



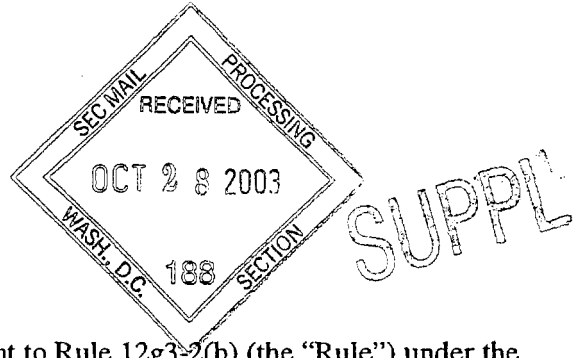
October 21, 2003

82-5035

RE: Rule 12g3-2(b) submission by F-Secure Corporation (formerly, Data Fellows Corp.)

Securities and Exchange Commission
Judiciary Plaza
450 Fifth Street, N.W.
Washington, D.C. 20549
USA

Attention: Division of International Corporate Finance



Ladies and Gentlemen:

I refer to the above-referenced exemption pursuant to Rule 12g3-2(b) (the "Rule") under the Securities Exchange Act of 1934, as amended (the "Act"), granted previously to F-Secure Corporation (formerly Data Fellows Corp.). I hereby transmit to you, in accordance with the provisions of Rule 12g3-2(b)(4) of the Act, a recent press release published by F-Secure.

As stated in paragraph (5) of the Rule, the Company understands that its furnishing the Securities and Exchange Commission with the information set forth above and the documents being transmitted herewith pursuant to the Rule shall not constitute an admission for any purpose that the Company is subject to the provisions of the Act.

Please contact the undersigned in connection with any of the points discussed in this letter.

Very truly yours,

PROCESSED
NOV 06 2003
h THOMSON FINANCIAL

Jaana Sirkiä
Corporate communicator

PP. Henrietta Ojalma

De 10/30

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE October 13, 2003

F-Secure's Security Solutions to TDC Cable TV's Internet Clients

F-Secure Corporation (HEX: FSC), and TDC Cable TV, the leading Danish cable TV and broadband Internet provider, today announced that they have signed a partnership to offer managed security services to TDC Cable TV's residential and small business Internet customers.

TDC Cable TV provides high-speed and high-quality Internet services in Denmark and now provides a managed antivirus and personal firewall service, to its customers. Automatic updates of the signature database, ease of use together with powerful antivirus and firewall applications are the main benefits of the service. While TDC Cable TV markets, sells and provides technical support for the services, F-Secure provides the security applications as well as the back-end technology to manage subscriptions, and hosts the service on behalf of TDC Cable TV. The services are offered to all WebSpeed Broadband Internet customers.

"As penetration of broadband Internet grow, Internet users in Denmark are more and more exposed to various security threats. F-Secure's Security as a Service solution brings clear benefits to TDC Cable TV in today's competitive business environment and offers multiple service extension possibilities. The F-Secure solution brings a lot of additional value to our existing access services. Automatic updates of the virus base, ease of use together with powerful antivirus and firewall application are main benefits of the service. We are happy to cooperate with F-Secure to offer our customers best possible protection", says Jeanette Dorthe Hansen, Vice president of TDC Cable TV.

"Service providers have to respond to the needs of the changing world. We feel that it is the service providers' responsibility to help their customers to get easy to use solutions for secure Internet use. As today's virus attacks combine multiple threats also using hacking methods, traditional antivirus is not enough. The only way to protect our computers against these attacks is to have always-on and frequently up-dated virus protection combined with a firewall. We are pleased to partner with TDC Cable TV to provide the needed security solutions to their customers," says Kimmo Alkio, COO at F-Secure Corporation.

F-Secure's security solutions as a subscription service are provided by the leading Telco operators and ISPs across Europe: Deutsche Telekom in Germany, Wanadoo in France, TeliaSonera in Sweden and Finland, Glocalnet in Sweden, Lietuvos Telekomas in Lithuania, Elion (former Eesti Telefon) in Estonia, Czech Telecom in Czech Republic, BlueCom in Norway and Elisa Oyj in Finland.

About F-Secure Corporation

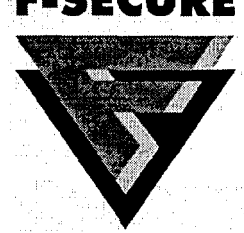
F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For more information, please contact:

F-Secure Corporation
Mr. Kalle Korpi
Sales Manager
Service Provider Solutions
Tammasaarencatu 7, PL 24
FIN-00181 Helsinki, Finland
tel: +358 9 2520 4123
e-mail: kalle.korpi@f-secure.com

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

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE October 13, 2003

F-Secure leads the way in mobile security with a new service platform and wireless security clients for smartphones

F-Secure Corporation today introduced a new groundbreaking security service solution for mobile operators and mobile phone vendors who are planning to provide consumers and corporate customers with wireless virus protection services.

The customers of mobile operators are concerned about harmful content on their mobile devices, but should not be troubled with security any more than is absolutely necessary. The burden of managing and updating security applications should be taken out of their hands.

The easiest and the most efficient way for the operator to accomplish this is to offer the required protection as an outsourced service, which allows automated distribution of the security software and updates directly to the mobile device over a wireless connection. The security application can also be pre-installed to the mobile devices before distribution and activated later when it is needed.

The F-Secure wireless security service solution consists of two components:

F-Secure Mobile Services™ is a platform for hosting automatic subscription-based security services with wireless connectivity and a patented SMS update mechanism. The platform offers several secure methods for efficiently distributing data to mobile terminals and secure web interfaces for sales and subscription management. Digitally signed downloads and updates ensure system security at all times.

F-Secure Anti-Virus for Series 60 is a fully automatic security solution that offers transparent real-time protection against harmful content locally on the Symbian OS device. It is the only security solution in the world that can be incrementally updated with SMS messages. It also detects a GPRS connection automatically and can update the threat database of the phone on the background over the Internet without any user interaction.

“It is the responsibility of the operators and hardware manufacturers to help their customers to get protection against harmful content. The success of our security services with the biggest Internet service providers in Europe proves that PC users prefer the subscription-based security service model to traditional software licensing. The same model will be dominant in the mobile telecom business, where the operators are starting to offer similar protection for the users of mobile terminals”, said Risto Siilasmaa, President and CEO of F-Secure Corporation.

Protection against all kinds of harmful content, not just viruses

The introduced security solution can be used for blocking harmful content from undesired messages to malfunctioning applications. This kind of harmful content exists already for mobile terminals, although the virus situation is not as demanding as in the PC environment. The antivirus client can also be used for deleting the malware from the infected terminals to restore their functionality. In general, history has shown that three things are needed for a new platform to become an interesting target for writers of malicious applications: enough functionality (for the malware to work), enough connectivity (for the malware to spread) and enough target terminals (for the platform to become interesting to the malware writers). These factors are starting to be in place for the most common handheld platforms, such as the Symbian Series 60 terminals.

When a new instance of harmful content appears, be it a virus, a malformed message or a malfunctioning application, the users who have subscribed to the F-Secure service before the incident get the fastest possible protection for their devices. In the vast majority of cases, the protection is active a long time before the device would become affected.

For the operators and hardware manufacturers, a wireless antivirus service is preventive insurance against end user support load, terminal downtime, negative user experience and bad publicity. The wireless virus protection service and the new antivirus clients for Series 60 terminals will be available through mobile operators and F-Secure in cooperation with hardware manufacturers. Service pilots with selected operators and terminal vendors are currently taking place. The F-Secure service solution is based on a partnership model, where F-Secure hosts the production environment and maintains the service platform. In operator cooperation, the virus protection service is sold and marketed by the operator and its sales channel. In hardware vendor cooperation, the antivirus clients are pre-installed to the terminals with a pre-paid service period, after which the users are redirected to F-Secure or local operator partners to buy continuation to the service.

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in France, Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia.

For more information, please contact:

F-Secure Corporation

Matias Impivaara, Manager, New Business Development

PL 24

FIN-00181 Helsinki

Tel +358 9 2520 5318

Email: Matias.Impivaara@F-Secure.com

Fax +358 9 2520 5001

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

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

F-SECURE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE October 13, 2003

F-Secure's Security Solutions to BlueCom AS Broadband Internet customers

F-Secure Corporation (HEX: FSC), and BlueCom AS, one of the leading Broadband Internet providers in Norway, today announced that they have signed an agreement to offer managed antivirus services to all BlueCom's broadband customers.

BlueCom is known for its high-quality Internet Services and automatic updates of the signature database, ease of use together with powerful antivirus application are the main benefits of the service to BlueCom's customers. While BlueCom AS markets, sells and provides technical support for the services, F-Secure provides the security applications as well as the back-end technology to manage subscriptions, and hosts the service on behalf of BlueCom. The services are offered to all BlueCom Broadband Internet customers.

"As BlueCom's customer base grows rapidly we want to offer our customers quality products for secure and reliable use of the Internet. By offering F-Secure's Security as a Service F-Secure solution to our customers we are able to introduce a lot of additional value to our existing broadband customers and increase our ARPU. By using a fully customized solution BlueCom also shows to the customer that security is an important matter in our strategy", says Harald Baardseth, Product Manager of BlueCom.

"Feedback from a growing broadband penetration in Norway confirms significant market demand for automated desktop security services. As information security is an essential part of today's Internet world, it is important that the service providers consider the needs of the end users, and offer them an easy way to secure their Internet use. We are pleased to partner with BlueCom to offer industry leading up-to-date security solutions to their broadband customers," says Kimmo Alkio, COO at F-Secure Corporation.

F-Secure's security solutions as a subscription service are provided by the leading Telco operators and ISPs across Europe: Deutsche Telekom in Germany, Wanadoo in France, TeliaSonera in Sweden and Finland, Glocalnet in Sweden, Lietuvos Telekomas in Lithuania, Eesti Telefon in Estonia, Czech Telecom in Czech Republic and Elisa Oyj in Finland.

About F-Secure Corporation

F-Secure Corporation is the leading provider of centrally managed security solutions for

the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia.

For more information, please contact:

F-Secure Corporation
Mr. Björn Werling, Sales Manager
Service Provider Solutions
Tammasaarenkatu 7, PL 24
FIN-00181 Helsinki, Finland
Tel. +358 9 2520 5670
E-mail: bjorn.werling@f-secure.com

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

About BlueCom AS

BlueCom is one of the leading Broadband ISP in Norway. The company provides a wide set of products and services to both corporate and residential customers in the Norwegian market. BlueCom values its customers above all and since the start in 1997 a rapid growth has been secured through satisfied customers and their "word of mouth". The company's core focus is to distribute xDSL broadband access, but typically complimentary products such as web hosting, domain registration and administration, security, IP-telephony and content are also important value drivers. The company's headquarter is situated in Oslo, while its customer support division is situated in Sandefjord, Norway. BlueCom has a highly skilled nationwide network of sales representatives, resellers and distributors serving corporate customers such as Statoil, Siemens and Aker/Kvaerner, as well as hotel- and store chains with numerous subsidiaries all over the country. Bluecom demands high standards from their suppliers to be able to continuously deliver superior products and services to its customers. This is secured through partners such as Telia, Telenor, F-Secure, Global Crossing, Alcatel and Siemens.

For more information please contact:

BlueCom AS
Mr. Harald Baardseth
Product Manager
Sommerrogaten 13-15
N-0255 Oslo
Norway
Tel: +4722121400
e-mail: hb@bluecom.no
<http://www.bluecom.no>

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

F-SECURE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE October 6, 2003

F-Secure's Security Solutions to Czech Telecom's Customers

F-Secure Corporation (HEX: FSC), and Czech Telecom, the leading Czech Republic Telecommunications company, today announced that they have signed a partnership to offer managed security services to Czech Telefon's residential and small business Internet customers.

Czech Telecom provides high-speed and high-quality Internet services in Czech Republic and has launched a managed antivirus and personal firewall service, under the name IOL Secure to its customers. Automatic updates of the virus base, ease of use together with powerful antivirus and firewall application are main benefits of the service. While Czech Telecom markets, sells and provides technical support for the services, F-Secure provides the security applications as well as the back-end technology to manage subscriptions, and hosts the service on behalf of Czech Telecom. The services are offered to the ADSL users and also for dial-up modem customers.

"As internet penetration and number of ADSL customers grow, customers in Czech republic are more and more exposed to various security threats. F-Secure Security as a Service solution bring clear benefits to Czech Telecom in today's competitive business environment and offers multiple service extension possibilities. By offering F-Secure solution to our customers we are able to introduce a lot of additional value to our existing access services and increase our ARPU. By using a fully customized solution Czech Telecom also shows to the customer that security is an important matter in their strategy. We are happy to cooperate with F-Secure to offer our customers best possible protection", says Jan Záruba, Director of Internet Products Development of Czech Telecom.

"Feedback from end users and a growing ADSL penetration confirms significant market demand in Czech Republic for automated antivirus services. It is important the service providers respond to the needs of the changing world and provide users with easy to use solutions for secure Internet use. As today's virus attacks combine multiple threats also using hacking methods, traditional antivirus is not enough. The only way to protect our computers against these attacks is to have always-on and frequently up-dated virus protection combined by a firewall. We are pleased to partner with Czech Telecom to offer industry leading up-to-date security solutions to their customers," says Kimmo Alkio, COO at F-Secure Corporation.

F-Secure's security solutions as a subscription service are provided by the leading Telco

operators and ISPs across Europe: Deutsche Telekom in Germany, Wanadoo in France, Glocalnet in Sweden, TeliaSonera in Sweden and Finland, Lietuvos Telekomas in Lithuania, Eesti Telefon in Estonia and Elisa Oyj in Finland.

About F-Secure Corporation

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia.

For more information, please contact:

F-Secure GmbH

Mr. Jari Heinonen Sales Manager, Service Provider Solutions

Hoffmanstraße 7

81379 Munich, Germany

Phone +49 (0) 89 787 467-42

mobile +49 (0) 171 4693290

Fax +49 (0) 89 787 467-99

Email: Jari.Heinonen@F-Secure.com

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

Vladan Crha

Press Spokesman

tel: (+420) 271 463 359

fax: (+420) 271 469 896

e-mail: press.dept@ct.cz

About Czech Telecom

ČESKÝ TELECOM, a.s., continues to strive to improve the quality of its services. The firm implements system management that satisfies the requirements of internationally-recognised ISO 9000:2000 norms, earning it certification from Lloyd's Register Quality Assurance Limited. Certificates have already been issued for the Service Wholesale Division, for Corporate Client Services in the Telecommunications Services Division, as well as Purchasing and Logistics.

With roughly 3.6 million telephone lines in operation, ČESKÝ TELECOM, a. s., is the leading telecommunications company in the Czech Republic. Through its subsidiary company Eurotel Praha, spol. s r.o., it also has a significant presence in the Czech mobile services market. ČESKÝ TELECOM pays close attention to the improvement in the growth potential of data and Internet services. According to GfK, a prominent market research firm, IT managers regard ČESKÝ TELECOM as the best data service provider in the Czech Republic. The company also intends to position itself as the

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

country's leading comprehensive service provider in the realms of e-commerce and other non-traditional business. It also places great emphasis on the presentation of its products and services through its web pages. The company's web site ranked first in an evaluation of all Czech Top 100 corporate sites.

Signum Temporis has consistently awarded ČESKÝ TELECOM for being one of the domestic capital market's most transparent firms in terms of providing information. Based on an open vote of specialists, members of the press and a nine-member committee, ČESKÝ TELECOM placed first in 2003, just as it did in 2001. ČESKÝ TELECOM ranks among the most prominent firms on the Czech capital market in terms of capitalization and trading volumes. Its shares are also traded on the London Stock Exchange in the form of GDRs. ČESKÝ TELECOM's credit rating is the highest a Czech corporation can receive from top international rating agencies.

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE September 19, 2003

New Computer Worm Exploits False Security Update

F-Secure Corporation warns the computer users about a new worm known as Swen. F-Secure has today increased the alert level to Radar Level 1, as the worm is spreading rapidly worldwide. This is the highest alert level for a computer virus.

Swen is a mass-mailer, which was first found on Thursday, September 18th, 2003. This rather complex worm uses several different techniques to spread and can, unlike most other e-mail worms, execute automatically when an infected e-mail message is received. Swen can also, in addition to e-mail, use IRQ chat, Kazaa networks and shared folders in local area networks to spread.

The infected messages that carry the Swen worm are spoofed to look like security updates from Microsoft. These false security updates are quite realistic and mimic the look and feel of Microsoft web pages. "The Swen worm clearly tries to ride on the publicity created by the Lovesan/Blaster worm in August. The importance of installing security updates was stressed many times", says Mikael Albrecht, the Product Manager of F-Secure. "It is therefore natural that people open what they think is a security patch. However, the attached file is not a patch, it is a virus", he continues. Swen is not the first worm to use this trick, but the spoofed message created by Swen is the most professional looking so far.

It is important to note that the real security updates from Microsoft are always published on the web or distributed through automatic update channels. They are never sent by e-mail.

Detailed technical description of the worm as well as screenshots are available in the F-Secure Virus Description Database at <http://www.f-secure.com/v-descs/swen.shtml>.

F-Secure Anti-Virus can detect and stop the Swen worm. F-Secure Anti-Virus can be downloaded from <http://www.f-secure.com>

More information on the F-Secure Radar warning system can be found from <http://www.f-secure.com/products/radar/>

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus and

network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For more information, please contact:

Finland:

F-Secure Corporation

Mikael Albrecht, Product Manager

PL 24

FIN-00181 Helsinki

Tel. +358 9 2520 5640

Mobile: +358 40 550 9349

Email: Mikael.Albrecht@F-Secure.com

Media contact in the USA:

F-Secure Inc.

Heather Deem,

675 N. First Street, 5th Floor

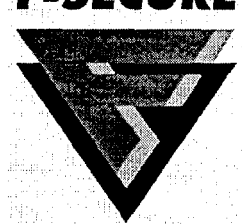
San Jose, CA 95112

Tel +1 408 350 2178

Fax +1 408 938 6701

Email Heather.Deem@F-Secure.com

F-SECURE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE September 2, 2003

F-Secure launches first truly integrated solution against viruses, worms and hackers in corporate environments

Helsinki, Finland, September 2, 2003 - F-Secure Corporation (HEX: FSC), a leading provider of content security solutions, today announced the immediate availability of F-Secure Anti-Virus Client Security. Recent virus outbreaks highlight urgent need for companies to upgrade protection to a centrally managed solution integrating antivirus, distributed firewall, application control and intrusion prevention into a seamless cost-efficient solution to protect desktops and laptops against network worms, such as Blaster/Lovsan. F-Secure Anti-Virus Client Security is the first antivirus solution to fully satisfy the new requirements.

"The past few weeks have been the busiest in virus history. In the case of Blaster a traditional antivirus, even with the most recent update, allowed the worm to enter the computer. This proves that the era of traditional antivirus products is over. Antivirus with an integrated firewall is the only protection against these attacks", says Kimmo Alkio, Chief Operating Officer of F-Secure's Anti-Virus Business.

F-Secure Anti-Virus Client Security is designed to protect company desktops and laptops against today's complex threats. The product offers unique protection against viruses, hackers, network worms as well as the use of networking software that violates corporate security policies. The centralized management system, F-Secure Policy Manager, provides an easy and cost efficient way to deploy the product and to monitor the security level of the whole network.

"The recent virus outbreaks (Blaster, Sobig.F) have started a new era in the fight against viruses. You need a robust and scalable solution to be properly protected. F-Secure Anti-Virus Client Security provides a complete and fully manageable solution against modern threats. Thanks to its unique features we can concentrate on our core business even in the case of major virus outbreaks", says Ola Johansson, Technical Manager of The National Social Insurance Board of Sweden.

F-Secure Anti-Virus Client Security also features virus news delivery, location based security levels and centrally managed application control. The virus news feature delivers instant notification messages of serious security events around the globe and informs the user when the computer is protected against the new threat. The product is also able to raise its security level based on the location, e.g. the security level is higher

when the laptop is connected to the network outside office premises. With the application control the network administrator can prevent the use of networking software that violates company security, such as spy ware, peer-to-peer and internet relay chat (IRC) software.

Availability

F-Secure Anti-Virus Client Security is immediately available through F-Secure's worldwide network of value-added resellers, distributors and systems integrators. For more information contact F-Secure at <http://www.f-secure.com/products/partners/worldwide/> .

F-Secure Anti-Virus Client Security can be bought as part of the multi-layer solution F-Secure Anti-Virus Total Suite or separately.

The product is available at 29,75 €/seat for 100 seats.

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For further information, please contact:

F-Secure Corporation
Topi Hautanen, Product Marketing Manager
PL 24
FIN-00181 Helsinki
Finland
Tel +358 9 2520 5596
Fax +358 9 2520 5018
Email: Topi.Hautanen@F-Secure.com

Media contact in the USA:

F-Secure Inc.
Heather Deem, 675 N. First Street, 5th Floor
San Jose, CA 95112
Tel +1 408 350 2178
Fax +1 408 938 6701
Email: Heather.Deem@F-Secure.com

www.F-Secure.com

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE September 2, 2003

F-Secure Internet Gatekeeper stops the modern Internet based security threats

Helsinki, Finland, September 02, 2003 - F-Secure Corporation [HEX: FSC] announces the immediate availability of a new product, F-Secure Internet Gatekeeper, through F-Secure partners worldwide. F-Secure Internet Gatekeeper is a firewall and mail server-independent solution specially engineered for high speed scanning of web (HTTP and FTP over HTTP) and e-mail (SMTP) traffic for viruses and other undesirable content.

The vast majority of new complex viruses and other malicious code spread via e-mail as well as web browsing and file downloads. Without effective and automated protection at the gateway level, viruses can easily penetrate and infect servers and end user machines, stealing confidential files, forwarding e-mails, corrupting data or causing large amounts of traffic. By scanning traffic already at the edge of the network, mass mailing viruses, like the recent Sobig.F, can be easily stopped before they enter corporate mail systems.

F-Secure Internet Gatekeeper allows administrators to control the content downloaded from the web and exchanged by e-mail. Blocking undesired content, such as movie files, sound files and other non-work related content, and preventing employees from accessing inappropriate web sites, the solution optimizes network performance and improves employee productivity. In addition, the solution provides reduces the risk for legal liability and protects the company reputation by, for example, preventing employees from downloading illegal software and ensuring that virus-infected messages are not sent to their customers and business partners.

"High performing F-Secure Internet Gatekeeper is well suited for both large customers as well as for small and medium sized businesses (SMB) that are running their own e-mail server and firewall," says Jyrki Tulokas, Product Line Manager at F-Secure. "With easy and fast installation and ability to run all parts on one Windows server, F-Secure Internet Gatekeeper provides a cost effective choice for SMB customers. On the other hand, large corporations with multiple offices and high network traffic benefit from the ability to distribute the scanning over multiple servers."

Managing and installing the product is fast and easy. The product can be managed either locally stand-alone or remotely with F-Secure's centralized management system F-Secure Policy Manager. With F-Secure Policy Manager the administrators also get

detailed virus incident reporting and alerting, keeping them well informed about corporate web and e-mail traffic content. Protecting your network could not be easier and more secure. F-Secure Internet Gatekeeper runs on Windows 2000 Server and Windows 2003 Server platforms. F-Secure Internet Gatekeeper can be bought as part of the multi-layer solution F-Secure Anti-Virus Total Suite or separately.

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For further information, please contact:

F-Secure Corporation
Jyrki Tulokas, Product Line Manager
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 5683
Fax: +358 9 2520 5004
Mobile: +358 40 769 7683
E-mail: Jyrki.Tulokas@F-Secure.com

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

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE August 23, 2003

Close Call - the Sobig.F activation was prevented

F-Secure helped to shut down servers needed by the attack

The expected Internet activation of the Sobig.F worm has been prevented. The activation was programmed to take place on Friday the 22nd of August at 19:00 UTC. The activation was prevented through a 24-hour race against the clock by various organizations around the world. Everything started from the detailed analysis of the worm by the F-Secure research team, which found and decrypted the list of 20 Encrypted compromised server IP addresses from within the worm. Armed with the list of 20 IP addresses F-Secure, various internet service providers, CERT organizations from around the world, FBI and Microsoft were able to locate and disconnect or shut down most of the master servers necessary for the activation to be successful.

Six hours before the deadline, 11 of them were disconnected from the Internet. Just before the activation, 18 of them were disconnected. One of the remaining servers was unreachable, perhaps turned off. One was still operating when the attack started, but it immediately became unreachable as tens of thousands of infected machines from around the world started sending traffic to it.

F-Secure has been attempting to connect to all the 20 machines from three different sensors in three different countries to confirm that they are down. So far, we've been unable to connect even once. If we can't connect, neither can the infected machines - and the activation won't succeed.

Sobig.F, which is currently the most widespread worm in the world, contains an encrypted list of 20 servers located in USA, Canada and South Korea. The worm tried to connect to these servers to download the address of another server from which the worm would have downloaded an unknown application. The application would have then been immediately executed on all the infected computers.

More information about the Sobig.F worm and the attempted attack is available at <http://www.F-Secure.com>

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the

Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For more information, please contact:

Finland:

F-Secure Corporation
Mikko Hypponen, Director, Anti-Virus Research
PL 24
FIN-00181 Helsinki
Tel +358 9 2520 5513
Fax. +358 9 2520 5001
Email Mikko.Hypponen@F-Secure.com

Media contact in the USA:

F-Secure Inc.
Heather Deem,
675 N. First Street, 5th Floor
San Jose, CA 95112
Tel +1 408 350 2178
Fax +1 408 938 6701
Email Heather.Deem@F-Secure.com

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

F-SECURE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE August 22, 2003

A potentially massive Internet attack starts today

*Sobig.F downloads and executes a mysterious program
on Friday at 19:00 UTC*

F-Secure Corporation is warning about a new level of attack to be unleashed by the Sobig.F worm today.

Windows e-mail worm Sobig.F, which is currently the most widespread worm in the world, has created massive e-mail outages globally since it was found on Tuesday the 18th of August – four days ago. The worm spreads itself via infected e-mail attachments in e-mails with a spoofed sender address. Total amount of infected e-mails seen in the Internet since this attack started is close to 100 million.

However, the Sobig.F worm has a surprise attack in its sleeve. All the infected computers are entering a second phase today, on Friday the 22nd of August, 2003. These computers are using atom clocks to synchronize the activation to start exactly at the same time around the world: at 19:00:00 UTC (12:00 in San Francisco, 20:00 in London, 05:00 on Saturday in Sydney).

On this moment, the worm starts to connect to machines found from an encrypted list hidden in the virus body. The list contains the address of 20 computers located in USA, Canada and South Korea.

“These 20 machines seem to be typical home PCs, connected to the Internet with always-on DSL connections”, says Mikko Hypponen, Director of Anti-Virus Research at F-Secure. “Most likely the party behind Sobig.F has broken into these computers and they are now being misused to be part of this attack”.

The worm connects to one of these 20 servers and authenticates itself with a secret 8-byte code. The servers respond with a web address. Infected machines download a program from this address – and run it. At this moment it is completely unknown what this mystery program will do.

F-Secure has been able to break into this system and crack the encryption, but currently the web address sent by the servers doesn't go anywhere. “The developers of the virus know that we could download the program beforehand, analyse it and come up with countermeasures”, says Hypponen. “So apparently their plan is to change the web address to point to the correct address or addresses just seconds before the deadline. By the time we get a copy of the file, the infected computers have already downloaded and run it”.

Right now, nobody knows what this program does. It could do damage, like deleting files or unleash network attacks. Earlier versions of Sobig have executed similar but simpler routines. With Sobig.E, the worm downloaded a program which removed the virus itself (to hide its tracks), and then started to steal users network and web passwords. After this the worm installed a hidden email proxy, which has been used by various spammers to send their bulk commercial emails through these machines without the owners of the computers knowing anything about it. Sobig.F might do something similar – but we won't know until 19:00 UTC today.

“As soon as we were able to crack the encryption used by the worm to hide the list of the 20 machines, we've been trying to close them down”, explains Mikko Hypponen. F-Secure has been working with officials, authorities and various CERT organizations to disconnect these machines from the Internet. “Unfortunately, the writers of this virus have been waiting for this move too.” These 20 machines are chosen from the networks of different operators, making it quite likely that there won't be enough time to take them all down by 19:00 UTC. Even if just one stays up, it will be enough for the worm.

The advanced techniques used by the worm make it quite obvious it's not written by a typical teenage virus writer. The fact that previous Sobig variants were used by spammers on a large scale adds an element of financial gain. Who's behind all this? “Looks like organized crime to me”, comments Mikko Hypponen.

F-Secure is monitoring the Sobig.F developments through the night on Friday the 22nd. Updates will be posted to Sobig.F's virus description at http://www.f-secure.com/v-descs/sobig_f.shtml

F-Secure Anti-Virus can detect and stop this worm. F-Secure Anti-Virus can be downloaded from <http://www.f-secure.com>

About F-Secure

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For more information, please contact:

Finland:
F-Secure Corporation
Mikko Hypponen, Director, Anti-Virus Research
PL 24
FIN-00181 Helsinki
Tel +358 9 2520 5513

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

Fax. +358 9 2520 5001
Email Mikko.Hypponen@F-Secure.com

Media contact in the USA:
F-Secure Inc.
Heather Deem,
675 N. First Street, 5th Floor
San Jose, CA 95112
Tel +1 408 350 2178
Fax +1 408 938 6701
Email Heather.Deem@F-Secure.com

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

F-SECURE RELEASE
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



FOR RELEASE August 19, 2003

Worst virus week continues

Four new major virus cases within 24 hours

"This reminds me of fall 2001", comments Mikko Hyppönen, Director of Anti-Virus Research at F-Secure Corporation. "Year 2001 still stays in history as the worst virus year ever, but this is starting to get just as bad. Within one week we've seen several major virus outbreaks as well as some completely new techniques in viruses".

Lovsan

The Lovsan (or Blaster) network worm started to spread on Monday, August 11, 2003. The worm spreads in an executable named MSBLAST.EXE to Windows 2000 and Windows XP systems unless recent Windows security patches have been applied. The infection is completely invisible to the end user and the worm will then keep on replicating from every infected machine. Lovsan has already infected hundreds of thousands computers and addition to the first Lovsan three new variants have been found. The latest one, Lovsan.D, was discovered on August 19, 2003.

Welchi

Welchi (or Nachi) worm was first discovered on August 18, 2003. It uses the same RPC hole to infect machines as Lovsan. However, Welchi also tries to infect web servers running Microsoft IIS 5.0, by exploiting a WebDAV vulnerability found in March 2003.

Welchi is clearly much more advanced than the relatively simple Lovsan worm. When infecting a computer that already has been infected by Lovsan, Welchi kills Lovsan and removes the infection. In addition to this feature, the worm will try to apply the Microsoft patch to close the RPC hole. Welchi is programmed to die on January 1st, 2004. After this date the worm will uninstall and remove itself from infected systems. Biggest side effect of Welchi is that it generates lots of network traffic - enough to cause problems for some routers and switches.

Sobig.F

This worm is part of the Sobig family, which was started by Sobig.A in January 2003. Sobig.F, which was discovered on August 19th, is then the fifth variant of this worm. Sobig variants all stop spreading on certain date. When the previous variants expired, the next variant would start spreading. All Sobig versions have spread widely.

"Sobig.E was programmed to die on July 14th, and we expected to see the next version around that time. However, apparently the virus writer has been on vacation since it took four weeks for Sobig.F to appear", Mikko Hyppönen says.

Sobig variants typically install backdoors to infected systems. Some of them have been used to send massive amounts of spam.

Lovsan.D

Lovsan.D is a new variant of the Lovsan worm, with modified attachment name. Instead of msblast.exe the attachment is now named mspatch.exe.

Dumaru

Dumaru was found on August 19th and it exploits the fuss caused by the Lovsan worm. Dumaru will send an email message spoofed to be from support@microsoft.com. According to the body text the attached PATCH.EXE file will fix the vulnerability. If this attachment is opened, the machine will be infected. Dumaru also installs a backdoor through which the virus writer can remotely control the machine.

Detailed technical descriptions of the worms as well as screenshots are available in the F-Secure Virus Description Database at http://www.f-secure.com/v-descs/sobig_f.shtml
<http://www.f-secure.com/v-descs/welchi.shtml>
<http://www.f-secure.com/v-descs/msblast.shtml>
<http://www.f-secure.com/v-descs/dumaro.shtml>
<http://www.f-secure.com/v-descs/lovsand.shtml>

F-Secure Anti-Virus can detect and stop these worms. F-Secure Anti-Virus can be downloaded from <http://www.f-secure.com>

About F-Secure Corporation

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

Media queries to:

Mikko Hyppönen, Director, Anti-Virus Research
F-Secure Corporation
Tel. +358 9 2520 5513
Email: Mikko.Hypponen@F-Secure.com

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700,
fax +358 9 2520 5001

Mikael Albrecht, Product line Manager
Tel. +358 9 2520 5640
Email: Mikael.Albrecht@F-Secure.com

Media contact in the USA:

F-Secure Inc.
Heather Deem,
675 N. First Street, 5th Floor
San Jose, CA 95112
Tel +1 408 350 2178
Fax +1 408 938 6701
Email Heather.Deem@F-Secure.com

www.F-Secure.com



FOR RELEASE August 18, 2003

A new worm installs security patches

An anti-virus-virus is spreading

F-Secure has analysed a new Windows network worm, known as Welchi or Nachi. This worm is similar to the Lovsan or Blaster worm, which has been spreading massively in the internet for the last week.

Welchi uses the same RPC hole to infect machines, although Welchi only infects machines running Windows XP operating system. However, Welchi also tries to infect web servers running Microsoft IIS 5.0, by exploiting a WebDAV vulnerability found in March 2003.

Welchi is clearly much more advanced than the relatively simple Lovsan worm. In particular, it has three features, which make it interesting:

1) Welchi kills Lovsan.A.

As this new worm is using the same hole as Lovsan, it will obviously end up infecting machines, which are already infected by Lovsan. Welchi removes this infection.

2) Welchi installs the Microsoft RPC security patch.

After infecting a machine, the worm will try to apply the Microsoft patch to close the RPC hole. It will attempt to download the patch from Microsoft web site. As the patch is different for different localized versions of Windows, the worm will check the local language and apply a suitable patch for English, Korean, Chinese and Simplified Chinese versions of Windows.

3) Welchi dies.

This worm has a built-in expiration date. After January 1st, 2004, the worm will uninstall and remove itself from infected systems. Users can use this feature to easily remove the worm: change the date to 2004 and reboot the system. After this the date can be set back.

"So, we seem to have an anti-virus-virus here", says Mikko Hypponen, Director of Anti-Virus Research at F-Secure Corporation. "We've seen similar things before, but not to the extent of actually applying Microsoft's own patches to the system. Unfortunately Welchi is not perfect and will create some additional problems."

The Welchi virus contains these hidden texts:

I love my wife & baby :)
~~~ Welcome Chian~~~  
Notice: 2004 will remove myself :)  
~~ sorry zhongli~~~

## QUESTIONS AND ANSWERS ON THE WELCHI WORM

Q: Is this a variant of the Lovsan worm?

A: No. It has similarities and uses the some RPC hole, but it's not a variant.

Q: How does it spread to workstations?

A: If an unprotected machine is connected to the internet, the worm will access it directly with connections to TCP port 135 and infect it remotely. The user sees nothing.

Q: How does it spread to web servers?

A: If an unpatched IIS 5.0 machine is connected to the internet, the worm will access it directly and use the WebDAV vulnerability to infect it remotely.

Q: Which Windows platforms are vulnerable?

A: Apparently only Windows XP.

Q: Does Microsoft have a patch to close the RPC hole?

A: Yes, at <http://www.microsoft.com/security/incident/blast.asp>

Q: Does Microsoft have a patch to close the WebDAV hole?

A: Yes, at <http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>

Q: Could it get behind firewalls?

A: Yes, just like Lovsan (on laptops, through external net connections made from behind the firewall). In some cases the web server might serve as a gateway to pass the infection from the public internet to intranets.

Q: What kind of emails does this worm send?

A: None. This is not an email worm. It never sends any emails.

Q: I'm running German version of Windows. Will this worm patch my machine?

A: No. It will still infect it though.

Q: Is it ok to remove this virus by changing the date momentarily to 2004?

A: Yes, it seems to work fine.

Q: Is this a good virus?

A: No.

Q: Why not?

A: For many reasons. It's unauthorised. It's not tested. It creates compatibility problems. It might crash RPC services. It creates unnecessary network traffic (lots of it). And for many other reasons. For full discussion on this, see Dr. Vesselin Bontchev's infamous F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700, fax +358 9 2520 5001

paper "Are "Good" Computer Viruses Still a Bad Idea?", available at <http://www.virusbtn.com/old/OtherPapers/GoodVir/>

Q: Where is this worm from?

A: Probably from South Korea, Taiwan or mainland China.

Detailed technical description of the worm as well as screenshots are available in the F-Secure Virus Description Database at <http://www.f-secure.com/v-descs/welchi.shtml>

F-Secure Anti-Virus can detect and stop the Welch worm. F-Secure Anti-Virus can be downloaded from <http://www.f-secure.com>

F-Secure's firewall products protected against Welch, Lovsan and variants even before they were written. Consider using a good quality firewall on your Windows systems.

### **About F-Secure Corporation**

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

Media queries to:

Mikko Hypponen, Director, Anti-Virus Research  
F-Secure Corporation  
Tel. +358 9 2520 5513  
Email: [Mikko.Hypponen@F-Secure.com](mailto:Mikko.Hypponen@F-Secure.com)

Media contact in the USA:  
F-Secure Inc.  
Heather Deem,  
675 N. First Street, 5th Floor  
San Jose, CA 95112  
Tel +1 408 350 2178  
Fax +1 408 938 6701  
Email [Heather.Deem@F-Secure.com](mailto:Heather.Deem@F-Secure.com)

F-SECURE RELEASE  
F-Secure Corporation  
PL 24  
FIN-00181 Helsinki  
Tel. +358 9 2520 0700  
Fax. +358 9 2520 5001  
<http://www.F-Secure.com>



**FOR RELEASE August 16, 2003**

## **Worm attack succeeds and fails at the same time**

The Lovsan worm that has been spreading since Monday has now activated around the world.

Windows 2000 and XP machines that get infected after this moment will try to launch a distributed denial-of-service attack against Microsoft's windowsupdate.com. Similarly, machines which were infected before midnight on 15th of August (local time) will start the attack the next time they are rebooted. This will continue until the end of the year 2003.

Microsoft made drastic changes in their Internet set up on Friday, changing the operations of their main servers. As to windowsupdate.com, they just surrendered.

"They figured out - quite correctly - that no web server could survive under the attack load generated by tens of thousands of infected computers. So Microsoft simply disconnected this server from the web and removed it's name from domain name systems" explains Mikko Hypponen, Director of Anti-Virus Research at F-Secure Corporation. "Windowsupdate.com will probably never return. So in this sense, the worm accomplished what it wanted: windowsupdate.com is no more."

As a result, the worm can't find a target address for the attack - and won't attack. The change was done so late that probably some affected machines still had cached IP address for windowsupdate.com and a limited amount of attack packets are going around the net - but not enough to cause disruption for the internet itself.

So, Microsoft sacrificed their server to save the rest of the net. Now there will be no floods of packets to overflow routers and switches at ISPs around the world. This probably was an easy decision for Microsoft, as windowsupdate.com was not used much.

The official address for Microsoft's Windows Update Service is windowsupdate.microsoft.com. This is also the address built-in to Windows 98, ME, 2000, XP and 2003. Most likely this was the address the virus writer tried to attack, but she made a slight mistake in the address (which used to be redirected to the same update service).

F-Secure estimates that the Lovsan worm to continue to spread around the world in measurable amounts at least until 2005.

## **About F-Secure**

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include antivirus, file encryption and network security solutions for major platforms from desktops to servers and from laptops to handhelds. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since November 1999. The company is headquartered in Helsinki, Finland, with the North American headquarters in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and HP.

For more information, please contact:

F-Secure Corporation  
Mikko Hypponen, Director of Anti-Virus Research  
PL 24  
FIN-00181 Helsinki  
Tel +358 9 2520 5513  
Fax. +358 9 2520 5001  
Email: [Mikko.Hypponen@F-Secure.com](mailto:Mikko.Hypponen@F-Secure.com)

Media contact in the USA:  
F-Secure Inc.  
Heather Deem,  
675 N. First Street, 5th Floor  
San Jose, CA 95112  
Tel +1 408 350 2178  
Fax +1 408 938 6701  
Email [Heather.Deem@F-Secure.com](mailto:Heather.Deem@F-Secure.com)