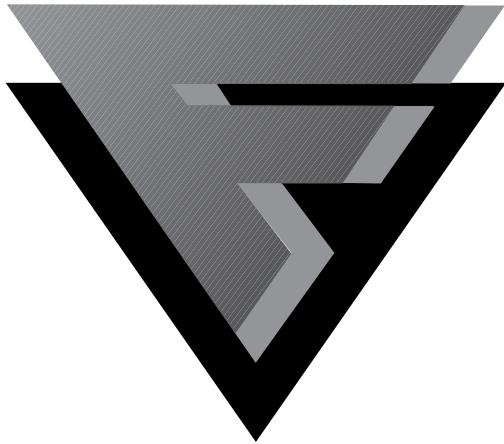


# F-SECURE



## *Double Protection*

With the previous version of F-Secure Anti-Virus, we introduced the groundbreaking Countersign technology. We offered you a possibility to test the power of this new technology by running two scanning engines in parallel under one hood.

Your feedback has been very positive. Therefore, we have decided to ship from now on by default two engines to all our customers.

On another note; with some sadness, we say farewell to two long-time competitors of ours. UK-based Dr. Solomon's Software was acquired by US-based Network Associates in the end of August, and earlier during the summer 1998, IBM sold the rights of their anti-virus research to Symantec.

As might be expected, Dr. Solomon's Anti-Virus Toolkit and IBM Anti-Virus will be discontinued.

In effect, this leaves Data Fellows as the leading European computer security vendor. Being European is especially important when considering the export-restrictions imposed on US-made encryption products.

Data Fellows is already offering a security suite solution, with integrated virus protection, local hard drive encryption and network encryption with strong export-free cryptography.

We estimate that integrated suite products such as *F-Secure Workstation Suite* will globally replace stand-alone virus protection and encryption products in the near future.

## *Table of Contents*

<b>News .....</b>	<b>2</b>
Data Fellows awarded "Best Bootstrap" by Red Herring .....	2
<b>Viruses on CD-ROMs and the Web .....</b>	<b>2</b>
July 1998.....	2
August 1998.....	2
<b>Virus News .....</b>	<b>3</b>
WM/PolyPoster.....	3
Back Orifice .....	4
First Java Virus Found .....	4
CIH.....	4
Marburg .....	5
Ivana .....	6
BadSector.....	6
New hoaxes .....	7
<b>Common Questions &amp; Answers .....</b>	<b>7</b>
<b>F-Secure Anti-Virus Technical Support Services.....</b>	<b>8</b>
Virus Descriptions on the Web .....	8
<b>Changes in F-Secure Anti-Virus 4.02.....</b>	<b>9</b>

## *F-Secure Anti-Virus Update Bulletin 4.02*

Copyright © 1998 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/>

## News

### Data Fellows awarded “Best Bootstrap” by Red Herring

Red Herring Magazine, the global authority on the Business of Technology, listed the world's Top 100 Technology Companies in their September 1998 issue.



Data Fellows was one of the “Private Company Superstars”, and was named the “Best Bootstrap” company.

Red Herring lauds us for our customer base, profitability and the fact that we have never used any venture capital.

## Viruses on CD-ROMs and the Web

During the summer, a surprisingly large amount of viruses was distributed by accident by software vendors.

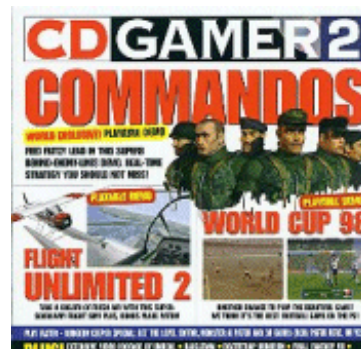
### July 1998

The Win95/Marburg virus got widespread circulation when it was included by accident on the cover CD of the UK-based **PC Gamer** magazine.

The infected files were on “CD Gamer 2”, and were called

```
\UTILS\XEARTH\XEARTH.EXE
\UTILS\QPAINT\QPAINT.EXE
\VIDEO\SMACKPLW.EXE
```

The SMACKPLW program is automatically executed when any of the preview videos from the CD are viewed.



There are localized versions of the PC Gamer magazine in circulation in addition to the UK edition. The Swedish edition had these files infected instead of the ones listed above:

```
\SHARE\3DJONG\M3DJONGG.EXE
\PATCHAR\QUAKE2\Q2-315-8.EXE
\SPEL\KKN2\DIRECTX\DDHELP.EXE
```

The Slovenian edition had the same infected files as the UK edition.

The Italian July/August edition was clean.

The Win95/CIH virus had infected a downloadable file on the **Yamaha** web in late July. The infected file was a CD-R driver update called yamaha10n.exe

There was also a widespread copy of game demo called **SIN** which was infected by Win95/CIH in July. However, this demo was infected *after* it was released by its manufacturers.

### August 1998

The Win95/Marburg was included on the master CD of the popular MGM/EA PC CD-ROM game **Wargames**.



The CD contained one file infected by the Marburg virus:

```
\EREG\EREG32.EXE
```

This CD was only distributed in USA. MGM is replacing the CDs for anybody affected.

Win95/Marburg was also on the cover CD of the Australian **PC Power Play** magazine.

This CD contained two files infected by the virus:

```
\GAMES\MAX2\MAX2BETA.EXE
\GAMES\STARTREK\FURYDEMO.EXE.
```

A version of the popular Wing Commander game called **Secret Ops** was available as an infected version on the Origin Systems web site in the Internet. The game was infected by the Win95/CIH virus.

## Virus News

### WM/PolyPoster

This virus uses advanced replication methods to spread within Microsoft Word documents. Once a machine becomes infected by the virus, all Word documents manipulated in it will become infected and the virus will spread within them to new machines.

However, the most disturbing part of the virus is in its activation routine. The virus activates at random times, and will try to send the user's Word documents to public Usenet news discussion groups. As an end result, the virus could post, for example, company confidential data or private love letters for the whole world to see.

The messages posted by the virus look like they are coming from the real user of the machine, complete with the user name and signature. The virus contains this list of newsgroups where it will attempt to post the messages:

```
alt.aol-sucks
alt.binaries.cracks
alt.binaries.pictures.erotica
alt.binaries.warez.ibm-pc
alt.conspiracy
alt.drugs.pot
alt.fan.hanson
alt.flame
alt.hacker
alt.sex
alt.sex.necrophilia
alt.sex.stories
alt.sex.zoophilia
alt.windows95
alt.sex.passwords
alt.binaries.warez
alt.binaries.sounds.mp3
alt.comp.virus
alt.2600
alt.2600.hackerz
alt.skinheads
alt.sex.babies
alt.sex.bondage
```

With these subjects:

```
Free XXX Passwords
Check this out!
Official WaReZ site list
Easy Money!
My first f**k by Todd
Hanson rulez!
WareZ mailing list details
Crackz mailing list details
Learn to hack!
Attn: All k3wl h4ck3rz
Important Info
New Virus Alert!
Serial Number List!
Official mp3 site list
Elite XXX site list
New erotic story
Important Princess Diana Info
Important Monica Lewinsky Info
How to find child pornography
Cable TV descrambler instructions!
Kewl N64 Emulator & MP3 sites
```

These groups have hundreds of thousands of people reading them all over the world.

To top it all, the posted documents are always infected by the virus, and users who view them in Word will get infected - and the virus will continue to spread from their machines.

Viruses which activate by simply deleting data are easy to recover from - by using backups. However, there is no way to recover from an incident where a virus posts confidential documents publicly to the Internet.

Traditional security methods like firewalls or Windows NT security settings will not prevent attacks like this. Viruses like WM/PolyPoster will arrive to users through



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

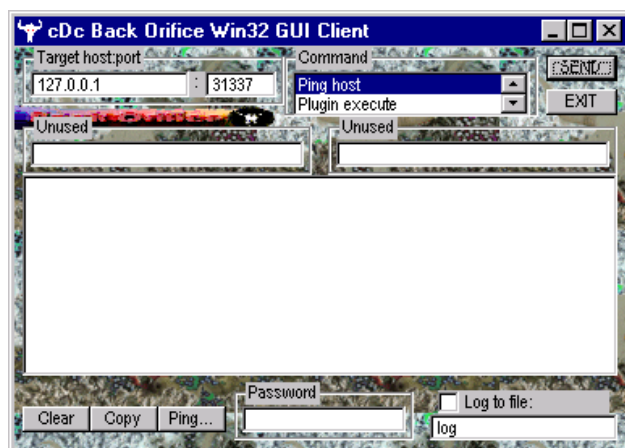
normal e-mail document attachments, and will further spread from the company's network with e-mail or standard Usenet news postings.

WM/PolyPoster is not known to be in the wild anywhere in the world.

F-Secure Anti-Virus detects and disinfects the WM/PolyPoster virus.

## Back Orifice

Back Orifice is a remote control tool released by the Cult of the Dead Cow (cDc) group. The trojan horse allows an intruder to monitor and tamper with Windows 95 and Windows 98 computers over the Internet. There is no easy way for a computer user to know the attack is taking place, and there is no easy way to stop the attack once Back Orifice has installed itself on the computer.



In a typical attack, the intruder sends the Back Orifice trojan horse to his victim as a program attached to e-mail. When the e-mail recipient executes the program attachment, the trojan horse opens connections from the computer to the Internet. This allows the intruder to control the computer. The trojan horse is invisible and will restart itself automatically even if Windows is re-booted.

Back Orifice allows a hacker to view and modify any files on the hacked computer. It can create a log file of the computer user's

actions. It can take screen shots of the computer screen and send them back to the hacker. Or it can simply crash the computer.

F-Secure Anti-Virus detects and removes the Back Orifice trojan.

## First Java Virus Found

Found in August 1998, StrangeBrew was the first virus to infect Java files. It is unable to infect or spread from Java applets which are executed over the Internet. However, it is able to spread from one Java applet to another if executed locally with a tool like Java Appletviewer.

StrangeBrew does not create new .class files, it searches for existing .class files and modifies them to include a copy of itself.

When the "infected" .class file is executed, the virus gains control and then passes control to the original code in the file.

When run, StrangeBrew searches the current directory for .class files. It includes its own code in the middle of the host .class files and modifies them to start the execution from the virus part. Virus adds the call to its own code as the first line of the "getParameter" method of the infected class.

StrangeBrew does not do anything else but spread. As such, it can not be considered a realistic threat. It has not been found in the wild.

## CIH

CIH virus infects Windows 95 and 98 EXE files. After an infected EXE is executed, the virus will stay in memory and will infect other programs as they are accessed.

It was first located in Taiwan in early June. After that, it has been confirmed to be in the wild globally. CIH has been spreading very quickly.



It seems that at least four underground pirate software groups got infected with the CIH virus, and they inadvertently spread the virus globally in pirated software they released through their own channels. These releases include some new games which spread world-wide very quickly.

What makes the CIH case really serious is that the virus activates destructively. While active, the virus overwrites most of the data on the computer's hard drive. This can be recovered with recent backups.

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

The Flash routine will work on many types of Pentium machines - for example, on machines based on the Intel 430TX chipset. On most machines, the Flash BIOS can be protected with a jumper. By default, protection is usually off.

CIH works under both Windows 95 and Windows 98, but it does not work under Windows NT.

There are four known closely-related variants of CIH:

CIH v1.2 (CIH.1003): Activates on April 26th. This is the most common variant. It contains this text:

```
CIH v1.2 TTIT
```

CIH v1.3 (CIH.1010.A and CIH.1010.B): Activates on June 26th. It contains this text:

```
CIH v1.3 TTIT
```

CIH v1.4 (CIH.1019): Activates on 26th of every month. It is in the wild, but not particularly common. It contains this text:

```
CIH v1.4 TATUNG
```

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

## Marburg

Marburg is a polymorphic Windows 95/98 virus which contains this text:

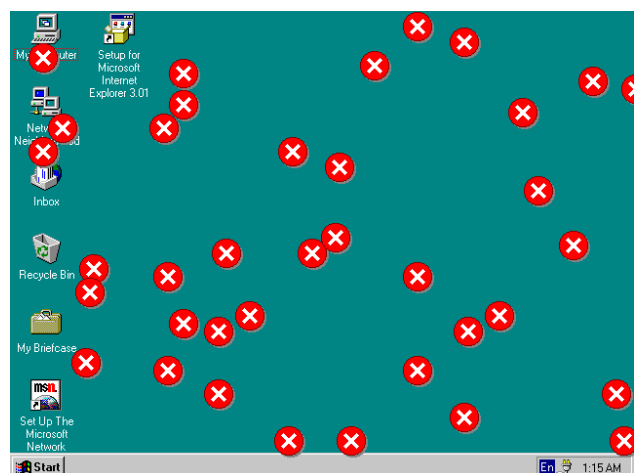
```
[ Marburg ViRuS BioCoded by GriYo/29A ]
```

Marburg infects Win32 EXE and SCR (screen saver) files, encrypting its own code with a variable polymorphic encryption layer.

The polymorphic engine of the virus is advanced. It encrypts the virus with 8, 16 and 32 bit keys using several different methods. The virus uses slow polymorphism, which means that it changes the decryptor of itself very slowly.

Marburg deletes integrity databases of several anti-virus products. It also avoids infecting many known anti-virus product executable files, including any executable which has the letter "V" in its name. This is to avoid triggering the self-check of these programs.

Marburg activates three months after the initial infection. If an infected application is executed exactly on the same hour as the initial infection, the virus displays the standard Windows error icon (white cross in red circle) in random positions all over the screen.



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

## Ivana

Ivana is a Word macro virus. It spreads when infected documents are exchanged.

Ivana contains the following text strings:

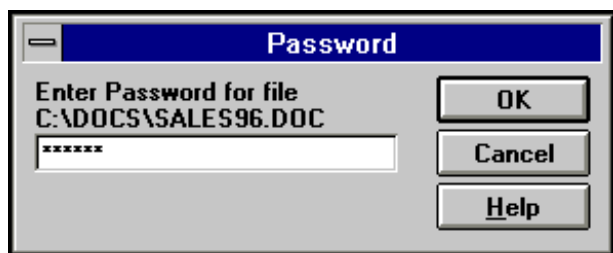
```
' Dedicated to Ivana, the only one
' [by utik]
```

This virus has a sequence of payloads. On Sundays the virus removes the Word formatting bar from the screen. On Mondays it removes the vertical scroll bar from the document window.

On the 13th day of each month the virus inserts 10 empty lines and the following text to the end of the infected document:

```
'Na kraju, samo jos da kazem: volim te, Ivana
[by utik]
'And finally, I would like to say: I love you,
Ivana [by utik]
```

On the 4th of July the virus performs its nastiest trick. It adds the word 'Ivana' to the end of the document, sets the document password to 'Ivana' and saves the document to disk. The document becomes inaccessible to the user who doesn't know the password.



The Ivana virus also disables 25% of all undo operations. Finally the virus changes the function of 'Underline' macros - instead of changing font properties to underlined the macro changes them to **bold**.

F-Secure Anti-Virus detects and disinfects the WM/Ivana virus.

## BadSector

*By Eugene Kaspersky*

This trojan was sent to several newsgroups in August 1998. It was also mailed directly to thousands of people with a spam e-mail program. The e-mail message presented the trojan as a file named IE080898.EXE and claimed it was a security update for Internet Explorer.

The faked spam message looked like it was coming from Microsoft:

```
From: IESupport@microsoft.com
(Microsoft Internet Explorer Support)
Date: 08/07/98 03:40:04 PM
Subject: FREE! Your upgrade for Microsoft
Internet Explorer
```

```
As user of Microsoft Internet Explorer
Microsoft Corporation provide you an upgrade
for your Microsoft Internet Explorer. Please
run Ie080898.exe to install the upgrade. This
file will fix some serious bugs in your
Internet Explorer.
```

```
For more information please visit Microsoft
Internet Explorer Home Page at:
http://www.microsoft.com/ie/
```

```
Attachment: Ie080898.exe
```

In fact, the original e-mail message was sent from Bulgaria.

When executed, the trojan installs itself as part of the Windows system and randomly sends e-mail messages to the Internet. These messages are sent to a list of addresses - obviously to irritate these people.

The trojan itself is a 25 KB Windows executable file written in Pascal. It accesses network and sends random messages to the Internet.

When run for the first time the trojan just installs itself in the system. It copies itself to the Windows system folder with the name SHELL32.EXE.

The trojan then terminates with no side effects. After the next reboot the trojan stays in the Windows memory as a hidden task, sleeps and periodically initializes Windows Socket APIs and opens a stream



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

socket with TCP/IP protocol for sending messages.

The messages have random selected addresses, subject and data. The "Mail From" address is randomly constructed from the following parts:

```
1 bulgaria badsector hacker omega vali-pedali
eunet digsys

2 main vt linux aix unix mail www host abc
server veliko-tar

3 prodigy compuserve kurva putka gerry tetra
europe amstel usa

4 com edu org mil gov net bg tr gr uk ca ro jp
```

For example, bulgaria@main.prodigy.com

The recipient address is randomly selected from these:

```
gerry@tetra.bg
administrator@tetra.bg
tetrinet@tetra.bg
root@vt.bitex.com
peterc@vt.bitex.com
ivanp@vt.bitex.com
root@tarnovo.eunet.bg
master@tarnovo.eunet.bg
webmaster@tarnovo.eunet.bg
root@server.vt.bia-bg.com
webmaster@mail.vt.bia-bg.com
webmaster@tetra.bg
```

The subject is randomly selected from these variants:

```
Ha-ha-ha
Bad Sector wi razkaza igrata :))
Greetings from Bad Sector ! Po-zdrawi
Vleze li wi sega?
Re
Hi, kak e?
Ko staa, ima problemi li
Bad Sector
Kogato grum udari...
```

The sentences of the message body are randomly constructed from a large set of verbs, other words and sub-sentences. Some of these are vulgar, and they are mostly written in Bulgarian.

F-Secure Anti-Virus detects and removes the BadSector trojan.

## New hoaxes

Hoax messages keep circulating the Internet.

### Disney World hoax

This is a chain letter. Although this one is not related to viruses at all, we list it here as it has become seriously widespread.

The hoax looks like this:

```
If you read below you will see the note from
Walt Disney Jr. & Management at Disney World.
Basically if this messages reaches 13,000
people, everyone will receive $5,000.00 or a
free, all expenses paid, trip to Disney World
in anytime during the summer of 1999.
```

Do not forward this chain letter.

### Bud Frogs

This warning about a possible trojan horse circulates the Internet. No antivirus lab has seen a sample of the original file, so this can be considered a hoax.

Here's a copy of the original warning:

```
DANGER! VIRUS ALERT!
```

```
THIS IS A NEW TWIST. SOME CREEPOID SCAM-ARTIST
IS SENDING OUT A VERY DESIRABLE SCREEN-SAVER
{{THE BUD FROGS}}. IF YOU DOWN-LOAD IT,
YOU'LL LOSE EVERYTHING!!!! YOUR HARD DRIVE
WILL <<>> CRASH!!
```

```
DON'T DOWNLOAD THIS UNDER ANY CIRCUMSTANCES!!!
IT JUST WENT INTO CIRCULATION ON 05/13/97, AS
FAR AS I KNOW!!
```

```
PLEASE DISTRIBUTE THIS WARNING TO AS MANY
PEOPLE AS POSSIBLE...
```

Ignore this warning and do not pass it on.

## Common Questions & Answers

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

**I'm running Windows 95. It seems that my machine is accessing the Internet on its own. Also, I found a suspicious task called TSADBOT from my computer's memory. Is this a virus?**

Some shareware applications install a Win95/98 process by this name. Tsadbot is a process which connects to an



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

advertisement server over the Internet and downloads new advertisements to the display while using the product.

Tsadbob is included at least with the Windows version of the popular PKZIP archive utility.

For more information, see <http://www.timesink.com>.

### **I upgraded to Windows 98. Does F-Secure Anti-Virus for Windows 95 work in Windows 98?**

Yes, it does. From a technical point of view, Windows 98 is very similar to Windows 95, and most programs written for 95 work also in 98.

### **My machine started playing music by itself. It does this even if I cold boot from a clean floppy. I formatted my hard drives and it still won't stop!**

Is the song "Für Elise"?

Some motherboards play music when there is a hardware problem, check your hardware manual.

For more information, see:

<http://www.dfiusa.com/music.asp>

### **I'm running a palmtop machine based on the Windows CE operating system. Do viruses work on it?**

No, they don't, yet.

Known binary Win32 viruses won't work under Windows CE, as CE uses different API calls. In fact, most of the CE machines are not even running on Intel processors.

DOS viruses won't work, as Windows CE has no DOS.

Word and Excel macro viruses won't work, as the included Pocket Word and Pocket Excel lack the support for macro languages.

So, in effect, you can't infect your CE machine at this time.

Of course, you can receive an infected file and transmit it to someone else via a CE.

### **My F-Secure Anti-Virus runs very slowly after upgrading from Windows 95 to Windows 98. Is there a solution?**

Try uninstalling and reinstalling F-Secure Anti-Virus.

## **F-Secure Anti-Virus Technical Support Services**

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

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/anti-virus/support/>

If you would like to see a new feature developed (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



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

Database, choose the Virus Descriptions on the Web command 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 4.02

New version detects and removes over 1000 viruses more than version 4.01 – although most of these updates have been available through Internet for weeks.

New F-Secure Anti-Virus for Windows 95/98 supports Windows 98 fully.

Incompatibility with a display driver for a *Number Nine* display card has been fixed.

Earlier version caused extra network traffic by reading the communication directory every six minutes.

F-Secure Anti-Virus now has better support for scanning corrupted Word document files.