Contact Information

The developers of InoculateIT Personal Edition have always aimed to provide software that will operate in the background until a virus attempts to infect and damage your PC.

If you have a technical support question please see the FAQs for immediate answers, or email IPE_Support@cai.com. InoculateIT Personal Edition technical support staff have a support level target to answer all e-mail with 48 hours of it being delivered.

If you suspect that you have a file that is infected with a virus that IS NOT detected by InoculateIT Personal Edition please email a copy of the file to IPE_Virus@cai.com. The InoculateIT Personal Edition virus dissection team will send an updated DAT file back to you within 48 hours. This will allow you to detect and clean the virus. (Standard response time is within 24 hour hours).

Computer Associates International has offices in the following countries:

Argentina, Australia, Austria, Bahrain, Belgium, Brazil, Canada, Chile, China, Colombia, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Malaysia, Mexico, The Netherlands, New Zealand, Norway, Philippines, Poland, Portugal, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Kingdom, United States and Venezuela.

Select an office for additional details. If you are not sure which office serves you, call 1-516-DIAL CAI (342-5224) for information.

ARGENTINA

Computer Associates de Argentina S.A.
Av. Davila 400 - Piso 2
1107 Buenos Aires
Argentina
Tel: (54)(1) 317-1500
Fax: (54)(1) 317-1515

AUSTRALIA

Computer Associates Pty. Ltd.
407 Pacific Highway
Artarmon, NSW, AUS 2064
Tel:(61)(2) 9937-0500
Fax:(61)(2) 9937 0600

AUSTRIA

Computer Associates Ges. m. b. H.
A-1100 Wien
Wienerbergstrasse 3
Tel:(43)(1) 605 80-0
Fax:(43)(1) 605 80-99

BAHRAIN

Computer Associates Middle East
Ground Floor, Diplomat Tower
Building 315
Road 1705, Block 317
Manama
Tel:(97)(3) 537 977

BELGIUM

Computer Associates S.A. - N.V.
34, Boulevard de la Woluwe
Woluwedal
B-1200 Bruxelles
Tel:(32)(2) 773 28 11

BRAZIL

Computer Associates do Brasil Ltda.
Av. Engenheiro Luiz Carlos Berrini
1253 - 1,5,6 andares
São Paulo - SP
04571-010
Tel:(55)11 5503-6000
Fax:(55)11 5503-6001

CANADA

Computer Associates Canada Ltd.
5935 Airport Road
Mississauga, Ontario L4V 1W5
Tel:(1)(905) 676-6700

CHILE

Computer Associates de Chile Ltd.
Av. Andres Bello, 2777
Oficina 1501
Edificio La Industria
Santiago
Tel:(56)(2) 203-3151
Fax:(56)(2) 203-3161

CHINA

Computer Associates (China). Ltd.
Room No. 2307, Capital Mansion
No. 6, Xin Yuan Nan Road
Chao Yang District
Beijing 100004
People's Republic of China
Tel: +86-10-6466 0322/0336
Fax: +86-10-6466 1135

COLOMBIA

Computer Associates Colombia
Avenida 82 No. 12-18
Oficina 305
Santafé de Bogotá - DC
Tel:(57)(1) 623 7886

CZECH REPUBLIC

Computer Associates Czech Republic
Donska 9
100 00 Praha 10
Czech Republic
Tel: ++420-2-67206360
Fax: ++420-2-67206363

DENMARK

Computer Associates A/S
Kongevejen 195B
DK-2840 Holte
Denmark
Tel: +45 45 47 41 41
Fax: +45 45 47 41 10

FINLAND

Computer Associates Finland OY
Itälahdenkatu 15-17
Helsinki SF-00210
Tel:(358) 9 34 84 84
Fax: (358) 9 348 48 585

FRANCE

Computer Associates S.A.
14 Avenue François Arago
BP 313
92003 Nanterre Cedex, 92003
Tel:(33)(1) 40-97-50-50

GERMANY

CA Computer Associates GmbH
Hauptverwaltung Darmstadt
Marienburgstrasse, 35
64297 Darmstadt
Tel:(49)6151 / 949-0
Fax:(49)6151 / 949-100

HONG KONG

Computer Associates International Ltd.
21/F World Trade Centre
280 Gloucester Road
Causeway Bay, Hong Kong
People's Republic of China
Tel:(852)2587-1388
Fax:(852)2587-1018

HUNGARY

Computer Associates Hungary
Kapas u. 11-15
1027 Budapest

Tel: +361 457 91 40

INDIA

Computer Associates India
511/512 Merchant Chambers
98A Hill Road
Bandra, Mumbai 400 050
India
Tel: 91 22 643 4681/82
Fax: 91 22 643 0843

INDONESIA

Computer Associates Indonesia
Wisma 46, Kota BNI
Level 34-05/06
Jl Jend Sudirman Kav. 1
Jakarta - 10220
Indonesia
Tel: 62-21-251-5030
Fax: 62-21-251-5029 / 251-5038

IRELAND

Computer Associates Plc
Embassy House
Ballsbridge
Dublin 4
Ireland
Tel:(353)(1) 478 0800

ISRAEL

C.A. Computer Associates
Israel Ltd.
Debora Hanevia St.
Neve Sharet, Atidim
Tel Aviv 61580
Tel:(972)(3) 6481120

ITALY

Computer Associates S.p.A.
Palazzo Leonardo
Via Francesco Sforza, 3
Milano 3 City
20080 Basiglio Milan
Tel:(39)2 90 464 1
Fax:(39)2 90 464 2501

JAPAN

Computer Associates Japan
Computer Associates Japan, Ltd
Shinjuku Mitsui Bld.

2-1-1 Nishi-Shinjuku, Shinjuku-ku
Tokyo, 163-04 Japan
Tel : +81-3-5320-8080
Fax : +81-3-5320-8095

KOREA

Computer Associates Korea Ltd.
11th Floor, Textile Center Bldg.
944-31, Daechi-Dong
KangNam-Ku
Seoul, Korea
Tel: +82-2-528-4100
Fax: +82-2-528-4111

MALAYSIA

Computer Associates (Malaysia) Sdn. Bhd
Suite 32/03, Level 32
Menara Lion
165, Jalan Ampang
50450 Kuala Lumpur
Malaysia
Tel: +60-3-230-2022
Fax: +60-3-230-6453

MEXICO

Computer Associates Mexico
Insurgentes Sur
1787 - Piso 10
Col. Guadalupe-Innc Morales
Mexico D.F. 11570
Tel:(52)5 327 5210

THE NETHERLANDS

Computer Associates B.V.
Wattbaan 27
3439 ML
Nieuwegein
(31) (30) 604 83 45

NEW ZEALAND

Computer Associates (NZ) Ltd.
Level 11, 34-42 Manners Street
P O Box 997, Wellington, N.Z.
Tel:(64)(4) 801 7654
Fax:(64)(4) 801 7655

NORWAY

Computer Associates Norway AS
Fornebuvn. 7-9
Pb. 450

N-1324 LYSAKER
Norway
Tel. +47 67 52 40 00
Fax +47 67 52 40 01

PHILIPPINES

Philippine Computer Associates International, Inc.
20/F Antel Corporate Center
139 Valerio Street
Salcedo Village, Makati City
Metro Manila
Philippines
Tel: +632-812-1441
Fax: +632-812-8896

POLAND

Computer Associates Poland
Centrum LIM
Al. Jerozolimskie 65-79
00-697 Warszawa

PORTUGAL

Computer Associates International, Inc.
Rua Tomas da Fonseca
Torres de Lisboa, Torre G-3
1600 Lisboa
Tel:(35)(1)727 35 33
Fax:(35)(1)727 35 25

RUSSIA

Computer Associates CIS, Ltd.
Representation Office
Business Center
Tokmakov per.,5
107066, Moscow, Russia
Tel./Fax: +7-095-937-48-50

SINGAPORE

Computer Associates Pte. Ltd.
9 Temasek Boulevard
#10-01/03 Suntec Tower 2
Singapore 038985
Tel: (65) 337 2822
Fax: (65) 337 4822

SOUTH AFRICA

Computer Associates Africa
6 Kikuyu Road
Sunninghill Park
Sunninghill Ext. 56

2157 Sandton
South Africa
Tel.: +27 11 807-5920
Fax: +27 11 807-2151

SPAIN

C.A. Computer Associates S.A
Calle Carabela La Niña, 12
Barcelona 08017
Tel:(34)3 2278100

SWEDEN

Computer Associates Sweden AB
Box 540
Berga Backe 4
182 15 Danderyd
Tel:(46)8-622 22 00
Fax:(46)8-622 58 68

SWITZERLAND

CA Computer Associates AG
Industriestraße, 30
Kloten CH-8302
Tel:(41)(1) 814 03 00

TAIWAN

Computer Associates Taiwan Ltd.
6th Floor, 105, Sec. 2, Tun Hwa South Road
Taipei, Taiwan
Tel: +886-2-2700-9218
Fax: +886-2-2700-9318

THAILAND

Computer Associates Pte. Ltd.
33rd Floor, Abdulrahim Place
990 Rama IV Road
Silom, Bangrak
Bangkok 10500
Thailand
Tel: 66-2- 636-2467-9
Fax: 66-2- 636-2470

TURKEY

Computer Associates Ltd. Sti.
Büyükdere Cad. Oyal Is Hani
Kat: 5 No. 108-1
80280 Esentepe - Istanbul
Tel:(90)(212) 27 27 172

UNITED KINGDOM

Computer Associates Plc
Computer Associates House
183-187 Bath Road
Slough
Berkshire SL-14AA
Tel:(44)(1753) 5777 33

UNITED STATES

Computer Associates International, Inc.
One Computer Associates Plaza
Islandia, NY 11788-7000
Tel:(1)516-DIAL CAI (342-5224)

VENEZUELA

Computer Associates (CAI) de Venezuela
Av. Principal de la Castellana Centro
Letonia Torre Ing Bank - Piso 10 - Ofic. 105
Caracas 1060 - Venezuela
Tel: +58 (2) 264-5144 / 264-4744

Year 2000 Support

We are pleased to advise you that InoculateIT PE currently supports Year 2000 processing.

Computer Associates' basic support for the millennium date change (Year 2000) provides or will provide for proper operation of our products according to the published documentation. In most cases, this means simply assuring that dates are evaluated and processed properly for sequence and comparison. Testing and Quality Assurance processes are carried out to validate the operation of these products as related to the millennium date change, and any functional errors will be accepted as issues (bugs) and resolved according to our standard maintenance and support policies.

As long as your license for each respective CA program remains in effect and active on maintenance, you will be entitled to all of the benefits of CA's implementation of Year 2000 date support as described above. Of course, nothing herein should be deemed to modify in any way any of the terms or conditions of any existing license between us respecting any CA program.

Eicar - A file to test your configuration

This is a program from the **European Institute for Computer Anti-Virus Research** that can help test the virus detection capabilities of Anti-Virus software.

This is a small .COM file for DOS that simply prints the message

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

when executed. It has the useful property that it consists entirely of printable ASCII characters, so you can easily email or fax it to someone.

Many anti-virus products will detect this file as if it had a virus. Most will give a special message to make it clear that this is a test file and not a real virus. For example, when the EICAR file is scanned, the following message will be displayed:

Detected the EICAR test string. Not a virus.

The main use of the EICAR test file is to test that your Anti-Virus software is configured and operating as you want it to. For example, it could be used to test that Real-Time protection is active and behaving as you expect.

While this file obviously has absolutely no virus code in it, you should only distribute it to people who have a clear understanding of what it does. Also, do not store it on production machines that run anti-virus software (except as part of a deliberate test), as it will probably trigger whatever alarm bells are in place.

Please refer to the EICAR Standard Anti-Virus Test File web page (www.eicar.org/anti_virus_test_file.htm) for more information.

Here is the EICAR test string, in its entirety:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Welcome to InoculateIT Personal Edition

Congratulations on choosing InoculateIT Personal Edition (InoculateIT PE) to protect your computer against viruses, trojans and other malicious software.

InoculateIT is a world class range of anti-virus software which can be deployed to suit any business or organisation. InoculateIT PE is a cutting edge, high performance virus package specifically designed to protect small businesses and home users from everyday virus threats.

InoculateIT PE is designed to protect individual computers without having to be installed from a network server. If you wish to install anti-virus protection to many computers in a business environment we recommend you evaluate other anti-virus products in the InoculateIT range.

This high quality anti virus tool comes with FREE software updates to registered users. It also comes with a promise that if you find a virus that InoculateIT PE is unable to detect or clean we will send you an emergency signature update in approximately 48 hours of receiving a copy of the suspected infected file.

Registered users will also receive FREE Internet E-mail support. The answers to many support questions can be found in the online help. If you open InoculateIT PE then select Help | Help Topics then select "How to get technical support and FAQs" you will find the answers to around 80% of the questions that are asked of our support team.

By registering, you are automatically subscribed to our FREE Virus Threat Notification System as well as our Update Notification Service. Anytime a new virus is found that is actually spreading around the world, this service will send an E-mail to you when a new virus signature update is available. This handy service will ensure that you are kept up to date so that you are protected against the very latest viruses. The Update Notification Service will only alert you when a new virus signature is posted on the Internet.

Frequently Asked Questions

The InoculateIT PE support team has compiled a considerable database of support questions. This appendix lists the more common questions as well as their corresponding answers.

To make finding questions easier, they are grouped into categories. Please take the time to read this appendix before contacting InoculateIT PE for advice as you may already have the answer you need.

This appendix also contains the common error messages that InoculateIT PE may display, and what they mean. If InoculateIT PE reports an error that you do not understand, and which is not listed here, please E-mail your question to ipe_support@cai.com for advice.

Installation/Setup/Configuration Problems

This section of the Frequently Asked Questions contains questions that you may have while installing InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) How do I check which version of InoculateIT PE I am running?
2) I want to install a program and it has told me to disable my anti-virus software. How do I disable InoculateIT PE?
3) After installing InoculateIT PE my icons have changed. Why is this, and how can I change them back?
4) When I remove InoculateIT PE from my Windows 95 system it gets to Removing Lines from the Dosstart.bat file and terminates with an error? How can I get around this problem?
5) I have configured my Windows 95 PCs to use 'user profiles' with access to the Registry disabled. I am now having problems installing InoculateIT PE. What can I do?
6) I get a General file transfer error -3 when I am performing an installation of InoculateIT PE. What is the cause, and the solution?

How do I check which version of InoculateIT PE I am running?

1. In Windows 95, 98 & NT, go to Start | Programs | InoculateIT PE (using the start menu).
2. Open the InoculateIT PE Program Window and go to Help | About.

You should regularly check the InoculateIT PE website www.cai.com/antivirus/personal for newer releases of InoculateIT PE, to keep your Antivirus protection up-to-date. Also, check our website for information on subscribing to our free e-mail notification service so you are informed via e-mail when a new version of InoculateIT PE is released.

I want to install a program and it has told me to disable my anti-virus software. How do I disable InoculateIT PE?

We advise that you don't disable InoculateIT PE Real-Time Protection under any circumstances because while InoculateIT PE is disabled, you are vulnerable to virus infection. Product or demo CD's shipping with viruses unintentionally attached is a rare but genuine threat, which is why the installation of new software is the worst time to disable InoculateIT PE.

However, if it is absolutely necessary to disable InoculateIT PE Real-Time Protection, please follow these instructions.

1. Open the InoculateIT PE program window using the taskbar icon in Windows 95/98/NT
2. Go to Options | Real-Time Protection | Enabling
3. Deselect the Boot Sector Monitoring box and the File / Macro Monitoring box.

You will then need to reboot the computer.

To confirm that InoculateIT PE Real-Time protection. is disabled, you can do the following:

1. Right Click on the InoculateIT PE Icon in the Taskbar
2. Select Status
3. There should be 2 red crosses displayed to indicate the Real-Time protection is disabled.

WARNING: Ensure that you enable the Real-Time Protection Modules by repeating the steps (1-3), this time checking the boxes to again enable the InoculateIT PE Real-Time protection.

After installing InoculateIT PE my icons have changed. Why is this, and how can I change them back?

This can sometimes happen when InoculateIT PE is being installed while other programs are running. This is not a serious problem and can be easily fixed. Simply exit Windows and re-start the computer in safe mode (to restart in safe mode hit the F8 key when the Starting Windows 95 message appears). Once into Safe Mode reboot the PC selecting Normal mode and you will find your icons will return to their original state.

When I remove InoculateIT PE from my Windows 95 system it gets to Removing Lines from the Dosstart.bat file and terminates with an error? How can I get around this problem?

Move the Dosstart.bat file to the C:\ directory and attempt the un-install again.

I have configured my Windows 95 PCs to use 'user profiles' with access to the Registry disabled. I am now having problems installing InoculateIT PE. What can I do?

InoculateIT PE can only use the privileges of the user that is logged in at the time of installation. For InoculateIT PE to complete a successful installation it must have access to the registry. Therefore, a user who has sufficient privileges to the registry must log in and then perform the InoculateIT PE installation.

I get a General file transfer error -3 when I am performing an installation of InoculateIT PE. What is the cause, and the solution?

During installation InoculateIT PE creates some registry entries, which can normally only be done if you have system administrator privileges. Please ensure that you are logged into the PC with Administrator rights.

Problems Using InoculateIT PE

This section of the Frequently Asked Questions contains questions that you may have while using InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) InoculateIT PE is causing an illegal operation when Windows starts up, What can I do?
2) I have installed InoculateIT PE for Windows 95 with the Plus Pack. I have noticed that it contains the McAfee Virus Scanner. Is it safe to run both InoculateIT PE and McAfee at the same time?

InoculateIT PE is causing an illegal operation when Windows starts up, what can I do?

This may happen when windows starts up and InoculateIT PE is doing a memory scan. To fix this, run the InoculateIT PE main program. From the top menu select Options | Programs | Startup. Select Customized start-up command and type in the following command line:

C:\Program Files\InoculateIT PE\VET95.EXE. RECURSIVE /WAITSTART=15

This will delay the InoculateIT PE startup scan so that the conflict will be bypassed.

I have installed InoculateIT PE for Windows 95 with the Plus Pack. I have noticed that it contains the McAfee Virus Scanner. Is it safe to run both InoculateIT PE and McAfee at the same time?

It is not advisable to run 2 Anti-Virus programs concurrently. You will need to disable the McAfee software during the installation of the Plus Pack or uninstall the program if it is already installed on the computer.

General

This section of the Frequently Asked Questions contains questions that are not about either installation or using InoculateIT PE. If your question is not answered here then click here to return to the main menu.

1) InoculateIT PE says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

2) Am I protected while using the Internet?

3) Why do some zip files take a long time to scan?

4) What are exotic viruses?

5) How can I tell that automatic protection is installed in Windows?

6) Year 2000 Support

7) When I run InoculateIT PE it says it is out of date.

8) Can you please tell me how to check e-mail attachments for viruses

9) I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

10) Everytime I turn on my PC InoculateIT PE starts up and runs a scan. How do I turn it off?

11) I need to disable InoculateIT PE as I need to load some new software. How do I turn it off?

12) InoculateIT PE reported that a document may be infected by a virus. What should I do?

13) Another AntiVirus product is reporting the bloodhound virus. Why is InoculateIT PE not detecting this virus?

14) Are `Good Times' `Win a holiday' & `Budweiser' viruses or a hoax?.

15) InoculateIT PE has informed me that I have either Back Orifice or Netbus trojan on my system, and that it was not restored. What are these trojans, and how do I remove them?

InoculateIT PE says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

When InoculateIT PE reports that the MBR or DBR has changed, it is comparing a snapshot of this information that was taken when you installed InoculateIT PE, to the current MBR and DBR. Changes may occur when a new operating system is loaded onto the PC.

Also, if you install InoculateIT PE to a PC that was already infected with a boot sector virus and clean it, InoculateIT PE will report the boot sector has been changed.

Am I protected while using the Internet?

Yes. InoculateIT PE Real-Time Protection will scan for viruses when you download files to your computer. That is, as soon as you actually download any files and save them to your hard disk, InoculateIT PE will scan and clean them. Downloading and opening infected files is the only method of virus transfer at the moment, so with InoculateIT PE you are completely covered. To check that Real-Time protection is enabled, move the pointer over the InoculateIT PE symbol in the system tray (located in the bottom right of the taskbar near the clock). You can also open the InoculateIT PE program and select options | Real-Time Protection

Why do some zip files take a long time to scan?

Zip files contain many files inside them which each require scanning and possible cleaning. Zipped files may also contain additional internal zip files which need to be scanned. It takes time to unzip, scan then rezip each file.

What are exotic viruses?

InoculateIT PE distinguishes between "in-the-wild" viruses (viruses that have been reported from a genuine infection) and "exotic" viruses - viruses we have in our collection, but which we have never seen reported as infecting users. If InoculateIT PE says a file "may have" virus X, please send a sample of the file to Computer Associates at ipe_virus@cai.com. If it is a genuine infection, a removal procedure will be added to InoculateIT PE and the virus will be upgraded from "exotic" to "in-the-wild" status.

How can I tell that Real-Time protection is installed in Windows95 or 98?

Run InoculateIT PE for Windows 95/98, then select Options | Real-Time Protection. The box at the bottom of each Real-Time Protection tab reports the current status of that component of the Real-Time Protection.

InoculateIT PE year 2000 support

If you open the InoculateIT PE program window and go to Help | Help Topics | Year 2000 support, you will find Year 2000 Support documentation.

When I start my computer InoculateIT PE displays the out-of-date warning message. What does this mean and why am I getting this message if I have the latest release?

Please ensure that latest InoculateIT PE has been installed properly by opening InoculateIT PE | Help | About, and check the date that the current DAT file was created. If the DAT file is more than a month old you should consider downloading a newer version of the files from www.cai.com/antivirus/personal/updates and installing them.

Can you please tell me how to check e-mail attachments for viruses?

InoculateIT Personal Edition Real-Time protection will check and clean any infected e-mail attachments when you open them. You can also Save the attachment to the hard disk and scan it using the main InoculateIT PE program. To check that Real-Time protection is enabled, move the pointer over the InoculateIT PE symbol in the system tray (located in the bottom right of the taskbar near the clock).

I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

Something odd happens, the user goes delving with their favourite disk editor and finds garbage or suspicious messages on the end of all the files. What is more, it changes when they copy a file to another location. "HELP! VIRUS!" Thankfully, no. MSDOS always allocates an integral number of whole clusters, but the file hardly ever fills the last cluster and the remaining space normally contains random rubbish.

Everytime I turn on my PC InoculateIT PE starts up and runs a scan. How do I turn it off??

Some InoculateIT PE users require the ability to conduct a scan when they start their PC each day. During the installation you will be asked if you would like this option enabled. Once enabled, the Start Up Scan can scan a set number of executable and document files on the boot drive every time the computer is started.

You can stop the scan at any time by selecting the CANCEL button from the progress meter.

To permanently stop this scan being started open InoculateIT PE and select Options | Program | Start-up

I need to disable InoculateIT PE to load some new software. How do I do it?

This is a dangerous thing to do. When you are loading new "shrink-wrapped" software people tend to believe that the software must be clean because it is direct from the software manufactures. This is not the case. Everytime you load files onto your PC you should have the Real-Time protection running to catch viruses.

If you have tried to load a piece of software and InoculateIT PE has refused to let you:

1) If the software is on a CD, send it back. Viruses cannot be removed from CDs.

2) If the software is on disks, check that they are write enabled and allow InoculateIT PE to remove the virus before installing the software.

3) If the Real-Time protection is clashing with the new software, do the following. Open InoculateIT PE and select Options | Enable Real-Time Protection. Click the check boxes so that they do not have a check in them and select OK. Close InoculateIT PE and reboot your PC.

When you have finished loading your software you MUST reverse the process and put a check in each box to re-activate the Real-Time protection.

InoculateIT PE reported that a document may be infected by a virus. What should I do?

InoculateIT PE uses heuristics to detect polymorphic viruses and certain strains that re occur in the wild. Heuristic or generic scanning is a technique for detecting viruses that performs analysis of virus structure and behaviour instead of using specific virus templates and signatures. The advantage of Heuristic Detection is that it can catch unknown viruses - the disadvantage is that it requires a high level of user expertise to use it correctly, and is prone to false alarms. If you are faced with this problem please forward the files to our Support Team through ipe_virus@cai.com.

Another AntiVirus product is reporting the bloodhound virus. Why is InoculateIT PE not detecting this virus?

Bloodhound is a generic name used by one of our competitors indicating that a specific file may have a virus, but they can't work out if it is definitely a virus or if it is a false alarm. Can you please forward any suspect files to our support team through ipe_virus@cai.com. They will be checked as soon as possible. If the files do contain a real virus, we will incorporate support for detecting and cleaning it in our next update, and send an update back to you to clean up the problem.

Are `Good Times' `Win a holiday' & `Budweiser' viruses or a hoax?

The Good Times, Win A Holiday and Budweiser virus message are all hoaxes.

It is currently impossible for your computer to be attacked when you read an e-mail message. If you would like more info, have a look at our website www.cai.com/antivirus

If you ever get any messages that sound similar and could also be a hoax, please e-mail them to the Technical Support Team at ipe_support@cai.com and we will let you know whether it is a real virus or not! Always verify the authority of such messages (by checking with us or a respected website) before forwarding them to your acquaintances. While hoaxes don't do any damage, they DO reduce people's overall confidence in using computers.

Remember the golden rule: You cannot infect your computer by just opening and reading an e-mail. You can only get infected by opening/running files that are attached to the e-mail. (And provided you have your Real-Time protection enabled you can open/run attachments without fear of a virus infecting your system.

InoculateIT PE has informed me that I have either Back Orifice or Netbus trojan on my system, and that it was not restored. What are these trojans, and how do I remove them?

A Trojan Horse is a malicious program masquerading as a legitimate program. The name comes from the Greek legend of soldiers hiding in a wooden horse which was supposed to be a gift, but which actually allowed them to infiltrate and burn the city of Troy. The best protection against them is to be very careful about obtaining all your software from reputable sources. BackOrifice and Netbus exploit a security flaw in your system, and allows certain remote users to delete your files, use your internet account, open and close your programs and many other undesirable options. If InoculateIT PE reports that BackOrifice or Netbus is on your system, please contact our technical support department by E-mail to ipe_support@cai.com for instructions on how to remove them immediately.

Glossary Of Terms

Unfortunately the computer industry uses a lot of technical terms that the general public has difficulty understanding. Below is a list compiled from customer enquires, if the word or term that you are interested in does not appear below please e-mail InoculateIT PE technical support.

AV short for Anti Virus
CARO short for Computer Anti-virus Research Organisation
Companion viruses
DLL short for Dynamic Link Library
DBR short for DOS Boot Sector (DBR)
Encrypting Viruses
Exotic viruses
File Viruses
GUI short for Graphical User Interface
Heuristic Detection
In the wild
Link viruses
Macro viruses
MBR short for Master Boot Record (MBR)
Multipartite Viruses
ICSA short for International Computer Security Association
OLE2 short for Object Linking and Embeding Version2
Payload
Parasitic viruses
Poly-Morphic Viruses
Real-Time Protection
Stealth
Trojan Horse
VBA5 short for Visual Basic for Applications version 5
VxD short for Virtual device Driver
Warheads
Worms

CARO (Computer Antivirus Research Organisation)

An informal world wide group of anti viral researchers. If a new virus is found by any of the companies that the researchers work for, samples are forwarded to the other members. This allows protection to be built into InoculateIT PE and other anti viral products before the virus is spread. (InoculateIT PE will also forward samples of new viruses to all other members to protect computer users overseas.)

DLL (Dynamic Link Library)
A collection of small programs that can be loaded and used by other programs.

GUI (Graphical User Interface)
A GUI product is one that allows you to "point and click" rather than typing in commands.

ICSA (International Computer Security Association)
A U.S. company that provides quality assurance ratings for products. InoculateIT PE is NCSA accredited. For further information see http:\\www.icsa.com.

OLE2 (Object Linked and Embedding version 2)

A standard for applications to exchange information across application boundaries. This standard allows for example embedding an Excel spreadsheet into a Word documents. It includes specifications for visual editing (in-place editing).and storage of data. Microsoft Office applications use the OLE2 provided storage mechanisms to store documents, including macros.

VBA5 (Visual Basic for Applications version 5)

This is the macro programming language used by most recent MS applications. The macro language used for Word 6.0 and 7.0 was WordBasic.

VxD (Virtual Device Driver)

When you install a new device into your PC you also need to install a driver so that the operating system can communicate with the new device. A Virtual device driver lets the operating system communicate with software as if it were a physical hardware device.

Stealth

A virus using stealth techniques takes active measures to hide its presence. For example if you read the boot sector of a disk infected with the Brain virus while it is active, it shows you the original boot sector, not the infected one. Frodo infects files, but the infection cannot be detected while it is active, as it disinfects files before it lets you read them. DIR will show the correct file lengths and programs that monitor checksums will report that infected files have not been modified. Frodo does not trap any interrupts, but instead modifies DOS itself so that monitor programs do not detect any unusual activity. However, these tricks make the virus extremely finicky and it will not run on some PCs and many infected programs will crash.

A few viruses have gone to such lengths to hide themselves that they are called Armoured viruses. The best known of these is the Whale virus. This research virus is multiply encrypted and only decrypts each section immediately before use and then re-encrypts it using a different key. The whole virus is further encrypted, using one of a number of alternative encryption procedures, chosen at random, so that there is no single signature to search for. However, like all armoured vehicles, it is extremely cumbersome and slows an infected PC down so much that it is immediately obvious.

What is Real-Time Protection

When Real-Time protection is loaded it will automatically check files and floppy disks for viruses as you go about your daily work. Real-Time Protection is loaded every time you start your PC, unless you specifically requested that it not be loaded during installation.

The level of protection can be modified from the Real-Time Protection dialog. See the on-line Help topics in your version of InoculateIT PE for further details as the method for altering these settings is different for each operating system.

File Viruses

Although there are a lot of different ways of grouping and classifying viruses, we can say that file viruses are those viruses which spread via files that are either executable or contain executable components.

File viruses can be further divided into the following groups:

- Parasitic viruses
- Companion viruses
- Link viruses
- Macro viruses

Parasitic Viruses

These represent the majority of all file viruses and they spread by modifying the code of executable programs. A parasitic virus attaches itself to an executable file and changes its contents in order to activate itself as soon as the operating system tries to execute an infected program.

Since there are a few ways in which a virus can attach its code to another file, we can subdivide still further, into overwriting, appending, prepending and inserting viruses. An overwriting virus simply overwrites the beginning of the file so that the infected file doesn't change its length but it no longer runs. Because of their destructive nature, overwriting viruses are relatively easy to detect and are not very common.

Appending and prepending viruses add their code to the start or the end of the file (respectively) and redirect the entry of the infected program to the start of the virus code. In that way infected programs increase in length but since the virus can pass control to the original program, the difference between executing a clean and an infected file is hard to notice.

Inserting viruses place their code (in one or more blocks) inside infected programs. They can search for an unused area (e.g. headers of .EXE files) or split the files and add their code in between the blocks of the infected file.

Companion Viruses

These take advantage of the DOS system's feature related to the sequence of loading and executing programs. If the file specified for execution has no extension, the system always tries to execute fname.COM, then fname.EXE and at last fname.BAT. A companion virus infects .EXE file by copying itself to a file with the same name but with .COM extension and usually hidden attributes. If the user enters the fname command, the file fname.COM (ie the virus) will be executed first.

A companion virus doesn't modify the infected program and usually passes control to the original .EXE file, but once detected it is easy to clean - you simply delete the relevant .COM file.

Link Viruses

These infect programs by changing information in the directory structure and modifying the file pointers, so every infected program starts at the same location (usually the last cluster on the disk) which contains virus code. Cleaning disks infected with a link virus requires a specific approach.

Every file virus can incorporate different techniques to improve the infection rate or to avoid detection. Each of the above viruses can be memory-resident, can have stealth capabilities, can use encryption or can use a polymorphic engine.

Macro Viruses

Technically another form of parasitic virus, the thing that makes macro viruses rate a class of their own is that they are transmitted as an executable component in an otherwise non- executable data file. Most macro viruses are written in WordBasic (Microsoft Word's macro language in version prior to version 8) or VBA (the macro language developed for other Microsoft products including Word version 8).

Macros are executable code intended to automate tasks in applications. However the underlying macro language is extremely powerful, and can call out to external programs, making macro viruses potentially quite dangerous. They are also the first "platform independent" virus, in that they will run on Macintosh computers as well as PCs. Another way of looking at it is that they depend on MS products (Word, Excel, Access etc) as their platform. Macro viruses have rapidly become the most reported viruses in the world.

Multi-Partite Virus

This is a virus that infects both boot sectors and executable files and exhibits characteristics of both boot sector and parasitic viruses.

Encrypting Virus

This is a virus which hides its code or even a whole infected file by encrypting it. The only plain text that can be seen inside an infected file is a decrypting procedure.

Polymorphic Virus

This is a self-modifying encrypting virus. Polymorphic viruses incorporate a special algorithm to create many different-looking copies of the same virus. Every next generation of a polymorphic virus can look slightly or even completely different from the previous one. The majority of new polymorphic viruses use specially designed libraries (engines) containing subroutines to produce different encryption schemes and encryption keys. The most famous polymorphic engines are:

DAME or MTE (Dark Avenger Mutation Engine);

TPE (Trident Polymorphic Engine);

SMEG (Simulated Metaphoric Encryption Generator).

Trojan Horse

This is a program that doesn't replicate and doesn't infect any other executable files and whose execution will result in undesired (often destructive) effects.

Worm

This is a program that distributes multiple copies if itself across the system. The most famous was the Internet Worm, which in 1988 virtually shut down the Internet in the US. It exploited holes in the Unix sendmail and finger programs.

Warheads (Also known as Payload)

The first virus writers were content with proving that they could write a virus, but later writers have become more ambitious and added a payload. This can be a taunt (Your Computer is now Stoned!) or it may interfere with the operation of the computer in an amusing, irritating, or destructive manner. Again there is a conflict between the desire to show off and the need to be inconspicuous, so that the virus will propagate widely. This is usually achieved by making the payout wait some time or depend on some rather unusual event, so that the virus does not declare itself until it has had a chance to propagate. It is generally unwise to deliberately trigger a virus's warhead; we know of at least one user who was infected with the Michelangelo virus who advanced his system clock to March 6th just to see what would happen and thereby lost the data on his hard disk. Even joke viruses aren't funny when they go wrong on a non-standard PC.

Heuristic Detection

Heuristic or generic scanning is a technique for detecting viruses that instead of using specific virus templates and signatures, performs analysis of virus structure and behaviour. The advantage of Heuristic Detection is that it can catch unknown viruses - the disadvantage is that it requires a high level of user expertise to use it correctly, and is prone to false alarms.

Contents of Virus Information

The on-line virus information is broken down into a number of more manageable topics;

Information on a Specific Virus
Software Problems that are not viruses
General Virus Information
Different Types of Viruses
Technical Support contact details

Viruses and Windows

If an infected program is run before Windows is opened, the virus appears to operate normally. In our tests, Jerusalem infected WIN.COM, but did not infect Windows applications. When a DOS file infected with Jerusalem was run from Windows, Windows helpfully reported: *Your Pop-up program has been loaded, and you may activate it as you would normally*. However the virus was apparently not able to infect other files and was not found in memory. We got the same message and result when we ran a file infected with AntiCad, but it did manage to infect the Master Boot Record. When we ran Windows with *Frodo* already installed, or attempted to run a file infected with *Frodo* from Windows, the system crashed. Some viruses (eg *Junkie*) will cause Windows to report a message about not being able to use 32-bit disk access when it has been previously able to.

Windows files have a dummy .EXE header which gives a message about loading Windows if you try to run them under DOS. If you do so and the PC is infected, this header will become infected. Jerusalem and its descendants will destroy the file in the process, but most viruses will not have any effect on the program's operation under Windows. If Windows files do become infected, your anti-virus software will detect and remove the virus in the normal way.

Sabotage

By now, most large organisations have been hit by viruses, but far more data is still destroyed by careless, incompetent or malicious users. You can reduce the risks from careless and incompetent users by education and by using well designed software, but it is much harder to prevent sabotage. The best protection against both sabotage and mechanical failures is to establish and use good backup procedures. Proprietary backup programs enable you to take a quick snapshot of your PC, but unless you immediately restore the data onto a second PC, preferably at another location, the only time you will know if your backup is any use is when it is too late. We strongly recommend that you use COPY, or XCOPY, to copy all vital data to floppies. Check that you can read the files (on another PC) and store them somewhere else. BACKUP, supplied with the PC, is notoriously unreliable and boot sector viruses will ruin most proprietary backup disks if they infect them.

More Information

There are many potential sources of virus information but not all can be relied upon as being accurate and unbiased. Here are some reliable sources of information:

1. Virus Bulletin

21 The Quadrant
Abingdon Science Park
Oxfordshire, OX14 3YS
United Kingdom

This publication is owned by Sophos Ltd, publishers of Sweep Anti-Viral software, and it provides accurate technical information on viruses. Virus Bulletin can be obtained on a subscription basis from your anti-virus distributor.

2. Secure Computing

West Coast Publishing Limited
William Knox House
Britannic Way, Llandarcy
Swansea, SA10 6EL
United Kingdom

This monthly journal provides good quality technical articles and information on new viruses.

3. Computer and Security

Elsevier Advanced Technology
PO Box 150
Kidlington
Oxford, OX5 1AS
United Kingdom
Email: j.meyer@elsevier.co.uk

This journal contains many papers on the subjects of computer viruses and security. For research purposes, this is a very valuable resource.

4. VIRUS-L / comp.virus

The *Frequently Asked Questions* (FAQ) document is available by anonymous ftp from **ftp.cert.org**

This is a USENET newsgroup, also available as a mailing list, on the Internet. For information about it, as well as much useful information, see the FAQ file. Many of the well-known anti-virus researchers use this to exchange much useful information.

Viruses and Anti-Social Software

Unfortunately there are as many misfits among computer users as anywhere else and over the last few years, a wide range of anti-social software has appeared. This software surreptitiously interferes with the user's computer, without the perpetrator having to gain direct access to the computer. Software of this type can be divided into three main groups:

- Worms
- Trojan Horses
- Sabotage

If users are have problems executing a program, it may not always be a virus infection. Some other possible causes are:

- Bugs
- Invalid Boot Sectors

There are also a number of Hoaxes that keep circulating on the Internet. If you receive an email warning about a new virus it may be that it is actually a hoax.

Hoaxes

A hoax is a message, typically distributed via email or newsgroups, that is written to deliberately spread fear, uncertainty and doubt. Hoaxes prey on the lack of technical knowledge and goodwill of all those that receive a hoax. Generally, hoaxes are warnings about threats to your computer that do not actually exist.

A common characteristic of a hoax is that it asks you to forward the warning on to as many people as possible. This is how the hoax "spreads" itself. If you receive any form of message that asks you to forward it on to others, you should check out the accuracy of the message before forwarding it on to anyone else, otherwise you may help perpetuate a hoax.

How can you check a message for accuracy?
See http://caitest.ca-nethaven.com/virusinfo/encyclopedia/ and select the `Hoaxes' link.

Worms

A *worm* is a program that has been written to replicate through a network of computers and unlike a virus, does not need a carrier program in order to multiply. The main difference between a worm and a virus is that a worm actively tries to infect other computers, whereas viruses rely on the users to spread them, albeit inadvertently. Worms haven't been a threat to PC networks in the past since none existed of sufficient size or uniformity, however the growth of the Internet and the greater availability of common applications for it may change this.

Trojan Horses

A *Trojan Horse* is a malicious program that hides inside a legitimate program, as in the soldiers in the wooden horse of Troy. There are lists of programs known to contain Trojan Horses, but the best protection is to be very careful to obtain all your software from reputable sources. The only way to prove that a program does not contain a Trojan Horse is to do a total disassembly and this is impractical for any but the most trivial program.

Validation programs, such as VCRC, calculate Standard Cyclic Redundancy Codes for any file and validation data is available for many Shareware products. If the validation data for a file does not match the published values, the code has been tampered with after the final release.

Viruses

In biology, a virus is a small particle of living material which is not capable of breeding by itself, but which has sufficient genetic material to enable it to enter a living cell and subvert the active processes of the cell so that the cell replicates the virus, producing new particles of virus which can attack other cells. An example is the Ecoli virus which infects humans.

By analogy, a *computer virus* is a program which attaches itself to another program, but modifies the action of that program so that the virus is able to propagate. There are thousands of viruses which differ widely in the types of program they infect, the way they propagate and in the side effects that they have. Some are extremely destructive while others are relatively benign. Viruses can be classified in several different ways, but the most common way is to classify them by what they infect:

How Viruses Work:

Choice of Vehicle

In principle, any program could serve as a vehicle for a virus, but for a virus to propagate effectively it must attack a program which is both common and likely to be swapped between users. Some viruses are specific and attack a single program, while others have more catholic tastes and attack a wide range of programs.

Common vehicles are:

1. DOS boot sector
2. Master boot record
3. Executable files (eg those with COM and EXE extensions)
4. Files containing an executable code (eg Word or Excel documents containing auto-macros).

It is also possible to design viruses which infect device drivers and batch files. Both types of virus exist, but neither is common.

Boot sector viruses are fairly easy to design and were probably the first to appear. They are relatively inconspicuous (if they don't display messages etc.) but are also easy to keep out of your system. Viruses which infected executable files soon followed and now there are multipartite viruses which infect both program files and boot sectors.

Some viruses alternate between boot sector and programs. This makes them harder to study, as it is impossible to generate test files without infecting a hard disk.

Propagation Mechanisms

If a virus is too aggressive in its efforts to propagate, it will be conspicuous by causing excessive disk activity, but if it is too coy it will probably not infect many files. There are two main classes of infection mechanism:

When a program infected with a *direct infector* is run, the virus actively searches for a file or files to infect. It may search the current drive or directory, or selected directories, such as the directories specified in the PATH. It then loads the infected file and runs it. Direct Infectors do not remain in memory and they are not very common, as the infection mechanism is not very efficient and the additional disk activity is obvious, especially when all files are already infected.

When a program infected with an *indirect infector* is run, the virus installs itself in memory, usually redirects one or more interrupts and then runs the original program. Most indirect infecting program viruses infect every file which is loaded for execution and some infect every executable file which is loaded for any reason.

Boot sector viruses usually act like indirect infectors when infecting floppy diskettes and like direct infectors when infecting hard drives.

Location in Memory

Program viruses which use DOS Function 31h to go resident, stay in low memory and other programs use the memory above them. Viruses which modify the memory allocation chain usually move themselves to the top of normal memory and set the top of memory marker down. Boot sector viruses normally occupy the top of memory. A few viruses move themselves to the top of memory, but do not reserve any memory to protect themselves. These cannot be detected by checking the available memory, but most large programs will crash the system when they overwrite the virus. The EDV virus searches for memory in the system area (0A000:0000h - 0F000:FFFFh). There are many programs that use this area now and it is likely that this virus will also crash many systems.

A few viruses have tried to find other hiding places. The Troi family install themselves in the top half of the Interrupt Table and others hide in the DOS buffer area.

Stealth

A virus using stealth techniques takes active measures to hide its presence. For example if you read the boot sector of a disk infected with the *Brain* virus while it is active, it shows you the original boot sector, not the infected one. *Frodo* infects files, but the infection cannot be detected while it is active, as it disinfects files before it lets you read them. DIR will show the correct file lengths and programs that monitor checksums will report that infected files have not been modified. *Frodo* does not trap any interrupts, but instead modifies DOS itself so that monitor programs do not detect any unusual activity. However, these tricks make the virus extremely finicky and it will not run on some PCs and many infected programs will crash.

A few viruses have gone to such lengths to hide themselves that they are called Armoured viruses. The best known of these is the Whale virus. This research virus is multiply encrypted and only decrypts each section immediately before use and then re-encrypts it using a different key. The whole virus is further encrypted, using one of a number of alternative encryption procedures, chosen at random, so that there is no single signature to search for. However, like all armoured vehicles, it is extremely cumbersome and slows an infected PC down so much that it is immediately obvious.

Macro viruses will remove menu items in an attempt to stop users checking the name of the macros that are currently in use. A classic example is editing Word so that when you select the Tools menu there is no option to select Macro.

Encryption

Virus scanners generally detect a virus by looking for a sequence of instructions or template characteristic to it. Some viruses are encrypted, usually by some simple procedure like XORing each byte with a key chosen at random for each new copy. These viruses are detected by looking for the decryption procedure at the start of the virus.

Warheads (also known as Payload)

Some viruses exist just to propagate, others have *payloads* or *warheads*. This can be the display of a taunt (eg *Your Computer is now Stoned!*) or it may interfere with the operation of the computer in an amusing, irritating, or destructive manner. Generally a virus will propagate more widely if its warhead doesn't activate immediately; the payload is usually triggered on some event, or after a certain amount of time. It is unwise to deliberately trigger a virus's warhead.

Bugs

The opportunities for testing viruses are limited and it is impossible to recall faulty products, so most viruses have bugs. These may reduce the viability of the virus or make it more obvious, but often they make the virus unintentionally destructive when they interact with another program (or virus!) or a non standard piece of hardware. On a number of occasions infections with normally trivial viruses have become disasters because a bug in the virus has interacted fatally with the PC's particular configuration. Some viruses betray themselves by causing Critical Error Messages when they try to infect a write-protected disk.

Invalid Boot Sectors

A normal boot sector contains a parameter table specifying the number of tracks, heads and sectors, size of sectors, numbers of FATs and so on. This takes up bytes 0bh to 1ch and includes the media descriptor byte. This was originally intended to indicate the type of disk, but most programs don't use it. Many viruses (including Brain, Computer Ogre and Stoned) overwrite the parameter table. The results are unpredictable and apparently depend on the size of the disk, the last disk read, the DOS version and possibly the BIOS. MSDOS doesn't usually seem to mind with 360K disks, but will often refuse to read other size disks, or will not find some or all files.

Type of Viruses

There are many different viruses loosely grouped into families. Each of these families is explained below;

- Boot Sector Viruses
- File Viruses
- Boot Sector and File Viruses
- Parasitic Viruses
- Companion Viruses
- Overwriting Viruses
- Polymorphic Viruses
- Macro Viruses

Boot Sector Viruses

The Boot Sector viruses can only infect your system if you boot from an infected disk. However, the disk does not have to be a system disk to transfer the virus. A major weakness of the IBM PC in its most common configuration, is that it will always first try to boot from drive A. If you never boot your PC from a floppy disk you are generally safe from boot sector viruses, but even booting with a floppy disk inadvertently left in drive A can infect your PC. So always check the floppy drive is empty before switching on or rebooting your computer.

As the boot program is very short, it cannot contain both the virus and the original boot program and the virus has to make sure that it is run first. Therefore, when a virus infects a new disk, it has to store the original boot program (and often most of the virus as well) somewhere else on the disk and then put its own installation procedure in the boot sector. Some viruses simply move the boot sector to a fixed place, trying to choose somewhere which won't be too obvious. The Stoned virus puts the old boot sector at the end of the directory where it won't be noticed unless the disk contains more than 96 files in the main directory (on a 360K disk). The Yale virus occupies the last sectors of the last track and will only be noticed if the disk is completely full, while the Den Zuck virus formats an extra track on the disk above the normal last track (where it is completely inaccessible to any normal procedure and to most disk editing utilities).

Other viruses look for an unused cluster on the disk, put themselves in it and then mark the cluster(s) used as bad, so that MSDOS will not try to use them for something else. On a normal disk, the loss of capacity is insignificant, but if the disk has a non standard data structure the virus may overwrite something vital when it writes to an apparently empty cluster.

If a virus also infects hard disks, the process is similar but the virus can infect either the Master Boot Record or the DOS boot sector. On normal hard disks, Sector 1 (the MBR) is the only sector used on Cylinder 0, Head 0 and many viruses store themselves in the empty sectors. Unfortunately these sectors are not empty on some non-standard PCs, and infecting them may have dire consequences.

File Viruses

Also called *program viruses*, these generally attach themselves to executable files and are grouped according to the class(es) of program they infect. They can be extremely infective and are much harder to counter than boot sector viruses because of the wide range of potential targets. There is a greater number of file viruses than boot sector viruses, but boot sector virus incidents are far more common.

File viruses can be further divided into Parasitic Viruses, Overwriting Viruses, Companion Viruses and Linking Viruses.

All of the above can use some of the following techniques Stealth, Encryption or Polymorphism.

Multipartite (Boot Sector and File) Viruses

These viruses infect both boot sectors and files. This generally makes them far more effective in propagating, since they can be spread by booting from an infected disk, or by running an infected file, and thus there is more chance of being infected. The Junkie virus is an example of a common multipartite virus; it has been prevalent in Australia for the last couple of years.

Parasitic Viruses

Parasitic viruses are those that attach themselves to files in order to propagate. They generally keep most of the file intact and either add themselves to the start (prepending viruses) or end of the file (appending viruses). COM files are easiest to infect, as they are simply loaded directly into memory and execution always starts at the first instruction. Thus a virus can simply insert its self at the beginning of the file. Then when the file is run, the virus is loaded before the actual program. This is how early viruses infected .COM files. The infection process is quicker if the virus is appended to the file but this causes some complications, as the first few bytes of the file must be saved and replaced with a jump to the virus and the virus is not at a fixed offset from the start of the code segment.

While .COM files cannot be longer than 64 kilobytes, .EXE files can be of any length (provided they will fit in memory), but the file structure is more complex. The program can be built up from a number of segments and the file has a header which specifies the size of the program, the segments used and how they are to be linked together and where execution is to start. When a virus infects an .EXE file, it must save the original contents of the header, copy itself to the end of the file and modify the header so that the virus is loaded as part of the file and executed first.

Once virus writers had learned how to handle .EXE files, most found it easiest to treat .COM files in the same way. Thus many viruses put the virus at the end of both .COM and .EXE files. Many files contain empty space and some viruses exploit this by overwriting it with their own code, so that they don't change the length of the file. At least one virus (*Command Bomber*) comes in several sections, which are inserted at various locations in the file.

Companion Viruses

If you try to run a program without specifying a file extension, the system will always try to find and execute the .COM program first and if it cannot be located then .EXE file will be called next. Companion viruses make use of this to provide an infection mechanism which does not modify the original file in any way. These viruses only infects .EXE files and do so by writing a companion .COM file with the same name. Then, when the user runs an infected program, the .COM file containing the virus is run. It looks for another .EXE file to infect, then loads the requested .EXE file and runs it. An example of a companion virus is the *AIDS II* virus.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate. However, this makes these viruses extremely obvious, so they are unlikely to spread far. The Zeroto-0, or Australian 403 virus, is of this type. When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains virus. The original file is destroyed, so infected files appear to run, but do nothing.

Polymorphism

Polymorphism is an advanced form of encryption in that the key changes all the time, rather than staying the same. Typically, in polymorphic viruses, the decryption procedure will use three or four registers and each is chosen randomly from the set of registers available. Additionally, the procedures often include variable numbers of randomly chosen instructions which do nothing, but act as inert fill, or noise. Writing procedures to detect these viruses is more difficult than using a template, but the viruses are also much harder to write and there are not many of them, even though engines are available to add polymorphism to a normal virus (a prime example is TPE). The main problem with polymorphic viruses is that detection is more difficult and less reliable, and it is sometimes not practical to disinfect files that have been infected.

Macro Viruses

The majority of macro-viruses are written in WordBasic which is used for the Microsoft range of products, most notably MS Word. MS Word is available on a number of platforms and in a number of languages giving a greater variety of environments where macro-viruses can propagate. People copy, edit and share Word documents more often than sharing a floppy disk, this allows macro viruses to spread faster than other varieties of viruses. Macro viruses also use the growing popularity of attaching Word documents to E-mail and downloading files from the Internet as additional vehicles to infect many more computers.

They arrive attached to a spreadsheet or document, when the file is opened it will transfer from the document to the application template. Any new or existing file that is saved will have the virus inserted into it. The virus will spread to other files via a variety of methods, the most common is the File | Save As sequence which is used to save file or by using Save As to save a different version of an existing file.

By default Macro viruses (including the Excel macro virusesmacrolaroux) will automatically be detected and cleaned.

How To Find Information About A Specific Virus

This help file provides the names of specific viruses detected by this version of InnoculateIT PE.
It also provides information regarding types of viruses. If you wish to check if a specific virus is detected by this version please open the VIRUSES.HLP file and search for the virus by name.

If you need detailed information about a specific virus or a virus family, please refer to Computer Associates Virus Encyclopedia on the World Wide Web. Computer Associates Virus Encyclopedia is updated as new viruses and other threads emerge almost daily. The latest version of the encyclopedia can be found at:

http://www.cai.com/virusinfo/encyclopedia/

Please note that the encyclopedia does not contain descriptions for all viruses detected by InoculateIT PE, it only contains information about viruses that have been actually encountered by real users (found in the wild).