



CERT-FI VUOSIKATSAUS 2004

Tietoturvahaukien kehitykseen vaikutti vuoden 2004 aikana erityisesti taloudellisen hyödyn tavoittelu ja haittatoiminnan ammattimaistuminen, mikä toi erittäin suuria haasteita tietoturvahaukilta suojautumiseksi. Näkyvimpinä esimerkkeinä olivat nk. bot-haittaohjelmien aiheuttamat ongelmat, joihin liittyi mm. kansainvälisiin online-toimijoihin, kuten verkossa vedonlyöntitoimintaa harjoittaviin yrityksiin, kohdistunut kiristys sekä tietomurrot.

Merkittävä trendi oli niin ikään haavoittuvuuksien lisääntynyt hyväksikäyttö ennen korjaustiedoston ilmestymistä. Sama suuntaus jatkuu todennäköisesti myös tulevaisuudessa. Viimeisellä vuosineljänneksellä Microsoft Internet Explorer -selainohjelman sekä PHP-ohjelmointikieleen liittyviä haavoittuvuuksia käytettiin runsaasti hyväksi. Viimeisellä vuosineljänneksellä julkaistiin myös matkapuhelimille kohdistetun Cabir-haittaohjelman lähdekoodi. Matkapuhelimiin kohdistuvat haittaohjelmahuikat todennäköisesti lisääntyvät kuluvana vuonna.

Kansainvälisesti, tosin ei Suomessa, vuoden 2004 merkittävimpiä ilmiöitä oli ns. phishing-toiminta, jolla pyritään hankkimaan taloudellisesti hyödynnettävissä olevaa tietoa.

Haittaohjelmat

Alkuvuoden 2004 virustilastoja synkensivät ns. virussodassa mukana olleet sähköpostimadot. Bagle-, Mydoom- sekä Netsky-viruksista ilmestyi alkuvuoden aikana lukuisia eri variaatioita, joiden tarkoituksena oli paitsi saastuttaa kohdejärjestelmä, usein myös poistaa järjestelmästä muut haittaohjelmat. Eri haittaohjelmien tekijät lähettivät toisilleen myös viestejä haittaohjelmakoodin välityksellä. Kilpailu roskapostin lähetyskanavista johti haittaohjelmien tekijöiden ja roskapostittajien väliseen virussotaan.

Witty-verkkomato aloitti leviämisensä maaliskuun loppupuolella. Se käytti hyväkseen ISS:n tietoturva-tuotteista löydettyä haavoittuvuutta vain päivän haavoittuvuuden julkaisemisen jälkeen. Leviäminen oli erittäin nopeaa ja maantieteellisesti laajamittaista, vaikka ISS:n ohjelmistot eivät kuulu yleisimmin käytettyihin ohjelmistoihin. Madon levittämisessä käytettiin ensimmäistä kertaa pelättyä kohdelista-tekniikkaa. Kohdelista sisältää ennalta etsittyjä haavoittuvia järjestelmiä, jotka mato saastuttaa maksimoidakseen alkuvaiheen leviämisenopeuden.

Toukokuussa 2004 liikkeelle lähtenyt Sasser-verkkomato levisi laajamittaisesti ja aiheutti merkittäviä ongelmia myös suomalaisissa yrityksissä ja muissa organisaatioissa. Sasser-mato levisi käyttäen hyväkseen kaksi viikkoa aikaisemmin julkaistua Windows-käyttöjärjestelmän LSASS-haavoittuvuutta. Useimmat organisaatioiden sisäverkoissa havaitut Sasser-matoepidemioiden olivat seurausta saastuneen kannettavan tietokoneen kytkemisestä sisäverkkoon.

Koko vuotta 2004 leimasi erityisen voimakkaasti ns. bot-haittaohjelmien esiintyminen tuhansine eri variaatioineen. Merkittävimmät bot-haittaohjelmat olivat Sdbot- sekä Phabot-haittaohjelmien eri variantit. Bot-haittaohjelmien ominaisuudet kehittyivät vuoden aikana erittäin monipuolisiksi. Saastuneista tietojärjestelmistä muodostui usein tuhansia tietojärjestelmiä sisältäviä bot-verkkoja, joita hyökkääjä hallitsi IRC-kanavan välityksellä. Bot-haittaohjelmien levittämisen tehokkuutta selitti osittain haittaohjelmien tekijöiden halu varmistaa, etteivät virustorjuntaohjelmistot tunnista uutta liikkeelle lähetettävää varianttia. Bot-haittaohjelmat aloittivat usein uuden haavoittuvuuden hyväksikäytön erittäin nopeasti haavoittuvuuden julkaisemisen jälkeen. Bot-haittaohjelmien uusien varianttien nopea ilmestymissykli aiheutti suuria haasteita perinteisen virustorjuntaohjelmiston kyvyille havaita niitä.



Roskaposti

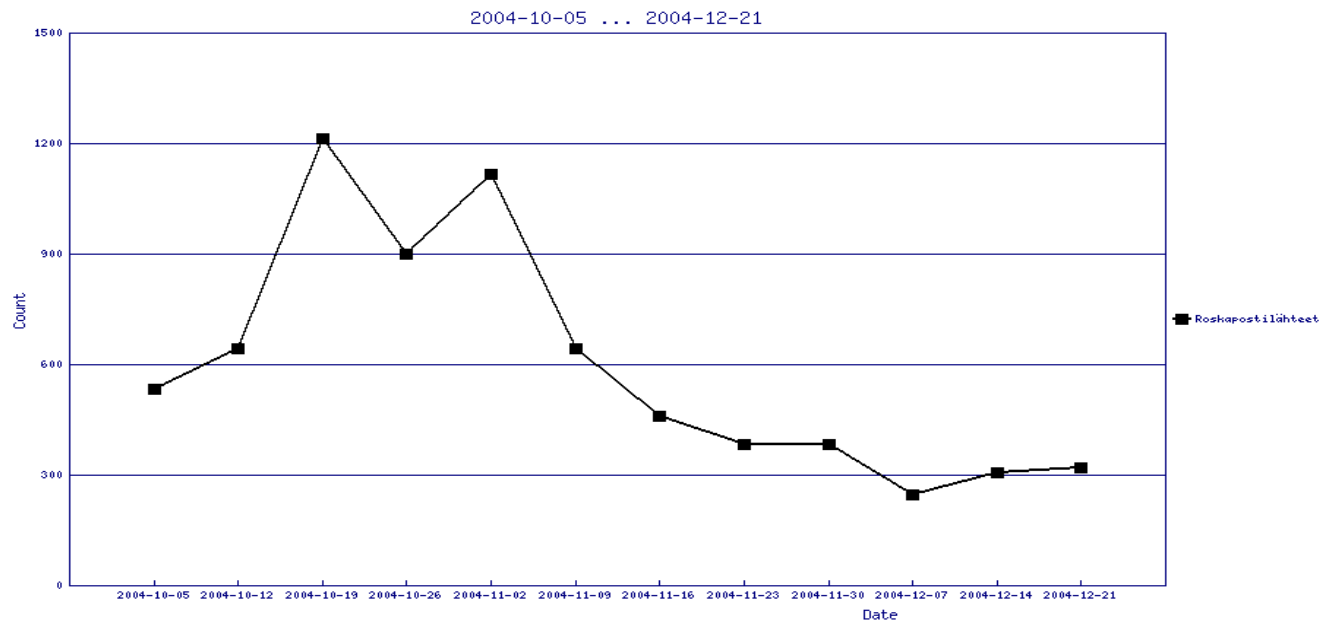
Roskapostin määrä kasvoi edelleen vuoden 2004 aikana, mikä aiheutti lisääntyvää kuormitusta sekä palveluntarjoajien että yritysten ja muiden organisaatioiden sähköpostipalvelimille. CERT-FI:n havaintojen mukaan roskapostien suhteellinen määrä oli loppuvuodesta tehdyn seurannan mukaan Suomessa noin 38 prosenttia kaikista sähköpostiviesteistä. Yksittäisten roskapostihuippujen suhteellinen määrä oli kuitenkin pahimmillaan jopa 80 prosenttia kaikista sähköposteista. Roskapostin määrä vaihteli kuitenkin suuresti eri kohdeorganisaatioiden välillä. Samoin tarkasteluajankohta vaikutti merkittävästi roskapostin suhteelliseen määrään, koska roskapostia lähetetään usein purskeittain.

Kansainväliset vertailut osoittavat suhteellisen roskapostin määrän olleen muualla maailmassa noin 40 - 60 prosenttia kaikista sähköposteista huippulukujen yltäessä jopa lähelle 90 prosenttia.

Ongelmatietojärjestelmien lukumäärä Suomessa

CERT-FI:n tietoon tulleiden bot-haittaohjelmilla haltuunotettujen tietojärjestelmien määrät vaihtelivat vuoden 2004 aikana tarkastelujaksoittain 500 saastuneesta tietojärjestelmästä aina 2000 saastuneeseen tietojärjestelmään. Vuoden viimeisellä vuosineljänneksellä bot-haittaohjelmatartuntoja oli Suomessa vähemmän kuin aiemmin. Saastuneiden tietojärjestelmien määrä jäi alle 500:n.

CERT-FI:n saamien tietojen mukaan Suomessa roskapostilähteinä toimineiden tietojärjestelmien määrän arvioitiin olleen tarkastelujaksoittain keskimäärin noin 500. Enimmillään roskapostien lähteitä oli yli 1000. Roskapostilähteiden määrä laski selvästi viimeisellä vuosineljänneksellä. Viestintävirasto antoi viimeisellä vuosineljänneksellä teleyrityksille määräyksen sähköpostipalveluiden tietoturvasta ja toimivuudesta.



Kuva 1. Roskapostilähteinä toimineet tietojärjestelmät viimeisellä vuosineljänneksellä 2004.



Hyväksikäytetyimmät haavoittuvuudet

Vuoden 2004 aikana hyväksikäytetyimmät ohjelmistohaavoittuvuudet olivat Microsoft Windows -käyttöjärjestelmän LSASS- sekä useat Internet Explorer –selainohjelman haavoittuvuudet. Windows LSASS-haavoittuvuutta käytettiin hyväksi erityisesti eri haittaohjelmien välityksellä. Viimeisellä vuosineljänneksellä käytettiin hyväksi erityisesti Internet Explorer –selainohjelman IFRAME- sekä HTML Help –haavoittuvuuksia. IFRAME-haavoittuvuutta hyödynnettiin murtamalla palvelin, joka jakoi usealle suosituille sivustolle mainosbannereita. Bannereihin sisällytettiin haavoittuvuutta hyödyntävä ohjelmakoodi.

Vuoden 2004 aikana koettiin erityisen paljon SSH-palveluun kohdistuneita hyökkäyksiä, joissa yritettiin arvata kohdejärjestelmän oikeita käyttäjätunnus- ja salasana- ja salasanapareja. Hyökkäys ei kohdistunut varsinaiseen ohjelmistohaavoittuvuuteen.

Vuoden 2004 aikana CERT-FI:n tietoon tuli useita merkittäviä tietomurtojen sarjoja. Tietomurroissa käytetyt työkalut, esimerkiksi menetelmät ohjelmistopalomuurien ohittamiseen, kehittyivät yhä tehokkaammiksi ja vaikeammin havaittaviksi. Viimeisellä vuosineljänneksellä ilmestyi runsaasti myös haavoittuvuuden hyödyntämismenetelmiä, jotka toimivat Microsoft Windows XP Service Pack 2:lla varustetuissa tietojärjestelmissä.

Viimeisellä vuosineljänneksellä nousivat esille Microsoft Windows -käyttöjärjestelmän WINS-haavoittuvuuden sekä PHP-ohjelmointikieleen liittyvien haavoittuvuuksien hyväksikäyttö. WINS-haavoittuvuuden hyväksikäyttö kasvoi selvästi joulukuun alkupuolella sekä aivan vuoden lopussa. PHP-haavoittuvuuksien hyväksikäyttö kohdistui erityisesti haavoittuviin phpBB-ohjelmistoihin.

Tulevaisuuden näkymät

Seuraavalla vuosineljänneksellä bot-haittaohjelmien kehitys tulee jatkumaan. Hyökkääjät pyrkivät suojaamaan bot-verkkojen komentokanavia yhä aggressiivisemmin mm. kohdistamalla palvelunestohyökkäyksiä ulkopuolisia komentokanavalle yrittäviä toimijoita vastaan.

Matkapuhelimiin kohdistetut haittaohjelmat kehittyvät tämän hetken "Proof of Concept" -tasolta. On mahdollista, että tulevaisuudessa havaitaan älypuhelimiin kohdistuvia hyökkäyksiä, joilla voidaan tavoitella myös taloudellista hyötyä.

Phishing-toiminta ja taloudellisen hyödyn tavoittelu lisääntyy alkaneena vuonna. Aasian luonnononnettomuuden kaltaiset, koko maailmaa syvästi järkyttävät tapahtumat, antavat tilaisuuden hyökkääjille huijata ihmisiltä rahaa esimerkiksi www-sivustojen välityksellä tekeytymällä avustusjärjestöiksi.

Organisaatioiden varautumistoimet Internetin uhkia, kuten palvelunestohyökkäyksiä, vastaan korostuvat jatkossa. Varautumistoimet vaativat yhä enemmän aktiivisia toimia ja tilanteiden harjoittelua. IRT (Incident Response Team) -ryhmien merkitys korostuu.

Haavoittuvuuksia käytetään jatkossa hyväksi yhä useammin ennen korjaustiedostojen julkaisemista. Tietoverkkojen tietoturvaohjelmat kohdistuvat myös entistä enemmän kotitietojärjestelmiin. Palomuurin, turvallisen selaimen ja ajantasaisen virustorjunnan käyttö sekä ohjelmistojen päivittäminen, turvalliset asetukset ja oikeat käyttöoikeudet korostuvat myös jatkossa kotitietojärjestelmissä. Windows XP Service Pack 2 tulee todennäköisesti vähentämään onnistuneiden LSASS- sekä RPC-tyyppisten, suoraan verkon kautta hyväksikäytettävien, haavoittuvuuksien hyödyntämistä.