F-Secure

F-SECURE®

03032594

August 12, 2003

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

82-5035

SUPPL

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

Attention: Division of International Corporate Finance

PROCESSED
OCT 09 2003
THOMSON FINANCIAL

SEC MAIL PROCESSING
RECEIVED
OCT 06 2003
WASH. D.C. 155 SECTION

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,

dlw 10/8

Jaana Sirkiä
Corporate communicator

P Henrietta Malmari

Press release

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 12, 2003

World's First RPC Worm found

Experts forecast large-scale infections

SEC MAIL PROCESSING
RECEIVED
OCT 06 2003
WASH. D.C. 155 SECTION

F-Secure is issuing an international alert on a new network worm known as Lovsan or Msblast. This worm spreads to Windows servers and workstations as MSBLAST.EXE, using the well-known RPC hole. The worm will launch an attack against windowsupdate.com on 16th of August.

"The IT security industry has been waiting in horror for a new major worm to appear since the RPC/DCOM hole was found on the 16th of July", says Mikko Hypponen, Director of Anti-Virus Research at F-Secure. "Now it's here".

First sample of this worm was received to F-Secure Anti-Virus Research Labs at 20:22 GMT on 11th of August, 2003. The worm spreads in a 6176 byte executable named MSBLAST.EXE to Windows 2000 and Windows XP systems unless recent Windows security patches have been applied.

The worm will scan addresses in the internet to locate vulnerable Windows machines. Once found, it will copy itself over and modify the system so the worm will be executed every time the machine is started. The worm will keep on replicating from every infected machine.

The Lovsan worm contains these texts:

I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your software!!

"There seems to be clear attack routine in the worm", observes Hypponen. On the 16th of August the worm will start a distributed denial-of-service attack against the windowsupdate.com server. "If our initial spreading data is correct and the worm continues to spread fast, the attack might take down the whole Windows Update service".

QUESTIONS AND ANSWERS ON THE LOVSAN WORM

Q: What makes this worm special?
A: It spreads using the MS03-026 DCOM/RPC hole, "Buffer Overrun In RPC Interface" - which is one of the most common security holes in the world right now.

Q: When was it found?
A: First sample of this worm was received to F-Secure Virus Research Labs at 20:22

GMT on 11th of August, 2003.

Q: How does it spread?
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: Which Windows platforms are vulnerable?
A: At least Windows 2000 and Windows XP. It seems that Windows NT 4 and Windows 2003 might be affected, but this has not yet been confirmed either way.

Q: Does Microsoft have a patch to close this hole?
A: Yes, at http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

Q: How many machines it could infect?
A: There are potentially tens of millions of machines to infect. For reference, Slammer worm only had around 100,000 potential SQL servers to infect and even Code Red had less than 2 million machines IIS web servers. Then again, most of the workstations with the RPC hole are behind firewalls.

Q: Could it get behind firewalls?
A: In several ways. There might holes in the firewall rules, or people might make direct unfiltered connections from behind the firewall (with modems or WLAN). Or somebody might just carry an infected laptop to the company premises.

Q: Will there be different versions of this worm?
A: Most likely there will be several variants, yes.

Q: What kind of emails does this worm send?
A: None. This is not an email worm. It never sends any emails.

Q: Is this a 'Warhol' worm?
A: No. It has no hitlist and it doesn't spread as fast as for example the Slammer worm did in February 2003.

Q: Does it do direct damage to infected machines?
A: No. But it does try to take down windowsupdate.com after midnight local time on 16th of August.

Q: Where is this worm from?
A: We don't know.

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/msblast.shtml

F-Secure Anti-Virus can detect and stop the Lovsan 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 Amercan 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 licening 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, Antivirus Research
PL 24
FIN-00181 Helsinki
Tel +358 9 2520 5513
Fax. +358 9 2520 5001
GSM +358 400 648 180
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