



Ethical Hacking and Countermeasures

Version 6



Module IX

Viruses and Worms

FBI Warns of Valentine's Day E-Mail Virus

Thursday, February 14, 2008

FOX NEWS

Happy Valentine's Day! You've got a computer virus!

IT managers around the world braced themselves Thursday for an expected onslaught of romantic "e-cards" surreptitiously carrying the nastiest virus around: the Storm Worm.

"Once the user clicks on the [e-mail] link, malware is downloaded to the Internet-connected device and causes it to become infected and part of the Storm Worm botnet," warns a public alert posted on the FBI's Web site Monday.

▪ [Click here to visit FOXNews.com's Cybersecurity Center.](#)

"The Storm Worm virus has capitalized on various holidays in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail," says the FBI. "Valentine's Day has been identified as the next target."

Haven't heard of the Storm Worm? That's because it hasn't "struck" yet, even though researchers first noticed it more than a year ago after it cropped up in e-mails showing photos of damage from European windstorms in January 2007.

Since then, it's steadily infected an estimated 10 million Windows-based PCs around the world, all under the command of unknown "bot herders" who've silently fashioned them into a "zombie army" or "botnet" — a massive network of "enslaved" PCs awaiting the signal to launch a cyberattack.

ADVERTISEMENT

SIX DEGREES
COULD CHANGE THE WORLD

ROLLOVER TO
EXPERIENCE **SIX DEGREES**

NOW AVAILABLE
IN HD ON DEMAND

comcast NATIONAL
GEOGRAPHIC
CHANNEL HD

Source: <http://www.foxnews.com>

Ricky, a software professional with a reputed organization, received a mail which seemed to have come from some charitable organization. The mail was having a .ppt attachment with name “demo of our charity work”. Just before leaving for his home he downloaded and played the attached presentation. The presentation consisted of images of poor people being served.



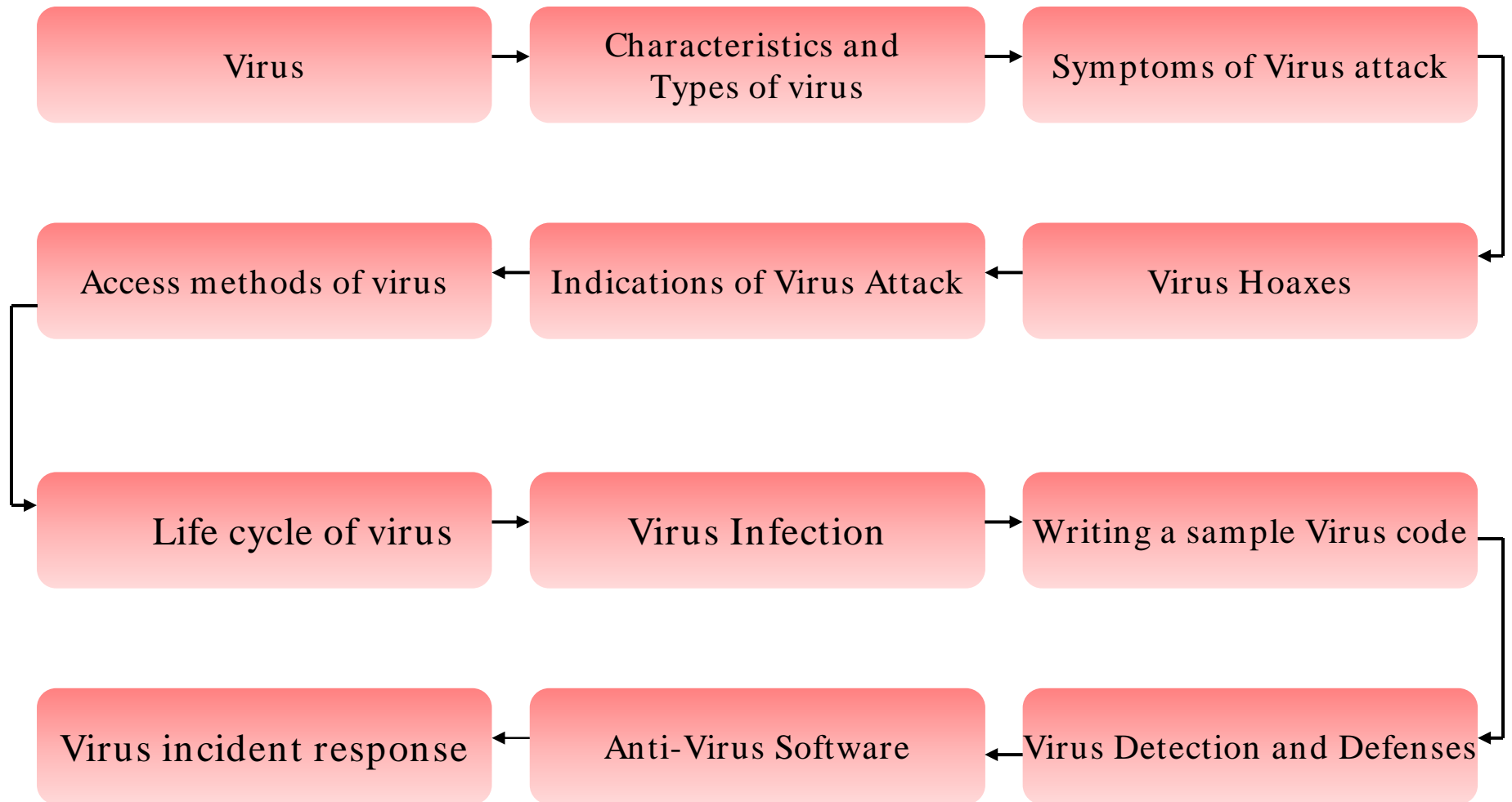
What could be the dangers of opening an attachment from unknown source?

What could be the losses if attachment that Ricky opened had viruses or worms?

This module will familiarize you with :

- Virus
- History of Virus
- Different characteristics and types of virus
- Basic symptoms of virus-like attack
- Difference between Virus and Worm
- Virus Hoaxes
- Indications of virus attacks
- Basic working and access methods of virus
- Various damages caused by virus
- Life cycle of virus
- Virus Infection
- Various virus detection techniques
- Top ten virus of 2005
- Virus incident response

Module Flow

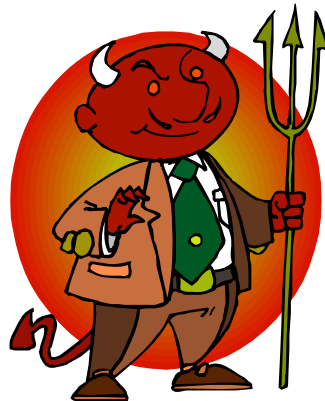


Introduction to Virus

Computer viruses are perceived as a threat to both business and personnel

Virus is a self-replicating program that produces its own code by attaching copies of itself into other executable codes

Operates without the knowledge or desire of the computer user



Virus History

Year of Discovery	Virus Name
1981	Apple II Virus- First Virus in the wild
1983	First Documented Virus
1986	Brain, PC-Write Trojan, & Virdem
1989	AIDS Trojan
1995	Concept
1998	Strange Brew & Back Orifice
1999	Melissa, Corner, Tristate, & Bubbleboy
2003	Slammer, Sobig, Lovgate, Fizzer, Blaster/ Welchia/ Mimail
2004	I-Worm.NetSky.r, I-Worm.Baqle.au
2005	Email-Worm.Win32.Zafi.d, Net-Worm.Win32.Mytob.t

Characteristics of a Virus

Virus resides in the memory and replicates itself while the program where it is attached is running

It does not reside in the memory after the execution of the program

It can transform themselves by changing codes to appear different

It hides itself from detection by three ways:

- It encrypts itself into the cryptic symbols
- It alters the disk directory data to compensate the additional virus bytes
- It uses stealth algorithms to redirect disk data



Working of Virus

Trigger events and direct attack are the common modes which cause a virus to “go off” on a target system

Most viruses operate in two phases:

Infection Phase:

- Virus developers decide when to infect the host system’s programs
- Some infect each time they are run and executed completely
 - Ex: Direct Viruses
- Some virus codes infect only when users trigger them which include a day, time, or a particular event
 - Ex: TSR viruses which get loaded into memory and infect at later stages

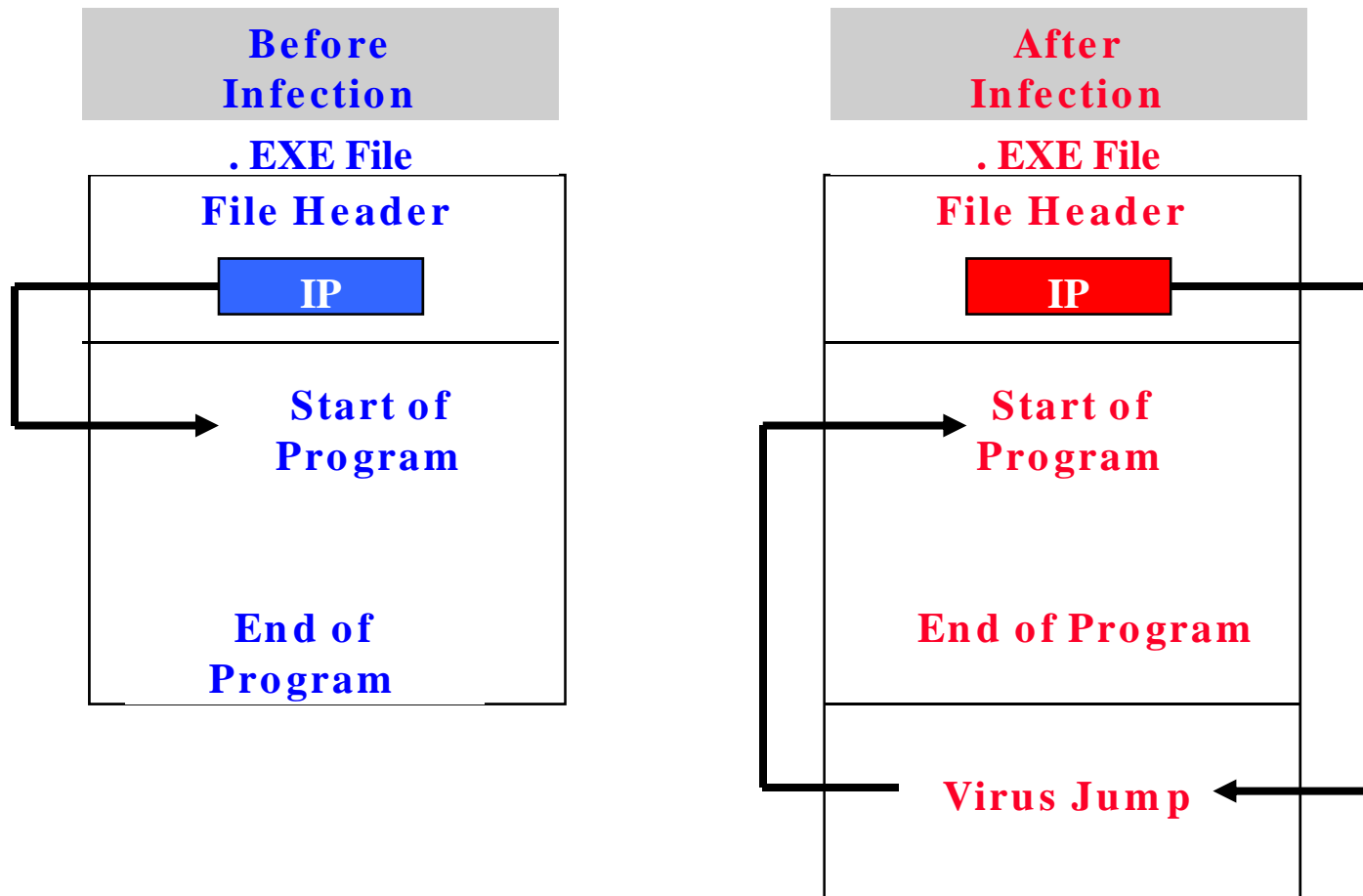
Attack Phase:

- Some viruses have trigger events to activate and corrupt systems
- Some viruses have bugs that replicate and perform activities like file deletion and increasing the session time
- They corrupt the targets only after spreading completely as intended by their developers



Working of Virus: Infection Phase

Attaching .EXE File to Infect the Programs



Why People Create Computer Viruses

Virus writers can have various reasons for creating and spreading malware

Viruses have been written as:

- Research projects
- Pranks
- Vandalism
- To attack the products of specific companies
- To distribute the political messages
- Financial gain
- Identity theft
- Spyware
- Cryptoviral extortion



Symptoms of Virus-Like Attack

If the system acts in an unprecedented manner, you can suspect a virus attack

- Example: Processes take more resources and are time consuming

However, not all glitches can be attributed to virus attacks

- Examples include:
 - Certain hardware problems
 - If computer beeps with no display
 - If one out of two anti-virus programs report virus on the system
 - If the label of the hard drive change
 - Your computer freezes frequently or encounters errors
 - Your computer slows down when programs are started
 - You are unable to load the operating system
 - Files and folders are suddenly missing or their content changes
 - Your hard drive is accessed often (the light on your main unit flashes rapidly)
 - Microsoft Internet Explorer "freezes"
 - Your friends mention that they have received messages from you but you never sent such messages



Virus Hoaxes

Hoaxes are false alarms claiming reports about a non-existing virus

Warning messages propagating that a certain email message should not be viewed and doing so will damage one's system

In some cases, these warning messages themselves contain virus attachments

They possess capability of vast destruction on target systems

Being largely misunderstood, viruses easily generate myths. Most hoaxes, while deliberately posted, die a quick death because of their outrageous content



MY ROOM



DO NOT ENTER

Virus Hoaxes (cont'd)

Subject: [Fwd: Beware of the Budweiser virus--really!]

This information came from Microsoft yesterday morning. Please pass it on to anyone you know who has access to the Internet. You may receive an apparently harmless Budweiser Screensaver, If you do, DO NOT OPEN IT UNDER ANY CIRCUMSTANCES, but delete it immediately. Once opened, you will lose EVERYTHING on your PC. Your hard disk will be completely destroyed and the person who sent you the message will have access to your name and password via the Internet.

As far as we know, the virus was circulated yesterday morning. It's a new virus, and extremely dangerous. Please copy this information and e-mail it to everyone in your address book. We need to do all we can to block his virus. AOL has confirmed how dangerous it is, and there is no Antivirus program as yet which is capable of destroying it.

Please take all the necessary precautions, and pass this information on to your friends, acquaintances and work colleagues.

End of message.

EMAILCHIEF

Chain Letters

SAMPLE CHAIN LETTER TEXT

VIRUS WARNING

A new Virus - WOBLER is on the loose. It will arrive on e-mail titled "HOW to GIVE A CAT A COLONIC". IBM and AOL have announced that it is very powerful, more so than Melissa.

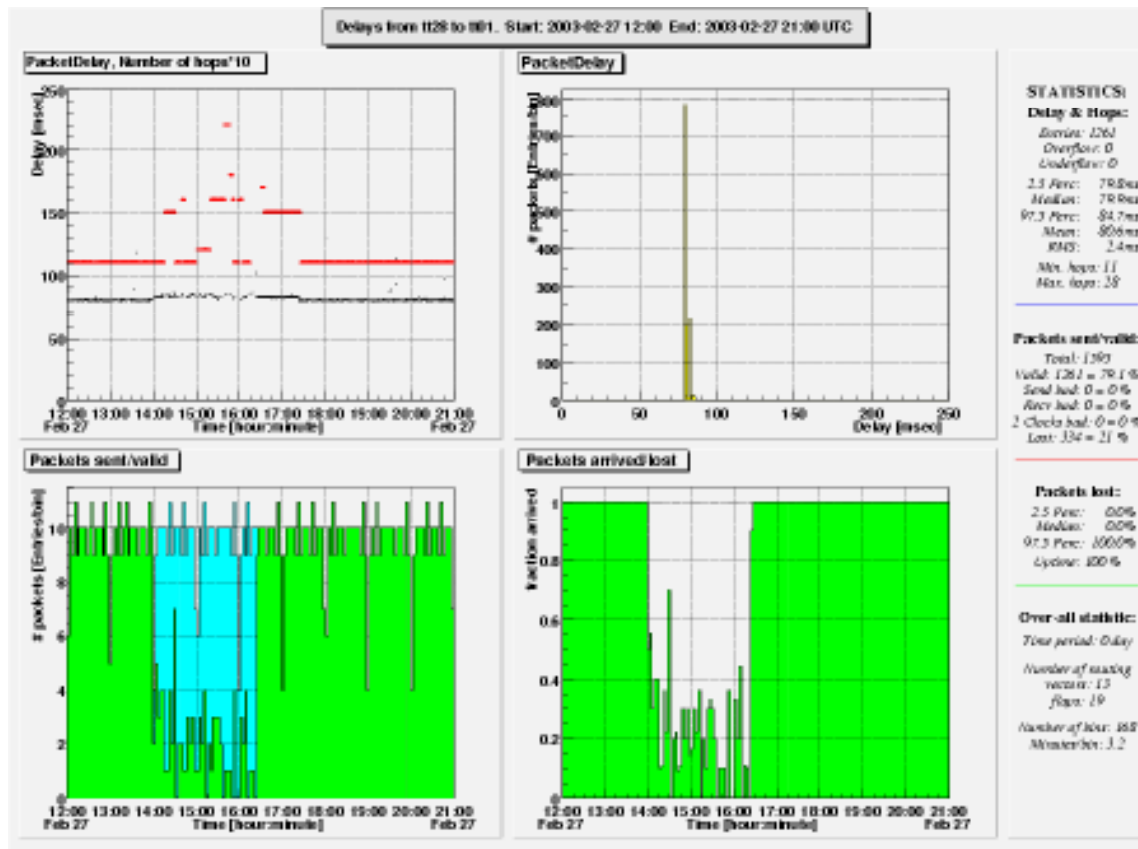
There is no remedy. It will eat all your information on the hard drive and also destroys Netscape Navigator and Microsoft Internet Explorer. Do not open anything with this title and please pass this message on to all your contacts and anyone who uses your e-mail facility. Not many people seem to know about this yet so propagate it as fast as possible. This information was announced yesterday morning by IBM.

Please share it with everyone in your address book so that the spreading of the virus may be stopped. This is a very dangerous Virus and there is no remedy for it at this time. Please practice cautionary measures and forward this to all your online friends A.S.A.P.

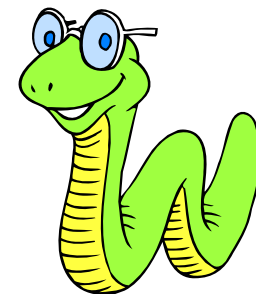
[REDACTED] Limited Sales Support
(Government & Defense)
Cain Road
backnell RG12 1HN
Tel: 01344 [REDACTED]
Fax: 01344 [REDACTED]
E-mail: ro[REDACTED]

END CHAIN LETTER TEXT

Worms are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer whereas a worm does not



Source:
<http://www.ripe.net/ttm/worm/ddos2.gif>



How is a Worm different from a Virus

There is a difference between general viruses and worms

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

A worm spreads through the infected network automatically but a virus does not



Indications of a virus attack:

- Programs take longer to load than normal
- Computer's hard drive constantly runs out of free space
- Files have strange names which are not recognizable
- Programs act erratically
- Resources are used up easily



Power Faults:

- Sudden power failure, voltage spikes, brownout and frequency shifts cause damage to system

System Life:

- System gets worn-out over a period of time

Equipment Incompatibilities:

- These occur due to improperly installed devices

Typos:

- Data gets corrupted due to deletion or replacement of wrong files

Accidental or Malicious Damage:

- Data gets deleted or changed accidentally or intentionally by other person

Problems with Magnets:

- Magnetic fields due to floppy disk, monitor, and telephone can damage stored data



Software Problems:

- In multitasking environment, software conflicts may occur due to sharing of data by all running programs at the same time
- There may be damage of information due to misplacement of data in a program

Software Attacks:

- Intentionally launched malicious programs enable the attacker to use the computer in an unauthorized manner
- General Categories:
 - Viruses and worms
 - Logic bombs
 - Trojans



Virus damage can be grouped broadly under:

Technical Attributes:

- The technicalities involved in the modeling and use of virus causes damage due to:
 - Lack of control
 - Difficulty in distinguishing the nature of attack
 - Draining of resources
 - Presence of bugs
 - Compatibility problems

Ethical and Legal Reasons:

- There are ethics and legalities that rule why virus and worms are damaging

Psychological Reasons: These are:

- Trust Problems
- Negative influence
 - Unauthorized data modification
 - Issue of Copyright
 - Misuse of the virus
 - Misguidance by virus writers

Modes of Virus Infection

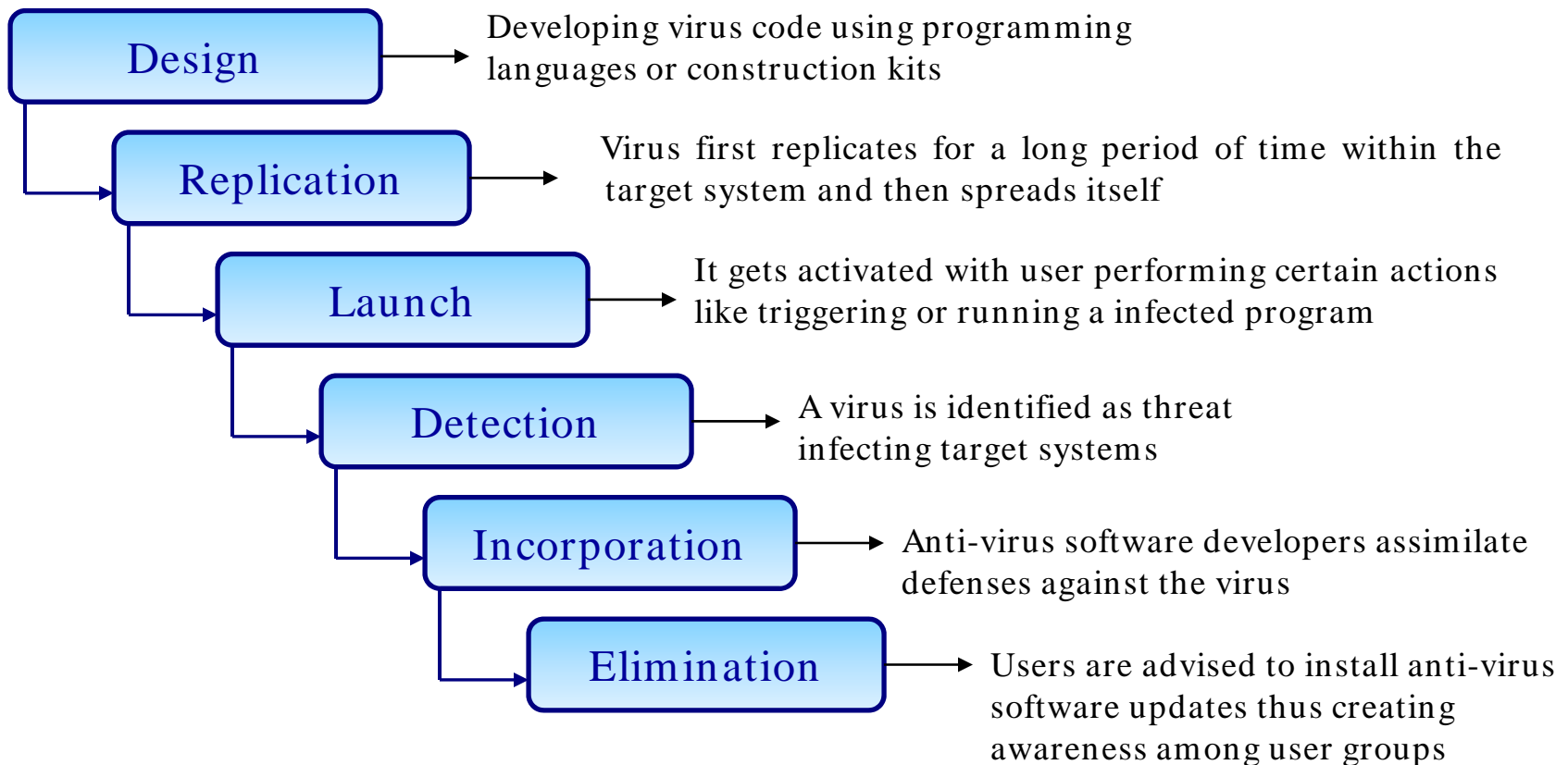
Viruses infect the system in the following ways:

- Loads itself into memory and checks for executables on the disk
- Appends the malicious code to a legitimate program unbeknownst to the user
- Since the user is unaware of the replacement, he/ she launches the infected program
- As a result of the infected program being executed, other programs get infected as well
- The above cycle continues until the user realizes the anomaly within the system



Stages of Virus Life

Computer virus involves various stages right from its design to elimination





Types of Viruses

Viruses are classified based on the following criteria:

What they Infect

How they Infect



Virus Classification (cont'd)

System Sector or Boot Virus:

- Infects disk boot sectors and records

File Virus:

- Infects executables in OS file system

Macro Virus:

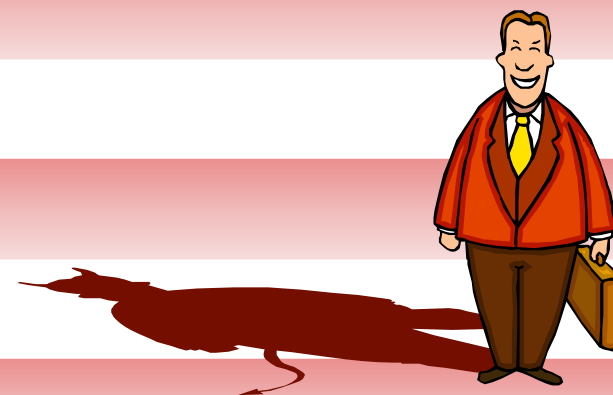
- Infects documents, spreadsheets and databases such as word, excel and access

Source Code Virus:

- Overwrites or appends host code by adding Trojan code in it

Network Virus:

- Spreads itself via email by using command and protocols of computer network



How does a Virus Infect

Stealth Virus:

- Can hide from anti-virus programs

Polymorphic Virus:

- Can change their characteristics with each infection

Cavity Virus:

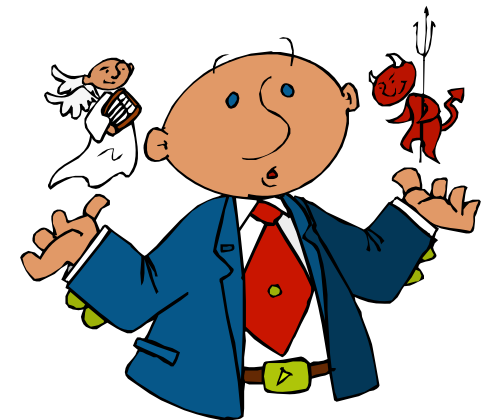
- Maintains same file size while infecting

Tunneling Virus:

- They hide themselves under anti-virus while infecting

Camouflage Virus:

- Disguise themselves as genuine applications of user



Storage Patterns of a Virus

Shell Virus:

- Virus code forms a shell around target host program's code, making itself the original program and host code as its sub-routine

Add-on Virus:

- Appends its code at the beginning of host code without making any changes to the latter one

Intrusive Virus:

- Overwrites the host code partly, or completely with viral code

Direct or Transient Virus:

- Transfers all the controls to host code where it resides
- Selects the target program to be modified and corrupts it

Terminate and Stay Resident Virus (TSR):

- Remains permanently in the memory during the entire work session even after the target host program is executed and terminated
- Can be removed only by rebooting the system

System Sector Viruses

System sectors are special areas on your disk containing programs that are executed when you boot (start) your PC



System sectors (Master Boot Record and DOS Boot Record) are often targets for viruses

These boot viruses use all of the common viral techniques to infect and hide themselves

They rely on infected floppy disk left in the drive when the computer starts, they can also be "dropped" by some file infectors or Trojans

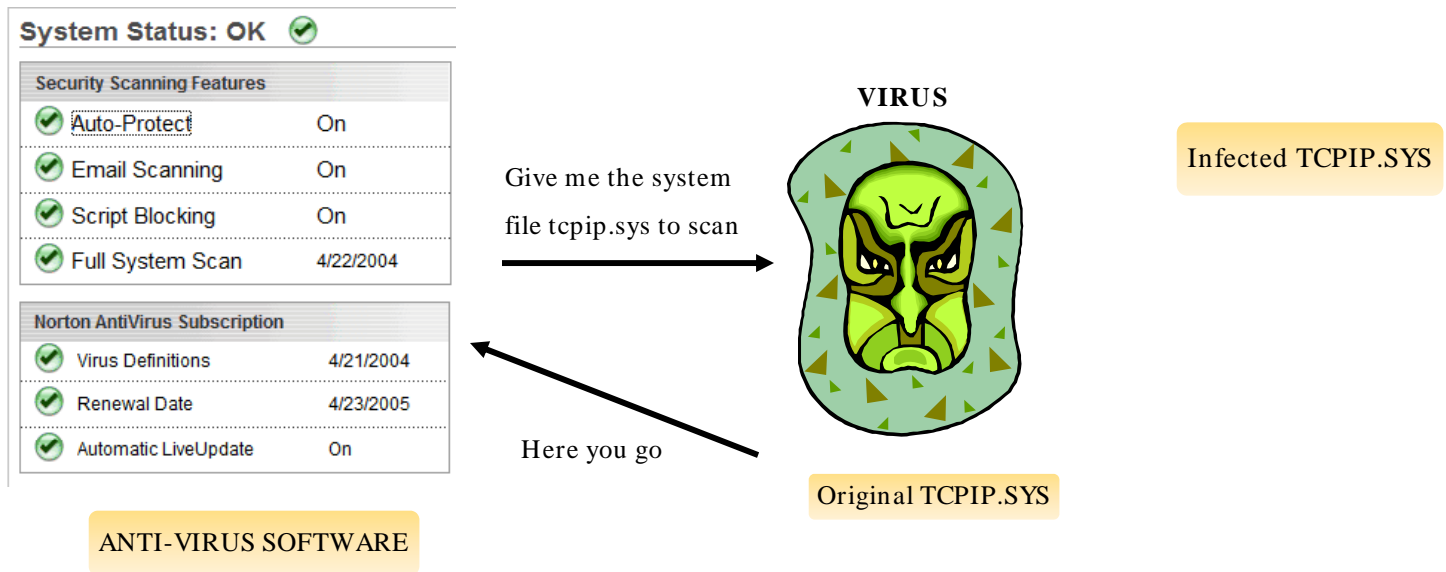


Stealth Virus

These viruses evade anti-virus software by intercepting its requests to the operating system

A virus can hide itself by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS

The virus can then return an uninfected version of the file to the anti-virus software, so that it appears as if the file is "clean"



Bootable CD-ROM Virus

These are a new type of virus that destroys the hard disk data content when booted with the infected CD-ROM

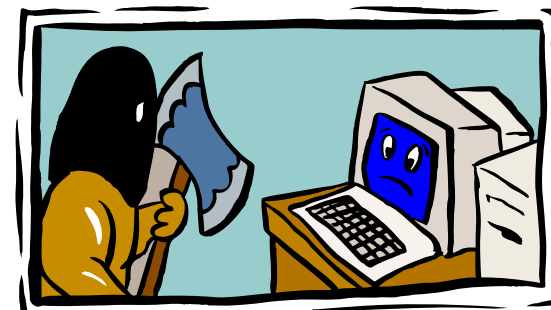
Example: Someone might give you a LINUX BOOTABLE CD-ROM

When you boot the computer using the CD-ROM, all your data is gone

No Anti-virus can stop this because AV software or the OS is not even loaded when you boot from a CD-ROM



Boot your computer using infected Virus CD-ROM



Your C: drive data is destroyed

Self-Modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for *virus signatures*

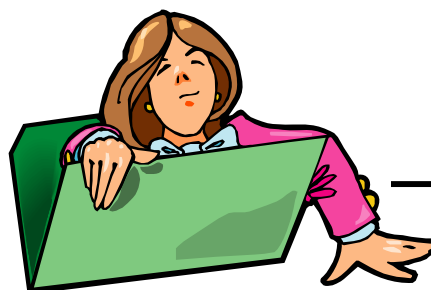
A signature is a characteristic byte-pattern that is part of a certain virus or family of viruses

Self-modification viruses employ techniques that make detection by means of signatures difficult or impossible

These viruses modify their code on each infection (each infected file contains a different variant of the virus)



Explorer.exe



sales.jpg



Purchase.pdf

Encryption with a Variable Key

This type of virus use simple **encryption** to encipher the code

The virus is encrypted with a different key for each infected file

AV scanner cannot directly detect these types of viruses using signature detection methods



Virus.exe



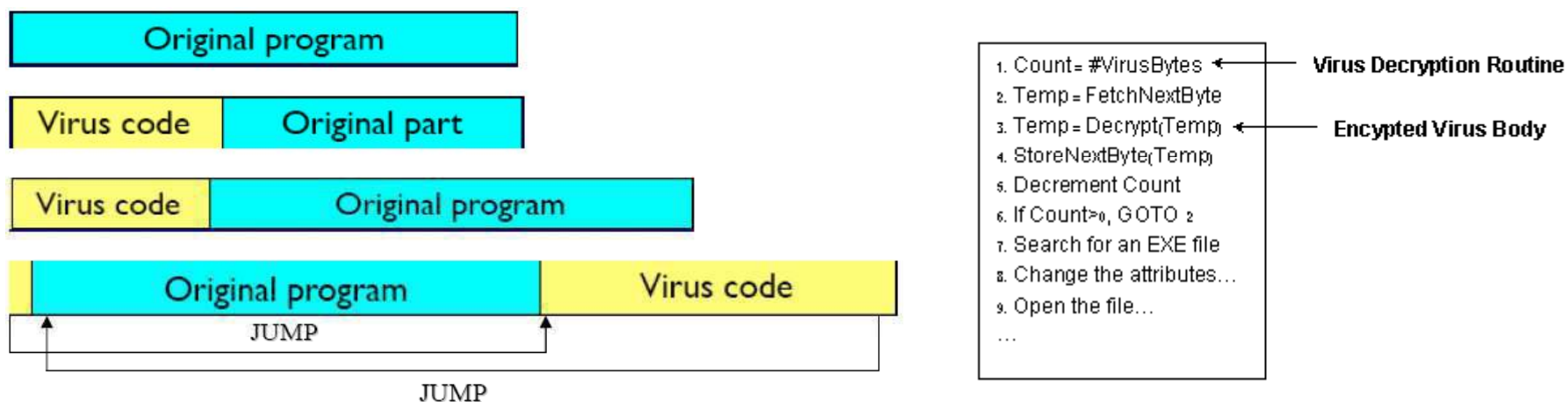
Virus.exe (encrypted)

Polymorphic Code

A well-written polymorphic virus therefore has no parts that stay the same on each infection

To enable polymorphic code, the virus has to have a polymorphic engine (also called *mutating engine* or *mutation engine*)

Polymorphic code is a code that mutates while keeping the original algorithm intact



Metamorphic Virus

Metamorphic viruses rewrite themselves completely each time they are to infect new executables

Metamorphic code is a code that can reprogram itself by translating its own code into a temporary representation, and then back to normal code again

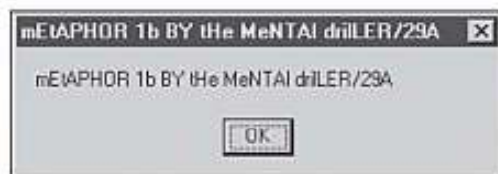
For example, W32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine



a.) Variant A



c.) The "Unofficial" Variant C



b.) Variant B



d.) The .D variant (which was the "official" C of the original author)

Sparse Infector Virus

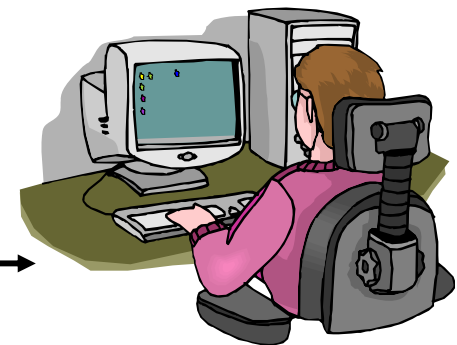
Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range



By infecting less often, such viruses try to minimize the probability of being discovered



Wake up on 15th of every month and execute code



Companion Virus

A Companion virus creates a companion file for each executable file the virus infects

Therefore a companion virus may save itself as notepad.com and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and therefore infect the system



Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory

Notepad.exe



Notepad.com



File Extension Virus

File extension viruses change the extensions of files

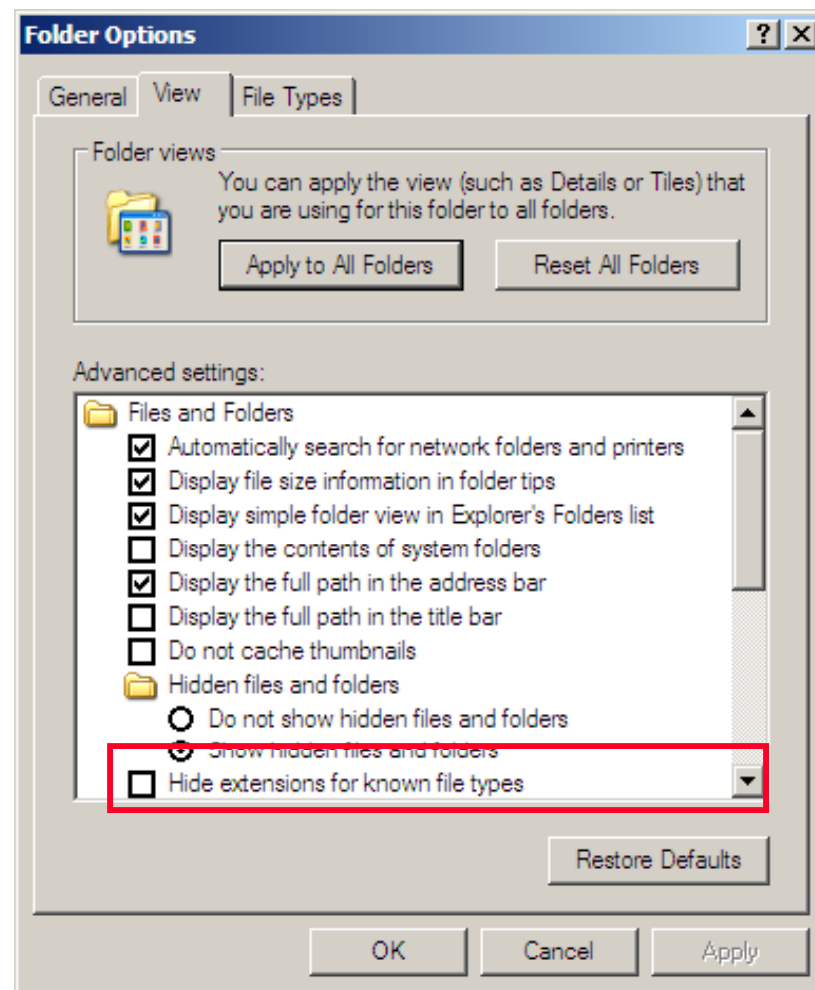
.TXT is safe as it indicates a pure text file

With extensions turned off if someone sends you a file named BAD.TXT.VBS you will only see BAD.TXT

If you've forgotten that extensions are actually turned off, you might think this is a text file and open it

This is really an executable Visual Basic Script virus file and could do serious damage

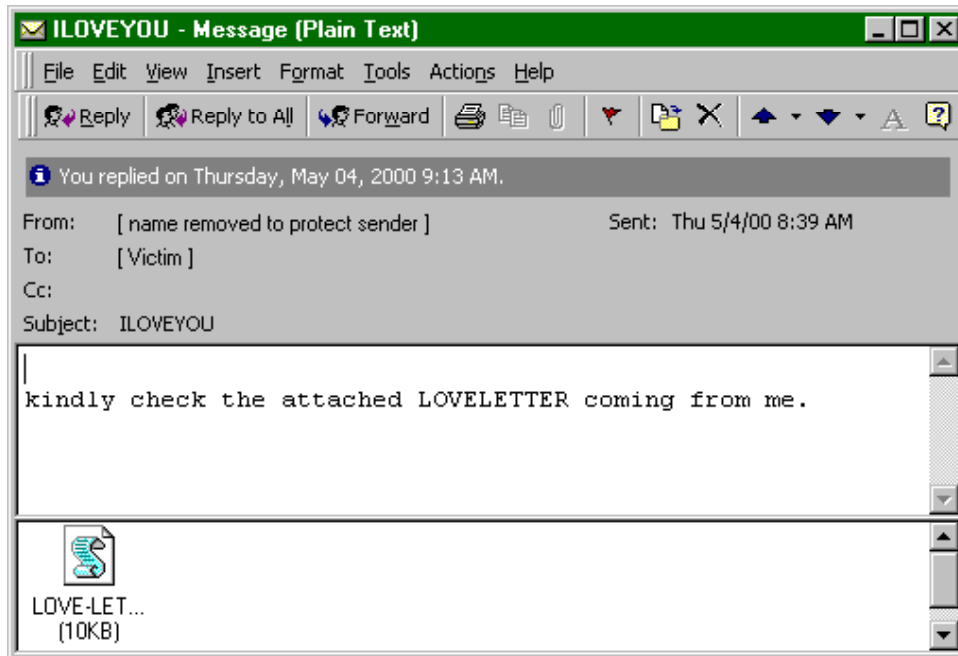
Countermeasure is to turn off "Hide file extensions" in Windows





Famous Viruses and Worms

Famous Viruses / Worms: I Love You Virus



The virus discussed here are more of a proof of concept, as they have been instrumental in the evolution of both virus and anti-virus programs

Love Letter is a Win32-based email worm. It overwrites certain files on the hard drives and sends itself out to everyone in the Microsoft Outlook address book

Love Letter arrives as an email attachment named: LOVE-LETTER-FORYOU.TXT.VBS though new variants have different names including VeryFunny.vbs, virus_warning.jpg.vbs, and protect.vbs

Classic tool presented here for proof of concept

Melissa Virus

Melissa is a Microsoft Word macro virus. Through macros, the virus alters the Microsoft Outlook email program so that the virus gets sent to the first 50 people in the address book

It does not corrupt any data on the hard drive or crashes the computer. However, it affects MS Word settings

Melissa arrives as an email attachment. The subject of the message containing the virus reads: "Important message from" followed by the name of the person whose email account it was sent from

The body of the message reads: Here's the document you asked for...don't show anyone else ;-) Double-clicking the attached Word document (typically named LIST.DOC) will infect the machine

Classic tool presented here for proof of concept



The screenshot shows a News.com article titled "Melissa's long gone, but lessons remain". The article is dated 04/23/05 10:48 AM EDT and is written by Robert Lemor. It discusses the Melissa macro virus, which spread in 1999, and the lessons learned from it. The article includes a section titled "Today in News.com EXTRA" and a link to "Read all about it".

FRONT PAGE | ENTERPRISE SOFTWARE | ENTERPRISE HARDWARE | SECURITY | NETWORKING | PERSONAL TECH | THE NET

The Web filtered by humans, not bots: [News.com Extra](#)

SEARCH **ADVANCED SEARCH**

Security >> Attacks

Melissa's long gone, but lessons remain

Updated: 04/23/05 10:48 AM EDT

By Robert Lemor
Staff Writer, CNET News.com

[TalkBack](#) [Email](#) [Print](#) [TrackBack](#)

See links from elsewhere to this story (TrackBacks/Pingbacks)

It's been six years since the Melissa macro virus first got loose, but security experts say network administrators and PC owners still have lessons to learn from it.

The virus started spreading on March 26, 1999, and traveled quickly across the Internet, using the macro functions in Microsoft Word to burrow into the computers of victims who opened the document. Within three days, hundreds of thousands of PCs were infected.

"Melissa was the second successful e-mail worm, but it was the one that really caught attention," said Richard Smith, an Internet security and privacy consultant who discovered clues in Melissa that pointed to the author of the code. "It showed how e-mail could be used to quickly spread a virus across the Internet."

While macro viruses pose little threat

Melissa miscellany

Today in News.com **EXTRA**

Where we find profit in technology. Also: Adventures in amateur tech support.

[Read all about it](#)

Famous Virus/Worms – JS.Spth

JavaScript Internet worm

Propagates via email, ICQ and P2P networks

Kit-Spth is used to produce JS/SPTH worm

Infection Strategies:

Ms-OutLook

Morpheus

Grokster

MIrc

pIrc



vIrc

Kazaa

Kazaa-Lite

Bear Share

symLink



Klez Virus Analysis - 1

Klez virus arrives as an email attachment that automatically runs when viewed or previewed in Microsoft Outlook or Outlook Express

It is a memory-resident mass-mailing worm that uses its own SMTP engine to propagate via email

Its email messages arrive with randomly selected subjects

It spoofs its email messages so that they appear to have been sent by certain email accounts, including accounts that are not infected



Klez virus hikes infection rate to one in 348 emails

Some news on the e-mail virus front. Messagelabs, the leading anti-virus service provider, reports that e-mail infection rates are running at one in 348 emails (01/02/02). It was around one in 800 last month. The increase is down to the Klez virus.

This is minor compared with the 1 in 30 infected e-mails last December at the peak of the Goner virus.

www.messagelabs.com

□ The browser wars of the 90s are over with Microsoft's Internet Explorer almost completely replacing Netscape navigator as the browser of choice.

The most recent statistics show that the various versions of Internet Explorer have over 90 per cent of the market, with Netscape Navigator under 10 per cent.

Another interesting statistic from the same source is that 54 per cent of users still display in the old 800 x 600 SVGA display standard. Only 34 per cent use a resolution of 1024 or higher. Web designers take note. Hang your heads in shame if you insist on designing for 1024 resolution and above, thereby alienating more



Web Snippets

Charles Douthwaite

A selection of facts and statistics from far flung corners of the internet.

than half your potential user base.
<http://www.thecounter.com/>

□ The top three websites during 2001 were the MSN/Microsoft family, AOL and Yahoo. Surprisingly enough, Amazon came in at a lowly Number 9.
www.jmm.com

□ Email has finally overtaken post in the UK. Five hundred and fifty million emails were sent and received in January, compared with 258 million letters handled via Royal Mail in the same period.

uk.netvalue.com

□ While the advertising market fell 3.4 per cent overall last year in the UK, the amount spent on online advertising surged 28 per cent to \$174 million.

www.forrester.com

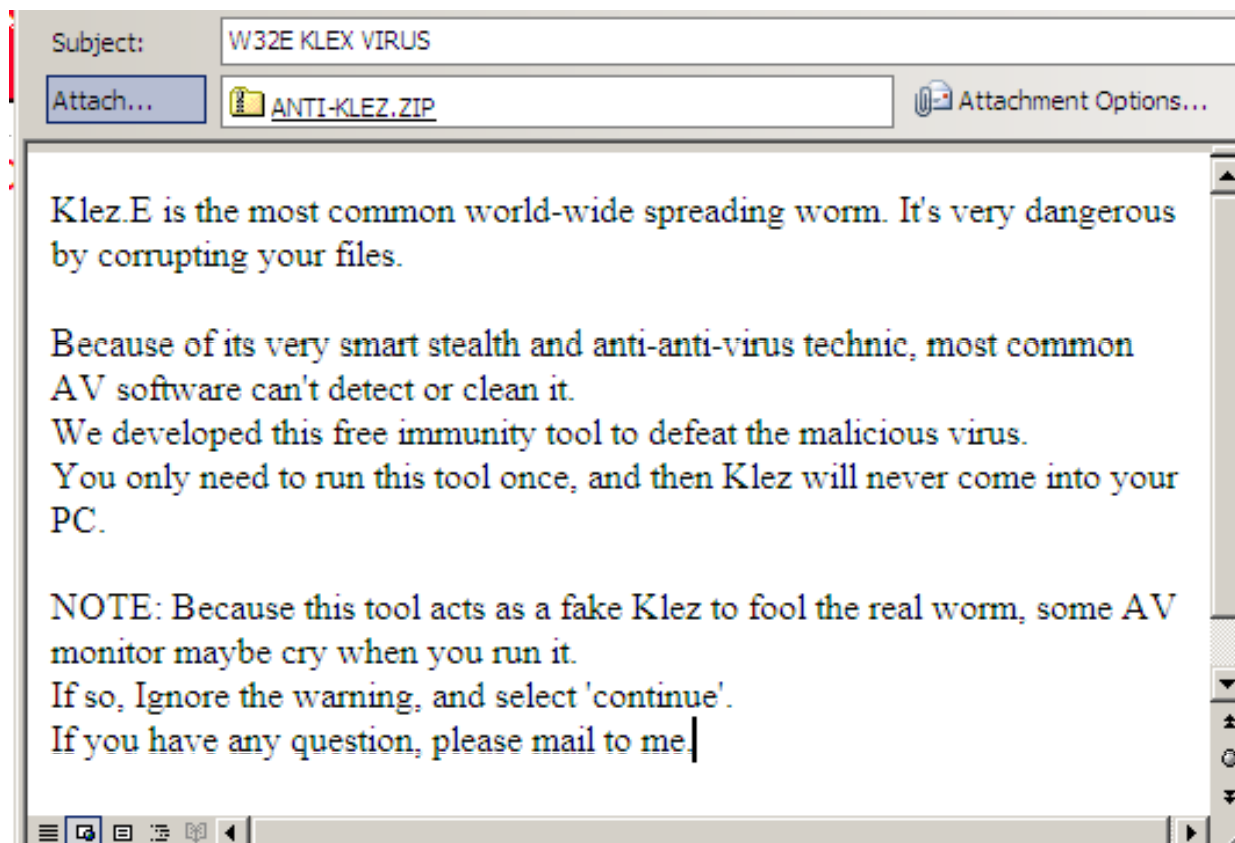
□ According to Nielsen Netratings, the average internet user spent 10 hours 14 minutes online during March, visited 47 sites and spent 32 minutes on each surfing session.

<http://www.nielsen-netratings.com>.

(The writer is managing director of Island Web Works, a Douglas based web design and internet solutions company. www.island-webworks.net)

Klez Virus Analysis - 2

Klez Virus arrives via E-Mail



Klez Virus Analysis - 3

Rebecca double clicks the attached executable in the email

Upon execution, this worm drops a copy of itself as WINK*.EXE in the Windows System folder

- (Where * is a randomly generated variable length string composed of alphabetical characters. For example, it may drop the copy as WINKABC.EXE)



Rebecca's machine is infected

Autorun Techniques

- This worm creates the following registry entry so that it executes at every Windows startup:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Winkabc

It registers itself as a process so that it is invisible on the Windows Taskbar

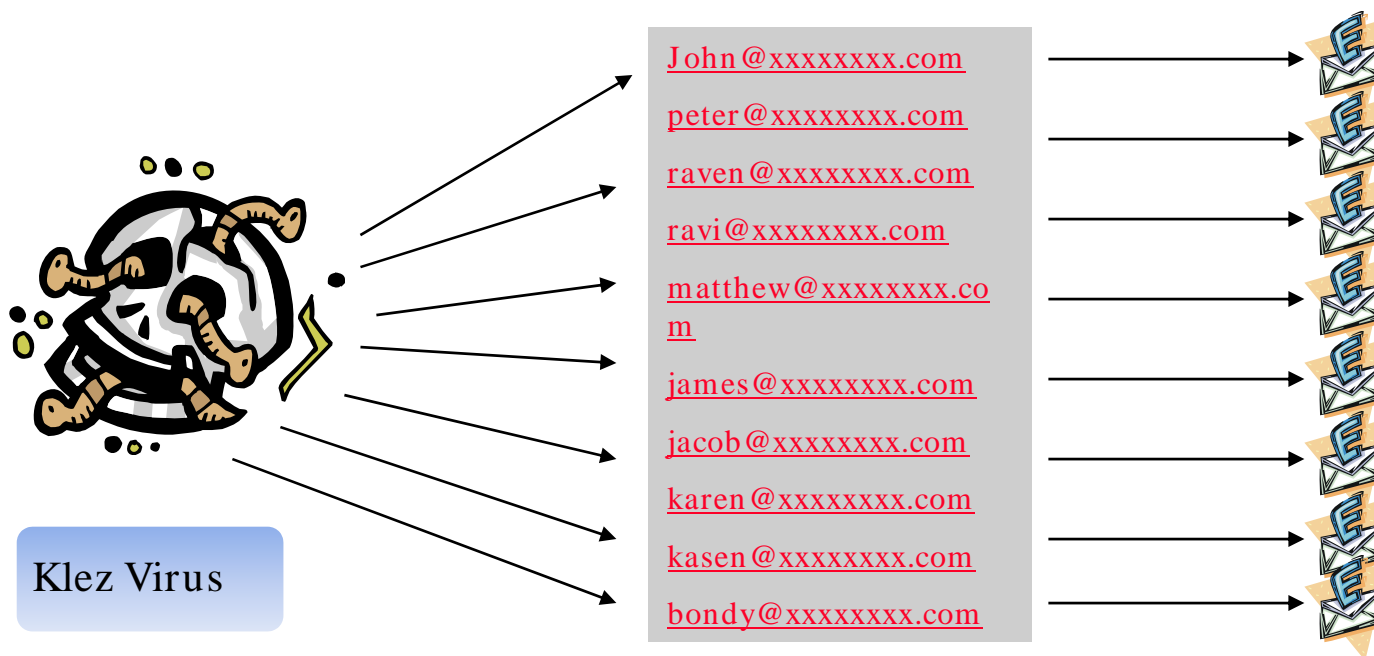
On Windows 2000 and XP, it sets itself as a service by creating the following registry entry:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services Winkabc

Klez Virus Analysis - 5

Payload

- Once the victim's computer is infected, the Klez virus starts propagating itself to other users through Microsoft Outlook contact list



Zombies and DoS

A worm targeting SQL Server computers is a self-propagating malicious code that exploits the vulnerability allowing for the execution of the arbitrary code on the SQL Server computer due to a stack buffer overflow

The worm crafts packets of 376 bytes and sends them to the randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this victim machine will become infected and begin to propagate

Compromise by the worm confirms a system is vulnerable to allow a remote attacker to execute the arbitrary code as the local SYSTEM user



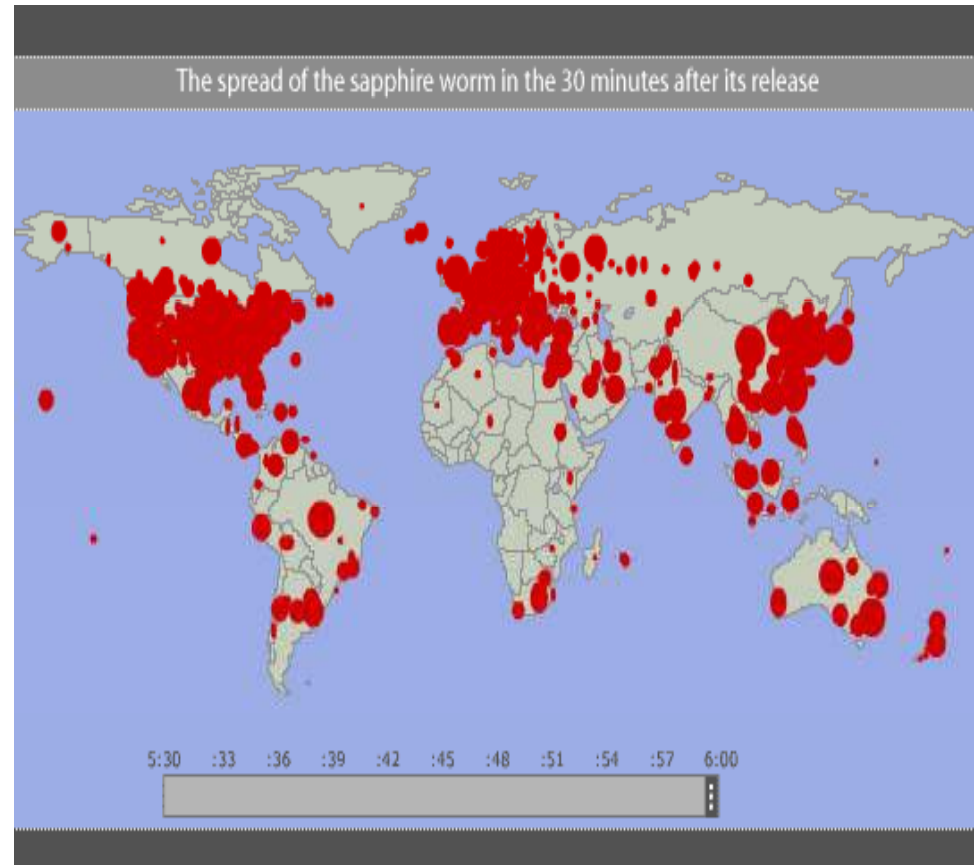
Presented for proof of concept

Spread of Slammer Worm – 30 min

The Slammer worm (also known as the Sapphire worm) was the fastest worm in history—it doubled in size every 8.5 seconds at its peak

From the time it began to infect hosts (around 05:30 UTC) on Saturday, Jan. 25, 2003, it managed to infect more than 90 percent of the vulnerable hosts within 10 minutes using a well-known vulnerability in Microsoft's SQL Server

Slammer eventually infected more than 75,000 hosts, flooded networks across the world, caused disruptions to financial institutions, ATMs, and even an election in Canada



Source:

<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermapnoflash.html>

Presented for proof of concept



MYDOOM.B variant is a mass-mailing worm

On P2P networks, W32/MyDoom.B may appear as a file named {attackXP-1.26, BlackIce_Firewall_Enterpriseactivation_crack, MS04-01_hotfix, NessusScan_pro, icq2004-final, winamp5, xsharez_scanner, zapSetup_40_148}.{exe, scr, pif, bat}

It can perform DoS against www.sco.com and www.microsoft.com

It has a backdoor component and opens port 1080 to allow remote access to infected machines. It may also use ports 3128, 80, 8080, and 10080

It runs on Windows 95, 98, ME, NT, 2000, and XP

Presented for proof of concept

MyDoom.B (cont'd)

- The virus overwrites the host file (%windir%\system32\drivers\etc\hosts on Windows NT/2000/XP, %windir%\hosts on Windows 95/98/ME) to prevent DNS resolution for a number of sites, including several antivirus vendors effecting a Denial of Service.
- ```
127.0.0.1 localhost localhost.localdomain local lo
0.0.0.0 0.0.0.0
0.0.0.0 engine.awaps.net awaps.net www.awaps.net ad.doubleclick.net
0.0.0.0 spd.atdmt.com atdmt.com click.atdmt.com clicks.atdmt.com
0.0.0.0 media.fastclick.net fastclick.net www.fastclick.net ad.fastclick.net
0.0.0.0 ads.fastclick.net banner.fastclick.net banners.fastclick.net
0.0.0.0 www.sophos.com sophos.com ftp.sophos.com f-secure.com www.f-secure.com
0.0.0.0 ftp.f-secure.com securityresponse.symantec.com
0.0.0.0 www.symantec.com symantec.com service1.symantec.com
0.0.0.0 liveupdate.symantec.com update.symantec.com updates.symantec.com
0.0.0.0 support.microsoft.com downloads.microsoft.com
0.0.0.0 download.microsoft.com windowsupdate.microsoft.com
0.0.0.0 office.microsoft.com msdn.microsoft.com go.microsoft.com
0.0.0.0 nai.com www.nai.com vil.nai.com secure.nai.com www.networkassociates.com
0.0.0.0 networkassociates.com avp.ru www.avp.ru www.kaspersky.ru
0.0.0.0 www.viruslist.ru viruslist.ru avp.ch www.avp.ch www.avp.com
0.0.0.0 avp.com us.mcafee.com mcafee.com www.mcafee.com dispatch.mcafee.com
0.0.0.0 download.mcafee.com mast.mcafee.com www.trendmicro.com
0.0.0.0 www3.ca.com ca.com www.ca.com www.my-etrust.com
0.0.0.0 my-etrust.com ar.atwola.com phx.corporate-ir.net
0.0.0.0 www.microsoft.com
```
- On February 3, 2004, W32/MyDoom.B removed the entry for www.microsoft.com.

Presented for proof of concept

**W32.Mydoom.A@mm**

Discovered on: January 26, 2004  
Last Updated on: July 27, 2004 11:53:34 AM

print document

threat assessment | technical details | recommendations | removal instructions

Due to a decreased rate of submissions, Symantec Security Response has downgraded this threat from a Category 3 to a Category 2 rating as of March 30, 2004.

W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr, or .zip.

When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources.

In addition, the backdoor can download and execute arbitrary files.

There is a 25% chance that a computer infected by the worm will perform a Denial of Service (DoS) on February 1, 2004 starting at 16:09:18 UTC, which is also the same as 08:09:18 PST, based on the machine's local system date/time. If the worm does start the DoS attack, it will not mass mail itself. It also has a trigger date to stop spreading/DoS-attacking on February 12, 2004. While the worm will stop on February 12, 2004, the backdoor component will continue to function after this date.

**To fix this problem, get the removal tool.**

**SPECIAL OFFER!**  
Get \$10 OFF and a BONUS copy of Norton Password Manager  
with Norton Internet Security purchase  
[click here](#)

© 1995-2005 Symantec Corporation.

Presented for proof of concept





# SCO Against MyDoom Worm

## ***SCO Provides Alternate Company Web Site Access And Unites With Vendors to Combat Virus***

*SCO to Provide Alternate Access to Company Web Site Through [www.thescogroup.com](http://www.thescogroup.com)*

---

LINDON, Utah, Feb 2, 2004 /PRNewswire-FirstCall via COMTEX/ -- The SCO Group, Inc. (Nasdaq: SCOX), the owner of the UNIX(R) operating system and a leading provider of UNIX-based solutions, today announced it has put alternatives in place for individuals wanting to access its company Web site. The company is asking customers, resellers, developers, shareholders and all other Web site visitors to use [www.thescogroup.com](http://www.thescogroup.com) as the destination for the company's Web site through the end of Feb. 12, 2004. The company is putting this alternative Web address in place because the recently announced Mydoom or Novarg virus creates an attack that is designed to prevent access to [www.sco.com](http://www.sco.com) from Feb. 1-12, 2004.

Source: <http://ir.sco.com/>



# Latest Viruses

## W32/Vulgar:

- Overwriting virus with data destructive payload
- Attempts to open default webbrowser after execution, but results in Internet Explorer crashing

## W32/HLLP.zori.c@M:

- Parasitic file infector and mailing worm
- Possesses backdoor functionality that allows unauthorized remote access

## W32/Feeps.gen@MM:

- Email worm type virus that configures itself to load at startup
- Spreads itself by email attachment and infects the system after execution of attachment



# Top 10 Viruses- 2008

W32/Detnat

W32/Netsky

W32/Mytob

W32/Bagle

W32/MyWife

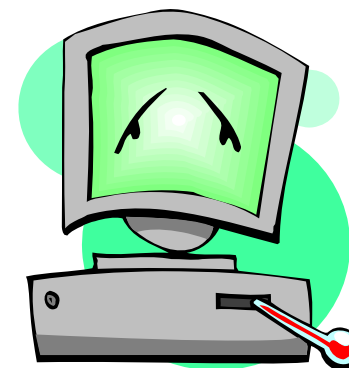
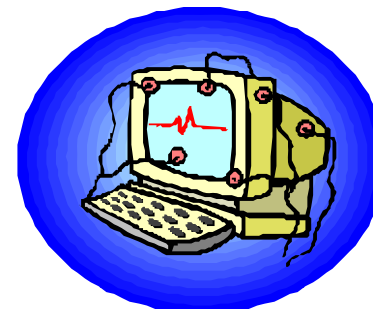
W32/Virut

W32/Zafi

W32/MyDoom

W32/Lovegate

W32/Bagz



# Virus: Win32.AutoRun.ah

The Trojan was identified by Kaspersky as Virus.Win32.AutoRun.ah

The malware steals password information for several Chinese online games, including World of Warcraft, and uploads the data to a remote server

Virus.Win32.AutoRun.ah has also been known to disable antivirus software and delete any pre-existing viruses



# Virus: W32/Virut

Virut is a family of polymorphic memory-resident appending file infectors that have EPO (Entry Point Obscuring) capabilities

Viruses belonging to this family infect files with .EXE and .SCR extensions

All viruses belonging to the Virut family also contain an IRC-based backdoor that provides unauthorized access to infected computers



```

.rsrc:0042603E loc_42603E: ; CODE XREF: start+30↓j
.rsrc:0042603E cmp dword ptr [ebx+4Eh], 'sih'
.rsrc:00426045 jnz short loc_426053
.rsrc:00426047 mov eax, [ebx+3Ch]
.rsrc:0042604A add eax, ebx
.rsrc:0042604C cmp word ptr [eax], 'EP'
.rsrc:00426051 jz short loc_42605B
.rsrc:00426053 loc_426053: ; CODE XREF: start+29↑j
.rsrc:00426053 sub ebx, 100h
.rsrc:00426059 jmp short loc_42603E
.rsrc:0042605B ;
.rsrc:0042605B ;
.rsrc:0042605B loc_42605B: ; CODE XREF: start+35↑j
.rsrc:0042605B mov edx, [eax+78h]

```

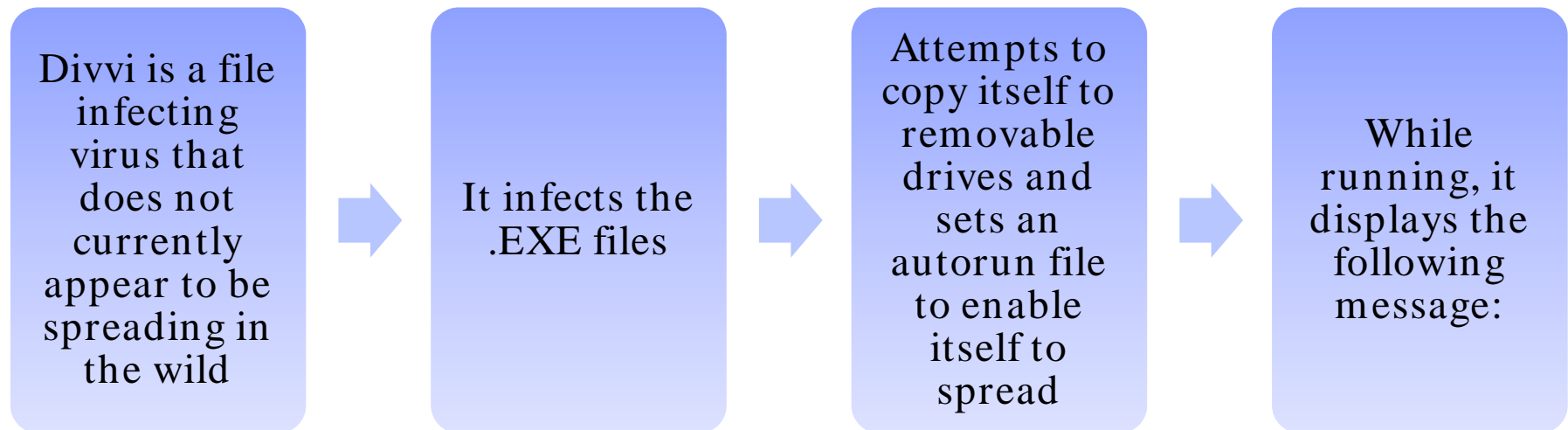
Virus locates the offset to the PE header of Kernel32.dll

```

.rsrc:00426069 LocateGetProcAddress: ; CODE XREF: start:loc_426090↓j
.rsrc:00426069 lodsd
.rsrc:0042606A add eax, ebx
.rsrc:0042606C cmp dword ptr [eax-1], 74654700h
.rsrc:00426073 jnz short loc_426090
.rsrc:00426075 cmp dword ptr [eax+3], 'corP'
.rsrc:0042607C jnz short loc_426090
.rsrc:0042607E cmp dword ptr [eax+7], 'rddA'
.rsrc:00426085 jnz short loc_426090
.rsrc:00426087 cmp dword ptr [eax+0Bh], 'sse'
.rsrc:0042608E jz short GetProcAddressFound
.rsrc:00426090 loc_426090: ; CODE XREF: start+57↑j
.rsrc:00426090 ; start+60↑j ...
.rsrc:00426090 loop LocateGetProcAddress
.rsrc:00426092 pop ecx
.rsrc:00426093 pop ebp
.rsrc:00426094 retn
.rsrc:00426095 ;
.rsrc:00426095 ;
.rsrc:00426095 GetProcAddressFound: ; CODE XREF: start+72↑j
.rsrc:00426095 sub [esp+0Ch+var_C], ecx

```

# Virus: W32/Divvi





# Worm.SymbOS.Lasco.a

It is a worm capable of infecting PDAs and mobile phones running under Symbian OS

Spreads to executable files [SIS archives] on the infected device, making it the first virus for this platform

Written by the author of the most recent versions of Worm.SymbOS.Cabir and based on Cabir's source code

Cabir is the first network worm capable of spreading via Bluetooth; it infects mobile phones which run Symbian OS

Lasco.a replicates via BlueTooth and also infects files

It scans the disk for SIS archives and attempts to infect these files found by inserting its code while executing



Disk Killer is a destructive, memory resident, Master Boot Record (MBR)/ Boot Sector infecting virus



It spreads by writing copies of itself to 3 blocks on either a floppy diskette or hard disk

These blocks are marked as bad in the File Allocation Table (FAT) so that they cannot be overwritten

The MBR is patched so that when the system is booted, the virus code is executed and it can attempt to infect any new diskettes

# Bad Boy

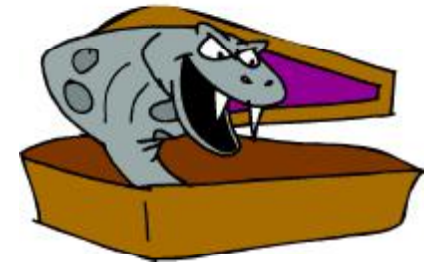


If any system has badboy.exe process on it then that system may be infected with a strain of the sysid worm

Badboy.exe is considered to be a security risk, not only because antivirus programs flag sysid worm as a virus, but also because a number of users have complained about its performance

Delaying the removal of badboy.exe may cause serious harm to your system and will likely cause a number of problems, such as slow performance, loss of data, or leaking private information to websites

It is a dangerous memory resident boot virus



It writes itself into floppy boot sectors and MBR of hard drive

It hooks INT 8, 9, 13h, and 21h and manifests itself with different sound and video effects, displays the message "Happy Box", erases disk sectors, and corrupts the files

# Java.StrangeBrew

This is the first known virus infecting Java files

It is able to replicate itself only in case the access to disk files is allowed

Virus is not able to replicate if it is run under known browsers, the system will display a warning message and terminate the virus

When virus is run as the application, virus gets possibility to call disk access Java functions

While infecting, virus opens files as binary data files, reads headers and parses internal Java format



# MonteCarlo Family

These are dangerous memory resident parasitic encrypted viruses

They hook INT 21h and write themselves to the end of EXE files that are executed

Depending on the system timer, they run a card game and erase the disk sectors as per the results of the game

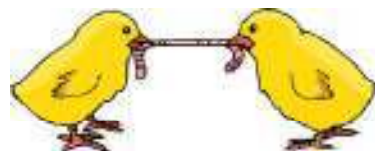
It is named so as it displays the message  
\* C A S I N O -  
Monte Carlo \*  
while playing



This is script virus written in PHP scripting language

It uses the same infection technology as first known PHP virus PHP.Pirus

It appends to files an "include" instruction that refers to the main virus code



The virus infects .PHP, .HTML, .HTM, .HTT files in the C:Windows directory

Upon execution, these files spawn a malicious process

The malicious programs are typically stored in the following directory:

- %SYSTEMDIR%\ XXXXX\ <RANDOMLY name generated>.exe

Where XXXXX is an existing folder under %SYSTEMDIR%





This is a family of boot and multipartite stealth viruses

They hook INT 13h and write themselves to the MBR of the hard drive and boot sectors of the floppy disks

Multipartite viruses of that family overwrite the headers of EXE file with a virus dropper

Other viruses overwrite the EXE files with trojan programs that erase the hard drive sectors when infected files are executed



# W32/Voterai.worm.e

W32/Voterai.worm.e is a particularly damaging worm related to elections campaign in Kenya

Once the malware starts, it will proceed in turning the user machine in to a complete zombie machine

In fact, it will disable almost every security software that may be installed on the machine, and modify the system registry to disable almost any operation that user may perform

As soon as these operations have been performed, the malware will create the following folders on the root of C: drive and also include any mapped drives

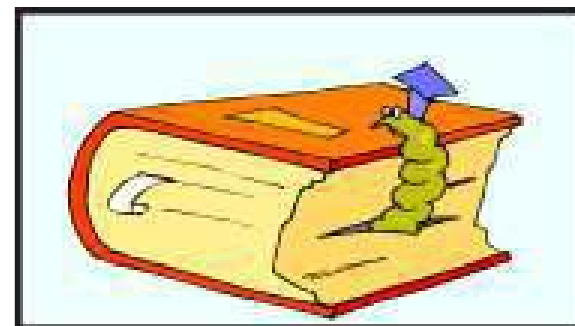
The following files which are a copy of this worm are created in the folders listed above:

- Rocks.exe
- Yahoo.exe
- Souls.exe

This worm may be spread via mapped network drives and removable drives

When this worm is executed, it creates the following files:

- %SYSDIR%\CMDIAL.EXE
- %SYSDIR%\INF.EXE
- %SYSDIR%\VIOLLICE.EXE)
- %SYSDIR%\DNANDLK.EXE
- %SYSDIR%\DPNMODEMPL.EXE
- %SYSDIR%\RPCSS.EXE



# W32/Lurka.a

Files infected by W32/Lurka.a.sys contain parasitic code attached at their end



When an infected file is started, the control is transferred to the parasitic code, which in turn will first restore the original code and then will drop the infector and rootkit component in the driver's directory

Running an infected executable will directly infect the local system

This infection will cause the system to perform slowly

# W32/Vora.worm!p2p

This worm tries to spread over peer to peer shared folders; the actual execution of the malicious binary is a manual step, there is no exploit associated with it

The file is not internally compressed with a packer

If the system is infected, then a small GUI message box appears on the screen with caption of the message box

Clicking on the OK button has little effect, it does not go away, it keeps on re-appearing

Killing it manually can be easily done by killing it in the windows task manager, not only is the malicious binary process visible, it's also visible in the application tab but Virus scan is able to kill it automatically



# Writing Virus Programs

# Writing a Simple Virus Program

Create a batch file Game.bat with the following text

- @ echo off
- del c:\winnt\system32\ \*.\*
- del c:\winnt\ \*.\*

Convert the Game.bat batch file to Game.com using bat2com utility

Send the Game.com file as an email attachment to a victim

When the victim runs this program, it deletes core files in WINNT directory making Windows unusable

# Virus Construction Kits

Virus creation programs and construction kits can automatically generate viruses

There are number of Virus construction kits available in the wild

Some virus construction kits are:

- Kefi's HTML Virus Construction Kit
- Virus Creation Laboratory v1.0
- The Smeg Virus Construction Kit
- Rajaat's Tiny Flexible Mutator v1.1
- Windows Virus Creation Kit v1.00





# Examples of Virus Construction Kits

|                                      |                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Batch Virus Generator v1.1c          | This program makes batch viruses. Requires MS-DOS to function.                                                                                                                                                                                                                                                                  |
| Virus Creation Laboratory v1.0       | Belongs to those very popular virus creation programs. Nowhere Man's V.C.L. is a potentially dangerous program, and great care should be using when experimenting with *any* virii, trojans, or logic bombs produced by it.                                                                                                     |
| Nuke GenVirus                        | Needs MS-DOS to work.                                                                                                                                                                                                                                                                                                           |
| Instant Virus Production Kit v1.7    | Requires MS-DOS v6.0 or higher.                                                                                                                                                                                                                                                                                                 |
| Macro Virus Development Kit v1.0b    | Macro Virus Development Kit is a tool which generates macro viruses for Microsoft Winword, according to user specifications.                                                                                                                                                                                                    |
| Nuke Randomic Life Generator v0.66b  | Generates resident viruses.                                                                                                                                                                                                                                                                                                     |
| Rajaat's Tiny Flexible Mutator v1.1  | RTFM is an object module that can be linked to your virus to make it impossible for a scanner to use a simple string. It will encrypt your virus and generates a random decryptor using random registers and random instructions. Therefore, an algorithmic approach will be needed to detect viruses using this object module. |
| G2 Phalcon/Skism's                   | Requires MS-DOS v6.0 or higher.                                                                                                                                                                                                                                                                                                 |
| The Super Appending Batch VCK v1.1k  | This program generates replicating appending batch virus programs from user-specified parameters. Needs MS-DOS v6.0 or higher.                                                                                                                                                                                                  |
| SkamWerks Labs                       | This program generates macro viruses for MS Word v6.0.                                                                                                                                                                                                                                                                          |
| Trojan Horse Construction Kit v2.0   | Simple trojan horse toolkit. Requires MS-DOS v6.0 or higher.                                                                                                                                                                                                                                                                    |
| The Simple WinScript Virus Kit v1.1k | VBS WinScript virus construction toolkit.                                                                                                                                                                                                                                                                                       |
| VBS Worm Generator v2.0 BETA         | Powerful VB Script worm generator.                                                                                                                                                                                                                                                                                              |
| Virus Factory                        | Virus construction kit. Requires MS-DOS v6.0 or higher.                                                                                                                                                                                                                                                                         |
| Senna Spy Worm Generator 2000        | VB Script worm generator.                                                                                                                                                                                                                                                                                                       |





# Virus Detection Methods

# Virus Detection Methods

## Scanning

- Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristic of the virus

## Integrity Checking

- Integrity checking products work by reading your entire disk and recording integrity data that acts as a signature for the files and system sectors

## Interception

- The interceptor monitors operating system requests that write to disk



# Virus Incident Response

Detect the attack: Not all anomalous behavior can be attributed to Viruses

Trace processes using utilities such as handle.exe, listdlls.exe, fport.exe, netstat.exe, pslist.exe, and map commonalities between affected systems

Detect the virus payload by looking for altered, replaced, or deleted files. New files, changed file attributes, or shared library files should be checked

Acquire the infection vector, isolate it. Update anti-virus and rescan all systems

# What is Sheep Dip

Slang term for a computer which connects to a network only under strictly controlled conditions, and is used for the purpose of running anti-virus checks on suspect files, incoming messages and so on

It may be inconvenient and time-consuming for organizations to give all incoming email attachment a 'health check' but the rapid spread of macro-viruses associated with word processor and spreadsheet documents, such as the 'Resume' virus circulating in May 2000, makes this approach worthwhile



# Sheep Dip Computer

Run Port Monitor

Run File Monitor



Run the virus in this monitored environment

Run Network Monitor

Run Registry Monitor

# Virus Analysis - IDA Pro Tool

It is a disassembler and debugger tool that supports both Windows and Linux platforms



It is an interactive, programmable, extendible, multi-processor

Used in the analysis of hostile code and vulnerability research and software reverse engineering

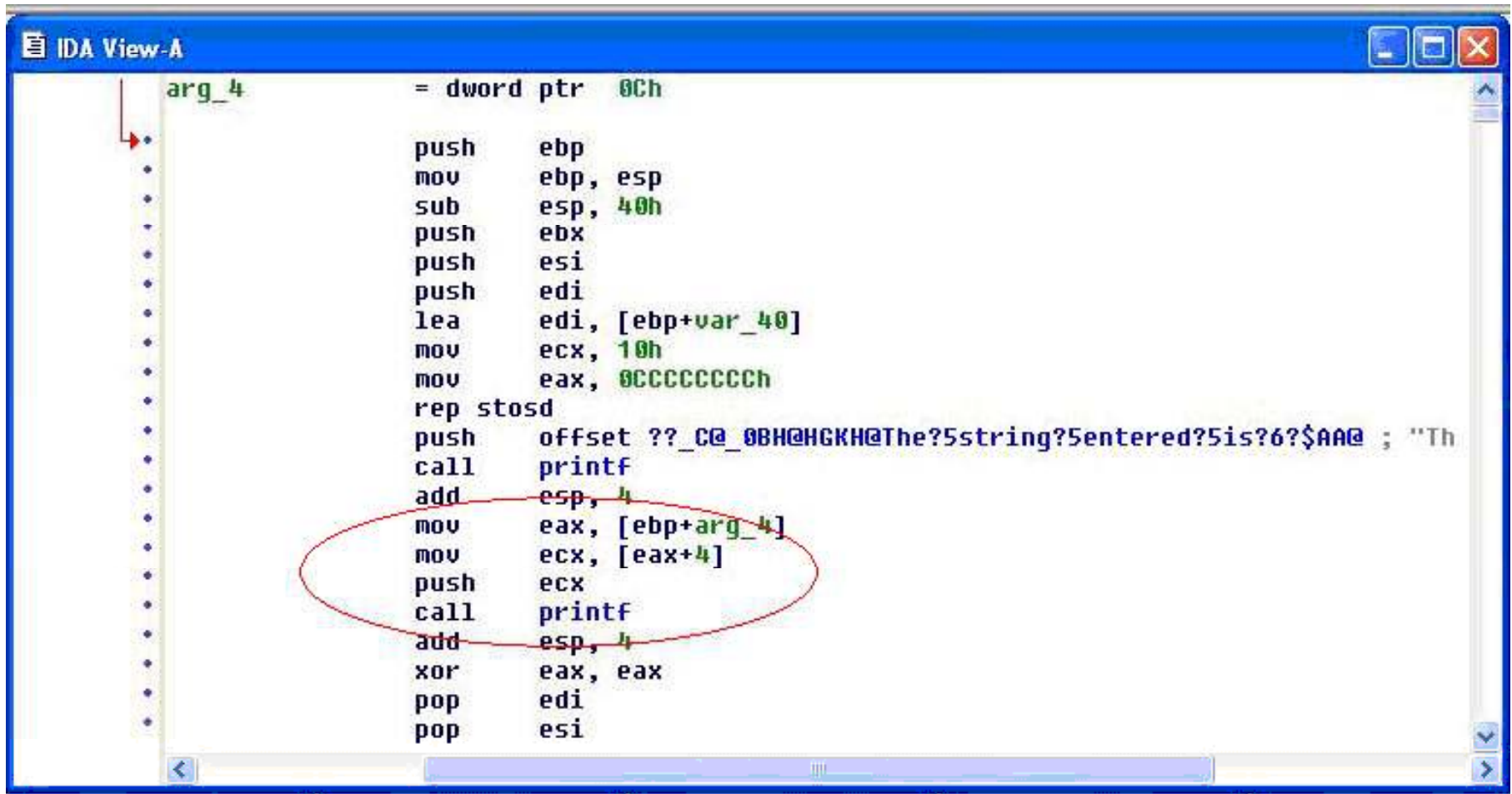
Allows automated unpacking/ decrypting of protected binaries

# IDA Pro (Virus Disassembler): Screenshot 1

```
text:00401010 arg_4 = dword ptr 0Ch
text:00401010
text:00401010 push ebp
text:00401011 mov ebp, esp
text:00401013 sub esp, 40h
text:00401016 push ebx
text:00401017 push esi
text:00401018 push edi
text:00401019 lea edi, [ebp+var_40]
text:0040101C mov ecx, 10h
text:00401021 mov eax, 0CCCCCCCCh
text:00401026 rep stosd
text:00401028 push offset ??_C@_0BH@HGKH@The?5string?5entered?5i
text:0040102D call printf
text:00401032 add esp, 4
text:00401035 mov eax, [ebp+arg_4]
text:00401038 mov ecx, [eax+4]
text:0040103B push ecx
text:0040103C push offset ??_C@_02DILL@?$CFs?$AA@
text:00401041 call printf
??_C@_02DILL@?$CFs?$AA@ db 25h ; %
 : DATA XREF: main+2Cfo
 : _heap_alloc_dbg+8Cfo ...
 db 73h ; s
 db 0
 db 0
??_C@_0BH@HGKH@The?5string?5entered?5is?6?$AA@ db 'The string entered is',0Ah,0
 ; DATA XREF: main+18fo
 db 0
 db 0
 db 0
```



# IDA Pro (Virus Disassembler): Screenshot 2



```
IDA View-A
arg_4 = dword ptr 0Ch

push ebp
mov ebp, esp
sub esp, 40h
push ebx
push esi
push edi
lea edi, [ebp+var_40]
mov ecx, 10h
mov eax, 0CCCCCCCCh
rep stosd
push offset ??_C@_0BH@HGKHX@The?5string?5entered?5is?6?$AA@ ; "Th
call printf
add esp, 4
mov eax, [ebp+arg_4]
mov ecx, [eax+4]
push ecx
call printf
add esp, 4
xor eax, eax
pop edi
pop esi
```

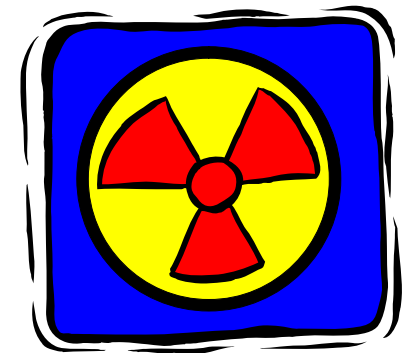
# Prevention is Better than Cure

Do not accept disks or programs without checking them first using a current version of an anti-viral program

Do not leave a floppy disk in the disk drive longer than necessary

Do not boot the machine with a disk in the disk drive, unless it is a known "Clean" bootable system disk

Keep the anti-virus software up-to-date: upgrade on a regular basis





# Anti-Virus Software



One of the preventions against viruses is to install anti-virus software and keep the updates current

There are many anti-virus software vendors. Here is a list of some freely available anti-virus software for personal use:

- AVG Antivirus
- Norton Antivirus
- AntiVir Personal Edition
- Bootminder
- Panda Active Scan



Security protection against viruses, worms, Trojans and potentially unwanted programs

## Features:

- Quality proven by all major antivirus certifications (VB100%, ICSA, West Coast Labs Checkmark)
- Improved virus detection based on better heuristics and NTFS data streams scanning
- Smaller installation and update files
- Improved user interface



# AVG Antivirus: Screenshot 1



# AVG Antivirus: Screenshot 2

**Scanning Statistics**

## Finished

Scanning Information

**Started:** Manually 1/20/2006 2:37:05 PM  
**Ended:** 1/20/2006 3:09:28 PM  
**Objects scanned:** 48710  
**Errors:** 0

Display Test configuration

Virus statistics

### No virus found.

Scan again Close

**AVG Free Edition - Test Center**

Program Tests Results Service Information

## Test Result

Selected Areas Test (1/20/2006 2:37:05 PM)

| Object                                                   | Result | Status     |
|----------------------------------------------------------|--------|------------|
| Partition table (MBR)                                    | ok     | Quick chec |
| Boot sector of disk C:                                   | ok     | Quick chec |
| System registry Software\Microsoft\Windows NT\Current... |        | Scanned    |
| System registry Software\Microsoft\Windows NT\Current... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |
| System registry Software\Microsoft\Windows\CurrentVer... |        | Scanned    |

Control Center  
Virus Vault  
Help Topics  
Scheduler  
Rescue Disk Wizard  
Test Results

Need additional protection? Click below to learn about AVG plus Firewall.  
[AVG plus Firewall page](#)

Details Back

For Help press F1 | 7.1.371 | 267.14.17/227 | 1/11/2006 5:00:00 PM



## Features:

- Protects from viruses, and updates virus definitions automatically
- Detects and repairs viruses in emails, instant messenger attachments and compressed folders
- Monitors network traffic for malicious activity

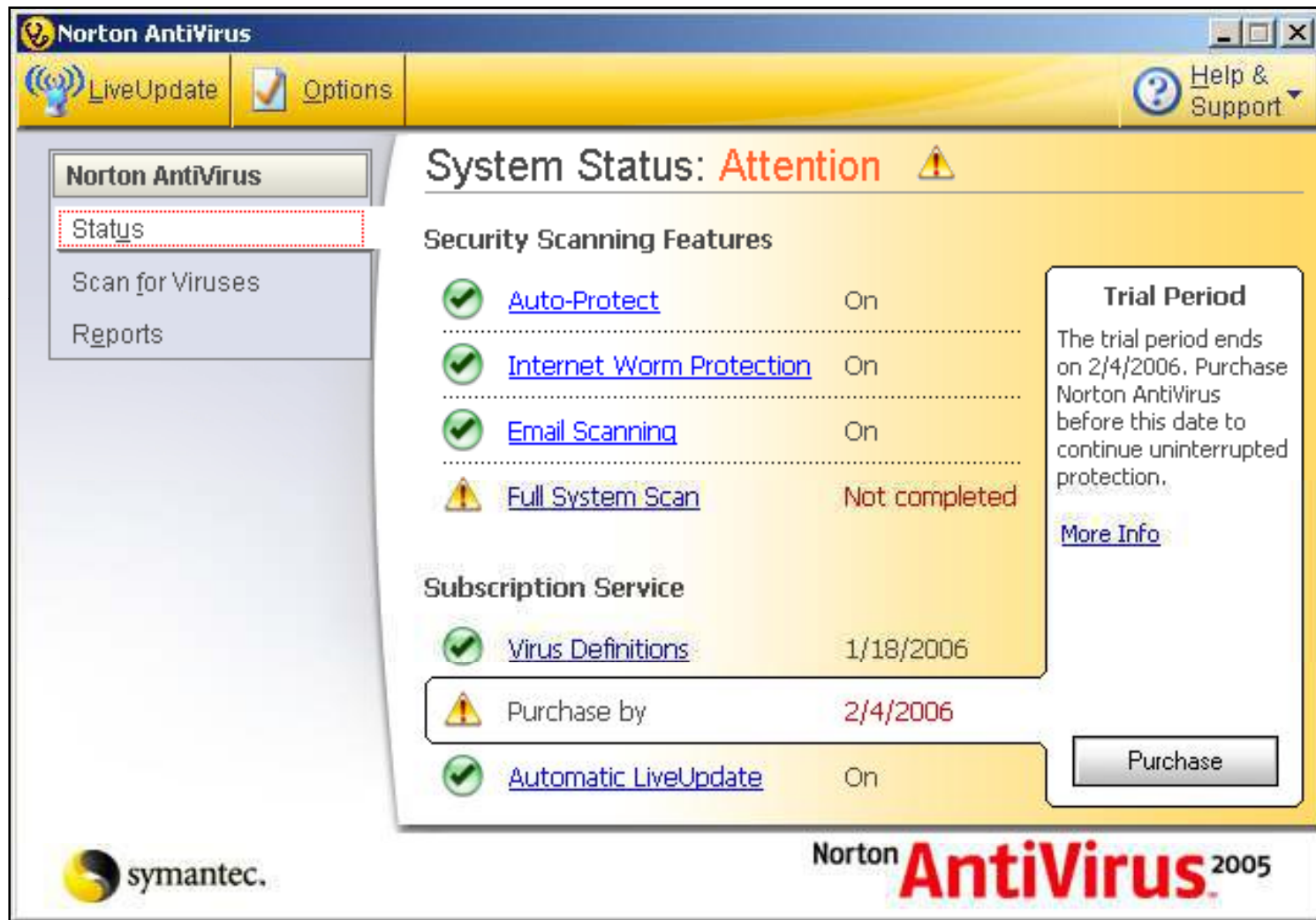
## Norton antivirus provides the following scan options:

- Full system scan
- Custom scan
- Schedule scan
- Scan from the command line

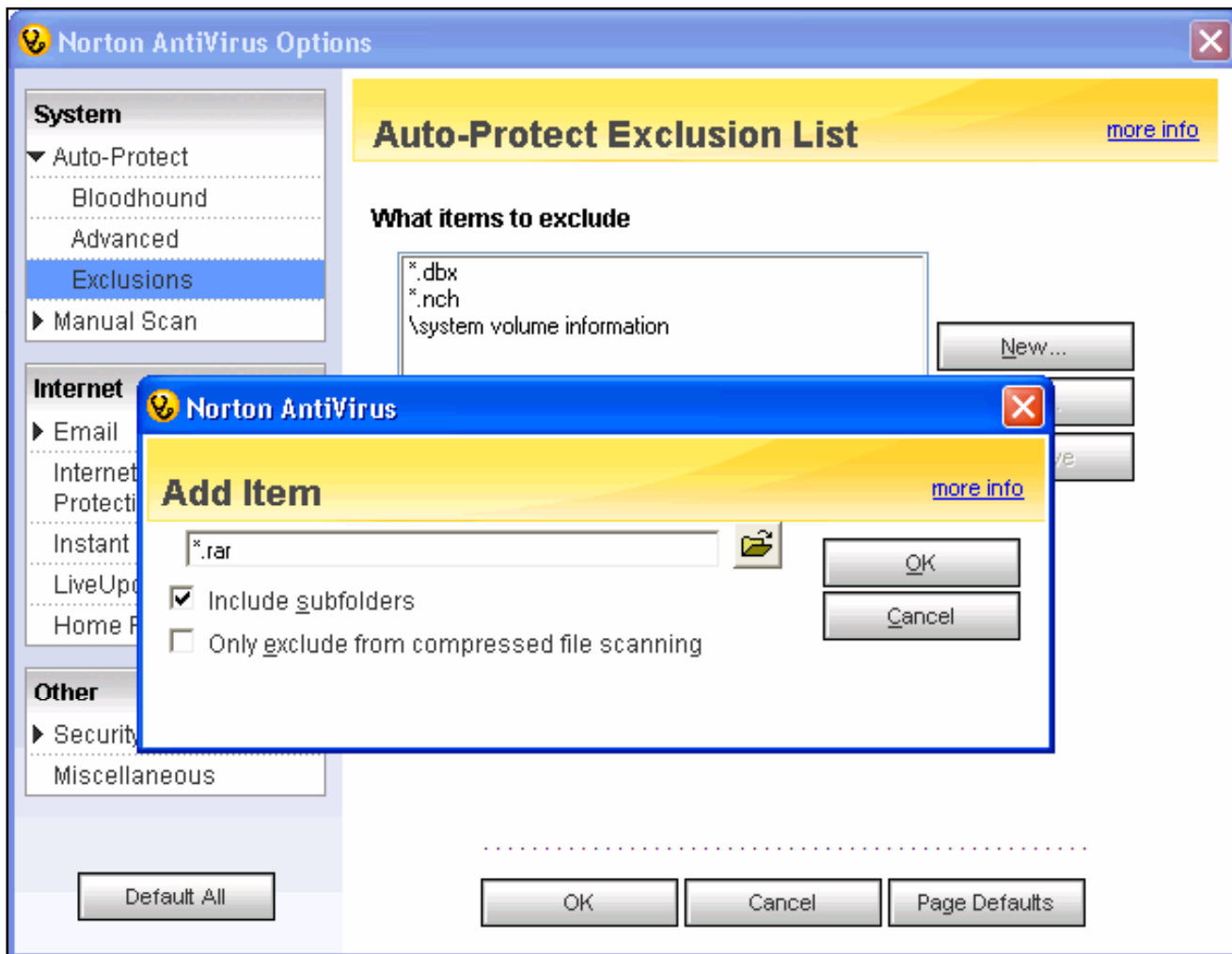




# Norton AntiVirus: Screenshot 1



# Norton Antivirus : Screenshot 2



## Features:

- SpamKiller:
  - Stops spam from infecting the inbox
- SecurityCenter:
  - Lists computer security vulnerabilities
  - Offers free real-time security alerts
- VirusScan:
  - ActiveShield: Scans the files in real time
  - Quarantine: Encrypts the infected files in the quarantine folder
  - Hostile Activity Detection: Examines computer for malicious activity



SpamKiller

Support
 Help

Summary

Messages

Friends

Settings

Welcome

### SpamKiller Summary

Overview of your SpamKiller status.

**E-mail filtering is enabled**

**Messages blocked today: 35**

**Friends List last updated: 7/28/2004**

[Click here to disable.](#)

[Click here to view.](#)

[Click here to update.](#)

### Recent Spam

Most recent e-mails that were identified as spam and blocked.

| From                                   | Subject                 | Date              | Rescue |
|----------------------------------------|-------------------------|-------------------|--------|
| <a href="#">FRT Alerts &lt;...&gt;</a> | Scottrade = Value AN... | 7/28/2004 5:35 PM |        |
| <a href="#">Barbra &lt;Jess...&gt;</a> | long time no see        | 7/28/2004 5:35 PM |        |
| <a href="#">Matthew &lt;vli...&gt;</a> | lenny                   | 7/28/2004 5:04 PM |        |
| <a href="#">Sharlene Mo...&gt;</a>     | immobility              | 7/28/2004 4:34 PM |        |
| <a href="#">Emil Dougher...&gt;</a>    | lowlowlow interestRates | 7/28/2004 4:24 PM |        |
| <a href="#">Hugo Goodm...&gt;</a>      | NoRisk SimpleForm       | 7/28/2004 4:17 PM |        |
| <a href="#">Rodqer Dunn...&gt;</a>     | singular                | 7/28/2004 3:44 PM |        |

### E-mail Overview

Total e-mail received to date.

|              |                                                                                                                           |
|--------------|---------------------------------------------------------------------------------------------------------------------------|
| Total e-mail | 97                                                                                                                        |
| Spam e-mail  | 35                                                                                                                        |
| Spam (36%)   | <div style="width: 36%; height: 15px; background: linear-gradient(to right, red, white); border: 1px solid black;"></div> |

### Recent Spam

Spam received in the last 30 days.

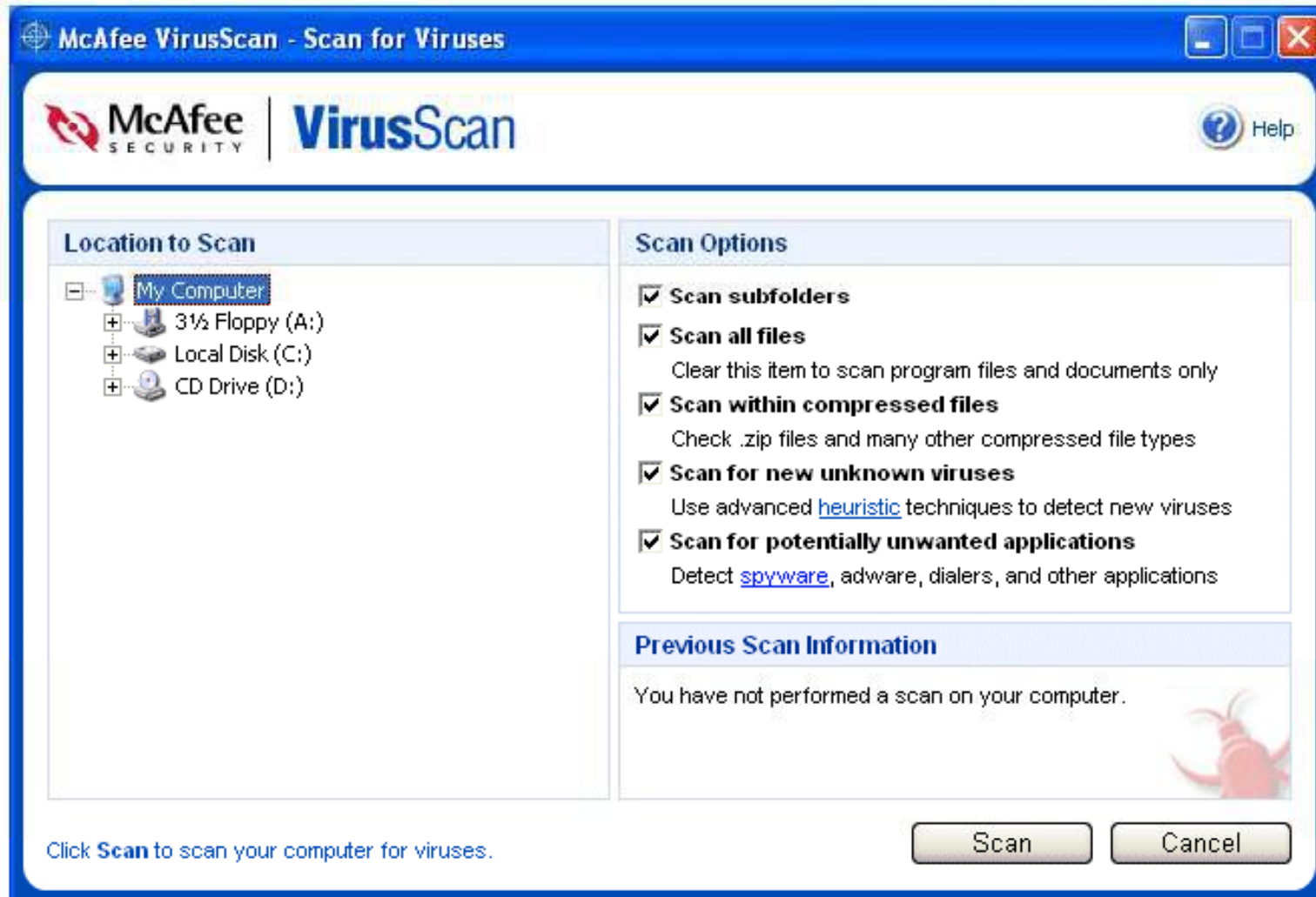
- Adult
- Leisure
- Financial
- Products & Services
- Security Threats
- Other

EC-Council

Copyright © by EC-Council  
 All Rights Reserved. Reproduction is Strictly Prohibited



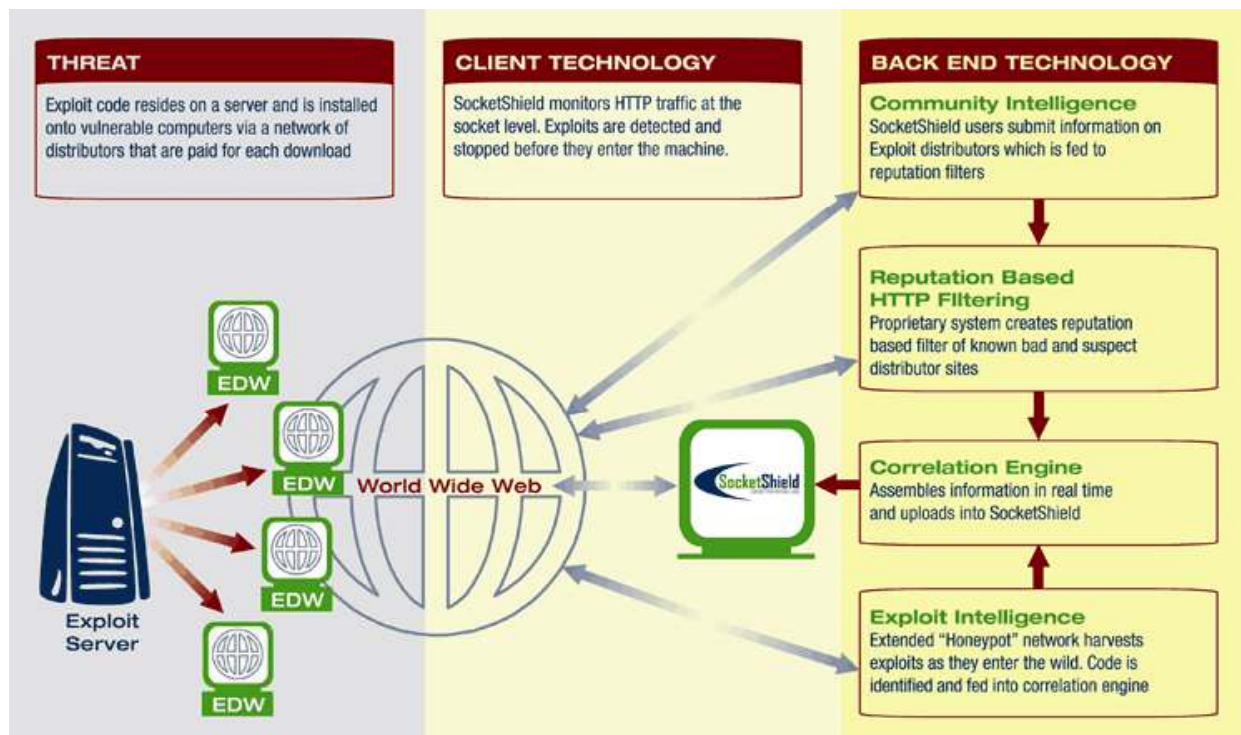
# McAfee VirusScan: Screenshot



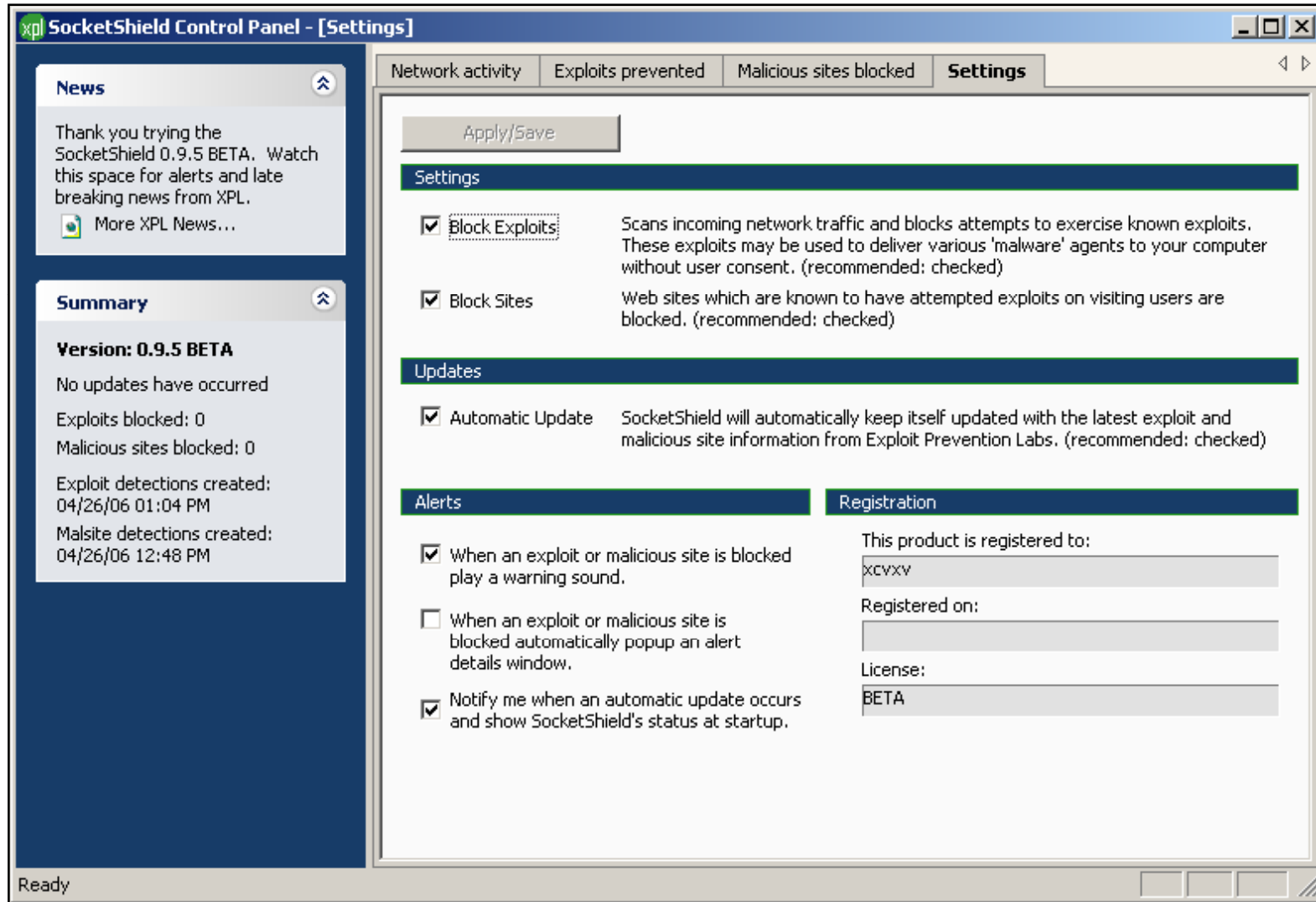
# SocketShield

SocketShield is a zero-day exploit blocker

SocketShield can block exploits from entering the computer, regardless of how long it takes for the vendors of vulnerable applications to issue patches



# SocketShield: Screenshot





BitDefender 2008 is an outstanding product with a user–friendly interface

It scans all existing files on computer, all incoming and outgoing emails, IM transfers, and all other network traffic

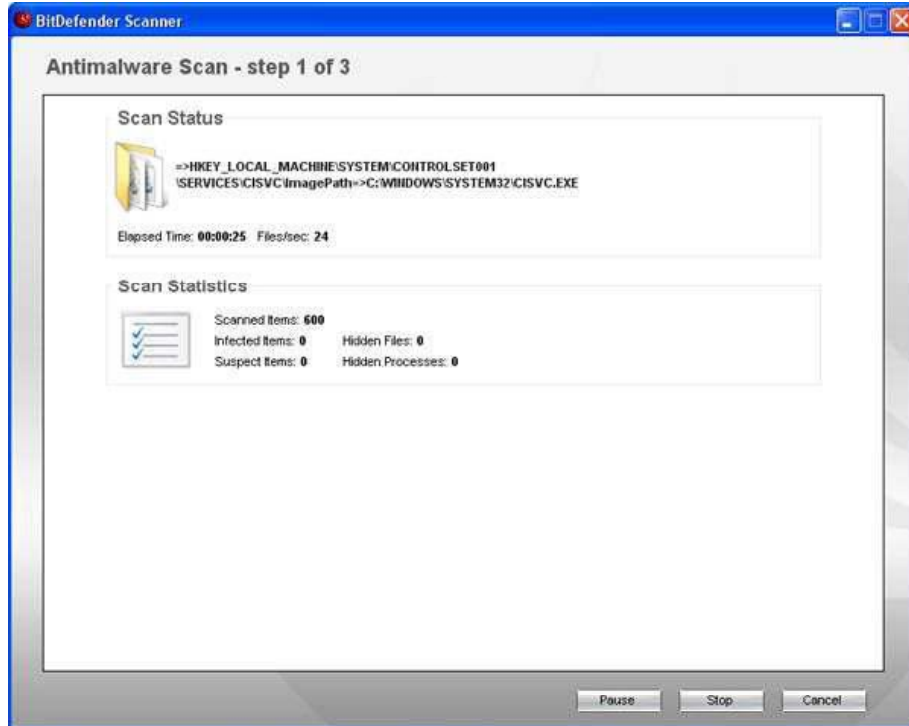
BitDefender has also improved their existing B–HAVE feature that runs pieces of software on a virtual computer to detect code that could be an unknown virus

## Features:

- “Privacy Protection” for outgoing personal information
- “Web Scanning” while you are using the Internet
- “Rootkit Detection and Removal,” which detects then removes hidden virus programs



# BitDefender: Screenshot



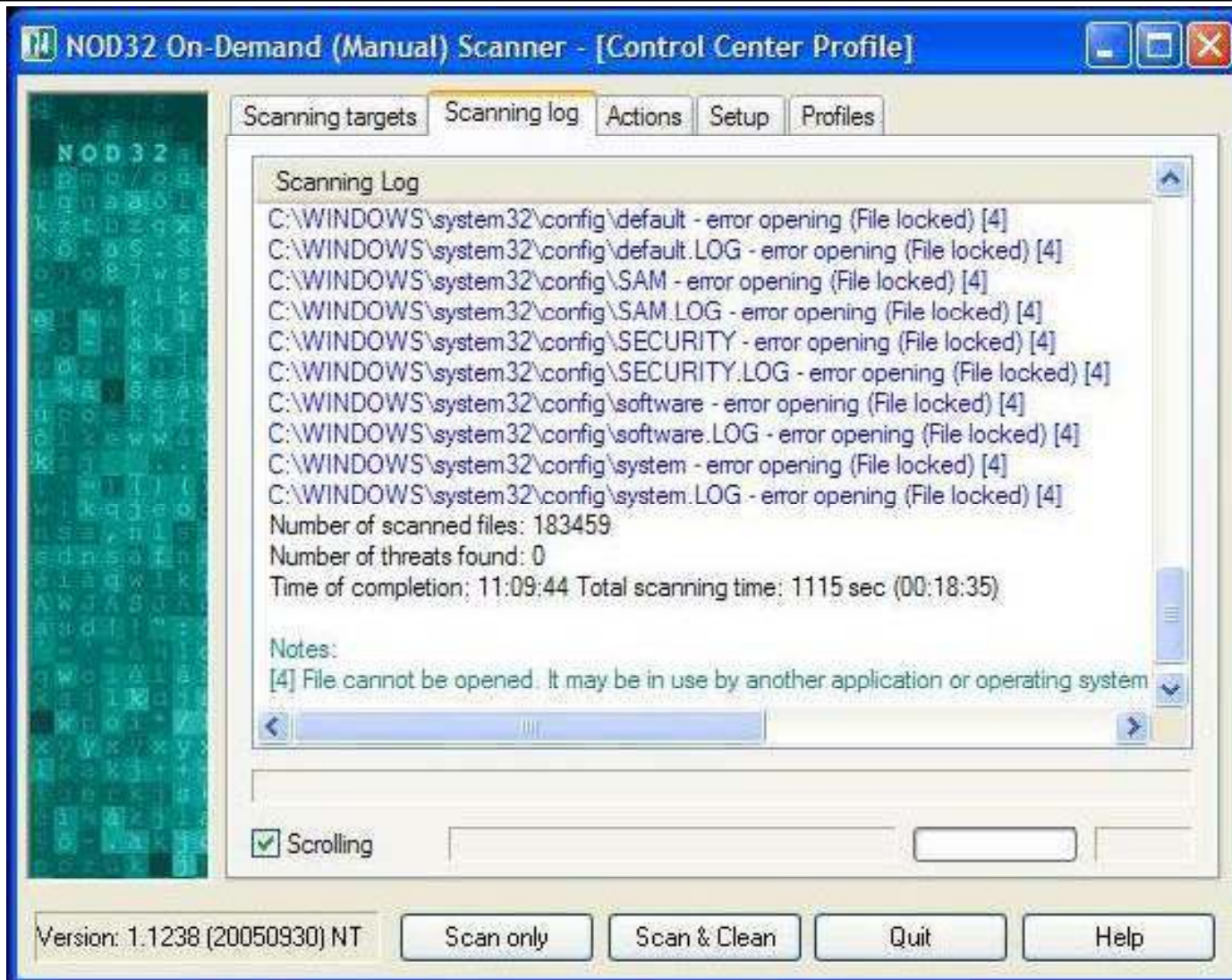
NOD32 antivirus contains a minimal-impact, high performance virus scanning engine

Offers integrated real-time protection against viruses, worms, trojans, spyware, adware, phishing, and hackers

Has a number of practical features to help you monitor your computer's security including outbreak notices and history/ report logging

NOD32 stops more zero-day threats on first sight

# ESET Nod32: Screenshot



CA Anti-Virus provides comprehensive protection against viruses, worms, and Trojan horse programs

Detects viruses, worms, and Trojans

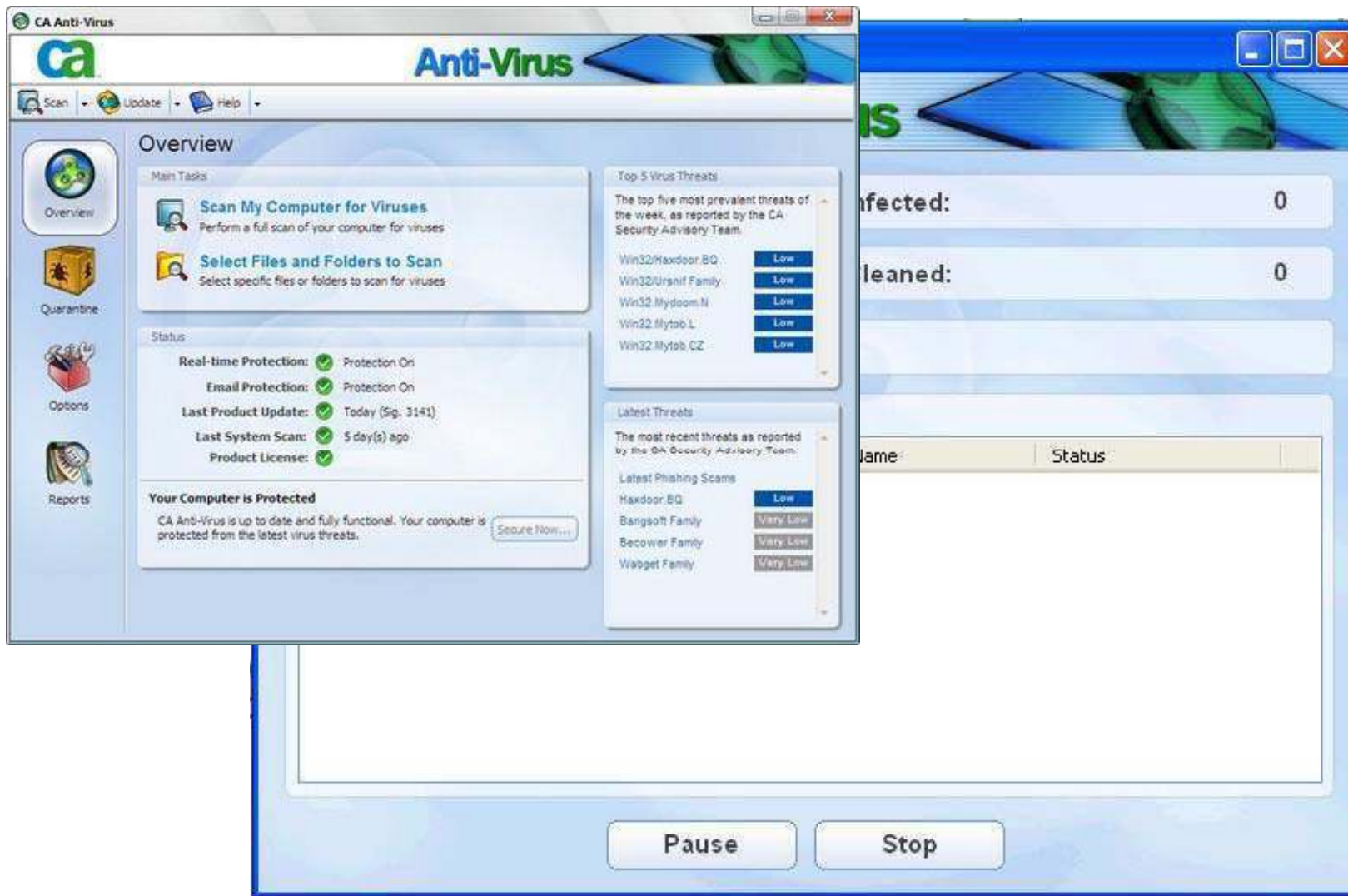
Scans emails automatically

Defends against emerging viruses

Protects files, downloads, and attachments



# CA Anti-Virus: Screenshot



# F-Secure Anti-Virus

F-Secure Anti-Virus 2007 is an anti-virus tool software developed by F-Secure Corporation

Offers an easy to use protection for your computer against viruses, worms, and rootkits

## Features:

- Protects computer against viruses and worms
- The new F-Secure DeepGuard technology protects you against zero-day and other future threats
- Detects and removes spyware from computer
- E-mail scanning
- Easy to install and use
- The fastest protection against new virus outbreaks



# F-Secure Anti-Virus: Screenshot





# Kaspersky Anti-Virus

Provides traditional anti-virus protection based on the latest protection technologies

Allows users to work, communicate, surf the Internet, and play online games on computer safely and easily

Protects from viruses, Trojans and worms, spyware, adware, and all types of keyloggers

Protection from viruses when using ICQ and other IM clients

Detects all types of rootkits

Provides three types of protection technologies against new and unknown threats:

- Hourly automated database updates
- Preliminary behavior analysis
- On-going behavior analysis

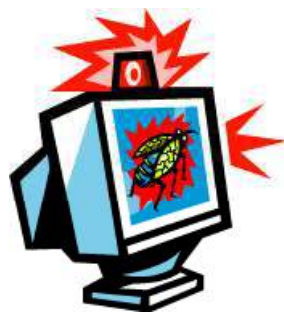
# Kaspersky Anti-Virus: Screenshot



# F-Prot Antivirus

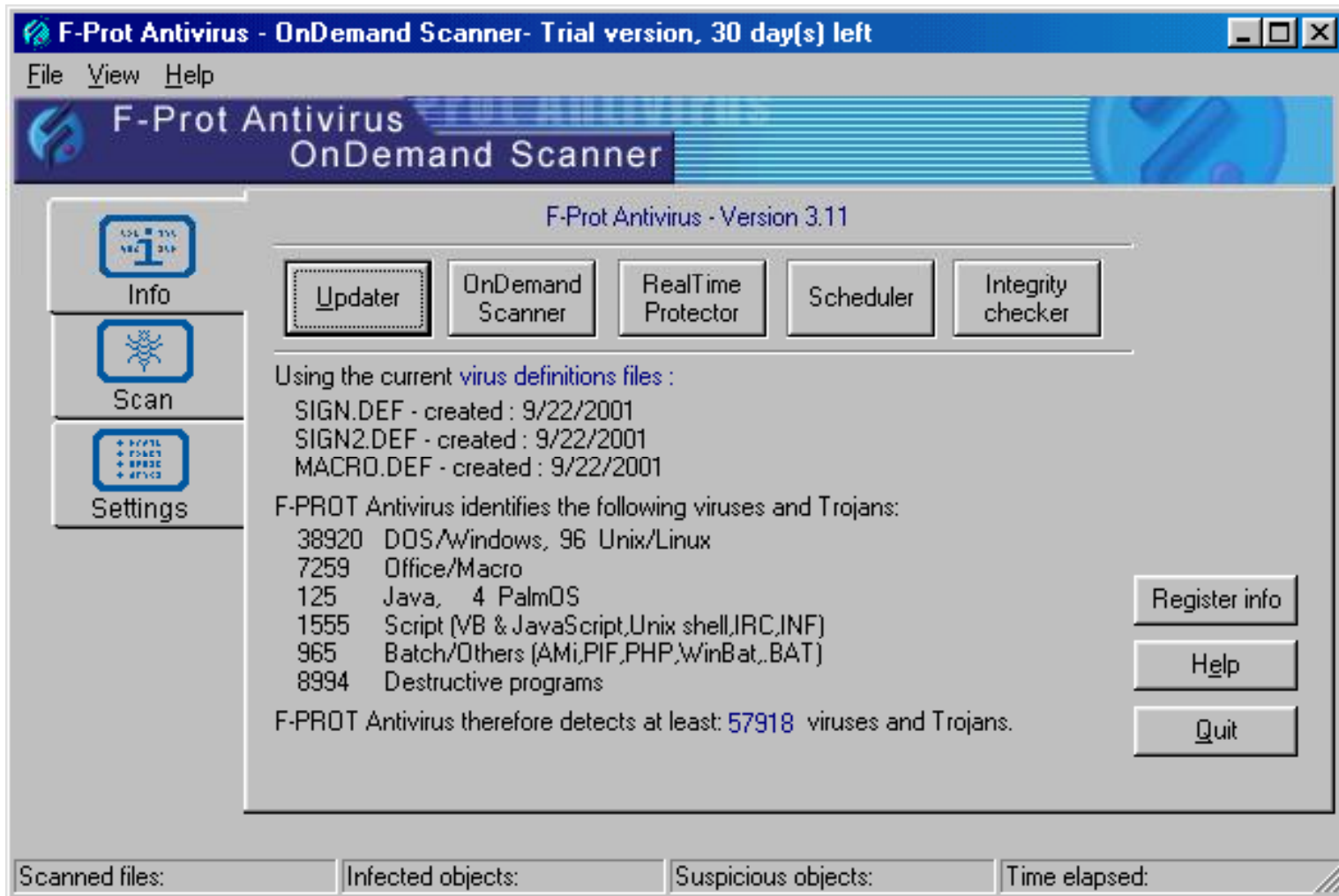
F-Prot Antivirus is an antivirus software package, which protects your data from virus infection and removes any virus that may have infected your computer system

It features real-time protection and email scanning, as well as heuristic detection of suspected viruses



Automatic updates ensure that any new virus is immediately added to the F-Prot Antivirus detection and disinfection database

# F-Prot Antivirus: Screenshot



# Panda Antivirus Platinum

Panda Antivirus Platinum transparently eliminates viruses at the desktop and TCP/IP (Winsock) level

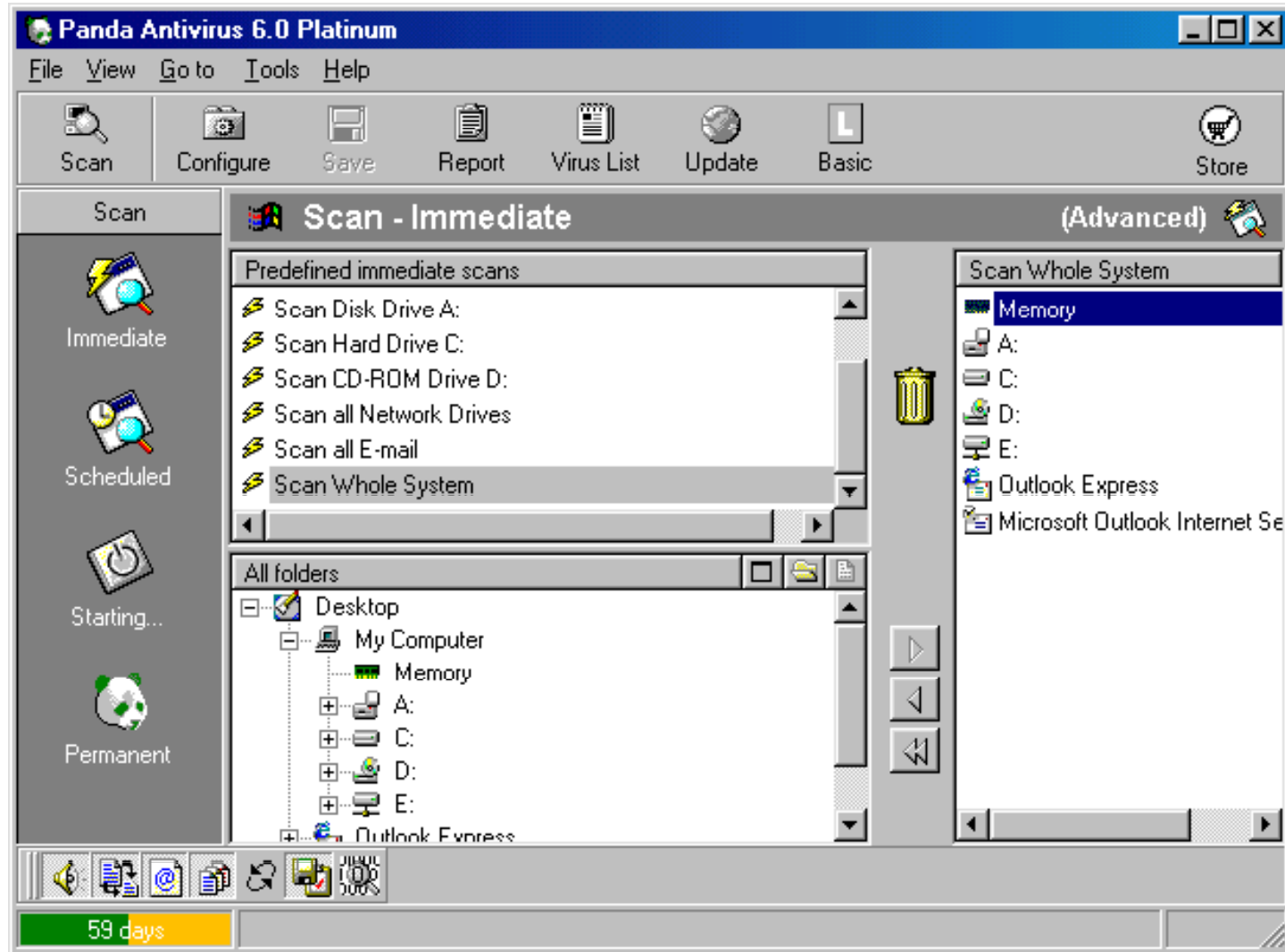
It detects and disinfects viruses before they can touch your hard drive

It can protect your computer from more than 60,000 different viruses, including encrypted, polymorphic, boot, file, macro (Word, Excel, and Access), trojans, Java applets, ActiveX controls, malignant Web sites, email, and Internet viruses

It includes an email and Internet protection resident that will scan POP3, SMTP, HTTP, FTP, mIRC, and NNTP traffic



# Panda Antivirus Platinum: Screenshot



# avast! Virus Cleaner

avast! Virus Cleaner removes selected virus & worm infections from your computer

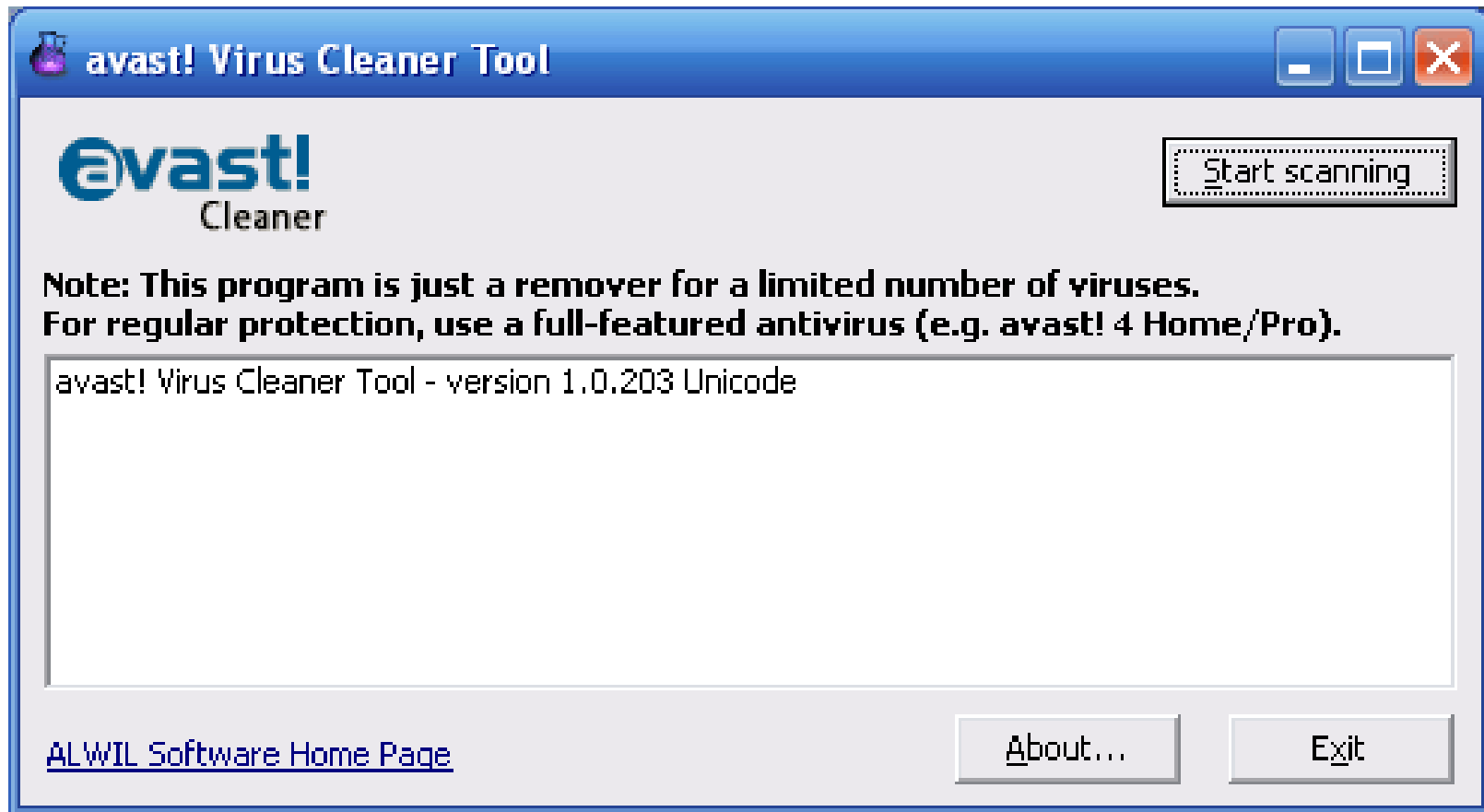
It deactivates the virus present in memory

It identifies and removes the following worm families:

- MyDoom and Beagle/ Bagle
- Badtrans
- BugBear
- Nimda
- Opas
- Sircam
- Sobig



# avast! Virus Cleaner: Screenshot



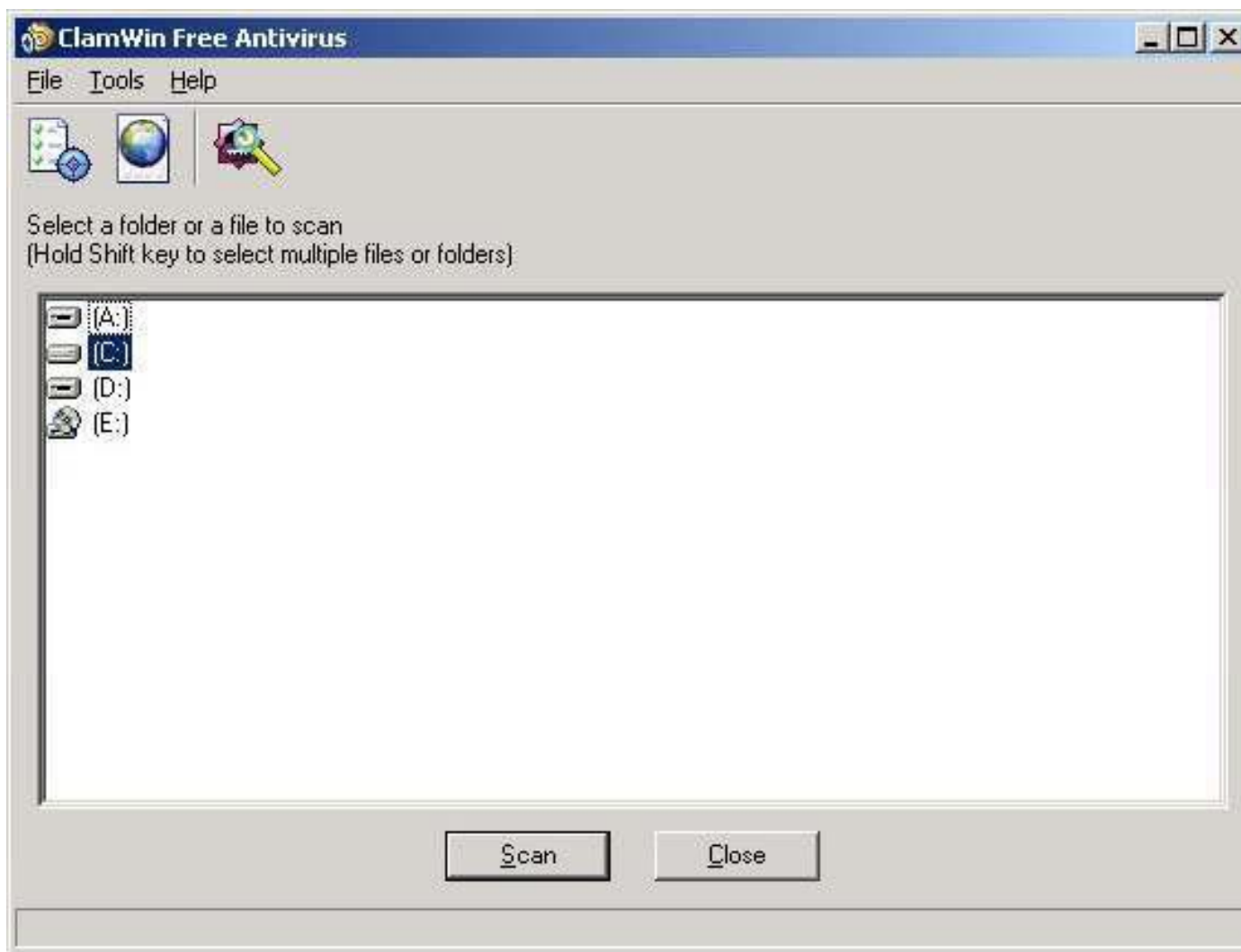


Clam Win detects and removes a wide range of viruses and spyware and offers email scanning

It performs automatic Internet updates, scheduled scans, and email alerts on virus detection



# ClamWin: Screenshot 1



# ClamWin: Screenshot 2



# Clam Win: Screenshot 3



# ClamWin: Screenshot 4



# Norman Virus Control

Uses the same core components as the corporate version, except network and network management functionality

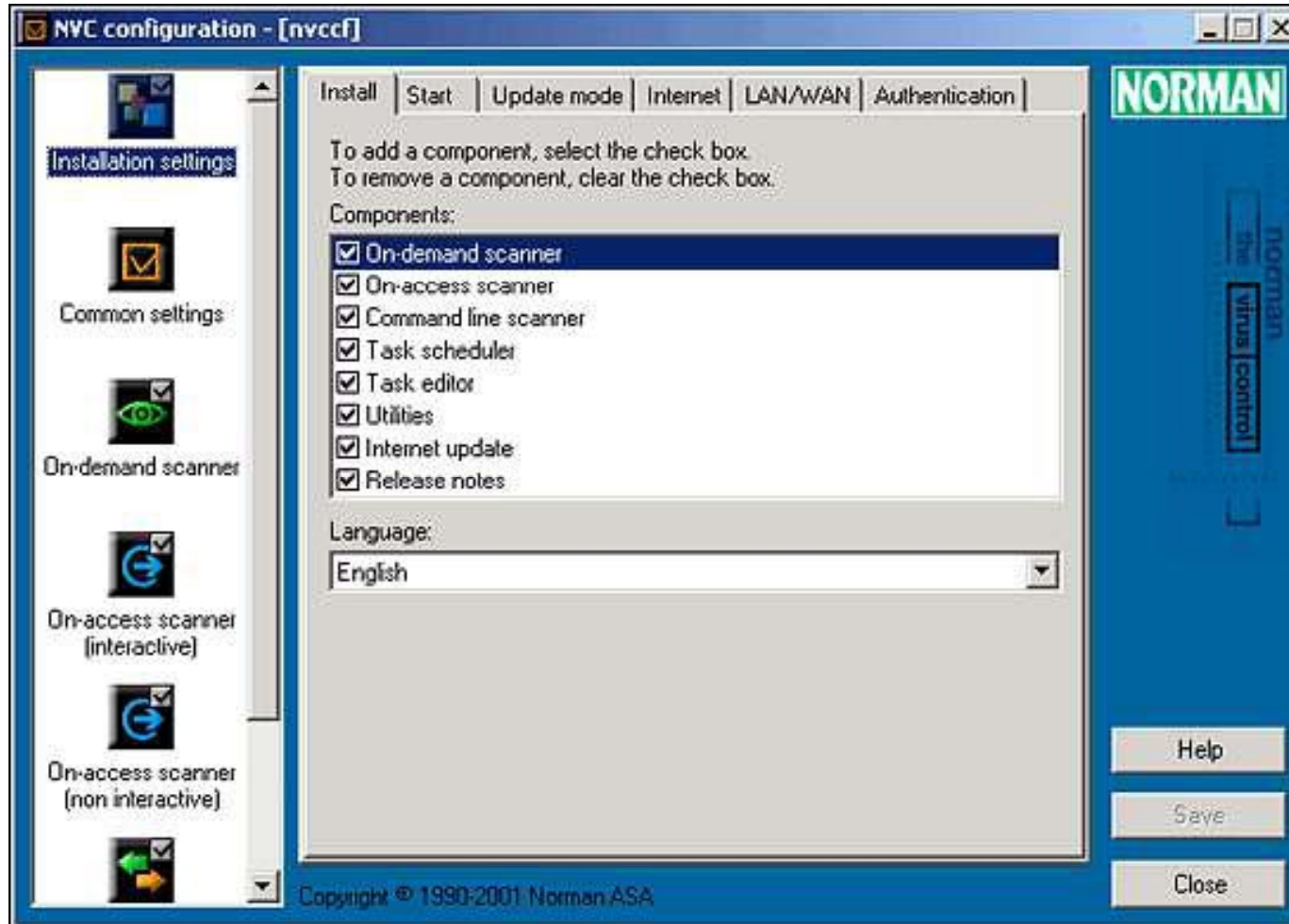
The unique Norman SandBox II technology protects against new and unknown computer viruses, worms, and trojans

Downloads from newsgroups can be scanned for malware before they are made available to the user

## Features of Norman Virus Control:

- Email scanning for malicious programs
- Real-time scanning of files
- Norman SandBox technology to include detection of unknown viruses, trojans, and worms
- Automatic Internet update

# Norman Virus Control: Screenshot



# Popular Anti-Virus Packages

Aladdin Knowledge Systems <http://www.esafe.com/>

Central Command, Inc. <http://www.centralcommand.com/>

Computer Associates International, Inc. <http://www.cai.com>

Frisk Software International <http://www.f-prot.com/>

Trend Micro, Inc. <http://www.trendmicro.com>

Norman Data Defense Systems <http://www.norman.com>

Panda Software <http://www.pandasoftware.com/>

Proland Software <http://www.pspl.com>

Sophos <http://www.sophos.com>





# Virus Databases

The following databases can be useful if you are looking for specific information about a particular virus:

**Proland - Virus Encyclopedia**

[http://www.pspl.com/virus\\_info/](http://www.pspl.com/virus_info/)

**Norman - Virus Encyclopedia**

<http://www.norman.com/Virus/en-us>

**AVG - Virus Encyclopedia**

<http://www.grisoft.com/doc/Virus+Encyclopaedia/Ing/us/tp1/tp101>

**Virus Bulletin - Virus Encyclopedia**

<https://www.virusbtn.com/login>

**F-Secure Virus Info Center**

<http://www.f-secure.com/vir-info/>

**McAfee - Virus Information Library**

<http://vil.mcafee.com/>

**Panda Software - Virus Encyclopedia**

<http://www.pandasoftware.com/library/>

**Sophos Virus Information**

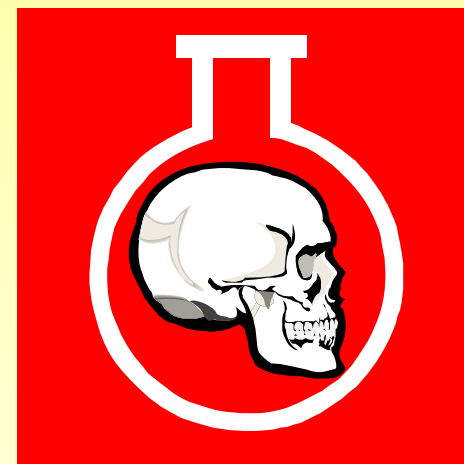
<http://www.sophos.com/virusinfo/>

**Symantec AntiVirus Research Center**

<http://www.symantec.com/avcenter/index.html>

**Trend Micro - Virus Encyclopedia**

<http://www.antivirus.com/vinfo/virusencyclo/default.asp>





SUBSCRIBE



SNOPES  
COMMUNITY



CONTACT US



RANDOM



SITE INFO

Search



E-mail this

Print this



Advanced search



[Home](#) --> [Computers](#) --> [Virus Hoaxes & Realities](#) --> [Postcard](#)

## Postcard

**Virus:** You've Received a Postcard from a Family Member!

**Status:** *Real virus.*

**Examples:**

Ads b

[ww](#)  
Urb:  
Con  
Sea  
[www](#)

[The](#)  
The  
look  
can

# What Happened Next

Next day when he switched on his system, Ricky was surprised at the irregular behavior of his system. His system was hanging down frequently and strange error messages were popping up. He suspected virus attack on his system. He updated his anti-virus software which he has not updated since long and scanned the system.

Scan result showed that his system was infected by a deadly virus.

# Summary

Viruses come in different forms

Some are mere nuisances, others come with devastating consequences

Email worms are self replicating, and clog networks with unwanted traffic

Virus codes are not necessarily complex

It is necessary to scan the systems/networks for infections on a periodic basis for protection against viruses

Antidotes to new virus releases are promptly made available by security companies, and this forms the major countermeasure

Copyright 2003 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it’s time to go home.”**

Copyright 2005 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“I’ve installed a comprehensive program that will protect our computer against viruses, trojan horses, worms, cooties, hissy fits, conceptions, and the heebie-jeebies.”**

Copyright 2003 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



"MOM SAYS I CAN ONLY USE THE COMPUTER THREE HOURS A DAY.  
IT TAKES LONGER THAN THAT JUST TO DELETE MY SPAM!"

© 2000 Randy Glasbergen.  
www.glasbergen.com



**“Oh, the usual stuff. Spam from the Joker,  
another e-mail virus from the Penguin,  
an illegal chain letter from Cat Woman....”**