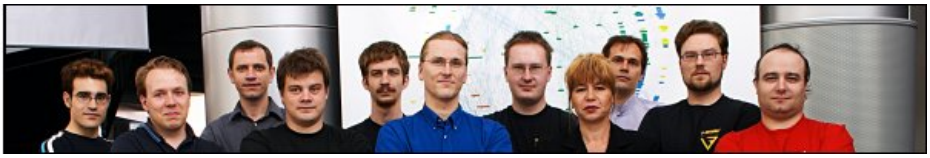
F-SECUREN TIETOTURVAYHTEENVETO

heinäkuu–joulukuu 2005



Vuoden toisella puoliskolla virusten määrän kasvu jatkui hälyttävällä tahdilla. Määrä nousi vuoden loppuun mennessä ennennäkemättömälle tasolle, 110.000 viruksesta 150.000 virukseen. Verkkomatojen avulla tehtyjen massahyökkäysten määrä kuitenkin laski samaan aikaan huomattavasti. Tällaisia hyökkäyksiä ilmeni vain kaksi: syyskuussa havaittiin laajoja tietokatkoja kansainvälisesti aiheuttanut Zotob-mato ja marraskuun lopussa Sober.Y-mato kuormitti sähköpostijärjestelmiä. Aiemmin vuoden aikana otsikoihin oli noussut Zafi.D-mato.

Heinäkuussa 2005 tietoturva-ammattilaiset osallistuivat Las Vegasissa järjestettyyn DEFCON-konferenssiin, joka on suurin koskaan järjestetty "alamaailman" tietokonetapahtuma. Kuten aiempina vuosina, paikalla oli osanottajia tietoturvayhteisön molemmilta puolilta: black-, grey- ja whitehat -hakkereita, tietoturva-alan ammattilaisia, viranomaisia ja salaisia agentteja.

Myös Helsingissä järjestettiin mielenkiintoinen nelipäiväinen Assembly'05 -demotapahtuma, johon osallistui yli 5 000 tietokonenörttiä. Tietoturvalaboratorion asiantuntijat olivat erityisen kiinnostuneita tapahtumasta, koska demojen koodauksessa käytetään perustason kääntäjiin perustuvia tekniikoita ja tiukat tilarajoitukset ratkaistaan kehittyneillä pakkaustekniikoilla.

Vuoden aikana tuomittiin useita haittaohjelmien kirjoittajia eri puolilla maailmaa. Heinäkuussa Venäjällä järjestetyissä ratsioissa pidätettiin kolme parikymppistä miestä. Näiden miesten johtama kiristysrengas oli suunnannut laajoja palvelunestohyökkäyksiä vedonlyöntisivustoihin ja vaatinut tämän jälkeen 50 000 dollaria hyökkäysten lopettamisesta.

Kiristyksen tuotot kierrätettiin Venäjälle Karibian ja Latvian kautta, mutta Iso-Britannian poliisi onnistui seuraamaan rahavirtaa, mikä johti lopulta näihin pidätyksiin. Lain pitkä koura tavoitti myös monia muita virustehtailijoita, kuten Suomessa kiinni saadun VBS/Lasku-viruksen kirjoittajan ja Taiwanissa pidätetyn Peep-takaoviviruksen kirjoittajan. Ehkä kaikkein kuuluisin tapahtuma oli Sasser- ja Netsky-madot luoneen Sven Janschenin kiinniottaminen ja tuomitseminen ehdolliseen vankeuteen ja 30 tunnin yhteiskuntapalvelukseen miljoonien dollarien vahingot aiheuttaneen madon luomisesta.

Roskaposti on haitaksi terveydelle

Joskus haittaohjelmien ja roskapostin pysäyttämisessä saatetaan turvautua äärimmäisiin keinoihin. Heinäkuussa venäläiset tiedotusvälineet kertoivat American Language Center -yrityksen omistajan, Vardan Kushnirin kuolemasta. Tiedotusvälineiden mukaan Moskovan asunnostaan kuolleena löydetty Kushnir oli menehtynyt päähän kohdistuneen iskun seurauksena. American Language Center järjestää venäläisille suunnattuja englanninkielen kursseja ja on vastuussa Venäjän suurimmasta roskapostikampanjasta.

Kampanjan yhteydessä yritys lähetti roskapostia yli 20 miljoonaan venäläiseen sähköpostiosoitteeseen. Kampanja oli niin mittava, että on lähes mahdotonta löytää venäläistä, joka ei olisi saanut American Language Center -yritystä mainostavaa

sähköpostiviestiä. Kushnirin kuolema ei välttämättä liity hänen yrityksensä roskapostikampanjaan, vaikka moni kampanjan uhreista lienee toivonut Kushnirin kiinnijäämistä. Venäjän viranomaiset tutkivat rikosta parhaillaan. Epäiltyjen määrä lasketaan tuhansissa.

Verkkohuijaus kannattaa

Financial Times -lehden saksalainen painos kertoi heinäkuussa, että saksalaiset pankit menettivät phishing-tyylisten verkkohuijausten seurauksena viime vuonna 70 miljoonaa euroa ja että tämä luku kasvaa nopeasti. Mikäli tappiot ovat näin mittavat yhdessä maassa, voimme päätellä, että verkkohuijaukset ovat merkittävä ja erittäin tuottava tulonlähde rikollispiireille.

Onneksi verkkohuijausten yleistyminen on myös tarjonnut viranomaisille uusia keinoja niiden havaitsemiseen. Tämän kehityksen seurauksena perinteisesti suuryritysten, kuten on Citibankin, eBayn, Paypalin ja US Bankhaven, asiakkaisiin keskittyneet hyökkäykset ovat vaihtumassa hyökkäyksiksi pienempien kohteiden asiakkaisiin, jotka eivät ehkä ole vielä tottuneet verkkohuijausviesteihin.

Tällaisten hyökkäysten kohteeksi ovat joutuneet muun muassa saksalaiset pankit ja niistä varsinkin Deutsche Bank ja Postbank. Hyökkäysten seurauksena sekä Deutsche Bank että Postbank ottavat käyttöön kertakäyttöiset salasanat, joilla varmistetaan online-tapahtumien oikeellisuus.

Todisteiden perusteella näyttäisi siltä, että verkkohuijausten takana olevat rikollisorganisaatiot siirtyvät maantieteelliseltä alueelta toiselle uusia kohteita etsiessään. Ensimmäiset hyökkäykset ilmenivät Yhdysvalloissa, josta ne siirtyivät Australiaan ja Iso-Britanniaan. Saksassa verkkohuijausviestit oli käännetty saksaksi, aivan kuten aiemmin 2005 Tanskassa havaitut viestit käännetty tanskaksi.

Hyökkäysten leviäminen muihin Pohjoismaihin ei kestänyt kauaa, sillä Ruotsin Nordea joutui laajan verkkohuijausyrityksen kohteeksi elokuussa. Nordea on Pohjoismaiden suurin pankki, jonka Internet-pankki on yksi maailman suurimmista (neljä miljoonaa Internet-asiakasta kahdeksassa maassa).

Verkkohuijauksen organisoija lähetti suuren määrän tekaistuja sähköpostiviestejä, joissa oli linkki väärennettyyn kopioon pankin Internet-sivuista. Viestit oli käännetty ruotsiksi, mutta tällä kertaa hyökkäyksessä pyrittiin rikkomaan myös Nordean kertakäyttöisten salasanojen järjestelmä.

Ruotsin Nordea jakaa asiakkailleen salasanalistat, jossa käytettävä vahvistuskoodi raaputetaan esille erikseen kullakin käyttökerralla. Tällaiseen mekanismiin perustuvan sivuston suojauksen murtaminen on paljon haastavampaa kuin esimerkiksi Saksassa käytetyn järjestelmän, jossa pankin asiakkaat käyttivät aina samaa käyttäjätunnusta ja nelinumeroista pin-koodia.

Valesähköpostissa kerrottiin, että Nordea oli ottamassa käyttöön uusia tietoturvamenetelmiä, jotka olivat käytössä sivuilla www.nordea-se.com ja www.nordea-bank.net (molemmat Etelä-Koreassa sijaitsevia valesivustoja). Nämä valesivustot olivat hämäävän aidonnäköisiä, ja niillä pyydettiin käyttäjää antamaan käyttäjätunnuksensa, tunnuslukunsa ja seuraava raaputettava vahvistuskoodi. Aina kun vahvistuskoodi annettiin, sivusto ilmoitti koodiin liittyvästä virheestä ja pyysi antamaan seuraavan vahvistuskoodin. Näin verkkohuijarit yrittivät saada selville peräkkäiset vahvistuskoodit omaan käyttöönsä.

Ruotsin Nordea ei aliarvioinut uhkaa, vaan sulki koko Internet-pankkinsa siksi aikaa, että huijausyritys saatiin tutkittua ja pysäytettyä. Näin toimittiin, jotta huijarit eivät pystyisi käyttämään selville saamiaan koodeja rahan siirtämiseen.

Syyskuuhun mennessä verkkohuijausyritysten määrä tasaantui mutta samaan aikaan roskapostin määrä kasvoi. Suurin osa roskapostiliikenteen kasvusta näytti johtuvan seuranhakupalvelujen roskapostista. Yksikin aktiivinen roskapostin lähettäjä näyttäisi siis voivan vaikuttavan sähköpostin määrään merkittävästi.

Huijarit hyödyntävät kirjoitusvirheitä

Alkuvuonna havaittiin todisteita kirjoitusvirheitä hyödyntävistä huijareista. Käyttäjät, jotka kirjoittivat Google-hakukoneen osoitteen väärin muotoon "googkle", johdatettiin Googlen sijasta mitä erilaisimmille haittaohjelmia sisältäville sivustoille. Syksyllä havaittiin vielä laajempi samaan menetelmään perustuva hyödyntämisyritys, mikä sinänsä ei ollut yllätys, mutta luotujen osoitteiden määrä, 150, oli vaikuttava. Monet näistä muistuttivat tietoturvayhtiöiden osoitteita.

Havaittuja kirjoitusvirheitä hyödyttäviä osoitteita ovat muun muassa "www-f-secure.com" ja "wwwf-secure.com", jotka tällä hetkellä siirtävät käyttäjän Web-sivustoon "nortpnantivirus.com". Onneksi tätä sivustoa ei ainakaan tällä hetkellä käytetä verkkohuijaukseen tai troijalaisten lataamiseen. Muita tietoturvayritysten verkko-osoitteiden väärinkirjoittamiseen liittyviä osoitekopioita ovat muun muassa f-secue.com, mesagelabs.com, mcafeeantiviru.com, bitdefneder.com, pestpatorl.com, wwwbullguard.com, pandafirewall.com, sendamil.org ja centralcomand.com.

Terroristihyökkäysten ja luonnonkatastrofien hyödyntäminen

Luonnonkatastrofien ja terroristihyökkäysten suuri määrä synnytti merkittävän ja valitettavan ilmiön, jossa haittaohjelmien kehittäjäyhteisö pyrkii hyödyntämään muiden ihmisten kärsimystä.

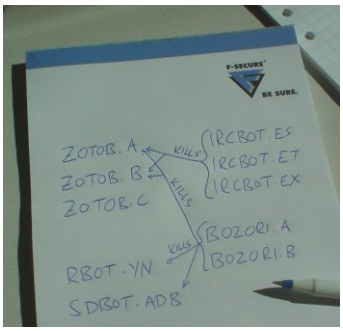
Pian 11.9.2001 tehtyjen New Yorkin World Trade Center -iskujen jälkeen havaittiin haittaohjelmia, jotka yrittivät saada käyttäjiä avaamaan iskuihin liittyviä haitallisia sähköpostiliitteitä. Vain kaksi viikkoa syyskuun iskujen jälkeen havaittiin sähköpostimato W32/Vote.A@mm ja tasan vuosi iskujen jälkeen toinen sähköpostimato W32/Chet@mm. Vote.A-mato ei levinnyt laajalti toisin kuin Chet-mato, josta annettiin tason 2 F-Secure Radar -varoitus.

Sama kaava toistui tämän vuoden heinäkuussa Lontoon maanalaiseen kohdistuneen terroristi-iskun jälkeen. Ensimmäinen troijalainen havaittiin sähköpostiviesteissä pian pommi-iskun jälkeen. Viesteissä oli liitteenä iskuun liittyvään videoleikkeeseen viittaava ZIP-tiedosto "London Terror Moovie.avi <124 spaces> Checked By Norton Antivirus.exe". F-Secure havaitsi tämän Troijan hevoseksi SpamTool.Win32.Delf.h ja lähetti virustunnistepäivityksen pikaisesti.

Syyskuussa ilmoitettiin roskapostiviesteistä, joiden otsikoissa viitattiin hirmumyrsky Katrinan aiheuttamiin tuhoihin. Varsinainen viesti vaikutti Katrinaa käsittelevältä uutisartikkelilta, mutta todellisuudessa viesti ohjasi lukijan nextermest.com -sivustoon. Lisätutkimuksissa tämä sivusto paljastui peitesivustoksi, joka päivittyessään siirtää käyttäjän sivulle, joka yrittää ladata troijalaisen Trojan-Downloader.JS.Small.bq malware.

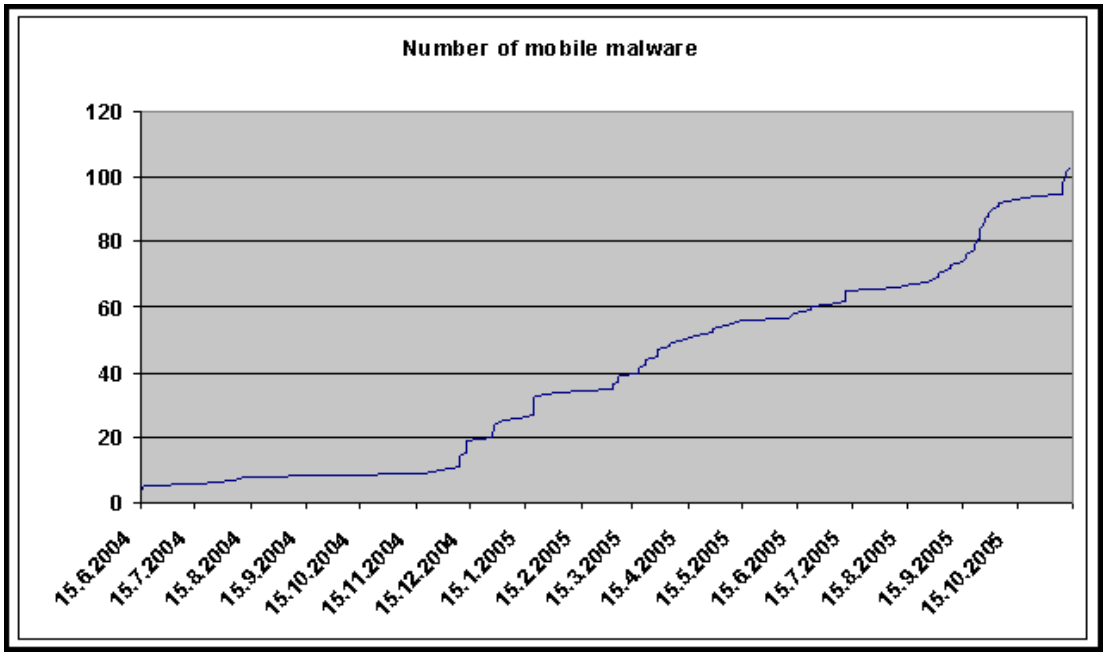
Elokuussa huomattavia virusepidemioita

Elokuussa F-Securen tietoturvalaboratorion Helsingin pääyksikössä seurattiin bot-matojen kamppailua, joka kasvoi kansainväliseksi virusepidemiaksi, ennen kuin se saatiin pysäytettyä. Kaikki alkoi lounasaikaan havaitusta Microsoft-tietoturvapäivitykseen MS05-039 liittyvää PnP-tietoturva-aukkoa hyödyntävästä viruksesta. Virus iski levitessään CNN-uutistoimistoon, Financial Timesiin, The New York Timesiin ja ABC-televisioyhtiöön.



Zotob-virukseen perustuvaa hyökkäystä tuettiin bot-matojen erilaisilla versioilla tehdyillä hyökkäyksillä. Mielenkiintoista tässä oli se, että nämä bot-matojen eri versiot kilpailivat virustartunnan saaneista tietokoneista ja korvasivat toisiaan omilla versioillaan. Keskenään kamppailevia matoja oli kaksi ryhmää: IRCBot- ja Bozori-madot vastaan Zotob-madot ja muut bot-madot. Tämä virusepidemia saatiin lopulta aisoihin, mutta varsinkin mediayrityksissä laajalle levinneestä häiriöstä uutisoitiin F-Securen seurannan mukaan yli 500:ssa eri lehdessä seuraavina päivinä. Pian virusepidemian jälkeen tehtiin kaksi Zotob-PnP-matoon liittyvää pidätystä. Marokossa viranomaiset ottivat kiinni viruspiireissä Diabl0-nimellä tunnetun Farid Essebarin ja Turkissa pidätettiin Coderina tunnettu Atilla Ekici. Epäillyt ovat 18- ja 21-vuotiaita.

Mobiililaitteiden haittaohjelmat lisääntyivät räjähdysmäisesti



Kiinnostus mobiililaitteiden haittaohjelmia kohtaan kasvaa tiedotusvälineiden aiheeseen liittyvän uutisoinnin lisääntyessä. F-Secure saa jatkuvasti yhä enemmän tiedusteluja mobiiliviruksista. Tätä artikkelia kirjoitettaessa haittaohjelmia on jo yli 100.

Suurin osa mobiililaitteiden haittaohjelmista on Symbian-päätelaitteille suunnattuja. Mielenkiinto Symbian-ympäristöä kohtaan on osoitus Symbian-laitteiden suosiosta, sillä haittaohjelmien kirjoittajia kiinnostaa juuri laaja käyttäjäkunta.

Kaikki tunnetut Symbian-ympäristön troijalaiset ja madot näyttävät useita varoituksia jo niiden asennuksen aikana, joten haittaohjelmatartunnat olisi helppo panna käyttäjien osaamattomuuden ja välinpitämättömyyden piikkiin. Tavat, joilla Cabir-mato ja muut Bluetooth-madot leviävät, osoittaa kuitenkin, että syyt eivät ole näin yksiselitteiset.

Ensinnäkin suuri osa Symbian-ohjelmista edellyttää Bluetooth-yhteyttä toimiakseen kunnolla. Osa näistä ohjelmista kytkee Bluetooth-yhteyden päälle varmistamatta sitä käyttäjältä tai näyttää yhteyden aktivointipyynnön sellaisessa muodossa, että käyttäjä todennäköisesti hyväksyy pyynnön. Lisäksi on olemassa lukuisia Bluetooth-yhteyttä hyödyntäviä yhteisöllisiä verkkosovelluksia, kuten YOU-WHO ja CrowdSurfer. Koska Bluetooth-tekniikkaa käytetään sosiaalisessa verkostoitumisessa ja pelaamisessa, monien henkilöiden kynnys hyväksyä tuntemattomilta henkilöiltä lähtöisin olevia yhteyksiä ja tiedostoja on alentunut merkittävästi.

Monet Cabir-variantit leviävät melko nopeasti ja lähettävät Bluetooth-yhteyspyyntöjä toistuvasti, vaikka käyttäjä hylkäisi ne. Tämän seurauksena monet käyttäjät turhautuvat ja vastaavat kaikkiin pyyntöihin myöntävästi päästäen madon valloilleen.

Commwarrior-viruksen leviäminen jatkuu

Tietyt virukset jatkavat yhä leviämistään esteettömästi, pahamaineisimpana esimerkkinä Commwarrior, joka on nyt havaittu 20 maassa Intiasta Etelä-Afrikkaan.

Elokuussa F-Securelle lähetettiin näyte uudesta Symbian-ympäristön troijalaisesta Doomboot.A:sta, joka asentaa Commwarrior.B -viruksen ja vahingoittaa puhelinta niin, ettei sitä voi enää käynnistää. Monet aiemmat troijalaiset ovat asentaneet erilaisia Cabir-viruksen versioita, mutta Doomboot.A on ensimmäinen tunnettu troijalainen, joka asentaa Commwarrior-viruksen ja hajottaa puhelimen uuden tekniikan avulla.

Kuten useimmat Symbian-ympäristön troijalaiset, Doomboot.A on naamioitu Symbian-pelin piraattikopioksi. Käyttäjät, jotka eivät lataa ja asenna pelien piraattikopioita, ovat siis turvassa tältä uhalta.

Doombootin huolestuttava piirre on se, miten siinä on yhdistetty Doomboot- ja Commwarrior-haittaohjelmien haittavaikutukset puhelimelle. Doomboot.A estää puhelimen käynnistämisen ja Commwarrior synnyttää niin paljon Bluetooth-liikennettä, että puhelimen akku kuluu loppuun alle tunnissa. Jos Doomboot.A iskee käyttäjän puhelimeen, hänellä on alle tunti aikaa selvittää, mitä on tapahtumassa ja puhdistaa puhelin, mikäli hän haluaa välttää tietojen häviämisen.

Syyskuussa havaittiin ominaispiirteiltään tyypillisen oloinen Symbian-ympäristön troijalainen SymbOS/Cardtrap.A, joka avasi uuden oven mobiililaitteiden haittaohjelmissa. Tämä troijalainen voi näet tartuttaa myös tietokoneen, kun käyttäjä liittää puhelimen muistikortin tietokoneeseen.

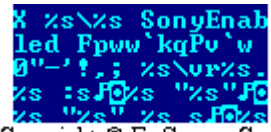
Kun Cardtrap.A tartuttaa Symbian-puhelimen, se kopioi puhelimen muistikortille Win32/Padobot.Z- ja Win32/Rays-madot. Padobot.Z-madon mukana kopioidaan autorun.inf-tiedosto, jonka avulla mato yritetään suorittaa automaattisesti, kun muistikortti liitetään Windows-tietokoneeseen. Rays-mato kopioidaan tiedostonimellä SYSTEM.EXE, ja sen kuvakkeena käytetään Windowsin järjestelmäkansion kuvaketta. Tällä pyritään siihen, että käyttäjä napsauttaisi Rays-madon käynnistystiedostoa järjestelmäkansion sijasta. F-Secure Anti-Virus kuitenkin havaitsee sekä Padobot.Z- että Rays-madon, ja näiden matojen tunnistus- ja puhdistustiedot on lisätty myös F-Secure Mobile Anti-Virus -ohjelmaan.

Virukset levisivät MP3-soittimiin ja pelikonsoleihin

Elokuun lopussa ilmoitettiin, että yleisesti myytävän MP3-soittimen mukana toimitettiin virus. Creative ilmoitti toimittaneensa vahingossa lähes 4 000 MP3-soitinta, jotka sisälsivät Windows-viruksen. Tämä tapahtui Japanissa uusille viiden gigatavun Zen Neeons -soittimille. Soittimien tiedostojärjestelmässä on tiedosto, joka sisältää sähköpostimadon Wullik.B (tunnetaan myös nimellä Rays.A). Onneksi mato tartuttaa tietokoneen vain, jos käyttäjä selaa soittimen tiedostoja tietokoneella ja kaksoisnapsauttaa tartunnan saanutta tiedostoa.

Lokakuussa ilmoitettiin Sonyn Playstationin haittaohjelmasta. Se paljastui laiteohjelmiston päivitystyökaluksi naamioiduksi troijalainen, joka teki PSP-käsikonsolista käyttökelvottoman. Tämä PSP Team -ryhmän päivitysohjelma poistaa laitteen flash-muistista tärkeitä järjestelmätiedostoja ja estää näin järjestelmän käynnistämisen. Monet tahot ovat uutisoineet tästä ohjelmasta ensimmäisenä PSP-viruksena.

F-Securen määritysten mukaan ohjelma voidaan kuitenkin luokitellaan korkeintaan troijalaiseksi, koska se ei pysty kopioimaan itse itseään. Mielenkiintoisena yksityiskohtana todettakoon, että Sonyn mukaan luvattoman koodin suorittaminen PSP-käsikonsolissa kumoaa laitteen takuun välittömästi. Heti ensimmäisen PSP-konsolin troijalaisen jälkeen tietoturvalaboratorio sai tiedon ensimmäisestä troijalaisesta Nintendon kannettavassa DS-käsikonsolissa. Tämä DSBrick-nimellä tunnettu yksinkertainen troijalainen kirjoittaa tärkeiden muistialueiden päälle ja estää näin konsolin käynnistämisen.



Sony palasi parrasvaloihin uudelleen marraskuussa, kun Sony BMG:n CD-musiikkilevyissä havaittiin rootkit-tiedosto, jonka yhtiö oli itse sijoittanut CD-äänilevyihin osana niiden kopiosuojausta. Rootkit-tekniikan avulla voidaan valvoa asiakkaan toimintaa hyödyntämällä Digital Rights Management -ohjelmistoa, joka asennetaan, kun käyttäjä asettaa CD-levyn Windows-tietokoneeseen ja hyväksyy lisenssisopimuksen. Käyttäjän tietämättä ohjelmiston mukana asennetaan myös rootkit-tiedosto, jonka asennusta ei voi poistaa millään keinolla. Rootkit-järjestelmä avaa lisäksi takaoven viruksille (ja muille haittaohjelmille), jotka voivat kyseisen järjestelmän avulla piilottaa itsensä. Hyvä uutinen on se, että F-Securen maaliskuussa julkaistu BlackLight-tarkistusohjelma havaitsee sekä Sony DRM -rootkit-järjestelmän että sen avulla piilotetut haittaohjelmat.

F-Securen toimitusjohtaja Risto Siilasmaa totesi Sonyn tapauksesta seuraavaa: "Todellinen uutinen ja arvokas opetus tässä tapauksessa on se, että monet yritykset yhdistävät tuotteisiinsa ICT-tekniikkaa. Tämän johdosta niiden on myös perehdyttävä tietoturva-asioihin, luotava prosessit

vastuuvahinkovaateita varten, koulutettava PR-henkilönsä selviytymään tällaisista tilanteista ja niin edelleen. Sadat kuluttajatekniikkaa myyvät elektroniikkayritykset ovat samassa veneessä Sonyn kanssa."

Marraskuun lopulla F-Secure antoi lisäksi korkeimman tason Radar-hälytyksen uudesta Sober-versiosta, joka oli vuoden suurin sähköpostimatohyökkäys. Se saastutti Internet-operaattoreiden mukaan useita miljoonia sähköpostiviestejä. Sähköpostiviesteissä oli valeviestejä, joiden lähettäjiksi mainittiin FBI:n ja CIA:n kaltaisia tahoja ja joissa pyydettiin viestin vastaanottajaa avaamaan viestissä oleva liite. Tämä liite sisälsi version Sober-madosta.

Ensimmäinen Sober-madon versio havaittiin yli kaksi vuotta sitten lokakuussa 2003. F-Secure uskoo, että kaikki tämän jälkeen havaitut madon 25 versiota on kirjoittanut sama henkilö, joka toimii jossakin päin Saksaa. Tämä virustehtailija näyttäisi kuuluvan virusohjelmien kirjoittajien vanhaan sukupolveen, jota ei motivoi taloudellinen hyöty vaan maine.

Onnistuneita tuotejulkaisuja ja laajentuminen ohjelmistosta laitteistoon

Kesäkuussa F-Secure julkaisi F-Secure Client Security 6.0 -ohjelmiston ja sen arvosteluja alettiin saada heti kesälomakauden jälkeen. F-Securelle näistä merkittävin oli Infoworldin syyskuussa julkaistu laaja virustorjuntaohjelmien arvostelu, jossa F-Secure ja F-Secure Anti-Virus Client Security 6.0 asetettiin tärkeimpien kilpailijoidensa edelle.

Lehdessä todettiin seuraavasti: "Valmistajat tarjoavat vaihtelevaa tukea reaaliaikaiselle suojaukselle. McAfeen, Trend Micron ja Tenebrilin versiot sallivat haittaohjelmien asentamisen, mutta estävät niiden suorittamisen. Haittaohjelmat pysyvät siis asennettuina, kunnes suoritetaan poistotarkistus. Muut tuotteet estävät useimpien mutta eivät kaikkien haittaohjelmien asennuksen (esimerkiksi Sunbelt CounterSpy) ja poistavat haittaohjelmien jäänteet seuraavan tarkistuksen yhteydessä (esimerkiksi Trend Micro). Parhaiten asennusten estämisestä suoriutui F-Secure, joka esti kaikkien vakoilu- ja haittaohjelmien hyökkäykset."

F-Secure julkisti kuluttajille suunnatun lippulaivatuotteensa F-Secure Internet Security 2006:n syyskuussa. Tuotteen uusimmassa versiossa on monia uusia toimintoja, jotka varmasti tuottavat positiivisia arvioita vielä myöhemmin tänä vuonna.

Lisäksi F-Secure lanseerasi syyskuussa merkittävän sähköpostin suojaukseen tarkoitetun F-Secure Messaging Security Gateway™ -ratkaisun.

Laite sijoitetaan sähköpostipalvelimen viereen ja se suodattaa roskapostin ja virukset sähköpostiliikenteestä automaattisesti. Laite on valmistettu yhteistyössä yhdysvaltalaisen Proofpointin kanssa. Ensiarviot tuotteesta ovat olleet positiivisia.