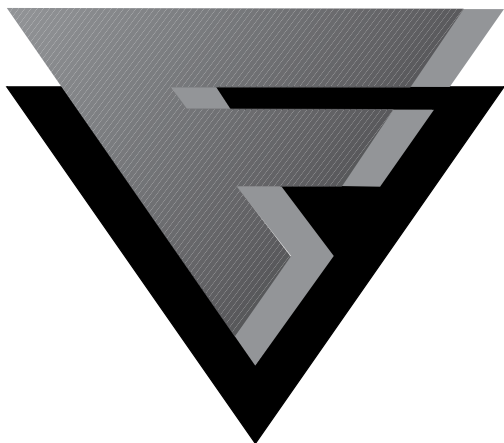


F-SECURE



Update Bulletin 4.06

Dear Customer,

Welcome to the latest edition of the Virus Bulletin. With this issue we bring you important news about the company and our partnerships, as well as late-breaking news about viruses and malicious code. Perhaps the biggest news for us is that we joined the ranks of such world-class companies as Nokia and Sonera when we became listed on the Helsinki Stock Exchange. This is an important step for the company as it will enable us to broaden our reach, acquire new technology and better serve our growing customer base. In addition, it represents a big vote of confidence in the company by thousands of investors around the world, and we will repay that confidence by continuing to provide excellent products and support. Don't miss the article below on our partnership with Digital Island, the first of many based on our Security as a Service™ concept. Through this partnership, we extend our vision of integrated security management through a single framework, F-Secure, to the many Digital Island customers around the world.

Best Regards,

Tanya Candia
Vice President of Worldwide Marketing

Contents

News	2
Data Fellows Corp. goes public	2
Digital Island partners with Data Fellows	2
F-Secure Anti-Virus for Firewalls 3.0 integrates fully into F-Secure Framework	2
Data Fellows' Products Receive Recognition	2
Support for Windows 2000	3
F-Secure Anti-Virus Updates	3
FSUPDATE	4
F-Secure BackWeb	4
Virus News	4
Corner — the first MS Project virus	4
VBS/Freelink	4
Infis	5
Triplex	5
Ringzero	6
Nastysex	7
F-Secure support on call during Y2K	7
Frequently Asked Questions & Answers	7
Support for Windows NT 3.50 Ceasing	8
Changes in the DOS versions	8
F-Secure Anti-Virus Release 4.06	8
What's New in F-Secure Anti-Virus Release 5.01 build 5364	9
Fixed Problems	9
Known Problems	9

Copyright © 1999 Data Fellows Corporation. All Rights Reserved. This material may be freely quoted as long as the source is mentioned.



<http://www.DataFellows.com/>

F-Secure Anti-Virus Update Bulletin 4.06

News

Data Fellows Corp. goes public

Data Fellows is now a public company, trading under the symbol FSC in the Helsinki Stock Exchange main list.

The Data Fellows IPO broke several records at the Helsinki Stock Exchange, including the biggest oversubscription (31 times) and biggest increase in share price in a day - the stock rose from 7,7 Euros to 27,45e during the first trading day.

Data Fellows would like to thank all of our loyal customers over the years and to welcome the thousands of new owners to the company.

Digital Island partners with Data Fellows



Digital Island Inc. has selected Data Fellows' F-Secure as its security management solution. Digital Island will be standardizing on F-Secure as a secure remote access solution for its customers to manage their servers and applications.

Digital Island (NASDAQ: ISLD), a leading provider of network services for globalizing e-business applications, serves corporations operating in multiple countries that need to securely and consistently extend business-critical applications for marketing, selling, servicing or distributing products via the Internet. Digital Island recently merged with Sandpiper Networks.

"Digital Island selected Data Fellows as its security solution vendor because of the company's global reach and its vision for integrated security management through a single Framework, F-Secure," said Allan Leinwand, Vice President of Engineering and Chief Technology Officer at Digital Island. "By offering security through F-Secure, Digital Island lets its corporate customers achieve higher productivity while reducing the costs associated with offering products and services on the Internet. With secure methods of storing and distributing information, our customers can maintain a competitive advantage and increase profits."

In addition, Digital Island also plans to resell the F-Secure client application as part of its server management product offerings in the near future. Specifics of this agreement are still under negotiation.

F-Secure Anti-Virus for Firewalls 3.0 integrates fully into F-Secure Framework

F-Secure Anti-Virus for Firewalls 3.0, now takes full advantage of Data Fellows' F-Secure Framework.

F-Secure Anti-Virus for Firewalls stops malicious code at the firewall before its entry to the corporate network. The firewall sends web browsing, FTP, and email traffic to be scanned by the anti-virus server. The co-operation between the anti-virus software and firewall is based on the Content Vectoring Protocol (CVP). Most firewalls, including Check Point Firewall-1 are CVP-compliant.

F-Secure Framework provides F-Secure Anti-Virus for Firewalls with centralized policy-based management features, which make Anti-Virus for Firewalls easy to deploy and manage in a corporate environment. Among others, the product now supports F-Secure Management Server and is able to send virus alerts to F-Secure Administrator.

Data Fellows' Products Receive Recognition

Data Fellows has once again received recognition for the virus searching capabilities of its F-Secure Anti-Virus malicious code detection software. The Virus Research Unit (VRU) at the University of Tampere has published its latest and largest Unit antivirus scanner analysis. F-Secure Anti-Virus was very successful in the tests.

VRU is one of the two most respected testing units in the malicious code prevention industry, the other being the Virus Test Center (VTC) at the University of Hamburg. In March, 1999, Data Fellows' F-Secure Anti-Virus was judged among the best in the world by the VTC as well as by West Coast Labs' Checkmark.

The testbed of VRU included only viruses that have been found 'In the Wild'. This means that at least two virus research laboratories have reported finding the virus in the field.

F-Secure Anti-Virus products found all the viruses that were included in the testbed. Today, perhaps the most important anti-virus software category is Windows 95 software. No other product in this category was able to find all the viruses.



The results of Windows 95 on-demand scanners were:

Windows 95 on-demand scanner	Boot sector viruses (%)	File viruses (%)	Macro viruses (%)
Avast32 7.70 (9.12.1998)	100	98.61	99.98
AVG 5.0, Build 1237	100	96.89	96.33
Dr. Solomon's Antivirus Toolkit 7.91	99.39	100	100
eSafe Protect 2.0	100	97.37	97.43
F-Secure Antivirus 4.02	100	100	100
H+BEDV Antivir 9X 1.08 (12.11.1998)	93.41	96	97.43
McAfee VirusScan 4.0.2	99.39	100	100
NOD32 1.12	100	100	99.98
Norman Virus Control 4.60	100	99.52	98.58
Norton Antivirus 5.00.00 (22.12.1998)	99.39	100	100
Sweep 3.16	100	99.72	100
Thunderbyte 4.00, Build 1111	100	99.99	99.8

The test results of the University of Tampere Virus Research Unit once more provide independent recognition that Data Fellows is the technology leader in virus protection.

Further information about the Virus Research Unit at the University of Tampere can be found at the following Web address:

<http://www.uta.fi/laitokset/virus/>

Complete analysis results can be found at:

<ftp://ftp.cs.uta.fi/pub/vru/documents/TEST1999.TXT>

Support for Windows 2000

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. F-Secure Anti-Virus 4 is year 2000 (Y2K)-compliant, but 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.

The first beta version of F-Secure Anti-Virus for Windows 2000 is now available for evaluation. This pre-release consists of the following components:

- F-Secure Anti-Virus Beta 5.02 build 5411 for Windows 2000
- F-Secure Management Agent for Windows 2000

The pre-release has passed the initial tests at Data Fellows, but the full testing process has not

been completed, and you should not use the pre-release on a production system. This pre-release has been tested on Windows 2000 Release Candidate 2 and it will not work on any other version of Windows 2000.

This package contains everything you need to install and test F-Secure Anti-Virus 5 for Windows 2000 on a stand-alone system. If you want to test the product as a part of the F-Secure Framework policy-based centralized management system, you'll need to use the Windows NT 4.0 based versions of the F-Secure Administrator and F-Secure Management Server tools.

Customers wishing to evaluate F-Secure Anti-Virus for Windows 2000 should contact fsav-beta-2000@DataFellows.com to receive instructions for downloading the beta version.

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 couple of months, but makes new virus signature databases available much more often via FSUPDATE and F-Secure BackWeb.



<http://www.DataFellows.com/>

FSUPDATE

The easiest way to download database updates for F-Secure Anti-Virus 4 is FSUPDATE, a self-contained executable that installs itself. You can simply download the latest FSUPDATE.EXE 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.DataFellows.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 totally automatically or with the click of a mouse after your review of 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 search the Web. For an overview of F-Secure BackWeb, see:

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

Virus News

Corner — the first MS Project virus

P98M/Corner is the first macro virus to infect the Microsoft Project application. This virus is capable of infecting both Project and Word and can travel between them.

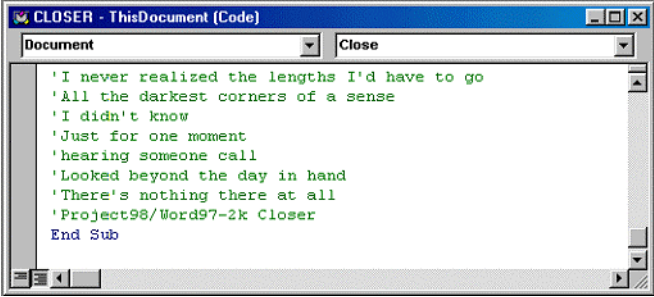
With the discovery of the first MS Project macro virus, almost all popular Microsoft applications are now susceptible to virus infections. Macro

viruses have been written for the following Microsoft applications:

- Microsoft Word 2.0
- Microsoft Word 95
- Microsoft Word 97
- Microsoft Word 2000
- Microsoft Excel 4.0
- Microsoft Excel 95
- Microsoft Excel 97
- Microsoft Excel 2000
- Microsoft PowerPoint 97
- Microsoft PowerPoint 2000
- Microsoft Access 97
- Microsoft Project 98

The Corner virus keeps on spreading from one user to another in infected Word "DOC" and Project "MPP" files. Other than spreading, the virus does not do anything.

The virus code contains these comments:



```

'I never realized the lengths I'd have to go
'All the darkest corners of a sense
'I didn't know
'Just for one moment
'hearing someone call
'Looked beyond the day in hand
'There's nothing there at all
'Project98/Word97-2k Closer
End Sub

```

Although the Corner virus does not do anything but replicate, it is still a serious risk to users of Microsoft Project. In the future, we're likely to see several new viruses using similar techniques.

Further technical information on the Corner virus is available on our web site at:

<http://www.DataFellows.com/v-descs/corner.htm>

VBS/Freelink

VBS/Freelink is a Melissa-like worm. It spreads by e-mailing a file called LINKS.VBS around.

VBS/Freelink is written in the VBScript language. By default, programs written in VBScript operate only under Windows 98 and Windows 2000 beta (unless Windows Scripting Host has been installed separately).

However, Microsoft Internet Explorer 5 installs Windows Scripting Host (WSH) also to Windows 95 and Windows NT 4.0 machines by default, making them vulnerable to this worm.

VBS/Freelink was originally found in Europe in



July 1999. However, it did not become common at that time, as it only operated under Windows 98 and beta versions of Windows 2000. Now that Microsoft Internet Explorer 5 has been released, more and more Windows 95 and NT users are vulnerable to this worm. Estimates on the current market share of Internet Explorer 5 range between 10% and 20%.

The worm arrives in e-mail message attachments named LINKS.VBS. When it is executed, the worm shows a message box with the following text:

```
This will add a shortcut to free XXX links
on your desktop.
Do you want to continue?
```

Whether the user clicks 'yes' or 'no', the program creates an Internet shortcut named "FREE XXX LINKS" to the desktop. This shortcut points to a porn web site.

After this, the worm searches for mapped network shares on the local network. If the worm finds any network drives, it copies itself to the root directory.

The worm uses Outlook application to mass-mail itself to each recipient in each address book. The mass-mail portion is similar to the infamous Melissa virus.

The subject of the messages sent by the virus is "Check this" and the body of the message is "Have fun with these links. Bye."

The worm attaches itself as "Links.vbs" to the message. When the receiver double-clicks on the attachment, the worm executes and will mass-mail itself again.

VBS/Freelink removes the sent mail from the user's "Sent Mail" folder. In this way it tries to hide the mass mailings from the user.

As address books typically contain group addresses, the end result of executing the VBS/Freelink worm inside an organization is that the first infected user sends the message to everybody in the organization. After this, other users open the message and send the message again to everyone else. This quickly overloads e-mail servers.

Infis

Infis is the world's first driver-based virus for Windows NT.

Infis can replicate under Windows NT 4.0 with Service Packs 2, 3, 4, 5, 6 installed. It does not work on systems running Windows 95/98, Windows 2000, or other versions of Windows NT.

The virus usually arrives in an infected EXE file and being run installs itself. The virus copies its

body to the INF.SYS file in the Windows NT drivers folder WinNT\System32\Drivers. Then it creates a key with three subkeys in the Windows System Registry:

```
\Registry\Machine\System\CurrentControlSet\
Services\inf
Type = 1 - standard Windows NT driver
Start = 2 - driver start mode
ErrorControl = 1 - continue system loading on
error in driver
```

As a result the virus in INF.SYS file will be activated every time the operating system starts. When INF.SYS file is activated the virus first infects Windows NT memory. When this is done the virus takes control over some Windows NT internal undocumented functions. The virus traps the file opening routine and if any file is opened it checks the file name and the file's internal format and then calls the infection routine if the PE EXE file is opened.

The virus infects only PE (Portable Executable) EXE-files except CMD.EXE. When infecting, the virus increases the file length by the length of its "pure code" - 4608 bytes. The virus doesn't infect files twice. It recognizes already infected files by "date and time" stamp changed to -1value upon first infection.

The Infis virus does not have any destructive payload. However, it has bugs that could result in corruption of some files upon infection. When a corrupted file is run, the standard Windows NT application error message is shown.

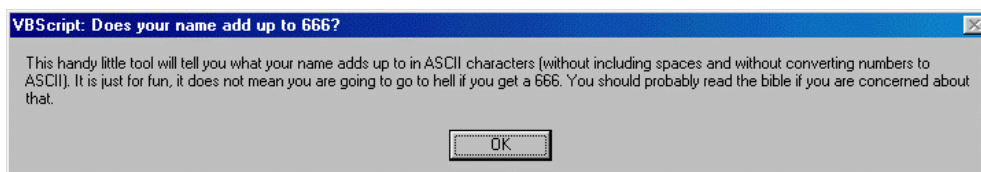
Analysis by Eugene Kaspersky, AVP Team

Triplesix

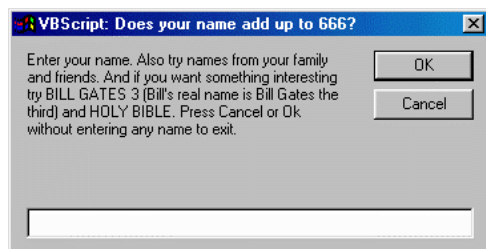
VBS/Triplesix is a Visual Basic Script worm. It uses the following applications to spread itself as an attached file "666TEST.ZIP":

- E-mail client Microsoft Outlook
- Chat application mIRC
- Chat application Pirch

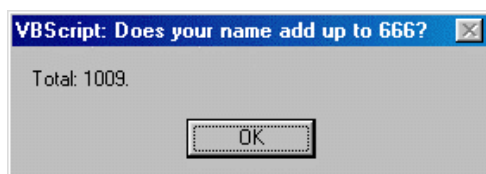
The archive contains one file, "666TEST.VBS". This is the worm itself. When the script is executed, it first shows a message box:



After this, the virus starts a simple game:



The game asks for users name. When the user enters anything in the dialog and presses the "OK" button, the sum of the ASCII characters is calculated.



If the user does not enter anything, or the game is cancelled, the worm drops a file named "WINTEMP.TXT". This file is used to create another file, "WINTEMP.EXE", which is a PkZip executable. These files are created in the Windows directory.

After creating the archive, VBS/Triplesix modifies the registry in such a way that this script will be executed when the system is restarted. When executed, this script attempts to locate any mIRC, Pirch and Pirch98 installations. If one or more of these IRC clients are found, the worm will overwrite their setup files ("script.ini" for mIRC, and "events.ini" for Pirch and Pirch98) so that the worm will send itself to other chat users when they join an IRC channel that has a user with an infected client.

Next, the worm attempts to send itself to everyone in the Outlook's address book. The message it sends has the subject "666 test" and the body of the message is:

```
Does your name add up to 666 in ASCII
characters?
Are you going to go to hell?
```

After mail has been sent, the worm will create the following registry key:

```
HKEY_LOCAL_MACHINE\Software\MIRC\
OUTLOOK\PIRCH.VanHouten
```

and set its value to "True", so the mass mailing will happen only once per infected machine.

In the fifth day of each month, the worm will drop another file to the Windows directory, "VANHOUTEN.BMP", and set it to Windows wallpaper.



Analysis by Katrin Tocheva and Sami Rautiainen, Data Fellows

Ringzero

RingZero is a trojan. It can arrive as an executable e-mail attachment. This trojan first arrived attached to a Winsock Version Checker program. The pure trojan has 2 parts — an executable part (an EXE file packed with Petite file compressor), and a small VXD part attached to the executable. The trojan can be also attached to any Windows executable.

When the trojan is run, it first installs itself to the system. It detaches itself from the file it came with and writes two files to the `Windows\System` directory. One file is always RING0.VXD, and the other can have different names:

```
TELNET23.EXE
EXPLUPD.EXE
PCT.EXE
ITS.EXE
```

A third file called A.EXE could also be created. Then the trojan makes necessary modifications so it can be always run with Windows. Being

active, the trojan scans the Internet for proxy servers. If a proxy server is found, the trojan writes its address to ITS.DAT (or to a differently named DAT file) and sends this file to a website with the following address: www.rusftpsearch.net (which has now been removed for security reasons).

It seems that the trojan was intentionally created to send data to that server. Most likely, the idea was to collect information about all proxy servers on the Internet and compile it into a database.

The trojan doesn't have any other payload and it doesn't work on Windows NT.

Analysis by Alexey Podrezov, Data Fellows

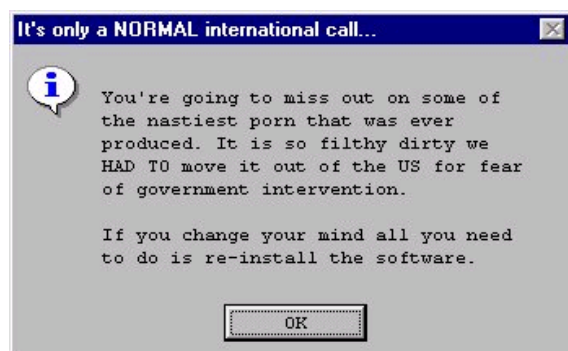
Nastysex

This is not a trojan or a virus. Nastysex is a program to display pornographic images. We sometimes get queries about it, because it can easily cause substantial phone costs to the victim.

The program is distributed in several different versions from a wide range of XXX web sites. Filenames include SEXWARE.EXE and XXXFILES.EXE.

When installing the software, it explains that the software is going to call out with a modem to download pornographic pictures "from another country" as they are "too explicit to be stored in USA".

The user has a free choice to decline the offer. If he does, he gets this display:



If the user enters his user info and his modem's COM port, the software will call out to Guyana in South America (phone number: +592 279 156), and will download XXX-rated pictures.

Although this can easily cause huge phone bills, the program does not try to hide the fact that it is going to call to another country. Thus, this is not a trojan and F-Secure Anti-Virus WILL NOT detect or stop this program. Keep your head when surfing the net.

F-Secure support on call during Y2K

Data Fellows is committed to providing its customers with first-class support during the millenium. The Anti-Virus Research and Technical Support teams are overseeing the turn of the year and respond to Y2K related data security threats through the night. For more information, go to:

<http://www.DataFellows.com/news/year2000.htm>

Frequently Asked Questions & Answers

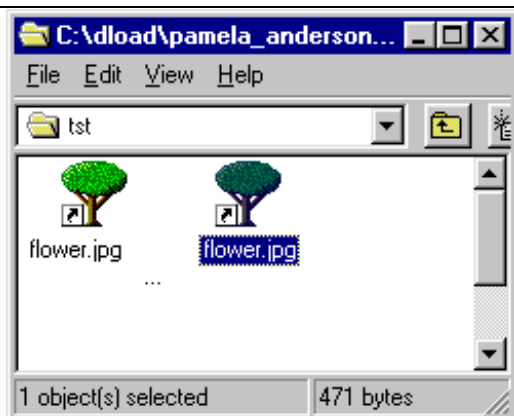
Data Fellows' Anti-Virus support provides help on all virus and data security questions. Contact information can be found at the end of this section.

Q: I've often heard that picture files can contain viruses. Is this true?

A: Common picture file formats (GIF, JPG, PNG, BMP, TIFF) cannot contain viruses. However, this does not mean that it is always safe to double-click on an unknown GIF file. We've recently seen several cases where an attacker has tried to make an executable file (EXE) appear to be an innocent picture file.

This could be done, for example, by naming the executable to something like "picture.jpg .exe", that is, by inserting a long row of space characters before the EXE extension.

If the filename becomes very long, the end is then typically truncated, and the user only sees something like "picture.jpg...", and might mistake the file for a jpg picture.



These files look the same, but the one on the left is an executable and the one on the right is a normal picture file.

Q: My friend was hit by the Tristate virus. How can we be totally sure the virus is gone?

A: The Tristate (or Triplicate) virus infects three common Microsoft applications: Word, Excel and Powerpoint. It does this by infecting files called NORMAL.DOT (for Word), BOOK1.XLS (for Excel) and BLANK PRESENTATION.POT (for Powerpoint).

F-Secure Anti-Virus is able to locate and clean Tristate. However, if you want to recreate clean, empty versions of these template files, simply close down Office applications, locate these files from MS Office directory, delete them and reboot.

Also remember that Office files can be renamed to any extension - it is recommended to do a scan of ALL files after any virus infection.

Q: Does the DOS version of F-Secure Anti-Virus detect Windows viruses?

A: Yes. Our DOS version is able to detect and disinfect 16-bit and 32-bit Windows viruses, just like the Windows versions. It is also able to detect and disinfect macro viruses.

Q: I heard about a virus called Autostart. Can my Windows 98 machine become infected?

A: Don't worry. Autostart is a Macintosh virus, affecting only users of Apple Macintosh. F-Secure Anti-Virus for Macintosh does detect and disinfect known versions of the Autostart worm.

Q: Where can I reach Data Fellows 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.DataFellows.com/anti-virus/webclub/>

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

<http://www.DataFellows.com/support/>

The daily updated virus descriptions can be found at:

<http://www.DataFellows.com/virus-info/>

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

Anti-Virus-Support@DataFellows.com

If you have a separate support contract, you should use the contact information given there, instead.

Support for Windows NT 3.50 Ceasing

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

While there are ways to make this older operating system work in the year 2000, Data Fellows will support Windows NT 3.50 with F-Secure Anti-Virus only until the end of 1999. Customers are encouraged to upgrade to a newer version of Windows NT.

F-Secure Anti-Virus for Windows NT 3.50 Release 4.06 build 1400, available on this CD-ROM, will be the last version of FSAV that supports Windows NT 3.50. Virus signature database updates available from the Data Fellows web site will continue to work until December 31, 1999.

Changes in the DOS versions

The 16-bit version of F-Secure Anti-Virus for DOS, AVP Edition, has been replaced with a version based on AVPLite. In effect, this means that the 16-bit DOS version does not have a user interface anymore. Instead, it operates as a command-line utility.

F-Secure Anti-Virus Release 4.06

The new version detects and removes many more viruses than version 4.05.

Updating from version 4.05 to 4.06 on the Windows NT environment does not require local administrative rights.



<http://www.DataFellows.com/>

Version 4.05 had a problem which caused huge amounts of disk space to be used during scanning of ARJ archives. This has been fixed.

Incompatibility with Utimaco's SafeGuard Lan Crypt under Windows NT has been solved.

FSAV 4.06 uses F-PROT scan engine v3.06 and AVP scan engine build 132.1360.

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 5.01 build 5364 is a service-pack release, focusing on fixing known issues with the product.

Fixed Problems

Floppy boot sector scanning was improved.

Trap messages were not always sent correctly.

Infected files were sometimes removed without confirmation.

Memory scanning was improved.

It used to be impossible to uninstall FSAV 5 after uninstalling FSAV 4.

Known Problems

Resetting statistics does not work.

Disinfected boot blocks are not shown in the user interface.

Scanning report doesn't always show all infections.

Suspected infections are not categorized correctly in scanning statistics.

Powerpoint viruses are not disinfected by FSAV 5.01.

There are problems sending traps about Floppy/MBR/Memory resident viruses.

There is a known incompatibility with the Zipmagic product