F-Secure Corporation

82-5035

September 16, 2002

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,

Jaana Sirkiä
Corporate communicator

P. Henrietta Malmari

Press release

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

F-SECURE®

FOR RELEASE September 15, 2002

Fast spreading Slapper worm enables attacker to take over infected servers

F-Secure reverse engineered worms network protocol -- real-time information on number and location of infected computers

The Linux.Slapper worm was first seen on Friday the 13th. Since then it has infected thousands of web servers around the world and continues to spread. What sets it apart from other worms is its peer-to-peer networking capability, which the worm author may utilize to take over any or all of the infected servers. This was apparently designed to launch distributed denial-of-service attacks with the worm, but it also results in a situation where anybody can take over an infected machine and do practically anything with it.

The Slapper is representative of the new breed of worms and viruses as it is as much an attack tool as it is a quickly spreading worm.

During the weekend following Friday the 13th, F-Secure engineers have reverse engineered the peer-to-peer protocol that the worm uses. F-Secure has now infiltrated the Slapper peer-to-peer attack network, posing as an infected web server. Through this fake server, the exact number of infected machines and their network names can be identified.

F-Secure's Global Slapper Information Center provides regularly updated information on the spread of the virus and numbers of infected servers categorized by the top-level domain. F-Secure is also sending a warning to the administrators of infected systems based on their IP addresses. A free version of F-Secure Anti-Virus for Linux will also be made available to the administrators of infected systems. The license allows the product to be used in a limited fashion to remove the worm from the system.

F-Secure is also contacting the national authorities in order to alert the administrators of infected systems. It is imperative that the servers are cleaned and patched to prevent future infections as soon as possible - both to stop the spreading of the worm and to prevent unauthorised access to the infected servers.

Global Slapper Information Center can be found from:
http://www.f-secure.com/slapper/

Situation on Sunday 15th of September 2002, at 17:00 GMT

By Sunday evening, the Linux.Slapper worm had been in circulation for less than 40 hours. In this time, the number of infected servers has grown from 0 to over 6000. For reference, Code Red - which is known as the worst web worm so far - managed to infect only a couple of hundred servers within similar time frame. Code Red went on to infect over 300,000 web servers during its beak in July 2001 and is still alive today. It is estimated that there are over 1,000,000 active OpenSSL installations in the public web. A very big part of those machines has not yet been patched to close this hole, and are thus prone for infection by the Slapper worm.

The worm infects unprotected Linux machines that are running Apache web server with OpenSSL enabled. Uniquely, the worm spreads in C source code format, recompiling itself on every infected machine.

Detailed technical description of the worm as well as a screenshot are available in the Global Slapper Information Center in http://www.f-secure.com/slapper/

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 Compaq.

For more information, please contact:

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

Press 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 14, 2002

F-Secure warns about a new Linux web worm

Helsinki, Finland – September 14th. F-Secure Corporation is warning about a new network worm called Slapper. Slapper is a network worm that spreads on Linux machines, using a flaw discovered in August 2002 in OpenSSL libraries. The worm was found in Eastern Europe late on Friday 13th, September 2002.

The worm typically affects Linux machines that are running Apache web server with SSL enabled. Apache installations cover more than 60% of public web sites in the internet. It could be estimated that less than 10% of those have enabled SSL services. SSL is most often used for online commerce, banking and privacy applications.

Once a machine gets infected, the worm starts to spread to new systems. In addition, the worm contains code to create a peer-to-peer attack network, where infected machines can remotely be instructed to launch a wide variety of Distributed Denial of Service (DDoS) attacks.

The worm works on Intel-based machines running Linux distributions from Red Hat, SuSE, Mandrake, Slackware or Debian. Apache and OpenSSL must be enabled and OpenSSL version must be 0.96d or older.

Slapper is very similar to the Scalper Apache worm, which was found in June 2002. The basic theory of operation is similar to the first widespread web worm, Code Red. Code Red infected more than 350000 websites running Microsoft IIS in July 2001.

"It is still early to say whether this will become a major problem or not", comments Mikko Hypponen, Manager of Anti-Virus Research at F-Secure. "In any case, we urge all Linux webmasters to make sure their systems are secured against this attack."

Detailed description of the worm as well as a screenshot are available at:
http://www.f-secure.com/v-descs/slapper.shtml

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 Compaq.

For more information, please contact:

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

Press 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 11, 2002

F-Secure informs about a 9/11-themed "Chet" e-mail worm

Helsinki, Finland September 11th - F-Secure Corporation informs that it has received copies of a new Windows e-mail worm called "Chet". This worm is themed around the September 11th terrorist attacks.

This worm was found on September 10th, 2002. As it contains serious bugs, the Chet worm will fail to function on most systems and can not be considered to be a major threat at this time. This advisory is published to prevent unnecessary hysteria on this worm.

The Chet worm tries to spread via an attachment file called 11september.exe. When this file is executed, the worm will attempt to send an e-mail to each address found from the Windows address book. The e-mail would always have "mail@world.com" as the sender and "All people!!" as the subject.

The e-mail tries to explain that the attached "11september.exe" file contains proof of a conspiracy between US government and Al-Qaeda. However, if user executes the file, nothing visible happens while the worm tries to send itself to every e-mail address listed in the computers address book. This worm has apparently been written in Russia.

"This seems to be a poor attempt from a wannabe virus writer to exploit the commemoration of September 11th", comments Mikko Hypponen, Manager of Anti-Virus Research at F-Secure. "However, as the worm seems to crash regularily, it won't go far".

Detailed description of the worm is available at: http://www.f-secure.com/v-descs/chet.shtml

About F-Secure Corporation

F-Secure Corporation is a leading provider of centrally managed security for today's mobile, wireless enterprise. The company offers a full range of award-winning, integrated anti-virus, file encryption, distributed firewall and VPN solutions for workstations, servers, gateways and mobile devices. F-Secure products are uniquely suited for delivery of Security as a Service(tm) which provides invisible, reliable, always-on, and up-to-date security for the most widely distributed user base. Whether provided by corporate IT or delivered by service providers, F-Secure solutions extend policy-based security and instant alerts to all devices where information is created,

stored or accessed. Founded in 1988, F-Secure Corporation is listed on the Helsinki Exchanges [HEX: FSC]. The company is headquartered in Helsinki, Finland with North American head office in San Jose, California, as well as offices worldwide.

For more information, please contact:

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