Lehdistötiedote

F-Secure Oyj
PL 24
02231 ESPOO
Tel. +358 9 859 900
Fax. +358 9 8599 0599
http://www.F-Secure.com

JULKAISTAVISSA HETI

F-Secure varoittaa uudesta "rakkauskirje"-viruksesta

VBS/LoveLetter saattaa olla jopa vaarallisempi kuin Melissa

Suomalainen tietoturvatoimittaja F-Secure Oyj varoittaa uudesta vaarallisesta VBS/LoveLetter -nimisestä virusmadosta. Virus leviää sähköpostin välityksellä LOVE-LETTER-FOR-YOU.TXT.vbs -nimisenä liitetiedostona. F-Secure Anti-Virus -ohjelmiston uusin päivitys (imuroitavissa osoitteesta www.F-Secure.com) löytää ja tuhoaa viruksen.

"Virus leviää hämmästyttävän nopeasti", tutkimuspäällikkö Mikko Hyppönen F-Securesta kertoo. "Saimme ensimmäiset havainnot Norjasta torstaina yhdeksän aikaan aamulla. Yhden aikaan iltapäivällä havaintoja oli kirjattu jo 20 maasta. Tartunnan saaneiden koneiden lukumäärä on todennäköisesti jo kymmeniä tuhansia. Epidemia saattaa olla sekä nopeudella että vahingollisuudella mitattuna pahempi kuin Melissa."

Aktivoituessaan LoveLetter -virus ylikirjoittaa kuva- ja musiikkitiedostoja paikallisilta ja verkkolevyasemilta. JPG-, JPEG-, MP3- ja MP2 -tiedostot tuhoutuvat ja ne pitää palauttaa varmistusratkaisujen avulla.

VBS/LoveLetter -virus tulee uhrinsa sähköpostiin LOVE-LETTER-FOR-YOU.TXT.vbs -nimisenä liitetiedostona. Jos .vbs-tiedostotarkennin ei ole Windows-oletusmääritysten takia näkyvissä, vastaanottaja voi luulla liitettä tavalliseksi .TXT-tekstitiedostoksi. Jos hän avaa tiedoston, virus leviää Microsoft Outlookin (jos se on asennettuna) kautta kaikille osoitehakemistossa oleville vastaanottajille - mukaan lukien yritysten ja organisaatioiden jopa tuhansia osoitteita sisältävät hakemistot.

Koska osoitehakemistoissa on yleensä erilaisia ryhmäosoitteistoja, yritykseen päässyt VBS/LoveLetter leviää ensimmäisen vastaanottajan kautta nopeasti koko organisaatioon. Seuraava liitetiedoston avaaja levittää viruksen omiin osoitteisiinsa ja niin edelleen, mikä ylikuormittaa sähköpostipalvelimen nopeasti.

Viruksen mukana tuleva/lähtevä viesti on seuraava:

> From: Tartunnan saaneen lähettäjän nimi
> To: osoitehakemistossa oleva nimi
> Subject: ILOVEYOU
>
> kindly check the attached LOVELETTER coming from me.
>
> Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

Lisäksi virus ylikirjoittaa paikalliskomennot ja HTML-tiedostot ja korvaa ne omalla koodillaan.

Virusmato on todennäköisesti kirjoitettu Filippiineillä. Ensimmäinen havainto siitä tehtiin varhain torstaiaamuna. Mukana oli seuraava teksti:

> barok -loveletter(vbe) <i hate go to school>
> by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
> Manila,Philippines

VBS/LoveLetter -virus on kirjoitettu VBScript-kielellä. VBScript-ohjelmat toimivat oletusmääritysten mukaan vain Windows 98- ja 2000 -käyttöjärjestelmissä, mutta tartuntavaarassa ovat myös sellaiset Windows 95- ja NT 4 -koneet, joissa on käytössä Microsoft Internet Explorerin versio 5.

Tekninen kuvaus viruksesta löytyy F-Securen viruskuvaustietokannasta osoitteesta http://www.F-Secure.com/v-descs/love.htm

Ruutuleikkeitä VBS/LoveLetter -viruksen saastuttamista sähköpostiviesteistä löytyy osoitteesta http://www.F-Secure.com/virus-info/v-pics/

F-Secure Oyj

Suomalainen F-Secure Oyj kehittää keskitetysti hallittavia mutta laajalle hajautettavia tietoturvaratkaisuja. Yrityksen tuotevalikoimaan kuuluu kattava joukko palkittuja integroituja virustentorjunta-, tiedostonsalaus- ja VPN-ratkaisuja työasemiin, palvelimiin ja gateway-koneisiin.

F-Secure-tuotteet ja niiden pohjana oleva F-Secure Framework soveltuvat erinomaisesti tietoturvan toimittamiseen palveluna (Security as a ServiceT). Security as a Service -toimittajia voivat olla esimerkiksi yritysten IT-osastot, Internet-palvelutarjoajat (ISP, Internet Service Provider), outsourcing-yritykset ja sovelluspalveluiden tarjoajat (ASP, Application Service Provider). Peruskäyttäjän näkökulmasta Security as a Service on näkymätön, automaattinen, luotettava, aina toimiva ja ajantasainen tietoturva. Ylläpitäjän näkökulmasta Security as a Service tarkoittaa kykyä toimittaa turvamenetelmäpohjaisia (policy-based) hallintapalveluita, ottaa vastaan hälytyksiä ja varmistaa laajalle hajautettujen tietoturvaratkaisujen keskitetty hallinta.

F-Secure Oyj on perustettu vuonna 1988. Yhtiön osakkeet on noteerattu Helsingin pörssin päälistalla. F-Secure Oyj:n pääkonttori on Espoossa. Sillä on tytäryhtiöt Yhdysvalloissa, Iso-Britanniassa, Ranskassa, Ruotsissa, Saksassa, Japanissa ja Kiinassa (Hong Kong) sekä kolme myyntikonttoria Yhdysvalloissa ja yksi Kanadassa. Valtuutettuja maahantuojia ja jakelijoita on yli 90 maassa ympäri maailmaa.

Lisätietoja
F-Secure Oyj
Mikko Hyppönen, tutkimuspäällikkö
PL 24 02231 ESPOO
puh (09) 8599 0513
fax (09) 8599 0599
sähköposti: Mikko.Hypponen@F-Secure.com

F-SECURE WARNS: LOVE LETTER E-MAIL WORM might exceed Melissa in severity

ESPOO, Finland, May 4th, 2000 - F-Secure Corporation (formerly Data Fellows) [HEX: FSC], a leading provider of security for mobile, distributed enterprises, is warning e-mail users of a new destructive e-mail worm called VBS/LoveLetter. This worm spreads by e-mailing a file called LOVE-LETTER-FOR-YOU.TXT.vbs around. F-Secure Anti-Virus detects and disinfects the virus, with the latest update available from www.F-Secure.com.

"This worm spreads at an amazing speed", comments Mikko Hypponen, Manager of Anti-Virus Research at F-Secure Corporation. "We got the first report around 9:00 a.m. on Thursday from Norway, and by 1 p.m. we had reports from over 20 countries. We estimate that total number of infected machines is already in tens of thousands. This epidemic might exceed Melissa in both speed and destructivity."

The worm arrives to users in e-mail message attachments called LOVE-LETTER-FOR-YOU.TXT.vbs. On a default Windows system, the ".vbs" extension is not visible, and users might mistake the file for a harmless text file (.TXT). If the recipient opens the attachment, the worm will use Microsoft Outlook (if installed) to send a message to everyone in any address books (including global access books of the organization these typically contains hundreds or thousands of addresses). The messages is as follows:

From: Name-of-the-infected-user
To: Random-name-from-the-address-book
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

As address books typically contain group addresses, the result of executing the VBS/LoveLetter worm inside an organization is that the first infected user sends the message to everybody in the organization. After this, other users open the message and send the message again to everyone else. This quickly overloads e-mail servers.

The LoveLetter worm activates by overwriting picture and music files from the local and network drives. Files with extension JPG, JPEG, MP3 and MP2 are overwritten and will have to be restored from backups.

In addition to spreading over e-mail, the worm also overwrites existing

local script and HTML files with its own code.

The worm was most likely written in the Philippines. It was first spotted in early morning, Thursday May 4. It contains the following text:

barok -loveletter(vbe) <i hate go to school>
by: spyder / ispyder@mail.com/ @GRAMMERSoft
Group / Manila,Philippines

VBS/LoveLetter is written in the VBScript language. By default, programs written in VBScript operate only under Windows 98 and Windows 2000. However, Windows 95 and NT 4 users are also vulnerable, if they have installed version 5 of Microsoft Internet Explorer.

A technical description of the virus is available in the F-Secure virus description database at: http://www.F-Secure.com/v-descs/love.htm

Sample pictures of e-mail messages generated by VBS/LoveLetter are available in the F-Secure virus screenshots center at: http://www.F-Secure.com/virus-info/v-pics/

About F-Secure Corporation

F-Secure Corporation is a leading developer of centrally managed security solutions for the mobile, distributed enterprise. The company offers a full range of award-winning integrated anti-virus, file encryption, distributed firewall and VPN solutions. F-Secure products and the underlying policy management framework enable corporate IT departments as well as service providers to deliver Security as a Service(tm). For the end-user, Security as a Service is invisible, automatic, reliable, always-on, and up-to-date. For the administrator, Security as a Service means policy-based management, instant alerts, and centralized management of a widely-distributed user base.

Founded in 1988, F-Secure is listed on the Helsinki Stock Exchange [HEX: FSC]. The company is headquartered in Espoo, Finland with North American headquarters in San Jose, California, as well as offices in Canada, China (Hong Kong and Beijing), France, Germany, Japan, Sweden and the United Kingdom. F-Secure is supported by a network of VARs and Distributors in over 90 countries around the globe.

For more information, please contact

USA:
F-Secure Inc.
Mr. Dan Takata, Manager, Training Division, Professional Services
675 N. First Street, 5th Floor
San Jose, CA 95112
Tel. +1 408 938 6700,

Fax +1 408 938 6701
e-mail Dan.Takata@F-Secure.com

Finland:
F-Secure Corporation
Mr. Mikko Hypponen, Manager, Anti-Virus Research.
PL 24
FIN-02231 ESPOO
Tel +358 9 8599 0513
Fax +358 9 8599 0599
E-mail: Mikko.Hypponen@F-Secure.com

http://www.F-Secure.com/

Note to Editors: Further technical information and a screenshot of the virus is available at:
http://www.F-Secure.com/virus-info/v-pics/

Marita Nasman-Repo tel: +358 9 8599 0613
Communicator fax : +358 9 8599 0599
mobile: +358 40 517 4613

F-Secure Corporation http://www.F-Secure.com

F-Secure products: Security for the mobile, distributed enterprise

---