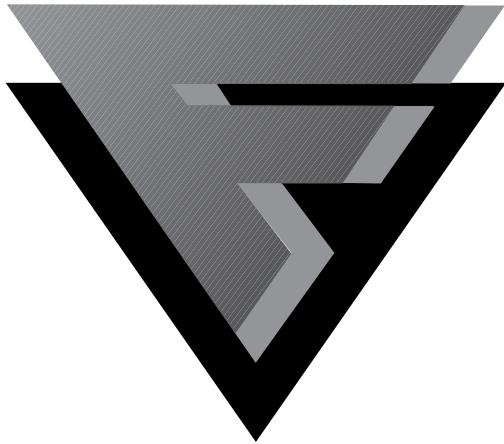


# F-SECURE



## Manage Your Security

As you read this, Data Fellows is getting ready to start the biggest product launch we've ever done: F-Secure Workstation Suite 4.0 is almost ready.

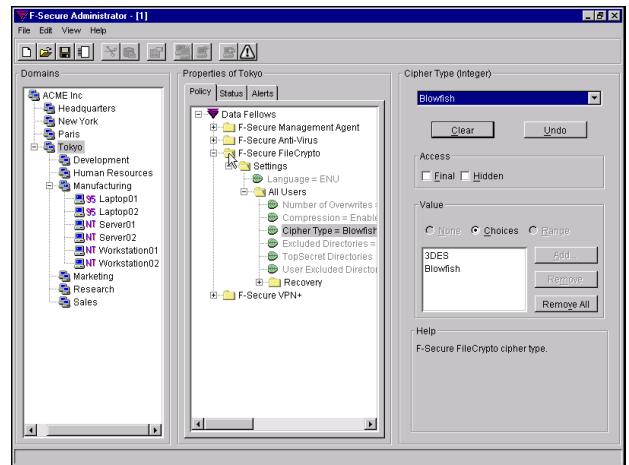
F-Secure Workstation Suite 4.0 truly integrates virus protection with file and network encryption - using strong cryptography. Best of all, the security suite can be managed with the advanced policy based three-tier management system.

## F-Secure Anti-Virus 4.03 Update Bulletin

Editor: Mikko Hypponen

### Index

News .....	2
F-Secure Anti-Virus Agent & Server now available .....	2
Data Fellows and CA announce technology development partnership .....	2
Data Fellows Joins the Microsoft Security Partners Program .....	3
Updates for F-Secure Anti-Virus .....	3
Virus News .....	4
CIH .....	4
Caligula .....	4
Russian New Year .....	5
Backnote .....	5
Happy99 .....	5
IE0199.EXE .....	6
Ethan .....	7
Netbus .....	7
Sattelite .....	9
New virus hoaxes .....	9
Common Questions & Answers .....	9
F-Secure Anti-Virus Technical Support Services .....	10
Changes in F-Secure Anti-Virus Release 4.03 .....	10



The Java-based graphical management system provides powerful management features, including the capability to deploy installations to new machines and monitor the status of individual machines or larger groups.

By integrating the major security products into one, we can provide better compatibility, better performance, better management and better value for money. Stay tuned. The future is almost here.

## F-Secure Anti-Virus Update Bulletin 4.03

Copyright © 1999 Data Fellows Ltd. All Rights Reserved.

This material may be freely quoted, when the source, F-Secure Anti-Virus Update Bulletin from Data Fellows, is mentioned.



<http://www.DataFellows.com/>  
Integrated Solutions for Enterprise Security

F-Secure Workstation Suite 4.0 will be announced in the CeBIT fair in Germany and shipments will start in April. You can read more about F-Secure Workstation Suite from our web site at <http://www.DataFellows.com/>.

As an F-Secure Anti-Virus customer, you'll be able to take advantage of the same centralized policy based management features in the coming releases of the product. To learn more about F-Secure Framework which makes all this possible, take a look at the F-Secure Framework self-running demonstration which is available on the F-Secure CD-ROM 4.03.

## News

### F-Secure Anti-Virus Agent & Server now available

Data Fellows has started shipping its new F-Secure Anti-Virus Agent & Server. This product provides corporate system services with centrally-managed, scalable protection against malicious code.

In this first phase, Data Fellows has shipped F-Secure Anti-Virus Agent for Microsoft Exchange Server and F-Secure Anti-Virus Agent for Firewalls. F-Secure Anti-Virus Agent for Internet Mail and F-Secure Agent for Lotus Domino will be released later. The product will replace F-Secure Anti-Virus for Firewalls.

F-Secure Anti-Virus Server provides core services to the Agents. This includes malicious code detection and removal; quarantine for the malicious data so it can be stored and processed further by the Administrator; and reporting and alerting functions.

The Agents and Servers are managed through F-Secure Administrator, the Data Fellows' policy-based management utility. The Administrator is able to partition the company network into "security zones". The policies may specify common settings for all workstations, servers and gateways in a zone or in the entire network. Alternatively, a policy may be set for a single computer.

"Protecting your system couldn't be easier, and it is also completely unobtrusive to the end user," says Mr. Ari Hypponen, Vice President, Product Management, for Data Fellows. "The beauty of this product is its scalability. Different services can use the same server, and more servers can be installed, if the number of Agents increases. Therefore, this is ideal for corporations of any size."

For more information, contact Data Fellows or your local F-Secure dealer.

### Data Fellows and CA announce technology development partnership

F-Secure Workstation Suite and Unicenter TNG to be integrated



Data Fellows has announced a technology development partnership with Computer Associates International, Inc. (CA) resulting in the integration of Data Fellows F-Secure Workstation Suite with CA's Unicenter TNG, the industry leading end-to-end enterprise management solution. Data Fellows has also joined the CA Development Partner Program and is making available the F-Secure Workstation Suite for Unicenter TNG.

F-Secure Workstation Suite for Unicenter TNG provides users of Unicenter TNG with an option to use the F-Secure Workstation Suite to configure, control and monitor their system and network security environment with encryption through Unicenter TNG. The integration is ideal for customers who have chosen Unicenter TNG as their enterprise management solution of choice and who also will use F-Secure Workstation Suite for their data security and want to combine it with Unicenter TNG's management capabilities.



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

"It is very important for Data Fellows to provide comprehensive security solutions that will work in the specific management environments in which our customers have invested," said Risto Sillasmaa, President and CEO of Data Fellows. "By combining F-Secure Workstation Suite with the extensive management capabilities of Unicenter TNG, our partnership with Computer Associates creates a new approach to securing data throughout the enterprise for our clients".

Integration between these two products will allow administrators to discover, manage and monitor all secured end-user workstations using Unicenter TNG and F-Secure Management Agent technology. The real-time alerts and event notifications of F-Secure Workstation Suite are automatically delivered to Unicenter TNG, which in turn delivers the appropriate response. The integration also allows distribution, installation configuration, activation, verification, updating and de-installation of F-Secure products from a central point using Unicenter TNG Software Delivery.

"F-Secure provides Unicenter TNG users with additional flexibility for meeting today's stringent security requirements," said Brian Shemilt, CA vice president of development partner programs. "We are pleased that F-Secure has joined the Unicenter TNG security solutions family."

## Data Fellows Joins the Microsoft Security Partners Program

Data Fellows was invited to join the Microsoft Security Partners Program in December 1998.



The Microsoft Security Partners Program (<http://www.microsoft.com/security/partners>) provides customers with the tools and information they need to establish, test and maintain effective information security for their computing infrastructure. The program brings

together software manufacturers, security consultants and security trainers, making it even easier for customers to provide robust security in their Microsoft Windows NT operating system-based networks.

Three Data Fellows products are included in the Microsoft Security Partners Program: F-Secure Workstation Suite, F-Secure VPN+ and F-Secure FileCrypto.

"Microsoft is pleased to include Data Fellows as part of its Security Partners Program," said Karan Khanna, Windows NT Security Product Manager at Microsoft Corp. "This program will help our mutual customers develop and deploy secure solutions built on the Windows NT platform."

## Updates for F-Secure Anti-Virus

F-Secure Anti-Virus is updated on daily basis. The version you have received with this bulletin is already out of date by the time you read this.

Data Fellows ships new CD-ROM upgrades to the software itself every few months. However, database updates to add detection of new viruses happens all the time. It is not enough to rely only to the updates coming with the CD-ROM upgrades. You need to download and distribute new definition files regularly, preferably on daily or weekly basis.

### FSUPDATE

Data Fellows has started making the updates available in a simple, self-installing form. Simply download the FSUPDATE.EXE tool from the F-Secure Anti-Virus Web Club, run it and relax; it will locate the product and update the relevant files.

FSUPDATE is automatically updated every day on our web site. For detailed instructions on how to download it and how to automate frequent updates for the whole company, visit the Web Club by clicking the world icon in F-Secure Anti-Virus or by browsing to:

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



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

## Virus News

### CIH

The activation date of the widespread Win95/CIH virus is getting closer. In the beginning of 1999, CIH was among the ten most common viruses globally.

This is quite serious, as the most common variant of CIH activates destructively on the 26th of April.

On this date, the virus overwrites most of the data on the computers hard drive. This can only be recovered with recent backups.

The virus also has another, unique activation routine: It will try to overwrite the Flash BIOS chip of the machine. If it succeeds in this, the machine will be unable to boot at all unless the chip is reprogrammed.

The CIH virus infects Windows executable files (EXE files). It does not infect Word or Excel documents. CIH works under both Windows 95 and Windows 98, but it does not work under Windows NT.

F-Secure Anti-Virus detects and disinfects Win95/CIH.

### Caligula

*Katrin Tocheva, Data Fellows*

W97M/Caligula is a Word macro virus that tries to attack the popular **PGP** (Pretty Good Privacy) encryption program.

The virus spreads within Word documents like any other Word macro virus. It hooks the Tools/Macro, Tools/Customize, View/Toolbar and View/Statusbar menus of Word. The Tools/Macro menu is greyed out and can't be accessed.

Caligula activates in three different ways. First, the summary information of infected documents is changed in the following way:

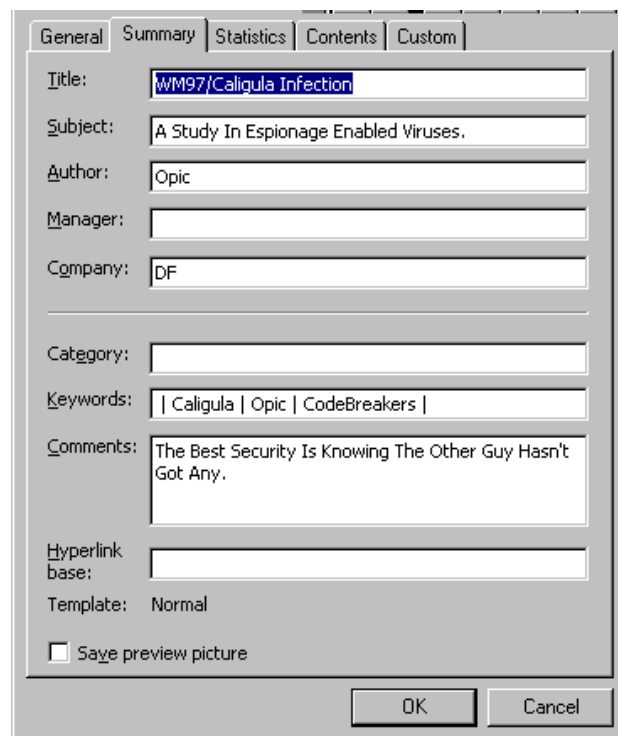
Title: *WM97/Caligula Infection*

Subject: *A Study In Espionage Enabled Viruses*

Author: *Opic*

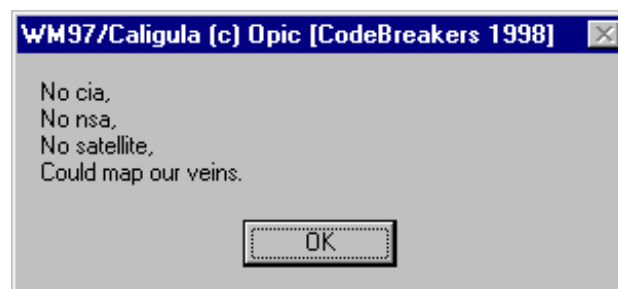
Keywords: */ Caligula / Opic / Codebreakers /*

Comments: *The Best Security Is Knowing The Other Guy Hasn't Got Any*



*W97M/Caligula modifies the document properties*

Furthermore, on the 31st of each month the virus shows a dialog with this message:



The really nasty part of the virus is related to PGP: the virus locates the secret keyring file of PGP (SECRING.SKR) and tries to send it through FTP to a site in the codebreakers.org domain (which is a known virus exchange site). To send the key the virus creates temporary file called c:\cdbrk.vxd.



If the attacker can break the passphrase, he can then open PGP-encrypted files sent to this user.

This is quite serious as passphrases are the weakest known link today in public key cryptography such as PGP. Also, people very commonly use passphrases that are too weak. With a copy of the keyring, massive brute-force attacks are possible for any period of time - and the user may not even know that a copy has been made of the keyring.

F-Secure Anti-Virus detects and disinfects W97M/Caligula.

## Russian New Year

The international media extensively discussed a new security problem called "Russian New Year" during the beginning of 1999. Russian New Year is not a virus, it is a well-known security hole in Microsoft Windows and Microsoft Excel.

This vulnerability, related to Excel's CALL function, allows an attacker to send an HTML email or modify a Web page so that when accessed, the Web page will automatically launch Excel and use it to run any program. This allows the attacker to do almost anything he wants to do on the host machine.

This attack is not widespread, and no real-world occurrences have been reported. However, there is a realistic possibility that malicious hackers might use this vulnerability to carry out attacks against unsuspecting users.

The problem has been partially solved with a Microsoft patch for Excel 97. This patch will disable the CALL command completely. No protection is available yet for Excel 95.

The latest versions of Netscape and Internet Explorer, with their latest patches, offer protection against this attack. However, they will not provide protection against some attacks which use HTML email.

Data Fellows' F-Secure Anti-Virus detects Excel files with harmful embedded CALL

commands and provides protection against this kind of attack.

This security hole was originally discovered in November 1998 by researchers at Kaspersky Lab, a partner company of Data Fellows located in Moscow. Microsoft reacted to the problem in December 1998. Finjan announced the problem in January 1999.

## Backnote

Backnote (also known as URLSnoop and PICTURE.EXE) is not a virus but a Windows-based trojan horse. This trojan was e-mailed using a spamming tool to tens of thousands of users around the world.

If the recipient ran the attached PICTURE.EXE, it would secretly copy itself to the Windows directory as a file called NOTE.EXE and register itself to be executed every time Windows boots up.

After this, the trojan gathers information from the machine, including the username and password, copies them to an encrypted DAT file and tries to send that file to e-mail addresses which are apparently located in China.

This trojan does not spread by itself. It is recommended that you change your password if you believe you are affected by this trojan.

F-Secure Anti-Virus detects and disinfects the Backnote trojan.

## Happy99

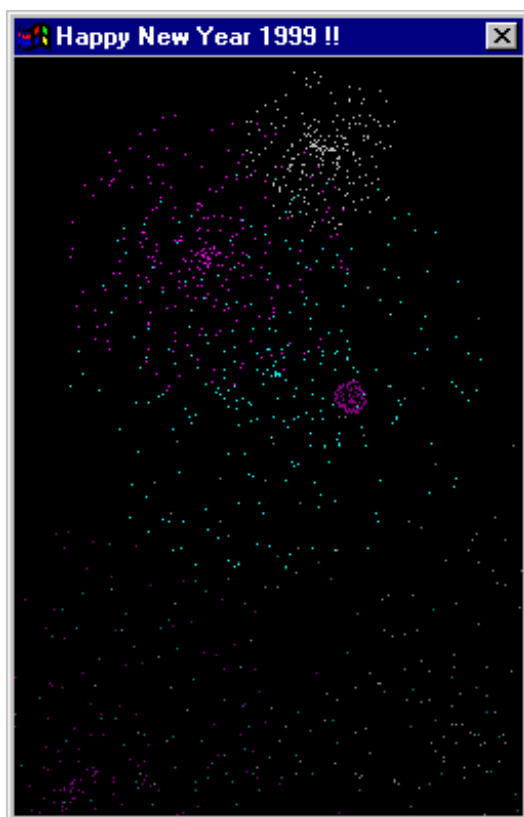
Happy99.exe is an e-mail worm which spread across the globe during February 1999.

The worm modifies e-mails and newsgroup postings by adding unauthorized attachments without the computer user's knowledge. As a side-effect, it can also create network slowdowns and, in a worst-case scenario, even crash corporate e-mail servers. While the computer worm does not destroy or alter files or otherwise cripple computers and networks, it creates a time- and energy-consuming



nuisance to network administrators. This worm works on Windows 95 and 98 platforms.

Happy99.exe (also known as I-Worm.Happy and Win95/SKA) is classified as a computer worm for its ability for self-replication. It arrives into a computer via an e-mail or newsgroup attachment, infecting machines that run the attachment. If the computer user runs the unauthorized attachment, Happy99.exe puts up an attractive fireworks display, which the computer user might mistake for a good-looking accessory to the message.



*Activation of Happy99.exe*

However, while the fireworks burst on-screen, the computer worm modifies the winsock32.dll file in order to monitor what e-mails and postings are made from the machine. All Internet access goes through the wsock32.dll file. Afterwards, Happy99.exe spams the newsgroup or e-mail recipient with copies of itself any time the computer user tries to send a message.

F-Secure Anti-Virus detects and disinfects the Happy99.exe worm.

## IE0199.EXE

*By Eugene Kaspersky, Kaspersky Lab*

The IE0199.EXE trojan, also known as AntiBTC and SNDVOL, was mailed to a large group of recipients in January 1999. The spammed messages were faked to look as if it was coming from Microsoft and claimed to contain an update for Internet Explorer. The e-mail contained a 28kB big attachment called IE0199.EXE.

### The original mail looked like this:

```
Date: Mon, 25 Jan 1999 20:00:26 -0500
From: "Microsoft Internet Explorer Support"
<IESupport@microsoft.com>
To: "Microsoft Internet Explorer User"<>'
Subject: Please Upgrade Your Internet Explorer
Microsoft
Corporation

1 Microsoft Way
Redmond, WA 98052
US
```

```
Dear Sir/Madam
As an user of the Microsoft Internet
Explorer, Microsoft Corporation provides
you with this upgrade for your web browser.
It will fix some bugs found in your Internet
Explorer. To install the upgrade, please save
the attached file (ie0199.exe) in some folder
and run it.
```

```
For more information, please visit our
web site at www.microsoft.com/ie/
```

```
-----
(c) 1995-1998 Microsoft Corporation. All
Rights Reserved
```

When the IE0199.EXE file is run, it extracts two files from its body (MPREXE.DLL and SNDVOL.EXE) and copies them to the Windows system directory. The trojan then registers the MPREXE.DLL file in the system to force the system to run this file on each reboot.

When executed the MPREXE.DLL file just executes the SNDVOL.EXE file and exits. The SNDVOL.EXE file enables auto-dialing by changing the system registry Internet options, randomly selects one of three Bulgarian Web servers (www.btc.bg, www.infotel.bg, ns.infotel.bg), connects them and sleeps for some time. The trojan does not perform any other actions. It simply tries to overload these three Bulgarian servers with connections coming from thousands of users around the world.

 **DATA FELLOWS**

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

F-Secure Anti-Virus detects and disinfects the IE0199.EXE trojan.

## Ethan

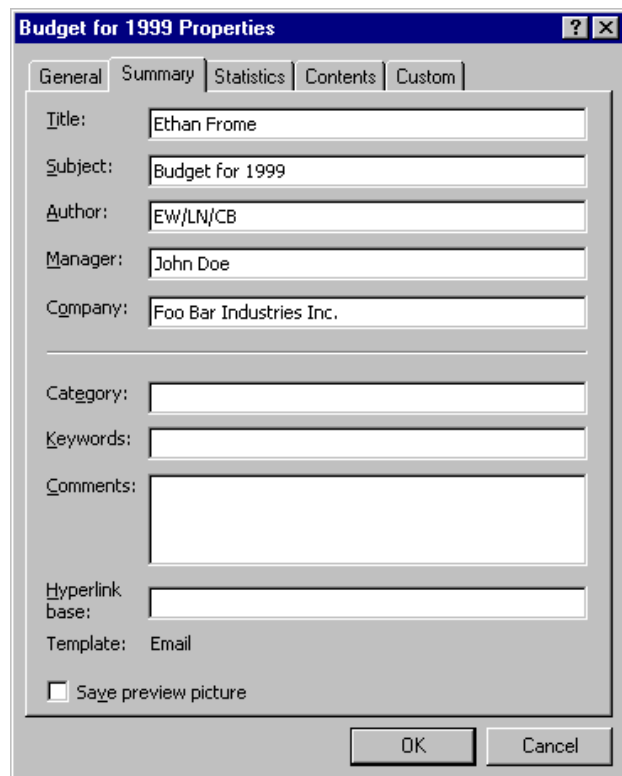
*Katrin Tocheva, Data Fellows*

W97M/Ethan is a Word macro virus that replicates under Word 97. It was found in the wild in January 1999.

Ethan is a simple macro virus, consisting of a single macro less than 50 lines long. It infects Word's NORMAL.DOT template and documents by prepending it's code to a module in the document.

To spread, the virus generates a file with the name "c:\ethan.\_\_\_\_". This file alone is harmless and can be deleted after the disinfection. The file is listed as a hidden system file.

W97M/Ethan activates randomly. Whenever a document is opened, there is a 3-in-10 chance that the virus will change the document's properties. If this happens, the virus changes the title of the document to "Ethan Frome", Author to "EW/LN/CB" and company to "Foo Bar Industries Inc."



"Ethan Frome" is a book written by Edith Wharton in 1911. It was also released as a movie in 1993, with Liam Neeson playing Ethan Frome.

In addition, W97M/Ethan checks if the machine is already infected with the W97M/Class virus and if so, it delete the class.sys file that W97M/Class uses to replicate.

F-Secure Anti-Virus detects and removes the Ethan virus.

## Netbus

*Alexey Podrezov, Data Fellows*

NetBus is not a virus, but it is considered to be a trojan. It is quite widespread and frequently used to steal data and delete files on computers. Netbus allows a hacker to access data and gain control over some Windows functions on a remote computer system.

Netbus is a remote administration tool, like the infamous Back Orifice. However, Netbus predates Back Orifice by several months and is also capable of working under Windows NT in addition to Windows 95 and 98.

Netbus is particularly widespread in Northern Europe. A Swedish computer magazine, Computer Sweden made a portscan on a large set of Swedish internet users in January 1999. According to their results, they found approximately 40,000 machines which were running the Netbus server and were open to access.

Netbus tool has client and server parts. The server part is installed on the remote system to be accessed. On execution the server part installs itself to the Windows directory and is executed automatically during the next Windows start-up. Typically the server part is hidden inside another application.

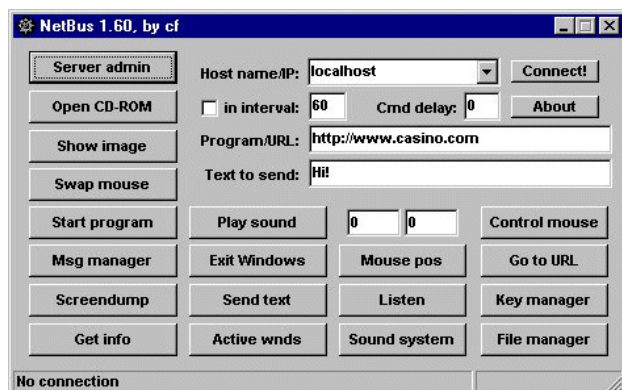
The server part takes steps to protect itself from being removed from the system - it hides its process name in Windows task manager and denies access to the file on attempts to delete or rename it.

The client part permits control of the remote computer system where the server part is



installed and activated. The client part has a dialog interface which allows it to perform tricks on the remote system and to receive/send data, text and other information.

The client and server parts use the TCP/IP protocol to communicate with each other. The client part has an option to scan a range of IP addresses to search for an active server part and connect to it.

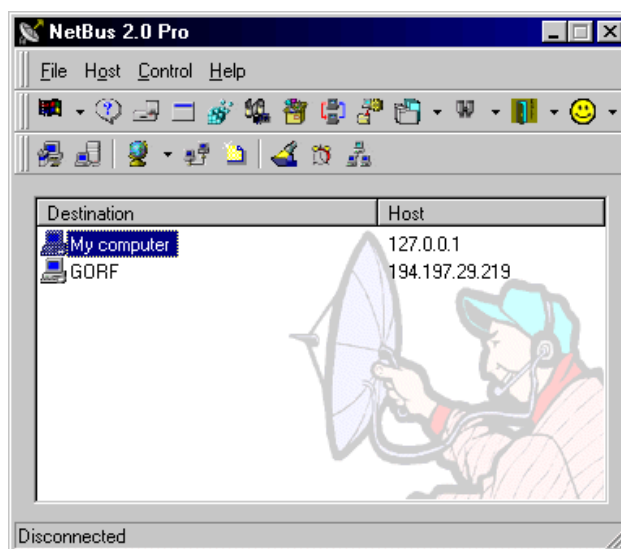


*User interface of NetBus 1.60*

Netbus has a wide variety of features, including:

1. Open/close the CD-ROM tray once or at intervals (specified in seconds);
2. Show optional BMP or JPG images (full path allowed);
3. Swap mouse buttons - the right button is given the left button's functions and vice versa;
4. Start an optional application (full path allowed);
5. Play an optional WAV sound-file (full path allowed);
6. Show a message dialog on the screen and allow the user on the remote system to answer it;
7. Shut down Windows, reboot, logoff or power off;
8. Go to an optional URL within the default web-browser;
9. Send keystrokes to the active application on the target computer;

10. Listen for keystrokes on the remote system and save them to file;
11. Get a screenshot from the remote computer;
12. Upload any file to the target computer or update the server part of Netbus;
13. Increase and reduce the sound-volume;
14. Record sounds that the microphone catches - to listen to what happens in the room in which the remote computer is located;



*User interface of NetBus 2.0 Pro*

What makes NetBus special among hacking tools is that it has gone commercial. Since February 1999, NetBus has been marketed by its developers on the Internet. The latest version of the tool has been enhanced with new features and can be used as a generic remote access tool.

Older, free versions of NetBus have been detected by most anti-virus programs as trojan horses or backdoor utilities. The controversy over NetBus 2.0 Pro has concerned the commercial aspect: should anti-virus programs detect a tool that people are actually buying and using for day-to-day remote access? NetBus 2.0 can be used for good or bad, just like any other remote access program. Therefore, if NetBus is detected, shouldn't other tools, such as PC Anywhere, be detected as well?

"When NetBus went commercial, we decided not to add detection of the new versions to F-Secure Anti-Virus", explains Mr. Mikko Hyppönen, Manager of Anti-Virus Research at Data Fellows. "Then we started getting requests from some big clients about the possibility to add detection anyway - because we detected the older versions. So we added it."

F-Secure Anti-Virus detects known versions of NetBus.

## Sattelite

W97M/Sattelite is a Word macro virus with extraordinary functions.

This virus encrypts and decrypts its own code on-the-fly, making analysis and detection of the virus problematic. The encryption is done with multiple layers of XOR-based substitution.

Sattelite spreads whenever Word documents are opened or closed. It checks to see whether it has already infected a document by searching for this text in the document macros:

```
SATTELITE V1.5
```

The virus activates by modifying the registry so that the registered owner name of Microsoft Windows 95 or 98 will be changed to:

```
ThE wEiRd GeNiUs
```

W97M/Sattelite was found in the wild in February 1999.

F-Secure Anti-Virus detects and disinfects W97M/Sattelite.

## New virus hoaxes

Hoax messages keep circulating on the Internet. The most common of the latest new hoaxes is the so-called Jesus hoax.

This is a widespread hoax warning of an e-mail virus called "It Takes Guts to Say Jesus". Such a virus does not exist.

Here's a copy of the original hoax warning:

```
Virus Warning!!!!
```

```
If you receive an email titled "It Takes Guts
to Say 'Jesus'"
DO NOT open it. It will erase everything on
your hard drive.
Forward this letter out to as many people as
you can. This is
a new, very malicious virus and not many people
know about it.
This information was announced yesterday
morning from IBM;
please share it with everyone that might access
the internet.
Once again, pass this along to EVERYONE in your
address book
so that this may be stopped.
```

If you receive a message like the one above, do not forward the hoax.

## Common Questions & Answers

Data Fellows Anti-Virus Support will assist you with whatever questions you might have related to viruses and computer security. Please see the end of this section for contact information.

I download updated definition files regularly, but I have wondered how can I identify the date of the virus definition files currently in use?

Start a scan with the on-demand scanner and have a look at the scanning report: it lists the version of the scanning engines in use and the dates of the definition files. We recommend that users update at least on a weekly bases. Updates are provided daily on the Data Fellows web site.

### What is the easiest way to update the definition files for F-Secure Anti-Virus?

The simplest way to update F-Secure Anti-Virus is to download the self-installing update utility FSUPDATE and run it. It will take care of the rest.

FSUPDATE.EXE is updated daily and can be downloaded from the FSAV Web Club. Click on the World icon in F-Secure Anti-Virus to access the Web Club.

Web Club also contains more information on how to completely automate the daily download of definition files.



### Does F-Secure Anti-Virus support multi-user systems such as Citrix WinFrame, MetaFrame and Windows Terminal Server?

Yes. F-Secure Anti-Virus for Windows NT Server supports these systems natively?????. They are based on a modified version of Windows NT Kernel, but F-Secure detects and supports these systems automatically.

### I found a suspicious program called "Agent007" in my system - is this a virus?

There is no virus by this name. However, we sometimes get queries about "Agent007", as a program by this name is sometimes installed by a Telia internet access package.

After installing such package, you might find a program called AGENT007.EXE in your Windows directory and see a process called Agent007 on your task list. You might also see a value called "Spy" added to the Run entry of the Windows registry, executing the AGENT007.EXE program every time Windows is started.

While running, this program does not appear to do anything. However, it might sometimes generate error messages stating:

```
Invalid data type for 'Completed'
```

Although all this appears suspicious, the Agent007 program from Telia does NOT try to spy on the user or do anything else dangerous. This has been confirmed with the officials at Telia. There is no need to be concerned.

The purpose of Agent007 is to collect information about a possible earlier Internet connection and use that in the registration program to ease the registration process.

## F-Secure Anti-Virus Technical Support Services

The technical support services are available on the World Wide Web, through electronic mail and on-line through your F-Secure Anti-Virus

program. Your local F-Secure dealer provides local support.

F-Secure Anti-Virus Web Club provides help and assistance to F-Secure Anti-Virus users. To enter, choose the Web Club command from the Help menu.

To connect to the Web Club directly from within your web browser, open this location:

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

For advanced support, the F-Secure Anti-Virus Support Center is available on the Web:

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

If you would like to have us develop a new feature (user interface, compatibility, functionality, etc.), please use the bug report / feature request form on our web server, available for each F-Secure product through the Support Center.

### Virus Descriptions on the Web

Data Fellows maintains a comprehensive collection of virus-related information on its web site. To view the Virus Information Database, choose the command Virus Descriptions on the Web from the Help menu.

Alternatively, to connect to the Virus Information Database directly, open this location:

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

## Changes in F-Secure Anti-Virus Release 4.03

The new version 4.03 of F-Secure Anti-Virus detects and removes significantly more viruses than version 4.02 - although most of these updates have been available through the Internet for weeks. Adding a large number of PS-MPC-generated viruses has boosted the number of detected viruses to over 40,000.

F-Secure Anti-Virus 4.03 implements version 3.04 of the F-PROT scanning engine and 3.00



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

build 129 of the AVP scanning engine (build 126 in Windows 3.1x version).

Under Windows NT, the updating of version 4.03 from version 4.02 does not need administration rights. However, to load the new version requires a reboot. Until the machine is rebooted, 4.02 continues to run. In general, the stability of installation under Windows NT has been improved.

Note! If you are upgrading from version 4.01 or older, users need local administration rights to perform the update and normally, this prevents using the "Send update" option to distribute the update. For such an environment, F-Secure Intelligent installer can be used.

The Autoinst Wizard (executed from Administration/Distribute Installations) now automatically launches the F-Secure Intelligent Installation Wizard to configure FSII for hands-free deployments in NT networks.

The 95/98 version of Gatekeeper now also scans files during creation - in addition to scanning them during execution and opening.

The Windows 3.x version of Gatekeeper is now using the new AVP engine. Unlike other versions, Gatekeeper under 16-bit Windows does not use multiple scanning engines.

The 32-bit version of F-Secure Anti-Virus for OS/2 is now also running the F-PROT 3.04 level engine.

The development of a 16-bit version of F-Secure Anti-Virus for OS/2 has been discontinued. Technical support is still provided but no further updates will be available. We recommend upgrading to the graphical 32-bit version.

New version has many improvements in Autoinst Wizard, including the possibility to update installable files without changing Autoinst settings. The Autoinst Wizard now supports UNC names everywhere.

Windows NT Gatekeeper sometimes froze during formatting or when unformatted floppy disks were used. This has been fixed.

F-Secure FileCrypto used to cause problems for disinfection of Gatekeeper. This has been resolved.

The AVP engine memory scanner has been implemented under 95/98, in addition to the F-PROT memory scanner.

Support for NetWare volumes with long filenames has been improved.

NT Gatekeeper is better able to cope with a situation where an MBR boot virus is found during NT boot-up.

The uninstall functions have been improved to clean up the Start Menu.

The report file does not contain double "Infection: Infection:" reports any more.

The 32-bit versions do not contain 16-bit code any more, except for some internal 16-bit components of Windows 95 Gatekeeper.

Fixed the bug causing disinfected versions of files to be sent to administrator by the on-demand scanner (if the "Send infected files to administrator" feature was enabled).

Improved support for localised languages such as Greek.