F-SECURE

Contents

Product News 2
F-Secure Anti-Virus 5 will replace version 4 2
F-Secure Anti-Virus 5 for Windows 2000 2
F-Secure Anti-Virus Victorious at Virus Bulletin 3
F-Secure and HP to work on Mobile E-Services 3
F-Secure VPN+ Certified Under Latest Criteria 3
F-Secure Partners with Ensim's ServerXchange™ . 4
F-Secure Anti-Virus for WAP Gateways Introduced 4
F-Secure Corporation Reports Strong Growth 5
F-Secure Receives Technology Pioneer Award 5

Virus News 6
Babylonia 6
Button 6
Kak and Irok Worms 7
Melting 8

Frequently Asked Questions & Answers 8

F-Secure Anti-Virus Updates 9
Update Central 9
F-Secure Anti-Virus 5 9
F-Secure Anti-Virus 4 9

What's New in F-Secure Anti-Virus 10

Dear Customer,

F-Secure is going Wireless!

F-Secure Corporation is extending its leadership as a provider of centrally managed security solutions for the mobile, distributed, increasingly wireless enterprise. In April 2000, we launched the F-Secure Wireless Security Competence Center, which will focuses entirely on research and development of security solutions for hand-held systems such as PDAs and mobile phones.

The new competence center was kick-started by acquiring privately-held Modera Point Corporation. Modera was founded in 1982. It has headquarters in Oulu, Finland, and a subsidiary in San Jose, California.

MODERA

Acquiring Modera Point is a logical step in further strengthening our position as the architectural leader of pervasive security solutions. We will continue to grow into new areas of security – to the wireless world and beyond.

Best Regards,

Tanya Candia
Vice President of Worldwide Marketing

P.S. As you may have noticed, the F-Secure CD-ROM's numbering system has changed. This CD-ROM is version 7030. The number will increase for each new CD-ROM. This will make it easy to identify the latest CD-ROM. The Update Bulletin numbering system has also changed.

Please visit our web site for the latest information about F-Secure products and services! We welcome you at www.F-Secure.com.

F-Secure Update Bulletin 7030

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

http://www.F-Secure.com/

Product News

F-Secure Anti-Virus 5 will replace version 4

F-Secure Anti-Virus 4, which is based on our well-established anti-virus technology, has won many awards over the past eight years. The scanning engines in F-Secure Anti-Virus 4 have been updated constantly to fight the threat from document viruses, Internet worms, backdoor Trojans etc. The management features of Release 4 are, however, not scalable and flexible enough for modern enterprise networks. F-Secure Anti-Virus 5, on the other hand, has been designed with the modern networks in mind. The same award-winning anti-virus technology has been built into a modern policy based management system.

Both versions have been maintained in parallel since the summer –99 when version 5.00, the first new-generation anti-virus, was released. Version 5 is going to replace the old F-Secure Anti-Virus in the long run and the next step towards this will be taken this summer. F-Secure Anti-Virus 5 is already a mature product and the support for version 4 is going to be stepped down gradually. Updated anti-virus databases will still be available for version 4 but new features will no longer be implemented.

For customers using Windows 95, 98, or NT 4.0

F-Secure Corporation will continue to develop and maintain F-Secure Anti-Virus 4 until the summer 2000. The product will continue to be supported with virus signature database updates and technical support services until the end of 2000.

It is probably a good idea to get familiar with the new version right away. This gives you time to plan the upgrade and make sure that it goes smoothly. See http://www.F-Secure.com/products/anti-virus/workstations/ for more details about how to choose the right upgrade strategy.

F-Secure Anti-Virus 5.0 Service Pack 3 can be installed from this CD-ROM. You will first need to uninstall F-Secure Anti-Virus 4 if it is on your computer. The next major version, F-Secure Anti-Virus 5.1, will support automatic upgrading from version 4 to version 5. This will make upgrading a lot easier for customers currently running F-Secure Anti-Virus 4. Version 5.1 can be obtained electronically by sending a message to fsav-2000-download@F-Secure.com. You will receive instructions about how to download the new version of F-Secure Anti-Virus.

For customers using other platforms

F-Secure Anti-Virus 4 will continue to be developed and maintained for the platforms which are not supported by F-Secure Anti-Virus 5. These platforms include Windows 3.1, Windows NT 3.51, Linux, NetWare, OS/2, and DOS.

Please see the Upgrade Guide to learn how you can easily make the transition and immediately enjoy the benefits of this new major release.

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

F-Secure Anti-Virus 5 for Windows 2000

F-Secure Anti-Virus 5.1 will add Windows 2000 to the list of supported platforms. 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 receive the release version of F-Secure Anti-Virus for Windows 2000 electronically, should send a message to fsav-2000-download@F-Secure.com. The new version will be available to all customers with the next scheduled update.

F-Secure Anti-Virus Victorious at Virus Bulletin

F-Secure Anti-Virus has again received recognition when it found more viruses than any of its competitors in the latest comparative review in Virus Bulletin magazine.

For the first time since its release, F-Secure Anti-Virus 5 was submitted for comparative testing to Virus Bulletin magazine, which published the results in its April issue. The results were excellent. F-Secure Anti-Virus was awarded the prestigious “VB100%” award.

In the comparative review, F-Secure Anti-Virus detected 100% of ‘in-the-wild’ viruses, macro viruses, and polymorphic viruses. It achieved better detection rates than any of the competing products. And F-Secure Anti-Virus 5 was able to scan more file formats than any of the competing products.

“F-Secure Anti-Virus has undergone something of a makeover since its last appearance in a Virus Bulletin Comparative. A quick glance at the results shows that the high detection rates associated with this product still remain,” comments Virus Bulletin magazine.

The Virus Bulletin 100% awards recognize anti-virus products that are most capable of detecting viruses known to be ‘in the wild’ as reported by the WildList Organization. Virus Bulletin uses the most up-to-date WildList in its tests. The products that are updated most frequently are the ones most likely to be granted VB 100% awards.

The April 2000 VB100% is the latest in the long list of awards given to F-Secure Anti-Virus. This list includes:

- Anti-Virus Checkmark Level 2, West Coast Labs, March 2000
- Perfect in-the-wild macro scanner, Virus Test Center Hamburg, February 2000
- Comparative review winner, PCM magazine, February 2000
- 100% detection rate, University of Tampere, September 1999
- Editors Choice, PC Professionell (PC Magazine Germany), July 1999
- ICSA Anti-Virus certification, ICSA.net, June 1999

F-Secure and HP to work on Mobile E-Services

F-Secure Corporation and Hewlett-Packard Company have announced that they will be cooperating on a new solution to provide security as an e-service, following F-Secure’s entry into HP’s Mobile E-services Bazaar. The first result of this co-operation is F-Secure’s Anti-Virus for WAP Gateways software which will run on HP’s WAP gateway.

During March and April, F-Secure and HP hosted a world-wide series of seminars aimed at helping telecom operators, service providers, and business executives understand security issues in the mobile space. F-Secure and HP have been working together since January to bring to market innovative new solutions that advance secure wireless connectivity to the Internet.

F-Secure VPN+ Certified Under Latest Criteria

F-Secure Corporation has announced that F-Secure VPN+ is among the first products certified by ICSA.net for Version 1.0A of the Internet Protocol Security (IPSec). According to ICSA.net, only nine companies were able to meet all of the criteria in Version 1.0, let alone the additional requirements of Version 1.0A.

Certification assures customers that F-Secure products meet the security requirements based on industry-recognized standards.

F-Secure joins IBM, Lucent Technologies, and a handful of other leading companies in the first group of vendors with products certified by ICSA.net, the worldwide leader in security assurance services.

ICSA's certification program provides assurance that certified products reduce security risks consistent with publicly vetted and industry-accepted criteria, and are frequently upgraded to keep up with changes in technology and risks.

F-Secure Partners with Ensim's ServerXchange™

F-Secure Corporation has joined Ensim Corporation's Application Partner Program. The arrangement calls for incorporating F-Secure's renowned Security as a Service (tm) offering into Ensim's ServerXchange service deployment platform.

Ensim's software platform, ServerXchange™, can be used by ISPs, ASPs, and other providers to rapidly and cost-effectively deploy and manage outsourced application services. This solution has been architected to be highly scalable and automated.

Security as a Service enables customers to secure their entire enterprise transparently through their service provider. By choosing F-Secure's technology as one of the key building blocks of its ServerXchange platform, Ensim will allow ISPs' customers to offer secure remote administration functionality as a monthly service.

F-Secure Anti-Virus for WAP Gateways Introduced

F-Secure Corporation has introduced virus protection software for the Wireless Application Protocol. F-Secure Anti-Virus for WAP Gateways is the first product that protects wireless communications, transactions and e-commerce from new and emerging vulnerabilities and exploits, such as those that have been so prominent in the news lately.

F-Secure Anti-Virus for WAP Gateways provides protection against malicious code by checking for viruses and Trojan horses in the content to be transferred to WAP-enabled devices. The product detects and disinfects WAP-related malicious content transparently and automatically, and provides timely updates on malicious code detection activity. Like all F-Secure products, F-Secure Anti-Virus for WAP Gateways is based on the F-Secure Framework security architecture, which provides centralized policy-based management. The Framework Architecture tightly integrates this product with the range of security applications from F-Secure, including Anti-Virus for workstations and servers, file encryption products, network encryption applications, and distributed firewall products.

Vendors of mobile phones and WAP Gateways have implemented a high level of security in the WAP infrastructure from the beginning to insure confidentiality, privacy and authentication. However, these new devices, such as WAP phones, are combine functions of PCs and phones, introducing content that is

mobile and executable. Security for content has been unheard of in the telecom world, while it has been a focus for years in the PC environment.

There are no known instances of in-the-wild malicious code for WAP-based devices, but like any computing environment, WAP could become a target for malicious code. Several types of malicious code are theoretically possible. It is important that an infrastructure be built that can be quickly updated in order to detect and remove any future malicious code threats.

For major customers of WAP technology, this announcement signals that enhanced security of their highly mobile, wireless environment is now a reality. Through the F-Secure platform, they will be able to react quickly to future threats

F-Secure Anti-Virus for WAP Gateways is scheduled to be available later this spring for the Windows NT® platform and later on for the Linux and HP-UX platforms.

F-Secure Corporation Reports Strong Growth

F-Secure Corporation continued its strong growth last year, as reported in our 1999 Annual Report.

The revenues of the Group rose by 91% during 1999, reaching EUR 23.3 million (up from 12.2 million the previous year). A full 60% of the revenues came from anti-virus products (65% in 1998), and 40% came from cryptography products (35% in 1998). Revenues from North America accounted for 33% of total revenues; Scandinavia 33%, the rest of Europe 26%, and the rest of the world 8%.

Operating results were negative EUR 4.0 million (0.0) for the year. The operating income is a result of the Group's strategy of significant investments into product development and the growth of the sales and marketing organization. Personnel growth continued vigorously and headcount reached 302 (up from the previous year's 140). Personnel increased by 116%.

The Group also continued to recruit powerful systems integration and distribution partners, such as Siemens in Germany, Newlink in France, and Bay Data Consulting in the United States. The number of countries with channel partners grew to 93.

F-Secure Receives Technology Pioneer Award

F-Secure Corporation has received the Technology Pioneer Award from the World Economic Forum. At the annual meeting in Davos, Switzerland, the Forum recognized F-Secure's contributions to the impact that technology is having on social change and world economics.

F-Secure was one of approximately 50 top companies from around the world to receive the award. Winners included market leaders such as Red Hat Software, Healthlink, Siebel Systems, and Onyx Software Corporation.

The criteria for receiving the award were Innovation and rate of growth. The Forum recognized the world's fastest growing and most technologically innovative companies as important players in the new economy.

The criterion for growth was strictly mathematical; it was based on the last three reporting years. Innovation is measured by the WEF's own criteria, based on their research and analyses of corporations, and the international Deloitte Touche Tohmatsu research institution, together with experts in various industries.

Virus News

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

Babylonia

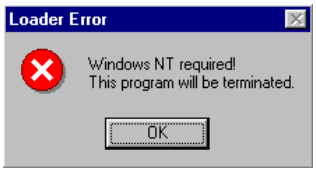
Babylonia is a Windows virus with worm and automatic update capabilities. The virus infects Windows executables and Help files (EXE and HLP). It also patches Windows socket library WSOCK32.DLL to send its copies to the Internet and drops an additional component that is able to download and install 'virus plugins' from the Internet.

The virus spreads itself by e-mail. It modifies the system so that every time the user sends an e-mail, the virus will include an attachment.

The attachment added by the virus is called X-MAS.EXE and it is about 17 KB long. Its icon looks innocent.

When the attachment is opened, the program displays fake error message boxes:

Under Windows 95/98, the virus displays 'Windows NT required', and under Windows NT, it displays 'Windows 95 required' to give the user the impression that the program is not compatible with the current operating system.



In fact, the virus works under Windows 95 and 98 quite okay. The virus uses calls that are allowed on Windows 95 and 98 only, so it is not able to infect Windows NT or Windows 2000 systems.

The virus also installs a file called BABYLONIA.EXE at the root of the C: drive. This program is designed to update the virus code on a regular basis. When the BABYLONIA.EXE file is run, it connects to a web site based in Japan and downloads a file called 'virus.txt' from there. This file contains a list of additional virus components or plugins. These files are then downloaded one by one. If there is no connection to the Internet, the update routine stays resident in Windows memory and each minute tries to connect to that site and get the files. When all files are downloaded and processed, the update routine exits.

The system seems to be designed to let the author of the virus continue developing additional malicious code to attach to the virus that is already in the system. The additional functionality could include installation of backdoors, fetching of documents, corruption of data, etc. This technology has never before been seen in a virus.

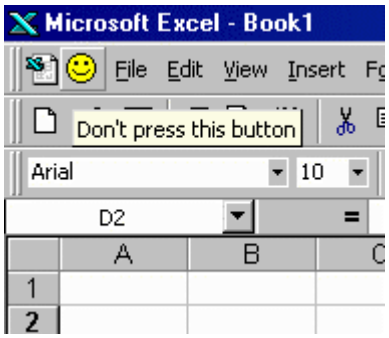
The website that was used to distribute the virus plugins has since been closed down.

F-Secure Anti-Virus detects and disinfects the Babylonia virus.

Button

X97M/Button is a simple Excel 97 macro virus. When an infected workbook is opened, X97M/Button.A infects all workbooks that are currently open in Excel.

During the process, it creates a temporary file, "C:\cmdbutton.bas", and adds a button of a smiling face to the menu bar of Excel.



F-Secure Anti-Virus detects and disinfects the Button virus.

Kak and Irok Worms

Two e-mail worms are currently spreading in several locations around the world. The Kak and Irok worms both spread via e-mail as electronic chain letters. F-Secure Anti-Virus detects and disinfects both Irok and Kak worms.

Technically, the Kak and Irok worms operate in very different ways, but both spread via Microsoft Outlook e-mail and are very widespread right now. The biggest difference to the end user is that Irok arrives in an attachment called IROK.EXE while Kak arrives in a normal e-mail, which apparently has no attachment at all.

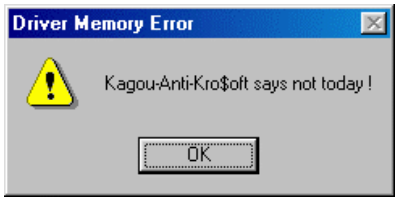
Both worms are only a threat to Microsoft Windows users and both worms only spread further via the Microsoft Outlook e-mail application.

The Kak worm is written in JavaScript. It works under English and French versions of Windows 95 and 98; it does not work under Windows NT or Windows 2000. Kak replicates further via e-mail only through Microsoft Outlook Express 5.0. It does not work with Microsoft Outlook.

The worm uses a known security vulnerability in Outlook Express to execute automatically when e-mail is viewed. Once the user receives an infected email message, and opens or views the message in the preview pane, the worm modifies the system in such a way that the next time the machine is started, the standard e-mail signature of the user is replaced with a HTML file infected by the virus.

As a result, every e-mail message after that will contain the worm and will infect the recipient's machine as soon as it is opened in Outlook Express.

The Kak worm activates on the first day of each month if the machine is restarted after 6 pm. At this time the virus will show this message:



After this, the worm will shut down Windows, but no permanent damage is done.

The Outlook Express security hole exploited by this worm can be closed by disabling "Active Scripting" in Outlook Express Preferences. Microsoft has also done an update to fix this problem. The update has been available since August 1999.

The Irok worm spreads as a 10001-byte sized program called IROK.EXE. It works under Microsoft Windows 95, 98, NT and 2000. It replicates further via e-mail if Microsoft Outlook is available. It does not work with Outlook Express.

When IROK.EXE is executed, the worm modifies the system so that during next time the machine is started, the worm will send an e-mail message to 60 e-mail addresses found in Outlook's address books. These addresses can be addresses of individual people or group addresses (such as mailing lists).

The message that the worm spreads itself with looks as follows:

From: (name of the infected user)
To: (random e-mail address from address book)
Subject: I thought you might like to see this.

Text: I thought you might like this. I got it from Paramount pictures
website. It's a Startrek screen saver.

Attachment: IROK.EXE

The virus also tries to locate the mIrc chat client and will attempt to modify it to spread the virus further via chat channels, and it infects COM and EXE program files found on the local hard drive.

Eventually, the virus will display a long message on the screen and will try to overwrite files on the hard drive.

F-Secure Anti-Virus detects and disinfects the Kak and Irok viruses.

Melting

Melting is an e-mail worm that appeared in March 2000. The worm itself is a 18kB l Windows program, written in VisualBasic. It spreads itself with e-mail messages by attaching its body as 'MeltingScreen.exe' to them. F-Secure Anti-Virus detects and disinfects the Melting worm.

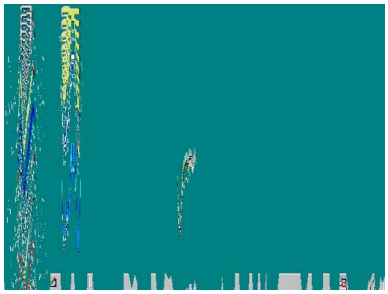
When an infected message is received and the attached worm executable is run by a user, the worm starts its spreading routine immediately. This routine connects to Microsoft Outlook, opens Address Book, gets e-mail addresses from there and sends messages with the attached worm body to these addresses. The infected message subject is 'Fantastic Screensaver', and the message body looks like this:

Hello my friend !

Attached is my newest and funniest Screensaver, I named it MeltingScreen.
Test it and tell me what you think.
Have a nice day my friend.

p.s.: Please install the Runtime Library for VB 5.0, before you run the ScreenSaver.

After this the worm renames all executables in \Windows\ directory from EXE to BIN, making the system unbootable. Finally the worm shows a video effect that resembles 'melting' of the screen:



The worm has bugs and often freezes the computer when run. It doesn't work if Visual Basic run-time libraries are not installed.

F-Secure Anti-Virus detects and disinfects the Melting virus.

Frequently Asked Questions & Answers

F-Secure Anti-Virus support provides help on all virus and data security questions. There is a comprehesive on-line FAQ database available in the F-Secure Anti-Virus Support Center at:

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

Q: Are UNIX systems immune to viruses?

A: Definitely not. Viruses can be written for any general-purpose operating system, and the very first viruses were actually written on UNIX systems. Still, viruses have never been a big problem on UNIX-based operating systems. It seems that this is because these operating systems haven't been as popular with people who write viruses.

Some new Linux-specific viruses have been found recently. Linux and other UNIX operating systems include many security features, but since viruses typically only require regular user-level access rights, they seem to spread happily on the systems. Fortunately, the number of Linux and UNIX viruses is still very small.

Q: I've heard of WAP viruses. Can WAP phones become infected?

A: No, not today. There are no known viruses in the wild that would be able to infect a WAP phone. The current WAP protocols do not have enough functionality to make real replicating viruses possible. A Trojan horse or social engineering type of attack is possible even with the current WAP systems, but currently there are no known incidents of these types of attacks.

The forthcoming WAP 1.2 standard will make it possible for downloaded WMLScript code to access telephony features of the phone, including browsing the phonebook, making calls, and sending text messages. This will make the phone much more vulnerable to attack, since the malicious code could send out copies of itself to other phones using these features.

Since all the new WAP phones are always networked, a virus outbreak could spread very fast from system to system. To provide customers with the ability to react fast and stop such viruses from spreading, F-Secure has announced a gateway-level product that lets the customer filter out unwanted content. F-Secure Anti-Virus for WAP Gateways is shipping on this CD-ROM.

Q: Where can I reach F-Secure Anti-Virus support services?

A: F-Secure Anti-Virus Web Club contains the most recent information on 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/

When contacting our support staff, it is best to use the support contact information you received when you bought the license. This will guarantee you the level of service you have paid for. However, you can always use the general support address:

Anti-Virus-Support@F-Secure.com

F-Secure Anti-Virus Updates

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

F-Secure Corporation ships new software versions on a CD-ROM every few months, but makes new virus signature databases available much more often via FSUPDATE and F-Secure BackWeb.

Update Central

For latest information about anti-virus updates, go to this web page:

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

F-Secure Anti-Virus 5

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

F-Secure BackWeb downloads files automatically, using bandwidth left unused by your other Internet applications. Therefore 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. F-Secure.com/ download-purchase/backweb.html

F-Secure Anti-Virus 4

The easiest way to download database updates for F-Secure Anti-Virus 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 F-Secure web server. The Web Club page has 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/

What's New in F-Secure Anti-Virus

- Added detection and disinfection of hundreds of new viruses since the last release.
- Improved disinfection of the PrettyPark virus.
- Removed false alarms from hard drive boot sectors.
- Accelerated scanning of very large executables and scanning of PowerPoint PPT files.
- NT version has improved compatibility with Novell's Client32.
- Fixed the "Macro.Word97.Polymac" false alarm.
- Added several new extensions to the default scanning list, including scanning of files with no filename extension.