Lehdistötiedote

F-Secure Oyj
PL 24
FIN-02231 ESPOO
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
http://www.F-Secure.com

JULKAISTAVISSA 14.2 2000

Kournikova-viruksen tekijän ottelu ohi

F-Securen yhteistyökumppani löysi Kournikova-viruksen tekijän

Espoo, 14. helmikuuta 2001, F-Secure Oyj [HEX: FSC], joka on johtava keskitetysti hallittavien tietoturvajärjestelmien kehittäjä mobiileja, hajautettuja yritysjärjestelmiä varten, ilmoittaa, että sen ruotsalainen yhteistyökumppani, Atremo AB, on saanut selville Kournikova-viruksen tekijän. Atremo luovutti nimen FBI:lle, joka totesi tiedon olevan oikean ja asianmukaisesti tutkittua. Atremo ja F-Secure päättivät kertoa asiasta yleisölle, jotta se olisi paremmin tietoinen tällaisen toiminnan vastuuttomuudesta.

Atremo löysi tekijän internetin keskusteluryhmien, web-foorumeiden ja kotisivujen kautta. Tekijä oli käyttänyt useita valenimiä ja sähköpostiosoitteita. Hän oli myös käyttänyt varsin epätavallista tervehdystapaa, mikä teki jälkien seurannan helpoksi Atremolle.

Tekijä siteerasi IDC:n tutkimusta, jossa todettiin, että "verkossa surffaavat ihmiset eivät ottaneet opikseen I Love You -viruksesta."

"Tämä voi osittain olla totta", totesi F-Securen toimitusjohtaja Risto Siilasmaa, "mutta huonoa suojausta ei tarvitse todistaa käyttäjien kimppuun hyökkäämällä. Eri puolilla maailmaa olevien sivustojen toimintaa haitattiin suurilla sähköpostimäärillä. Jotkut niistä saivat tuhansia turhia sanomia. Tämän vastuuttoman toiminnan vuoksi monet sähköpostipalvelimet kaatuivat, mikä laski tuottavuutta, hidasti asiakaspalvelua ja aiheutti muita vielä määrittelemättömiä ongelmia."

Tekijä yritti puolustella pilaansa ja väitti, että hänen tarkoituksensa ei ollut vahingoittaa sivustoa [jolta virus lähti] eikä hän pyrkinyt aiheuttamaan harmia ihmisille. Mutta hän lisäsi myös, että se oli käyttäjien oma vika, että heidän järjestelmänsä saastui tällä Anna Kournikova -viruksella, tai OnTheFly -viruksella tai miksi sitä sitten halutaankin kutsua.

Risto Siilasmaa tuomitsee tämän asenteen piittaamattomaksi, mutta toteaa myös, että tulokset osoittavat, että monet käyttäjät ovat jättäneet aiemmat vakavat varoitukset huomiotta. Monilla ei edelleenkään ole toimiviksi todettuja ja helposti saatavia

virustentorjuntaohjelmia koneissaan, tai he eivät ole kytkeneet Visual Basic Scripting -toimintoa pois päältä, mikä olisi yksinkertaisin tapa estää virustartunnat.

"Virusten aiheuttama vaara on suorassa suhteessa vallalla olevaan välinpitämättömyyteen", hän lisäsi.

Viime vuoden lopulla F-Secure laati luettelon suosituksista, jotka F-Secure on sijoittanut web-sivustolleen osoitteeseen: http://www.F-Secure.com/news/2000/news_2000112100.shtml.

Viisi tärkeintä kohtaa ovat seuraavat:

1. Asenna kunnollinen virustentorjuntaohjelma ja varmista, että se päivitetään päivittäin joko automaattisesti (kuten F-Securen tuotteet) tai manuaalisesti.

2. Useimmat madot, jotka käyttävät leviämiseen sähköpostia, hyödyntävät tässä Microsoft Outlook- tai Outlook Express -ohjelmaa. Jos käytössäsi on Outlook, hae Microsoftin sivuilta uusin Outlookin turvapäivitys ja asenna se. Yleisohje on, että käyttöjärjestelmä ja sovellukset kannattaa pitää mahdollisimman hyvin ajan tasalla asentamalla uusimmat korjauspäivitykset aina sitä mukaa kuin ne tulevat saataville. Turvallisinta on hakea nämä päivitykset suoraan ohjelman toimittajalta.

3. Määritä Windowsin asetukset niin, että tiedostotunnisteet tulevat aina näkyviin. Windows 2000:ssa tämä tehdään Resurssienhallinnan Työkalut-valikosta: Valitse ensin Työkalut/Kansion asetukset/Näytä ja poista sitten valintamerkki kohdasta "Älä näytä oikein rekisteröityjen tiedostojen tiedostotunnistetta". Näin vahingollisten tiedostojen (kuten EXE tai VBS) naamioiminen harmittomiksi tiedostoiksi (esimerkiksi TXT tai JPG) on vaikeampaa.

4. Älä avaa sellaisia tiedostoliitteitä, joiden tunnisteena on VBS, SHS tai PIF. Tällaisia tiedostoja ei yleensä koskaan käytetä normaaleina liitteinä, mutta virukset ja madot hyödyntävät niitä usein.

5. Kytke Visual Basic Scripting pois käytöstä - useimmat käyttäjät eivät tarvitse sitä, ja se on keino, jolla madot ja virukset pääsevät järjestelmään. Linkki, jossa kerrotaan VBScriptingin päältä kytkemisestä, löytyy F-Securen sivustolta, http://www.f-secure.com/virus-info/.

F-Secure Oyj

F-Secure Oyj on suomalainen yritys, joka toimittaa hajautettuja, keskitetysti hallittavia tietoturvaratkaisuja. F-Securen tuotevalikoima sisältää palkittuja, keskitetysti hallittuja virustentorjunta-, tiedosto- ja verkkosalaus- sekä hajautettuja palomuurituotteita yritysten kaikille keskeisille laitealustoille työasemista verkkolaitteisiin ja palvelimista langattomiin taskutietokoneisiin.

F-Securen tuotteet sopivat tietoturvan toimittamiseen myös palveluna (Security as a Service, SaaS). Palvelu tarjoaa luotettavan, aina toimivan ja ajanmukaisen tietoturvan hajautetulle käyttäjäkunnalle. F-Securen tuotteet ja ratkaisut voidaan toimittaa asiakkaiden omien IT-osastojen tai palveluntarjoajien kautta. Ratkaisujen avulla turvakäytäntöpohjainen tietoturva ja tarvittavat hälytykset saadaan kaikkiin laitteisiin, joilla tietoa luodaan ja tallennetaan tai joilta tietoa haetaan. Vuonna 1988 perustettu F-Secure Oyj on noteerattu Helsingin pörssissä. Yhtiön pääkonttori on Espoossa ja Pohjois-Amerikan pääkonttori San Josessa. Yhtiöllä on lisäksi toimistoja eri puolilla maailmaa.

Lisätietoja:

Mikael Albrecht, Product Manager
F-Secure Oyj
Pl 24
02231 Espoo

Tel. +358 9 2520 5640
Fax +358 9 2520 5001
Gsm 040 550 9349
E-mail: Mikael.Albrecht@F-Secure.com

http://www.F-Secure.com