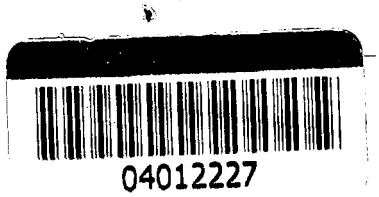
F-Secure



SUPPL 82-5035

December 19, 2003

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,

dlw 1/20

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

FOR RELEASE December 15, 2003

F-Secure Corporation's Data Security Summary for 2003

The Year of The Worm

Overview

The year 2003 has clearly been the worst in virus history. At the same time, the entire computer virus phenomenon saw its 20th birthday this year. New trends in 2003 were primarily the way spammers began to use viruses as a tool and how several critical infrastructure systems suffered from the consequences of virus outbreaks. The network worm problems encountered during the year have shown how important it is to equip every single computer with a personal firewall. The number of known viruses is at the moment some 90,000.

Virus problems seem to arrive in waves. Year 2001 was a very busy virus year, while 2002 was clearly quieter. Unfortunately, 2003 exceeded previous years in terms of both the number of virus outbreaks as well as their extensiveness and severity.

F-Secure Corporation classifies viruses on a scale called Radar according to their severity. The number of alerts of level one, or the most severe types, was seven in 2003. In 2002 the number was only two. The number of level two alerts was 25 in 2002 and 28 in 2003. Some of the 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.

When we look at the year as a whole, five cases were in a leaguer of their own: Slammer, Bugbear.B, Blaster, Sobig.F and Swen.

Case Slammer

The explosive outburst of the network worm Slammer (or Sapphire) in January 2003 was the biggest attack against the Internet ever. Slammer was a fully automatic network worm and it was able to infect computers directly over a network connection. In other words, it did not spread through e-mail like many other major outbreaks.

Slammer infected Windows systems with Microsoft SQL database software installed on them. Many widely used office applications automatically install this software on the systems. However, most of the computers around the world did not have it installed and Slammer could not infect them. In fact, the main problem was not that Slammer would have

infected that many systems, but the way it aggressively looked for new victims in the network and caused an enormous amount of network traffic.

In theory, there are some 4 billion public IP addresses on the Internet. The Slammer worm was released on January 25, 2003 around 04:31 UTC. By 04:45 it had scanned through all Internet addresses – in less than 15 minutes! This operation can be compared to an automatic system dialing all available phone numbers in the world in 15 minutes. As on the net, only a small number of phones would answer the call but the lines would certainly be congested.

The network jam caused by Slammer had dramatic consequences, which are discussed in more detail further on in this summary.

Case Bugbear.B

The e-mail worm Bugbear.B was detected on June 5. It was a successor of the widely spread Bugbear.A.

This virus was interesting because it tried to steal information from banks and other financial institutions. When Bugbear.B infected a computer, it checked if the affected computer was located in an internal network of a known financial institution. If this was the case, the virus gathered information and passwords from the system and sent them to ten pre-defined e-mail addresses.

To this end, the worm carried a list of network addresses of more than 1300 banks. Among them were network addresses of American, African, Australian, Asian and European banks. As soon as this functionality was discovered, F-Secure warned the listed financial institutions about the potential threat. The response time of the F-Secure Anti-Virus Research Unit was 3 hours 59 minutes from the detection of the worm to the release of an anti-virus update. F-Secure also published a free tool to clean systems affected by Bugbear.B.

The Bugbear.B worm propagated widely during the summer, but the amount of actual damage remains unknown.

Case Blaster

Blaster (or Lovsan or MSBlast), which was detected on August 11, was also an automatic network worm and basically similar to Slammer, but it was able to infect a significantly larger amount of computers. The vulnerability used by Blaster affected millions of Windows 2000 and Windows XP users, whose Windows operating system had not been appropriately updated. Blaster, however, propagated at a considerably slower speed than Slammer, yet it was significantly faster than viruses spreading through e-mail.

The RPC hole used by Blaster had been detected on July 16, less than a month earlier. As July – August is the main summer holiday season, many organizations had failed to install security patches before the worm appeared.

The first symptom of the Blaster virus was that Windows XP users started seeing a message about the shutdown of the RPC process and about Windows restarting in 60 seconds. After the system had restarted, the same message often appeared again in a few minutes. This was repeated until the user disconnected the computer from the Internet or updated Windows. It took some 10 minutes to download the security updates from Microsoft's

windowsupdate.com service. Many users running into the problem were unable to update the operating system as the system restarted over and over again because of the worm and the downloading process was interrupted.

The writer of the Blaster worm was probably a young hacker who wanted to express his or her hostility towards Microsoft. An indication of this is the text found inside the virus: "billy gates why do you make this possible? Stop making money and fix your software!!", and the fact that the worm was programmed to start its denial of service attack against the windowsupdate.com site five days after it was found. Since windowsupdate.com was not Microsoft's official update site, the company responded by removing the site from the Internet a few hours before the attack started, while addresses like windowsupdate.microsoft.com remained in operation. However, the virus got what it wanted: windowsupdate.com does not exist any more.

One of the consequences of the Blaster worm was that some competing virus writer created a virus fighting against Blaster. This virus, known as Welchi or Nachi, infected computers already infected by Blaster. As soon as Welchi had entered a system it destroyed Blaster and tried to download and install Windows security updates. In other words, it was an anti-virus virus. Too bad that the cure was worse than the disease: Welchi generated considerably more network traffic than Blaster and was the reason for most of the severe system outages in companies in mid-August.

Both Blaster and Welchi hampered the operation of important systems, such as automatic teller machines and public transportation. These are discussed in more detail in a separate section. However, it is important to note that especially Welchi still continues to spread. After several months since the actual epidemic, an unprotected Windows machine can get infected in just minutes when connected to network.

One of F-Secure's honeypot machines caught the first known sample of the Blaster worm on Monday evening, August 11, 2003. F-Secure warned CERT (Computer Emergency Response Team) on the new threat within an hour. The response time of F-Secure's Anti-Virus Research Team was 2 hours 3 minutes from the detection of the worm to the release of an anti-virus update. F-Secure also made available a free tool to clean systems affected by Blaster or Welchi.

Case Sobig.F

Only a week after Blaster was detected things started happening again. Early on Tuesday morning on August 19, 2003 F-Secure received a sample of a new e-mail worm. This turned out to be the latest addition to the Sobig virus family. It was the worst e-mail worm ever, sending over 300 million infected e-mail messages around the world.

The first virus belonging to the Sobig family was found in January 2003. New versions appeared at regular intervals. It was odd, however, that the different versions were programmed to stop spreading after a few weeks. Later, it was understood that this was a simple version management technique: the writers of Sobig wanted to remove old worm versions from the market to be able to release a new, enhanced version.

In addition to spreading through e-mail, different versions of Sobig had another common factor, too: they waited for a couple of days after infecting a machine and then turned affected machines into e-mail proxy servers. The reason soon became apparent: spammers, or organizations sending bulk e-mail ads, used these proxies, which Sobig had created, to

redistribute spam on a massive scale. Computers of innocent home users were taken over with the help of the worm and soon they were used to send hundreds of thousands of questionable advertisements without the owner being aware of this.

It is likely that there's a virus writer group behind Sobig. They planned the operation, then used the worm to infect a huge number of computers and then sold various spammer groups lists of proxy servers which would be open for spreading spam. It was clearly a business operation.

After Sobig.F was detected on Tuesday morning, F-Secure's Anti-Virus Research Team released its anti-virus update in 2 hours and 33 minutes. Soon after this the global flood of e-mail messages created by Sobig.F started. Some individuals reported that they had received thousands of infected messages in a day. Large organizations saw hundreds of thousands of messages, and some e-mail systems collapsed under the heavy load. AOL reported stopping more than 20 million infected messages by Wednesday, the 20th of August.

F-Secure's researchers continued studying the code of the worm and eventually found a functionality hidden in the virus code: computers infected by the worm were synchronized with an atomic clock to activate on Friday, August 22nd at 19:00 UTC. At this clock strike they would contact one of 20 pre-defined computers around the world and receive more specific instructions from them. When this functionality was found, F-Secure had less than 30 hours to disconnect those 20 computers from the net in order to stop the activation. By working in close co-operation with Internet operators, CERT units and the FBI, this was accomplished just in time. The last computer that needed to be disconnected was shut down only 15 minutes before the deadline.

F-Secure made available a free tool to remove the Sobig.F worm from infected machines. The tool proved to be very popular and it was downloaded hundreds of thousands of times during the Sobig.F week.

Case Swen

The Swen e-mail worm was detected on September 18, 2003, but the problems arising from it continued for weeks in e-mail systems around the world. E-mail messages sent by Swen were forged to look like genuine Microsoft safety updates. It is good to remember that Microsoft never sends updates as e-mail attachments.

For end users, Swen was not as visible a harm as Sobig.F. Instead, it caused severe problems to Internet operators. The reason was that the majority of the e-mails sent by Swen used incorrect e-mail addresses. Thus, the end users never saw them, but they generated error messages and the messages bounced back to the operators' networks. End result: several large Internet operators reported severe delays in email delivery. In some cases emails were delayed by weeks.

The problems caused by Swen were a concrete indication of how important the e-mail has become as a communications channel in only a few years.

The response time of F-Secure's Anti-Virus Research Team was 3 hours 57 minutes from the detection of the worm to the release of an anti-virus update. F-Secure also published a free tool to clean systems affected by the Swen.

Virus writers and spammers working together

One of the interesting trends during the year was that virus writers and spammers have found each other. The most conspicuous example of this was the Sobig virus family, but there are actually at least four ways in which the spammers take advantage of viruses:

- Collection of e-mail addresses
  - Spammers need e-mail addresses to send their advertisements to. Worms collect addresses from the user's address book and files. Additionally, viruses like Swen display false error messages to the users and ask them to enter their e-mail address and password for an error report – which they then forward to the virus writer.

- Setting up e-mail servers
  - Malware, such as Sobig, Slanper and Trojanproxy install a proxy or relay program on the user's computer. These are then used to relay spam through the infected home computer. This prevents anyone from tracking the actual sender of the spam. It is estimated that currently more than half of all spam mail is circulated through home computers infected like this.

- Setting up web servers for offending material
  - A large part of spam messages is connected to the advertising of products that are on the verge of being illegal. It is not easy for spammers to find www servers where they could maintain these kinds of sites. For example, the Fizzer worm installs a web server on infected machines. The outcome may be that a home computer of an unsuspecting user may serve as a web service offering hard porn.

- Attacks against anti-spam services
  - The worst enemies of a spammer are anti-spam activists. Variations of the Mimail worm, for example, activated massive denial-of-service attacks from infected computers against different anti-spam sites trying to shut them down or close them. They have been successful to some extent, too: four known anti-spam sites had to stop their operations because of the attacks. Nevertheless, the most important anti-spam operator, Spamhaus, is still up and running in spite of the attacks from the spammers.

Spamming is profitable. Spammers have considerable interests to defend, and they can also invest large amounts of money in the continuation of their operations.

"Suddenly the nature of our counterpart has changed completely," says Mikko Hypponen, Director of Anti-Virus Research at F-Secure. "Our enemy used to be amateurs who wrote viruses for the fun of it. Now viruses are generated by spammer gangs, who develop viruses professionally".

Viruses and critical infrastructure

Year 2003 saw virus induced problems in real-life systems which were unprecedented in their severity. The main culprits were Slammer, Blaster and Welchi. Additionally, the e-mail outages caused by Sobig.F and Swen hampered the operation of corporate systems.

The network congestion caused by Slammer dramatically slowed down the network traffic of the entire Internet. One of the world's largest automatic teller machine networks crashed and remained inoperative over the whole weekend. Many international airports reported that their air control systems slowed down. Emergency phone systems were reported to have problems in different parts of the USA. The virus even managed to enter the internal network of the Davis-Besse nuclear power plant in Ohio, taking down the computer monitoring the state of the nuclear reactor.

The RPC traffic created by Blaster caused big problems worldwide. Problems were reported in banking systems and in the networks or large system integrators. Also, several airlines reported problems in their systems caused by Blaster and Welchi, and flights had to be canceled. Welchi also infected Windows XP-based automatic teller machines made by Diebold, which hampered monetary transactions. The operation of the US State Department's visa system suffered. The rail company CSX reported that the virus had interfered with the train signaling systems stopping all passenger and freight traffic. As a result of this, all commuter trains around the US capital stopped on their tracks.

The media has given a lot of attention to the indirect effects of Blaster on the power blackout in the northeastern USA which occurred during the outbreak week. According to the intermediate report of the blackout investigative committee there were four main reasons behind the power failure, one of them being specifically computer problems. F-Secure believes that these problems were to a great extent caused by the Blaster. A separate official committee is still investigating this issue in detail.

It is important to note that even though the system problems caused by Slammer and Blaster were truly considerable, they were only byproducts of the worms. The worms only tried to propagate: they were not intended to affect critical systems. The viruses affected environments that had nothing to do with Windows: the massive network traffic caused by the worms alone disrupted their operation.

Network worms, such as Slammer, manage to spread into virtually isolated systems thanks to their effective and systematic operation: Slammer exhaustively scans every single Internet address it can reach. Therefore, if a critical computer is connected to any device which is linked to some public network, even indirectly, Slammer will find it sooner or later.

In principle, SQL or RPC-based worms should never be able to enter company intranets through the public Internet, because firewalls should prevent this type of traffic. Sometimes viruses were able to pass through the firewall because of errors in configuration, but a typical route to the internal networks was an employee's laptop that had been infected at home or for example in a hotel network. When the infected machine was taken back to the office, the worm was able to spread like wildfire in the company intranet. There have also been cases where a WLAN network card inserted in a company PC contacted a public network at the same time as the machine was connected to the intranet through a network cable.

Not all problems in critical systems were caused by viruses. In October 2003, a 19 year old British hacker was tried in court, because he had crashed information systems of the Port of Houston in USA. It was assumed that the reason behind the attack was jealousy.

Iraq

The war in Iraq, which started in March, had an indirect effect also on public information

networks. The phenomena were not caused by official network warfare between USA or Iraq forces, but by the activities of individual hackers, wanting to publish their own messages.

People behind the attacks were either patriotic hackers, extremists, or pacifists. The methods used in the attacks were mainly web defacements and to some extent also viruses.

Attacks seen in March included:
- Denial-of-service attack against the web site of Al-Jazeera TV network
- denial-of-service attack against the web site of the British prime minister
- several "Kill Saddam" defacement attacks
- attacks quoting the Koran against US and British web sites
- repeated attacks against the www sites of the US Army, Navy and Air Forces
- several computer viruses, which were spreading an anti-war message or tried in other ways to take advantage of the situation, such as Ganda, Lioten, Prune and Vote.D.

The number of defacements was more than 20 times higher during the week the war started if compared to the previous week.

Samples of network defacements during the Iraqi war are available at:
http://www.f-secure.com/virus-info/iraq.shtml

Other observations

The virus problems in 2003 concentrated on the Windows platform. No new major viruses were detected in the Linux or Mac environment. No viruses aimed at PDAs or mobile phones were encountered either.

During the spring and fall, there were several court cases in UK, where the accused defended themselves by explaining that even though their computers had been involved in crimes, the body behind the crime was not the owner of the computer but a virus, which had infected the system.

Ways to protect computers

F-Secure recommends four basic methods to protect computers:

1. Apply operating system patches regularly
2. Switch the computer off or disconnect the network cable whenever the computer is not in use
3. Install an automatically updated anti-virus program.
4. Install a personal firewall - this concerns also desktop computers inside company's internal network

In September, F-Secure announced the new **F-Secure Anti-Virus Client Security** software. It consists of an anti-virus program and integrated firewall software as well as intrusion control and application control. With this application, firewall is added to each computer along with the anti-virus system.

Outsourcing security to a service provider or Internet operator has proved an efficient way for home users or small companies to solve everyday data security problems. F-Secure

continues to work together with operators in this field to provide applicable solutions.

We would also like to point out that the only way to protect critical computer systems is to keep disconnected from all networks.

Future

Attacks against data systems will increase and become more and more professional. The virus technology used by spammers is threatening to change the entire Internet into a battle field. The people behind the network attacks are hackers, activists, industrial spies, terrorist groups and organized crime, but the modern society must be able to function in spite of attacks against data security.

"I'm afraid there will be a lot of work for us also in 2004", says Mikko Hypponen, Director of Anti-Virus Research at F-Secure.

Appendix: Major security events in 2003

January
- The Slammer worm attacked: the most biggest attack against the Internet ever
- The first member of the Sobig virus family, Sobig.A was found
- Dedicated to Canadian singer Avril Lavigne, Lirva.A and Lirva.B worms spread widely through e-mail, file sharing and peer-to-peer networks

February
- Lovgate.A out in the wild. Lovgate guessed user passwords and infects the computer through network sharing or e-mail

March
- Deloader.A and new variants of Lovgate spreading. They both allot user passwords
- The Ganda e-mail worm, which took advantage of the Iraq war was going around

May
- The Fizzer worm spread all over the world. The virus is strongly linked to spammers.
- Second and third variants of Sobig (B and C) are detected. They both spread very extensively

June
- Bugbear.B attacking banks spreads around the word.
- Fourth and fifth variant of Sobig (D and E) are detected. The D version fails to spread. On the other hand, version E becomes the most widely spreading variant this far

August
- The worst virus month in history
- The first member of the Mimail virus family is detected
- Blaster spreads globally
- Welchi spreads globally
- Sobig.F spreads globally

September
- The Swen worm is detected. The e-mail problems caused by it go on for months
- Several new viruses are detected on the anniversary of the terror attacks of September 11, for example Mimail.B and Vote.K, which contain text "WORLD TRADE CENTER, REVENGE"

October
- The Mimail.C worm is detected and launches denial of service attacks

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

- The Sober worm sends infected e-mail messages, which look as if they originated from anti-virus companies

November

- Ten new variants of the Mimail virus were detected during the month. The variants attacked anti-spam sites, among others, or stole users' credit card details
- At least four significant servers of Linux developers were broken into and distribution packages or source codes were modified. In some cases it took several weeks before the problem was detected

More information on the above mentioned viruses can be found at: http://www.f-secure.com/v-descs/
Pictures and screenshots of the viruses can be found at: http://www.f-secure.com/virus-info/v-pics/

For more information, please contact:

Mikko Hypponen, Director of Anti-Virus Research
F-Secure Corporation
Box 24
FIN-00181 Helsinki
Finland
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 December 17, 2003

TeliaSonera expands F-Secure's Security as a Service concept also to small and medium businesses

In addition to offering anti-virus and firewall services to home users, TeliaSonera now offers the workstation-based services also to small and medium businesses. The service is based on F-Secure's Security as a Service concept, which includes automatic data security updates directly from F-Secure's server.

Sonera Desktop Security, which is the name of the service, is especially suited for small and medium businesses that do not currently run any anti-virus or firewall programs. The new security service contains a workstation-based software that effectively helps to prevent all attempted virus and hacking attacks.

Sonera Desktop Security also enables different client based security rules to be defined for adjusting the network traffic between the Internet and the workstation. The service includes pre-configured virus and firewall rules, which help when first taking the service into use. Both the software as well as the manual are in Finnish.

"The importance of antivirus and firewall solutions is growing due to new very fast worms, trojan horses and other malicious viruses. Protection should be extended to cover workstations, servers and corporate networks. Together with F-Secure we can cost-efficiently offer the most efficient security solutions to our enterprise customers' workstations," says Pasi Tolonen, Director, TeliaSonera Finland Oyj.

"We are very happy to extend our cooperation to offer data security solutions also to TeliaSonera's enterprise customers. Internet Service Providers need to be able to respond to the changing environmental needs and to take the responsibility to offer easy-to-use solutions to safe use of the Internet. TeliaSonera has successfully offered F-Secure's security products through Security as a Service concept to consumers already for years and we are constantly developing our services", says Kimmo Alkio, COO of F-Secure Corporation.

For more information, please contact:

F-Secure Oy
Björn Werling
Director, Key Account Management

Service Provider Solutions
Tel. +358 9 2520 5670
E-mail: bjorn.werling@f-secure.com

TeliaSonera Oyj
Tommi Vänninen, Product Manager
Tel. +358 400 291 050
E-mail: tommi.vanninen@teliasonera.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 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 licencing and distribution agreements, the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia.

www.F-Secure.com

TeliaSonera Finland Oyj, the Finnish profit centre of TeliaSonera, offers products and services under the Sonera brand.

TeliaSonera is the leading telecommunications company in the Nordic and Baltic regions. At the end of September 2003 TeliaSonera had 11,558.000 mobile customers and 8,025,000 fixed customers and 1,555,000 internet customers in its home markets. Outside the home markets TeliaSonera has extensive interests in the growth markets in Russia, Turkey and Eurasia. TeliaSonera is listed on the Stockholm Exchange, the Helsinki Exchanges and the Nasdaq Stock Market in the USA. Pro forma net sales January-September 2003 amounted to SEK 60,7 billion (EUR 6.8 billion). The number of employees was 26,216.

www.teliasonera.com