Copyright And Disclaimer

Perforin for WinWord Manual

Windows 95/NT 4.0 Edititon

Version 2.0

Revision Date: June 1997

WARNING

Disclaimer

The developers and distributors of Perforin make no warranty of any kind, either express or implied, with respect to this software and accompanying documentation. In no event shall the developers be liable for any damages arising out of the use of or inability to use the included programs. The entire risk as to the results and performance of this software package is assumed by the customer. We specifically disclaim any implied warranties of merchantability or fitness for any purpose. Use at your own risk.

The developers and distributors of Perforin reserve the right to revise the software and accompanying documentation and to make changes in the contents without obligation to notify any person of such revision or changes.

Table Of Contents

What is Perforin anyway?

Medicine men define Perforin as follows:

"**Perforin** is a lymphocyte component essential for killer cell mediated cytotoxicity (cell toxicity). Perforin is unique in that it creates large transmembrane pores causing membrane damage and allowing the uptake of other toxic factors leading to target cell apoptosis (cell death).

Perforin/granzyme mediated DNA release is blocked by caspase inhibitors, while perforin mediated Cr release is not. **Perforin,** unlike granzyme, Fas-ligand, and TNF thus **is capable of killing cells independent of their cooperation**."

So.... Perforin is another one of nature's hatchet men sent out to put bad cells out of their misery. Apparently, it's quite an effective solution.

We are developing different versions of Perforin to address new virus problems. The first addition to the series is Perforin for WinWord that can deal with macro viruses targeting Word documents. The current implementation works only under Windows 95 and NT 4.0.

Perforin

This part of the manual describes the operation of Perforin and provides you with contact information to reach us.

Introduction

In 1995, we saw the proliferation of a new breed of computer virus that was discussed only in theory before; **macro virus.** As commonly used applications software packages got more sophisticated in their programmability, creation of macro viruses became more feasible. In fact, there are macro languages that exceed the boundaries of simple automation tools and stray into the domain of general purpose programming languages. WordBasic is a good example of one.
Macro viruses we have seen so far mostly plague the documents created by a popular word processor called WinWord or **MS Word for Windows versions 6.0 and later**. Although such viruses can be created for other environments that offer macro capability, they are not as vulnerable as the WinWord environment. There are several reasons for this. We will discuss the most obvious reasons in the following paragraphs.

Other products **keep the macros in a separate file** while **WinWord** macros can be **included as part of the document** the user is processing. Thus the virus can spread as the infected documents are exchanged among users. As we know from our experience with other kinds of viruses in the PC world, such uncontrolled spread is what makes viruses a big threat. Other auxiliary damage routines programmed by the virus author only adds more to the risks created by the uncontrolled spread. Since documents can contain important data, they are not as simple to replace. With program files, we could advise people to reinstall the software using the original copy; the same cannot be said for documents.

To complicate matters even further, **WinWord 6 does not warn the user about the presence of macros** in a document. Even worse, there are certain macros, called **auto macros** in WinWord parlance, that run when WinWord opens or closes a document. **The user is not consulted for confirmation** at all. On top of all this, such **macros can override or redefine default definitions** in WinWord. In other words, **FileSaveAs** command can now be doing more than what it used to due to the virus macro. WinWord 6 does not even warn you that a default operation has been modified. It should be obvious even to the casual observer that viruses can flourish in an environment that provides them with some of the following:

1. A suitable **carrier often exchanged among computer users** without much awareness for it containing potentially dangerous executable program sequences. Documents are perceived as containing nothing but data. For many other products, that is indeed true.

2. A mechanism that allows the virus to **gain control of the environment in an automatic way** without any warnings shown to the user.

3. A flexible and powerful language in which manipulation of potential hosts to include a copy of the macros is easy to do.

4. A **widely used environment** available on multiple hardware platforms such as IBM PC and Macintosh computers.

5. **Networks that are not designed to prevent modifications of documents** in that sharing would be severely hindered if they impose the same restrictions on data files as they do on program files. Note that practically all common local area networks fit this definition. So, there is no simple remedy by changing rights and flags on the server.

6. A **persistent storage medium that can further the viral spread even after the infected document is deleted**. In the case of WinWord, a default global template called **NORMAL.DOT** has become the favorite **jumping point for macro viruses**. This is similar to a boot sector virus that invades the master boot record of the hard disk and from then on,

it infects the unprotected floppy diskettes used on that machine.

7. Readily available tools to write such viruses and the ease of learning how to **program macros with little programming experience**. In addition, virus code is readily available from some WWW sites on the Internet. If the virus is not marked as execute-only macro, then the full source code of the virus is available to a new wannabe virus programmer. Many viruses are simple hacks of existing ones.

8. **Inadvertent release of infected documents to power users** who tend to interact with a large number of technically oriented users.

The very popular MS WinWord product provides most of these features, and some of them are inherent in the modern computing environments.

It is not surprising that macro viruses have been reported all over the world only after a brief period of introduction to the computing environments. In addition, several companies, including the manufacturer of WinWord itself, have released documents containing macro viruses by mistake. Users whose documents have been exposed to macro viruses did not even realize what was happening until the media got into the act, and boosted everyone's awareness to this new development in malware. Now **macro viruses are among the most commonly reported viruses in the world**.

Microsoft responded by releasing solutions based on the very same mechanisms viruses use, i.e. they wrote anti-macro virus macros. These were meant to detect and remove the most prevalent of these viruses, namely the **Concept** or **Prank** virus as Microsoft dubbed it. However, it soon became apparent that such simpleminded solutions were too limited to curb the spread of viruses. In fact, some of the macros in this tool were snatched by some viruses that assume that there are no other macros in the document besides the virus macros, and this resulted in new variants.

In reaction to the persistence of this problem, **Microsoft revised the WinWord software so that a warning is issued when a document containing any macros is about to be opened**. The user has the option to disable the macro but load only the text portion. Of course, this approach suffers from the **cry wolf** syndrome in that it warns of all macros present in a document including those the user wants to keep. The result is that the user is forced to turn off the warnings completely. Note that this early warning mechanism could be very effective as a preventive measure; however, it would be naive to think that it is adequate. Furthermore, this option is available only in the Windows 95 and Windows NT versions of WinWord. People who are using WinWord 6 do not have this option.

Naturally the antivirus companies responded to the users' needs for a better solution by offering a slew of tools that can detect the presence of rogue macros in documents and remove them without damaging the contents of the text portion. It still remains somewhat risky to remove viruses from data files, but nonetheless it is the preferred choice of many users. In addition, WinWord uses a fairly complicated data file format. Microsoft considers this format proprietary information. Antivirus companies had to make do with the little information Microsoft provided after many requests by the antivirus developers, and only under strict nondisclosure agreements. To date, the information provided remains inaccurate and incomplete. However, there are some recent developments that indicate Microsoft is aware of these problems and it intends to address some of the issues raised by antivirus vendors.

Another dimension to this problem is the cross-platform availability of WinWord and the shared document format. Macintosh users who prefer WinWord for their word processing needs are also at risk from some of the same macro viruses that PC users dread. Before macro viruses appeared on the scene, such an interoperable virus was merely a conjecture. **Due to certain differences in the implementation of the Word macro language, many PC macro viruses are not likely to be viable on different platforms such as the Mac**.

What Is The Best Solution?

Now that we have explained why and how macro viruses are a threat, we will discuss some solutions that you may choose to guard your systems against them. Although there can be no panacea to the macro virus problem as long as WinWord offers certain programmable facilities to be included as part of documents, there are several measures you can take to reduce your risk.

Some people may suggest that the most obvious solution is not to use WinWord 6.0 and later for word processing. After all, there are other, even better, word processing packages in the market. They do not have the same security flaws as WinWord. However, many companies have already invested in WinWord. Besides financial concerns, they have trained personnel who have been using WinWord for quite some time. Although conversion of documents from Word format to other word processors is quite possible and automatic, there may be difficulties with some of the more complex documents. In other words, this drastic solution is feasible mostly for new users who do not have a compelling reason to insist on using WinWord.

At any rate, we encourage all current and potential Word users to contact Microsoft to express their concern over this growing problem. We are dismayed to say that Microsoft has not addressed this issue adequately. They have the ultimate control over how WinWord implements macros. Your feedback will help them get a better feel for the scope of the problem their customers are facing, and perhaps implement certain measures to curb the macro virus nuisance.

We could tell you to avoid sharing documents, but that would be an unrealistic advice in this highly networked world. On the other hand, you should definitely avoid opening documents from outside sources without first checking them. This is not as obvious as it sounds. Some email programs are configured to automatically recognize the type of the file attached to a message and launch the registered application for that file. If that application happens to be WinWord and the file is an infected document, this operation could possibly unleash a virus. You should find out if your email program has such a setting and turn it off.

As we have already mentioned, the Word documents serve as the carrier for the virus. To eliminate this possibility, you can avoid using the WinWord document format in any files you are sending out. For example, you can use the SaveAs command and choose the **RTF** file format. For many documents, the RTF format is adequate to retain the layout of the text, and it does not suffer from the macro virus problem since RTF files cannot have the same macros. WinWord and many other word processors can read RTF files just fine.

A complementary precaution is to keep a good backup of your **NORMAL.DOT** template. This is the file that most macro viruses implant their macros in, and use it as a jumping point. If you suspect a macro virus is present, and your antivirus software does not catch it, then exit WinWord immediately and back up the current NORMAL.DOT to another file, and then copy the good backup over it. This might slow down the infection, but it is not a cure. The first time an infected document is opened again, the vicious cycle starts all over again. You should send the suspicious copy of the NORMAL.DOT along with any possibly infected documents to us for analysis. If it is a virus, we will issue an updated detection and removal database or external signature file for Perforin. It is usually a simple matter of editing a text file and letting Perforin use it as an external signature file.

Another area that some viruses target is the templates in the STARTUP directory. WinWord loads these automatically, and the virus can gain control. You can also back up the files in the STARTUP directory and use the clean copies to replace the suspicious ones later.

In a large environment where computer users have varying degrees of knowledge of the WinWord package, such precautions are not going to be adequate. The best approach is to use an antivirus product that is capable of dealing with macro viruses. Some people may say that you could open infected documents in another word processor, such as WordPerfect, to read just the text and get rid of the Word document, to remove virus macros. But this is not a convenient method for cleaning a large number of documents. **With something like Perforin, you can scan and clean thousands of documents easily and automatically**. It would take several weeks to do the same manually, and most people have better things to do than remove macro viruses by hand. If you feel compelled to do so, Perforin has an Examine Document command that allows you to zap even one macro at a time. It is meant for analysis purposes only of course, not cleaning many documents.

If you do not have access to a system with Windows 95 or Windows NT 4, then you might wish to try another excellent antivirus solution for macro viruses. One such product, called F-Macrow, is included as part of the F-prot antivirus package. Another one, called F/Win, is also available for DOS users. F/Win has some advanced heuristics that can detect some new variants. You can find both products over the Internet.

A WinWord Macro Virus Solution for Windows 95 and Windows NT 4.0

Under any other name, a macro virus spreads just as easily. If you exchange WinWord documents with other people, then you may be at risk, and worse yet, you may be putting others at risk. It is wise to install an antivirus product designed to handle such viruses. Our product, **Perforin**, offers a usable, effective, and affordable solution to this problem. Perforin has one of the highest macro virus detection rates in the world, and it is updated as new viruses appear.   We are making a trial version available for download so that you can evaluate the product and decide for yourself. If you have any questions or suggestions about Perforin, please feel free to contact us any time. We strive to improve our products to meet your needs.

Updated copies can be downloaded from:

http://www.vdsarg.com

If you discover an infected document or suspect something may have a new virus, you can email it to **virushlp@vdsarg.com** for analysis. There is no charge for this service whether you are a registered user or not. You can also put the suspect documents in the **C:\PERFORIN\VARIANTS** directory and use the built-in **Upload Suspicious Document** command in the Perforin Tools menu to transfer them to our **FTP** area over the Internet. Note that you must have an active Internet connection to be able to use this feature.

If you run into any problems with Perforin, please send us a message describing the problem and your system configuration. We are always interested in user suggestions to improve our products.

Program Features

Perforin is a professionally developed product. We strive to improve it based on user suggestions. Please feel free to contact us if you think we should add a certain feature or even remove one.

The following are some of Perforin's currently implemented features:

- It can **scan for and disinfect over 1000** known WinWord macro viruses.
- **Polymorphic macro virus detection and cleaning**.
- **GPF-proof implementation** even when using the buggy MS OLE2 DLLs.
- Supports **Far Eastern** Word 6/7 documents.
- It can identify and **report multiple infections**, and remove each one.
- It can **scan inside password protected documents** and **even disinfect them** on the fly all transparently without disturbing the protection. Thanks to **StripSearch(tm)** Technology, Perforin can discover viruses hiding in protected files. In addition, you will **see the password for infected/disinfected documents** (but not clean ones). Some viruses add password protection, and sometimes use random passwords rendering your data unavailable without the password.
- **Reliable yet fast operation**. Perforin examines **all files except those usually known not to be documents** (such as EXE, DLL),not just ones with .DOC or .DOT extensions since the name of a file is not a good indicator of its contents. **Many products will miss them by default**.
- Instant **signature updates over the Internet at the click of a button**. No extra payment or other hassle. Perforin will even try the next distribution site if it cannot reach our primary server. All automatically.
- **Smart removal** capability allows Perforin to determine if all macros should be excised automatically. Some viruses require this option for proper cleaning. The user does not need to know the details of each virus or specify unusual options. Perforin will do the right thing on a virus by virus basis.
- **Frequent updates** to identify newly discovered variants.
- Suspicious document **quarantine and isolation capability**.
- **Heuristic scan** capability to isolate **new viruses**.
- **User-adjustable heuristic** levels.
- Ability to **scan inside PkZIP compressed archives**.
- Option to **show all documents that have macros**, not just infected ones. This is useful when you suspect a new virus infection that is not detected yet.
- **Flexible operation for advanced users**. You can disinfect just the way you want. Many options to choose from.

- **Context-sensitive help**.

- **Readable online documentation** with brief information on dozens of common macro viruses.

- **ZooSort option** that can turn a bunch of infected documents into a well-organized directory tree **based on the CARO names** of known macro viruses. This feature uses long filenames.

- **Audit log** that shows each infected file and the virus found.

- **Long filename support and 32-bit implementation** for Win95 and NT 4.0.

- Compatible with **FAT32** and **NTFS** partitions.

- Excellent **network support and UNC compatible path** usage.

- Includes a **simple installation** program that automates creating a shortcut, and adding the necessary registry keys.

- **Automatic uninstall** feature thru Setting|Control Panel|Add/Remove Programs.

- Fairly **self-contained operation**. Perforin installs only a few Microsoft DLLs if they are needed to enable MS Internet APIs. These are distributed with the Win95 OSR2 release. They are required only if you have the Aug '95 release and you have not installed Internet Explorer 3.0. All other files Perforin installs or creates during its operation are confined to the Perforin home directory.

- **Free program updates for a year** over the Internet.

- **Self-check capability** to recognize if Perforin.exe and the signature database are damaged or modified.

- **Suspicious document upload** to our tech support area over the Internet **at the click of a button**.

- **External signature** support. You can easily create an external signature file (a text file) that contains identification and cleaning data for new variants that you may encounter. All you need is an infected document that did not have any macros before infection.

- **Examine Document capability** to browse thru the macros in a document without having to worry about activating the virus. No more risky ToolsMacro problems. You can zap macro at a time, save macros to a file, and more. Researcher options.

- **ExamineDoc can even show you which viruses use a particular macro**. Since 75% of currently known macros are borrowed from other viruses or innocent macro packages, this feature allows you to determine if a new variant is related to a known virus.

- **Simple and elegant user interface** with tooltips, right-click help, tabbed dialogs, status bar, 3D-look ...

- **Affordable prices** to fit everyone's budget. The standard edition can be had only for **$40** including S/H in the States. The Pro edition sells for $80 and offers some advanced features that can be helpful to consultants or to those in charge of tech support. The standard one is all what most people will ever need to scan and clean their documents.

Program Requirements

Perforin requires the following:

- Windows 95 or newer, including Windows NT 4.
- Availability of OLE32 DLLs (default in Windows 95).
- 2 megabytes of free disk space on the destination drive.
- Read access to the documents for scanning.
- Write access to the documents for cleaning and reporting.
- Basic understanding of the language the version is using. Trial copy is in American English. We are working on localizing Perforin for other common languages.
- **FTP/HTTP** access over the Internet for automatic online updates for the signatures. If you can use a browser such as Netscape or MSIE, then Perforin should be able to access the Internet just fine.
- Email or modem access to our tech support BBS for uploading suspicious documents. Alternatively, Internet access to upload the samples to our FTP area.

How To Install Perforin

Automatic Setup

We include an automated setup program for Perforin called INSTALL.EXE. If you downloaded the trial copy off the Internet, then you need to unzip the archive in a temporary folder and run INSTALL from there.

If you received the Perforin program diskette, follow these steps to install Perforin on your hard drive:

1. Put the Perforin program diskette in drive A:

2. Click on the **Start** button and choose **Run** frome the menu.

3. In the **Open:** edit box, type in the following:
   A:\INSTALL.EXE

4. Click on the **OK** button to run the installation program.

5. You will see the INSTALL main dialog. The **source** should be already set to A:\. If not, type in the correct path for the folder where the original Perforin files are located. In the **destination** edit box, type in the path for the folder that you wish Perforin to use as its home folder. It will be set to **C:\PERFORIN** by default. It will also create a few subfolder under the home folder that it needs for temporary file, quarantine area and so on.

6. Click on the **Install** button to start the installation process.

7. After the installation is completed, click on the **Exit** button to get back to Windows.

8. Now that Perforin is installed, you should see its **shortcut icon on your desktop**. Double-click on the Perforin icon to run it. Choose the folder you wish to scan and click on the **Scan** button on the toolbar to check your documents for macro viruses.

Manual Install

You can also manually install Perforin. Simply create a folder and copy all the Perforin files into that folder. The first time it runs, Perforin looks for Perforin.INI file, if it cannot find it, it will create one. You also need to create the following subfolders under the Perforin home folder:

VARIANTS
ZOO
TEMP

If you are not happy with the operation of Perforin, you can **uninstall** it very easily. You need to click on the **Start** button and choose **Settings|Control Panel**. Once it comes up, double-click on the **Add/Remove Programs** applet. If Perforin was properly installed, you should see it in the automatically removable software list. Highlight it and then click on the Add/Remove button.

To uninstall Perforin manually, please refer to the next section in this help file.

How To Uninstall Perforin

You can uninstall Perforin manually if you wish. You need to be familiar with the **RegEdit.exe** program included with Windows 95 to remove two keys from the registry. One key is located under:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstal\Perforin

Delete this key. It is used for the automatic uninstall feature.
The other key you need to remove is under:

HKEY_LOCAL_MACHINE\SOFTWARE\VDSARG\PERFORIN

Delete this key as well. If you don't have any other VDSARG products, such as our VDS 4.0 for Windows 95, then you can also remove the VDSARG portion of the key shown above.

After cleaning the registry, delete the **C:\Perforin** folder or the one you used for installation. Perforin keeps almost all its files in the **C:\Perforin** folder. If there are any debug logs in the C:\ directory, then you need to remove them as well. The last step required is to delete the shortcut file. You can use Explorer to go to the **C:\WINDOWS\DESKTOP** folder and delete the shortcut file named **Perforin.LNK**. Note that if you specified different paths for the report log or other settings, you will need to manually delete them yourself.

How Does Perforin Work

The operation of Perforin is **interactive** and almost **automatic**. It also offers several options to guide its functions according to the user's requests. We kept the user interface to a bare minimum not to get bogged down in fancy but little used features. Our development philosophy has always been to keep things as simple as possible yet functional enough to deliver an effective solution. Some of the most advanced features in Perforin may not be of general interest but they do not get in the way either. We also made judicious use of the new visual enhancements in Windows 95 and NT 4 to keep the interface consistent with other Windows 95 products.

Perforin presents a window populated by several large buttons across the top. Each button has a picture that suggests its possible function. The buttons also include a descriptive label in plain language when you place the mouse cursor on them. These are the tooltips. You can click on the button titled **Browse** to bring up a familiar folder browser and navigate thru the hierarchy of drives and folders much like you do with Explorer in Windows 95. After finding the folder you are interested in searching for macro viruses, you click on the OK button to finalize your selection. By clicking on the Scan button in the toolbar, you can start scanning your files. It uses certain default settings, which can be changed in the **Options** dialog that you can reach by clicking on the Options button. You might wish to designate a different **report log** file, or perhaps a different **quarantine directory** where infected documents should be copied to before the virus is removed. The documents that end up in the quarantine directory should be sent to us for analysis. You can simply delete them if you do not wish to send them out.

As the Perforin is searching thru the folders and files, it displays the name of each file in the box at the bottom of the dialog. The upper half of the dialog will have a list of infected documents. By clicking on the title of a column, you can sort this list. If there are infected documents, you can click on each entry and double click with the left mouse button. This action will give you brief information about that particular virus found in the document shown. You can also view information about macro viruses Perforin knows about using the **Help menu**, and selecting **Virus List** option. You can see the statistics such as how many files are examined, how many are infected and so on in the status bar at the bottom of the scan dialog.

After the scan is completed, you can click on the Cancel button to get back to the main window. If you wish to examine the report log, you can simply click on the **View Log** button. After you are finished with your scan, you can click on the **Exit** button to quit Perforin.

If you have not registered your trial copy of Perforin yet, you can click on the Register button to load the ORDER.TXT. Once we receive your order, we will send you a full-featured edition of Perforin that will not expire.

Details of Operation

Now we will present the operational details in more technical terms. Perforin uses the Windows 95 shell interface APIs to locate what is known as **OLE2** files. WinWord versions 6 and 7 documents are written to the files on disk using the OLE2 APIs. Once a file is found, it is opened using the same OLE2 APIs WinWord uses, and the contents are examined for certain **marker ID**s to make sure Perforin is dealing with a WinWord document.

Based on the information we **licensed from Microsoft**, Perforin can locate the key **tables and commands** inside the Word documents. Armed with this information, it **decrypts** each macro body if necessary, and then examines it to see if it matches any of the rogue macros in viruses Perforin has in its **identification database**. If an exact match is not found, Perforin will try to find similarities between the existing viruses it knows about and the macros in the document. If there is sufficient similarity, it will report the suspicious macros as potentially belonging to a **variant** of the virus that is known to have similar macros.

If the user wants to remove the virus macros, indicated either with option settings or interactively, Perforin will clear the contents of the rogue macros, and update the relevant tables and data structures within the OLE2 document. Its operation is based on the recommendations Microsoft supplied, and also on our study of the macro viruses. If the quarantine option is on, then Perforin will make a copy of the infected document in the designated quarantine area before it cleans it. The repaired document will no longer contain virus macros, however the data should be intact.

A line displaying the infected document and the name of the virus found will be written to the report log if you have chosen to create a report file. Perforin repeats this for all files in the folder chosen and in the subfolders **recursively** depending on the option settings. Perforin is optimized to perform **reasonably fast** on common PC hardware. It is nevertheless an I/O intensive application, and examining a large number of folders and documents can take several minutes. Since the extension of a file has nothing to do with its contents except for indicating what kind of file it might be, Perforin examines every file except those usually known not to be documents (such as EXE, DLL). Although this is a slower method, it is more reliable and safer.

Program Components

Perforin consists of the following components:

- Perforin.EXE

  This is the main application program. It is designed and programmed to run under Windows 95 or newer. It also runs under Windows NT 4 or later.

- Install.EXE

  This is the setup program that automates loading Perforin on your hard drive and setting up shortcuts.

- VDSMSIGS.SIG

  This is the signature database Perforin uses to identify and clean macro viruses. We make updates to this file available over the Internet. This file needs to be in the same directory as the Perforin executable file.

- Perforin.HLP and Perforin.CNT

  These are the online help and table of contents files. They need to be in the same directory as Perforin executable file.

- Perforin.INI

  This file stores the optional program settings. You can change it thru the options button in Perforin or manually using a text editor. This file needs to be in the same directory as the Perforin executable file.

- WHATSNEW.20a

  This file will contain changes to the program since last revision. Its extension will reflect the version of the program it is included with.

- ORDER.TXT

  This file contains information on how to register Perforin to get a full-featured copy that does not expire.

How To Configure Perforin

How Perforin Settings Are Stored

Perforin keeps all its settings in the **PERFORIN.INI** file located in the Perforin home folder. This is a simple text file that can be edited. However, you should change these settings thru the Options dialog from inside Perforin.

What Settings Are Available

When you click on the Change Program Settings button, you will see a tabbed dialog with two tabs: Scan/Clean Options and Paths.

On the **Scan/Clean Options**, you will the following settings:

Auto Clean
This options instructs Perforin to clean infected documents without asking for user confirmation.

Ask Before Cleaning
Perforin will ask you before cleaning each document.

Don't Clean
Infected documents will remain infected.

If you choose one of the cleaning actions to take, then the next section will become available:

Only The Macros That Are Part Of The Virus
If you select this option, Perforin will remove the macros it recognized as belonging to a virus. Other macros will be left intact. Perforin does not attempt cleaning a document unless it has an exact match for a virus in its database. Note that this option may leave behind some unknown macros that could still continue to spread. We do not recommend this option to be used unless you are certain that the remaining macros are not viral and you need to keep them. Use the Examine Document command to view them.

All Macros In the Document
If you select this option, Perforin will remove all of the macros present in the document. This is the safest approach, but it will also eliminate your personal macros. If you do not have any custom macros or you simply want to make sure no virus remains behind, then this is the option to use. This option can be used to remove new variants or remnants of known viruses.

All Known Viral Macros In Addition To This Virus
If you select this option, Perforin will remove known viral macros, including those that may belong to other viruses which have not been identified exactly. This option gives you the best compromise between keeping your personal macros and stopping a potential new virus that may be a new variant of a known virus, a common occurrence. Note that if there are unknown macros left behind, they may still continue to spread as another variant of the virus.

Leave Macros Alone, Just Turn Off Template Flag (Risky)
This setting will instruct Perforin not to remove the macros from the document.

Perforin will only clear the template flag of the document so that macros will not run automatically. Note that this option is not safe; the macro bodies and other information remain intact in the document. It is intended for advanced users who wish to examine things for themselves. You can use the Examine Document command to turn on or off the template flag.

Always Turn Off Template Flag If There Are Macros Left After Cleaning

This option is an extra precaution that Perforin offers in addition to its default cleaning mode. If some unknown macros were left behind, they may still be able to spread. To reduce that risk, Perforin can turn off the template flag so that the macros will not be automatically loaded.

Scan Subfolders

If this option is selected, Perforin will look for infected documents in the subfolder beneath the one you have specified.

Generate Debug Log

This option instructs Perforin to create a debug trace log in the root directory of drive C:. It will be named **PERFORIN.DBG**. This is a diagnostic feature that helps us pinpoint any problems Perforin may run into on your computer. If something does not seem to work right with Perforin, we ask you to send us this debug log to assist us resolving the problem. It is a simple text file.

Heuristic Scan

If this option is on, Perforin will look for certain features commonly found in macro viruses. If no virus is identified, heuristic scan can sometimes locate a new virus. Note that not every document reported as suspicious contains a virus. To find out for sure, we ask you to submit a sample. You can send samples thru the Internet using the Upload Suspicious Document command under Tools menu.

Find Variants Of Known Viruses

This option forces Perforin to go thru its database and look for a close match with one of the known virus strains. Most of the macro viruses we have seen are minor hacks of existing viruses. There may be a new macro added, a message changed, or a macro body corrupted. Perforin can isolate such viruses in many cases.

Scan Inside Zip Files

If this option is set, Perforin can unzip unencrypted PkZip archives and examine the documents found in the archive for macro viruses.

On the **Paths** tab, you will the following settings:

Generate Report Log

This option instructs Perforin to write a line showing the full path of the infected document and its status. If a virus was identified, it will be shown in the log. The edit box below this option has the full path of the log file. You can change it using the Browse button to the right.

Quarantine Infected Documents

If this option is turned on, Perforin will make a copy of the infected document in the **VARIANTS** folder under the Perforin home folder. If you wish to send us these samples for analysis thru the Internet, you can use the Upload Suspicious Document command under the Tools menu. This command look at in the VARIANTS folder and gives you the option to send the files found there. You can change the location of the quarantine folder by editing the path displayed in the edit box below or using the

Browse button to the right.

External Signatures

This path specifies the location of the file that contains the user-defined signatures for new viruses. This feature is meant for adding emergency detection and cleaning for a new virus found in the field. Based on the infected documents and templates, it is very easy to extract identification data and enter it into this external signature file. You can also do this using the Examine Document command. This is a simple text file that can be edited. It has a specific format Perforin expects to see.

ZooSort

Perforin can create a directory tree based on the CARO names of viruses it can identify. This option is useful to those who wish to organize their confirmed samples. It is not useful for end-users. Each sample will be copied to the appropriate folder. You can change the base folder in the edit box below this option or use the Browse button to the right.

Copy Missed Variants

This option can make a copy of any document that Perforin did NOT find a virus in. The purpose of this feature is to help us isolate samples Perforin has missed. You can change the location of the variants in the edit box shown below this option or use the Browse button to the right.

How To Get The Updated Signatures

To make it easier for you to obtain updated signature database, Perforin offers an automated signature retrieval command. To be able to use this command, you need to have an active Internet connection capable of supporting **HTTP** protocol transfers. If you can use a WWW Browser such as **Netscape** or **MS Internet Explorer** on your computer, then you should be able to retrieve the signatures just fine. All you need to do is **click on the WWW button** and then Get Updated Signatures Button. Perforin will do the rest to go out to our website and retrieve the latest signatures for you. After the file is download successfully, you should exit and restart Perforin so that the new signatures will be loaded in memory.

If you have difficulty retrieving the signatures, please contact our tech support via email and have him look into the problem or send you the signatures some other way. Note that this service is available only for registered customers.

We do not make the updated signatures for the trial copy available as often as the registered copy. There may be a new signature database every month or as we deem it necessary to issue one. If you run into a new variant Perforin cannot identify, please contact us so that we can take care of the new virus. We will issue an updated signature database or send you an external signature file to handle it.

How To Register

You can register **Perforin** and get a full copy of the product. This will encourage us to enhance the program and to provide you with a more complete tool. All you need to do is print out the order form, fill it out legibly, enclose a check made out to **VDS Advanced Research Group** for the amount shown, and mail it to us. You should receive a registered full copy on diskette within a week or so. All fields in bold letters must be filled in for correct processing of your order. Please use all capital letters and avoid cursive if possible.

Here are some of the features available only in the registered copy:

- External signature capability
- Frequently updated signature database
- No expiration date
- Advanced Examine Document command
- ZooSort option
- Free program updates for one year over the Internet
- No reminder screens about registration
- No pauses during scanning
- Scanning/cleaning password-protected documents
- Automatic cleaning option

If you wish to continue using Perforin, you are expected to buy a registered copy. The trial edition is made available only for evaluation purposes.

Order Form

VDS Advanced Research Group
P.O. Box 7573 York, PA 17404, U.S.A.

BBS: (717) 846-3873 info@vdsarg.com http://www.vdsarg.com

Perforin 2.0a Order Form

* All bold fields must be filled out. All sales are final.

Date: ___/___/_____

Name:____

Address:____

_______________**City**:________________ **State**: _____ **Zip**:_________

Phone: ( ) - Alt Phone: ( ) -

Email address: _______________________Contact Person:_____________

Number of Copies:_____________

Quantity:______________________ Price/Unit: $37.00

Sub-total:_____________________ (multiply quantity by price/unit)

Shipping:_____$3.00_(add another $15 if you are outside the U.S.)

Sales Tax (6% in PA):__________ (multiply sub-total by 0.06)

TOTAL:_________________________ (add sub-total, shipping, and sales tax)

Payment Method:

( ) Check #:_________ (payable to VDS Advanced Research Group)

( ) Credit Card:
( ) VISA ( ) Mastercard ( ) Discover ( ) AmEx

Card Number: _________________________ Exp. Date: ___________

Name on the Card:____

Customer's Signature:____

Where did you get Perforin?

( ) http://www.vdsarg.com ( ) http://www.ccso.com
( ) http://www.psnw.com/~joe ( ) AOL ( ) Other:______________________

-Name one thing you like about it:___________________________________

-May we add your email address to our list to notify you of new releases?
( ) Yes ( ) No

* Fill in the blanks, enclose a money order (outside the U.S.) or check for the total amount and mail it to our address. Allow 1-2 weeks for delivery. All sales are final. You can also pay by credit card and request electronic delivery over the Internet.

===
==========

For us to serve you better, please answer the following questions:

1. If any, which virus(es) infected your PCs so far? ______________________

2. Which antivirus software did you use to find/remove them? _____________

3. Do you use WinWord at home? ( ) No   ( ) Yes___version:________

4. Do you use WinWord at work?   ( ) No   ( ) Yes____version:________

5. Do you use any other word processing program besides WinWord?
   ( ) No   ( ) Yes _________________

6. Have you ever lost data due to a computer virus infection?   ( ) No   ( ) Yes

7. Do you own a Pentium multimedia PC?   ( ) No   ( ) Yes

===
============

* You can direct all questions/suggestions to   info@vdsarg.com

How To Submit A Suspicious Document

If you come across a document that Perforin reports as infected with a variant of a certain virus, then please send us a copy for analysis. We will examine the document for virus or trojan macros and usually provide you with information on its operation.

We also ask you to report **any** virus infections discovered on your computers to us for statistical survey purposes. You do not have to submit a sample in these cases unless you need a confirmation or a tech report.

We keep all submissions strictly confidential and try to replicate all virus samples we receive and destroy the originals. If the infected document contains sensitive business information, please mention that in your message and it will be handled with extra care, and the contents of the text portion will be overwritten with blanks before analysis.

Submission procedure is very simple. Here are the options we offer:

For PGP users:

If you are using a WWW browser like Netscape or MS Internet Explorer, then go to **http://www.vdsarg.com** and get a copy of VDSARG's public key. Add this key to your public key ring in PGP. After that encrypt the document with this key. Zip the resulting PGP encrypted file and send it to **help@vdsarg.com** as a binary attachment and a brief message telling us about the file and if you wish to receive a tech report.

Others:

If you are familiar with using FTP, then you can also upload suspicious documents to our FTP area over the Internet:

login anonymously to **ftp.vdsarg.com and** upload it to the **incoming** directory**.**

You can use the **PkZip** program to encrypt a file with the **-s** option. You can then email the zip file to **help@vdsarg.com** as a binary attachment along with a brief message about the file and if you wish to receive a tech report. In another message, email the password you have used to encrypt the document to **tyetiser@blazenet.net**. Please use a key that is 7 characters or longer. If you prefer better security, you can call **(717) 846-2343** and talk to an associate, and provide him with the password.

If you do not have email access, then you can upload the suspicious document to our tech support **BBS** at **(717) 846-3873**. Leave a brief message for **Tech Support** on the BBS. You should zip the file first, and choose ZMODEM protocol to transfer the file. Our BBS software has more trouble with other protocols. Set your modem to auto negotiate (ATN1) for more reliable connections. Our BBS uses 28.8K US Robotics modems.

You can also send us the suspicious document on a floppy diskette via surface mail. Please mark it clearly and send it to:

Attn: Tech Analysis
1500 N George St, Suite 15A
York, PA 17404

Information On Some Macro Viruses

We will be adding more information to this section as we analyze more viruses. If you find that any of the virus descriptions in this section are inaccurate, please contact us so that we can make the necessary corrections. Please send all messages to:

joe@vdsarg.com

You can find Hartmann's In-The-Wild Macro Virus List in the next section. We also added a list of viruses and passwords they use to encrypt documents as part of their damage routine.

Some of the entries describe trojan horse macros, rather than viruses. You can easily locate the description for a virus by using the Index of Viruses we have set up. For the sake of consistency, Perforin tries to use CARO names for the variants it can identify.
You can find brief information on how macro viruses work in the next section.

We use the following fields for each virus entry:

Virus name:	Common name of the virus
Number of macros:	Viral macros it adds to documents
Encrypted:	If the viral macros are encrypted
Macro names:	Names of the viral macros present
Size of macros:	Total size of the viral macros
Place of origin:	Country or city where it was first found or believed to be from
Date of origin:	Season of the year when it was first discovered
Destructive:	If it has intentional damage routines
Seen In-The-Wild:	Commonly found in the use community
Description:	Brief description of what the virus does and how

How Does A Macro Virus Work

Word macro viruses are written in the WordBasic language. This language is interpreted by WinWord. The virus code may reside in several subroutines. These are called macros, and they are usually kept in template files. However, it is very simple to convert a document to the template format so that the macros can be carried inside the documents.

Certain macros are loaded and executed by WinWord as soon as the document is opened. These are called auto macros. Many current macro viruses take advantage of this facility to gain control of the WinWord environment. Once the virus macro runs, it usually copies its macros to the global template file, by default   the global template file name is NORMAL.DOT. The reason for that is WinWord automatically loads and runs any macros found in NORMAL.DOT. This offers a perfect jumping point for the virus. When the user restarts WinWord and opens a clean document, the virus macros will be loaded from NORMAL.DOT and the virus can proceed to infect the document at an opportune time, such as when the document is saved. If the newly infected document is sent to another users, as it commonly happens, the infection cycle starts all over again on another user's machine.

There are other ways for a macro virus to gain control. Practically any command in Word can be subverted for the purposes of the virus. WinWord, by design, is very flexible and allow macros to override its default settings and commands.

With some viruses, the infection process is rather obvious. For example, WinWord will try to save your documents as templates with the .DOT extension for no apparent reason. In other cases, you will see unusual macro names listed if you look at them using the Tools menu in WinWord.

Other viruses conceal their presence by overriding certain commands in Word. It may be very difficult to find out if there is a virus from within Word. Some viruses have a damage routine and they may corrupt the contents of your documents or even password protect them and lock you out of your important data. A few macro viruses even drop conventional PC viruses on your hard drive or delete certain system configuration files.

To deal with macro viruses, you need to make sure the virus cannot gain control of the environment during examination of the documents. The only guaranteed way to do this is from outside WinWord. With tools such Perforin, the macro virus can be found and removed easily. However, it cannot be guaranteed that the data in your document was not altered by the virus already. You need to check the contents of the document after cleaning to see if everything looks fine.

Scanning process involves going thru your folders and files one by one, and examining the files that conform to the WinWord document format. If there are macros present, they are checked against an identification database we have built based on the existing macro viruses we are aware of. If there is a match, the name of the virus is displayed. Depending on the options you have set, the document can be cleaned.

Cleaning is a little trickier since there may be other macros besides the ones that belong to the virus. By default, Perforin will not remove unknown macros. It will remove all known virus macros. This way, you have the option to keep your good macros intact. Note that there is a possibility that the remaining macros belong to another virus unknown to Perforin at that time. To eliminate this possibility, you can set the cleaning option to Remove All Macros. We highly recommend that you configure Perforin to use this setting instead.

Once the documents are cleaned, you can start WinWord without the virus macros activating.

Passwords Some Viruses Use

Some viruses encrypt the documents as part of their damage routine when it triggers. We have a list of some of the more common macro viruses and the corresponding passwords you might be able to use to unlock your documents. If you run into other variants and passwords, please let us know. The following list is not yet complete, and we are going to be updating it.

Atom.A,B,C,D,E,F,G,J :	Atom#1
Atom,H :	ADULTSEX#1
Helper.A :	help
DMV.D :	exorcise
Andry.A :	Andry Christian
Bandboy.A :	gangsta
Friday.A :	Friday13
KillProt.A :	WhatTheHell
Talon.B :	talon
Talon.C :	talon3
Talon.D :	talon4
Talon.E :	talon5
Talon.F :	talon4
Reflex.A :	Guardian
Sam.A:Tw :	Sam
Dub.A :	wwsbmv
CountTen.A :	What the hell are you doing?
Xenixos.A :	XENIXOS

Some others ask for user input, either in a message box or on the status bar:

Goldfish.A :	fishfood, worms, pryme, core
Hassle.A :	Bill Gates, Microsoft, 666
Kompu.A :	komm
Spooky.A :	ykoops

Hartmann's In-The-Wild Macro Virus List

For a virus to be included **In the Wild** list, it has to be found in the "real world" at least once. However we decided to include only viruses that were reported at least twice by two different antivirus researchers. Our solution includes all the files that were reported to Joe Wells, who maintains a monthly list called the "Wildlist". A comprehensive set of all the Wildlists is available at the Virus Bulletin World Wide Web site: http://www/virusbtn.com

In addition to all the reported viruses from the "Wildlists" we asked for additional reports from other antivirus vendors and researchers. Whenever a virus was reported twice to us, we added it to the **Hartmann Macro Virus ITW List**.

List #1

WM.Appder.A (aka. FunYour)
WM.Bandung.A (a.k.a Jakarta)
WM.Bandung.I
WM.Boom.A (a.k.a. Boombastic)
WM.Buero.A (a.k.a. Bureau, BuroNeu)
WM.Cap.A
WM.Colors.A
WM.Concept.A (a.k.a. Prank, WW6Macro, Winword)
WM.Concept.B:Fr   (a.k.a. French)
WM.Concept.F (a.k.a. Parasite.A)
WM.Concept.J (a.k.a. Parasite.B)
WM.Date.A (a.k.a. AntiDMV, Infeczione)
WM.Divina.A (a.k.a. Roberta)
WM.Helper.A
WM.Hot.A
WM.Hybrid.A (a.k.a. Silly)
WM.Imposter.A
WM.Irish.A
WM.Johnny.A
WM.MDMA.A (a.k.a. StickyKeys, MDMA_DMV)
WM.MDMA.D
WM.Niceday.A
WM.NOP.A
WM.NPad.A (a.k.a. D0Eunpad)
WM.NPad.D
WM.Nuclear.A (a.k.a. Alert)
WM.Nuclear.B
WM.Rapi.A
WM.Rapi.AA2
WM.Sharefun.A
WM.ShowOff.C (a.k.a. Ofxx)
WM.TWNO.A (a.k.a Taiwan_1)
WM.Wazzu.A
WM.Wazzu.C
WM.Wazzu.E
WM.Wazzu.F (a.k.a. Bosco)
WM.Wazzu.J
WM.Wazzu.P
WM.Wazzu.X

In addition to the main ITW list, we prepared a second In-the-Wild list set, which includes macro viruses reported as being real-world problems by only one anti-virus researcher.

List #2

WM.Alien.A (a.k.a. Chandi)
WM.Alliance
WM.Anak.A
WM.Appder.B
WM.Attack.A
WM.Bandung.G
WM.Cap.D
WM.Cap.L
WM.Chaos.B
WM.Clock.A:De (a.k.a. Extra)
WM.Colors.B
WM.Colors.G
WM.Concept.AJ WM.Concept.AK
WM.Concept.B:Fr (a.k.a. French)
WM.Concept.C
WM.Concept.G (a.k.a. Parasite 0.8)
WM.Concept.O:Tw
WM.Concept.Q
WM.Concept.Z
WM.CountTen.A
WM.Date.B
WM.Divina.C
WM.Divina.D
WM.Dub.A
WM.Dzt.A (aka Hellgate.A) WM.Friday.A
WM.Goldfish.A (a.k.a.Fishfood)
WM.GoodNight.A
WM.Hassle.A (a.k.a Assistant)
WM.Helper.B
WM.Hiac.A
WM.Kompu.A
WM.Lunch.B
WM.Lunch.C
WM.Maddog.A
WM.Maddog.B
WM.MDMA.C
WM.MDMA.E
WM.MDMA.F
WM.MDMA.I
WM.MDMA.J
WM.Muck.B
WM.Nf.A
WM.Niceday.A
WM.Niceday.F
WM.Nop.B:Tw
WM.Nop.F:De
WM.Nop.J:De
WM.Nop.K
WM.Oval.A
WM.Paycheck.A
WM.Red.A

WM.Surabaya.A
WM.Swlabs.A
WM.Swlabs.C
WM.Temple.A
WM.Toten.A:De
WM.Theater.A:Tw
WM.Theater.B:Tw
WM.Wazzu.AV
WM.Wazzu.AW
WM.Wazzu.BS
WM.Wazzu.F (a.k.a. Bosco)
WM.Wazzu.H (a.k.a Microsloth)
WM.Wazzu.O
WM.Wazzu.Q
WM.Wazzu.X
WM.Weather.A (a.k.a Fish)
WM.Xenixos.A (Nemesis, XOS, Evil One)

If there are any questions regarding this document, please feel free to contact Joe Hartmann via email: **joe@vdsarg.com**

A - Virus Names Starting With The Letter A

B - Virus Names Starting With The Letter B

C - Virus Names Starting With The Letter C

D - Virus Names Starting With The Letter D

E - Virus Names Starting With The Letter E

F - Virus Names Starting With The Letter F

G - Virus Names Starting With The Letter G

H - Virus Names Starting With The Letter H

I - Virus Names Starting With The Letter I

J - Virus Names Starting With The Letter J

K - Virus Names Starting With The Letter K

L - Virus Names Starting With The Letter L

M - Virus Names Starting With The Letter M

N - Virus Names Starting With The Letter N

O - Virus Names Starting With The Letter O

P - Virus Names Starting With The Letter P

Q - Virus Names Starting With The Letter Q

R - Virus Names Starting With The Letter R

S - Virus Names Starting With The Letter S

T - Virus Names Starting With The Letter T

U - Virus Names Starting With The Letter U

V - Virus Names Starting With The Letter V

W - Virus Names Starting With The Letter W

X - Virus Names Starting With The Letter X

Y - Virus Names Starting With The Letter Y

Z - Virus Names Starting With The Letter Z

A - Virus Names Starting With The Letter A

Alien
Alliance
Appder
Atom

Alien

Virus name:	Alien.A
Number of macros:	3
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose, FileSaveAs
Size of macros:	7037 Bytes
Place of origin:	India
Date of origin:	November 1996
Payload:	Yes
Seen In-The-Wild:	No
Description:	

Alien infects the global tempate (normal.dot) when an infected document is opened. Further documents become infected when they are opened or closed.

Before infection Alien checks for the string "Alien". If already present, Alien does not infect.

The "ToolsCustomize" and "ToolsMacro" options are removed by Alien to make recognition of an infected file more difficult (called macro stealth technique).

With a probability of 50 percent Alien displays the following message, on August 1st, and hides the "program manager" in Windows 3.x:

"   Another Year of Survival   "

Users are then unable to shut down Windows.

Again with a probability of 50 percent Alien displays the following message:

"   It's Sunday & I intend to relax   "

Alien then tries to hide the "program manager" and terminate Microsoft Word without saving the active document.

Alien also displays varies other messages:

"   You Fascinate Me.   "
"   Look No Furhter...   "
"   Hi Beautiful !   "
"   I'll Be Back !   "
"   Three Cheers For The Alien. Hip Hip Hooray !   "
"   Don't Believe the Hype !   "
"   Always Back Up Your Data.   "
"   Don't Believe All Tips !   "
"   Never Trust An Alien !   "
"   Never Open Other Files !   "
"   The 'Alien' Virus Has Arrived !   "
"   The Alien Lives...   "
"   Longer File Names Should Be Used.   "

Alliance

Virus name:	Alliance
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen
Size of macros:	352 Bytes
Place of origin:	USA
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Upon opening an infected document, Alliance will infect the global template (NORMAL.DOT). Further documents become infected when they are opened ("AutoOpen").

Alliance is only infectious on the:

2nd day of each month.
7th day of each month.
11th day of each month.
12th day of each month.

Alliance adds the following comment to the File/Properties section:

"   You have been infected by the Alliance   "

Appder

Virus name: Appder.A (a.k.a.FunYour)
Number of macros: 2 or 3
Encrypted: No
Macro names: Appder, AutoOpen, AutoClose
Size of macros: 1912 Bytes in .doc file, 1126 Bytes in global template
Place of origin: Unknown
Date of origin: Unknown
Destructive: Yes
Seen In-The-Wild: No
Description:

Appder infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are closed. Appder adds a "NTTHNTA=xx" value to the [Microsoft Word] section of winword6.ini and increases the value by one when infecting documents. Upon reaching a value of 20, Appder triggers its destructive payload and deletes the following files:

C:\DOC\*.exe
C:\DOC\*.com
C:\WINDOWS\*.exe
C:\WINDOWS\SYSTEM\*.TTF
C:\WINDOWS\SYSTEM\*.FOT

As a result Windows 3.x does not work properly.

Virus name: Appder.B (a.k.a.FunYour)
Number of macros: 2 or 3
Encrypted: No
Macro names: Appder, AutoOpen, AutoClose
Size of macros: 1528 Bytes in documents   934 Bytes in global template
Place of origin: Unknown
Date of origin: Unknown
Destructive: No
Seen In-The-Wild: Yes

Description:

The difference between this new variant and the original Appder.A virus is that the payload has been deleted from the macro code. Therefore Appder.B does not delete any files.

Appder.B infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are closed (AutoClose).

Virus name: Appder.C (a.k.a.FunYour)
Number of macros: 2 or 3
Encrypted: No
Macro names: Appder, AutoOpen, AutoClose
Size of macros: 1912 Bytes in .doc files   1126 Bytes in global template
Place of origin: Unknown
Date of origin: Unknown
Destructive: Yes

Seen In-The-Wild: No

Description:

The difference between this new variant and the original Appder.A virus is that Appder.C has a one byte code modification.

Appder.C infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are closed (AutoClose). Appder.C adds a "NTTHNTA=xx" value to the [Microsoft Word] section of winword6.ini and increases the value by one when infecting documents. Upon reaching a value of 20, Appder.C triggers its destructive payload and deletes the following files:

C:\DOC\*.exe
C:\DOC\*.com
C:\WINDOWS\*.exe
C:\WINDOWS\SYSTEM\*.TTF
C:\WINDOWS\SYSTEM\*.FOT

As a result Windows 3.x does not work properly.

Atom

Virus name: Atom.A (a.k.a. Atomic)
Number of macros: 4
Encrypted: Yes
Macro names: Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros: 1029 Bytes
Place of origin: Ukraine
Date of origin: February 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

Atom infects the global template (Normal.dot) once an infected document is opened. Further documents become infected when a document is opened (FileOpen) or saved (FileSaveAs).

When the "FileSaveAs" macro is called, Atom checks the system clock for a value of 13 in the seconds field. If this is the case, Atom adds the password "ATOM#1" to the saved document.

The destructive payload inside the "Atom" is activated on the 13th of each month. On this day, Atom deletes all the files inside the current directory.

Virus name: Atom.B
Number of macros: 4
Encrypted: Yes
Macro names: Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros: 1053 Bytes
Place of origin: Unknown
Date of origin: December 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

The differences between this new variant and the original Atom.A virus are only minor. They do not affect the functionality of this new variant.

For more information, please refer to the Atom.A virus description.

Virus name: Atom.C
Number of macros: 4
Encrypted: Yes
Macro names: Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros: 1026 Bytes
Place of origin: Unknown
Date of origin: December 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

The differences between this new variant and the original Atom.A virus are only minor. They do not affect the functionality of this new variant.

For more information, please refer to the Atom.A virus description.

Virus name:	Atom.D
Number of macros:	4
Encrypted:	Yes
Macro names:	Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros:	1024 Bytes
Place of origin:	Unknown
Date of origin:	December 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

The differences between this new variant and the original Atom.A virus are only minor. They do not affect the functionality of this new variant.

For more information, please refer to the Atom.A virus description.

Virus name:	Atom.E
Number of macros:	4
Encrypted:	Yes
Macro names:	Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros:	1017 Bytes
Place of origin:	Unknown
Date of origin:	December 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

The differences between this new variant and the original Atom.A virus are only minor. They do not affect the functionality of this new variant.

The programming error from Atom.A, which activated the payload on the 13th of each month, has been fixed in this new variant. Atom.E activates only on the 13th of December.

For more information, please refer to the Atom.A virus description.

Virus name:	Atom.F
Number of macros:	4
Encrypted:	Yes
Macro names:	Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros:	1022 Bytes
Place of origin:	Unknown
Date of origin:	December 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

The differences between this new variant and the original Atom.A virus are only minor. They do not affect the functionality of this new variant.

For more information, please refer to the Atom.A virus description.

Virus name: Atom.G:De (a.k.a. Atomic)
Number of macros: 4
Encrypted: Yes
Macro names: Atom, AutoOpen, DateiOeffnen, DateiSpeichernUnter
Size of macros: 1120 Bytes
Place of origin: Germany
Date of origin: February 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

Atom.G infect the global template (Normal.dot) once an infected document is opened. Further documents become infected when a document is opened (DateiOeffnen) or saved (DateiSpeichernUnter).

When the "DateiSpeichernUnter" macro is called, Atom.G checks the system clock for a value of 13 in the seconds field. If this is the case, Atom.G adds the password "ATOM#1" to the saved document.

The destructive payload inside the "Atom" is activated on the 13th of December. On this day, Atom.G deletes all the files inside the current directory.

Atom.G only works with the German version of Microsoft Word, since it uses language specific macros.

Virus name: Atom.H (a.k.a. Adultsex)
Number of macros: 4
Encrypted: Yes
Macro names: Atom, AutoOpen, FileOpen, FileSaveAs
Size of macros: 1302 Bytes
Place of origin: Unknown
Date of origin: February 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

The difference between this new variant and the original Atom.A virus is that the payload has been changed in this new variant.

Instead of deleting files, Atom.H displays the following message when opening documents:

> KISS ME FUCK ME LOVE ME BITCH SUCK MY DICK ADULT SEX !!
> I LOVE SEX DRUGS CLASS A DRUGS YEAH MAN !
> I ASK YOU MY DARLING FOR ANAL SEX GIVE IT TO ME !
> EVER DANCED WITH THE DEVIL ON THE MOONLIGHT ?
> PREY FOR YOUR CUNT YOU SEXY HORNEY BITCH

The password, which is added to a saved document, was also changed from "ATOM#1" to "ADULTSEX#1".

For more information, please refer to the Atom.A virus description.

B - Virus Names Starting With The Letter B

Bandung
Birthday
Boom
Box
Buero

Bandung

Virus name: Bandung.A (a.k.a. Jakarta)
Number of macros: 6
Encrypted: No
Macro names: AutoExec, AutoOpen, FileSave, FileSaveAs
Toolsmacro, Toolscustomize
Size of macros: 4262 Bytes
Place of origin: Bandung, Indonesia
Date of origin: August/September 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

Bandung infects the global template (Normal.dot) when an infected document is opened. Further documents are infected with the "FileSave" and "FileSaveAs" command.

Bandung uses macro stealth techniques to hide itself. It uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique).

The destructive payload activates when Microsoft Word is started. It checks the date and time and in case of a date later than the 19th of each month and a time after 11:00 am, Bandung deletes all files in all directories. An execption for this are the files located in the following directories:

C:\WINDOWS
C:\WINWORD
C:\WINWORD6

After the file deletion, Bandung creates the file C:\PESAN.TXT. The file contains some Indonesian text telling the user: (translated into English)

" You are unlucky, all files on this machine have been deleted, "
" except for WINDOWS and WINWORD, don't panic, this is not your "
" fault, but this the result of my work......Whoever is able to "
" find a way to combat this virus, I will give the virus listing "
" to you!!!! And of course I will constantly return to greet you "
" with my new viruses .....good luck ! Bandung Monday, "
" June 28 1996, 13:00 pm "

Another payload replaces the letter "a" with "#@". This occurs when the "ToolsCustomize" macro is called.

Bandung also displays some WordBasic error messages.

Virus name: Bandung.B
Number of macros: 6
Encrypted: No
Macro names: AutoExec, AutoOpen, FileSave, FileSaveAs
Toolsmacro, Toolscustomize
Size of macros: 4262 Bytes
Place of origin: Bandung, Indonesia
Date of origin: August/September 1996
Destructive: No

Seen In-The-Wild:	No
Description:	

The difference between this new variant and the original Bandung.A virus is that the AutoExec, ToolsMacro and ToolsCustomize macros are corrupted.

Due to the corruption, Bandung.B does not activate its destructive payload. Instead of the payload activation, it displays various error messages. Bandung.B is still able to infect the global template and further documents.

Bandung uses "Toolsmacro" to make recognition of an infected file more difficult (called macro stealth technique).

Virus name:	Bandung.C
Number of macros:	6
Encrypted:	No
Macro names:	AutoExec, AutoOpen, FileSave, FileSaveAs, Toolsmacro, Toolscustomize
Size of macros:	5428 Bytes
Place of origin:	Bandung, Indonesia
Date of origin:	December 1996
Payload:	Yes
Seen In-The-Wild:	No
Description:	

The difference between this new variant and the original Bandung.A virus is that the "AutoExec" macro was replaced with the corrupted "AutoOpen" macro from the Rapi virus.

The payload replaces the letter "a" with "#@". This occurs when the "ToolsCustomize" macro is called.

Bandung.C uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique).

Due to the new macro code, Bandung.C displays a Syntax error message whenever Microsoft Word is started.

Virus name:	Bandung.D
Number of macros:	6
Encrypted:	No
Macro names:	AutoExec, AutoOpen, FileSave, FileSaveAs, Toolsmacro, Toolscustomize
Size of macros:	4262 Bytes
Place of origin:	Bandung, Indonesia
Date of origin:	December 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

The difference between this new variant and the original Bandung.A virus is that the "AutoExec" macro is corrupted. Even though there is a corruption in the "AutoExec" macro, Bandung.D still activates its destructive payload when Microsoft Word is started.

Another payload replaces the letter "a" with "#@". This occurs when the "ToolsCustomize" macro is called.

Bandung.D uses macro stealth technique to hide itself. It uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique).

Due to its macro corruption, Bandung.D displays some error messages.

For more information, please refer to the Bandung.A virus description.

Virus name: Bandung.E
Number of macros: 6
Encrypted: No
Macro names: AutoExec, AutoOpen, FileSave, FileSaveAs, Toolsmacro, Toolscustomize
Size of macros: 4262 Bytes
Place of origin: Bandung, Indonesia
Date of origin: January 1997
Payload: Yes
Seen In-The-Wild: No
Description:

The difference between this new variant and the original Bandung.A virus is that the "AutoExec" macro is corrupted.

The payload replaces the letter "a" with "#@". This occurs when the "ToolsCustomize" macro is called.

Bandung.E uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique).

Due to its macro corruption, Bandung.E never executes its destructive payload. Instead it displays the following Wordbasic error message:

" Out of Memory "

Virus name: Bandung.G
Number of macros: 6
Encrypted: No
Macro names: AutoExec, AutoOpen, FileSave, FileSaveAs, ToolsMacro, ToolsCustomize
Size of macros: 1990 Bytes
Place of origin: Bandung, Indonesia
Date of origin: January 1997
Payload: Yes
Seen In-The-Wild: No
Description:

The only difference between this new variant and the original Bandung.A virus is the "AutoExec" macro. Bandung.G contains only two lines. One line is empty and one contains a "DisableAutoMacros" statement.

The payload replaces the letter "a" with "#@". This occurs when the "ToolsCustomize" macro is called.

Bandung.G does not have the destructive payload from the original Bandung.A virus.

Virus name:	Bandung.I
Number of macros:	6
Encrypted:	No
Macro names:	AutoExec, AutoOpen, FileSave, FileSaveAs, ToolsMacro, ToolsCustomize
Size of macros:	1988 Bytes
Place of origin:	Bandung, Indonesia
Date of origin:	February 1997
Destructive:	No
Seen In-The-Wild:	No
Description:	

The only difference between this new variant and the original Bandung.A virus is the "AutoExec" macro. Bandung.I contains only three lines from an Anti-Virus solution, which disables all the automacros.

Bandung.I does not have the destructive payload from the original Bandung.A virus.

For more information, please refer to the Bandung.A virus.

Birthday

Virus name:	Birthday.A:De (a.k.a. PCW)
Number of macros:	2
Encrypted:	Yes
Macro names:	AutoOpen, DateiSpeichernUnter
Size of macros:	1039 Bytes
Place of origin:	German computer magazine
Date of origin:	July 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Birthday infects the global template (normal.dot) when an infected document is opened. Further documents become infected when the "DateiSpeichernUnter" command is used.

It displays the following message:

" Happy Birthday! Herzlichen Glückwunsch... "

Boom

Virus name:	Boom.A:De (a.k.a. Boombastic)
Number of macros:	4
Encrypted:	Yes
Macro names:	AutoExec, AutoOpen, DateiSpeichernUnter, System
Size of macros:	2863 Bytes
Place of origin:	Germany
Date of origin:	July 1996
Payload:	Yes
Seen In-The-Wild:	Yes
Description:	

Boom is the second macro virus written for the German version of Microsoft Word.

Boom's destructive payload renames the menu structure of Word to:

Datei	->	Mr.Boombastic
Bearbeiten	->	and
Ansicht	->	Sir WIXALOT
Einfuegen	->	are
Format	->	watching
Extras	->	you
Tabelle	->	!
Fenster	->	!
Hilfe	->	!

A sound is send to the PC speaker during the renaming process. After the menu change, Boom will create a new global template and insert the following text:

" Greetings from Mr. Boombastic and Sir WIXALOT !!! "

" Oskar L., wir kriegen dich!!! "

"Dies ist eine Initiative des Institutes zur Vermeidung und Verbreitung von "
" Peinlichkeiten, durch in der Oeffentlichkeit stehende Personen, unter der " "
Schirmherrschaft von Rudi S. ! "

This text will be printed by Boom.

Box

Virus name:	Box.B
Number of macros:	7
Encrypted:	Yes
Macro names:	Box, Dead, AutoOpen, AutoClose, FilePrint, FilePrintDefault, ToolsMacro
Size of macros:	1988 Bytes
Place of origin:	Taiwan
Date of origin:	February 1997
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Box.B infects the global template and further documents when an infected document is opened (AutoOpen) or closed (AutoClose).

Box.B uses "ToolsMacro" to make recognition of an infected file more difficult (called macro stealth technique).

Box.B consists of several destructive payloads. One payload formats the C:\ drive, another one drops the Dos-based virus "One Half.3544".

A third payload displays the following messages and adds it to printed documents:

"   Taiwan Super No. 1 Macro Virus   "
"   Twno1-S   "
"   Today is my Birthday   "

Box.B only works with the Chinese version of Microsoft Word.

Buero

Virus name: Buero.A (a.k.a Bureau, BuroNeu)
Number of macros: 2
Encrypted: Yes
Macro names: AutoOpen (DateiSpeichern), BueroNeu
Size of macros: 697 Bytes
Place of origin: Germany
Date of origin: August 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

Buero is another macro virus written for the German version of Microsoft Word.

Buero infects the global template (Normal.dot) when an infected document is opened. Further documents become infected with the "DateiSpeichern" (only in the global template) command.

After August 15th, 1996, Buero renames the system file "IO.SYS" to "IIO.SYS". This action will leave the computer unbootable. The second destructive payload searches for C:\*.DOC files and deletes them.

C - Virus Names Starting With The Letter C

Cap
Cebu
Clock
Colors
Concept
CountTen

Cap

Virus name:	Cap.a
Number of macros:	Variable
Encrypted:	Yes
Macro names:	CAP
Size of macros:	Variable
Place of origin:	Unknown
Date of origin:	December 1996
Destructive:	No
Seen In-The-Wild:	Yes

Description:

Cap.A is another complex macro virus that is able to spread on various localized versions of Microsoft Word. While some macros keep the same name, others are automatically assigned new names from the localized version of Word.

When Cap.A infects the global template, it deletes all existing macros. It infects the global tempalate when an infected document is opened.

Cap.A uses "ToolsMacro" and "FileTemplates" to make recognition of an infected document more difficult (called macro stealth technique).

Cebu

Virus name:	Cebu.A
Number of macros:	4 or more
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose, AutoExec, MSRun
Size of macros:	1237 Bytes
Place of origin:	Hong Kong
Date of origin:	Spring 1997
Destructive:	Yes
Seen In-The-Wild:	No

Description:

Cebu infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen) or closed (AutoClose).

When Cebu triggers (probability of 59/60), it replaces the word " Asian " with the Word " Cebu ". This happens when Microsoft Word is started (AutoExec) and sixty-four minutes later (new probability: 2/15).

Cebu is one of very few macro viruses that copies user macros, therefore it can exist with 4 or more macros. We recommend that you de-install macro anti-virus solutions (such as Scanprot) in order to prevent Cebu from snatching macros.

Virus name:	Cebu.B
Number of macros:	4 or more
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose, AutoExec, MSRun
Size of macros:	1976 Bytes
Place of origin:	Unknown
Date of origin:	May 1997
Destructive:	Yes
Seen In-The-Wild:	No

Description:

Cebu.B infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen) or closed (AutoClose).

The main difference between this new variant and the previous Cebu.A virus is that Cebu.B has some modified code and also contains various bugs.

For more information, please refer to the Cebu.A virus description.

Clock

Virus name: Clock.A:De (a.k.a Extra)
Number of macros: 11
Encrypted: Yes
Macro names: Action, AutoExec, AutoOpen, Extrasmakro, DateiSchliessen,
Datumunduhrzeit, DateiDokVorlagen, Dateiallesspeichern,
Oeffnen, Speichern
Size of macros: 3795 Bytes
Place of origin: USA
Date of origin: Summer 1996
Payload: Yes
Seen In-The-Wild: No
Description:

Clock is another macro virus written for the German version of Microsoft Word. It uses "ExtrasMakro" and "DateiDokVorlagen" to make recognition of an infected document more difficult (called macro stealth technique).

When an infected document is opened after the 26th of each month, Clock will display a window containing the time. It will also activate one of its payloads, which sets the system clock to a value of 33 in the seconds field. Clock does this every 2 to 3 minutes, which results in a less accurate system clock.

The second payload will start in 1997. Clock will check the system clock, and in case of a minute value smaller than 5, it will flip the "FileOpen" and "FileSave" macros.

This effect will only happen on:

1st of each month
2nd of each month
13th of each month
21st of each month
27th of each month

Colors

Virus name:	Colors.A (a.k.a Rainbow)
Number of macros:	9
Encrypted:	Yes
Macro names:	AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro
Size of macros:	6470 Bytes
Place of origin:	Portugal
Date of origin:	Posted to Usenet in October 1995
Payload:	Yes
Seen In-The-Wild:	Yes
Description:	

Colors is the first macro virus that can still infect, even when all the Auto-macros are turned off. It also uses "ToolsMacro" to make recognition of an infected file more difficult (called macro stealth technique).

Upon activation of one of its macros (all except for AutoExec), Colors tries to infect the global template (normal.dot). It checks if all its macros are already present in the global template and if this is not the case, it transfers the virus macros or replaces already existing ones.

The global template becomes infected when a document is opened, saved, closed or Microsoft Word is exited. Further documents become infected when a file is created (FileNew) or saved (FileSave, FileSaveAs).

The destructive payload is located in the "macros" macro. Once activated Colors creates a variable in the [Windows] section of Win.ini with the name "countersu", which counts upwards from zero. After each 300th call, Colors changes the color palette of 21 Windows desktop elements. Background, buttons and borders will have new randomly selected colors, which will leave the user with a sometimes unusual looking desktop.

Virus name:	Colors.B (a.k.a Colo-b)
Number of macros:	9
Encrypted:	Yes
Macro names:	AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro
Size of macros:	7006 Bytes
Place of origin:	Portugal
Date of origin:	April 1996
Payload:	Yes
Seen In-The-Wild:	No
Description:	

Colors.B seems to be a variant of the previous found Colors.A virus. All of the macros seem to be identical to Colors.A, except for the "AutoOpen" macro, which seems to come from the Concept virus. It looks like a Colors infected document was re-infected with Concept, which replaced the "AutoOpen" macro with its own.

Colors.B is still able to replicate, even though it has new virus code from a different virus. Colors.B is the first virus that combines virus code from 2 different viruses (Colors.A and Concept.A).

Virus name:	Colors.C (a.k.a Colo-c)

Number of macros: 9
Encrypted: Yes
Macro names: AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro
Size of macros: 6493 Bytes
Place of origin: Unknown
Date of origin: July 1996
Payload: Yes
Seen In-The-Wild: No
Description:

Colors.C seems to be a corrupted variant of the previous found Colors.A virus. The submitted virus sample infected the global template (normal.dot) and new documents, yet the new infected documents were unable to infect further documents. Only the first generation was able to infect other files. Colors.C is therefore very unlikely to survive in the wild.

Virus name: Colors.D (a.k.a Colo-d)
Number of macros: 9
Encrypted: Yes
Macro names: AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro
Size of macros: 19688 Bytes
Place of origin: Unknown
Date of origin: August 1996
Payload: Yes
Seen In-The-Wild: No
Description:

Colors.D seems to be a combination of the previous found Colors.A virus and the Microsoft macro virus solution "Scanprot".

Even though Colors.D has part of an Anti-Virus solution in its code, it is still able to spread and infect the global template (normal.dot) and further documents.

Concept

Virus name:	Concept.A (a.k.a Prank, WW6Macro, Winword, WBMV)
Number of macros:	4
Encrypted:	No
Macro names:	AutoOpen, AAAZAO, AAAZFS (FileSaveAs), Payload
Size of macros:	1968 Bytes
Place of origin:	USA
Date of origin:	July 1995
Destructive:	No
Seen In-The-Wild:	Yes
Description:	

Concept was the first macro virus found "In-the-Wild". It was discovered in July-August 1995 and is now the most common virus.

Concept activates when an infected document is opened (AutoOpen). Upon activation, Concept checks for a previous infection of the global template (normal.dot). If none of the macros are present, Concept copies its virus macros. The "AAAZFS" macro is saved under the name "FileSaveAs".

After infecting the global template, Concept makes an entry in the Win.ini file. It sets "WW6I=1" and displays a window with a "1" in it.

Concept does not contain any destructive payload, even though is has a macro with the name "Payload". The "Payload" macro is empty except for the following text:

"   That's enough to prove my point   "

Virus name:	Concept.B
Number of macros:	4
Encrypted:	No
Macro names:	AutoOpen, AAAZAO, AAAZFS (FileSaveAs), Payload
Size of macros:	2016 Bytes
Place of origin:	France
Date of origin:	Spring 1996
Destructive:	No
Seen In-The-Wild:	Yes
Description:	

The only difference between Concept.A and Concept.B is that the virus author translated the "FileSaveAs" macro into its French equivalent. Therefore this new variant only works with the French version of Microsoft Word.

Virus name:	Concept.C
Number of macros:	4
Encrypted:	No
Macro names:	AutoOpen, F1, F2, Boom, FileSaveAs
Size of macros:	1834 Bytes in .doc files , 1559 Bytes in .dot files
Place of origin:	Unknown
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

The difference between this new variant and the original Concept virus can be found in the macro names and the content of the "Boom" macro. Concept.C activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved with the "FileSaveAs" command.

Concept.C displays a message box with a " 1 " in it.

The "Boom" macro contains another message, yet not displayed:

" Fight racism; Smash Fascizm "

Virus name:	Concept.D (a.k.a. Haha)
Number of macros:	4
Encrypted:	3 of the 4 macros
Macro names:	AutoOpen (FileSaveAs), EditSize, FileSort, HaHa
Size of macros:	2129 Bytes in .doc files, 2041 Bytes in .dot files
Place of origin:	Unknown
Date of origin:	Summer 1996
Payload:	Yes
Seen In-The-Wild:	No

Concept.D activates when an infected file is opened (AutoOpen). Further documents become infected when they are saved with the FileSaveAs command.

Upon infection of a new document, Concept.D changes the font color of all the existing text to white, which creates the impression that all the text disappeared (or was deleted). Concept.D then adds the following text to the active document:

" i said: say goodbye to all your stuff (look at that hard drive spin!). "

Upon an attempt to save an infected document, Concept.D tries to save the document 100 times, causing an unregular disk activity.

Virus name:	Concept.E
Number of macros:	4
Encrypted:	No
Macro names:	AutoOpen (FileSaveAs), AAAZAO, AAAZFS, Load
Size of macros:	1657 Bytes in .doc files, 1472 Bytes in .dot files
Place of origin:	Unknown
Date of origin:	Summer 1996
Payload:	Yes
Seen In-The-Wild:	No
Description:	

The difference between this new variant and the original Concept virus can be found in the names of the macros and the content of the "Load" macro. Concept.E activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved with the FileSaveAs command.

Upon infection of a new document, Concept.E displays a message with a " 1 " in it.

Concept.E also has virus code that tries to save the active document in the T:\VIR directory.

Virus name:	Concept.F (a.k.a. Parasite 1.0, P-Site)
Number of macros:	7

Encrypted: Yes
Macro names: K, A678, Para, Site, I8U9Y13, Paylaod, AutoOpen
Size of macros: 3673 Bytes in .doc files, 3453 Bytes in .dot files
Place of origin: USA
Date of origin: July 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

Concept.F has various payloads. The first one replaces the following words in infected documents:

"and" with "not".

The second payload is a little bit more comprehensive. Concept.F checks the system time for a specific value in the days section. In case of a 16 (16th of each month), it activates its payloads. It then replaces the following letters/words in infected documents:

"." (dot) with "," (comma)

"and" with "not"

"a" with an "e"

This new Concept variant also displays the following window:

" Parasite Virus 1.0 "

" Your computer is infected with the Parasite Virus, Version 1.0! "

Virus name: Concept.G (a.k.a. Parasite 0.8, P-Site)
Number of macros: 7
Encrypted: Yes
Macro names: K, A678, Para, Site, I8U9Y13, Paylaod, AutoOpen
Size of macros: 3670 Bytes in .doc files, 3450 Bytes in .dot files
Place of origin: USA
Date of origin: July/August 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

According to the Concept.G virus code, this new variant is a beta release of the Concept.F (version 1.0) virus. Concept.G has various payloads. The first one replaces the following words in infected documents:

"and" with "not"

The second payload is a little bit more comprehensive. Concept.G checks the system time for a specific value in the days section. In case of a 16 (every 16th of the month) it activates its payloads. It then replaces the following letters/word in infected documents:

"." (dot) with "," (comma)

"and" with "not"

"a" with an "e"

Virus name: Concept.I
Number of macros: 4 or 5
Encrypted: No
Macro names: AAAEED, AAAUUO, IPayload, DocClose, ToolsSpelling
Size of macros: 2885 Bytes
Place of origin: USA
Date of origin: September 1996
Destructive: No
Seen In-The-Wild: No
Description:

Concept.I activates when an infected document is closed (DocClose).

Further documents become infected in two different ways. It infects when the user selects the option "Tools/Spelling" or when an infected document is closed (DocClose).
Depending on the selected infection routine, a new infected document contains 5 (DocClose infection routine) macros or only 4 (Tools/Spelling infection routine) macros.

Upon infection of a new document, Concept.I displays a message with
a " 1 " in it.

Virus name: Concept.K:NL (a.k.a. Pheeew)
Number of macros: 4
Encrypted: No
Macro names: AutoOpen, IkWordNietGoed1, IkWordNietGoed2, Lading
Size of macros: 2759 Bytes
Place of origin: Unknown
Date of origin: Unknown
Destructive: Yes
Seen In-The-Wild: No
Description:

Concept.K is the first Dutch macro virus.

When an infected document is opened, Concept.K checks for a previous infection of the global template (normal.dot). It does this by looking for the two names of the macros "Lading" and
"BestandOpslaanAls". Is the global template not infected, Concept.K copies its virus macros into the global template. The macro "IkWordNietGoed2" is saved under the name "BestandOpslaanAls" ("FileSaveAs"). Further documents become infected when the "FileSaveAs" command is used. After infection the virus shows various windows with the following text:

Window 'Important':

"   Gotcha !   "

Window 'FINAL WARNING!':

"   STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC   "

If a user clicks the "No" button on the last window, a destructive payload is activated. All files in the "C:\" and "C:\DOS" directory are deleted. This leaves the computer unbootable.

Virus name:	Concept.L (a.k.a. BlastC)
Number of macros:	7
Encrypted:	No
Macro names:	Alignment, AutoOpen, BorderSet, FileSaveAs, AutoClose, ExitRoutine, BlastCDrive
Size of macros:	3744 Bytes
Place of origin:	USA
Date of origin:	Unknown
Payload:	Yes
Seen In-The-Wild:	No
Description:	

Concept.L activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved (FileSaveAs).

Concept.L displays 2 messages:

Upon activiation:

" Welcome to the 'WINWORD.BLAST_C' macro virus... "

After infection of the global template (Normal.dot):

" Uh Ohhh. NORMAL.DOT just got infected... "

Upon closing the active document on the 24th of each month, Concept.L will start its destructive payload. It will launch the File Manager and delete the directory C:\DELETEME.

Virus name:	Concept.M (a.k.a. New_Horizon)
Number of macros:	5
Encrypted:	No
Macro names:	Alignment, AutoOpen, BorderSet, FileSaveAs, AutoClose, ExitRoutine
Size of macros:	2432 Bytes in .doc files, 2055 Bytes in global template
Place of origin:	USA
Date of origin:	Unknown
Destructive:	No
Seen In-The-Wild:	No
Description:	

Concept.M activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved with the "FileSaveAs" command.

This new Concept variant displays 2 messages:

Upon activation:

" Uh Ohhh. NORMAL.DOT just got infected... "

Upon opening of an infected document:

" Welcome to the Winword.New_Horizons macro virus "

CountTen

Virus name:	CountTen.A (a.k.a. SaveCount)
Number of macros:	3
Encrypted:	Yes
Macro names:	AutoOpen FileSave, FileSaveAs
Size of macros:	956 Bytes
Place of origin:	United States
Date of origin:	December 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

CountTen infects documents when an infected document is opened and saved via the "FileSave" and FileSaveAs" command.

When CountTen infects a file, it sets the variable "SaveCount". When an infected file is saved, the variable is increased. This technique is used to keep track of the number of times an infected document has been saved. Upon reaching 10, CountTen sets the following password:

"   What the hell are you doing?   "

This password is too long for the Microsoft Word password box and therfore users can not change the password.

To get access to a password encrypted file, remove the viral macros and create an "AutoOpen" macro with the following information in the global template (NORMAL.DOT):

```
Sub Main
    ToolsUnprotectDocument.DocumentPassword="What the hell are you doing?"
End Sub
```

D - Virus Names Starting With The Letter D

Daniel
Date
Dietzel
Divina
DMV
Doggie
Dub
Dzt

Daniel

Virus name: Daniel.A (a.k.a Daniel_1F)
Number of macros: 2
Encrypted: Yes
Macro names: AutoOpen (Word6Menu), MacroManager
Size of macros: 2718 Bytes
Place of origin: Unknown
Date of origin: September 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

Daniel activates when an infected document is opened (AutoOpen).

By removing the Tools/Macro option, Daniel tries to make recognition of an infected file more difficult (called macro stealth technique).

Daniel also redifines the File/Save menu item. Instead of the original action, it will run the MacroManager.

When a file is opened with a non standard extension (not .doc or .dot), Daniel will change the document summary info. Under the keyword "Daniel_Stone" the following comment can be found:

"   All information should be free   "

Date

Virus name:	Date.A (a.k.a. AntiDMV, Infezione)
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoOpen
Size of macros:	1042 Bytes
Place of origin:	USA
Date of origin:	1996
Destructive:	Yes
Seen In-The-Wild:	Yes
Description:	

Date infects the global template (normal.dot) once an infected document in opened. Further documents become infected when they are opened. Infection occurs only until June 1st, 1996. By the time you read this document, Date should not be a threat anymore even though infected documents might still be around.

Date is also known under the name AntiDMV. This name was chosen because it removes the "AutoClose" macro from documents. The macro virus "DMV", which has only one "AutoClose" macro, can therefore be removed with the Date virus.

Dietzel

Virus name: Dietzel.A
Number of macros: 5
Encrypted: Yes
Macro names: DATEISchliessen, EXTRASMakro, DATEIDokVorlagen, DATEISpeichernUnter, DATEIBeenden
Size of macros: 3987 Bytes
Place of origin: Germany
Date of origin: August 1996
Destructive: No
Seen In-The-Wild: No
Description:

Activation of Dietzel occurs when an infected document is closed (DATEISchliessen) or when Microsoft Word is exited (DATEIBeenden).

Dietzel tries to make recognition of an infected document more difficult by replacing the Tools/Macro option with a dialog box very similar to the original one (called macro stealth technique). It displays only the macros in the global template, except for the virus macros.

Dietzel's infection routine isvery similar to that of traditional companion viruses.
The original document remains untouched, instead for each saved document Dietzel creates a copy of the infected global template. This new file is stored in the same directory but with a .BAK extension. The saved document is then registered based on this new infected template. Whenever an infected document is closed the associated infected template will be loaded as a global template.

Divina

Virus name:	Divina.A (a.k.a. Roberta)
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoClose
Size of macros:	2357 Bytes
Place of origin:	Italy
Date of origin:	1996
Destructive:	No
Seen In-The-Wild:	Yes
Description:	

Divina infects the global template (normal.dot) when an infected document is opened and then closed. Further documents become infected when they are closed via the "AutoClose" command.

Devina has two payloads. The first payload checks the system time, and in case of a value of 17 in the minutes field, it will display a set of windows. Between each displayed box it will pause and beep.

"   ROBERTA TI AMO!   "

"   Virus 'ROBERTA' is running. Hard Disk damaged. Start antivirus?   "

"   Exit from system and low level format are recommended.   "

"   Exit from System?   "

After the last message Divina tries to exit Windows.

The second payload is activated on May 21st. Divina will again check the system clock, and if a document is being closed between the 10th and 20th or between the 40th and 50th minute, it will display another 2 windows.

"   DIVINA IS THE BEST!   "

Even though Devina does not contain any destructive payloads, a scared users might low level formating his hard drive.

DMV

Virus name:	DMV.A (a.k.a. Demonstration)
Number of macros:	1
Encrypted:	No
Macro names:	AutoClose
Size of macros:	3002 Bytes
Place of origin:	USA
Date of origin:	Fall 1994
Destructive:	No
Seen In-The-Wild:	No
Description:	

DMV was the first macro virus written by Joel McNamara, who published a detailed paper about macro viruses. It is believed that DMV invited additional virus authors to write Word macro viruses. While the paper was not published until Concept was discovered, it helped virus authors to use new techniques. Joel McNamara also published an Excel macro virus, which is non functional (Excel.DMV.A)

DMV infects the global template (normal.dot) when an infected document is closed. Further documents become infected when they are alse closed.

Upon infection, DMV displays the following messages:

" Counting global macros "

" AutoClose macro virus is already installed in NORMAL.DOT. "

" Infected NORMAL.DOT with a copy of AutoClose macro virus. "

" AutoClose macro virus already present in this document. "

" Saved current document as template. "

" Infected current document with copy of AutoClose macro virus. "

" Macro virus has been spread. Now execute some other code "
" (good, bad, or indifferent). "

Doggie

Virus name:	Doggie.A
Number of macros:	3
Encrypted:	No
Macro names:	AutoOpen, Doggie, FileSaveAs
Size of macros:	610 Bytes
Place of origin:	USA
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No

Doggie infects the global template (normal.dot) when an infected document is opened. Further documents become infected with the "FileSaveAs" command.

Doggie is one of very few non-destructive macro viruses. It only infects other files and displays the following message:

"   Doggie   "

Dub

Virus name:	Dub.A
Number of macros:	13
Encrypted:	Yes
Macro names:	AutoExec, NewDocInsert, ToolsMacro, FileTemplates FileSaveAs, FcDub, AeDub, Annhilator, Message SearchDestroyer, ExeKiller, KillIt (FileClose)
Size of macros:	22669 Bytes in Documents 25325 Bytes in global template
Place of origin:	Baku, Azerbaijan
Date of origin:	Spring 1997
Destructive:	Yes
Seen In-The-Wild:	No

Description:

When Dub becomes active, it searches the C:\ drive for documents (C:\*.DOC). It infects all documents that have the Word 6/7 format. After each infection, Dub writes a log file where it mentions all the killed documents (existing text is replaced with "666").

Dub.A uses "ToolsMacro" and "FileTemplates" to make recognition of an infected document more difficult (called macro stealth technique). We advise not to access the two menu items, because it will result in the execution of Dubs viral code.

Dub contains various payloads:

1. When an infected document is saved (FileSaveAs) at 4:00 o'clock, Dub displays the following message:

"   Do you believe in Satan?   "

2. When Microsoft Word is started (AutoExec) on the 13th of each month, Dub tries to delete the following files:

"   *.EXE   "

3. Upon infection, all existing text is replaced with " 666 ".

Dzt

Virus name: Dzt.A
Number of macros: 2
Encrypted: Yes
Macro names: AutoOpen (FileSave), FileSaveAs
Size of macros: 2033 Bytes
Place of origin: Indonesia
Date of origin: April 1996
Destructive: No
Seen In-The-Wild: Yes

Description:

Dzt.A activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved with the "FileSave" and "FileSaveAs" command.

When infecting a document, Dzt.A adds the following text to the Comments section of File| Properties:

"   DZT   "

Virus name: Dzt.B
Number of macros: 1
Encrypted: Yes
Macro names: AutoOpen (FileSave)
Size of macros: 1214 Bytes
Place of origin: Indonesia
Date of origin: April 1996
Destructive: No
Common In-The-Wild: Yes
Description:

Dzt.B activates when an infected document is opened (AutoOpen). Further documents become infected when they are saved with the "FileSave" command.

The main difference between this new variant and the original Dzt.A virus is that the "FileSaveAs" macro is missing.

Virus name: Dzt.C
Number of macros: 1
Encrypted: Yes
Macro names: FileSaveAs
Size of macros: 819 Bytes
Place of origin: Indonesia
Date of origin: April 1996
Destructive: No
Common In-The-Wild: Yes
Description:

The main difference between this new variant and the original Dzt.A virus is that the "AutoOpen" macro is missing.

Dzt.C was most likely created by an older version of a popular Anti-Virus product. The disinfection routine was faulty and forgot to remove the "AutoOpen" macro.

Virus name: Dzt.D
Number of macros: 2
Encrypted: Yes
Macro names: AutoOpen (FileSave), FileSaveAs
Size of macros: 2584 Bytes
Place of origin: Indonesia
Date of origin: April 1996
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and the original Dzt.A virus is that the comment in the File|Properties section was changed from "DZT" to "DZT'96".

The "FileSaveAs" macro is also partially corrupted.

For more information, please refer to the Dzt.A virus description.

E - Virus Names Starting With The Letter E

Easy
Epidemic

Easy

Virus name:	Easy.A (a.k.a. EasyMan)
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoOpen
Size of macros:	1090 Bytes
Place of origin:	Austria
Date of origin:	September 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Easy activates when an infected document is opened (AutoOpen). If the "AutoOpen" macro already exists in the global template, Easy will not infect.

The following text will be inserted at the top of an opened document at a random date and with a random color:

" It's Easy Man "

After that Easy displays the following text at the status bar:

" Word.EasyMan, written by Spooky "

Epidemic

Virus name:	Epidemic.A
Number of macros:	2
Encrypted:	Yes
Macro names:	AutoOpen, AutoExec
Size of macros:	38746 Bytes
Place of origin:	Taiwan
Date of origin:	January 1997
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

When an infected document is opened, Epidemic infects the global template (normal.dot). Further documents become infected when they are opened (AutoOpen) or Microsoft Word is started (AutoExec).

Epidemic has various destructive payloads:

1. On April 27th, Epidemic formats the hard disk (similar to FormatC).

2. On June 17th, it uses DEBUG.EXE to drop the Dos-based virus "Natas" into the C:\MOUSE.COM file. It also modifies C:\AUTOEXEC.BAT to call C:\MOUSE.COM upon next boot-up.

3. On October 10th, it deletes the following files:

" C:\IO.SYS "
" C:\MSDOS.SYS "
" C:\COMMAND.COM "

This action will leave the computer unbootable.

It then displays the following message:

" EPIDEMIC Macro Virus V1.1 "

Epidemic only works with the Chinese version of Microsoft Word.

F - Virus Names Starting With The Letter F

FormatC
Friendly
FutureNot

FormatC

Virus name:	Trojan.FormatC (a.k.a. TrojanFormat)
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen
Size of macros:	81 Bytes
Place of origin:	Posted to Usenet
Date of origin:	Unknown
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

FormatC is not a virus but a trojan horse, which does not replicate.

When an infected document is opened, the trojan triggers the destructive payload, which types " Format C: /U " in a minimized DOS box and then formats the C drive.

FormatC is very unlikely to spread since it does not infect other files.

Friendly

Virus name:	Friendly.A:De
Number of macros:	20
Encrypted:	No
Macro names:	Abbrechen, AutoExec, AutoOpen, Cancel, DateiBeenden, DateiNeu, DateiOeffnen, DateiSchliessen, DateiSpeichern, DateiSpeichernUnter, ExtrasMacro, ExtrasMakro, Fast, FileExit, FileNew, FileOpen, FileSave, FileSaveAs, Infizieren, Talk
Size of macros:	9867 Bytes
Place of origin:	Germany
Date of origin:	May 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Friendly was an effort to write a virus for more than one language, yet due to some wrong translations (ExtrasMacro instead of ToolsMacro) Friendly does not work with other versions than the German version of Microsoft Word.

Friendly tries to infect the global template (normal.dot) when an infected document is opened. It checks the global template for a previous infection by looking for the text "Friendly", Author = Nightmare". After the macros have been transfered the destructive payload is called from the "Fast" macro.

Friendly infects other documents whenever new ones are created, an action is canceled, and whenever documents are opened, closed, saved, or Exited from Word. Friendly does not check for a previous   document infection. It simply overwrites existing macros.

The destructive payload, inside the "Fast" macro, is called when the system clock has a second value smaller than 2. Friendly then creates a debug script inside the C:\DOS directory and executes the the DOS DEBUG.EXE command. In addition, Friendly adds an entry into AUTOEXEC.BAT, so the DOS based virus is started after the next boot-up. The DOS based virus inside Friendly has a size of 395 Bytes and is a memory resident companion virus encrypted with CryptCOM.

Friendly displays the following message on January 1st:

"   Ein gutes neues Jahr !   "

and infects EXE files upon execution. COM files are created with the same name and with the attributes "READ-ONLY" and "HIDDEN".

If the virus is active, the following text is displayed when people try to look at the macro list:

"You can't do that!"
"I'm very anxious!"
"Hello my friend!"
"<< Friends >> Virus"

(translated:)

"Du kannst das nicht tun!"
"Ich bin sehr aengstlich!"

"Hallo mein Freund!"
"<< Friends >> Virus"

After May 1st Friendly displays the following text when infecting documents for the first time (except for NORMAL.DOT).

"Hallo mein Freund!"
"Ich bin der << Friends >> Virus und wie heiát du?"
"Gib doch bitte anschlieáend unten deinen Namen ein:"
"Also ..... ich habe eine gute und eine schlechte Nachricht fuer dich!"
"Die schlechte Nachricht ist, daá ich mich auf deiner Platte eingenistet" "habe und die gute ist, daá ich aber ein freundlicher und auch nuetzlicher "Virus bin. Druecke bitte OK fuer Weiter!"

"Wenn du mich nicht killst, dann fuege ich ein Programm in deine" "Autoexec.bat ein, daá deine lame Tastatur etwas auf Touren bringt."
"Also ...., gib dir einen Ruck und kill mich nicht. Goodbye!"

(translated:)

"Hello my Friend!"
"I'm the << Friends >> Virus and how are you?"
"Can you give me your name, please?"
"Hello .... I have a good and a bad message for you! The bad message is that" "you have now a Virus on your Harddisk and the good message is that I'm "harmless and useful. Press OK!"

"If you don't kill me, I will insert a programme in your AutoExec.bat thats "your Keyboard accelerated. Please .... don't kill me. Goodbye!"

The entered name will then also be displayed.

FutureNot

Virus name:	FutureNot.A (a.k.a. Anti-IVX, Future)
Number of macros:	1 or 2 (in global template)
Encrypted:	No
Macro names:	AutoOpen (FileSaveAs)
Size of macros:	Polymorphic
Place of origin:	Unknown
Date of origin:	1997
Destructive:	No
Seen In-The-Wild:	No
Description:	

FutureNot is the first polymorphic macro virus.

When an infected document is opened, FutureNot infects the global template. It creates two macros in the global template. One is always "FileSaveAs" and the second one is a copy of "AutoOpen" with a randomly chosen name.

While the second macro remains the same, the FileSaveAs macro changes due to randomly selected comments.

FutureNot also modifies the C:\AUTOEXEC.BAT file. It adds the following comment to the end of the file:

"   @ATTRIB -R C:\MSOFFICE\WINWORD\TEMPLATE\NORMAL.DOT > NUL   "

This clears the Read-Only attribute from the global template.

G - Virus Names Starting With The Letter G

Gangsterz
Goldfish

Gangsterz

Virus name:	Gangsterz.A (a.k.a Big Daddy Cool)
Number of macros:	2
Encrypted:	Yes
Macro names:	Gangsterz, Paradise
Size of macros:	4250 Bytes
Place of origin:	Germany
Date of origin:	Unknown
Payload:	Yes
Seen In-The-Wild:	No
Description:	

Gangsterz uses a new triggering mechanism. Instead of using automatic macros (AutoOpen etc.) or redefining built-in Word commands, it uses assigned keys to start up its macros.

The "Gangsterz" macro is associated with pressing space and the "Paradise" macro with pressing 'e'. If a user presses any of the two keys while working on an infected document, the associated macros are activated.

If a document is infected on January 1st, a new document is created with the following text:

"   Big_Daddy_Cool virus generated by NJ   "

and then filled with scrolling O's.

If the value of the XOP setting in the [intl] section of win.ini is not set to "Installed", Gangsterz drops an intended batch file virus after activation.

Goldfish

Virus name:	Goldfish.A (a.k.a Fishfood)
Number of macros:	2
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose
Size of macros:	9867 Bytes
Place of origin:	USA
Date of origin:	July 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Goldfish infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are also opened ("AutoOpen"). Goldfish is one of very few non-destructive macro viruses. It only infects other files and displays the following message:

"   I am the goldfish, I am hungry, feed me.   "

The message will not go away until the user types in an acceptable response. Available answers are:

"fishfood"
"worms"
"worm"
"pryme"
"core"

H - Virus Names Starting With The Letter H

Hassle
Helper
Hiac
Hot
Hybrid

Hassle

Virus name: Hassle.a (a.k.a Bogus)
Number of macros: 7
Encrypted: Yes
Macro names: AutoClose, Toolsmacro, Microsoft01, Microsoft02, Microsoft03, Microsoft04, Microsoft05
Size of macros: 8283 Bytes
Place of origin: USA
Date of origin: August 1996
Destructive: No
Seen In-The-Wild: No
Description:

Hassle is another virus that uses the macro "ToolsMacro" to make recognition of an infected document more difficult. (called macro stealth technique).

If the user selects any command, it will show the following message and close Microsoft Word:

" Out of Memory or System Resources "

Hassle is one of very few non-destructive macro viruses. It only infects other files and displays the following text window

" Are you sure to Quit? "

This happens only very few times. The chances are only one in 20, (a probability of 5 percent). Another payload asks the user to register software with Microsoft. Hassle will only accept one answer, which is as followed:

"Bill Gates", "Microsoft" and "666"

Whenever the user selects the Tools/Macro command, Hassle will display the following text on the bottom of the screen:

" Microsoft Word Assistant Version 6.2 "

Helper

Virus name:	Helper.B
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoClose
Size of macros:	409 Bytes
Place of origin:	Unknown
Date of origin:	1997
Payload:	No
Seen In-The-Wild:	Yes

Description:

Helper.B infects the global template (normal.dot) when an infected document is closed. Further documents become infected when they are also closed.

The main difference between this new variant and the original Helper.A virus is that someone modified the payload routine. Due to a mistake, Helper.B does not save any documents with the "help" password.

Hiac

Virus name:	Hiac.A
Number of macros:	2
Encrypted:	Yes
Macro names:	AutoClose, HI (AC)
Size of macros:	576 Bytes
Place of origin:	Australia
Date of origin:	Spring 1997
Destructive:	No
Seen In-The-Wild:	Yes

Description:

Hiac.A is another "do nothing" virus that does nothing else besides infecting other files. Infection occurs when a user closes a document (AutoClose).

Its code is faulty and forgets to set the template bit of infected documents, therfore it is unlikely to spread its code to other files.

Hot

Virus name: Hot.A
Number of macros: 4
Encrypted: Yes
Macro names: AutoOpen, DrawBringInFrOut, InsertPBreak, ToolsRepaginat, FileSaveAs, StartOfDoc
Size of macros: 5515 Bytes
Place of origin: Unknown
Date of origin: January 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

When an infected document is opened the virus is activated by the AutoOpen macro. Some replicated Hot samples also display the following error message:

"   Unable to load the specified library   "

Hot turns off the prompting of Word to ensure a hidden infection of the global template (normal.dot). It also checks the file "WINWORD6.INI" for the following entry: "QLHot". If not present, Hot records a "hot date", 14 days in the future. Is this variable is not already set, the global template becomes infected.

The InsertPBreak/InsertPageBreak insert a page-break into the current document. However, it is also used by the virus to recognise if a document is already infected.

Some of the macros are renamed when they are copied by the WordBasic "MacroCopy" command:

"AutoOpen"	becomes	"StartOfDoc"
"DrawBringInFrOut"	becomes	"AutoOpen"
"InsertPBreak"	becomes	"InsertPageBreak"
"ToolsRepaginat"	becomes	"FileSave"

In addition the global template contains the following macros:

"FileSave" (similar to "ToolsRepaginat")
"StartOfDoc" (similar to "AutoOpen")

Hot also uses special functions from the Windows file "KERNEL.EXE" (Win API). It uses the API to find the path for Windows and to open files which are only very simple functions. It should be noted that many other options were available to the virus author.

The destructive payload, which is reached upon arrival of the hot date" set under the "QLHot" section in the WINWORD6.ini file, deletes text from the current active document. This payload is bypassed if the file EGA5.CPI is present in the "C:\DOS" directory.

A comment in the virus source code suggests that this is a "feature" designed to protect the virus author and his friends.

Hybrid

Virus name:	Hybrid.B
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose, FileSaveAs
Size of macros:	2815 Bytes
Place of origin:	Unknown
Date of origin:	February 1997
Destructive:	No
Seen In-The-Wild:	No
Description:	

Hybrid.B is a new variant based on the original Hybrid.A virus. The only difference between the two viruses is that the "AutoClose" macro, snatched from the Anti-Virus macro solution ScanProt, is corrupted. Due to the corruption Microsoft Word displays a WordBasic error message whenever a document is closed.

For more information, please refer to the Hybrid.A virus description.

I - Virus Names Starting With The Letter I

Imposter
Irish
Italian

Imposter

Virus name: Imposter.A
Number of macros: 2
Encrypted: No
Macro names: AutoClose, DMV (FileSaveAs)
Size of macros: 907 Bytes
Place of origin: England
Date of origin: March 1996
Destructive: No
Seen In-The-Wild: Yes
Description:

Imposter infected the global template (normal.dot) when an infected document is closed and the macros "DMV" and "FileSaveAs" are not already present. When Imposter.A copies the "DMV" macro, it renames it to "FileSaveAs" and displays the following message:

"   DMV   "

Further documents become infected when the "FileSaveAs" command is used.

The following text can be found inside Imposter.A, but is not displayed:

"   just to prove another point   "

This text is based on the Concept virus, which has "this is enough to prove my point" in its virus code.

Virus name: Imposter.B
Number of macros: 2
Encrypted: No
Macro names: AutoClose, DMV (FileSaveAs)
Size of macros: 907 Bytes
Place of origin: England
Date of origin: March 1996
Destructive: No
Seen In-The-Wild: No
Description:

The only difference between this new variant and the original Imposter virus is the spelling of a comment in the virus code.

Please refer to Imposter.A for more information.

Irish

Virus name: Irish.A
Number of macros: 4
Encrypted: No
Macro names: AutoOpen, WordHelp, AntiVirus, WordHelpNT
Size of macros: 4152 Bytes
Place of origin: USA
Date of origin: Spring 1996
Destructive: No
Seen In-The-Wild: No
Description:

Irish infects the global template (normal.dot) when an infected document is opened. Further documents become infected when the "FileSave" command is used.

Two of the macros, "WordHelp" and "WordHelpNT", do not run automatically. However, when executed manually by the user, they will change the Windows desktop color to green.

The macro "WordHelpNT" contains a payload which attempts to activate the screen saver and display the following message:

"   Happy Saint Patties Day   "

However the payload seems to be faulty and does not work under Windows 95 (Irish only exists Microsoft Word).

Italian

Virus name:	Italian.A
Number of macros:	3
Encrypted:	Yes
Macro names:	FileMacro, FileChiudi, FileEsci, FileSalva, WordMacro1, WordMacro2
Size of macros:	1438 Bytes
Place of origin:	Italy
Date of origin:	January 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Italian is the first functional virus written for the Italian version of Microsoft Word.

When an infected document is opened on the 7th, 13th, 17th or 31st of each month it displays the following message:

```
"    Your PC is infected by    "
"    Word.Macro.ITALIAN Virus    "
"    Written Jan,1996.    "
```

J - Virus Names Starting With The Letter J

Johnny

Johnny

Virus name:	Johnny.B
Number of macros:	5 (or 6)
Encrypted:	Yes
Macro names:	AutoOpen, Presentv, Presentw, Presentz, vGoJohnny
Size of macros:	3992 Bytes
Place of origin:	UK
Date of origin:	January 1997
Payload:	Yes
Seen In-The-Wild:	No
Description:	

The differences between this new variant and the original Johnny.A virus is that Johnny.B is now able to infect the French version of Microsoft Word.

The following 2 macros are changed:

"FichierEnregistre" instead of "FileSave" and "FichierEnregistreSous" instead of "FileSaveAs".

For more information, please refer to the Johnny.A virus description.

K - Virus Names Starting With The Letter K

Kerrang
KillDll
KillProt

Kerrang

Virus name:	Kerrang.A
Number of macros:	5
Encrypted:	Yes
Macro names:	AutoExec, FileOpen, FileSaveAs, FilePrintDefault, ToolsMacro
Size of macros:	972 Bytes
Place of origin:	Unknown
Date of origin:	February 1997
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Kerrang activates when an infected document is opened. After the global template becomes infected, it disables the Microsoft Word virus protection every time Microsoft Word is started (AutoExec).

Further documents become infected when they are saved with the FileSave and FileSaveAs command.

Kerrang uses "ToolsMacro" to make recognition of an infected file more difficult (called macro stealth technique). When the user selects this option, Kerrang creates 65 new documents.

Kerrang has various payloads. It checks for the system time and if the time is 18:00 (6:00 p.m.) is adds the following text to the printed document:

"   Kerbaffely Urgo Kerranga! Kerranga!!!!   "

After that it launches its second payload which deletes all files with the extension *.DOC in the current directory.

KillDll

Virus name:	KillDll.A
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen
Size of macros:	284 Bytes
Place of origin:	Unknown
Date of origin:	Summer 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

KillDLL activates when an infected document is opened (AutoOpen).

KillDLL is one of very few destructive viruses. Upon each startup of Word, it will delete all files in the WINDOWS directory, matching the extensions:

*.D??

Affected are mostly .DLL files and .DRV files, which are essential for Microsoft Windows.

KillProt

Virus name:	KillProt.A
Number of macros:	4
Encrypted:	Yes
Macro names:	AutoExec, FileOpen, FileSaveAs, ToolsMacro
Size of macros:	2272 Bytes
Place of origin:	Unknown
Date of origin:	1997
Payload:	Yes
Seen In-The-Wild:	No
Description:	

KillProt.A infects the global template when an infected document is opened (FileOpen) or the ToolsMacro command is selected. Further documents become infected when they are opened (FileOpen) or saved (FileSaveAs).

KillProt's name was chosen because KillProt deletes the following macros:

"AutoExit"
"InstVer"
"ShellOpen"

All of them are located in the Anti-Virus macro solution "ScanProt".

KillProt also modifies .INI settings in the Windows directory. It creates the entry "Count=xxx" under the "Infector" section. Whenever a document is saved with the FileSaveAs command, KillProt increases the value. The payload triggers whenever 10 documens have been saved. It then adds the following password to the saved document:

"   WhatTheHell   "

L - Virus Names Starting With The Letter L

Lunch

Lunch

Virus name:	Lunch.A
Number of macros:	3
Encrypted:	No
Macro names:	AutoOpen (FileSave), NEWAO, NEWFS
Size of macros:	1579 Bytes in .doc files, 1718 Bytes in global template
Place of origin:	Unknown
Date of origin:	Unknown
Destructive:	No
Seen In-The-Wild:	**Yes**
Description:	

Lunch infects the global template (normal.dot) when an infected document is opened. The "AutoOpen" macro is renamed to "FileSave" when Lunch infects the global template. As a result, further documents become infected when they are saved with the FileSave command.

When an infected document is saved at 12:01 pm, Lunch displays the following message:

"   !Whatya doin'here? Take a lunch break!   "

Virus name:	Lunch.B
Number of macros:	3
Encrypted:	No
Macro names:	AutoOpen (FileSave), NEWAO, NEWFS
Size of macros:	1375 Bytes in .doc files, 1463 Bytes in global template
Place of origin:	Unknown
Date of origin:	Unknown
Destructive:	No
Seen In-The-Wild:	**Yes**
Description:	

The difference between this new variant and the original Lunch.A virus is that Lunch.B does not check for the presence of the "FileOpen" or "AutoExit" macros. Instead it checks for the presence of the "FileSave" macro before infecting the global template (normal.dot).

For more information, please refer to the Lunch.A virus.

M - Virus Names Starting With The Letter M

Maddog
MDMA
Muck

Maddog

Virus name:	Maddog.A
Number of macros:	6
Encrypted:	No
Macro names:	AutoOpen, AutoClose, AutoExec, FileClose, AopnFinish, FcFinish
Size of macros:	4209 Bytes
Place of origin:	USA
Date of origin:	July 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

MadDog infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are closed with the "FileClose" command. Upon closing a document, MadDog saves various times to "Temp1" and then saves the active document.

Infected documents contain the text string "MadDog".

MDMA

Virus name:	MDMA.A (a.k.a. StickyKeys, MDMA_DMV)
Number of macros:	1
Encrypted:	No
Macro names:	AutoClose
Size of macros:	1635 Bytes
Place of origin:	USA
Date of origin:	July 1996
Destructive:	Yes
Seen In-The-Wild:	Yes
Description:	

MDMA is the first macro virus that will work on Windows, Windows 95, Macintosh and Windows NT. It can be a very destructive virus, and Word users are strongly advised to check their system with an up-to-date Anti-Virus program.

MDMA infects the global template (normal.dot) when an infected document is opened and then closed. Further documents become infected when they are closed ("AutoClose").

If an infected document is loaded on the first of each month, MDMA activates its destructive payload. Due to a bug in the code MDMA will always call the Windows 95 payload, even though there are other payloads for other operating systems. Below are all the payloads:

```
Windows:
--------
Kill "c:\shmk."; "deltree /y c:" is added to autoexec.bat
```

This will delete all the directories on the C:\ drive.

```
Windows NT:
-----------
Kill "*.*"; Kill "c:\shmk."
```

This will delete all the files on the C:\ drive

```
Macintosh:
----------
Kill MacID$("****")
```

This will delete all file on the harddrive.

```
Windows 95:
-----------
Kill "c" \shmk."; Kill "c:\windows\*.hlp";
Kill "c:\windows\system\*.cpl"
SetPrivateProfileString ("HKEY_CURRENT_USER\Control Panel\Accessibility\Stickykeys", "On",
"1", "") SetPrivateProfileString ("HKEY_LOCAL_MACHINE\Network\
Logon","ProcessLoginScript", "00","") SetPrivateProfileString ("HKEY_CURRENT_USER\Control
Panel\Accessibility\HighContrst", "On", "1", "")
```

This will delete important windows files.

MDMA will also display the following message:

```
"   You are infected with MDMA_DMV. Brought to you by MDMA     "
"             (Many Delinquent Modern Anarchists).     "
```

Muck

Virus name:	Muck.A
Number of macros:	6
Encrypted:	No
Macro names:	AutoExit, AutoOpen, AutoClose, AutoNew, FileSave, FileSaveAs
Size of macros:	5329 Bytes
Place of origin:	Africa
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	Yes

Description:

Muck infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are saved (FileSave, FileSaveAs).

With a chance of 1/5 (probability 20 percent), Muck displays the following message:

" MUCK "

Muck also has 3 Anti-Virus macros from an ineffective Anti-Virus package called ScanProt (produced by Microsoft). They are named:

" AutoClose, AutoExit and AutoNew "

Virus name:	Muck.B
Number of macros:	6
Encrypted:	No
Macro names:	AutoExit, AutoOpen, AutoClose, AutoNew, FileSave, FileSaveAs
Size of macros:	2718 Bytes
Place of origin:	Africa
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	No

Description:

Muck.B infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are saved (FileSave, FileSaveAs).

With a chance of 1/5 (probability 20 percent), Muck displays the following message:

" MUCK "

Muck also has 2 Anti-Virus macros from an ineffective Anti-Virus package called ScanProt (produced by Microsoft). They are named:

" AutoClose and AutoNew "

Virus name:	Muck.C
Number of macros:	6
Encrypted:	No

Macro names:	AutoExit, AutoOpen, AutoClose, AutoNew FileSave, FileSaveAs
Size of macros:	4327 Bytes
Place of origin:	Unknown
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	No

Description:

Muck.C infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are saved (FileSave, FileSaveAs).

With a chance of 1/5 (probability 20 percent), Muck displays the following message:

"   MUCK   "

The difference to previous Muck viruses is that this new variant has 2 macros ("AutoNew" and "AutoClose") which are already known as "AutoExit" in variant B.

Virus name:	Muck.D
Number of macros:	6
Encrypted:	No
Macro names:	AutoExit, AutoOpen, AutoClose, AutoNew FileSave, FileSaveAs
Size of macros:	1619 Bytes
Place of origin:	Unknown
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	No

Description:

Muck.D infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are saved (FileSave, FileSaveAs).

With a chance of 1/5 (probability 20 percent), Muck displays the following message:

"   MUCK   "

The difference to previous Muck viruses is that this new variant was successful to infect Microsoft Word 97 (Word 8).

N - Virus Names Starting With The Letter N

NF
Nop
NPad
Nuclear

NF

Virus name:	NF.A (a.k.a. Names)
Number of macros:	2
Encrypted:	Yes
Macro names:	AutoClose, NF
Size of macros:	286 Bytes
Place of origin:	USA
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

NF infects documents when are closed (AutoClose). Infected documents are converted internally to templates which is very common for macro viruses.

Upon infection, NF will display the following message on the bottom of the screen:

"   Traced!   "

Nop

Virus name:	Nop.A:De
Number of macros:	2
Encrypted:	No
Macro names:	AutoOpen, NOP (DateiSpeichern)
Size of macros:	246 Bytes
Place of origin:	Germany
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	Yes

NOP.A is very primitive virus and has only very few necessary commands to in order to replicate. The only special characteristic for the NOP virus is that it turns off the prompting of Word before saving the global template (NORMAL.DOT).

When an infected document is opened, NOP transfers itself to the global template and renames "NOP" into "DateiSpeichern". Additional documents become infected when they are saved.

Virus name:	Nop.B:De
Number of macros:	2
Encrypted:	No
Macro names:	AutoOpen, NOP (DateiSpeichern)
Size of macros:	250 Bytes
Place of origin:	Germany
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

The difference between the this new variant and NOP.A is that NOP.B does not turn off the prompting of Microsoft Word before saving the global template (normal.dot). It also enters the word "Testvirus" at the insertion point.

For more information, please refer to the NOP.A virus.

Virus name:	NOP.D
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen, NOP
Size of macros:	234 Bytes
Place of origin:	USA
Date of origin:	January 1997
Destructive:	No
Seen In-The-Wild:	No
Description:	

NOP.D is a new variant based on the original Nop.A virus. The only difference between the two viruses is that NOP.D is able to infect the English version of Microsoft Word, while NOP.A only works with the German version.

For more information, please refer to the NOP.A virus.

NPad

Virus name:	NPad.A (DOEUNPAD)
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoOpen
Size of macros:	1831 Bytes
Place of origin:	Bandung, Indonesia
Date of origin:	March 1996
Payload:	Yes
Seen In-The-Wild:	Yes
Description:	

NPad activates when an infected document is opened (AutoOpen).

NPad.A also modifies the "compatibility" section inside the WIN.INI file. It adds a counter under the name of "NPAD328" and each time the virus is activated, it adds 1 to its value. Upon reaching a value of 23 it resets the counter and displays the following message in the status bar:

"   DOEUNPAD94 v 2.21 (c) Maret 1996 Bandung, Indonesia   "

Nuclear

Virus name: Nuclear.A (a.k.a. Alert)
Number of macros: 9
Encrypted: Yes
Macro names: AutoExec, AutoOpen, DropSuriv, FileExit, FilePrint, FilePrintDefault, FileSaveAs, InsertPayload, Payload
Size of macros: 10556 Bytes
Place of origin: Australia
Date of origin: September 1995
Destructive: Yes
Seen In-The-Wild: Yes

Nuclear was the second macro virus found "In-the-Wild" (after Concept). It was distributed, over the Internet in a document with information about the Concept virus. It was also the first macro virus that uses Execute-Only (encrypted) macros to make analysis more difficult.

Nuclear is activated with the "AutoExec" and "AutoOpen" macro. Before it infects the global template (normal.dot), it checks for a previous infection. It does not infect if it finds the "AutoExec" macro. Documents become infected when they are saved with the "FileSaveAs" command.

After the virus macros have been transfered to the global template, Nuclear calls some destructive payloads. The first payload tries to drop the "Ph33r" virus. Between 17:00 and 17:59, Nuclear creates a text file including a script of the DOS/Windows-EXE virus "Ph33r". It then uses the DOS command "DEBUG.EXE" to convert the file into an executable file. It also creates the "EXEC_PH.BAT" batch file, and calls it via a Dos shell. This last infection routine is faulty, the DOS-window is closed immediately, and the "Ph33r" virus never infects the system.

The second payload, upon printing a document, Nuclear checks the system time and in case of a value bigger than 55 in the seconds field, it adds the following text to the end of the printed document:

"   And finally I would like to say: "

"   STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC   "

The third destructive payload is activated on April 5th, when Nuclear deletes the system files "C:\IO.SYS", "C:\MSDOS.SYS" and "C:\COMMAND.COM.

This leaves the computer unbootable.

Virus name: Nuclear.B
Number of macros: 7
Encrypted: Yes
Macro names: AutoExec, AutoOpen, FilePrint, FilePrintDefault, FileSaveAs, InsertPayload, Payload
Size of macros: 3458 Bytes
Place of origin: France
Date of origin: March 1996
Destructive: Yes
Seen In-The-Wild: Yes
Description:

The difference between this new variant and the Nuclear.A virus is that Nuclear.B does not try to drop the "PH33r" virus.

For more information, please refer to the Nuclear.A description.

O - Virus Names Starting With The Letter O

Oval
Outlaw

Oval

Virus name:	Oval.A
Number of macros:	1
Encrypted:	Yes
Macro names:	AutoOpen
Size of macros:	339 Bytes
Place of origin:	Texas, USA
Date of origin:	April 1997
Payload:	Yes
Seen In-The-Wild:	Yes

Description:

Oval.A infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

When Oval triggers, it changes the font size (probability of 10 percent) of the active document. It also shows the following message in the status bar:

"   Be sure to drink your Ovaltine   "

Outlaw

Virus name:	Outlaw.A
Number of macros:	3
Encrypted:	No
Macro names:	randomly selected
Size of macros:	21410 Bytes
Place of origin:	Germany
Date of origin:	September 1996
Payload:	Yes
Seen In-The-Wild:	No

Outlaw has 3 unencrypted macros with a size of 21410 Bytes.

Each macro name consists of 5 characters made of:

2 letters (A-X) corresponding to the hour field of the time and 4 randomly selected numbers.

Outlaw redefines build-in macro commands. One macro is associated with the letter " E " and another macro with the "spacebar". Since both keys are very common, the probability of an infection is very high. Outlaw is considered the first (semi) polymorphic virus, since it changes its macro names.

Outlaw modifies the "Int1" section of Win.ini (Windows directory). It puts the three random macro names under Name=, Name1= and Name2=. This modification is used for recognition of an already infected global template. Outlaw does not infect the global template if the macro names, mentioned in Win.ini (Name=xxxxxx), already exist.

It also modifies the following 3 document variables:

VirName
VirNameDoc
VirNamePayload

Outlaw.A does not infect a document if the value of the VirNameDoc variable already exists in a document.

Upon infection of a document on January 20th, Outlaw launches its payload (works only under Windows 95). It plays a laughing sound on the PC speaker and creates a new document with the following text:

" You are infected with "

" Outlaw "

" A virus from Nightmare Joker. "

Virus name:	Outlaw.B
Number of macros:	3
Encrypted:	Yes
Macro names:	randomly selected
Size of macros:	21434 Bytes
Place of origin:	Germany
Date of origin:	September 1996
Payload:	Yes

Seen In-The-Wild: No
Description:

The difference between this new variant and the original Outlaw.A virus is that Outlaw.B has three encrypted macros while the macros in Outlaw.A are unencrypted.

For more information, please refer to the Outlaw.A description.

P - Virus Names Starting With The Letter P

Paper
Paycheck
Phantom
Phardera
Polite

Paper

Virus name:	Paper.A
Number of macros:	5
Encrypted:	No
Macro names:	mswFS, FileClose, AutoOpen, ToolsMacro, AutoExec, FieSave, mswFC, mswAO
Size of macros:	3608 Bytes
Place of origin:	Unknown
Date of origin:	Unknown
Destructive:	No
Seen In-The-Wild:	No
Description:	

When Paper infects a document, or the global template, it copies all its virus macros and then renames them. If the "AutoOpen" and "FileClose" macros already existed in the global template, they are deleted. In a similar fashion, the "FileSave" macro is deleted from documents.

Paper replaces the Tools/Macro option with a dummy macro in order to make recognition of an infected file more difficult (called macro stealth technique). If a user selects the Tools/Macro option nothing happens.

Paycheck

Virus name:	PayCheck.A
Number of macros:	7
Encrypted:	Yes
Macro names:	AutoExec, AutoOpen, FileOpen, FileSave FileSaveAs, ShellOpen, ToolsMacro
Size of macros:	8489 Bytes
Place of origin:	Unknown
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	Yes

Description:

Paycheck infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are saved.

It uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique).

It also checks the system time and in case of a 25,26,27,28,29,30, or 31 in the day field, it displays the following message:

" Sekarang adalah tanghal 25, sudahkah anda mengabil gaji? "
" He..he..selamat. Kalau bisa, lebih keras lagi kerjany a. "
" Bravo Bukit Asam!!! "

When a user saves a document between the 20th and the 31st of each month, Paycheck displays another message:

" Internal error was occurred in module UNIDRV.DLL. "
" Your application may not be work normally. "
" Please contact Microsoft Product Support. "

Phantom

Virus name:	Phantom.A (a.k.a Teaside, Guess, HiSexy)
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen
Size of macros:	1126 Bytes
Place of origin:	Germany
Date of origin:	May 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

When an infected document is opened, Guess checks if the document variables are set to "populated". If this is not the case, a new global template (normal.dot) is created and the virus macro "AutoOpen" is copied into the new document. After that the variable is set to "populated" in order to mark the file as infected. If the variable
is already set, the virus infects the new document by transfering the "AutoOpen" macro using the MakroCopy command. Guess is the first macro virus to use the document variables as a checking mechanism for already infected documents.

Because of an error inside the virus code, the virus does not replicate properly.

Upon a random number (between 0 and 100), Guess activates various destructive payloads. It changes the active font size or creates a new document including the following text:

"   The word is out.   "
"   The word is spreading...   "
"   The Phantom speaks...   "
"   Sedbergh   "
"   is CRAP   "
"   The word spreads...   "

The text will then be printed out.

The following texts will be inserted into the active document upon a calculated random number:

"   This school is really good.   NOT   "
"   We all love Mr. Hirst.   "
"   M.R.Beard   "
"   This network is REALLY fast.   "
"   Hi Sexy!   "
"   Who's been typing on my computer?   "
"   Well helloooo there!   "
"   Guess who?   "

Phardera

Virus name:	Phardera.A (a.k.a. Phandera)
Number of macros:	1
Encrypted:	Yes
Macro names:	FileOpen
Size of macros:	1673 Bytes
Place of origin:	Batavia, Indonesia
Date of origin:	July 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Phardera activates when an infected document is opened (FileOpen).

Phardera will not infect the global template or documents if one of the following macro is already present:

"FileOpen"
"ToolsCustomizeMenus"
"ToolsOptionsSave"
"ToolsOptionsGeneral"

Phardera tries to hides its presence by removing Tools/Macro, Tools/Customize and File/Templates from the options menu (called macro stealth technique). This part of the virus works only with the English version of Microsoft Word.

Upon infection of a document on the 13th of each month, Phardera displays the following message:

"   Dianita DSR. [I Love Her!]   "

A second message is displayed when a document is infected on the 31st of each month.

"   Phardera was here!   "

Polite

Virus name:	Polite.A (a.k.a. WW2Demo)
Number of macros:	2
Encrypted:	No
Macro names:	FileClose, FileSaveAs
Size of macros:	1918 Bytes
Place of origin:	USA
Date of origin:	March 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Polite was first created with Microsoft version 2.0, yet also works with higher versions of Microsoft Word.

Polite can be called a demonstration virus and is very unlikely to spread. Before each attempted infection, it displays a window with the following question:

" Shall I infect the file ? "

If the user answers with the "No" button, no document becomes infected. While it asks for permission to infect files, it does not ask for permission to infect the global template (NORMAL.DOT).

Upon infection of the global template (when an infected document
is closed), Polite displays the following message:

" I am alive! "

Once Polite infects a Word 6.0/7.0 document it can not infect Word 2.0 documents anymore.

R - Virus Names Starting With The Letter R

Rapi
Reflex

Rapi

Virus name: Rapi.A
Number of macros: 7 or 11 (global template)
Encrypted: No
Macro names: RpAe, RpFO, RpFS, RpTC, RpTM, RpFSA, AutoOpen
Size of macros: 6172 Bytes or 11228 Bytes
Place of origin: Indonesia
Date of origin: December 1996
Destructive: No
Seen In-The-Wild: Yes
Description:

Rapi infects the global template when an infected document is opened (AutoOpen). Further documents become infected when they are opened (FileOpen) or saved (FileSave and FileSaveAs).

Upon infection, Rapi displays the following message:

"   Thank's for joining us !   "

The "AutoExec" macro contains a destructive payload to delete files, yet due to some REM's it never triggers. However, Rapi.A drops a file (C:\BACALAH.TXT) to the root directory.

The file contains the following Indonesian text: (translated into English)

" Assalamualaikum..., sorry @Rapi.Kom disturbs you. This message "
" was originally called PESAN.TXT. It appears in the root directory "
" after running Word 6.0 and the global template (normal.dot) is "
" already infected by this macro. This macro virus (before the change " " by Rapi@Kom) cam from a Word 6.0 file (*.doc) which was already "
" infected by this virus. When the file is opened (Open doc), the "
" macro automatically executes the instructions i.e. "
" copies itself to the global template (normal.dot). On a certain "
" date and time the macro will delete all files in the directory "
" levels 1, 2, and 3 (except for hidden directories........ "
" Malang (date and time of infection) @Rapi.Kom "

Rapi uses "ToolsMacro" and "ToolsCustomize" to make recognition of an infected file more difficult (called macro stealth technique). If a user selects one of the two options, Word displays a WordBasic error message.

Rapi.A devolves into Rapi.A1 and Rapi.A2, which contain 6 or 3 macros (5607 Bytes or 3626 Bytes).

Virus name: Rapi.AA2
Number of macros: 3 or 5 (global template)
Encrypted: No
Macro names: RpAe, RpFS, AutoOpen
Size of macros: 4626 Bytes or 8571 Bytes (global template)
Place of origin: Unknown
Date of origin: Spring 1997
Destructive: No

Seen In-The-Wild: Yes

Description:

Rapi.AA2 infects the global template when an infected document is opened (AutoOpen). Further documents become infected when they are saved (FileSave).
Rapi.AA was discovered in its last devolved form, therefore the name Rapi.AA2.

The main difference to previous Rapi viruses is that the "RpAe" macro is corrupted. Microsoft Word does not care about corrupted macros, therefore Rapi.AA2 is still able to infect further documents.

Reflex

Virus name:	Reflex.A (a.k.a RedDwarf)
Number of macros:	3 or 4
Encrypted:	Yes
Macro names:	AutoOpen, FClose, FileClose, FA
Size of macros:	897 Bytes in .doc files, 1226 Bytes in global template
Place of origin:	Ireland
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

An infected global template contains one more macro ("FA"). Upon infection, Reflex turns off the prompting of Word to ensure a hidden infection of the global template (normal.dot). Infected documents are saved with the password "Guardian".

Reflex was written at an anti-virus conference after an Anti-Virus company announced a challenge to hackers to break its new technology. Any author of a new undetected macro virus was supposed to receive champagne as a reward.

When Reflex infects a file it displays the following window:

"   Now, Where's that Jerbil of Bubbly?   "

S - Virus Names Starting With The Letter S

Satanic
Saver
ShareFun
ShowOff
Spooky
Surabaya
Stryx

Satanic

Virus name:	Satanic.A
Number of macros:	5
Encrypted:	Yes
Macro names:	AutoOpen, AutoClose, AutoExec, AutoExit, AutoNew
Size of macros:	53249 Bytes
Place of origin:	Germany
Date of origin:	Summer 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Satanic activates when an infected document is opened (AutoOpen).   Satanic does not infect when the "AutoExit" macro already exists in the global template or a document. Further documents become infected when they are created (AutoNew), closed (AutoClose) or Microsoft Word exited (AutoExit).

Satanic deletes the Tool/Customize, Tool/Macro and Tools/Option menu items to make recognition of an infected document more difficult. (called macro stealth techinique).

Satanic also inserts "Installed=Yes" into the "Control" section of win.ini. If it does not find the entry (first activation or deleted) then it tries to drop and launch a DOS based virus (NC.COM).

Upon exiting Microsoft Word (AutoExit) on October 1st, Satanic will format drive C:\ unconditionally, resulting in the loss of valuable information.

A second payload will activate on September 30th. Satanic will then display the following message:

"   You are infected with Satanic   "

Saver

Virus name:	Saver.A (a.k.a. SaverSex)
Number of macros:	1
Encrypted:	Yes
Macro names:	DateiSpeichern
Size of macros:	602 Bytes
Place of origin:	Austria
Date of origin:	September 1996
Destructive:	No
Seen In-The-Wild:	No
Description:	

Saver activates when an infected document is saved (DateiSpeichern).
It does not infect when the "DateiSpeichern" macro already exists in the global template.
The same is true for documents.

Upon activation of the virus on April 21st the following message will be displayed:

"   Saver(SEX) written by Spooky. Austria 1996   "

ShareFun

Virus name:	ShareFun.A
Number of macros:	9
Encrypted:	No
Macro names:	AutoExec, AutoOpen, FileExit, FileOpen, FileSave FileClose, ToolsMacro, FileTemplates, ShareTheFun
Size of macros:	1777
Place of origin:	USA
Date of origin:	1997
Payload:	Yes
Seen In-The-Wild:	Yes
Description:	

ShareFun infects the global template when an infected document is opened (AutoOpen). Further documents become infected when they are opened (FileOpen), saved (FileSave), closed (FileClose) or on activation of FileExit, ToolsMacro and FileTemplates.

When an infected document is opened, the "ShareTheFun" macro is called (probability of 25 percent) and the document is saved to the root direcorty with the following name:

"Doc1.doc"

After that ShareFun looks for an active copy of MSMail. There are two different outcomes:

1. MSMail is inactive

Result: Sharefun shuts down Windows.

2. MSMail is active

Result: Sharefun tries to take control of MSMail and mails 3 e-mail messages to 3 randomly picked names from the address book. Attached to the e-mail message, with the header "You have GOT to read this!", is the infected document.

By doing this ShareFun tries to spread itself to new users.

The payload from ShareFun, described above, does not always work.

ShareFun also uses "ToolsMacro" and "FileTemplates" to make recognition of an infected document more difficult (called macro stealth technique).

Even though ShareFun was hyped by the marketing department of one Anti-Virus company, it is very unlikely that you will become infected with this virus. It remains to be a research virus.

ShowOff

Virus name:	Showoff.A (Showofxx)
Number of macros:	3
Encrypted:	Yes
Macro names:	AutoOpen, Show, Cfxx, Ofxx, AutoClose, AutoExec
Size of macros:	6789 Bytes
Place of origin:	Unknown
Date of origin:	Unknown
Payload:	No
Seen In-The-Wild:	No
Description:	

Showoff.A is most likely a corrupted "mutation" of another variant. The "Show" macro ("AutoExec" macro after infecting the global template) contains invalid Wordbasic instructions.

As a result, Showoff displays an error message whenever Word attempts to execute the "Show" macro. The following message will be displayed to the user:

"   Out of memory   "

Microsoft Word does not bother with garbage code, it just copies the code to further documents.

Spooky

Virus name:	Spooky.A
Number of macros:	9
Encrypted:	Yes
Macro names:	autoexec, AutoOpen, dateidokvorlagen, dateidrucken, dateidruckenstandard, extrasmakro, DateiSpeichernUnter, DateiOeffnen, Spooky
Size of macros:	3114 Bytes
Place of origin:	Austria
Date of origin:	September 1996
Payload:	Yes
Seen In-The-Wild:	No
Description:	

Spooky activates when an infected document is opened (AutoOpen).
Further documents become infected when they are opened (DateiOeffnen)
or saved (DateiSpeichernUnter). Spooky does not infect when the "Spooky" macro already exists in the global template (normal.dot) or a document.

It also disables the File/Templates and Tools/Macro menu items in order to make recognition of an infected file more difficult (called macro stealth technique).

If a user tries to select one of the two options he is prompted for a password. Upon entering "ykoops" at the prompt in the status bar, the original menus reappear.
Any other password creates the following message:

"   Sie haben das falsche Passwort eingegeben   "

translated:

"   You have entered the wrong password   "

Spooky randomly displays the following message in the status bar:

"   Word.Spooky   "

If the time value is between 55 and 59 and the user prints a document, Spooky inserts the the following text to the end of the printout:

"   Word.Spooky   "

Surabaya

Virus name:	Surabaya.A
Number of macros:	6
Encrypted:	No
Macro names:	AutoExec, AutoOpen, ToolsMacro, Plong FileTemplates, FileSaveAs
Size of macros:	1619 Bytes
Place of origin:	Surabaya
Date of origin:	Spring 1997
Payload:	Yes
Seen In-The-Wild:	Yes

Description:

Surabaya infects the global template when an infected document is opened. Further documents become infected when they are saved (FileSaveAs).

Surabaya uses "ToolsMacro" and "FileTemplates" to make recognition of an infected document more difficult (called macro stealth technique).

When a user selects one of the two options, Surabaya displays the following message:

" Sorry... "

Surabaya also adds the following section to WIN.INI:

" Author] "
" Name=TeBeYe`93 The ICE-Man "

When Microsoft Word is started from an already infected global template, Surabaya displays the following message in the status bar:

" Lontong Micro Device (c) 1993 By ICE-Man "

Stryx

Virus name: Stryx.A
Number of macros: 4
Encrypted: Yes
Macro names: DateiSchliessen, DokumentSchliessen, Stryx1, Stryx2, StryxOne, StryxTwo
Size of macros: 25669 Bytes
Place of origin: Germany
Date of origin: September 1996
Payload: Yes
Seen In-The-Wild: No
Description:

While Stryx has 4 macros, some of them are only available in the global template or in documents.

"Stryx1" (only in global template)
"Stryx2" (only in global template)
"StryxOne" (only in documents)
"StryxTwo" (only in documents)

Activation of Stryx occurs when a document is closed (DateiSchliessen and DokumentSchliessen). Stryx then modifies the "Int1" section of win.ini (Windows directory). It sets a YES to the value of the installed init string and creates a .GIF picture of a dragon (based on a hex dump). Upon closing a document on December 1st, a new document is created and the picture of the dragon is inserted. Followed by the dragon is:

"   STRYX!!!!   "
"   Look at your HD! :-)   "
"   Sorry, but it's so funny!   "
"   NJ 1996   "

Stryx does not infect when the "Stryx2" macro already exists in the global template or when the "StryxTwo" macro already exists in a document.

T - Virus Names Starting With The Letter T

Target
Tedious
Tele
Temple
Twister
TwoLines

Target

Virus name:	Target.B (a.k.a LoneRaider)
Number of macros:	1 (German version of Word), 2 (Any other version of Word)
Encrypted:	Yes
Macro names:	LoneRaider (LoneRaiderTwo)
Size of macros:	3463 Bytes
Place of origin:	Germany
Date of origin:	Unknown
Destructive:	No
Seen In-The-Wild:	No

Target activates when the assigned key (SPACE) is pressed. Target is an attempt to fool heuristic macro virus scanners. Its virus macros do not contain the command to copy viruses. Instead it creates a second macro (LoneRaiderTwo) and copies all the commands for activation and infection into it. After execution the second macro is deleted.
As a result, some heuristic scanners do not flag Target as suspicious. When Target is activated from a non-German version of Microsoft Word it will not spread and the second macro will not be deleted.

Upon pressing "SPACE" on January 1st of each year, Target creates a new document with the following text in it:

"   Enjoy the first F/WIN Killer!   "
"   LoneRaider!   "
"   Nightmare Joker   "
"   1996   "

When Target was released to the public, F-WIN Heuristic Anti-Virus, written by Stefan Kurtzhals, was unable to detect Target due to the reasons above. This was changed immediately and every up-to-date Anti-Virus program should be able to catch this virus.

Tedious

Virus name:	Tedious.A
Number of macros:	4
Encrypted:	Yes
Macro names:	AutoNew, FileSaveAs, VAutoNew, VFileSaveAs
Size of macros:	1082 Bytes
Place of origin:	Unknown
Date of origin:	August 1996
Payload:	No
Seen In-The-Wild:	No
Description:	

Tedious infects documents when the "FileSaveAs" command is used. Infected documents are converted internally to templates which is very common for macro viruses. Since Tedious uses English macro names it will not work with Non-English versions of Microsoft Word.

Even though one major US Anti-Virus company reported Tedious as being destructive, users do not have to fear this virus. Tedious is harmless and does nothing else besides replicating.

Tele

Virus name:	Tele.A (a.k.a LBYNJ, Telefonica, Tele-Sex)
Number of macros:	7
Encrypted:	Yes
Macro names:	AutoExec, AutoOpen, DateiBeenden, DateiDrucken, DateiNeu, DateiOeffnen, Telefonica
Size of macros:	22256 Bytes
Place of origin:	Germany
Date of origin:	April 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Tele's "AutoExec" macro includes the infection routine for the global template (normal.dot), which will not get infected when inside the WIN.INI file (entry "Compatibility"), the string "0x0030303" is set to "LBYNJ".

Tele uses the "Telefonica" macro to check for a previous infection. It will not infect the global template if the macro is already present.

Documents are infected upon "DateiBeenden" ("FileClose"), "DateiNeu" ("FileNew") and "DateiOeffnen" ("FileOpen"), whereby at the end of "DateiOeffnen" ("FileOpen") the macro "Telefonica" is called again. Infected documents are changed to templates, which is very common for macro viruses.

Tele has two destructive payloads. The first one can be found in the "DateiDrucken" (FilePrint) macro. Upon printing a documtent, Tele checks the system time and in case of a value less than 10 in the seconds field, it will add the following text to the end of the printed document:

"   Lucifer by Nightmare Joker (1996)   "

The second payload is activated from the "Telefonica" macro when the second field has a value of 0 or 1. ("Telefonica" is called from "AutoOpen", "AutoExec" and "DateiOeffnen"). Is this the case, Tele creates a Debug script, (filename: TELEFONI.SCR), inside the "C:\DOS" directory which includes the DOS based virus "Kampana.3784".

After creating the script file, LBYNJ executes the "TELEFONI.BAT" batch file which uses the DOS command "DEBUG.EXE" to convert the script file into an executable DOS-based virus and then starts it.

Temple

Virus name:	Temple.A
Number of macros:	4
Encrypted:	No
Macro names:	AutoOpen (TempAutoOpen), TempAutoExec (AutoExec) TempFileOpen (FileOpen), TempFileSave (FileSave)
Size of macros:	1011 Bytes
Place of origin:	Unknown
Date of origin:	Spring 1997
Destructive:	No
Seen In-The-Wild:	No

Description:

Temple is another do-nothing macro virus. It is only infectious.

Temple.A infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are also opened (AutoOpen) or saved (FileSaveAs).

Twister

Virus name: Twister.A
Number of macros: 8
Encrypted: No
Macro names: FileSaveAs, AutoExec, twAC, FileSave, AutoExit, twFC, twFE, twFQ, twFSA, twAE, AutoClose, twFS, twEX, FileClose, FileExit, FileQuit
Size of macros: 4628 Bytes
Place of origin: Unknown
Date of origin: Unknown
Payload: No
Seen In-The-Wild: No
Description:

Twister is a very simple virus that does nothing but replicate. It has 2 set of macros: one for infecting the global template and one for infecting documents. It swaps them at activation and at infection.

The AutoExec macro contains the following text string:

"   Twister 2000" v.1 (c) Neo-Luddite Inc.   "
"   For Robin Hood   "

TwoLines

Virus name: TwoLines.A
Number of macros: 5 and 4 for A1
Encrypted: Yes
Macro names: MSRun, AutoExec, AutoOpen, AutoClose, FileSaveAs
Size of macros: 1817 Bytes or 1767 Bytes
Place of origin: Unknown
Date of origin: February 1997
Destructive: No
Seen In-The-Wild: No
Description:

TwoLines infects the global template when an infected document is opened (AutoOpen) or closed (AutoClose). As the name suggests it adds 2 empty lines to the active document when the minute field of the system time shows 20 minutes. Responsible for this action is the "MsRun" macro.

The "FileSaveAs" macro converts documents to templates, yet does not infect them.

Twolines.A devoles into Twolines.A1, which does not contain the "FileSaveAs" macro.
For this to happen certain conditions have to be present:

1. Automacros are disabled when opening an infected document.
2. Document is closed (AutoClose).
3. Global template contains macros.

W - Virus Names Starting With The Letter W

Wazzu
Wieder

Wazzu

Virus name:	Wazzu.A
Number of macros:	1
Encrypted:	No
Macro names:	AutoOpen
Size of macros:	632 Bytes
Place of origin:	Washington, USA
Date of origin:	Posted to Usenet in April 1996
Destructive:	Yes
Seen In-The-Wild:	Yes
Description:	

When an infected document is opened, Wazzu.A checks the name of the active document. If it is "normal.dot", then the virus macro is copied from the global template to the open document. Otherwise normal.dot becomes infected.

Wazzu does not check if a document is already infected. It simply overwrites the "autoopen" macro.

Wazzu has a destructive payload. It picks a random number between 0 and 1 and if the number smaller than 0.2 (probability of 20 percent), the virus will move a word from one place in the document to another. This is repeated three times. So the probability for a Word to be moved is 48.8 percent. After the third time, Wazzu picks a final random number (between 0 and 1) and if the value is higher than 0.25 (probability of 25 percent), the word "Wazzu" will be inserted into the document.

After an infected documents is cleaned, it has to be checked really careful because chances of having a modified document (words swapped or added) are over 61 percent. This can be a very time consuming job with large documents.

Wazzu is a nickname for the Washington State University.

Virus name:	Wazzu.C
Number of macros:	1
Encrypted:	No
Macro names:	autoOpen
Size of macros:	433 Bytes
Place of origin:	Unknown
Date of origin:	Summer 1996
Destructive:	No
Seen In-The-Wild:	Yes
Description:	

The difference between this new variant and the original Wazzu.A virusand is that Wazzu.C does not have any destructive payload. It is only infectious.

Virus name:	Wazzu.D
Number of macros:	1
Encrypted:	No
Macro names:	autoOpen
Size of macros:	331 Bytes
Place of origin:	Unknown
Date of origin:	Summer 1996
Destructive:	No

Seen In-The-Wild: No
Description:

The difference between this new variant and Wazzu.C is that some unused code is missing in Wazzu.D. The difference to the original Wazzu is that it does not contain any destructive payload, such as changing documents. Wazzu.D is only infectious.

Virus name: Wazzu.E
Number of macros: 1
Encrypted: No
Macro names: autoOpen
Size of macros: 318 Bytes
Place of origin: Unknown
Date of origin: September 1996
Destructive: No
Seen In-The-Wild: Yes
Description:

The difference between this new variant and Wazzu.D is that some unused code is missing in Wazzu.E. The difference to the original Wazzu is that it does not contain any destructive payload, such as changing documents. Wazzu.E is only infectious.

Virus name: Wazzu.F
Number of macros: 1
Encrypted: Yes
Macro names: autoOpen
Size of macros: 450 Bytes
Place of origin: Unknown
Date of origin: September 1996
Destructive: No
Seen In-The-Wild: Yes
Description:

Wazzu.F is a minor variant of Wazzu.C with two changes. Wazzu.F displays a message with a 1:10 chance and its code is encrypted. The difference to the original Wazzu is that Wazzu.F does not contain any destructive payload, such as changing documents. Wazzu.F is only infectious.

The following message is displayed with a 1:10 chance:

"   This one's for you, Bosco.   "

Virus name: Wazzu.AA
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 1624 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The difference between this new variant and the original Wazzu.A virus is that Wazzu.AA does not add the word "wazzu" to newly opened documents.

Wazzu.AA infects the global template (normal.dot) when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AB
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 323 Bytes
Place of origin: Australia
Date of origin: February 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AB is another "do-nothing" macro virus with no payload and some modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AC
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 433 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AC is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AD
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 332 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AD is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AE
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 618 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AE has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. There is a 3/5 chance that one word is moved to another position in the active document.

Virus name: Wazzu.AF
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 1484 Bytes
Place of origin: USA
Date of origin: December 1996
Destructive: No
Common In-The-Wild: No
Description:

Concept.AF is a new variant based on the older Wazzu.D virus. The only difference between the two viruses is that the first blank line has been deleted.

For more information, please refer to the Wazzu.D virus description.

Virus name: Wazzu.AG
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 332 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AG is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AH
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 557 Bytes
Place of origin: USA
Date of origin: February 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AH has some code modifications.

Its payload inserts the word "YaHoo" instead of "wazzu". The second payload, which moves words from one position to another, is similar to Wazzu.A.

Wazzu.AH infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AI
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 794 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AI is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AJ
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 430 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AJ is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AK
Number of macros: 1
Encrypted: No
Macro names: autoOpen
Size of macros: 344 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AK is another "do-nothing" macro virus with code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AL
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 643 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AL has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. For additional information, please refer to the Wazzu.A virus description.

Virus name: Wazzu.AM
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 606 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AM has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. There is a 3/5 chance that one word is moved to another position in the   active document.

Virus name: Wazzu.AN
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 375 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AN is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

It also contains the following comment in its code:

"   REM This macro wipes out the Wazzu Virus!   "

Virus name: Wazzu.AO
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 626 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AO has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. For additional information, please refer to the Wazzu.A virus description.

Virus name: Wazzu.AP
Number of macros: 1
Encrypted: No
Macro names: autoOpen

Size of macros: 432 Bytes
Place of origin: USA
Date of origin: February 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AP is another "do-nothing" macro virus with some code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AQ
Number of macros: 1
Encrypted: No
Macro names: autoOpen
Size of macros: 437 Bytes
Place of origin: USA
Date of origin: February 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AQ is another "do-nothing" macro virus with a corrupted payload and some missing commands.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AR
Number of macros: 1
Encrypted: No
Macro names: autoOpen
Size of macros: 563 Bytes
Place of origin: Germany
Date of origin: February 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AR has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. For more information, please refer to the Wazzu.A virus description.

Virus name: Wazzu.AS
Number of macros: 1
Encrypted: No

Macro names: AutoOpen
Size of macros: 352 Bytes
Place of origin: Unknown
Date of origin: 1996
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and Wazzu.L is that Wazzu.AS has some modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

When a user opens a document, Wazzu.AS adds the following text to the end of the document:

"   ladderwork!   "

Virus name: Wazzu.AT
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 576 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AT has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. There is a 3/5 chance that one word is moved to another position in the active document.

Virus name: Wazzu.AU
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 630 Bytes
Place of origin: Unknown
Date of origin: 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AU has a slightly modified code.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

The payload is similar to the original Wazzu virus. For additional information, please refer to the Wazzu.A virus description.

Virus name: Wazzu.AV
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 321 Bytes
Place of origin: Unknown
Date of origin: Spring 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AV is another "do-nothing" macro virus with small code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AW
Number of macros: 1
Encrypted: Yes
Macro names: AutoOpen
Size of macros: 1135 Bytes
Place of origin: USA
Date of origin: February 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AW is a combination of the Wazzu virus and the ShareFun virus. It contains payloads from both viruses.

Wazzu.AW moves words from one place to another, it enters the word "wazzu" to the active document, and tries to mail an infected document (C:\doc1.doc) to 3 randomly chosen addresses from the MS Mail addres book.

For further details, please refer to the Wazzu.A and Sharefun.A virus description.

Virus name: Wazzu.AX
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 343 Bytes
Place of origin: USA
Date of origin: Spring 1997
Destructive: No
Common In-The-Wild: No

Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AX is another "do-nothing" macro virus with small code modifications and no payload.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AY
Number of macros: 1
Encrypted: No
Macro names: AutoOpen
Size of macros: 632 Bytes
Place of origin: Unknown
Date of origin: February 1997
Destructive: No
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AY is another "do-nothing" macro virus with a corrupted payload and a 2 byte code modification.

It infects the global template when an infected document is opened. Further documents become infected when they are also opened (AutoOpen).

Virus name: Wazzu.AZ
Number of macros: 1
Encrypted: No
Macro names: AutoClose
Size of macros: 659 Bytes
Place of origin: USA
Date of origin: February 1997
Destructive: Yes
Common In-The-Wild: No
Description:

The main difference between this new variant and previous Wazzu viruses is that Wazzu.AZ has some code modifications.

Its payload inserts the word "uzzaw" (wazzu backwards).

Wazzu.AZ also uses the "AutoClose" macro instead of "AutoOpen". It infects the global template when an infected document is closed. Further documents become infected when they are also closed (AutoClose).

Wieder

Virus name:	Trojan.Wieder.A (a.k.a. Pferd, Wiederöffnen)
Number of macros:	2
Encrypted:	No
Macro names:	AutoOpen, AutoClose
Size of macros:	638 Bytes
Place of origin:	Germany
Date of origin:	Spring 1996
Destructive:	Yes
Seen In-The-Wild:	No
Description:	

Wieder is a not a virus but a trojan horse. It does not infect other files.

When an infected document is opened, Wieder creates the directory "C:\TROJA", and moves the system file "C:\AUTOEXEC.BAT" into the newly created directory. After moving the file the original files are deleted.

When closing an infected document, the following text is displayed:

" Auf Wiederöffnen "

" P.S: Falls Sie Ihre AUTOEXEC.BAT - Datei "
" gerne wiederhaben moechten, sollten Sie einen "
" Blick in das neue Verzeichnis C:\TROJA werfen... "

The original document, which included the trojan, has the following text:

" Trojanisches Pferd "
" Wenn Sie diese Zeilen lesen, wurde bereits Ihre AUTOEXEC.BAT- "
" Datei aus dem Hauptverzeichnis C:\ entfernt. Hoffentlich haben " " Sie eine Kopie davon ? "

" Genauso einfach waere es gewesen, Ihre Festplatte zu loeschen "
" und mit ein klein wenig mehr Aufwand koennte man auch einen "
" Virus installieren. "

X - Virus Names Starting With The Letter X

Xenixos

Xenixos

Virus name: Xenixos.A (a.k.a. Nemesis, Evil One, XOS)
Number of macros: 11
Encrypted: Yes
Macro names: AutoExec, AutoOpen, DateiBeenden, DateiDrucken, DateiDruckenStandard, DateiOeffnen, DateiSpeichern, SateiSpeichernUnter, Drop, Dummy, ExtrasMakro
Size of macros: 31342 Bytes
Place of origin: Austria
Date of origin: February 1996
Destructive: Yes
Seen In-The-Wild: No
Description:

Xenixos was the first macro virus that was written especially for the German version of Microsoft Word. All macro names are in German, and therefore it only works with the German Word version.

The infected global template (normal.dot) includes the following additional macros:

"AutoClose"
"AutoExit"
"AutoNew"

When an infected document is opened, Xenixos infects the global template unless the "DateiSpeichernUnter" macro is already present. Further documents become infected when using the "DateiSpeichern" and "DateiSpeichernUnter" command.
Files with the name "VIRUS.DOT" will not become infected.

During infection, Xenixos checks the system date and then activates various destructive payloads according the the date. During the month of May it adds the following text to "C:\AUTOEXEC.BAT":

"   @echo j format c: /u > nul   "

This will format the C:\ drive.

During the month of March, Xenixos tries to activate the DOS-Virus "Neuroquila" by using a DOS DEBUG script. This part of the virus is faulty (it tries to create an .EXE file) and therefore the DOS-based virus never infects the system.

The third destructive payload checks the system time, and in case of a value bigger than 45 in the seconds field, it will add the password "XENIXOS" to a saved document.

Upon printing a document, Xenixos checks the system time again, and in case of a value smaller than 30 in the seconds field, it will add the following text to the end of the printed document:

"   Nemesis Corp.   "

Xenixos also replaces the Tools|Macros to make recognition of an infected document more difficult (called macro stealth technique). The new code displays the following error message instead of the activation of Word's built-in macro viewer/editor:

"   Diese Option ist derzeit leider nicht verfuegbar   "

In addition, Xenixos changes section "Compatibility" inside the win.ini file. It sets the variable "RR2CD" to the value "0x0020401", and the variable "Diag$" to "0". The WIN.INI variables can be used to deactivate the virus. Setting the variable "Diag$" to "1" will prevent most of the destructive payloads.

Z - Virus Names Starting With The Letter Z

Zero

Zero

Virus name:	Zero.A:De
Number of macros:	9
Encrypted:	Yes
Macro names:	dok, dsu, wrd, extrasmakro, dateischliessen, dateispeichern, dateidokvorlagen,dokumentschliessen, dateispeichernunter
Size of macros:	727 Bytes
Place of origin:	Germany
Date of origin:	February 1997
Destructive:	No
Seen In-The-Wild:	No
Description:	

Zero uses a new infection technique. Instead of infecting the global template (normal.dot), it creates a file (0.DOT) in the "STARTUP" (default: C:\MSOFFICE\WINWORD\STARTUP) directory.

Zero activates when the "DokumentSchliessen" or "Extrasmacro" option is used. After creating the 0.dot file it copies its virus macros to the active document when the "DateiSpeichern" and "DateiSpeichernUnter" option is used.

Zero also uses "Extrasmacro" to make recognition of an infected document more difficult (called macro stealth technique).

U - Virus Names Starting With The Letter U

UglyKid

UglyKid

Virus name:	Uglykid.A
Number of macros:	3-4
Encrypted:	Yes
Macro names:	AutoOpen, (ToolsMacro, FileSave)
Size of macros:	Polymorphic
Place of origin:	Slovakia
Date of origin:	April 1997
Payload:	Yes
Seen In-The-Wild:	No

Description:

Uglykid.A is another Polymorphic macro virus, that can not be detected with a simple signature or with exact CRC detection. In June 1997, many scanner were unable to detect UglyKid reliably.

UglyKid.A uses "ToolsMacro" to make recognition of an infected document more difficult (called macro stealth technique). It also removes the File|Templates menu item so users can not look for viral macros on an infected system. It is advised not to select the "ToolsMacro" menu item, since it is used to execute the virus code. UglyKid.A also infects further documents when the "FileSave" command is used.

While most other Polymorphic viruses are fairly slow and visible to the user, UglyKid.A tries to hide the macro editing bar. Instead it shows a grey bar for a very short time.

The payload of UglyKid.A changes the "User Info" item in the Tool|Option menu. It adds the following comments:

"   Name: Nasty   "

"   Initial: Ugly   "

In order to detect UglyKid.A, we advise you to use an antivirus program that does smart checksumming (Example: Perforin 2.0).