F-Secure Corporation

82-5235

December 30, 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

SUPPL

Attention: Division of International Corporate Finance

PROCESSED
JAN 22 2003
THOMSON
FINANCIAL

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

pp. Henriitta Mallmann

SEC MAIL PROCESSING
RECEIVED
JAN 07 2003
WASH. D.C. 155 SECTION

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 December 17, 2002

F-Secure Corporation's Data Security Summary for 2002

In 2002 the data security world was characterized by new types of threats. Virus outbreaks in Linux systems, attacks utilizing open source code, breaks into home computers and increasing activity of Asian virus writers kept data security companies busy. Known viruses today amount to some 80,000.

Computer viruses still pose the greatest single problem, even though the number of worldwide outbreaks was clearly smaller in 2002 than in 2001. F-Secure Corporation classifies viruses on a scale called F-Secure Radar according to their severity. The number of alerts of level one, or the most severe types, was nine in 2001. In 2002, the number was mere two: the Slapper network worm attacking Linux systems and the Bugbear e-mail worm attacking Windows systems. Respectively, level two alerts were given 31 and 26 times. The majority of virus cases seen during the year were caused by old viruses, some of which have been out in the wild for a couple of years now.

Even though the number of outbreaks has been smaller than during the previous year, new viruses are detected more or less at the same rate as before. Every month, hundreds of new viruses are found. The total number of known viruses was some 80,000 at the end of year 2002.

One distinct change in 2002 has been the increase in the activity of Asian virus writers, and the number of viruses originating from Asia keeps growing. The most significant originator countries include China, Taiwan and South Korea. Since September 2001, there have been hardly any viruses written in North America: a more strict attitude towards crimes directed at the society has considerably decreased the number of viruses from the US.

Lively e-mail worms

There were two viruses competing for the title of the year's most bothersome virus: Klez and Bugbear. Of these, the Klez virus family has been out in the wild since October 2001 and is still spreading. Bugbear was found in September 2002 and spread all over the world in just a few days. Both Klez and Bugbear are e-mail worms. Also, they both put fake sender name and e-mail address in the "From" field of messages they send. Consequently, innocent persons may be accused of spreading viruses. The owner of the infected computer may be fully unaware of what has happened and is not prompted to clean his or her system. Bugbear was an example of another problem, which became

SEC MAIL PROCESSING
RECEIVED
JAN 07 2003
WASH. D.C. 155 SECTION

widespread in 2002: the inclusion of remote access properties into a virus. Each computer infected by Bugbear can be accessed remotely over the Internet. The attacker can therefore read, delete or edit any files on the infected machine.

Like many other e-mail worms detected during the year, Klez and Bugbear took advantage of the IFRAME vulnerability, thanks to which viruses were able to launch their own attachments while the infected message was read. The IFRAME hole appears to be a big problems even today, though Microsoft has offered a patch to it more than couple of years ago.

Use of file exchange networks and directories

Even though e-mail continued to be the most common route for viruses, other techniques were also seen. For example, the Benjamin, Roron and Lolol worms spread through the Kazaa file exchange network. These viruses try to distribute infected files to the peer-to-peer network by using attractive file names and by relying on the fact that some of the network users cannot make a difference between music or video files and program files.

The Opaserv and Lioten worm, on the other hand, spread from one computer to another through shared directories or folders. When Windows users share their folders with other users, they may not realize that files in those shared folders may be visible to people on the other side of the world. Opaserv looked for unprotected Windows 95 and 98 computers and broke the password protection of shared files, thereby becoming quickly a worldwide problem.

Attacking Linux systems

So far the most widespread Linux virus outbreak was seen in 2002. A network worm named Slapper was first detected on September 14th. It quickly infected thousands of Apache web servers around the world. The virus only infected servers and was mostly not seen by end users at all.

The most interesting characteristic of Slapper was its ability to create a distributed peer-to-peer attack network by means of which the writer of the worm was able to take control of any infected server. This feature was probably created to launch distributed denial-of-service attacks with the help of the worm. F-Secure's specialists managed to disassemble the peer-to-peer protocol used by the worm and the threat posed by the worm was eliminated in a few days. However, there is more to come on this front for certain.

Systems using open source code have been facing other security problems during 2002 as well. Backdoors were hidden in the distribution versions of OpenSSH, tcpdump and libcap programs. Even though these malicious additions could be seen by anyone in the source code, it took days before these changes were noticed in these cases.

Home computers subjected to attacks

Home computers are one of the biggest problems in the data security sector. Because home computers do not normally contain any major secrets their users do not take security as seriously as business users. However, computers are attacked for many other reasons besides theft of information.

Hacking for the sake of fun is increasing all the time. In these cases the attraction is the computer itself, not the data contained by it. A modern home computer has massive capacity: a several gigaherz processor, hundreds of megabytes of memory and dozens of gigabytes of disk space. All this with a continuously open connection to the network through a fast DSL or cable modem. When combined with an operating system supporting true multiprocessing it may be that the owner of the system can be working on his or her computer without noticing that the system is simultaneously accessed by fifty teenagers from different parts of the world downloading the most recently announced movie as an illegal Divx copy. A typical outcome of this kind of free-riding is that a home computer is used to distribute illegal or dubious material without the owner knowing about it. If the computer owner opens protected VPN connections to his or her employer's intranet, the consequences may be really serious.

The huge capacity of home computers may also lead to a situation where they are used as a medium in attacks against networks. When a suitable vulnerability is located in a popular network service, such as Kazaa, ICQ or MSN Messenger, a malicious user may get access to millions of Windows systems through it. An attack network consisting of them would be able to paralyze most of the Internet traffic for long periods. Modern society cannot and should not leave a threat like this without attention.

Mobile world

No mobile or PDA viruses were seen during 2002. In spite of this the security industry continues to research and build security systems in this area. The need for a strong protection of data on hand-held systems keeps on growing.

Because hand-held computers and mobile phones are becoming more and more like traditional computers, the security risks also become more concrete. As the GPRS and other fast mobile data networks get more common in the world, they will be one of objects of network criminals. It is easy to operate anonymously in mobile networks using so-called prepaid subscriptions. Operators play a key role in the security of home computers and mobile devices.

Future

"Attacks against data systems will increase and they will become more and more professional. New, fast network worm technologies may lead into a situation where a worm spreads around the world in just a few minutes after it has been launched. These attacks can be done by hackers, hactivists, industrial spies, terrorist groups or organized crime. Society must be able to function in spite of such network warfare" says Mikko Hypponen, Manager of Anti-Virus Research at F-Secure.

The complete summary is available at F-Secure's www site at http://www.F-Secure.com/2002

For more information, please contact:

Mikko Hyppönen, Manager, Anti-Virus Research
F-Secure Corporation
PO Box 24, FIN-00181 Helsinki
Tel. +358 9 2520 5513, Fax +358 9 2520 5001, Gsm +358 400 648 180
E-mail: Mikko.Hypponen@F-Secure.com http://www.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 November 20, 2002

F-Secure protects US taxpayers' data at IRS

Helsinki, Finland, November 20, 2002 - F-Secure Corporation announces that it has signed an agreement to provide encryption to the US Internal Revenue Service. The F-Secure FileCrypto product is used to protect and encrypt confidential data such as taxpayer information on laptops and desktops.

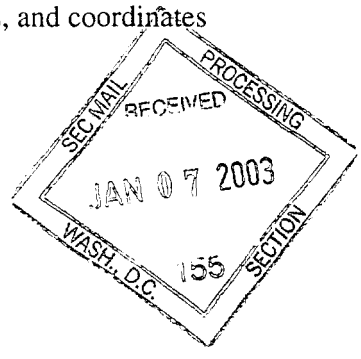
The proliferation of computer hacking and cracking as well as loss and theft of laptops and other equipment have made file level security even more critical. F-Secure FileCrypto is the first and only cryptographic solution based on a FIPS 140-2 certified module. The product is part of F-Secure's comprehensive security portfolio protecting against data theft, intrusions and viruses. F-Secure's products are centrally managed, policy based and transparent to the end user. This enables administrators to enforce organizational security policies and insures that critical information will be protected at all times.

GovConnection Inc. partnered with F-Secure to deliver F-Secure FileCrypto to the IRS. "We feel confident in recommending F-Secure to provide FIPS 140-2 certified security products for our government customers' needs," says Gary Sorkin, President of GovConnection, Inc. "The IRS technology implementation will give taxpayers and corporations absolute assurance that their tax information in the IRS's possession remains intact and unreachable by outsiders."

"At F-Secure, we are very proud of the fact that an organization with high security demands such as IRS has chosen F-Secure as their encryption provider," says Ilkka Starck, Executive VP of the Americas at F-Secure Corporation, San Jose, CA. "Automatic content security solution enables people to work in a more flexible manner without compromising security and confidentiality."

F-Secure was the first company in the world to be granted FIPS 140-2 certification for its security technology. The certification is necessary for successful dealing with US and Canadian governments and agencies. For more information on the certification, see http://csrc.nist.gov/cryptval/140-1/140crt/140crt237.pdf

FIPS-140-1 and FIPS-140-2 are security requirements for cryptographic modules and algorithms. The Computer Security Division at the National Institute of Standards and Technology (NIST) maintains a number of cryptographic standards, and coordinates validation programs for many of those standards.



About F-Secure Corporation

F-Secure Corporation is a leading developer of centrally managed security solutions for the mobile enterprise. The company's award-winning, integrated antivirus, file encryption and network security solutions for handhelds, laptops, desktops, servers, mail servers and firewalls provide centralized policy based management of widely dispersed user communities. Founded in 1988, F-Secure is listed on the Helsinki Stock Exchange [HEX: FSC]. Corporate headquarters is in Helsinki, Finland with North American headquarters in San Jose, California. The company maintains offices in Germany, Japan, Sweden and the United Kingdom, and is supported by a network of VARs and Distributors in over 90 countries around the globe.

For media requests, please contact:

Henrietta Malmari, Communications Assistant
F-Secure Corporation
PL 24
FIN-00181 Helsinki
Phone: +358 9 2520 5315
Mobile: +358 40 575 5646
Fax: +358 9 2520 5017
E-mail: Henrietta.Malmari@F-Secure.com

http://www.F-Secure.com