

F-SECURE

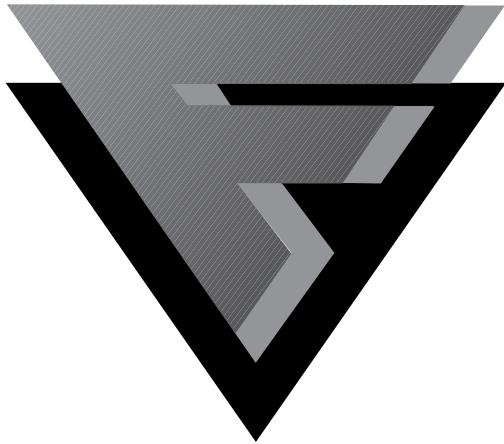


Table of Contents

F-Secure Anti-Virus: Phenomenal Success in the Press	2
Data Fellows Certified Anti-Virus Centers ...	4
Virus News	5
Number of macro viruses now over 2000	5
F-Secure Anti-Virus Disinfects Access Macro viruses.....	5
First Excel Formula viruses found	7
Win95/Anxiety.....	10
WM/Kompu.I.....	11
Win32/RedTeam	11
Win32/Net666.....	12
WM/NikNat	13
Hoaxes.....	13
CounterSign™ Framework	14
The Anti-Virus Challenge	14
Data Fellows Victory: Synergy Through CounterSign™ Technology	16
Upgrading from F-PROT Professional to F-Secure Anti-Virus.....	19
Common Questions & Answers	20

A New Era

This is the first update of F-Secure Anti-Virus to our existing F-PROT Professional customers. It marks the beginning of a new era, as we change from the traditional virus scanning architecture to CounterSign architecture.

CounterSign architecture has been in development for over a year. It is now delivering the promise of a universal Anti-Virus platform. Thanks to the open architecture, we can now use several independent scanning engines inside our product, boosting detection rates to maximum.

As a proof of the concept, this version of F-Secure Anti-Virus contains two scanning engines: The tested and trusted F-PROT engine and a newer engine from Russia called AVP (Anti-Viral Toolkit Pro). Together these engines will practically find any virus, old or new. The AVP engine is provided for free so you can test the concept - in future versions AVP scanning engines will be licensed separately, while the F-PROT engine is included in the base package.

Most of the changes in the new version are under the hood. The user interface and network functionality stays the same. The new version can reliably be updated over existing installations, like any other update.

At the same time with the big technological changes, also the name of the product changes. F-Secure Anti-Virus complements the Data Fellows range of F-Secure cryptography products, such as F-Secure Desktop and F-Secure VPN. F-PROT still continues as the name of the scanning technology within F-Secure Anti-Virus.

F-Secure Anti-Virus Update Bulletin 4.01

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/>

F-Secure Anti-Virus: Phenomenal Success in the Press

Ever since the F-Secure Anti-Virus product line was announced the feedback we've got has been overwhelmingly positive. On paper, it seems obvious that a product with several scanning engines should easily beat any other product using just a single engine. It was time to test this in practice.

Pre-release versions of F-Secure Anti-Virus have been tested by international press and the results are impressive: Our products have had a victory in every test they have participated: Eight victories in two months. The Anti-Virus industry has never seen anything like this.



ICSA CERTIFICATION May 5, 1998

F-Secure Anti-Virus, the world's first multi-engine anti-virus, has been certified by the International Computer Security Association, ICSA (formerly NCSA).

To be certified by ICSA, products and systems must pass a rigorous set of tests. ICSA performs the full set of tests annually, spot checking for compliance throughout the year using the latest version of each product. Buyers of ICSA Certified Products can be assured that these are the most secure products available.

Earlier this year, ICSA certified Data Fellows' F-Secure SSH and F-Secure VPN in its debut certification of cryptographic systems.



Personal Computer World (UK) February 1998

F-Secure Anti-Virus was awarded the "Highly Commended" title. It scored 99.9% overall detection being the best product, tested against Dr. Solomon's HomeGuard, IBM AntiVirus, Inoculan AntiVirus and McAfee VirusScan.

"Any doubts about the product's approach are dispelled by the results, which are outstanding."

"Best anti-virus software you can buy."



PCWindows Magazine (Italy) February 1998 comparative review

F-Secure Anti-Virus for Windows 95 received brilliant results in the PCWindows comparative review. CounterSign Technology was reported as being well above our competitors' technologies and the overall result was that F-Secure Anti-Virus can be recommended for all kinds of users. "This is the scanner virus writers hate the most". We could not have said it better ourselves.



PC World Magazine (Spain) February 1998 comparative review



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

The Spanish edition of the PC World magazine ran an extensive comparative review of Anti-Virus products in their February 1998 issue. F-PROT 3.01 was included, and it won the test and got the magazine's recommendation.

Results of the PC World review tests:

F-PROT 3.01	8.2
Panda Antivirus 5.0	8
Norton Antivirus 4.0	8
Dr Solomon	7.8
Antivirus Anyware	7.7
McAfee VirusScan 3.1.4	7.6
Thunderbyte Antivirus 8.03	6.8



Virus Bulletin February 1998 comparative review

Virus Bulletin Magazine is known as the authoritative publication on computer viruses worldwide. F-Secure Anti-Virus was awarded the sought-after VB 100% award in Virus Bulletin's extensive February 1998 DOS comparative review. The award means that F-Secure Anti-Virus detected all samples from Virus Bulletin's In the Wild File and In the Wild Boot virus collections.



PC Actual Magazine (Spain) February 1998 comparative review

The Spanish PC Actual magazine ran a comparative review of Anti-Virus products in their February 1998 issue. Our product won the test and got the magazine's recommendation.

F-Secure Anti-virus	93.1%
AVP	92.7%
Solomon	91.4%
ThunderByte	89.1%
Panda	88.3%
McAfee	87.9%
Norman	86.1%
Norton	85.5%
Anyware	79.2%



MikroDatorn Magazine (Sweden) January 1998 review

In the January 1998 issue of the Swedish MikroDatorn Magazine, our products were praised as having "excellent and simple functions for automatic updates and virus alerts over networks", and also emphasized how important it is that we can protect against unknown viruses. "Efficient!"

As final score, the product got 5 out of 5.



Tietokone Magazine (Finland) January 1998 comparative review

Here F-PROT was tested against five other leading Anti-Virus products. We got the highest score and were also awarded Editor's Choice.



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

The Tietokone magazine especially praised our manual, updates, language support and support services. Results:

F-PROT	46
Cheyenne	42
Sophos	42
Solomon	41
Norman	41
McAfee	38



Secure Computing Magazine January 1998 comparative review

Secure Computing is one of the most important trade publications in computer security field. They had an extensive comparative review on twenty Anti-Virus products in their January 1998 issue. In the test, F-Secure Anti-Virus found more macro viruses than any other product and was awarded the "SC Recommended" title. Here are the results of the Secure Computing macro virus detection tests:

F-Secure Anti-Virus	99.6
Antiviral Toolkit Pro	99.4
McAfee VirusScan	99.2
Dr Solomon's Anti-Virus	99.2
IRIS Antivirus	97.2
Sophos Anti-Virus	96.8
Norman Virus Control	96.5
ThunderByte	96.3
PC-cillin Corporate Edition	96.0
VACMan/AVAST32	94.0
Command Anti-Virus	93.9
IBM Antivirus	93.1
Norton Antivirus	92.9
VET	92.75
InocuLAN Antivirus	88.8
eSafe Protect	84.4
LANDesk Virus Protect	78.6
AVG	67.1
VirusUTILITIES	53.45
Panda Antivirus	52.99

Secure Computing writes: "...absolutely first rate detection of viruses in our in-the-wild test suite...detection of polymorphic viruses in our extended test suite is simply perfect... performance against our full collection of viruses is similarly impressive...product didn't return a single false alarm and this shows the excellence of the scanning engine which is precise and well-targeted..."

Data Fellows Certified Anti-Virus Centers

Data Fellows has created a worldwide chain of Certified Anti-Virus Centers (CACs). The centers provide highly qualified expertise in virus defense and research.

The chain is based on a certification program for the technical staff of its partner companies. CACs provide support against virus attacks, and actively participate in both local and global research.

Every Certified Anti-Virus Center is staffed by a dedicated team of world-class anti-virus experts. Each CAC has at least one Certified Anti-Virus Expert (CAE), who has passed the most stringent of tests by Data Fellows.

The CAE tests are extremely demanding. Certified Anti-Virus Experts are not just experts on the F-Secure Anti-Virus product line, but also on highly technical anti-virus issues. They monitor potential threats to end-users and corporations, predict future hazards, and detect and destroy computer viruses daily. Most CAEs have several years of experience in viruses and data security.

Over the past decade, Data Fellows has built an extensive network of partner companies and distributors in over 80 countries. Emphasis has always been



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

placed on potential partners' technical expertise, because we believe that this is the most crucial qualification in the data security field. Now we offer our highly knowledgeable partners the opportunity to become certified.



Data Fellows started the certification process in October 1997. So far, the tests have been conducted 41 times. Currently, the Data Fellows CACs are located in Belgium, Estonia, Finland, Germany, Hungary, Hong Kong, Italy, Japan, the Netherlands, Norway, the United Kingdom, Slovenia, South Africa, Sweden and the USA. The coverage will be extended to 10 more countries during 1998.

No other anti-virus vendor has such an extensive network of Certified Anti-Virus Centers. We are pleased to be able to offer our clients and the data security industry our unique anti-virus expertise.

Virus News

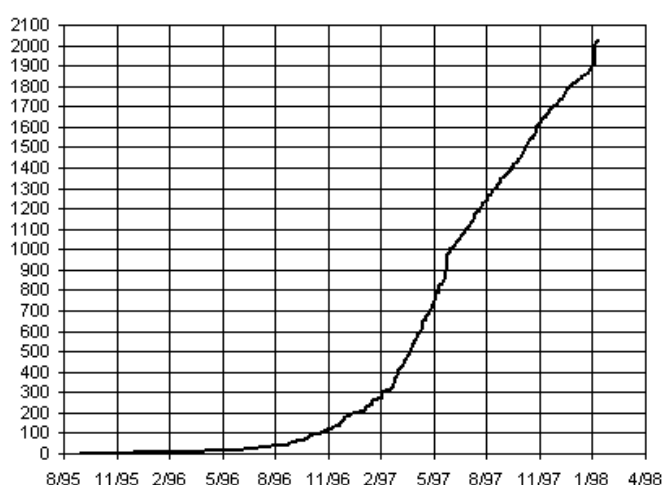
Number of macro viruses now over 2000

The number of known macro viruses soared over 2000 in February 1998. F-Secure Anti-Virus handles them all.

Macro viruses are computer viruses written in the macro or formula language of word processing and spreadsheet application programs. They spread when infected

documents are transferred. Currently, the most vulnerable applications are Microsoft Word and Microsoft Excel. Viruses such as Concept, Wazzu, Npad and CAP have spread internationally.

Many macro viruses do nothing significant beyond global spreading, but some overwrite data, modify the contents of documents, and even send documents out of a company via e-mail. To complicate matters, they can also "mutate," or change their form. Macro viruses cause most of the infections in the world today.



Number of macro viruses from August 1995 to March 1998

F-Secure Anti-Virus Disinfects Access Macro viruses

Data Fellows the First to Solve the New Macro Virus Problem

F-Secure Anti-Virus is the first anti-virus program to detect and disinfect the recently discovered Microsoft Access macro viruses.

Detecting Access macro viruses can be done simply by scanning the Microsoft Access database files (also known as MDB files) from beginning to end. However, the



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

size of a large database file can be several hundred megabytes, and using a simple scan would take hours. The time required can be shortened dramatically, if the scan is performed on the macro area of the file only. But in order to do this, an anti-virus product must be able to parse the complex and undocumented structure of Access database files.

Thanks to its modular CounterSign architecture, F-Secure Anti-Virus already has the technology to not only quickly detect, but also accurately remove macro viruses from Access files.

The quick solution to the Access virus problem was provided by AVP, one of the scanning engines used by F-Secure Anti-Virus. AVP is able to isolate the macro areas of Access files, and thus perform a scan in a fraction of the time needed by other engines. This technology also allows F-Secure Anti-Virus to disinfect Access macro viruses quickly and accurately.

As the AVP engine is extraordinarily extendible, its scanning behaviour can be changed dramatically with a simple update file. Therefore F-Secure Anti-Virus is already up-to-date with the new virus threat.

The different scanning engines within F-Secure Anti-Virus use different approaches to problems such as this, and enable F-Secure Anti-Virus to offer its users a comprehensive range of solutions.

About Access Macro Viruses

The first macro viruses to spread within Microsoft Access database files were found on the Internet at the end of March 1998. Until then, macro viruses had only been found in Microsoft Word and Microsoft Excel applications. However, Microsoft Access uses a macro language similar to that of Word and Excel, and can

therefore easily operate as a carrier for macro viruses.

At the moment, the risk of being infected by an Access macro virus is fairly small. Unlike Word and Excel documents, Access files are not frequently shared between companies or sent via e-mail. However, there are two ways in which Access macro viruses could become more common:

1. If a vendor (such as a third party developer using Access as a back-end server) ships a commercial application with an infected MDB file; or
2. if a virus-writer successfully creates a cross-platform virus which infects several MS Office application files, such as Word DOC, Excel XLS and Access MDB files.

Because of these possibilities, anti-virus research groups have put a lot of time and effort into developing the scanning of Access MDB files.

AM/AccessiV

AM/AccessiV infects Microsoft Access database file (*.MDB). It is known by several different names, such as AccessiV, JetDB, A97M/AccessiV and Jerk1n.

AccessiV only replicates under English Access 97.

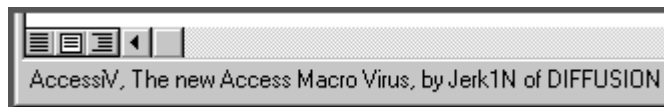
The virus replaces in databases the Autoexec script ("macro" in Access terms) and copies additional macro ("module" in Access terms) to the database. This macro is called "virus".

When infected database is opened, the Autoexec script is activated. It immediately calls virus function named "AccessiV" which searches for all databases (*.MDB) in the current directory and infects them. The current directory is normally the one set in Tools/Options/General/Default Database Folder, but can be something else if the user was working with files in another



directory before opening an infected MDB file.

While infecting, the virus changes the status bar message to 'AccessiV, The new Access Macro Virus, by Jerk1N of DIFFUSION'.



The virus displays this message in Access status bar while infecting other databases

The virus does not manifest itself in any other way. It contains these comments:

```
Find MS Database File!
Find another MS Database File!
```

A later variant, AM/AccessiV.B is also able to infect MDB files in other directories.

AccessiV.B activates on the 3rd of every month, by creating a program through DEBUG script and activating it.

AccessiV.B contains these texts:

```
I am the AccessiV virus, Strain B
AccessiV was/is the first ever Access Virus!!!
AccessiV - Strain B
```

It should be noted that AccessiV infections bloats the size of the infected databases, especially if the database has been infected multiple times. Once databases have been disinfected with F-Secure Anti-Virus, you can reclaim the wasted space by opening the database in Access and selecting Tools/Database Utilities/Compact Database.

A separate version of this virus, converted to work with Access 2.0, is also known to exist. Although the known versions of the virus do not work under Access 95, they are still able to infect MDB files made with it. If such files are opened to Access 95, nothing special happens and they work normally. However, if the same file is opened to Access 97, the virus will continue spreading.

AM/Detox.A

Detox is the third known macro virus to infect Access databases. This virus infects all database files all directories on the same drive as the virus.

Detox consists of a module called TDU and has a macro called Autoexec. Autoexec is automatically executed when an infected MDB file is opened. This virus can not be stopped by holding the shift key while opening the database. This is because the virus changes Access Properties including AllowSpecialKeys, AllowBreakIntoCode and AllowBypassKey respectively.

The virus does not activate in anyway but it does contain these comments:

```
The Detox Unit Access Macro Virus
written by Sin Code IV
(an old friend by any other name...)
```

Since the virus turns off the Show Hidden Objects flag and deletes the *Tools/Options* menu, the macro code can not be easily viewed. This can be bypassed by choosing *View/Toolbar/Customize/Reset* command. When doing this, the an infected database should be kept open - otherwise the virus in Autoexec macro would delete the Tools menu again.

First Excel Formula viruses found

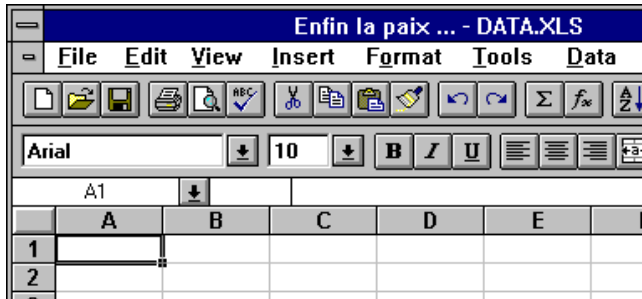
By Vesselin Bontchev

By the end of January 1998 we received an interesting sample of a new kind of macro virus for Excel. Reportedly, the virus was in the wild in France. The most interesting thing about it was that, unlike all Excel viruses known so far, it contained no VBA modules - so there were no traditional macros at all.

According to the initial reports, it worked only under the French version of Excel95 and was implemented entirely in as cell formulas. Its payload, invoked with a



probability of 1%, was to set the title of Excel's window from "Microsoft Excel" to "Enfin la paix..." ("Peace at last..." in French), so we decided to name it ExcelFormula/Paix.A, or XF/Paix.A for short.



XF/Paix activates by changing the title of Excel to "Enfin la paix ..."

The above preliminary information turned out to be not entirely correct. For instance, we discovered that the virus infects and replicates happily under any language version of Excel95. It is unable to infect a clean Excel97 system - however, if the system is already infected (e.g., because Excel95 was installed and used in the past and the virus has infected the system then), the virus will have no problems replicating under Excel97 too.

Also, calling it a "formula virus" isn't quite correct. We were afraid that, if the virus was indeed implemented as cell formulas, scanning for such viruses would cause a tremendous slowdown of our scanners - because essentially all useful Excel workbooks contain some kind of formulas, which means that there wouldn't be a fast and easy way of determining that a workbook is not infected. Fortunately, the virus does not consist of "normal" cell formulas. Instead, it is implemented as a Excel 4.0 macro sheet - although it relies heavily on the extensions to the Excel 4.0 macro language introduced first in Excel 5.0 and cannot run under Excel 4.0. An Excel 4.0 macro sheet has cells just like a normal sheet, and its operators look very

much like cell formulas - which explains the initial confusion.

The virus consists of five separate routines. We shall describe them one-by-one, in their order of appearance in the virus code.

The main purpose of the routine Auto_ouvrir (Auto_open in French) is determine whether the system is already infected, infect it if it is not the case, and activate the virus, so that it begins infecting. The routine first disables the error checking, so that Excel does not display any messages if an error occurs and continues with the execution of the macro. Then it disables the screen updating too. Its next task is to determine whether the name of the active workbook is "xlsheet.xla" and, if that is the case, to prevent the routine activation_feuille on the sheet !!!GO from running, if that sheet resides in a workbook named TEST1.XLS. That is probably how the virus writer's sample has been named and the above gymnastics prevent the virus from getting out of control on its author's system.

The next step is to convert the current workbook (i.e., the workbook where the virus is run from) to an add-in named "xlsheet.xla" and residing in the directory where the virus has decided to install itself. This is precisely the command which fails under Excel97 and this is the reason why this particular virus is unable to infect clean Excel97 systems.

Finally, the virus activates the !!!GO macro sheet containing its code, uses the add-in manager to instruct Excel that the xlsheet.xla add-in is installed and restores the screen updating and error handling.

The activation_feuille routine takes care of replicating the virus to new workbooks. Its first actions are to obtain the name of the currently active workbook, to turn off the screen updating and error reporting, activate the xlsheet.xla add-in, and to

unhide the !!!GO sheet both in the add-in and in the current workbook. If no error occurs during the last action, it means that the current workbook already contains a sheet named like that - so, it is assumed to be infected by the virus. In this case the virus calls the GO routine which contains its payload. Otherwise the virus copies the "!!!GO" macro sheet from the add-in to the active workbook and saves the workbook - i.e., it replicates. Finally, the virus hides the "!!!GO" macro sheet both in the add-in and in the newly infected workbook and restores the screen updating and the error handling.

The GO routine contains the payload of the virus. Its first action is to turn off the error messages. Then, with a probability of 1% it does the following. First, it hides all menus. Then it hides all the 13 standard button bars. Next, it hides the formula bar, the status bar, the display of outline symbols and zero value, the horizontal and vertical scroll bars, and the sheet tabs - all of these are configurable via the Tools/Options/View menu. Finally, the virus hides all opened workbooks and changes the title of Excel to "Enfin la paix...", leaving it (and the user) in a rather confused state. The last action of this routine is to re-enable the error messages.

An interesting question is, since the virus uses French names for its Auto_Open and Auto_Close routines, why does it replicate under any other language version of Excel too? The key to the answer lies in the protect routine and in the way Excel treats reserved names like Auto_Open, Auto_Close, etc.

For instance, the protect routine defines the name Auto_ouvrir in the following way:

```
=DEFINE.NAME("Auto_ouvrir", "=L2C1", 2, TRUE, 14)
```

If this line is executed under the English language version of Excel, it will not have the desired effect for two reasons. First,

there a cell is referred to as =RxCy - not as =LxCy and, second, there the name "Auto_ouvrir" does not have any special meaning. However, in the virus this line has been executed only once - by the virus author - and under a French language version of Excel. In that language version of Excel the cell reference is perfectly correct and the name "Auto_ouvrir" has a reserved meaning - it indicates a name which automatically receives control whenever a workbook is opened. So, the execution of the above line has instructed the French language version of Excel to record somewhere in the workbook that the macro starting from the cell which is at the intersection of row 2 and column 1 is to be executed automatically each time that workbook is opened.

Once this information is recorded in the workbook, it is preserved even when the workbook is opened by other language versions of Excel and the macro is executed there. However, if the source of the virus is extracted, then inserted into another workbook, and initialized by running the protect routine under an English version of Excel - then it would not replicate, unless extensive changes are made in the protect routine - to translate its language-dependent operators into English.

While the detection and disinfection of this new kind of macro virus poses no particular problems (even, for a change, all the necessary documentation of the respective stream formats and data structures is freely available from Microsoft), it nevertheless required significant re-design of the macro scanning engines.

F-Secure Anti-Virus 4.01 detects and disinfects known Excel Formula viruses.

Vesselin Bontchev is in charge of the macro detection engine of the F-PROT scanning engine. This article appeared



originally in *Virus Bulletin Magazines April 1998 issue*.

Win95/Anxiety

By Péter Ször

Month after month the Windows 95 environment is becoming more and more obvious for virus writers. It looks like the number of different ways to implement working viruses on Windows 95 is virtually endless. The latest example of this trend is Win95/Anxiety. This virus is not original but a slightly modified variant of Win95/Harry virus. Anxiety fixes a few small bugs in Harry which is why it becomes more successful even some fatal bugs still remain from the original release. Anxiety is known to be in the wild internationally, as it has been spread in internet extensively.

Win95/Anxiety infects PE (Portable Executable) programs under Windows 95. What makes it special is that it stays resident in Windows 95 memory space without using a virtual device driver (VxD).

The biggest operational difference between the two viruses is that Win95/Harry has an activation routine. It creates a cursor image file called C:\syringe.cur and tries to make this cursor be the active one by modifying the registry. Actually at this point the virus crashes most of the time. This could be the reason why Anxiety was modified by not to have the risky instructions from this routine anymore.

Anxiety does not have a new activation routine at this point, but this makes the virus able to be replicated under most Windows 95 environments without the original problems.



Syringe cursor file installed by Win95/Harry virus

Once the virus successfully hooks the file system, it is waiting for file opens. Whenever a suitable EXE file is opened, Anxiety infects it.

The bug

Unfortunately (from the disinfection point of view) Anxiety has the same problem as the Harry virus. When the virus infects a file it overwrites some part of the original program which usually contains zero, because of the section alignment. This makes the disinfection of the virus difficult and even impossible in many cases. Programs which end with program code here will not work after the infection and can not be repaired by a disinfectant. Most of the time however the application ends by having a long zero filled area. In those cases the virus works without any visual problem and the disinfection of those applications remains possible.

Other text in the virus code

The following text is viewable in the virus code, but never displayed:

```
Anxiety.Poppy.95 by VicodinES
```

Conclusion

Just like in the early days of DOS viruses the number of different techniques used by virus writers is growing quickly in the Windows environment also. The most successful infection methods (found by "pioneers") will eventually become the "standard" infection technique of the next century. The "standard" is still not ready yet, but will be finalized during the next few years. Since Windows virus writers are sharing source codes between each other, buggy viruses can be fixed by others which make them available to become in the wild.

F-Secure Anti-Virus 4.01 detects and disinfects the Win95/Anxiety virus.

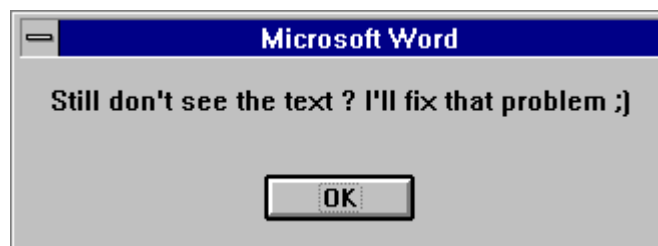
Péter Ször works as a senior virus analyst at Data Fellows Groups Espoo Offices. This article appeared originally in Virus Bulletin Magazines January 1998 issue.

WM/Kompu.I

This is a widespread variant of the Estonian macrovirus Kompu. It was originally found in late 1997.

Kompu.I activates by switching to normal view and setting document magnification to 200 percent.

This happens every time an infected document is opened. At this time virus also displays a message box with the following text:



The virus body contains this text:

```
=====
= INFORMATION ABOUT THIS VIRUS =
=====
Reason: Educational
Name: Spreader
Made in Estonia
Made by the TPAR team
=====
```

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

Win32/RedTeam

By Eugene Kaspersky

This virus infects Windows EXE files (NewExe) and sends itself to Internet by using Eudora e-mail - it is the first known virus that infects Windows and spreads via Internet.

To infect files the virus stays in Windows memory and infects program files as they are executed. To use Eudora e-mail to spread, the virus parses internal format of the mail database and adds "infected" messages. The virus is able to spread to Internet only if Eudora e-mail system is installed on computer, but recipients of infected messages may use any standard e-mail system.

Of course, the virus is not able to run itself automatically from infected message. It is not able to infect the system when an infected message is opened and read. To spread the virus the infected EXE attachment has to be extracted and executed.

The length of virus code and data is 4766 bytes. The virus was named after text strings that present in virus body (they are encrypted in infected files):

```
<<-RED TEAM->> (C) The Soul Manager.
Made in Australia - 06.97.
So, so, Herr Kurtzhals - Is F/Win able
to follow The Red Team?
```

F/Win is a German shareware Anti-Virus program made by Mr. Stefan Kurtzhals.

RedTeam infects the Windows Kernel file. When Windows is loaded with an infected Kernel file, the virus stays in the system memory as a part of it - no special action is necessary to do that because code of virus is placed in the same code segment as original Kernel's routines.

Under Windows 3.xx the virus hooks the WINEXEC function and infect files that are executed. The virus does this in quite clever way - it immediately passes control to original WINEXEC handler and then infects a file in background, so there is no delay when application are executed under infected environment. This is quite important for the virus because usually Windows 3.xx is installed on slower machines, and delays in execution might warn a user.

Under Windows95/NT the virus hooks INITTASK, so it intercepts control when programs are registering themselves in the system. The virus then infects applications as they are initializing.

While infecting a file with probability 1/8 the virus will drop an infected E-mail message to Eudora outbox. The virus uses these Eudora data files: NNDBASE.TOC, OUT.TOC, OUT.MBX. The first file (Nickname database) is used by virus to get names of recipients to whom the virus will send an infected message. The infected message is placed to OUT.MBX (Outbox database) and necessary references are placed to OUT.TOC file.

The message itself has a subject "Red Team", contains a warning text and an attached EXE file. The text looks as follows:

```
Hiya!
Just thought I'd warn you about a destructive
new e-mail virus. Here is some info:

> The "Red Team" virus is a complex new
> computer virus that spreads via
> the Microsoft Windows operating system, and
> Internet E-Mail. Although
> it is not the first virus to spread via
> E-Mail (that was "Good Times"),
> the Red Team virus is unparalleled in its
> destructive capabilities.
> Further more, the virus is exceedingly common
> - it has already been reported in much of
> western Europe, the USA, Russia, Australia,
> and Japan. In short, everywhere.
>
> We at QUEST, have spent several weeks
> analysing this virus, and are proud to
> announce that we finally have a cure! The
> program, named "K-RTEAM" (Kill Red Team),
> can be executed in any Microsoft Windows
> environment, and will reliably detect (and
> remove if necessary) the Red Team virus
> from your system buffers.
> --
> Julia Blumin
> QUALCOMM Enterprise Software Technologies
> World Wide Web: http://www.qualcomm.com

The reason I thought I should warn you, is that
we recently had a run in with this beast.
Luckily we managed to get a copy of the
excellent 'K-RTEAM' programme before the
destruction really started. Just in case you
should suffer the same misfortune, I have
included this programme for you too.

Bye!

P.S. Make sure you warn all your friends of
this new threat!
```

This text in the virus body is compressed, so the virus decompresses it before saving to Eudora outbox. The attached EXE file is named as K-RTEAM.EXE (Kill Red Team), and is 6351 bytes long. When this program is executed, it will infect the current system with the RedTeam virus.

K-RTEAM.EXE contains the following texts:

```
K-RTEAM - Red Team Anti-Virus
K-RTEAM
Red Team Virus Found!
Remove Virus?
Virus Removed!
Could not Remove Virus!
```

Win32/RedTeam has a bug which prevent the current version of the virus from spreading effectively under Windows 95 and NT. However, files that became infected under Windows 3.xx contain to operate normally under 95 and NT.

F-Secure Anti-Virus is able to detect and disinfect the Win32/RedTeam virus.

Eugene Kaspersky is in charge of the AVP scanning engine development.

Win32/Net666

This virus infects Windows EXE files. It spreads natively under Windows 95 and NT (making it the fourth known Windows NT - specific virus). It is also the first known "internet-aware" virus, as it sends messages over internet and opens up security vulnerabilities in infected machines.

After infecting a machine and waiting for some time, the virus sends a "ping" to four IP addresses located in New Zealand to announce which machines it has infected. After this, the infected machines open up port 531 for incoming connections, and the machines can be controlled by sending commands to this port. These commands could be used to delete, modify or steal files from infected machines.



There are several variants. The first 60416 byte variant contains these texts:

```
mylen=, c:\testexe.exe, NOTEPADX.EXE,
NOTEPAD.EXE, SETUP.EXE, EXPLORE.EXE,
EXPLORER.EXE, WINIPX.EXE, WINIPXA.EXE,
WINSRVX.EXE, E5.2, DEBUG, IMPL=ETHP v5.2
\IDENT.TXT
```

When the virus is active, it is visible in the process list as a number, typically "6.666". When exiting Windows, NT sometimes complains it can't close a task by this name.

SemiSoft was known to be in the wild in the end of 1997 and beginning of 1998.

F-Secure Anti-Virus detects and disinfects the Win32/Net666 virus.

WM/NikNat

Niknat is a simple Word Macro virus. It creates a hidden directory called C:\EvaHzg2 and writes a batch file into it. This batch creates a bitmap file (Evah.bmp) by using debug.exe from DOS.

Niknat activates on 23rd of October. Then the virus manipulates the registry in order to change the active Wallpaper to a new one. This new Wallpaper is the previously creates Evah.bmp which contains a picture of a naked girl.



WM/NikNat virus changes the Windows wallpaper to this picture

Niknat contains the 6 macros:

```
Evahzg
AutoClose
ToolsMacro
FileTemplates
TCloseAN
DCloseAN
```

Any attempt to use Tools/Macro or File/Templates menu causes the computer's speaker beep while this message box appears on the screen:



The virus body contains the following text which is never displayed:

```
by NAENBGOURSG
SO.HT.AI.KS
231076-GREECE
Thanks to NEURO
VRD 19-4-1997
VRP A.U.A
```

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

Hoaxes

E-mail hoax warnings continue to circulate. Classic hoaxes such as **Penpal Greetings**, **Join The Crew** and **Returned Or Unable To Deliver** still appear every now and then, but the most common hoax currently seems to be **Win A Holiday**. This is a false warning of a malicious e-mail which does not exist.

Here's an example of the hoax:

```
If you receive an email titled "WIN A HOLIDAY"
DO NOT open it. It will erase everything on
your hard drive. Forward this letter outto 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
(16/2/98) morning from Microsoft; 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. Also, do not open or even look at
any mail that says "RETURNED OR UNABLE TO
DELIVER" This virus will attach itself to your
computer components and render them useless.
Immediately delete any mail items that say
this. AOL has said that this is a very
dangerous virus and that there is NO remedy for
it at this time. Please practice cautionary
measures and forward this to all your online
friends = ASAP.
```

As usual, ignore these warnings and do not pass them on. Companies can lighten the burden caused by users forwarding false hoax warning by giving out simple rules:

1. It is not the duty of employees to forward virus warnings.
2. Such forwardings are forbidden.
3. If an employee receives a virus warning, he should forward it to local IT administrator, who will check if there is a need to take action

The local IT administrator can use our hoax database to see whether the warning is a known hoax or not. The hoax database is available on-line at <http://www.datafellows.com/news/hoax/>

CounterSign™ Framework

The Anti-Virus Challenge

As the computing industry moves toward the landmark year 2000, new virus challenges will continually develop. Organizations of all sizes and colors find that they are unable to secure their information systems without an anti-virus product. The widespread distribution and sophistication of today's viruses, especially the growing number of macro viruses, requires a new technique to ensure the security and integrity of mission-critical systems and data. Traditional scanning methods are, and will continue to be, one step behind fulfilling your needs:

- Detection of All Known Viruses
- Detection of Previously Unknown Macro Viruses
- Transparency

- Centralized Management
 - Single-point centralized administration support for all necessary hardware and operating system platforms
 - Single-point centralized administration support for anti-virus on desktop, server and network devices
 - Standards support (SMS, MMC, SNMP, HP OpenView, IBM Tivoli, IBM NetFinity, Computer Associates Unicenter)
 - Single-point centralized support for all network systems
 - Managing security policies instead of configuring systems.
- Integration with the Corporate Security Infrastructure
 - Increased networking or administration functionality
 - Ability to detect new types of viruses
 - More network related security problems
 - Anti-virus tools in servers, firewalls and gateways

Today's anti-virus methods

Although the 1997 NCSA study showed a 13% increase in the usage of anti-virus products, the incidence of computer virus infection has nearly tripled. According to the NCSA Virus Prevalence report, infections per 1,000 PCs were increasing at a rate of 2.5% per month.



Table 3. Infections Per 1,000 Computers

Date	Number
January, 1996	6.1
February, 1996	14.4
January, 1997	35.21
February, 1997	33.86

The 300 respondents represented a total of 728,798 desktop computers and 24,270 servers. Of these:

- 64% of desktop PCs are protected by a virus scanning policy alone (end-users are expected to scan diskettes and downloads before use) – up from 25% in 1996;
- 68% have automatic scanning for viruses on boot-up and 39% have automatic scanning at network log-in;
- 60% are configured to automatically scan for viruses as a background task.

Mixed Solutions

In today’s fast-evolving computing world, network administrators work with as many as eight different operating platforms and various versions of each operating system. Until now, it has been common for an administrator to require a mixture of anti-virus solutions for mixed environments.

Percentage of Organizations Running a Variety of Operating Systems

Operating System	In Use in Company
DOS only, no Windows	45.00%
Windows 3.1	90.67%
Windows 95	88.67%
Windows NT	72.67%
OS/2	38.67%
Macintosh	43.00%
Unix	47.33%
Other	4.67%

Incomplete Anti-Virus Coverage

After solving the challenge of finding adequate anti-virus coverage for the entire company, an administrator must try to

keep users from disabling workstation protection.

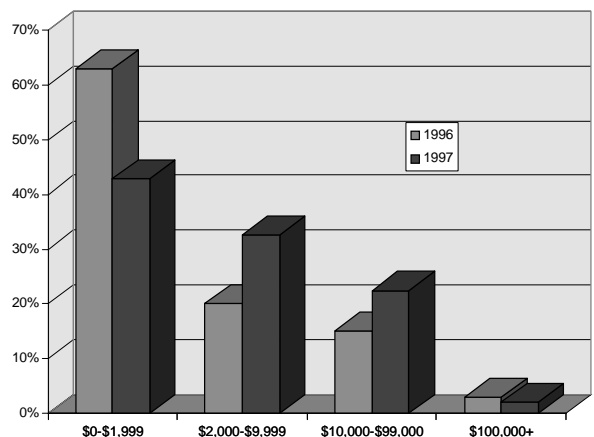
Desktop Virus Protection Methods Used

Protection	% of companies	# of PCs
Users check diskettes and downloads for viruses.	64%	320,268
Anti-virus software scans hard drive for viruses every boot-up	68%	402,598
Anti-virus software scans hard drive for viruses every login	39%	194,526
Anti-virus software scans hard drive for viruses full time in the background	60%	289,740
Other periodic anti-virus detection on the desktop	41%	132,770
Other full-time anti-virus detection on the desktop	20%	58,881
Other (specify)	5%	31,473
None	1%	
Don't know	<1%	

Virus Incident Costs

- False alarms
- Missed unknown viruses
- Interrupted work and on-site support need

The cost of a virus incident includes interrupted work recovery time.



Stated Cost of Virus Incidents, 1996-1997.



Clearly, more widespread use of anti-virus software cannot in itself eliminate the virus threat. Complete protection must include a multi-tiered detection solution as well as transparent and integral centralized management.

Stability: the Foundation of Progress

Where the anti-virus world has theorized several partial answers to the challenges described above, Data Fellows has implemented a cohesive, integral solution, complete with benefits of efficiency on all levels.

For 100% virus detection and optimal identification of false alarm incidents, the highest recommendation has been to use two or more anti-virus products in an organization. However, this has not been feasible until now because the cure is worse than the pain:

- Incompatibility on file access - when two different drivers try to access the same file at the same time, they easily clash and crash
- Confusing reports (different names for the same viruses, different terminology etc.)
- Different maintenance and administration mechanisms, difficult to maintain two systems side-by-side
- Different user interfaces -> confuses the end user and requires training, leads to a long learning curve

The idea of combining multiple anti-virus products into one common “framework” also endorses the integration of products that may currently be in use in the organization. This entire solution would ideally combine all these components into a cohesive and unified solution.

- Macro Viruses
- Transparency and Centralized Management

- Integration into the corporate security infrastructure with policy management support

Data Fellows Victory: Synergy Through CounterSign™ Technology

Managed from a single point, F-Secure Anti-Virus integrates transparent virus protection for easiest and most robust implementation over entire domains.

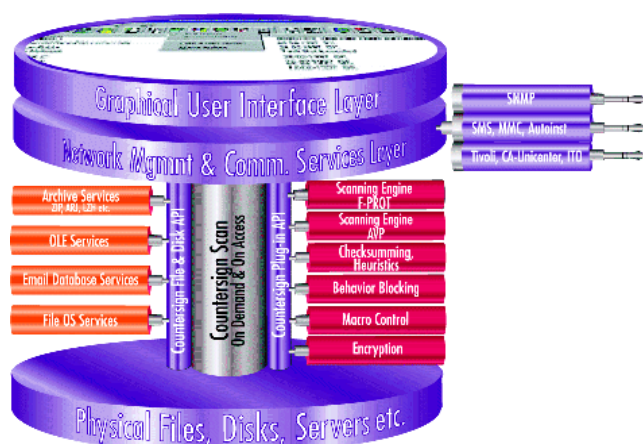
As the virus threat grows and operating systems change, it will be necessary for all anti-virus products to work within the common framework of the F-Secure Anti-Virus Framework. This framework provides an application programming interface for plugging in any anti-virus detection modules.

All the detection modules can transparently use services from the two service layers:

- File & disk services with extremely fast scanning inside nested archives or encrypted files
- Network management services

File & disk services include several sophisticated file format transformers. For instance, different types of archive contents (for instance, ZIP, ARJ and LZH) are seen as directories and files by the detection modules. The same applies for all sorts of compound documents like OLE files and mail server databases.





The Network Management services provide a means of communicating detection engine alerts, reports and messages to the administrator. In addition, the administrator is provided with remote configuration and policy management services to the anti-virus utilities.

Data Fellows understands that there has been a substantial investment in anti-virus protection. Certainly the NCSA's 1996 Virus Prevalence Study showed that virtually all the respondent companies had one or more anti-virus products on site. Therefore, as a result of Data Fellows' focused development efforts, F-Secure Anti-Virus will provide a method of combining your currently installed anti-virus product into the F-Secure Anti-Virus Framework.

The F-Secure Anti-Virus Framework will use an advanced heuristic analysis to detect previously unknown viruses therefore limiting the risk of false alarms. This intelligent scrutinizing method searches for patterns of changes in files, and behavior of programs, that are typical of known viruses. This is ordinarily how all anti-virus programs perform. F-Secure Anti-Virus goes a step further and analyses the behavior and change patterns and executes a series of tests, which eliminates false conditions. F-Secure Anti-Virus will then report the files or boot records as

"suspect" when it displays a comprehensive virus infection report.

Also available under the framework umbrella, F-Secure Anti-Virus supports an advanced change detection method. This checksum technology uses Data Fellows' advanced cryptography technology developed for military users of Data Fellows data encryption products to protect both the method of detecting change on the users system as well as protecting the F-Secure Checksum database.

We believe that a paradigm shift in anti-virus has happened. There is no way any anti-virus product not utilizing CounterSign™ technology can achieve the astounding detection rates of F-Secure Anti-Virus.

Advanced Network and Systems Management

F-Secure Anti-Virus is also complete with a wealth of network management and centralized distribution features such as:

- Installs desktop versions of F-Secure Anti-Virus automatically from a single workstation.
- Send updates to users with a single mouse click.
- Receive reports from workstations when a virus is found.
- Receive copies of infected files from workstations automatically.
- Receive copies of suspicious files from workstations automatically.
- From a central location, order workstations across the network to scan themselves transparently.
- Send F-Secure Anti-Virus update bulletins or other messages to users.



- Remotely change any setting or configuration in workstation installations

F-Secure Anti-Virus has the most advanced, network-independent centralized management system. Environments using Novell NetWare, Windows NT, Windows for Workgroups, Banyan Vines, IBM AS/400 PC Support, a Microsoft LAN Manager, Artisoft LANtastic, Digital Pathworks, Sun PC-NFS and FTP Software PC/TCP can take advantage of the powerful centralized network administration. All workstations on the network can be treated as a part of the server's hard disk as a shared logical disk.

In addition, F-Secure Anti-Virus first-time installations and periodic updates can also be accomplished through Microsoft Systems Management Server (SMS). Support for the forthcoming MMC will also be provided.

F-Secure Anti-Virus also supports the industry standard Simple Network Management Protocol (SNMP) for sending alerts to SNMP Control Centers such as HP OpenView or IBM NetView®. This allows enterprise network management support for WANs with special integration to IBM Tivoli, Hewlett Packard OpenView and Computer Associates Unicenter.

Easy-to-use interface

F-Secure Anti-Virus has a clear and easy-to-use interface:

- Windows 95/NT 4.0 look-and-feel.
- Customizable toolbar with instant Tool-Tips.
- Extensive and easy-to-understand virus description database, explaining what all the common viruses actually do

- Direct links to the Data Fellows Anti-Virus WWW services providing the most up-to-date information
- Easy-to-use Wizard for creating automatic network installation

Transparent background operation

The F-Secure Anti-Virus products feature the exclusive Gatekeeper technology, the world's first Windows® real-time anti-virus scanner (VxD). This complex technology has allowed Data Fellows to provide state-of-the-art real-time anti-virus technology to all Windows platforms, both client and server platforms. Workstation protection should be completely transparent and remotely controlled. The corporate network can not be secure from viruses without securing the desktop machines.

Also available from Data Fellows

F-Secure Anti-Virus Macro Control

covers document and spreadsheet macros. Using Data Fellows proprietary technology to authenticate macros from the network administrator's central console, F-Secure Anti-Virus for Macro Control can easily propagate trusted database information to every workstation.

F-Secure Anti-Virus Mail Gateway

delivers the most *complete* e-mail anti-virus product on the market today. With support for all the major e-mail clients such as Microsoft Mail, Microsoft Exchange, Lotus Notes, cc:Mail, Novell GroupWise and MHS and both Internet and MCI Mail. F-Secure Anti-Virus Mail Gateway supports all major Internet protocols including POP3, SMTP and UUCP via dial-up, ISDN or leased line.

F-Secure Anti-Virus for Firewalls

provides industry-leading NT and UNIX firewalls uninterrupted shielding from Internet-borne viruses. Developed in conjunction with leading firewall vendors'



specifications, F-Secure Anti-Virus for Firewalls scans and removes viruses before they enter your network. Coupled with F-Secure Network Management makes this the perfect solution for today's Internet-borne viruses.

Upgrading from F-PROT Professional to F-Secure Anti-Virus

Before starting installation, close all running Windows applications.

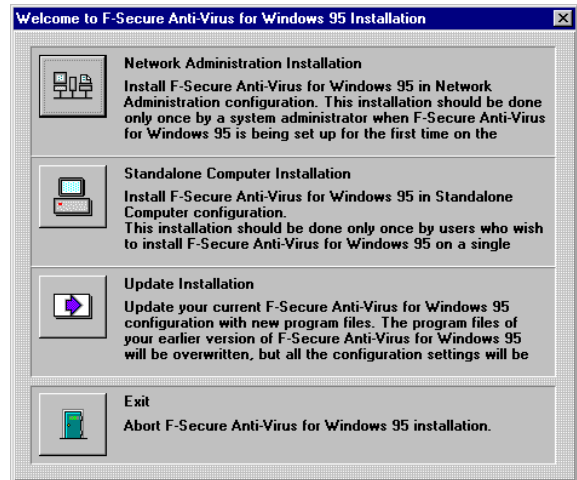
Insert the F-Secure Anti-Virus installation CD-ROM or installation diskette number one.

If you are running Windows 95 or Windows NT 4.x, the CD-ROM setupper will start automatically. If you're using diskettes, click the Start button, point to Settings, and click the Control Panel icon. Once in the Control Panel folder, double-click the Add/Remove Programs icon, choose "Install", and Setup.exe will be located automatically in one of your diskette drives. If Setup.exe has not been located automatically, click Browse and select the location of the Setup.exe file. Click Finish, and installation of F-Secure Anti-Virus will begin. Alternatively, choose Run from the Start menu, and type in the path and name of the Setup.exe file, for example, A:\Setup.

In Windows 3.1 or Windows NT 3.x, choose Run from the Program Manager File menu and type in the path and name of the Setup.exe file, for example, A:\Setup.exe or, for the CD-ROM version, R:\Install.exe.

If you install from a CD-ROM, you will first be presented with a choice of product and language version. Choose "F-Secure

Anti-Virus" for your current platform and the correct language before clicking ok.



In the "Welcome to the F-Secure Anti-Virus Installation" dialog box there are four options to choose from:

- Network Administration Installation
- Stand-Alone Computer Installation
- Update Installation
- Exit

Select the choice "Update Installation". If you are the administrator for a network of computers running F-PROT, choose the Send Update command from the Administration menu to distribute the new version to the users.

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've been told that it's possible to receive a virus by downloading an image file, as it is a binary file. Is this possible?

No. None of the common image types (GIF, JPG, PNG, BMP, TIF, TGA, ICO) contain executable data, even though they indeed can be considered to be binary files.

What you can do, of course, is this:

```
REN virus.exe image.gif
```

I.e. rename a virus program to look like an image file. Then you would, in theory, have a virus in an image file. But the image file would look corrupted to any viewing program and the virus couldn't execute unless you explicitly rename it back to EXE and execute.

So, in effect, you currently can not have viruses in image files.

Why are macro viruses so common?

Indeed macro viruses have bypassed boot and file viruses and are the most common virus type. It is estimated that over 80% of all infections nowadays are caused by macro viruses.

There are several reasons to this:

1. Macro viruses are easy to write. The programming language is Basic-like and easy to learn
2. The development environment is easily available. Anybody who has Word, Excel, Access or PowerPoint has the

required tools to start to write macro viruses

3. It is easy to find sources for existing macro viruses. Most macro viruses spread in unencrypted format, which means that anybody who's infected by the virus can read and understand the source code of the virus
4. Document files are ideal carriers for viruses. People do not exchange program files and floppy disks nearly as often as document files. E-mail attachment is the most common carrier for a macro virus
5. Word makes new variants of macro viruses by corrupting them. Some versions of Word have bugs which cause them to randomly modify macros as they are copied. As a result, Word often creates new, modified versions of macro viruses and they are still able to continue replicating.

For these reasons, macro viruses have become the biggest and most common threat to computer security.

Our machines were infected by the Raadioga virus. This virus activates by enabling the hardware BIOS password protection. Now our machines won't boot, as they are asking for an unknown boot-up password - how can we regain control of our machines?

There are several viruses which enable the BIOS password protection to annoy the user. Raadioga and Lego are the most common examples of such viruses.

You can usually reset the hardware password by opening up the machine and setting a DIP switch or by removing the CMOS battery. However, if you have a large number of infected machines, you might want to try some of the well-known backdoors in BIOS password systems.



These backdoors are default password which always work, regardless of the real password. As there are several different BIOSes, there are also several possibilities.

Try these with AMI (American Megatrends) BIOSes:

```
AMI
AMI_SW
```

Try these with Award BIOSes:

```
589589
Award
AWARD_SW
AWARD SW
J262
```

Also try these:

```
bios
setup
cmos
```

If you find the right password, enter CMOS setup and disable password protection immediately. If you can't find the right password, consult your hardware or motherboard manual for information on how to reset CMOS data (you will also lose other CMOS settings if you do this).

If you can't bypass the protection, contact your hardware vendor for system specific guidance.

Also note that you should not rely on BIOS password protection for real security, as many BIOS passwords can be bypassed with the above backdoors.

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 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/>



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