilaisten verkkopalveluiden tunnusten varastamiseen.

Haittaohjelmia levittävät roskapostikampanjat osuivat myös Suomeen

Huijauksiin pyrkivät roskapostikampanjat ovat kohdistuneet pääasiassa ulkomailla toimivien pankkien ja erilaisten yhdysvaltaisten toimijoiden, kuten Yhdysvaltojen veroviraston IRS:n sivustoihin.

Haitallista sisältöä välittäviltä roskaposteilta ei Suomessakaan vältytty. CERT-FI sai useita raportteja suomalaisiin osoitteisiin lähetetyistä roskaposteista, jotka ovat sisältäneet haittaohjelmalinkejä.

Roskapostiviestien sisältämistä linkeistä

löytyy usein jokin Zeus-haittaohjelma-perheen muunnelmä. Ohjelma tunnetaan myös nimellä Zbot ja WSNPOEM. Suomeenkin osuneessa Zeus-roskapostikampanjassa sähköpostin vastaanottaja sai viestin, jonka mukana olleen linkin kautta saisi ladattua Outlook-sähköpostiohjelman asetuksia määrittävän apuohjelman. Todellisuudessa linkki johti haittaohjelmaan.

Zbot-haittaohjelmia tiedetään käytetyn muun muassa verkkopalveluihin käytettyjen tunnusten sekä luottokorttitietojen varastamiseen. Osa haittaohjelma-perheen muunnelmista on myös varustettu eri verkkopankkeja tunnistavilla mekanismeilla. Toistaiseksi suomalaisia verkkopankkeja vastaan räätälöityä Zeus-haittaohjelmaa ei ole tavattu.

Confickerin tai Zbotin saastuttamat koneet ovat esimerkki siitä, miten käyttäjien tietokoneita otetaan luvatta haltuun ja käytetään monenlaisen haitalliseen toimintaan. Suuret etähallittavat botnetit voivat koostua jopa sadoista tuhansista kaapaetuista tietokoneista.

Haittaohjelmia levitettiin murrettujen www-sivustojen kautta

CERT-FI:lle raportoidaan jatkuvasti suomalaisista murretuista tai haavoittuvista www-sivustoista. Sivustojen sisältöä on muokattu lisäämällä sinne joko lukukelvottomaksi muunnettua JavaScript-koodia, tai piilotettu iframe-kehys. Käyttäjän vieraillessa murretulla websivulla selain lataa haittaohjelman sisältämän sivun.

Edellä kuvattua haittaohjelmien levitystapaa kutsutaan englanniksi drive by download -hyökkäykseksi. Käyttäjä ei välttämättä huomaa tartuntaa lainkaan ja tartunta voi tapahtua vieraillemalla luotettavanakin pidetyllä sivustolla.

Sivustoille voidaan lisätä haitallista sisältöä joko palvelimen haavoittuvuuksien tai varastettujen ylläpitotunnusten avulla.

Gumblar varastaa FTP-tunnuksia

Sivustojen ylläpitotunnuksia varastavat haittaohjelmat, kuten Gumblar, mahdollistavat sivujen sisällön luvattoman muokkaamisen. Ohjelma etsii tartunnan saaneelta tietokoneelta ylläpitoon käytettäviä FTP-tunnuksia ja niihin liittyviä salasanoja tutkimalla www-sivustojen ylläpitoon käytettyjen ohjelmien, kuten Filezilla tai Dreamweaverin salasanatiedostot.

Gumblar osaa myös tarkkailla tietokoneen ja FTP-palvelimen välistä verkkoliikennettä ja erottaa liikenteestä selkokielisenä lähetettävät tunnukset ja salasanat. Haittaohjelma käyttää näitä tunnuksia levitäkseen edelleen muokkaamalla www-sivustoja varastamiensa tunnusten avulla. Niiden avulla se lisää sivuille piilotetun iframe-kehiksen, jonka sisällä on linkkejä haitallisille sivustoille.

Käyttäjää houkutellessa haitallisille sivustoille hakukoneiden avulla

Haittaohjelmien levittämisen keinona käytetään myös internetin hakukoneiden tulosten manipuloimista. Haitallista sisältöä tarjoava www-sivusto pyritään nostamaan hakukoneen tuloksissa puhtaita sivustoja korkeammalle. Osa hakukoneista ottaa vastaan raportteja haitallisista sivustoista ja suodattaa ne pois hakutulosten joukosta.

Ajankohtaiset tapahtumat, kuten luonnonkatastrofit ja julkisuuden henkilöihin kohdistuvat skandaalit, ovat suosittuja hakukohteita. Sisällyttämällä sopivia hakusanoja sivuille ja linkittämällä SQL-injektioiden ja haittaohjelmien avulla paljon sivuja osoittamaan haluttuun kohteeseen, voidaan vaikuttaa hakukoneiden tuloksiin. Vuodenvaihteen jälkeen Haitin maanjäristys on ollut huijareidenkin suosikkiaihe.

Nimipalvelu altis väärinkäytösyrityksille

Nimipalvelu on niin olennainen osa internetin käyttöä, että se houkuttelee myös väärinkäytösyrityksiin. Haittaohjelmat voivat ohjata nimipalvelukyselyt hyökkääjän hallitsemaalle nimipalvelimelle, jolloin käyttäjä voidaan harhauttaa väärennetyille www-sivustolle.

Nimipalvelun vastausten varmentamiseksi on olemassa DNSSEC-niminen todentamismekanismi, mutta se ei ole toistaiseksi vielä kovin laajasti käytössä.

Oheisohjelmistojen haavoittuvuudet pitempään hyväksikäytettävissä

Haittaohjelmat käyttävät hyväkseen käyttöjärjestelmän tai ohjelmistojen haavoittuvuuksia. Käyttöjärjestelmä tai www-selain päivitetään usein automaattisesti, jolloin niissä olevat haavoittuvuudet tulevat korjatuiksi melko nopeasti.

Ohjelmien kohteena ovatkin usein muut ohjelmistot tai selaimiin asennettavat lisäosat. Viime aikoina on tavattu haittaohjelmia, jotka pyrkivät käyttämään hyväkseen esimerkiksi PDF-lukijan, Flash-soittimen tai Java-ympäristön haavoittuvuuksia.

Käyttäjä voidaan houkutella asentamaan haittaohjelma

Murretut www-sivustot voivat myös houkutella käyttäjän asentamaan haittaohjelman tietokoneeseen itse, jolloin käyttöjärjestelmän suojausten ohittaminen on helpompaa.

Sivustolla vieraileminen voi avata näytölle ponnahdusikkunan, joka varoittaa siitä, että tietokoneeseen olisi tarttunut haittaohjelma. Asentamalla ja suorittamalla ikkunassa suositellun ohjelman, kone tutkitaisiin haittaohjelmatartuntojen varalta ja mahdolliset haittaohjelmat poistettaisiin. Todellisuudessa asennettava ohjelma on itse haitallinen.

Pelotteluohjelmat voivat olla hyvin uskotavan näköisiä, eikä niistä voi suoraan sanoa, että ne eivät ole oikeita tietoturvaohjelmistoja. Ohjelmat voivat myös kysyä asennuksen yhteydessä luottokorttinumeroa lisenssimaksua varten ja asentaa tietokoneeseen käyttäjän näppäilyjä tallentavan ohjelman ja muita vakoiluohjelmia.

Tietoturvaohjelmilta näyttäviä valeohjelmia on tavattu jo usean vuoden ajan ja niiden määrän on arvioitu edelleen kasvavan.

Laajalevikkisiä ja kohdistettuja hyökkäyksiä

Haittaohjelmia voidaan levittää laajalla jakelulla ja pyrkiä siten vaikuttamaan mahdollisimman moneen tietokoneeseen ja käyttäjään. Tavoitteena voi olla hyökkäjän hallitseman botnet-verkon kasvataminen tai henkilöiden tietojen luvaton hankkiminen.

CERT-FI:n tietoon tuli myös tiettyihin organisaatioihin suunnattuja kohdistettuja hyökkäyksiä. Viestien lähettäjäksi on värennetty tunnettu taho, ja viestien aiheet ovat uskottavia ja organisaation normaaliin toimintaan liittyviä. Viesti voi olla esimerkiksi kutsu kokoukseen tai konferenssiin ja sen jakelu voi koostua organisaation avainhenkilöistä. Mukana jaetun haittaohjelman versio on tavallisesti ennestään tietoturvaohjelmistoille tuntematon.

Ghostnet

Vuoden 2009 maaliskuussa julkaistiin Kanadassa raportti, jossa kerrottiin laajasta kohdistettujen haittaohjelmajakelujen avulla tehdystä tietomurtojen sarjasta. Ghost-haittaohjelman avulla muodostettua etähallintayhteyttä käytettiin tietojen vakoilemiseen eri organisaatioiden tietokoneista.

CERT-FI:n tietojen mukaan haittaohjelmien levittäjien joukossa ei ollut suomalaisia tahoja. CERT-FI:n tietoon tuli kaksi suomalaisessa verkossa ollutta vieraan valtion tietokonetta.

Haittaohjelmilla peloteltiin myös aiheettomasti

CERT-FI:lle raportoitii vuoden 2009 aikana toistuvasti sähköposteissa liikkuneesta kiertokirjeestä, jossa varoitettiin sähköpostin liitteenä tulevasta haittaohjelmasta, jonka kerrottiin tuhoavan kiintolevyn tiedostot. Viesti on aikaisemmin levinnyt nettissä englannin- ja ruotsinkielisenä versiona. Joulukuussa 2009 viestin lähettäjäksi oli värennetty keskusrikospoliisin henkilökuntaan kuuluva henkilö.

CERT-FI:n tietojen mukaan ihmisten toisilleen ilmeisesti varoitustarkoituksessa lähetettävät kopiot viestistä eivät sisältäneet haittaohjelmaa tai linkkejä haittaohjelmia

sisältäville sivustoille. Mainitun kiertokirjeen lisäksi on liikkeellä ollut myös muita kiertokirjeitä, joissa on luvattu joko matkapuhelimia tai rahaa. Kiertokirjeissä on myös perinteisemmin luvattu onnea tai epäonnea riippuen siitä, kuinka usealle sähköpostin lähettää eteenpäin.

Perinteisempiä sähköpostina lähetettäviä huijausyriytyksiä on liikkeellä jatkuvasti. Niissä voidaan kertoa perinnöstä, arpa-jaisvoitosta tai tarjota työtä rahanvälittäjänä.

Matkaviestimissäkin turvallisuuspuutteita ja haittaohjelmia

Vuoden 2009 alkupuolella tuli esiin älypuhelimien asetusviesteihin ja WAP push -viesteihin liittyviä tietoturvaongelmia.

Matkapuhelinten verkkoasetusten asettamiseen tarkoitettujen asetustekstiviestien käsittelyyn liittyvät puutteet ovat olleet asiantuntijoiden tiedossa jo kauan. Kyse on siitä, että kaikki matkapuhelimet eivät tarjoa käyttäjälle mahdollisuutta varmistua asetustekstiviestien todellisesta lähettäjistä. Lisäksi puhelin voi joissakin tapauksissa hyväksyä asetukset käyttäjän tietämättä tai jättää muutettavat asetukset näyttämättä.

WAP push -viesti on puhelimelle lähetetty viesti, joka sisältää linkin WAP-osoitteeseen. Joidenkin Suomessa harvinaisten vanhempien puhelinmallien WAP Push -viestien käsittelyssä on ilmennyt ongelmia. Ongelmallisesti käyttäytyvä matkapuhelin saattaa WAP Push -viestin vastaanottaessaan ladata ja jopa asentaa viestissä määritellyn WAP-sisällön käyttäjän tietämättä.

Mato levisi iPhone-matkapuhelimissa

Applen iPhone-matkapuhelimissa tavattiin loppuvuodesta Ikee.B-nimellä tunnettu verkkomato, joka levisi puhelimesta toiseen sshd-palvelun ja vaihtamatta jätettyjen oletussalasanoiden avulla. Mato levisi vain niissä puhelimissa, joista on poistettu lukitus niin, että niissä voi käyttää myös muita kuin Applen virallisesti hyväksymiä ohjelmistoja. Lukitusta poistamatta sshd-ohjelmistoa ei voi asentaa.

Älypuhelimet ovat houkutteleva kohde

Älypuhelimien ominaisuudet lähestyvät henkilökohtaisia tietokoneita. Niillä on usein lähes jatkuva internetyhteys, ja niihin voi myös ottaa yhteyden internetistä. Käytettävät sovellukset ovat osittain samoja tai muistuttavat ominaisuuksiltaan varsinaisissa tietokoneissa käytettäviä ohjelmistoja.

Puhelimien käyttöjärjestelmien ja ohjelmistojen tietoturvatilanne on monella tavoin tavallisia tietokoneita huonompi. Puhelimiin ei tavallisesti ole asennettu tietoturvaohjelmistoja eikä niissä ole käytössä keskitettyä hallintaa tai automaattisia ohjelmistopäivityksiä. Puhelimia myös katoaa ja niitä varastetaan useammin. Matojen leviämistä edistää se, että puhelimet liikkuvat eri tietoverkkojen välillä.

Haittaohjelmia on tavattu myös muissa laitteissa

Suomesta löydettiin alkuvuodesta ADSL-päätelaitteita, joihin oli tartutettu botnet-haittaohjelma. Verkon aktiivilaitteissa olevan tartunnan havaitseminen voi olla vaikeaa ja laitteen suojaaminen ja ohjelmistojen päivittäminen vaikeampaa kuin työaseman ohjelmistopäivitysten pitäminen ajan tasalla.

Kansainvälistä yhteistyötä väärinkäytösten torjumiseksi

Haittaohjelmia laativat ja levittävät sekä botnet-verkkoja operoivat tahot ovat verkostoituneita ja niiden toiminta muistuttaa rakenteeltaan ohjelmisto- ja ICT-palveluteollisuudesta tuttua mallia.

Haittaohjelmien levitykseen ja botnet-verkkojen komentopalvelimiksi käytettäviä palvelimia vuokrataan usein suurilta palveluntarjoajilta, joilla voi olla lukuisia alihankintasuhteita fyysisen palvelinlaitteen vuokraajasta lopullisen www-palvelukapasiteetin vuokraajaan. Laittilojen tarjoaja ei välttämättä tiedä mitään rikollisesta loppuasiakkaasta. Toisena ääripäänä ovat ilmeisen kokonaisvaltaisesti rikolliseen toimintaan keskittyneet toimijat, jotka ulkoisesti pitävät yllä näennäisen asiallisen hosting-palveluntarjoajan kulis-seja.

Vuonna 2009 ei nähty merkkejä väärinkäytösten määrän kasvun hidastumisesta.

Voimakkaasti hajautettuun toimintaan pohjaavien botnet-verkkojen selvittely vaatii vastavuoroisesti hyvin laajamittaista kansainvälistä monitoimialayhteistyötä. CERT-toimijat, internet-palveluntarjoajien tietoturvakysiköt, tietoturvatutkijat yliopistoissa ja alan yrityksissä sekä poliisiviranomaiset ovat verkottumassa entistä tiiviimmin yhteistyöverkostoiksi. Verkostojen toiminta aktivoitui ja tiivistyi selvästi vuoden 2009 aikana.

Tietoturvayhteisöjen kansainvälinen yhteistyö on osoittautunut toimivaksi

Esimerkkinä tietoturvatyöryhmien yhteistyön toimivuudesta voidaan pitää syksyllä 2009 selvitettyä palvelunestohyökkäystä, joka kohdistui osaltaan myös suomalaiseen yritykseen.

CERT-FI sai kansainvälisen yhteistyön ansiosta selville hyökkäykseen käytetyn botnet-verkon komentopalvelimen noin tunnissa tietoturvaloukkausilmoituksen saapumisesta. Tehokkaat hyökkäyksen vaikutusta rajoittavat toimenpiteet voitiin käynnistää nopeasti. CERT-FI myös varoitti useita ulkomaisia tahoja, jotka olivat saman botnet-verkon hyökkäyksen kohteena. Komentopalvelimia siivottiin useista eri maista eri puolilta maailmaa.

Haitallista sisältöä tarjoavia operaattoreita suljettiin verkosta

Tietoturvayhteisöjen selvityksen perusteella useampikin haitalliseen toimintaan keskittynyt operaattori menetti verkkoyhteytensä vuoden 2009 aikana. Ehkä näkyvin tapaus oli yhdysvaltalainen 3FN-palveluntarjoaja. Kyseisen operaattorin verkossa ylläpidettiin useiden roskapostinlevitysverkon komentopalvelimia.

CERT-FI avusti islantilaisia kollegoita verkopankkijärjestelmien tunnuksia varastavan haittaohjelmatapauksen selvittelyssä. Tapauksen yhteydessä tunnistettiin Latviasta selvästi haitalliseen toimintaan keskittynyt palveluntarjoaja. Latvia on pohjoismaita lähin EU-maa, jossa voitiin havaita selvästi lisääntyneitä tietoturva-vaarantavien palveluiden tarjontaa.

Confickerin torjunta yhdisti tietoturvatyöntekijöitä

Yksi laajimmista kansainvälisten tietoturvatyöntekijöiden yhteisöistä suunnattiin Conficker-haittaohjelmaperhettä vastaan. Erityinen työryhmä, "Conficker Working Group", kehitti torjuntatoimia haittaohjelmaa vastaan. Mukana oli ensimmäistä kertaa myös internetin verkkotunnuksia hallinnoiva ICANN, koska torjuntatoimet vaativat suuren verkkotunnuksien rekisteröinnin estämistä yhteistyössä verkkotunnuksia rekisteröivien organisaatioiden kanssa.

CERT-FI toteutti vertailevan tutkimuksen eurooppalaisista CERT-toimijoista

CERT-FI saattoi vuoden 2009 aikana päätökseen tutkimuksen eurooppalaisista CERT-toimijoista. Tutkimuksen tarkoituksena oli vertailla yhdentoista CERT-yksikön toimintaa ja tunnistaa käytössä olevia hyviä toimintamalleja, joita voitaisiin hyödyntää CERT-FI:n ja Viestintäviraston toiminnassa. Tutkimus oli ensimmäinen laatuun Euroopassa ja sen tulokset ovat herättäneet kansainvälistä kiinnostusta.

Tutkimukseen osallistuneiden CERT-toimijoiden välillä löytyi odotetusti sekä yhteneväisyyksiä että eroavaisuuksia. Tulosten perusteella voidaan todeta, että kaikki vertailut yksiköt ovat ainutlaatuisia. Kukin on muokannut toiminnastaan sijoitumisvaltionsa ja asiakaskuntansa vaatimusten mukaisen kokonaisuuden.

Toiminnasta löytyi kuitenkin myös lukuisia yhteneväisyyksiä. Kaikki vertailussa mukana olleet yksiköt toimivat oman maansa kansallisena yhteyspisteenä tietoturvaloukkauksien käsittelyn osalta. Yhteyspisteenä oleminen edellyttää toimivia ja laajoja koti- ja ulkomaisia kontaktiverkostoja, joiden merkitystä kaikki toimijat korostivat.

Lisäksi kaikki yksiköt tarjoavat asiakaskunnalleen joukon peruspalveluja. Niihin kuuluvat omaan valtioon liittyvien tietoturvaloukkausten analysoiminen ja koordinoiminen, kansallisen tietoturvatilanteen seuraaminen sekä tietoturvan tilannekuvaus.

Tutkimuksessa selvisi myös, että valmiudet tulokselliseen CERT-toimintaan vaihtelevat varsin paljon Euroopan valtioiden välillä. Myös Euroopan komissio on kiinnittänyt huomiota asiaan.

Viestintävirasto mukana Afrikan maiden CERT-toimintojen kehittämisessä

Viestintävirasto on vuoden 2009 aikana antanut kansainvälistä asiantuntija-apua kansallisen CERT-toiminnan käynnistämiseksi. Ulkoasiainministeriön rahoittamassa projektissa Etelä-Afrikkaa on autettu kehittämään valmiuksia CERT-toimintojen perustamiseksi ja käyttöönottamiseksi.

CERT-FI:hin palkatun projektityöntekijän tehtävänä on ollut tukea Etelä-Afrikan kumppaniorganisaatiota perustettavan CERT-toiminnon suunnittelussa. Lisäksi hänen vastuullaan on ollut kansainvälisen yhteistyön aloittaminen ja koordinoiminen sekä tapahtumien ja koulutuksien järjestäminen.

Myös Kenian ja Tansanian viestintäviranomaisille on jaettu näkemyksiä perustettavien CERT-toimintojen suunnittelua ja käynnistämistä varten.

Autoreporter palkittiin

CERT-FI:n tuottama Autoreporter-palvelu palkittiin FIRSTin (Forum of Incident Response and Security Teams) ja CERT/CC:n (CERT Coordination Center) järjestämässä kilpailussa¹. Kilpailussa etsittiin parhaita käytäntöjä tietoturvaloukkausten havaitsemiseksi ja estämiseksi.

Autoreporter on CERT-FI:n tuottama palvelu, joka kokoaa automaattisesti suomalaisia verkkoja koskevia haittaohjelma- ja tietoturvaloukkaushavaintoja. Järjestelmä lähetti vuoden 2009 aikana suomalaisten verkkoalueiden ylläpitäjille runsaat 215 000 ilmoitusta. Edelliseen vuoteen verrattuna ilmoitusten lukumäärä on kasvanut yli 250 prosenttia. Lukumäärän kasvaminen selittyy osittain Conficker-verkkomatoon liittyvien ilmoitusten suuressa määrässä.

¹ <http://www.cert.fi/tietoturvanvaynt/2009/06/ttn200906301435.html>

CERT-FI julkaisee tarkempia tilastotietoja vuoden 2009 haittaohjelmahavainnoista seuraavassa tietoturvakatsauksessaan huhtikuussa 2010.

Laajavaikutteisia ohjelmistohaavoittuvuuksia julkaistiin useita

CERT-FI julkaisi vuoden 2009 aikana kahden laajan haavoittuvuuskoordinaatioprojektin tulokset. Ne koskivat TCP-protokollatoteutuksiin ja XML-tiedostojen käsittelyyn tarkoitettujen kirjastojen haavoittuvuuksia. Lisäksi julkaistiin Microsoftin ATL-kehityskirjastoon ja SSL-protokollaan liittyvät haavoittuvuudet.

TCP-protokollan haavoittuvuus

TCP-protokollan toteutuksiin liittyvät virheet mahdollistivat palvelunestohyökkäyksen hyvin pienillä liikennemäärillä. Syyskuussa julkistettuun haavoittuvuustiedotteeseen on loppuvuoden aikana tullut lausunto kuudeltatoista eri valmistajalta. Myös koordinaatiotyössä mukana olleet CPNI², JP-CERT³ ja US-CERT⁴ julkaisivat omat tiedotteensa.

XML-tiedostojen käsittelyn haavoittuvuudet

Suomalainen Codenomicon Oy toi vuoden alkupuolella CERT-FI:n koordinoitavaksi tuloksia XML-tiedostojen käsittelyyn liittyvien ohjelmien testeistä. Kaikkiaan kolmesta XML-tiedostosta käsittelevästä ohjelmakirjastosta löytyi haavoittuvuuksia.

Korjauksia ohjelmistoihin on ilmestynyt pitkin vuotta kahdeltatoista valmistajalta. Osa haavoittuvuuksista oli korjattu erään kyseessä olleen kirjaston koodijakelussa, mutta korjaus ei ollut levinnyt kaikkiin kirjastoa käyttäneisiin tuotteisiin. Tämä osoittaa, että haavoittuvuuksien korjaaminen ei rajoitu ongelman syyn poistamiseen. On tärkeää välittää viesti korjaustarpeista ja korjaukseen liittyvistä yksityiskohdista myös niille toimijoille, joiden tuotteisiin haavoittuvuus vaikuttaa.

Microsoftin ohjelmistokehitykseen käytetyissä kirjastoissa virheitä

Microsoftin tuottaman ATL-ohjelmakirjaston kehitysversiosta löydettiin haavoittuvuus, joka mahdollisti hyökkääjän ohjelmakoodin suorittamisen kohdejärjestelmässä. Vaikka kirjaston lähdekoodia ei varsinaisesti ole missään vaiheessa julkaistu tuotteena käyttäjille, on sitä silti käytetty lukuisissa ohjelmistoissa. Microsoft on julkaissut korjauksen haavoittuvuuteen ja kuukausittaisten päivitysten mukana on jaettu haavoittuvien komponenttien toiminnan salpaavia estolistoja.

Koska haavoittuvuus koskee Microsoftin ohjelmistojen lisäksi suurta joukkoa kolmansien osapuolten tuotteita, Microsoft ilmoitti, että se on ryhtynyt yhteistyöhön myös muiden valmistajien kanssa virheiden korjaamiseksi.

SSL/TLS-protokollan haavoittuvuus

Marraskuussa julkisuuteen tullut SSL/TLS-protokollaan liittyvä haavoittuvuus mahdollistaa joissakin tapauksissa sen, että suojatun yhteyden alkuun voi syöttää omaa sisältöä. Vaikka haavoittuvuus ei mahdollista luottamuksellisen tiedon vuotamista, pidetään sitä vakavana, sillä SSL-suojaus on tärkeä osa esimerkiksi sähköisen kaupankäynnin turvallisuutta.

Haavoittuvuus on harvinainen, sillä se johtuu virheestä protokollan suunnittelussa ja siten vaikuttaa käytännössä kaikkiin SSL/TLS-toteutuksiin. Mitä aikaisemmassa vaiheessa järjestelmän toteutusta haavoittuvuuden synnyttävä virhe on tehty, sitä suurempi haavoittuvuuden vaikutusalueesta muodostuu ja sitä hankalampaa haavoittuvuuden korjaaminen tulee olemaan.

Haavoittuvuus korjataan määrittelemällä TLS-protokollaan laajennus, joka mahdollistaa aukon sulkemisen.

2 <https://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>

3 <http://www.jpCERT.or.jp/english/at/2009/at090019.txt>

4 <http://www.kb.cert.org/vuls/id/723308>

Sähköisen viestinnän tietosuojalain muutokset voimaan

Sähköisen viestinnän tietosuojalain muutos tuli voimaan kesäkuussa. Tunnistamistietojen käsittelyoikeuksien lisäksi muutos koski myös lain 20 pykälää tietoturva-toimenpiteistä. Säännöstä muutettiin, jotta se vastaisi paremmin teleyritysten, lisäarvopalveluntarjoajien ja yhteisötilaajien tarpeita.

Tietoturvasäännöstä valmisteltaessa otettiin huomioon yhteiskunnan elintärkeiden toimintojen kiinteä riippuvuus viestintäverkosta, viestintäpalveluista ja tietojärjestelmästä. Kriittisen infrastruktuurin suojaamiseen kuuluu olennaisesti myös sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistaminen. Tietoturvaohjeiden haittavaikutukset on pystyttävä minimoimaan Suomessa tehtävillä toimenpiteillä, sillä ulkomaisiin toimijoihin ja järjestelmiin voidaan vaikuttaa vain rajallisesti.

Lain mukaan teleyrityksillä, lisäarvopalveluntarjoajilla ja yhteisötilaajilla sekä niiden lukuun toimivilla on oikeus ryhtyä laissa tarkemmin määriteltyihin välttämättömiin toimiin tietoturvasta huolehtimiseksi.

Ensinnäkin toimenpiteisiin voidaan ryhtyä viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Toinen toimenpiteet mahdollistava tilanne on viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaaminen. Kolmantena tietoturva-toimenpiteet oikeuttavana tilanteena on viestintäpalvelujen kautta laajamittaisesti toteutettavien maksuvälinepetosten valmistelun ehkäiseminen.

Uuden lain tarjoamia mahdollisuuksia käytettiin verkkopankkikäyttäjien suojaamiseksi

Viestintävirasto on lain voimaantulon jälkeen kerran suosittanut teleyrityksiä ryhtymään uudistetun sähköisen viestinnän tietosuojalain mukaisiin toimenpiteisiin suomalaisten verkkopankkien käyttäjien suojelemiseksi. Kyseisessä tilanteessa yhdysvaltalainen verkko-operaattori oli tois-

tuvasti osallisena verkkopankkien käyttäjiin kohdistuneissa verkkourkinta- ja pe-stopapauksissa.

Liikenteen suodattaminen ei edellytä teleyrityksiltä Viestintävirastolta saatua suositusta. Suodatustoimenpiteet voidaan aloittaa aina kun teleyritykset arvioivat, että suodatuksen edellytykset täyttyvät.

Ruotsin tiedustelutoiminta voi ulottua myös suomalaisten tietoliikenneyhteyksiin

Uusi signaalitiedustelua koskeva laki tuli voimaan Ruotsissa 1.12.2009. Lailla annettiin Ruotsin puolustusvoimien radiolaitokselle (Försvarets Radioanstalt) oikeus suorittaa maanpuolustustarkoituksessa signaalitiedustelua myös kiinteissä verkoissa Ruotsin rajat ylittävän sähköisen viestinnän osalta. Myös suomalaisten toimijoiden Ruotsiin ja Ruotsin kautta välitettävä tietoliikenne joutuu näin ollen tiedustelutoiminnan piiriin.

Ruotsin kautta kulkevan tietoliikenteen tiedustelutoiminta on otettu huomioon Viestintäviraston uudistetussa määräyksessä, joka koskee teleyritysten velvollisuutta ilmoittaa asiakkailleen ja Viestintävirastolle palveluihinsa kohdistuvista tietoturvaohjeista. Määräys on tullut voimaan vuoden 2010 alusta. Määräyksessä korostetaan erityisesti teleyritysten velvollisuutta tiedottaa asiakkailleen ulkomailla toteutettaviin, suomalaisille asiakkaille tarjottaviin palveluihin kohdistuvista tietoturvaohjeista. Tiedotusvelvollisuus perustuu sähköisen viestinnän tietosuojalakiin.

Viestintävirasto on muistuttanut teleyrityksiä tästä tiedotusvelvollisuudesta jo vuodesta 2007 alkaen. Samalla on tuotu esiin muun muassa se, että teleyritysten on toteutettava palvelunsa tietoturvallisesti. Jos teleyritys ei pysty toteuttamaan palvelua ilman tietoturvaan kohdistuvaa uhkaa, on teleyrityksen ilmoitettava uhkista asiakkailleen ja Viestintävirastoon. Ilmoitukset antavat asiakkaille mahdollisuuden arvioida, vastaako palvelu heidän omia tietoturvatarpeitaan. Myös Viestintävirasto on julkaissut tietoa viestinnän suojaamisesta.⁵

⁵ <http://www.ficora.fi/viestinsuojaus/>

Tulevaisuuden näkymiä

CERT-FI:n näkemyksen mukaan haittaohjelmia levittämällä pyritään edelleen hankkimaan taloudellista etua. Luottokorttinumerot ja käyttäjätunnukset ovat kiinnostavimpia ja helposti markkinoitavia kohteita.

Yhteisöpalvelut ovat otollisia kohteita monenlaisille huijausyrityksille. Osassa palveluista on maksullista sisältöä, jota voi myydä palvelun sisällä edelleen, mutta myös erilaiset käyttäjätunnusten ja maksuvälinetietojen urkkimisyrietykset ovat edelleen yleisiä.

Älypuhelinien ohjelmistoista löytyvien haavoittuvuuksien tutkimuksen lisäksi voidaan odottaa kiinnostuksen lisääntyvän myös matkaviestinverkoissa käytettävien protokollien ja verkon toiminnan tutkimiseen. Vuonna 2009 julkaistiin ohjelmistoja, joiden avulla voidaan simuloida matkaviestinverkon osien toiminnallisuutta ohjelmallisesti.

Suurin osa CERT-FI:n käsittelemistä yhteydenotoista liittyi erilaisiin haittaohjelmiin ja niistä johtuviin tietoturvaongelmiin.

CERT-FI-yhteydenotot nimikkeittäin	2009	2008	Muutos
Haastattelu	97	88	+10%
Haavoittuvuus tai uhka	148	375	-61%
Haittaohjelma	1828	2156	-15%
Neuvonta	387	359	+8%
Hyökkäyksen valmistelu	48	87	-45%
Tietomurto	120	187	-36%
Palvelunestohyökkäys	89	96	-7%
Muu tietoturvaongelma	118	43	+174%
Social Engineering	164	189	-13%
Yhteensä	2999	3580	-16%