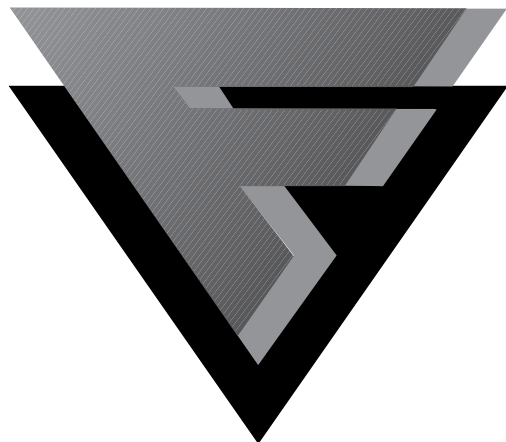


F-SECURE



Update Bulletin 4.07

Dear Customer,

Once again we're living exciting times in our company. In December 1999, our shareholders approved the proposal to officially change the public name from Data Fellows Corporation to F-Secure Corporation.

The Data Fellows name was well-known in some parts of the world, but our F-Secure brand was best known globally. The company's new name, F-Secure Corporation, is designed to better capture the key attributes of the company's core business — security for mobile, distributed enterprises — and to further build up the current success of its F-Secure brand and products. The company is headquartered in Finland with North American headquarters in San Jose, California, as well as offices in Canada, China, Germany, Hong Kong, France, Japan, Sweden and the United Kingdom.

We would also like to use this opportunity to welcome two new members to the F-Secure Board of Directors: Mr. Olli-Pekka Kallasvuo of Nokia and Mr. Kaj-Erik Relander of Sonera Corporation.

With these new additions and the new name, we're ready to take on the world. Join us!

Best Regards,

A handwritten signature in black ink, appearing to read 'Tanya'.

Tanya Candia
Vice President of Worldwide Marketing

Contents

Product News	2
Support for F-Secure Anti-Virus 4 extended.....	2
F-Secure Anti-Virus for Microsoft Exchange released	2
F-Secure Anti-Virus for MIMESweeper announced	3
Support for Windows 2000 announced	3
Support for Windows NT 3.50 discontinued	3
F-Secure to utilize iD2 Technologies' Smart Card authentication	4
F-Secure SSH Client 3.0 Enhanced Version released	4
Virus News	5
First Windows 2000 virus found	5
Plage 2000 Worm	5
W97M/Wallpaper	6
JS/The_Fly	7
VBS/BubbleBoy	8
Frequently Asked Questions & Answers	9
F-Secure Anti-Virus Updates	11
FSUPDATE	11
F-Secure BackWeb	11
What's New in F-Secure Anti-Virus Release 4.07	12
What's New in F-Secure Anti-Virus Release 5.01 build 5364	12
Fixed Problems	12
Known Problems	12

Copyright © 2000 F-Secure Corporation. All Rights Reserved. This material may be freely quoted as long as the source is mentioned.

F-Secure Anti-Virus

Update Bulletin 4.07

Product News

Support for F-Secure Anti-Virus 4 extended

F-Secure Anti-Virus 4 is based on anti-virus technology that is well-established and has won many awards over the past eight years. We are committed to maintaining this version until June 2000, extending the life of this version by a few more months, as requested by long-time customers of the product.

However, the future of F-Secure Anti-Virus development is with Release 5, which provides many new features and important benefits on top of the best-of-breed anti-virus technology inherited from Release 4.

F-Secure Anti-Virus 5.0 is ready for you to install from this CD-ROM. Please note that you'll have to uninstall F-Secure Anti-Virus 4 first if it's on the system.

The next new major version, F-Secure Anti-Virus 5.1, will support automatic upgrading from version 4 to version 5, making the upgrade a lot easier for customers currently running F-Secure Anti-Virus 4.

Please see the Upgrade Guide for more information:

<http://www.F-Secure.com/products/tech-info/fsav-migration-plan-4-to-5.pdf>

F-Secure Anti-Virus for Microsoft Exchange released

The F-Secure Anti-Virus Content Scanner product family gains a new member in F-Secure Anti-Virus for Microsoft Exchange. The new release, version 5.0 build 29, is available on this CD-ROM. There is also a patch available at <ftp://ftp.F-Secure.com/customer/release/>, which updates the agent to build 32.

F-Secure Anti-Virus for Microsoft Exchange protects e-mail users in real-time from malicious code found in server internal messages, incoming messages, outgoing messages and public folders. The product also supports on-demand scanning of mailboxes and public folders.

F-Secure Anti-Virus for Microsoft Exchange sends all messages that can contain a virus to the F-Secure Anti-Virus Content Scanner Server, which is the center for all of the Content Scanner products. The Content Scanner Server accepts connections from different agents, including CVP-compliant firewalls, Agent for Microsoft Exchange, and Agent for Lotus Domino.

F-Secure Framework provides F-Secure Anti-Virus for Microsoft Exchange with centralized policy-based management features, which make the product easy to deploy and manage in corporate environments.

F-Secure Anti-Virus for Microsoft Exchange is managed remotely with F-Secure Administrator. With its graphical user interface, this management console provides a centralized view of the domains and hosts in your network and lets you configure the security policies of all F-Secure components. F-Secure Administrator also allows you to view the status of F-Secure components.

F-Secure Anti-Virus for Microsoft Exchange uses the award-winning F-Secure Anti-Virus for Windows virus scanner, with its three scanning engines, to ensure the highest possible detection rate and disinfection capability.

Clients currently running F-Secure Mail Gateway for Internet can update to the new product at no cost by contacting their local F-Secure partner.

F-Secure Anti-Virus Total Suite customers with a valid maintenance contract get a license for this product automatically.

F-Secure Anti-Virus for MIMESweeper announced

F-Secure Anti-Virus for MIMESweeper enables you to combine F-Secure Anti-Virus with Content Technologies' MAILsweeper for SMTP 4.1 or later.

The integration module necessary for combining MAILsweeper with F-Secure Anti-Virus is available for download at:

<http://www.mimesweeper.com/downloads/utills.htm>

This integration module allows F-Secure Anti-Virus Content Scanner for MIMESweeper 5.0 or later to be used with MAILsweeper for SMTP Version 4.1. It works via the fast kernel-level Gatekeeper Handler API.

This product combination replaces F-Secure Anti-Virus Mail Gateway for Internet, which has been discontinued.

Customers with a valid maintenance contract for F-Secure Anti-Virus Mail Gateway for Internet can upgrade from the old product to F-Secure Anti-Virus for MIMESweeper by purchasing a new license for MAILsweeper 4.1 from Content Technologies at a special price. Please contact your local Content Technologies supplier for more information. To find the supplier closest to you, go to:

USA:
<http://www.us.mimesweeper.com/contact/>

Europe:
<http://www.mimesweeper.com/contact/>

Asia:
<http://www.mimesweeper.com.au/contact/>

Japan:
<http://www.contenttechnologies.com/japan/>

F-Secure provides these customers with a license for the F-Secure Anti-Virus for MIMESweeper module at no cost.

Customers who already have MAILsweeper for SMTP 4.1 or later can purchase the F-Secure Anti-Virus for MIMESweeper product and integrate the two with the integration module, which is available at no cost at the Content Technologies web site.

Support for Windows 2000 announced

F-Secure Anti-Virus 5 currently supports Windows 95, 98, and NT 4.0.

Support for Windows 2000 will be available 60 days after the release of Windows 2000. Windows 2000 is scheduled for release in February 2000.

F-Secure Anti-Virus 4 will not run under Windows 2000. If you plan to migrate to Windows 2000, that would be a good time to switch to F-Secure Anti-Virus 5.

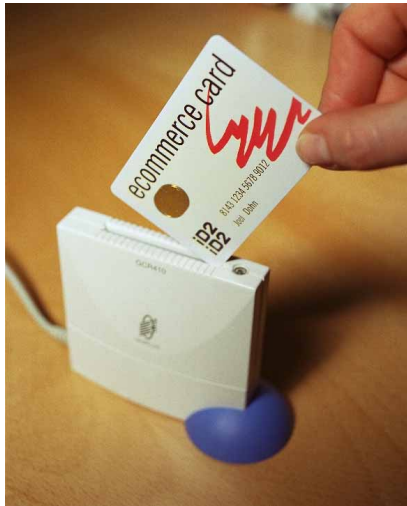
Customers who would like to test the beta version of F-Secure Anti-Virus for Windows 2000 should contact fsav-beta-2000@F-Secure.com.

Support for Windows NT 3.50 discontinued

Microsoft has announced that Windows NT 3.50 is not year 2000 compliant.

While there are ways to make Windows NT 3.50 work in the year 2000, F-Secure Corporation will no longer support it and F-Secure Anti-Virus for Windows NT 3.50 has been discontinued. Version 4.07 is the last version that will work under Windows NT 3.50. Customers are encouraged to upgrade to a newer version of Windows NT.

F-Secure to utilize iD2 Technologies' Smart Card authentication



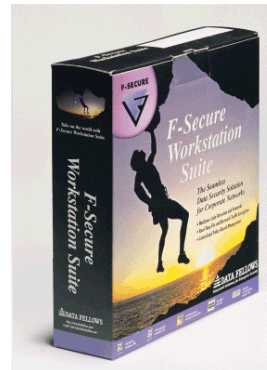
iD2 Technologies' smart card user authentication technology is being integrated into F-Secure security solutions. The first product to include the iD2 technology is the F-Secure VPN+ product suite. The new product will be released in Q1 2000.

With added smart card PKI support, F-Secure VPN+ will help organizations operating virtual private networks to guard against unauthorized network access without inhibiting remote access by authorized users.

"More and more people now work remotely and depend on their company's VPN to access their files," says Bjorn Gustavsson, President of iD2 Technologies. "However, unsecured VPNs run the risk of exposing intellectual property to people outside of the organization. Security solutions such as F-Secure VPN+ are essential in establishing secure 'tunnels' between corporate LANs that use IP technology. Now, with added user authentication technology, network managers can be sure that the person requesting access to the network is who they say they are," Gustavsson continues.

F-Secure VPN+ is the only security VPN client product in the market that is totally transparent to the end user. The end user need not worry about security settings. The software can be installed remotely by the central network administrator, and security management can even be outsourced to a service company. This makes the combination of the two companies' products very powerful in a corporate environment and for service providers. The solutions can be customized, offering support for a broad range of hardware.

F-Secure SSH Client 3.0 Enhanced Version released



A new version of the secure connections software, F-Secure SSH Client 3.0, has been released. The new version has a renewed look and feel. Several enhancements have been made, such as a new Key

Registration Wizard that helps the transfer of public keys to remote hosts, and the capability of creating TCP tunnels while a session is open. Several security improvements have also been added, such as clearing used host and user names, and clearing the screen and scrollbar buffer. The product now supports the new CAST128 algorithm, along with 3DES, Blowfish TwoFish, ArcFour, and DES.

A new version of F-Secure SSH server 2.0.13.1 for all major UNIX platforms was released simultaneously with F-Secure SSH Client 3.0. The new F-Secure SSH Client 3.0 is based on SSH protocol version 2.0 and is fully compatible with all versions of F-Secure SSH Server 2.x.

Virus News

Virus descriptions by Katrin Tocheva, Alexey Podrezov, Sami Rautiainen, Eugene Kaspersky and Mikko Hyppönen

First Windows 2000 virus found

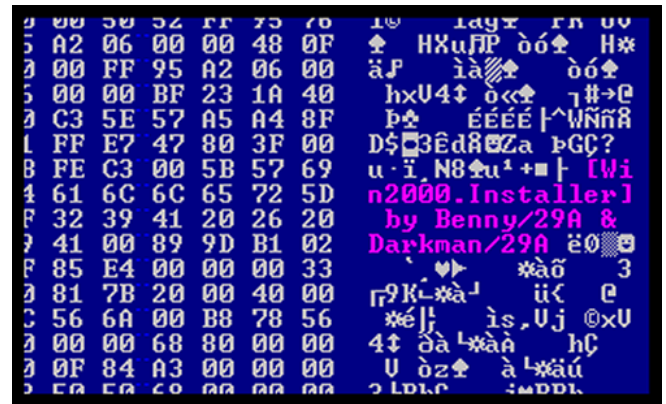
The first Windows 2000 virus was found in early January 2000, well before the operating system itself was released.

The new virus is called Win2K.Inta or Win2000.Install. It appears to be written by the 29A virus group. It operates only under Windows 2000 and is not designed to operate under older versions of Windows.

F-Secure has received no reports that this virus is in the wild, and it is not considered a big threat. The most important feature of the virus is its capability to spread under the new operating system. "Now we can expect virus writers to include Windows 2000 compatibility as a standard feature in new viruses," comments Mikko Hyppönen, Manager of Anti-Virus Research at F-Secure.

Win2K.Inta works by infecting program files, and it spreads from one computer to another when these files are exchanged. The infected files do not grow in size. The virus infects files with the following extensions: EXE, COM, DLL, ACM, AX, CNV, CPL, DRV, MPD, OCX, PCI, SCR, SYS, TSP, TLB, VWP, WPC, and MSI. This list includes several classes of programs that were not previously susceptible to virus infection. For example, this virus will analyze Microsoft Windows Installer files (MSI files), scan them for embedded programs, and infect them.

The virus contains the following text string, which is never displayed:



Plage 2000 Worm

The Plage 2000 worm was first found published on some virus distribution sites in early January 2000. Later it was found in the wild in several countries, including Finland.

The worm itself is a Windows program over 100kB in size. The worm has a WinZip icon pretending to be a self-extracting ZIP archive.

The Plage worm arrives as an e-mail attachment and when run, it installs itself to the system as INETD.EXE in the Windows folder. The worm then modifies the WIN.INI file and the registry so that it runs during subsequent Windows sessions. Being active in memory, the worm communicates with MAPI-compatible e-mail browsers, looks for unanswered messages and sends replies to them. The worm's reply message looks like an ordinary auto-reply that many people use when they can't read their e-mails:

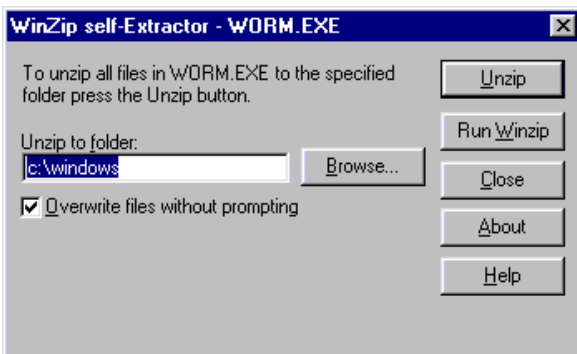
```
P2000 Mail auto-reply:
' I'll try to reply as soon as
possible.
Take a look to the attachment and
send me your opinion! '
> Get your FREE P2000 Mail now! <
```

The worm's body is always attached to the message. The file name of the attachment

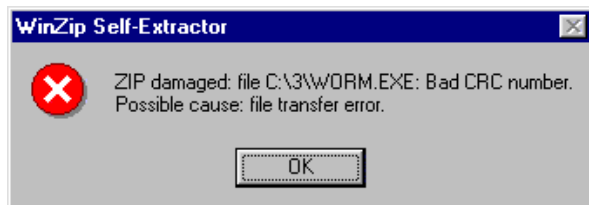
is randomly selected by the worm from the following variants:

pics.exe	images.exe
joke.exe	PSPGame.exe
news_doc.exe	hamster.exe
tamagotxi.exe	searchURL.exe
SETUP.EXE	Card.EXE
billgt.exe	midsong.exe
s3msong.exe	docs.exe
humor.exe	fun.exe

When a recipient gets this message and clicks on the attachment (which looks like a ZIP archive), the worm infects his system as well. First the worm displays the following dialog box, which resembles a WinZip Self-Extractor:



When a user clicks on the 'Unzip' or 'Run WinZip' button, the worm displays a fake error message and installs itself to the system:



After this, the worm becomes active and constantly monitors the date and time. Right after midnight on every Wednesday, it tries to display a dialog box with the following picture:



and the following text:

Fight against the plague of inhumanity.
This is Plage 2000 coded by Bumblebee/29a.

The worm does not have any destructive payload.

W97M/Wallpaper

Wallpaper is a Word macro virus. It activates its payload on the 31st day of each month. At this time, it attempts to replace the Windows desktop's wallpaper with a picture of a skull. This picture is saved as c:\windows\temp\sk2.bmp.

It also modifies c:\autoexec.bat and c:\windows\win.ini to perform the changes to the user's desktop.

Depending on the system time, it shows a message box with the skull image:

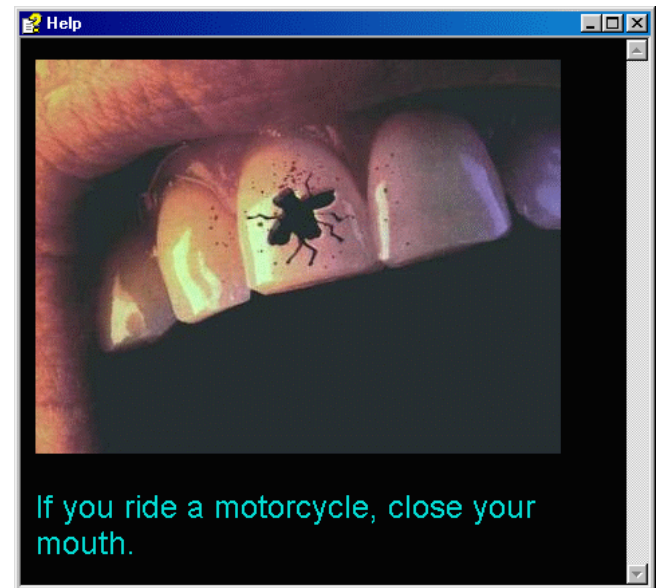


JS/The_Fly

JS/The_Fly is a worm that mass-mails itself. It is written with JavaScript and it is spread in a compiled HTML file. These files use extension "CHM".

When the worm is executed, it first copies itself to the Windows directory as "THE_FLY.CHM" and to the Windows system directory as "DXGFXB3D.DLL".

Next, it opens a window displaying the following picture:



After the window has been displayed, the worm drops a JavaScript file, "MSJSVM.JS", to the Windows system directory. Then it modifies the Windows registry so that this script will be executed during every system startup.

Then JS/The_Fly will use Outlook to mail itself to all recipients in all address books. The message it sends looks as follows:

```
Subject:    Funny thing
Body:      > If you ride a
motorcycle, close your mounth. :)
Attachment: THE_FLY.CHM
```

To hide itself, this worm removes sent mail from the user's "Sent items" folder.

When the system is restarted, the "MSJSVM.JS" script executes. This script will alter mIRC and Pirch98 IRC client settings in a such a way that the worm will be sent each time the user joins an IRC chat channel. It replaces the "script.ini" file from the mIRC installation directory and replaces the "events.ini" file from the Pirch98 installation directory.

Finally, when 30 minutes have elapsed, JS/The_Fly displays the following message box.



VBS/BubbleBoy

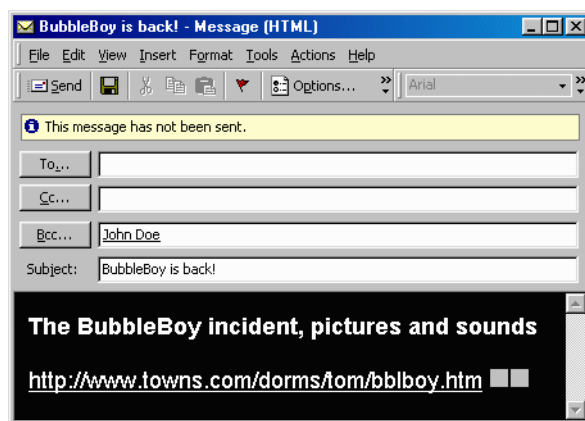
VBS/Bubbleboy is the very first worm that is able to spread via e-mail without opening an attachment. It executes immediately after the user has opened the message in Outlook. In Outlook Express, even viewing the message in "Preview Panel" causes the execution.

The message looks as follows:

From: (name of infected user)

Subject: BubbleBoy is back!

Body: The BubbleBoy incident, pictures and sounds



The reference to Bubbleboy and the above link are references to a character in an episode in the TV show "Seinfeld". Although the link shown by the virus appears to be out of order, it is most likely the same page as available at

<http://www.toptown.com/dorms/rick/bblboy.htm>

This page and its maintainer have nothing to do with the worm.

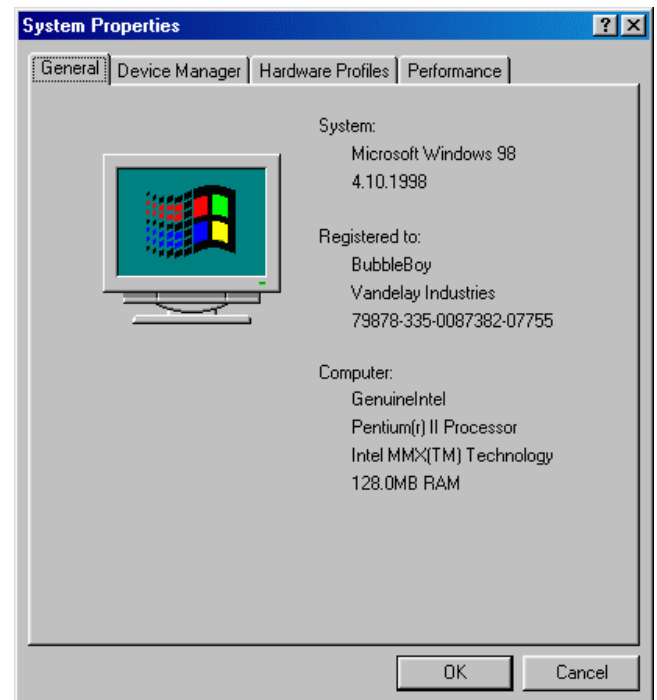
The receiver of the e-mail gets infected and spreads the worm without clicking any attachment. The message does not even have any attachments.

When the user receives such e-mail and opens it, the worm attempts to create two files, "c:\windows\start menu\programs\startup\update.hta" and "c:\windows\menu\inicio\programs\inicio\update.hta".

These locations specify the Windows startup directory for both English and Spanish versions.

After creating this file, the worm will perform no further action until the system has been restarted.

Then the worm will use ActiveX feature to access the system registry. It changes the Windows registered owner to "BubbleBoy" and the organization to "Vandelay Industries".



Then the worm uses ActiveX features to

open Outlook and uses it to send itself to all recipients in all address books, as the Melissa virus does.

Bubbleboy is only able to spread under Microsoft Outlook 98, Outlook 2000 and Outlook Express that comes with Internet Explorer 5. It does not replicate under Windows NT; it just fails without error messages.

Bubbleboy uses a known security hole in Microsoft Outlook to create the local HTA file.

If active scripting is disabled from Outlook, then the worm will not work.

Frequently Asked Questions & Answers

F-Secure Anti-Virus support provides help on all virus and data security questions. Contact information can be found at the end of this section.

Q: Will old viruses work under Windows 2000?

A: Some will, some won't. Most old macro viruses continue to be a problem in Windows 2000, as they only depend on the functionality of Microsoft Office to operate, which makes them more independent of the underlying operating system.

Some of the existing Win32 viruses will fail to operate under Windows 2000, others will work fine. And the first Windows 2000 aware viruses have already been found.

Q: Why did nothing happen during Y2K?

A: Some things did happen. However, as we predicted in late Fall, 1999, no special virus-related Y2K incidents occurred. F-Secure Y2K support was working over the new year and found no more viruses than during any normal weekend.

You can still read an hour-by-hour transcript of our Y2K watch at:

http://www.F-Secure.com/news/y2k_watch.html

As there were no news to report on the Y2K Virus front, we collected information on other types of Y2K problems. This information comes from a variety of sources, including several newswires:

- In Munich, Germany, 495 parking tickets were sent by the government with a due date of 11.1.00. The tickets were calculated with 100 years of interest.
- In the UK, a large set of credit card swipe machines failed to accept credit cards.
- Some Microsoft web sites listed open positions for several jobs starting "1.1.1900". Several other web sites had similar date problems, listing dates like 1900, 19100, 2099, or 20100.
- In Helsinki, Finland, the local taxi central office lost a database of all pre-ordered rides for January 2000. This loss happened some hours after midnight on January 1.
- Hospitals in Sweden and Egypt reported non-lethal bug bites in medical equipment.
- In Japan, a computer linked to radiation monitoring systems seized.
- Some locations in the USA, Spain, and Finland reported problems with electronic door locks, either keeping an area permanently open or closed.
- Several satellites had problems. In France, it was reported that one of its defense satellite systems lost the ability to detect equipment failures. Likewise, some U.S. spy satellites reported temporary problems.

- In Delaware, USA, several hundred slot machines shut down for a while at a Delaware horse track.
- Some taxi meters broke down in a China province.
- Egypt's national news wire service briefly stopped filing news reports, but quickly fixed the problem.
- In Tokyo, Japan, train ticket vending machines stopped briefly in 13 stations.

Q: Will there be problems on February 29, 2000?

A: Year 2000 meets a set of rarely seen rules which causes a non-standard leap day this year. We might see some date-related problems on this date, although most likely there will be even less problems than occurred over the new year.

We expect no special virus-related problems during this period.

Q: Why does the scanning of PowerPoint PPT files seem to be slow?

A: It takes several times longer to scan PPT files than DOC or XLS files. The delay is caused by the extended search performed to locate embedded objects within PowerPoint files.

The only solution to this problem is to completely disable the scanning of PowerPoint files by removing the PPT extension from the extension list.

Q: F-Secure Anti-Virus found a new, unknown virus. What to do?

A: First, update your definition files to the current state. The unknown virus might already be known to us. If updating does not change the report, send the sample to us via e-mail to Samples@F-Secure.com.

Whenever you're not sure what to do, contact our support services.

Q: Where can I reach F-Secure anti-virus support?

A: The Web Club contains the most recent information concerning our products. The Web Club can be found by clicking the globe icon on the toolbar of F-Secure Anti-Virus, or by opening the following address in your web browser:

<http://www.F-Secure.com/anti-virus/webclub/>

F-Secure Anti-Virus Support Center contains detailed support advice:

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

The daily updated virus descriptions can be found at:

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

You can contact our support staff by e-mail at:

Anti-Virus-Support@F-Secure.com

F-Secure Anti-Virus Updates

F-Secure Anti-Virus is updated every day. You should regularly update the version you get with this CD-ROM to ensure the best level of protection.

Data Fellows ships new software versions on a CD-ROM every other month, and makes new virus signature databases available much more often via FSUPDATE and F-Secure BackWeb.

FSUPDATE

The easiest way to download database updates for F-Secure Anti-Virus 4 is to run FSUPDATE, a self-contained executable that installs itself. You can simply download the latest FSUPDATE.EXE file from the F-Secure Anti-Virus Web Club, run it, and relax. FSUPDATE locates the correct file locations and updates them automatically.

FSUPDATE is updated every day on the Data Fellows web server. From the Web Club page, you can find detailed instructions for fetching and using the program, and for distributing the updates to your company's computers. To go to the Web Club, click the globe icon on the F-Secure Anti-Virus toolbar, or connect directly to this web address:

<http://www.F-Secure.com/anti-virus/webclub/>

F-Secure BackWeb

F-Secure Anti-Virus 5 supports F-Secure BackWeb, a new tool that provides you with automatic virus signature database updates directly from the Data Fellows web site. Updates are sent directly to F-Secure Management Server and forwarded to the workstations either automatically or with the click of the mouse after you have reviewed the update.

F-Secure BackWeb downloads files automatically, using bandwidth left unused by your other Internet applications, so you are automatically alerted when new information has been received, and you can always be sure that you'll have the latest updates, without having to look them up in the Web. For an overview of F-Secure BackWeb, see:

<http://www.F-Secure.com/download-purchase/backweb.html>

If you can't use the BackWeb service for some reason, the easiest way to update F-Secure Anti-Virus 5 is by downloading the latest definition files and importing them with F-Secure Administrator to the F-Secure Management Server.

To update all the computers, download the latest.zip file, start F-Secure Administrator, and select the Import Virus Signature Updates command from the Tools menu. The update will be unpacked to a directory on the F-Secure Management Server and the computers will retrieve it according to the policy set in F-Secure Administrator.

The latest definition files are always available at:

<http://www.F-Secure.com/download-purchase/updates.html>

What's New in F-Secure Anti-Virus Release 4.07

The new version detects and removes many more viruses than version 4.06. And several false alarms that troubled version 4.06 have been fixed.

F-Secure Anti-Virus 4.07 uses the F-PROT scan engine version 3.06 build 1302 and the AVP scan engine version 3.00 build 132.1360.

F-Secure Anti-Virus 4.07 might occasionally cause false alarms from certain boot sectors.

F-Secure Anti-Virus 4.07 might cause a delay during the start-up of programs installed by the Microsoft Office 97 Service Release 2 Upgrade. This problem doesn't affect other versions of Microsoft Office.

A hotfix that fixes both problems is available at:

<http://www.F-Secure.com/anti-virus/webclub/>

This hotfix upgrades the F-PROT scan engine to version 3.06 build 1306.

What's New in F-Secure Anti-Virus Release 5.01 build 5364

F-Secure Anti-Virus 5 includes significant improvements over version 4. The new version is based on F-Secure Framework, the enabling technology behind the new policy-based management architecture. Release 5.0 Service Pack 1 build 5364 is a maintenance release that fixes known problems with the product.

Fixed Problems

Floppy boot sector scanning has been improved.

It used to be impossible to uninstall F-Secure Anti-Virus 5 after uninstalling F-Secure Anti-Virus 4. This has been fixed.

Known Problems

Resetting the statistics counters does not work correctly.