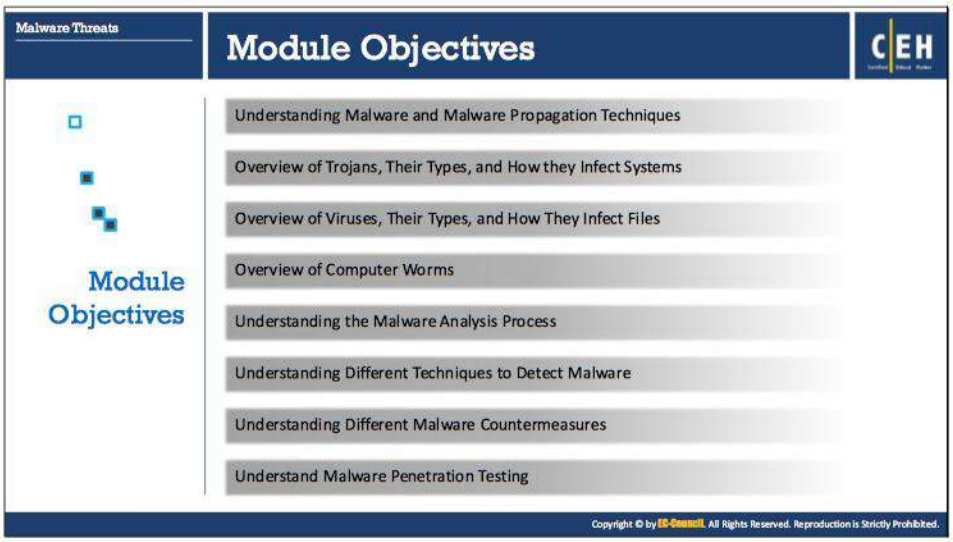
C|EH™
Certified Ethical Hacker

Module 07

Malware Threats

This page is intentionally left blank.

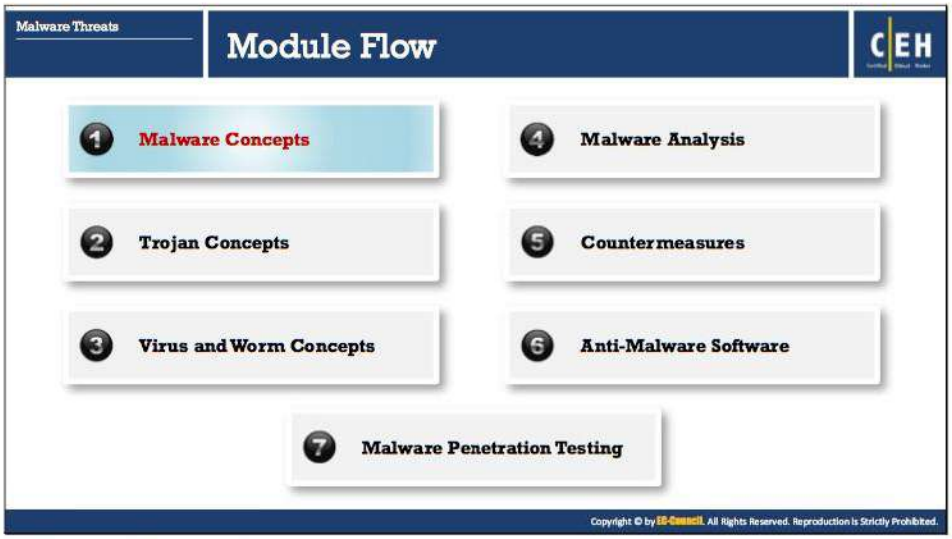


Module Objectives

The primary objective of this module is to provide the knowledge about various types of malware. It covers different types of Trojans, backdoors, virus, and worms, the way they work and propagate or spread on the Internet, their symptoms, and their consequences. The module also discusses different ways to protect networks or system resources from malware infection. Finally, it provides a brief discussion on the penetration testing process to enhance security against malware.

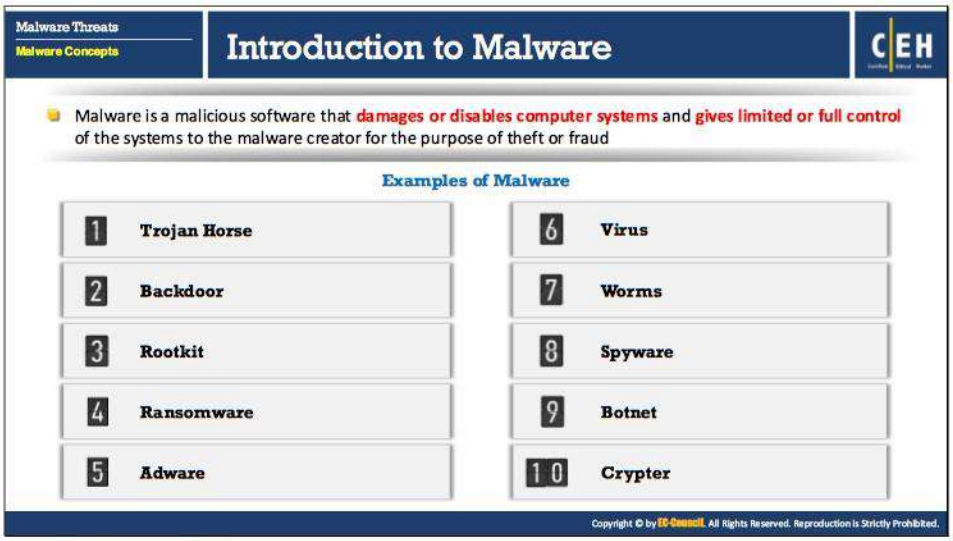
At the end of this module, you will be able to:

- Describe the concepts of malware and malware propagation techniques
- Describe the concepts of Trojans, their types, and how they infect systems
- Explain the concepts of viruses, their types, and how they infect files
- Explain the concept of computer worms
- Perform malware analysis
- Explain different techniques to detect malware
- Apply malware countermeasures
- Perform malware penetration testing



Malware Concepts

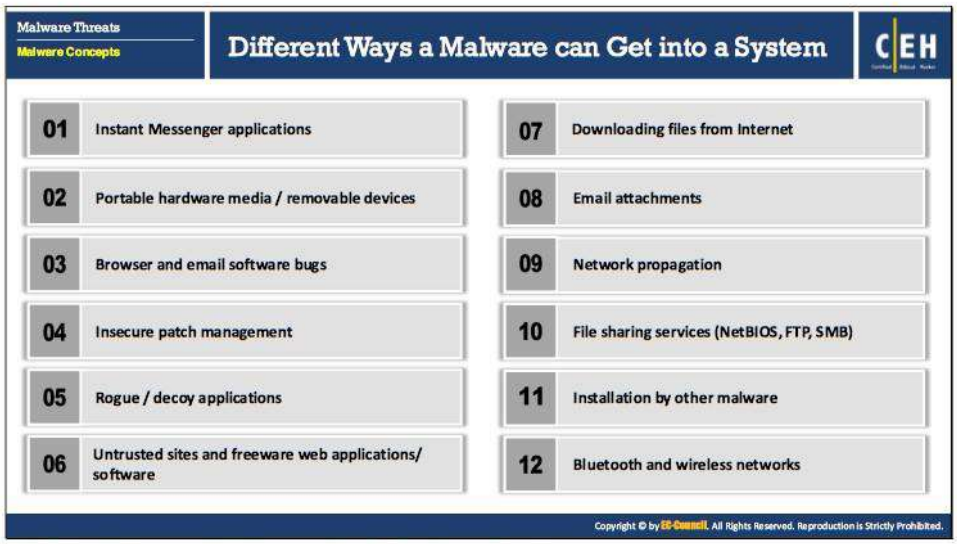
To understand various types of malware and their impact on network and system resources, we will begin with the basic concepts of malware. This section describes malware and highlights the common techniques attackers use to distribute malware on the Web.



Introduction to Malware

Malware is malicious software that damages or disables computer systems and gives limited or full control of the systems to its creator for theft or fraud. Malware includes viruses, worms, trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, etc. These may delete files, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing. Malware programmers develop and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in the substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails



Different Ways a Malware Can Get into a System

- **Instant Messenger Applications**

  Infection can occur via instant messenger applications such as Facebook Messenger, WhatsApp messenger, LinkedIn messenger, Google Hangout, ICQ or Yahoo Messenger. Users are at high risk while receiving files via instant messengers. No matter from whom or from where there is always some risk of infection by a Trojan. The user can never be 100% sure of who is at the other end of the connection at any particular moment. For e.g., if you receive a file through the instant messenger from a known person such as, Bob, you will try to open and view the file. This could be a trick where an attacker who hacked Bob's messenger ID and password wants to spread Trojans over Bobs friend's contacts list to trap more victims.

- **Portable Hardware Media /Removable Devices**

  - Portable hardware media like flash drives, CDs/ DVDs, and external hard drives can also inject malware into a system. The simple way of injecting malware into the target system is by physical access. For e.g., if Bob can access Alice's system in her absence then he can install a Trojan by copying the Trojan software from his flash drive onto the hard drive.
  - Another way of portable media malware infection is caused by Autorun function. Autorun also referred as Autoplay or Autostart, is a Windows feature that, if enabled, runs an executable program when a user inserts a CD/DVD in the DVD-ROM tray or connects a USB device. Attackers can exploit this feature to run malware along with genuine programs. They place an Autorun.inf file with the malware in a CD/DVD or USB and trick people to insert or plug it into their systems. Because many people are

not aware of the risks involved, their machines are always vulnerable to autorun malware. The following is the content of an Autorun.inf file:

```
[autorun]
open=setup.exe
icon=setup.exe
```

To mitigate such infection, turn off Autostart functionality. Follow the instructions given below to turn off the Autoplay in Windows 10:

1. Click **Start**. Type **Gpedit.msc** in the **Start Search** box, and then press **ENTER**.
2. If you are prompted for an administrator password or confirmation, type the password, or click **Allow**.
3. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.
4. In the **Details** pane, double-click **Turn off Autoplay**.
5. Click **Enabled**, and then select **All drives** in the **Turn off Autoplay** box to disable Autorun on all drives.
6. **Restart** the computer.

- **Browser and Email Software Bugs**

  Outdated web browsers often contain vulnerabilities that can pose an immense risk to the user's computer. A visit to a malicious site from such browsers can automatically infect the machine without downloading or executing any program. The same scenario occurs while checking e-mail with Outlook Express or some other software with well-known problems. Again, it may infect the user's system without even downloading an attachment. To reduce the risk of these variations, always use the latest version of the browser and e-mail software.

- **Insecure Patch management**

  Unpatched software poses a high-security risk. Users and IT administrators do not update their application software as often as they should, and many attackers take advantage of this well-known fact. Due to insecure patch management, the attackers can exploit the vulnerability by injecting malware into the software that can damage the data stored on the company's systems. This process can lead to extensive security breaches such as stealing confidential files and company credentials. Some of the applications that are found vulnerable and patched recently are MS Word (CVE-2017-0281), MS Excel (CVE-2017-0006), Internet Explorer (CVE-2017-0018), SQL Server (CVE-2016-7254), Oracle Java JDK (CVE-2017-3512), Adobe Acrobat Reader (CVE-2017-3118), and Adobe flash player (CVE-2017-2990). Patch management has to be effective to mitigate the threat, and it is vital to fix patches and update softwares on a regular basis.

- **Rogue/Decoy Applications**

  Attackers can easily lure a victim into downloading free applications/programs. If a free program claims to be loaded with features such as an address book, access to check

several POP3 accounts, and other functions, many will be tempted to try it. POP3 (Post Office Protocol version 3) is an email transfer protocol.

- If a victim downloads free programs and labels it as TRUSTED, the protection software such as antivirus will fail to indicate that the use of new software. In this situation, an attacker gets e-mail, POP3 account passwords, cached passwords, and keystrokes through email without the notice of anyone.
- Attackers thrive on creativity. Consider an example in which an attacker creates a fake Audio galaxy, a Web site for downloading MP3s. He or she could generate such a site by using 15 GB of space for the MP3s and installing any other systems needed to create the illusion of a Web site. This can fool users into thinking that they are merely downloading from other network users. However, the software could act as a backdoor and infect thousands of naive users.
- Some Web sites even link to anti-Trojan software, fooling users into trusting them and downloading infected freeware. Included in the setup is a readme.txt file. This can deceive almost any user, so any freeware site requires proper attention before downloading any software from it.
- Webmasters of well-known security portals, who have vast archives containing various hacking programs, should act responsibly regarding the files they provide and scan them often with anti-virus and anti-Trojan software to guarantee that their site is free of Trojans and viruses. Suppose an attacker submits, a program infected with a Trojan (e.g., a UDP flooder) to an archive's Webmaster. If the Webmaster is not alert, the attacker may use the opportunity to infect the files on the site with a Trojan. Users who deal with any software or Web application should scan their system on a daily basis. If they detect any new file, it is essential to examine it. If any suspicion arises regarding the file, it is also important to forward it to software detection labs for further analysis.
- It is easy to infect machines using freeware, thus extra precautions are necessary.

- **Untrusted Sites and Freeware Web Applications/Software**

  A website could be suspicious if located at a free website provider or one offering programs for illegal activities.

  - It is highly risky to download programs or tools located on "underground" sites such as NeuroticKat Software because they can serve as a conduit for a Trojan attack on target computers. Users must assess the high risk of visiting such sites before browsing them.
  - Many malicious Web sites have a professional look, huge archives, feedback forums, and links to other popular sites. Users should scan the files using antivirus before downloading them. Just because a Web site looks professional does not mean that it is safe.
  - Always download popular software from its original (or officially dedicated mirror) site, and not from third-party sites with links to the (supposedly) same software.

- **Downloading Files from Internet**

  Trojans enter a system when users download internet-driven applications such as music players, files, movies, games, greeting cards, and screensavers from malicious websites, thinking that they are legitimate. Microsoft Word and Excel macros are also used effectively to transfer malware and to download malicious MS Word/ Excel file can infect the systems. Malware can also be embedded in audio/video file formats and also can be embedded in video subtitle files.

- **Email Attachments**

  An attachment to e-mails is the most common medium to transmit malware. The attachment can be in any form and attacker uses innovative ideas to trick the victim to click and download the attachment. The attachments can be a document, song, video file, brochure, invoice, lottery offer letter, job offer letter, loan approval letter, admission form, contract approval, etc.

  Example 1: A user's friend is carrying out some research, and the user would like to know more about the friend's research topic. The user sends an e-mail to the friend to inquire about the topic and waits for a reply. An attacker targeting the user also knows the friend's e-mail address. The attackers will merely code a program to populate falsely the e-mail "From:" field and attach Trojan in the email. The user will check the email and think that the friend has answered the query in an attachment, download the attachment, and run it without thinking it might be a Trojan, resulting in an infection.

  Some email clients, such as Outlook Express, have bugs that automatically execute attached files. To avoid such attacks, use secure email services and investigate the header of the emails with attachments, confirm the sender's email address and if found legitimate, then download the attachment.

- **Network Propagation**

  Network security is the first line of defense in preventing information systems from any hacking incidents. However, due to various reasons such as the replacement of the network firewalls, mistakes of the operators' factors may sometimes intentionally or unintentionally allow unfiltered Internet traffic into private networks. Malware operators continuously attempt connections to the addresses within the Internet address range owned by targets to see if the opportunity for unfettered access may exist. Some malware propagates through technological networks. For e.g., the Blaster starts from a local machine's IP address or a completely random address and attempts to infect sequential IP addresses. Although the network propagation attacks that took advantage of vulnerabilities in common network protocols (e.g., SQL Slammer) have not been prevalent recently, the potential for such attacks still exists.

- **File Sharing**

  If NetBIOS (Port 139), FTP (Port 21), SMB (Port 145), etc. on a system is open for file sharing or remote execution, it can be used by others to access the systems. This can allow the attackers to install malware, and modify system files.

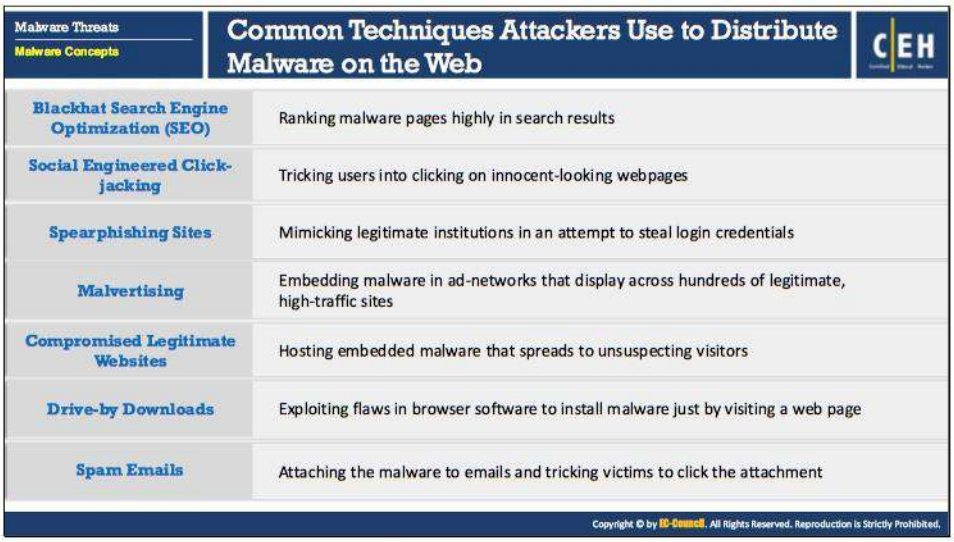
Attackers can also use a DoS attack to shut down the system and force a reboot so that the Trojan can restart itself immediately. To prevent from such attacks, ensure that the file sharing property is disabled. To disable the file sharing option, click **Start** and type **Control Panel**. In the result, click on the **Control Panel** option then navigate to **Network and Internet → Network and Sharing Center → Change Advanced Sharing Settings**. Select a network profile and under **File and Printer Sharing** section, select **Turn off file and printer sharing**. This will prevent file sharing abuse.

- **Installation by other Malware**

  A piece of malware that can command and control will often be able to re-connect to the malware operator's site using common browsing protocols. This functionality allows malware on the internal network to receive both software and commands from the outside. In this situation, malware installed on one system drives other malware to get installed on the network and cause damage to the network.

- **Bluetooth and wireless networks**

  Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to it. These open networks have software and hardware devices installed at the router level that could capture the network traffic, data packets and also find the account details including username and password.



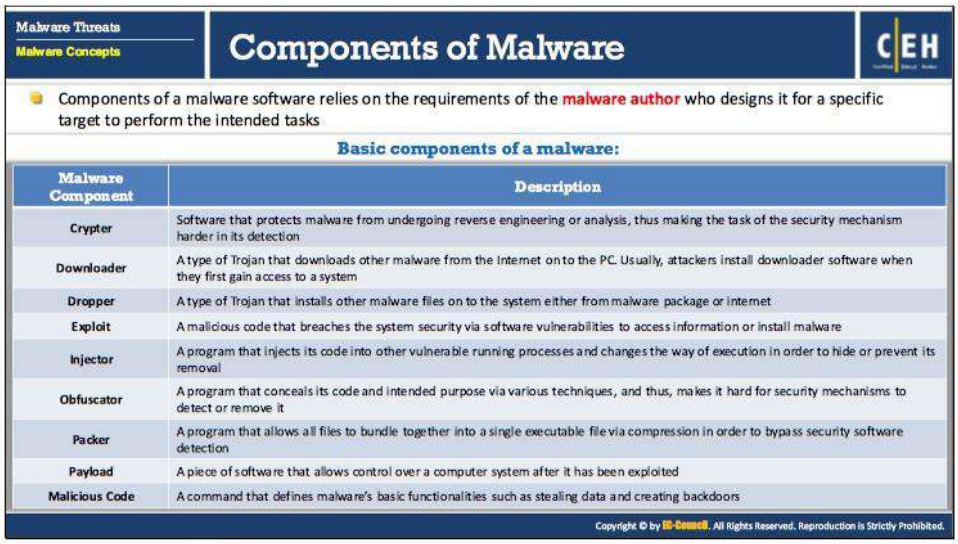
Common Techniques Attackers Use to Distribute Malware on the Web

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

Below are listed some of the standard techniques used to distribute malware on the web:

- **Blackhat Search Engine Optimization (SEO):** Blackhat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords to get higher search engine ranking for their malware pages.
- **Social Engineered Click-jacking:** Attackers inject malware into legitimate-looking websites to trick users by clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.
- **Spearphishing Sites:** This technique is used for mimicking legitimate institutions, such as banks, in an attempt to steal passwords, credit card and bank account data, and other sensitive information.
- **Malvertising:** Involves embedding malware-laden advertisements in legitimate online advertising channels to spread malware onto the systems of unsuspecting users.
- **Compromised Legitimate Web sites:** Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, the malware is unknowingly installed on the user's system and after that carries out malicious activities.
- **Drive-by Downloads:** The unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware just merely by visiting a website.

- **Spam Emails:** Attacker attaches a malicious file to an email and sends the email to multiple target address. The attacker tricks the victim to click the attachment, and when clicked, the malware gets executed, and the machine gets compromised. This technique is the most common way used by the attackers these days. Apart from the email attachments, an attacker may also use email body to embed the malware.



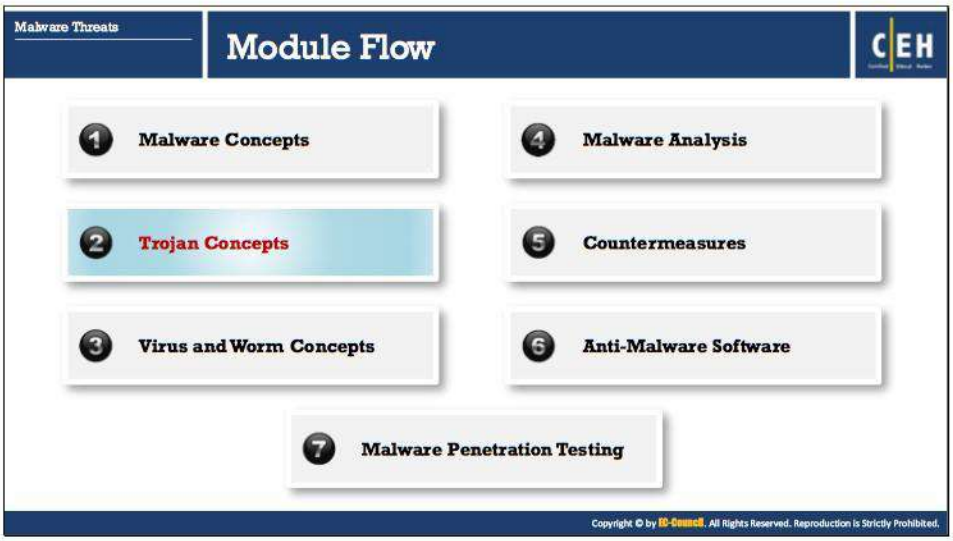
Components of Malware

Malware authors and attackers create malware using the components that can help them achieve their goals. They can use malware to steal information, delete data, change system settings, provide access or merely multiply and occupy the space. Malware is capable of propagating and functioning secretly.

Some of the essential components of most malware programs are:

- **Crypter:** Refers to a software program that can conceal the existence of malware. Attackers use this software to elude antivirus detection. It protects malware from undergoing reverse engineering or analysis, thus hard to get detected by the security mechanism.
- **Downloader:** Type of Trojan that downloads other malware (or) malicious code and files from the Internet on to the PC or device. Usually, attackers install downloader when they first gain access to a system.
- **Dropper:** Attackers need to install the malware program or code on the system to make it run, and this program can do the installation task covertly. The dropper can contain unidentifiable malware code undetected by the antivirus scanners and is capable of downloading additional files needed to execute the malware on a target system.
- **Exploit:** Part of the malware that contains code or sequence of commands that can take advantage of a bug or vulnerability in a digital system or device. It is the code the attackers use to breach the system's security through software vulnerabilities to spy the information or to install malware. Based on the type of vulnerabilities they abuse, the exploits have different categories including local exploits and remote exploits.

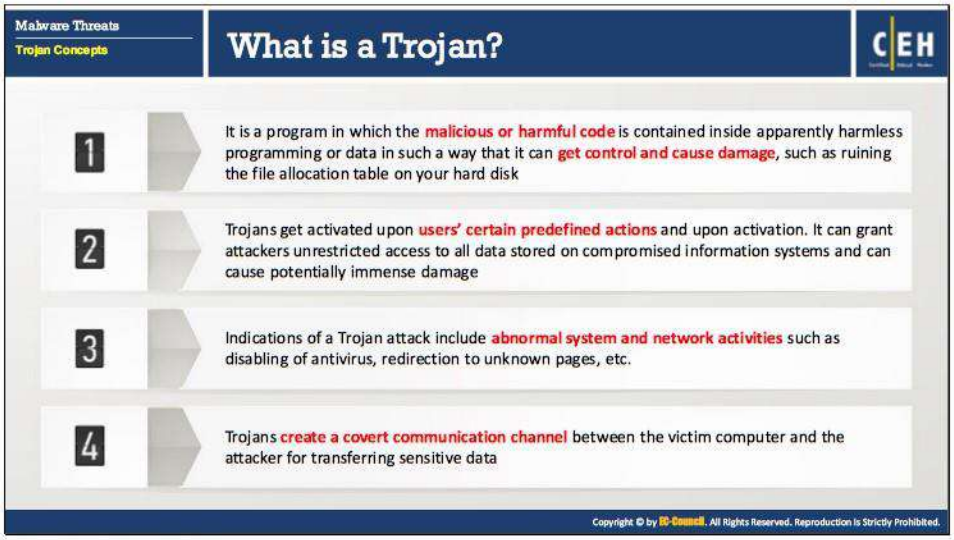
- **Injector:** This program injects the exploits or malicious code available in the malware into other vulnerable running processes and changes the way of execution to hide or prevent its removal.
- **Obfuscator:** A program to conceal the malicious code of malware via various techniques, thus making it hard for security mechanisms to detect or remove it.
- **Packer:** This software compresses the malware file to convert the code and data of malware into an unreadable format. The packers use compression techniques to pack the malware.
- **Payload:** Part of the malware that performs desired activity when activated. The payload may be used for deleting, modifying files, affecting the system performance, opening ports, changing settings, etc. as part of compromising the security.
- **Malicious Code:** This is a piece of code that defines the basic functionality of the malware and comprises commands that result in security breaches. It can take forms like:
  - Java Applets
  - ActiveX Controls
  - Browser Plug-ins
  - Pushed content



Trojans Concept

In this section we will discuss the basic concepts of Trojans to understand various Trojans and backdoors and their impact on network and system resources. This section describes Trojans and highlights their purpose, the symptoms of their attacks, and the common ports that they use. It also discusses the various methods adopted by the attacker to install Trojans on target systems to infect them and then carry out malicious activities.

This section also describes various types of Trojan. Every day, attackers discover or create new Trojans designed to discover vulnerabilities of target systems. Trojans are categorized by the way they enter and the types of actions they perform on these systems.



What is a Trojan?

In Ancient **Greek myth**, the Greeks won the **Trojan War** with the aid of a giant wooden horse, which the Greeks built for their soldiers to hide. The Greeks left it in front of the gates of Troy. The Trojans thought that it was a gift from the Greeks, which they had left before apparently withdrawing from the war and brought the horse into their city. At night, the Greek soldiers broke out of the wooden horse and opened the gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer trojan is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk. Attackers use computer Trojan horses to trick the victim into performing a predefined action. Trojans get activated upon users' specific predefined actions like installing a malicious software unintentionally, clicking on the malicious link, etc. and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and causing potentially immense damage. For e.g., users could download a file that appears to be a movie, but, when executed, unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

A Trojan is wrapped within or attached to a legitimate program, meaning that the program may have functionality that is not apparent to the user. Also, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal denial-of-service attacks.

Trojan horses work on the same level of privileges as victims. For e.g., if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks),

once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase the level of access, even beyond the user running it. If successful, the Trojan can use those increased privileges to install other malicious code on the victim's machine.

A compromise of any network system can affect other such systems. Those that transmit authentication credentials, such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, he or she may be able to record usernames and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate the remote system as the source of an attack by spoofing, thereby causing the remote system to incur liability. Trojans enter the system by means such as email attachments, downloads, and instant messages.

Symptoms of Trojan Attack

The following computer malfunctions are symptoms of a Trojan attack:

- The DVD-ROM drawer opens and closes automatically.
- The computer screen blinks, flips upside-down, or is inverted, so that everything is displayed backward.
- The default background or wallpaper settings change automatically. This can be performed by using pictures either on the user's computer or in the attacker's program.
- Printers automatically start printing the document.
- Web pages suddenly open without input from the user.
- Color settings of the operating system (OS) change automatically.
- Screensavers convert to a personal scrolling message.
- Sound volume suddenly fluctuates all the way up or down.
- Anti-virus programs are automatically disabled, and the data is corrupted, altered, or deleted from the system.
- The date and time of the computer change.
- The mouse cursor moves by itself.
- The right-click takes the function of the left-click, and vice versa.
- The pointer arrow of the mouse disappears completely.
- The mouse pointer and automatic clicks on icons are uncontrollable.
- The Windows Start button disappears.
- Pop-ups with bizarre messages that suddenly appear.
- Clipboard images and text appear to be manipulated.

- The keyboard and mouse freeze.
- Contacts receive emails from a user's email address that the user did not send.
- Strange warnings or question boxes appear. Many times, these are personal messages directed to the user, asking questions that require the victim to answer by clicking a Yes, No, or OK button.
- The system turns off and restarts in unusual ways.
- The taskbar disappears automatically.
- The Task Manager is disabled. The attacker, or Trojan, may disable the Task Manager function so that the victim cannot view the task list or be able to end the task on a given program or process.

FIGURE 7.1: Diagram showing how attacker extracts information from the victim system

Communication Paths: Overt and Covert Channels

"**Overt**" refers something that is explicit, obvious, or evident, whereas "**covert**" refers to something that is secret, concealed, or hidden.

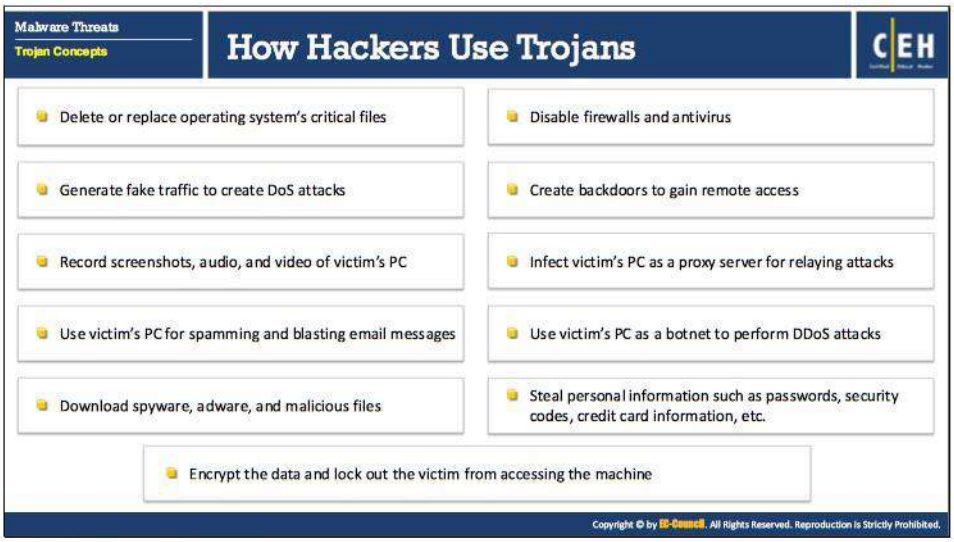
An ***overt channel*** is a legal channel for the transfer of data or information in a company network and works securely to transfer data and information. On the other hand, a ***covert channel*** is an illegal, hidden path used to transfer data from a network.

Covert channels are methods attackers can use to hide data in an undetectable protocol. They rely on a technique called tunneling, which enables one protocol to transmit over the other. Any process or a bit of data can be a covert channel. This makes it an attractive mode of transmission for a Trojan because an attacker can use the covert channel to install a backdoor on the target machine.

The table below lists the primary differences between overt and covert channels:

Overt Channel	Covert Channel
A legitimate communication path within a computer system, or network, for the transfer of data	A channel that transfers information within a computer system, or network, in a way that violates the security policy
An overt channel can be exploited to create a covert channel by using components of the overt channels that are idle	An example of covert channel is the communication between a Trojan and its command and control center

TABLE 7.1: Comparison between Overt Channel and Covert Channel



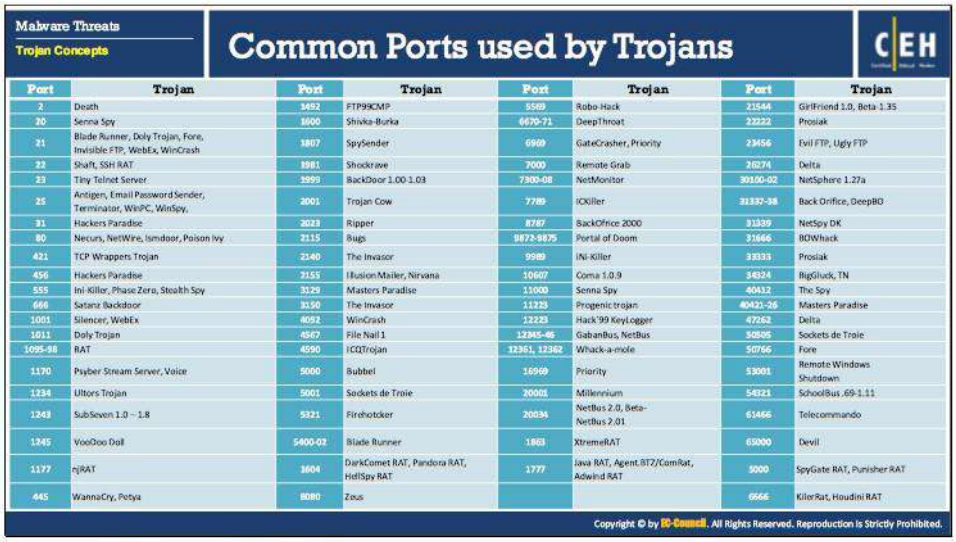
How Hackers Use Trojans

Following are some reasons why attackers create malicious programs such as Trojans:

- Delete or replace OS's critical files
- Generate fake traffic to create DoS attacks
- Record screenshots, audio, and video of victim's PC
- Use victim's PC for spamming and blasting email messages
- Download spyware, adware, and malicious files
- Disable firewalls and antivirus
- Create backdoors to gain remote access
- Infect victim's PC as a proxy server for relaying attacks
- Use victim's PC as a botnet to perform DDoS attacks
- Steal sensitive information, such as:
  - Credit card information, which is useful in domain registration, as well as for shopping using keyloggers
  - Account data such as email passwords, dial-up passwords, and web services passwords
  - Important company projects, including presentations and work-related papers
- Encrypt the victim machine and lock out the victim from accessing the machine
- Attackers can use the target system:

- To store archives of illegal materials, such as child pornography. The target continues using their system without realizing that attackers are using their system for illegal activities
- As an FTP Server for pirated software

- Script kiddies may just want to have fun with the target system; an attacker could plant a Trojan in the system just to make the system act strangely (e.g., the CD\DVD tray opens and closes frequently, the mouse functions improperly, etc.)
- Attacker might use a compromised system for other illegal purposes that makes the target responsible for all illegal activities if discovered by the authorities



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta 1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft, SSH RAT	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOffice 2000	31339	NetSpy DK
80	Necurs, NetWire, Ismdoor, Poison Ivy	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash	12223	Hack'99 KeyLogger	47262	Delta
1011	Doly Trojan	4567	File Nail 1	12345-46	GabanBus, NetBus	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12361, 12362	Whack-a-mole	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	16969	Priority	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	20001	Millennium	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20034	NetBus 2.0, Beta-NetBus 2.01	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	1863	XtremeRAT	65000	Devil
1177	njRAT	1604	DarkComet RAT, Pandora RAT, HidSpy RAT	1777	Java RAT, Agent.BT2/ComRat, Adwind RAT	5000	SpyGate RAT, Punisher RAT
445	WannaCry, Petya	8080	Zeus			6666	KilorRat, Houdini RAT

Common Ports used by Trojans

Ports represent entry and exit points of data traffic. There are two types of ports: hardware ports and software ports. Those within the OS are software ports and are usually entry and exit points for application traffic (e.g., port 25 is associated with SMTP for e-mail routing between mail servers). Many ports exist that are application-specific or process-specific. Various Trojans uses some of these ports to infect target systems.

Users need a basic understanding of the state of an "active connection" and ports commonly used by Trojans to determine whether a system has been compromised.

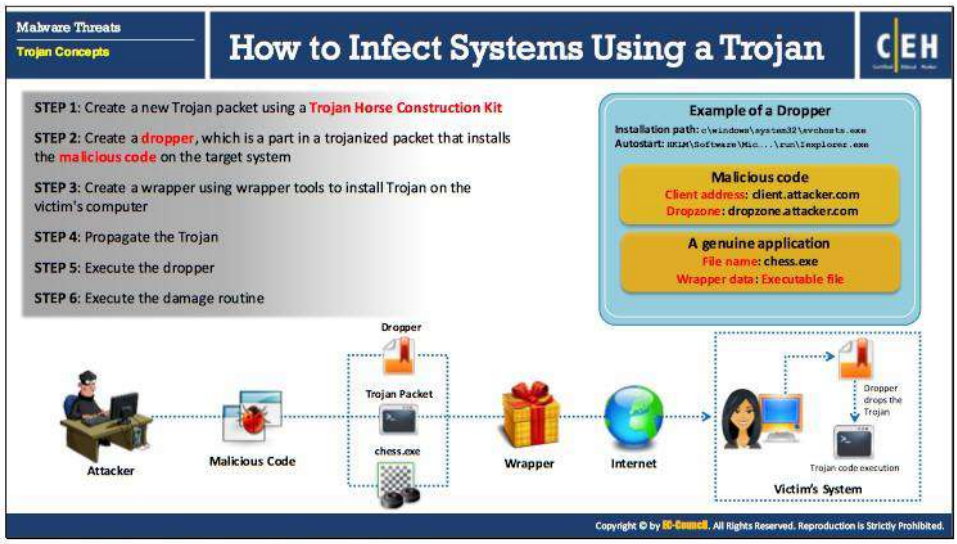
There are different states, but the "listening" state is the important one in this context. The system generates this state when it listens for a port number while waiting to connect to another system. Whenever a system reboots, Trojans move to the listening state; some use more than one port: one for "listening," the other(s) for data transfer. The below table shows the list of common ports used by different Trojans

Port	Trojan	Port	Trojan
2	Death	**1492**	FTP99CMP
20	Senna Spy	**1600**	Shivka-Burka
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	**1807**	SpySender
22	Shaft, SSH RAT	**1981**	Shockrave
23	Tiny Telnet Server	**1999**	BackDoor 1.00-1.03

25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	**2001**	Trojan Cow
31	Hackers Paradise	**2023**	Ripper
80	Necurs, NetWire, Ismdoor, Poison Ivy	**2115**	Bugs
421	TCP Wrappers Trojan	**2140**	The Invasor
456	Hackers Paradise	**2155**	Illusion Mailer, Nirvana
555	Ini-Killer, Phase Zero, Stealth Spy	**3129**	Masters Paradise
666	Satanz Backdoor	**3150**	The Invasor
1001	Silencer, WebEx	**4092**	WinCrash
1011	Doly Trojan	**4567**	File Nail 1
1095-98	RAT	**4590**	ICQTrojan
1170	Psyber Stream Server, Voice	**5000**	Bubbel
1234	Ultors Trojan	**5001**	Sockets de Troie
1243	SubSeven 1.0 – 1.8	**5321**	Firehotcker
1245	VooDoo Doll	**5400-02**	Blade Runner
1177	njRAT	**1604**	DarkComet RAT, Pandora RAT, HellSpy RAT
445	WannaCry, Petya	**8080**	Zeus
5569	Robo-Hack	**21544**	GirlFriend 1.0, Beta-1.35
6670-71	DeepThroat	**22222**	Prosiak
6969	GateCrasher, Priority	**23456**	Evil FTP, Ugly FTP
7000	Remote Grab	**26274**	Delta
7300-08	NetMonitor	**30100-02**	NetSphere 1.27a
7789	ICKiller	**31337-38**	Back Orifice, DeepBO
8787	BackOfrice 2000	**31339**	NetSpy DK
9872-9875	Portal of Doom	**31666**	BOWhack
9989	iNi-Killer	**33333**	Prosiak
10607	Coma 1.0.9	**34324**	BigGluck, TN
11000	Senna Spy	**40412**	The Spy
11223	Progenic trojan	**40421-26**	Masters Paradise
12223	Hack'99 KeyLogger	**47262**	Delta

12345-46	GabanBus, NetBus	**50505**	Sockets de Troie
12361, 12362	Whack-a-mole	**50766**	Fore
16969	Priority	**53001**	Remote Windows Shutdown
20001	Millennium	**54321**	SchoolBus .69-1.11
20034	NetBus 2.0, Beta-NetBus 2.01	**61466**	Telecommando
1863	XtremeRAT	**65000**	Devil
1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT	**5000**	SpyGate RAT, Punisher RAT
		6666	KilerRat, Houdini RAT

TABLE 7.2: Trojans and corresponding port of attack



How to Infect Systems Using a Trojan

An attacker can control the hardware as well as software on the system remotely by installing Trojans. Once Trojan installed on the system, the data become vulnerable to threats as well as the chances are that the attacker can perform attacks on the third-party system. Attackers deliver Trojans in many ways to infect target systems:

- Trojans are included in bundled shareware or downloadable software. When users download such files, the target systems automatically install the Trojans.
- Different pop-up ads try to trick users. They are programmed by the attacker in such a way that it does not matter whether users click YES or NO; a download will begin, and the Trojan will install itself on the system automatically.
- Attackers send the Trojans as email attachments. When users open these malicious attachments, the Trojans are installed automatically.
- Users are sometimes tempted to click on different kinds of files such as greeting cards, porn videos, and images, which might contain Trojans. Clicking on them installs the Trojans.

Below is the step-by-step process that attackers follow to infect a target machine using a Trojan:

- **Step 1**: Create a new Trojan packet using a Trojan Horse Construction Kit.

  New Trojan horses of your choice can be constructed using various Trojan horse construction Kits such as DarkHorse Trojan Virus Maker. New Trojans have a higher chance of succeeding in compromising the target system, as the security mechanisms might fail to detect them.

- **Step 2**: Create a dropper, which is a part of a Trojanized packet that installs the malicious code on the target system.
- **Step 3**: Create a wrapper, using various wrapper tools such as petite.exe, Graffiti.exe, IExpress Wizard, and Elite Wrap, to help bind the Trojan executable to legitimate files to install it on the target system.
- **Step 4:** Propagate the Trojan, implementing various methods such as sending it via email and instant messengers, tricking users to download and execute it. An active Trojan can perform malicious activities such as irritating users with constant pop-ups, changing desktops, changing or deleting files, stealing data, creating backdoors, etc.
- **Step 5:** Execute the Dropper, software used by attackers to disguise their malware (viruses, Trojans, worms, etc.). It is an executable file containing other compressed files. Dropper appears to users to be a legitimate application or well-known and trusted file. However, when run, the Dropper extracts the malware components hidden in it and executes them, usually without saving them to the disk, to avoid detection. Droppers include images, games, or benign messages in their package, which serve as a decoy to focus attention away from malicious activities.
- **Step 6:** Execute the damage routine. Most of the malware contains a damage routine that delivers payloads. Some payloads just display images or messages, whereas other payloads can even delete files, reformat hard drives, or cause other damage.

Trojan Horse Construction Kit

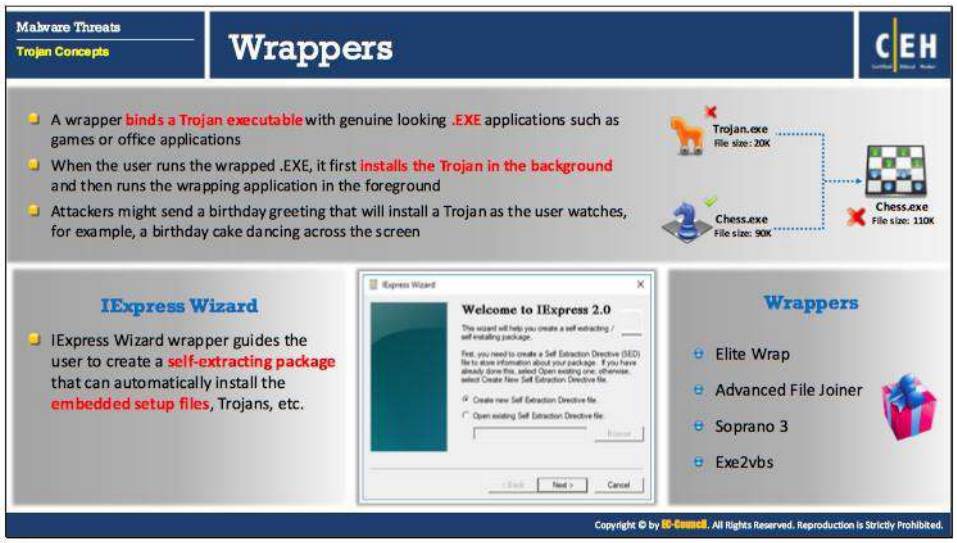
Trojan horse construction kits help attackers construct Trojan horses and customize them according to their needs. These tools can be dangerous and can backfire if not executed properly. New Trojans created by attackers go unnoticed when scanned through a virus or Trojan scanning tools, as they do not match any known signatures. This added benefit allows attackers to succeed in launching attacks.

- **DarkHorse Trojan Virus Maker**

  DarkHorse Trojan Virus Maker is used to creates user-specified Trojans by selecting from various options available. The Trojans created to act as per the options selected while creating them. For e.g., if you choose the option **Disable Process**, the Trojan disables all processes on the target system. The screenshot in the slide shows a snapshot of Dark Horse Trojan Virus Maker that displays its various available options.

Some of the additional Trojan Horse construction kits include:

- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker



Wrappers

Wrappers bind the Trojan executable with a genuine-looking .EXE application such as games or office applications. When the user runs the wrapped .EXE application, it first installs the Trojan in the background and then runs the wrapping application in the foreground. The attacker can compress any (DOS/WIN) binary with tools such as petite.exe. This tool decompresses an EXE file (once compressed) on runtime. This makes it possible for the Trojan to get in virtually undetected, as most anti-virus software is not able to detect signatures in the file.

The attacker can place several executables inside one executable as well. These wrappers may also support functions such as running one file in the background while another one on the desktop.

Technically speaking, wrappers are a type of "glueware" used to bind other software components together. A wrapper encapsulates several components into a single data source to make it usable in a more convenient fashion than the original unwrapped source.

The lure of free software can trick users into installing Trojan horses. For instance, a Trojan horse might arrive in an email described as a computer chess game. When the user receives the email, the description of the game may lead them to install it. Although it may, in fact, be a game, once the user installs the game file, the Trojan gets installed in the background and will be performing other actions that are not readily apparent to the user, such as deleting files or mailing sensitive information to the attacker. In another instance, an attacker sends a birthday greeting that will install a Trojan as the user watches, for e.g., a birthday cake dancing across the screen.

Wrapper Covert Programs

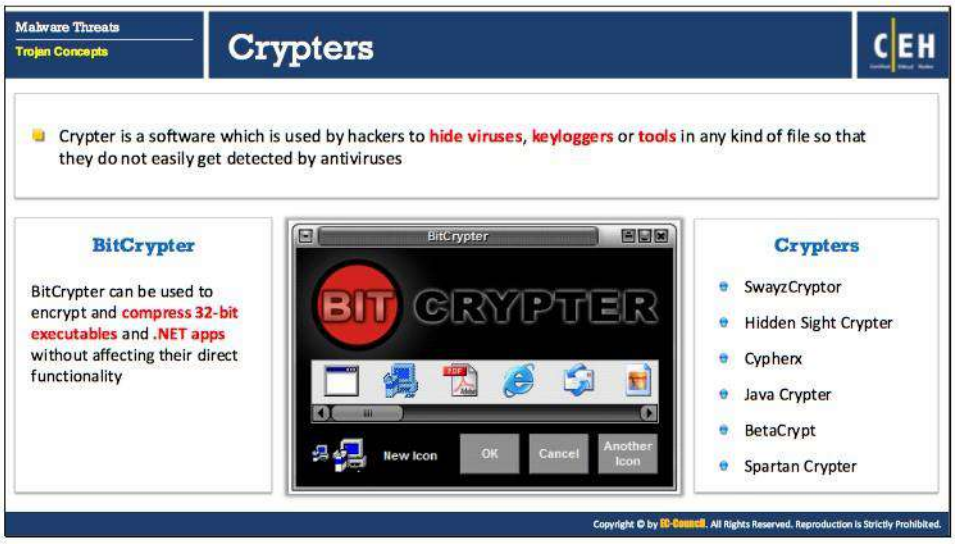
Given below are few Wrapper Covert programs that an attacker can use to carry out his/her malicious activities:

- **IExpress Wizard**

  IExpress Wizard is a wrapper program that guides the user to create a self-extracting package that can automatically install the embedded setup files, Trojans, etc. IExpress can remove the setup files after the executions which erase the trace of Trojans and then run a program or only extract hidden files. These embedded Trojans cannot be detected by anti-virus software.

Some of the additional wrapper tools include:

- Elite Wrap
- Advanced File Joiner
- Soprano 3
- Exe2vbs
- Kriptomatik



Crypters

Crypter is a software that encrypts the original binary code of the .exe file. Attackers use crypters to hide viruses, spyware, keyloggers, Remote Access Trojans (RATs), among others, to make them undetectable by anti-viruses. Follwng are few crypters that one can use to hide malicious programs from being detected by security mechanisms.

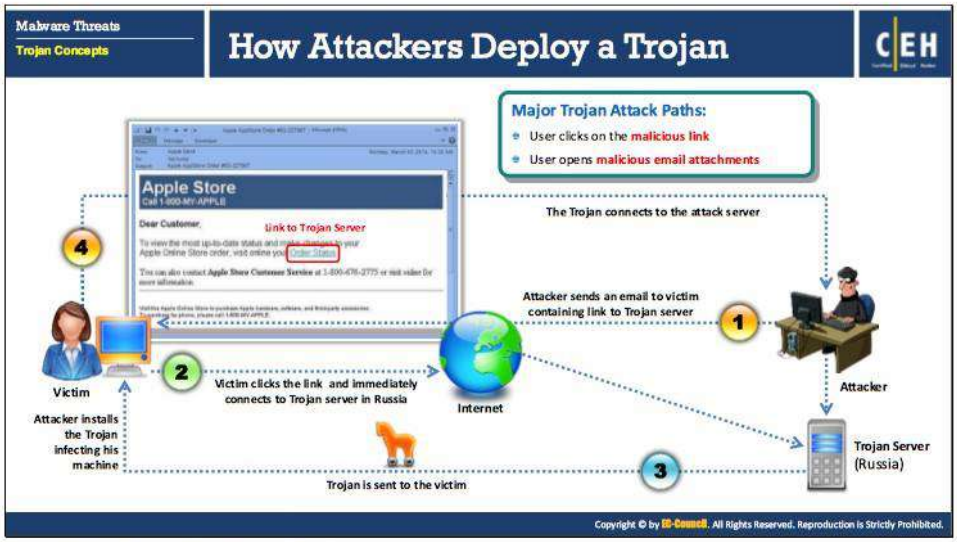
- **BitCrypter**

  Source: *https://www.crypter.com*

  BitCrypter can be used to encrypt and compress 32-bit executables and .NET apps without affecting their direct functionality. A Trojan or malicious software piece can be encrypted onto a legitimate software to bypass firewalls and anti-virus software. The BitCrypter supports a wide range of OSs from Windows XP to the latest Windows 10.

Some of the additional crypter tools include:

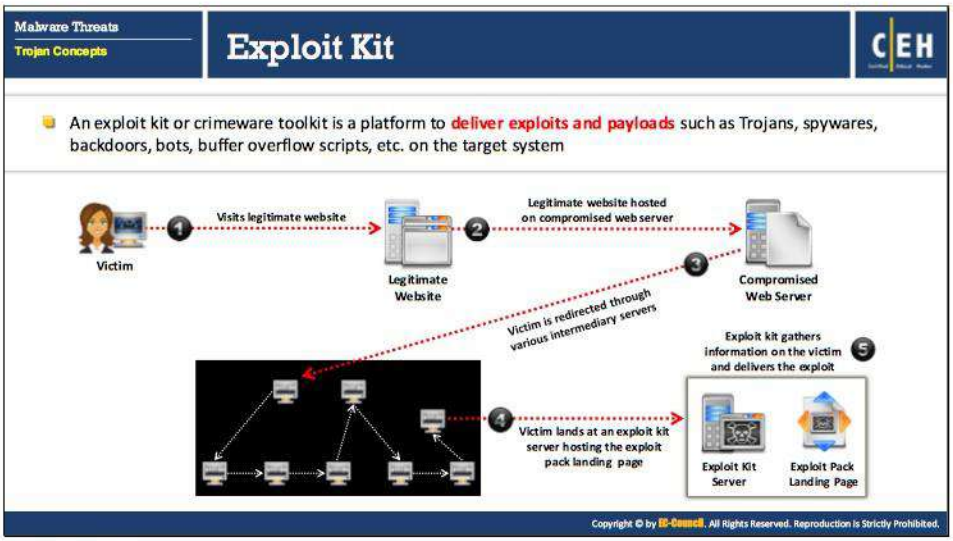
- SwayzCryptor (*https://www.nulledblog.com*)
- Hidden Sight Crypter (*http://www.best-fud-crypters.com*)
- Cypherx (*http://cypherx.org*)
- Java Crypter (*http://megacrypter.us*)
- BetaCrypt (*https://www.fudexploits.com*)
- Spartan Crypter (*https://spartanproducts.pw*)



How Attackers Deploy a Trojan

A Trojan is the means by which an attacker can gain access to the victim's system. To gain control over the victim's machine, an attacker creates a Trojan server, and then sends an email that lures the victim to click on a link provided within the mail. As soon as the victim clicks the malicious link sent by the attacker, it connects directly to the Trojan server. The Trojan server then sends a Trojan to the victim system that undergoes automatic installation on the victim's machine and infect it. As a result, the victim's device establishes a connection to the attack server unknowingly. Once the victim connects to an attacker's server, the attacker can take complete control over the victim's system and perform any selective action. If the victim carries out an online transaction or purchase, then the attacker can easily steal sensitive information such as credit card details and account information. In addition, an attacker can also use the victim's machine to launch attacks on other systems.

The Trojan may infect the computers when a user opens an email attachment that installs a Trojan on their computers that might serve as a backdoor for criminals for later access of the system.

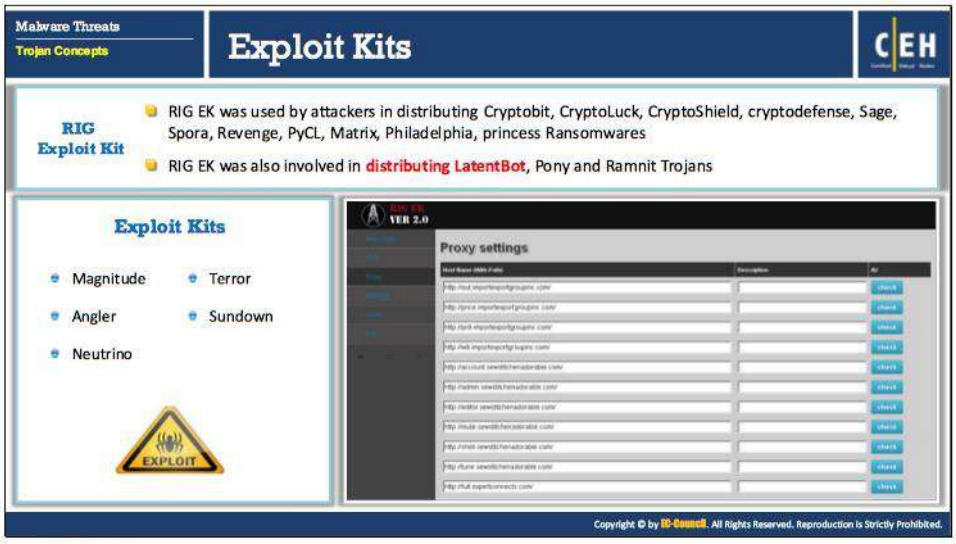


Exploit Kit

An exploit kit or crimeware toolkit is used to exploit security loopholes found in software applications such as Adobe Reader, Adobe Flash Player, etc. by distributing malware such as spyware, viruses, Trojans, worms, bots, backdoors, buffer overflow scripts, or other payloads to the target system. Exploit kits come with pre-written exploit codes. Thus it is easy to use for an attacker who is not an IT or security expert. They also provide a user-friendly interface to track the infection statistics and a remote mechanism to control the compromised system. Using Exploits kits, an attacker can target browsers, programs that are accessible using browser, zero-day vulnerabilities, and exploits updated with new patches. Exploit kits are used against users running insecure or outdated software applications on their systems.

The diagram above shows the general procedure for an exploit kit, though the process of exploiting a machine might vary for different exploit kits:

- The victim visits a legitimate website that is hosted on the compromised web server.
- The victim is redirected through various intermediary servers.
- The victim unknowingly lands on an exploit kit server hosting the exploit pack landing page.
- The exploit kit gathers information on the victim, based on which it determines the exploit and delivers it to the victim's system.
- If the exploit succeeds, a malware program is downloaded and executed to the victim's system.



Exploit Kits

- **RIG Exploit Kit**

  The RIG Exploit kit is one of the most popular exploit kits in recent times with its wide range of malware distribution. RIG EK was first discovered in 2014 and is working efficiently in distributing many exploits. RIG EK was used successfully by attackers in distributing Cryptobit, CryptoLuck, CryptoShield, CryptoDefense, Sage, Spora, Revenge, PyCL, Matrix, Philadelphia, and princess Ransomwares. RIG EK was also involved in distributing LatentBot, Pony and Ramnit Trojans. RIG was also involved in delivering the famous banking Trojan ZeuS. The latest version of the RIG exploit kit is taking advantage of outdated versions of applications such as Flash, Java, Silverlight, Internet Explorer, or Microsoft Edge to distribute the Cerber ransomware.

  Features:

  - RIG EK landing page is performed via a standard 302 Redirect
  - Domain auto-rotator to avoid blacklisting and detection
  - FUD (entirely undetectable) exploits
  - Combines different web technologies, such as DoSWF, JavaScript, Flash and VBScript to obfuscate the attack

RIG Exploit kit support for different browsers, as well as listing the following CVEs:

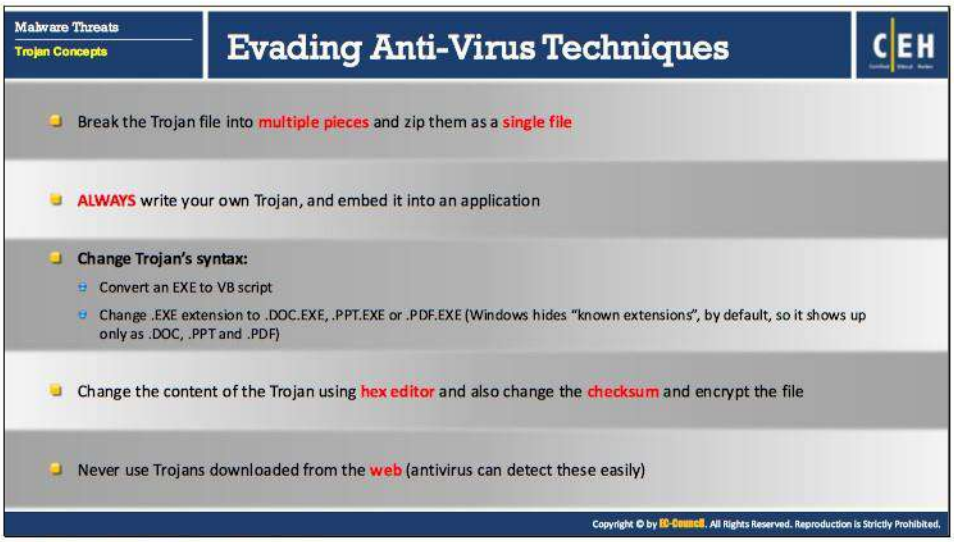
CVE-2013-2551	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0322	Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability
CVE-2014-0497	Adobe Flash Player Remote Code Execution Vulnerability

CVE-2013-0074	Microsoft Silverlight Double Deference Remote Code Execution Vulnerability
CVE-2013-2465	Oracle Java SE Memory Corruption Vulnerability
CVE-2012-0507	Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability
CVE-2014-6332	Windows OLE Automation Array Remote Code Execution Vulnerability.
CVE-2015-2419	JScript9 Memory Corruption Vulnerability
CVE-2016-0189	Scripting Engine Memory Corruption Vulnerability
CVE-2015-8651	Integer overflow in Adobe Flash Player Vulnerability

TABLE 7.3: List of CVEs for RIG Exploit Kit

Some of the additional exploit kits include:

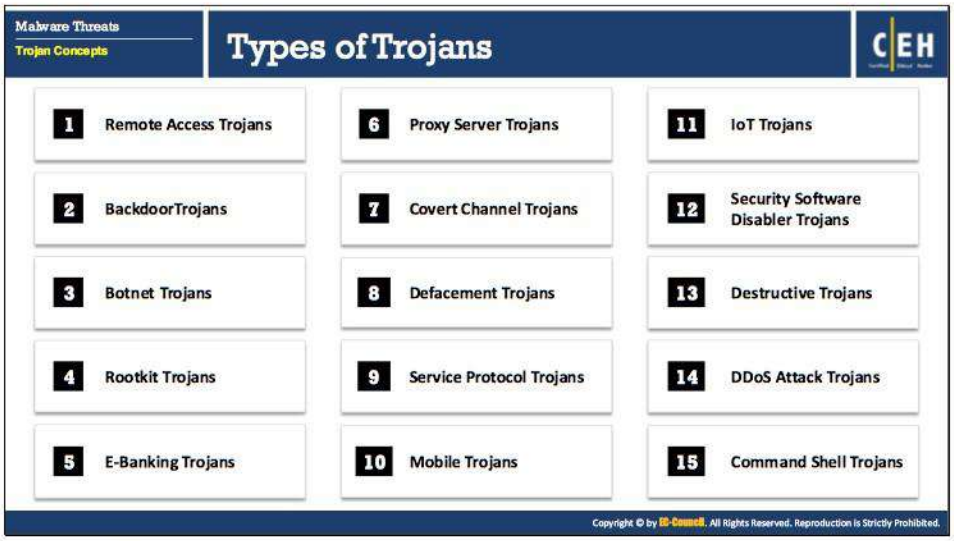
- Magnitude
- Angler
- Neutrino
- Terror
- Sundown
- Pheonix
- Blackhole
- Bleedinglife
- Crimepack
- Hunter
- Nuclear



Evading Anti-Virus Techniques

Following is the list of various techniques can be used to make malware such as Trojans, viruses, and worms, which are undetectable by anti-virus applications.

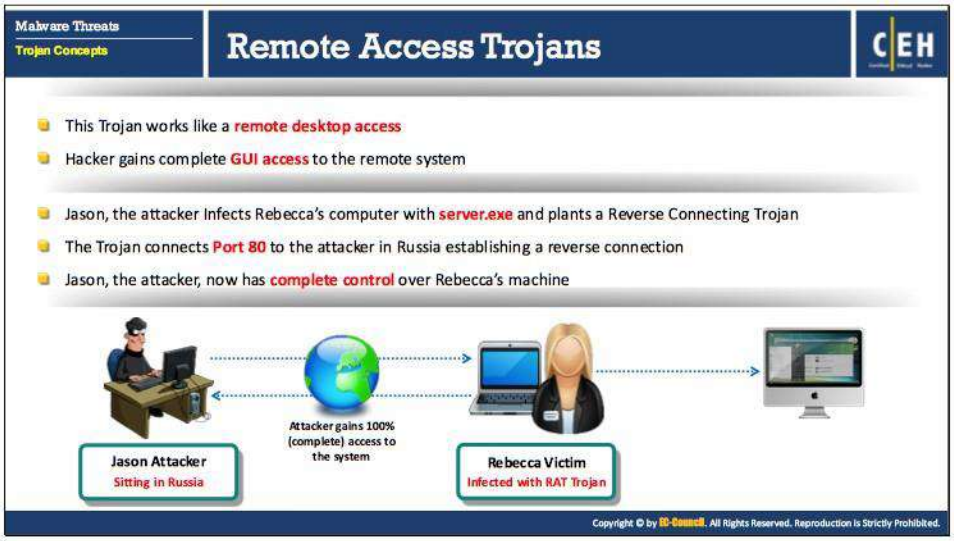
1. Break the Trojan file into multiple pieces and zip them as a single file.
2. Always write your Trojan and embed it into an application (an anti-virus program fails to recognize new Trojans, as its database does not contain the proper signatures).
3. Change the Trojan's syntax:
   - Convert an EXE to VB script
   - Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hides "known extensions," by default, so it shows up only as .DOC, .PPT and .PDF)
4. Change the content of the Trojan using a hex editor.
5. Change the checksum, and encrypt the file.
6. Never use Trojans downloaded from the Web (anti-virus detects these easily).
7. Use binder and splitter tools that are capable of changing the first few bytes of the Trojan programs.
8. Perform code obfuscation or morphing. Morphing is done to confuse the anti-virus program from differentiating between a malicious and harmless program.

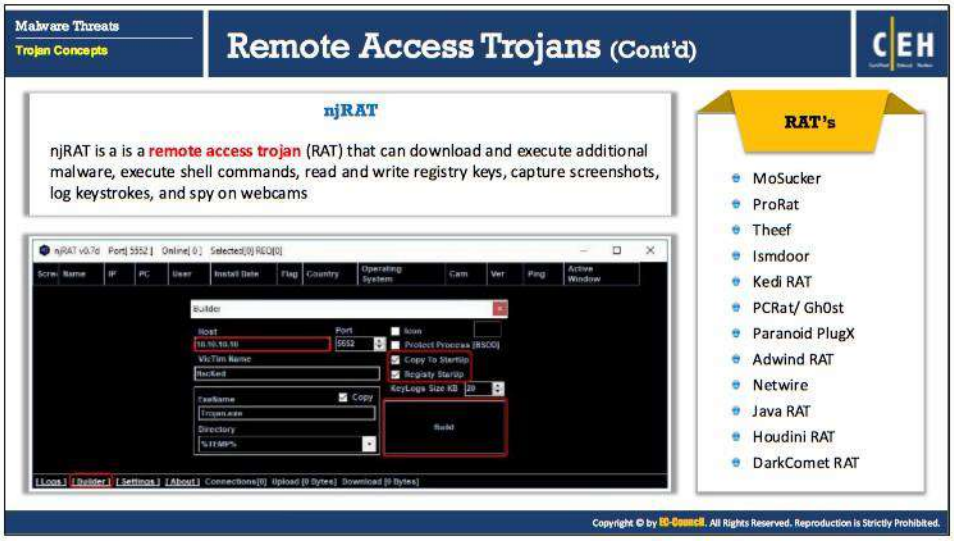


Types of Trojans

Trojan are classified into many categories depending on the exploit functionality. Following is the list of some of the Trojans types:

1. Remote Access Trojans
2. Backdoor Trojans
3. Botnet Trojans
4. Rootkit Trojans
5. E-Banking Trojans
6. Proxy Server Trojans
7. Covert Channel Trojans
8. Defacement Trojans
9. Service Protocol Trojans
10. Mobile Trojans
11. IoT Trojans
12. Security Software Disabler Trojans
13. Destructive Trojans
14. DDoS Attack Trojans
15. Command Shell Trojans





Remote Access Trojans

Remote access Trojans (RATs) provide attackers with full control over the victim's system, enabling them to remotely access files, private conversations, accounting data, and others. The RAT acts as a server and listens on a port that is not supposed to be available to Internet attackers. Therefore, if the user is behind a firewall on the network, there is less chance that a remote attacker would be able to connect to the Trojan. The attackers in the same network located behind the firewall can easily access Trojans.

For e.g., Jason is an attacker who intends to exploit Rebecca's computer to steal her data. Jason infects Rebecca's computer with server.exe and plants a Reverse Connecting Trojan. The Trojan connects to Port 80 to the attacker sitting in Russia, establishing a reverse connection. Now, Jason has complete control over Rebecca's machine.

Attackers use RATs to infect the target machine to gain administrative access. RATs help an attacker to remotely access complete GUI, control victim's computer without his or her awareness and are capable of performing screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and so on. It infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

- **njRAT**

  njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing the process and file manipulations, and viewing the victim's desktop.

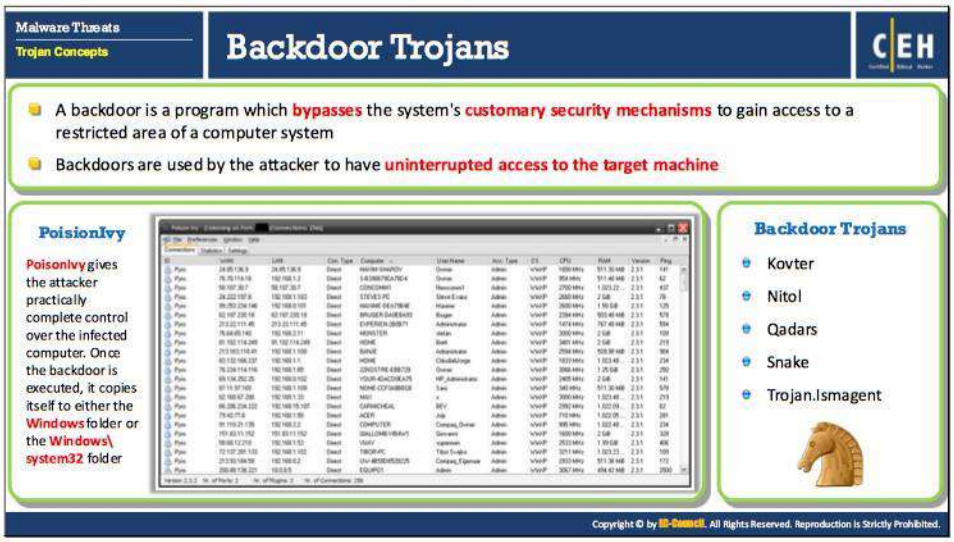
  This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

  Features:

  - Remotely access victim's computer
  - Collect victim's information like IP address, hostname, OS, etc.
  - Manipulate files and system files
  - Open active remote session providing attacker access to victim machine's command line
  - Log keystrokes and steal credentials from browsers

Some of the additional remote access Trojans include:

- MoSucker
- ProRat
- Theef
- Ismdoor
- Kedi RAT
- PCRat/ Gh0st
- Paranoid PlugX
- Adwind RAT
- Netwire
- Java RAT
- Houdini RAT
- DarkComet RAT
- Pandora RAT
- Xtreme RAT
- SpyGate – RAT
- KilerRat



Backdoor Trojans

A backdoor is a program which can bypass the standard system authentication or conventional system mechanism like IDS, firewalls, etc. without being detected. In these types of breaches, hackers leverage backdoor programs to access the victim's computer or a network. The difference between this type of malware and other types of malware is that the installation of the backdoor is performed without the user's knowledge. This allows the attack to perform any activity on the infected computer which can include transferring, modifying, corrupting files, installing malicious software, rebooting the machine, etc. without user detection. Backdoors are used by the attacker to have uninterrupted access to the target machine. Most of the backdoors are used for targeted attacks. Backdoor Trojans are often used to group victim computers to form a botnet or zombie network that can be used to perform criminal activities.

Backdoor Trojans are often initially used in the second (point of entry) or third (command-and-control [C&C]) stage of the targeted attack process. The main difference between a RAT and a traditional backdoor is that the RAT has a user interface, the client component, which can be used by the attacker to issue commands to the server component residing in the compromised machine whereas a backdoor does not.

For e.g., a hacker who is performing a malicious activity identifies vulnerabilities in a target network. Hacker implants **networkmonitor.exe** backdoor in the target network, and the backdoor will be installed in a victim machine on the target network without being detected by network security mechanisms. Once installed, **networkmonitor.exe** will provide uninterrupted access to the victim's machine and target network to the attacker.

- **PoisonIvy**

  PoisonIvy gives the attacker practically complete control over the infected computer. PoisonIvy Remote Administration Tool is created and controlled by a PoisonIvy management program or kit. The PoisonIvy kit consists of a graphical user interface, and the backdoors are small and are typically under 10kB in size.

  Once the backdoor is executed, it copies itself to either the **Windows** folder or the **Windows\system32** folder. The filename and locations of the backdoor are defined by the creator of the backdoor when using the PoisonIvy kit to create the server program. Some variants of PoisonIvy are capable of copying themselves into an Alternate Data Stream.

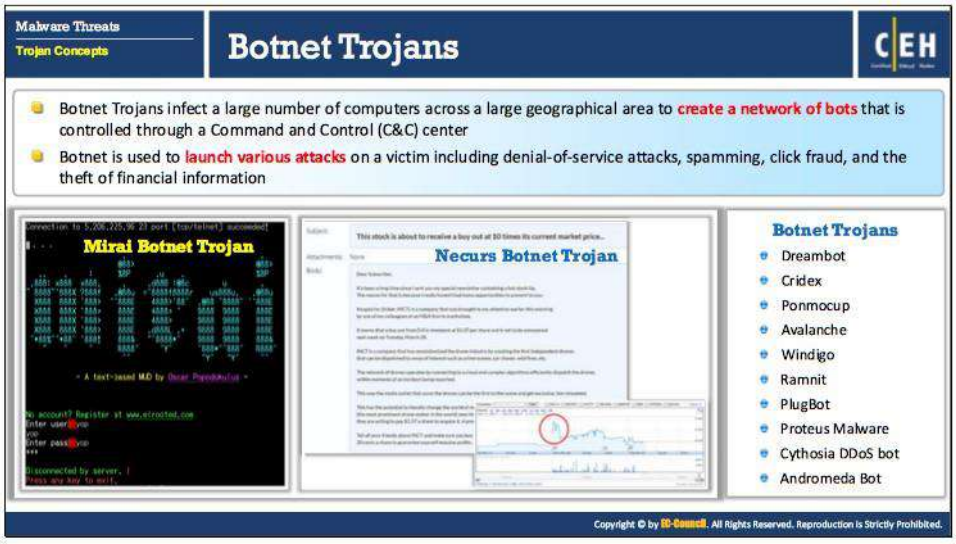
  A registry entry of the backdoor will be added to ensure that the backdoor is started every time the computer is booted up. The server then connects to a client using an address defined when the server-part was created. The communication between the server and client programs is encrypted and compressed. PoisonIvy can be configured to inject itself into a browser process before making an outgoing connection to help in bypassing firewalls.

  Features:

  - File modification, deletion, and transfer to and from the infected system
  - The Windows registry can be viewed and edited
  - Currently, running processes can be viewed and suspended or killed
  - Current network connections can be viewed and shut down
  - Services can be viewed and controlled (for example stopped or started)
  - Installed devices can be viewed, and some devices can be disabled
  - The list of installed applications can be viewed, and entries can be deleted or programs can be uninstalled
  - Access Windows Command shell on the infected computer
  - Steal information by taking screenshots of the desktop and recording audio or webcam footage
  - Access saved passwords and password hashes

Some of the additional backdoor Trojans include:

- Kovter
- Nitol
- Qadars
- Snake
- Trojan.Ismagent
- BackDoor.Ragebot.45
- z3r0 Remvio
- Backdoor.Psiload



Botnet Trojans

Today, most large information security attacks involve botnets. Attackers (also known as "bot herders") use Botnet Trojans to infect a large number of computers throughout a large geographical area to create a network of bots (or a "bot herd") that can control via a Command and Control (C&C) center. They trick regular computer users to download Trojan infected files to their systems through phishing, SEO hacking, URL redirection, among others. Once the user downloads and executes this Botnet Trojan in the system, it connects back to the attacker using IRC channels and waits for further instruction. Some of the botnet Trojans also have worm features and automatically spread to other systems in the network. They help an attacker to launch various attacks and perform nefarious activities such as denial-of-service attacks, spamming, click fraud, theft of application serial numbers, login IDs, and credit card numbers.

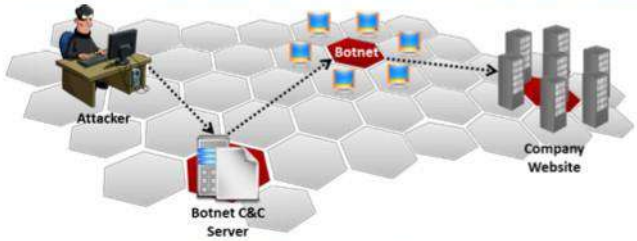


FIGURE 7.2: Functioning of Botnet

- **Necurs**

  The Necurs botnet is a distributor of many pieces of malware, most notably Dridex and Locky. It delivers some of the worst banking Trojans and ransomware threats in batches of millions of emails at a time, and it keeps reinventing itself. Necurs gets distributed by

Spam e-mails and downloadable content from questionable/illegal sites. Necurs is indirectly responsible for a significant portion of cybercrime. On 20 March 2017, Necurs botnet engaged in a pump&dump spam scheme that tried to boost Incapita company's stock market price artificially.

Features:

- Destruction of the system
- Turning PC into a spying tool
- Electronic money theft
- Botnet and mining
- Serving as a gateway for other viruses

- **Mirai**

  Mirai is a self-propagating botnet that infects poorly protected internet devices (IoT devices). Mirai uses telnet port (23 or 2323) to find those devices that are still using their factory default username and password. Most of the IoT devices use default usernames and passwords and Mirai botnet has the ability to infect such multiple insecure devices and co-ordinate them to mount a DDoS attack against a chosen victim.

  Features:

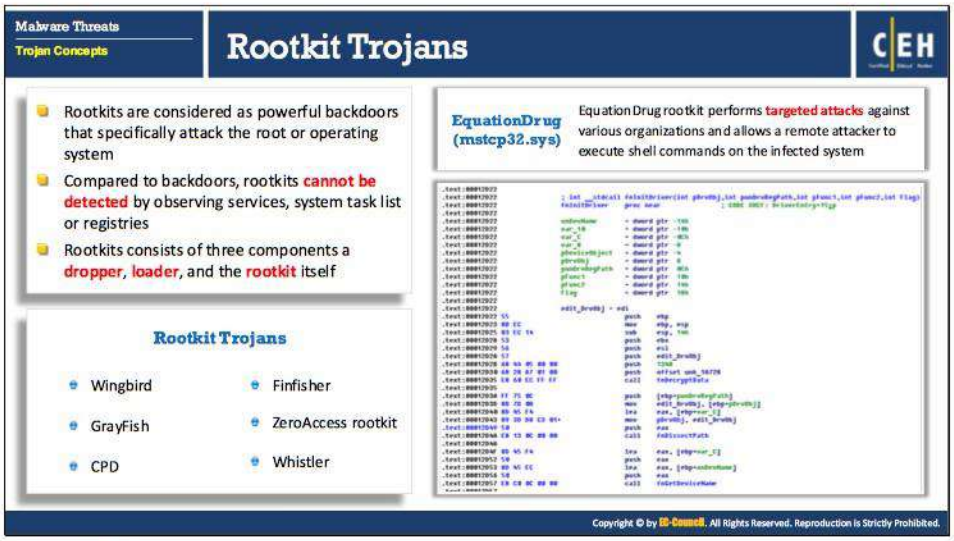
  - Login attempts with 60 different factory default username and password pairs
  - Built for multiple CPU architectures (x86, ARM, Sparc, PowerPC, Motorola)
  - Connects to CnC to allows the attacker to specify an attack vector
  - Increases bandwidth usage for infected bots
  - Identify and remove competing malware
  - Blocks remote administration ports

  Prevention:

  - Using Anti-Trojan softwares and updating usernames and passwords can prevent Mirai DDoS botnet Trojan attack.

Some of the botnet Trojans include:

- Dreambot
- Cridex
- Ponmocup
- Avalanche
- Windigo
- Ramnit
- PlugBot
- Proteus Malware
- Cythosia DDoS bot
- Andromeda Bot
- Dorkbot



Rootkit Trojans

As the name indicates, rootkit consists of two terms "Root" and "Kits" where "Root" is a UNIX/Linux term that is the equivalent of Administrator in Windows. The word "kit" denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit. Rootkits are, potent backdoors, which specifically attack the root or OS. Compared to backdoors, rootkits cannot be detected by observing services, system task list or registries. Rootkits provide full control of the victim OS to the attacker. Rootkits can not propagate by themselves, and that fact has precipitated a great confusion. In reality, rootkits are just one component of what is called a blended threat. Blended threats typically consist of three snippets of code: a dropper, loader, and rootkit. The dropper is the executable program or file that installs the rootkit. Activating the dropper program usually entails human intervention, such as clicking on a malicious e-mail link. Once initiated, the dropper launches the loader program and then deletes itself. Once active, the loader typically causes a buffer overflow, which loads the rootkit into memory.

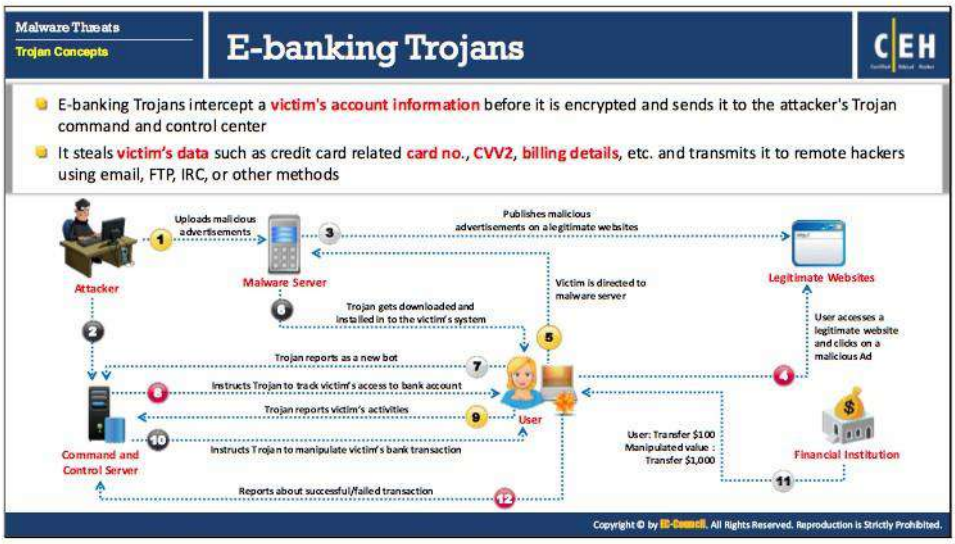
- **EquationDrug Rootkit**

  EquationDrug is a dangerous computer rootkit that attacks the Windows platform. It performs targeted attacks against various organizations and arrives on the infected system by being downloaded and executed by the Trickler dubbed "DoubleFantasy", covered by TSL20110614-01 (Trojan.Win32.Micstus.A). It allows a remote attacker to execute shell commands on the infected system.

Some of the additional rootkit Trojans include:

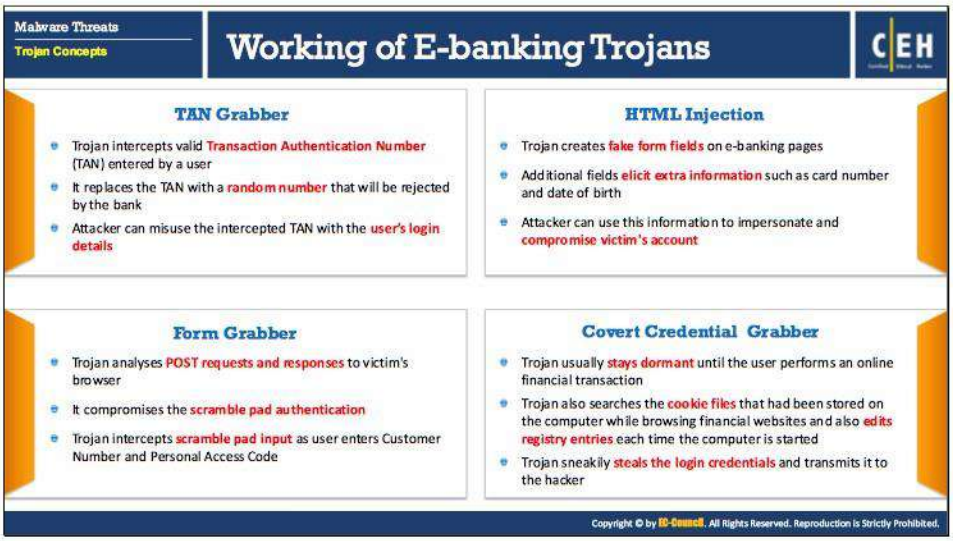
- Wingbird
- GrayFish
- SST
- Finfisher
- ZeroAccess rootkit
- Pihar

- CPD
- Whistler
- Mybios
- MBRoot (Sinowal)
- MBR Locker
- Mebroot
- Mayachok
- Mebratix
- Guntior
- Stoned
- Yurn
- Cidox
- Plite
- XPaj
- Alipop
- Fengd
- Fips
- Niwa
- Ponreb
- Yoddos
- Zegost
- AFX
- Vanquish
- HackerDefender



E-banking Trojans

E-banking Trojans are very dangerous and have become a significant threat to online banking. They intercept victim's account information before the system can encrypt it, and send it to the attacker's command-and-control center. Installation of these Trojans takes place on the target's computer when he or she clicks a malicious email attachment or a malicious advertisement. Attackers program these Trojans to steal minimum and maximum monetary amounts, so that they do not withdraw all the money in the account, which serves to avoid suspicion. These Trojans also create screenshots of the bank account statement, so that the victim thinks that there is no variation in bank balance and is not aware of this fraud unless checks the balance from another system or an ATM. These Trojans may also steal victims' data such as credit card numbers and billing details, and transmit them to remote hackers via email, FTP, IRC, or other methods.



Working of E-banking Trojans

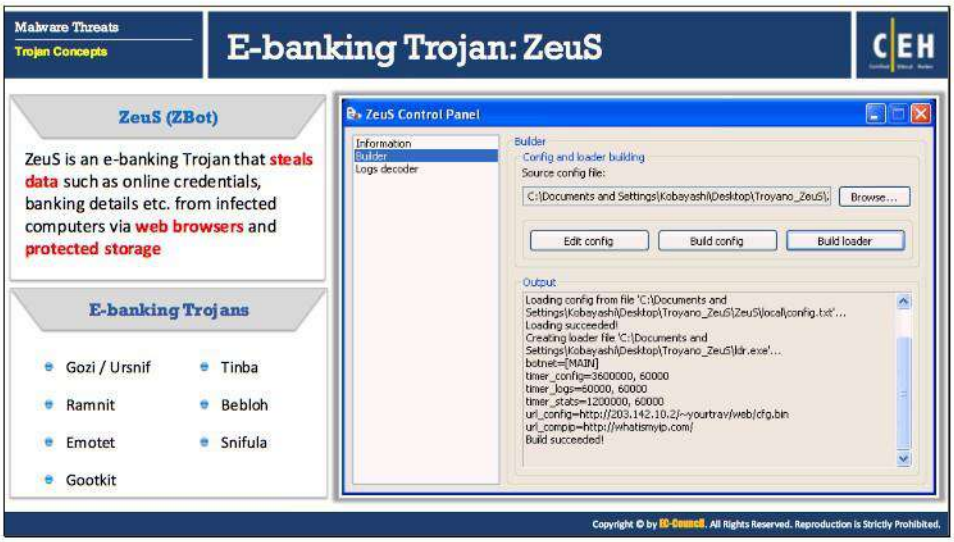
A banking Trojan is a malicious program that allows attackers to obtain personal information about users of online banking and payment systems.

The banking Trojan analysis includes:

- **Tan Gabber**: A Transaction Authentication Number (TAN) is a single-use password for authenticating the online banking transaction. Banking Trojans intercept valid TAN entered by a user and replace it with a random number. The Bank will reject this invalid random number. An attacker after that misuses the intercepted TAN with the target's login details.
- **HTML Injection**: Trojan creates fake form fields on e-banking pages. The attacker collects the target's account details, credit card number, date of birth, etc. The attacker can use this information to impersonate and compromise the target's account.
- **Form Grabber**: Form Grabber is a type of malware that captures a target's sensitive data such as IDs, passwords, and so on from a web browser form or page. It is an advanced method to collect the target's Internet banking information. It analyses POST requests and responses to victim's browser. It compromises the scramble pad authentication and intercepts scramble pad input as the user enters Customer Number and Personal Access Code.
- **Covert Credential Grabber**: This type of malware stays dormant until the user performs an online financial transaction. It works covertly to replicate itself on the computer and edit registry entries each time the computer is started. The Trojan also searches the cookie files that had been stored on the computer while browsing financial websites. Once the user attempts to make an online transaction, the Trojan covertly steals the login

credentials and transmits it to the hacker. Following are some of the methods in which Banking Trojans attempt to steal user's information:

- Keylogging
- Form data capture
- Inserting fraudulent form fields
- Screen captures and video recording
- Mimicking financial websites
- Redirecting to banking websites
- Man-in-the-middle attack



E-banking Trojan: ZeuS

ZeuS also called as ZBot is a banking Trojan horse program (or "crimeware") which was first detected in 2007 and is still one of the most successful and prolific banking trojans in the world. A ZBot trojan is created using a malicious toolkit available on hacker forums and underground marketplaces, which gives the attacker control over the functionality of the executable used to infect victims. ZeuS steals data such as online credentials, banking details, etc. from infected computers via web browsers and protected storage. The Zbot trojan is typically distributed through spam email campaigns and drive-by downloads. Once it is executed, the trojan identifies Internet Explorer, FTP, or POP3 credentials contained within Protected Storage (PStore), which are then compromised and used to authenticate and log in to an account as a legitimate user. It can be updated through a command and control (C2) server for additional functions such as downloading and executing additional files, shutting down or rebooting the victim device, or deleting system files. ZBot trojan also uses a "fast flux" technique to evade detection where Fast flux is a subset of botnets that increases the difficulty of blocking a given IP address range to defend against botnets since defending against the changing IP addresses used by the botnet is challenging, and many times leads to false positives.

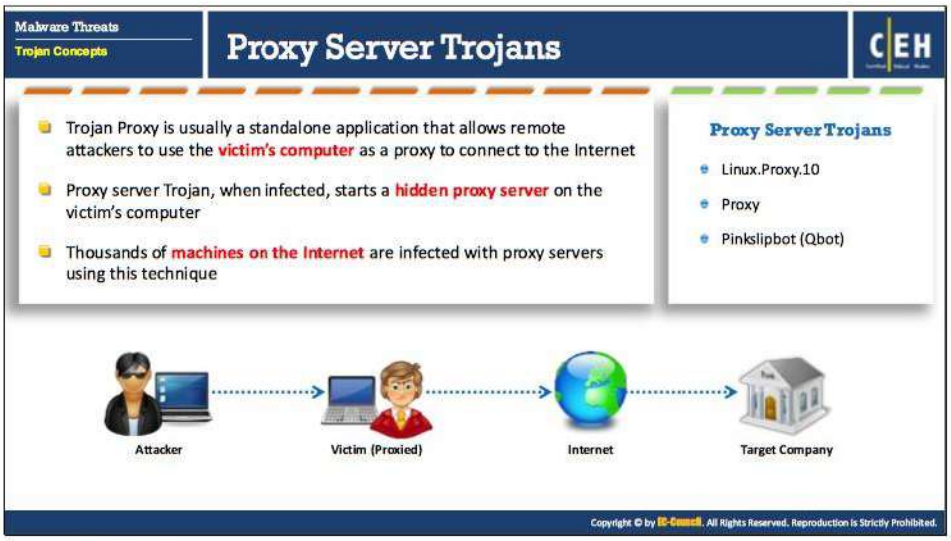
Features:

- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows Protected Storage
- Steals client-side X.509 public-key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies

- Modifies the HTML pages of target websites for information stealing purposes
- Redirects victims from target web pages to attacker-controlled ones
- Takes screenshots and scrapes HTML from target sites
- Searches for and uploads files from the infected computer
- Modifies the local host's file (%systemroot%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

Some of the additional e-banking Trojans include:

- Gozi / Ursnif
- Emotet
- Ramnit
- Gootkit
- Tinba
- Bebloh
- Snifula
- GozNym
- Neverquest
- Rovnix
- Trickbot

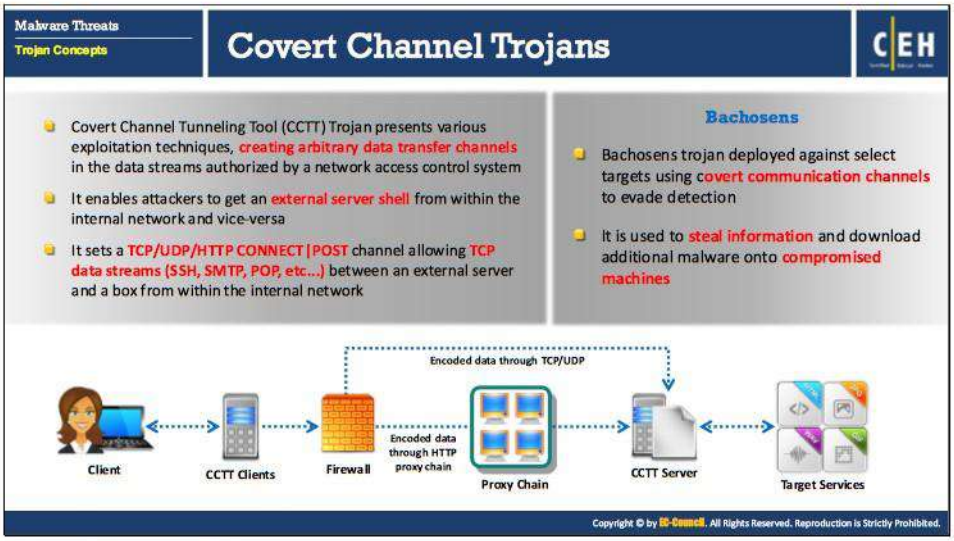


Proxy Server Trojans

Trojan Proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the Internet. Proxy server Trojan, when infected, starts a hidden proxy server on the victim's computer. Attackers use it for anonymous Telnet, ICQ, or IRC to purchase goods using stolen credit cards, as well as other such illegal activities. The attackers have full control over the users' systems and can launch attacks on other systems from an affected user's network. If the authorities detect illegal activity, the footprints lead to innocent users and not to the attackers, potentially leading to legal trouble for the victims, who are ostensibly responsible for their network or any attacks launched from it. Thousands of machines on the Internet are infected with proxy servers using this technique.

Some of the proxy server Trojans include:

- Linux.Proxy.10
- Proxy
- Pinkslipbot (Qbot)



Covert Channel Trojans

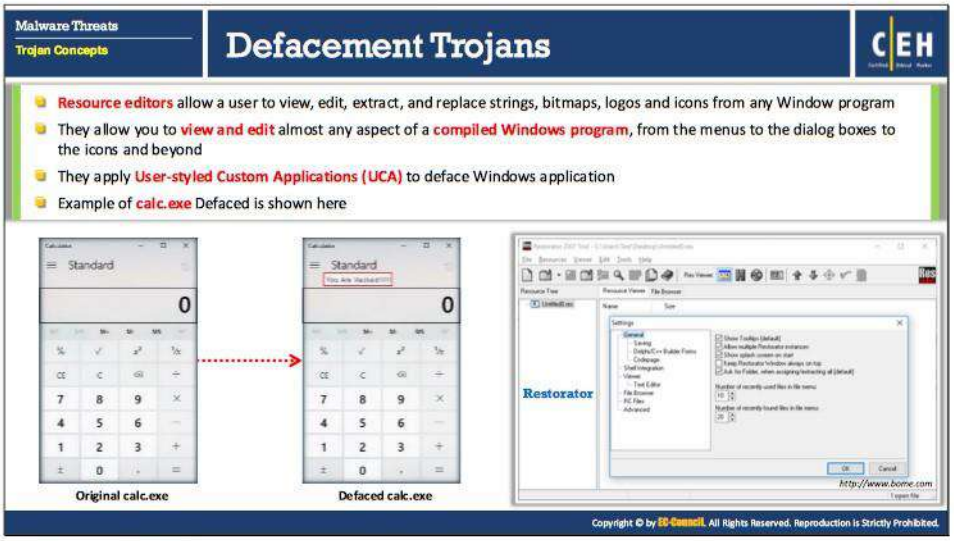
Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system. It enables attackers to get an external server shell from within the internal network and vice-versa. It sets a TCP/UDP/HTTP CONNECT|POST channel allowing TCP data streams (SSH, SMTP, POP, etc.) between an external server and a box from within the internal network.

- **Bachosens Trojan**

  Bachosens is a covert channel trojan discovered in February 2017 and deployed against select targets using covert communication channels to evade detection. It is used to steal information and download additional malware onto compromised machines.

  The trojan creates a registry entry to run every time Windows starts, opens a backdoor to connect to its C2 server, and can then execute the following functions:

  - Log keystrokes
  - Download and execute files
  - Copy files
  - List files
  - Delete files
  - Create directories
  - Delete directories
  - Change registry entries
  - List processes
  - Terminate processes



Defacement Trojans

Defacement Trojans, once spread over the system, can destroy or change the entire content present in a database. However, they are more dangerous when attackers target websites, as they physically change their underlying HTML format, resulting in the modification of their content. There is even significant potential loss resulting from the defacement of e-business targets by Trojans.

Resource editors allow one to view, edit, extract and replace strings, bitmaps, logos, and icons from any Windows program. It allows viewing and editing almost any aspect of a compiled Windows program, from the menus to the dialog boxes to the icons and beyond. They apply User-styled Custom Applications (UCAs) to deface Windows applications.

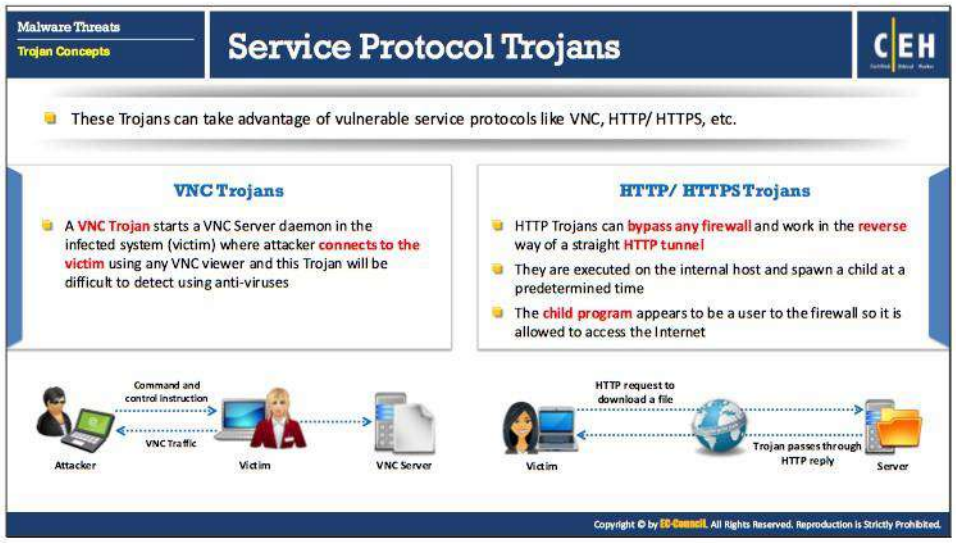
- **Restorator**

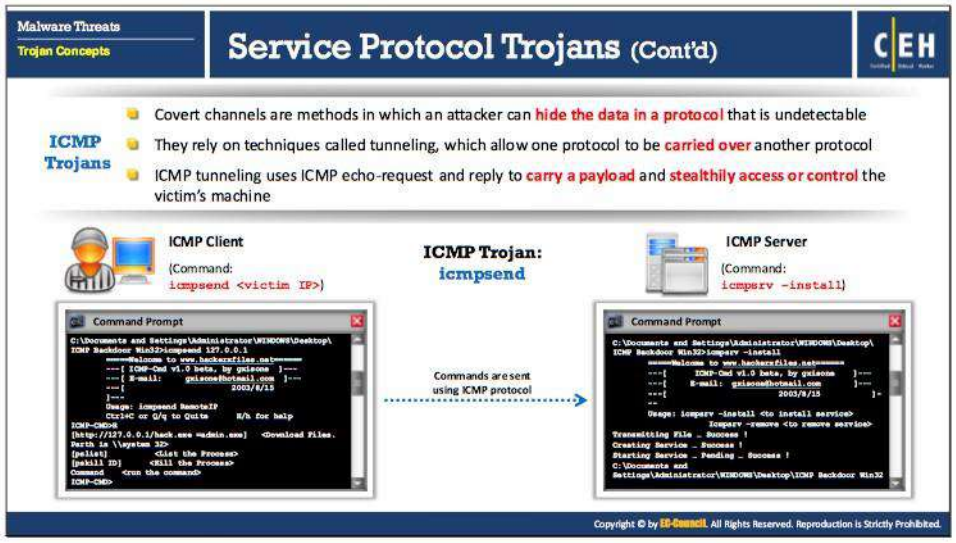
  Source: *http://www.bome.com*

  Restorator is a utility for editing Windows resources in applications and their components (e.g., files with .exe, .dll, .res, .rc, and .dcr extensions). It allows to change, add, or remove resources such as text, images, icons, sounds, videos, version, dialogs, and menus in almost all programs. Using this tool, one can perform translation/localization, customization, design improvement, and development.

  Features:

  - Translate existing applications (localization)
  - Customize the look and feel of programs
  - Replace logos and icons (branding)
  - Enhance control over resource files in the software development process
  - Hack into the inner workings of applications on the computer





Service Protocol Trojans

These Trojans can take advantage of vulnerable service protocols like VNC, HTTP/HTTPS, ICMP, etc. to attack the victim machine.

- **VNC Trojans**

  A VNC Trojan starts a VNC Server daemon in the infected system (victim) where attacker connects to the victim using any VNC viewer. Since VNC program is considered a utility,

this Trojan will be difficult to detect using anti-viruses. Top financial malware such as Dridex, Neverquest, and Gozi employed hvnc (hidden virtual network computing) module, which allows attackers to gain user-grade access to an infected PC

- **HTTP/HTTPS Trojans**

  HTTP/HTTPS Trojans can bypass any firewall, and work in reverse, as opposed to a straight HTTP tunnel. They use web-based interfaces and port 80. The execution of these Trojans takes place on the internal host and spawns a child program at a predetermined time. The child program appears to be a user to the firewall, so the firewall allows the program access to the Internet. However, this child program executes a local shell, connects to the web server that the attacker owns on the Internet through an apparently legitimate HTTP request, and sends it a ready signal. The apparently legitimate answer from the attacker's web server is in reality a series of commands that the child can execute on the machine's local shell. The attacker converts all traffic into a Base64-like structure and gives it as a value for a cgi-string, to avoid detection. The following is an example of a connection:

  Slave: **`GET/cgi-bin/order?`**
  `M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdb1He7krj HTTP/1.0`

  Master replies with: **`g5mAlfbknz`**

  The GET of the internal host (SLAVE) is the command prompt of the shell; the answer is an encoded "`ls`" command from the attacker on the external server (MASTER). The SLAVE tries to connect daily at a specified time to the MASTER. If necessary, the child spawn takes place if the shell hangs, the attacker can check and fix it the next day. In case the administrator sees connections to the attacker's server and connects it to his/her server, the administrator just sees a broken web server because there is a token (password) in the encoded cgi GET request. WWW proxies (e.g., squid, a full-featured web proxy cache1) support is available. The program masks its name in the process listing. The programs are reasonably small, the master and slave programs consisting of only 260 lines per file. Usage is easy: edit rwwwshell.pl for the correct values, execute "rwwwshell.pl slave" on the SLAVE, and run "rwwwshell.pl" on the MASTER just before it is the time at which the slave tries to connect.

  - **SHTTPD**

    SHTTPD is a small HTTP Server that can be embedded inside any program. It can be wrapped with a genuine program (game chess.exe), when executed it will turn a computer into an invisible web server. For instance, an attacker connects to the victim using Web Browser http://10.0.0.5:443 and infect the victim's computer with chess.exe with Shttpd running in the background and listening on port 443 (SSL).

  - **HTTP RAT**

    HTTP RAT utilizes web interfaces and port 80 to gain access. It can be understood simply as a HTTP Tunnel, except it works in the reverse direction. These Trojans are comparatively more dangerous as these work almost ubiquitously where internet can be accessed.

Features

- Displays ads, records personal data/keystrokes
- Downloads unsolicited files, disables programs/system
- Floods Internet connection, and distributes threats
- Tracks browsing activities and hijacks Internet browser
- Makes fraudulent claims about spyware detection and removal

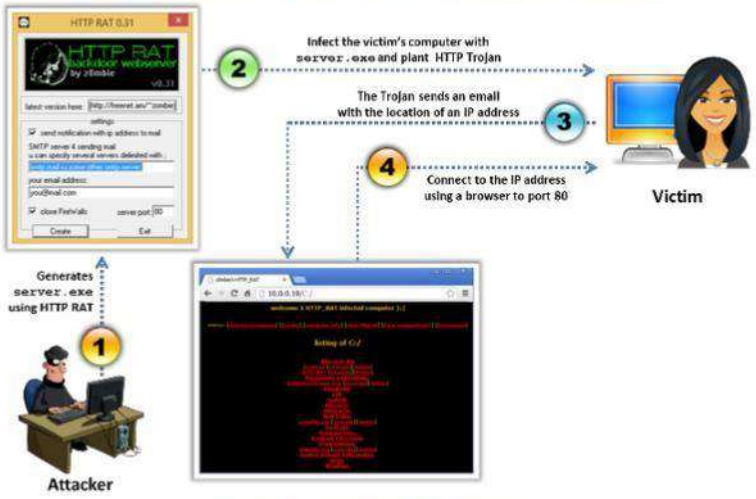


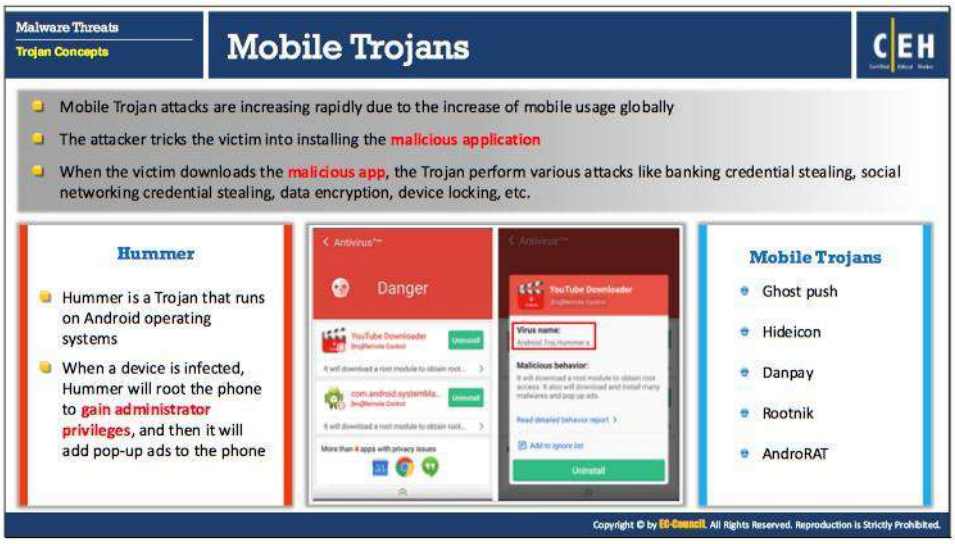
FIGURE 7.3: Working of HTTP RAT Trojan

- **ICMP Trojans**

  Internet Control Message Protocol (ICMP) is an integral part of IP, and every IP module must implement it. It is a connectionless protocol to provide error messages to unicast addresses. The ICMP protocol encapsulates the packets in IP datagrams.

  An Attacker can hide the data using covert channels are methods in a protocol that is undetectable. The concept of ICMP tunneling allows one protocol to be carried over another protocol. ICMP tunneling uses ICMP echo-request and reply to carry a payload and stealthily access or control the victim's machine. Attackers can use the data portion of ICMP_ECHO and ICMP_ECHOREPLY packets for arbitrary information tunneling. Network layer devices and proxy-based firewalls do not filter or inspect the contents of ICMP_ECHO traffic, making the use of this channel attractive to hackers.

  Attackers simply pass, drop, or return the ICMP packets. The Trojan packets themselves are masquerading as common ICMP_ECHO traffic. The packets can encapsulate (tunnel) any required information.



Mobile Trojans

Mobile Trojans are malicious software that targets mobile phones. Mobile Trojan attacks are increasing rapidly due to the global increase of mobile usage. The attacker tricks the victim to install the malicious application. When the victim downloads the malicious app, the trojan performs various attacks like banking credential stealing, social networking credential stealing, data encryption, device locking, etc.

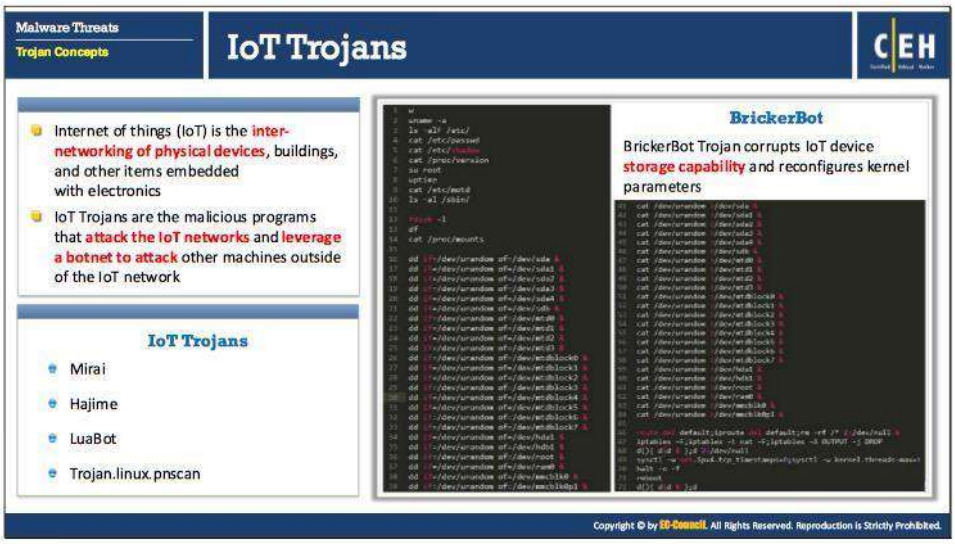
- **Hummer**

  Hummer is a Trojan that runs on Android OSs. The Trojan infected an average 1.19 million devices between January and June 2016, which is nearly double the number of every other known mobile malware. When a device is infected, Hummer will root the phone to gain administrator privileges, and it will add pop-up ads. It then pushes mobile games and installs porn apps in the background. When a user attempts to uninstall them, they will be reinstalled.

Some of the additional mobile Trojans include:

- Ghost push
- AndroRAT
- Hideicon
- Danpay
- Rootnik
- Idownloader
- Flexion
- Lotdoor
- Gedma
- Dowgin
- Ztorg
- Hummingbad
- Hiddad
- 888.apk

- Cron Bot
- Trojan-Banker.AndroidOS.Svpeng.ae
- DangerousObject.Multi.Generic
- Trojan-Banker.AndroidOS.Asacub
- Trojan-Ransom.AndroidOS.Pletor.d



IoT Trojans

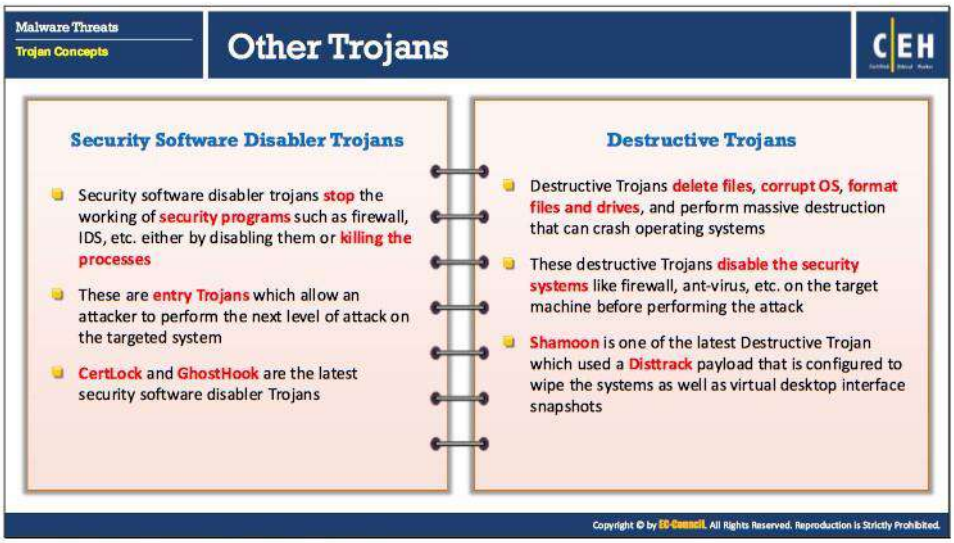
Internet of things (IoT) is the inter-networking of physical devices, buildings, and other items embedded with electronics. IoT Trojans are the malicious programs that attack the IoT networks. These Trojans leverage a botnet to attack other machines outside of the IoT network.

- **BrickerBot**

  BrickerBot is a new malware bricking IoT devices around the world by corrupting their storage capability and reconfiguring kernel parameters. Two different versions of BrickerBot were detected: BrickerBot.1 and BrickerBot.2. In the first stages of the attacks attempting a dictionary brute-force attack on devices with Telnet ports left open on the Internet takes place. If the target device is configured with the default credentials, BrickerBot logs in and performs a series of Linux commands.

Some of the additional IoT Trojans include:

- Mirai
- Hajime
- LuaBot
- Trojan.linux.pnscan



Security Software Disabler Trojans

Security software disabler Trojans stop the working of security programs such as firewall, IDS, etc. either by disabling them or killing the processes. These are entry Trojans which allow an attacker to perform the next level of attack on the targeted system.

Some of the security software disabler Trojans include:

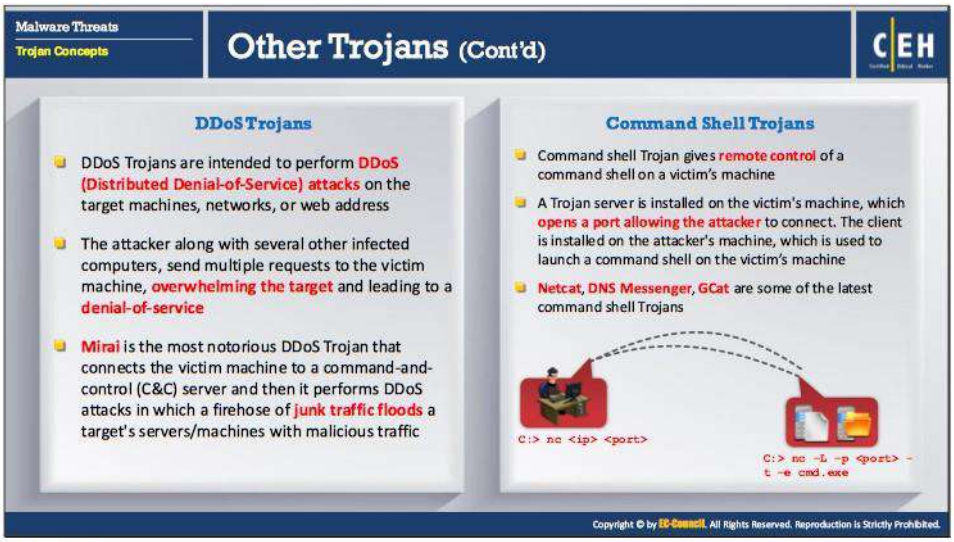
- CertLock
- GhostHook

Destructive Trojans

The sole purpose of writing destructive Trojans is to delete files on a target system. Antivirus software may not detect destructive Trojans. Once a destructive Trojan infects a computer system, it randomly deletes files, folders, and registry entries, and local and network drives often resulting in OS failures.

Destructive Trojans are written as simple crude batch files with commands like "DEL," "DELTREE" or "FORMAT." This destructive Trojan code is usually compiled as .ini, .exe, .dll or .com files. Thus, it is difficult to determine if a destructive Trojan causes a computer system infection. The attacker can activate these Trojans, or it can be set to initiate at a fixed time and date.

Shamoon is the destructive Trojan which attacked the majority of the organization in Saudi Arabia in 2016. Shamoon used a Disttrack payload that is configured to wipe the systems as well as virtual desktop interface snapshots. This Trojan propagated internally by logging in using legitimate domain account credentials, copying itself to the system and creating a scheduled task that executes the copied payload.



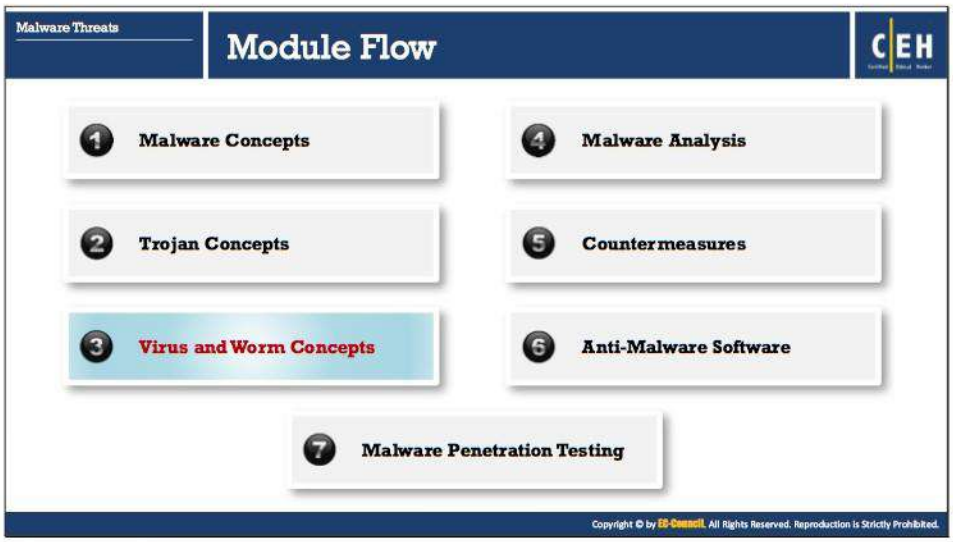
DDoS Trojans

These types of Trojans are intended to perform Distributed Denial-of-Service (DDoS) attack on the target machines, networks or web address. This type of Trojans makes the victim a Zombie to listen for commands sent from a DDoS Server on the internet. There will be numerous infected systems standing by for a command from the server and when the server sends the command to all or a group of infected systems since all the systems perform the command simultaneously, a considerable amount of legitimate requests flood to a target and make the service stop responding. In other words, the attacker, from his computer along with several other infected computers, send multiple requests to the victim, overwhelm the target leading to a denial of service. This can also be achieved by mass spam emailing.

Mirai botnet Trojan is one of the most famous DDoS attack Trojan. It identifies the unsecured devices in a network and enslaves them into a network and uses them to launch DDOS Attack on the victim machine. Once installed on a Windows computer, the Trojan connects to a command-and-control (C&C) server from which it downloads a configuration file containing a range of IP addresses to attempt authentication over several ports such as 22 (SSH) and 23 (Telnet), 135, 445, 1433, 3306 and 3389. Along with the infected Botnet zombies, it performs DDoS attacks in which a zombie flood a target's servers/machines with malicious traffic.

Command Shell Trojans

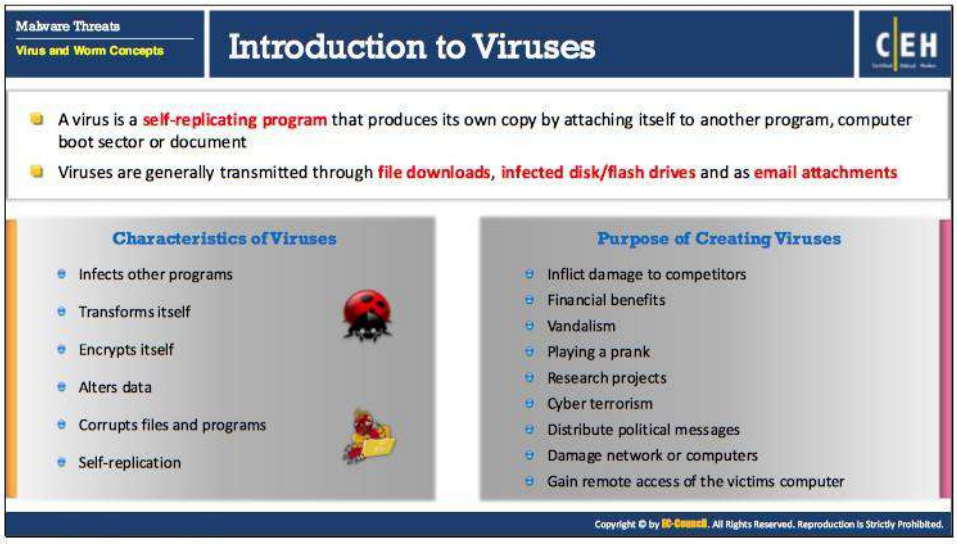
Command Shell Trojan gives the remote control of a command shell on a victim's machine. A Trojan server is installed on the victim's machine, which opens a port allowing the attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim's machine. Netcat, DNS Messenger, GCat are some of the latest Command Shell Trojans.



Virus and Worm Concepts

This section introduces you to various concepts related to viruses and worms and includes an introduction to viruses, stages of virus life, and the workings of viruses. It also explores why people create computer viruses, the indications of virus attack, virus hoaxes, fake antiviruses, and ransomware.

This section highlights different types of viruses, categorized by their origin, techniques used to infect target systems, the types of files they infect, where they hide, the sort of damage they cause, the kind of OS they work on, and so on. This section also deals with computer worms and discusses the difference between worms and viruses, and worm makers.



Introduction to Viruses

Viruses are the scourge of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce itself. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n* number of times.

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user. Like a biological 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. Viruses infect a variety of files, such as overlay files (.OVL) and executable files (.EXE, .SYS, .COM or .BAT). Viruses are transmitted through file downloads, infected disk/flash drives, and as email attachments.

Characteristics of Viruses

The performance of the computer is affected due to virus infection. This infection can lead to data loss, system crash, and file corruption. The following are some of the characteristics of the virus:

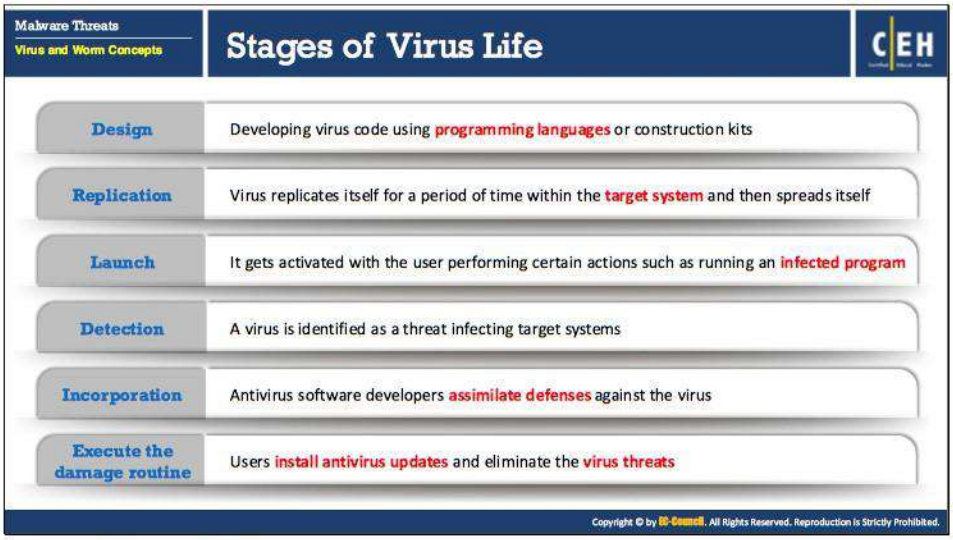
- Infects other programs
- Transforms itself
- Encrypts itself
- Corrupts data, files and programs
- Self-replication

Purpose of Creating Viruses

Attackers create viruses with disreputable motive. Criminals create viruses to destroy a company's data, as an act of vandalism, or to destroy a company's products; however, in some cases, viruses aid the system.

Some of the significant purposes for creating a virus by an attacker are mentioned below:

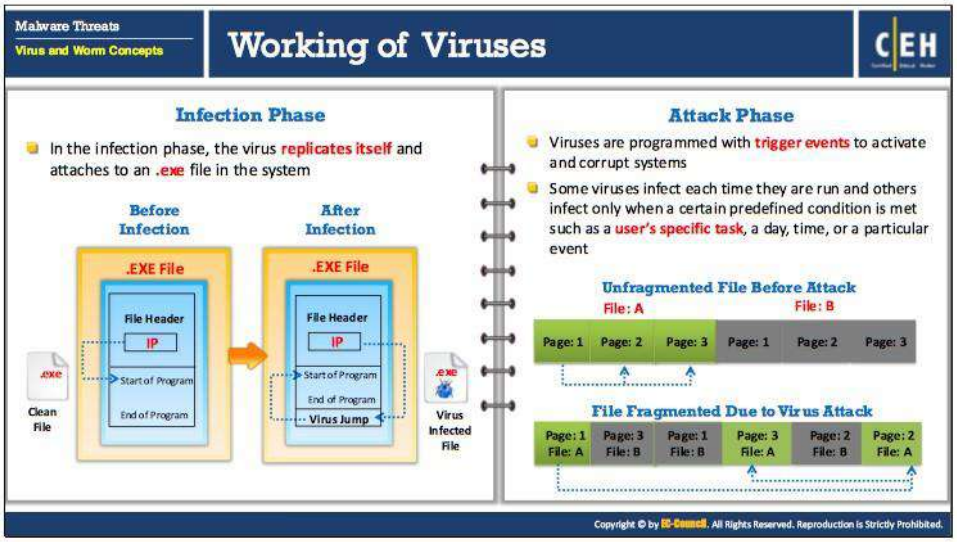
- Inflict damage to competitors
- Financial benefits
- Vandalism
- Play prank
- Research project
- Cyberterrorism
- Distribute political messages
- Damage network or computers
- Gain remote access of the victim's computer



Stages of Viruses Life

Following mentioned are the six stages of virus life from its origin to elimination.

1. **Design:** Developing virus code using programming languages or construction kits.
2. **Replication:** Virus replicates for a period within the target system and then spreads itself
3. **Launch:** It gets activated with the user performing specific 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. **Execute the damage routine:** Users install antivirus updates and eliminate the virus threats



Working of Viruses

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flash cards, pop-ups and so on. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings among others.

Viruses have two phases: the **infection phase** and the **attack phase**.

- **Infection Phase**

  Programs modified by a virus infection can enable virus functionalities to run on that system. The virus infects the target system after getting triggered and becomes active upon the execution of infected programs because the program code leads to the virus code. The two most important factors in the infection phase of a virus are the following:

  - Method of infection
  - Method of spreading

  A virus infects a system using the following sequence:

  - The virus loads itself into memory and checks for the executable on the disk.
  - The virus appends malicious code to a legitimate program without the permission or knowledge of user.

- The user is unaware of the replacement and launches the infected program.
- The execution of an infected program also infects other programs in the system.
- The above cycle continues until the user realizes there is an anomaly in the system.

Apparently, the user unknowingly triggers and executes the virus for it to function. There are many ways to execute programs while a computer is running. For e.g., if the user installs any software tool, the setup program calls various built-in sub-programs during extraction. If a virus program already exists, it can be activated with this kind of execution and infect the additional setup programs as well.

Specific viruses infect in different ways:

- A file virus infects by attaching itself to an executable system application program. Potential targets for virus infections:
  - Source code
  - Batch files
  - Script files
- Boot sector viruses execute their code in the first place before the target PC is booted.

Viruses spread in a variety of ways. There are virus programs that infect and keep spreading every time the user executes them. Some virus programs do not infect the programs when first executed. They reside in a computer's memory and infect programs later. Such virus programs 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. As illustrated in the slide above, 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 along with the application program immediately after executing it.

The following are the most popular methods by which a virus spreads:

- **Infected files**: A virus can infect a variety of files.
- **File-sharing services**: A virus can take advantage of file servers to infect files. When unsuspecting users open the infected files, their machines also become infected.
- **DVDs and other storage media**: When infected storage media such as DVDs, flash drives, and portable hard disks are inserted into a clean system, the system gets infected.
- **Malicious attachments and downloads**: A virus spreads if a malicious attachment sent via email is opened or by downloading apps from untrusted sources.

- **Attack Phase**

Once viruses spread themselves throughout the target system, they start corrupting the files and programs of the host system. Some viruses have the feature of triggering and corrupting the host system only after activating that triggering event. Some viruses have

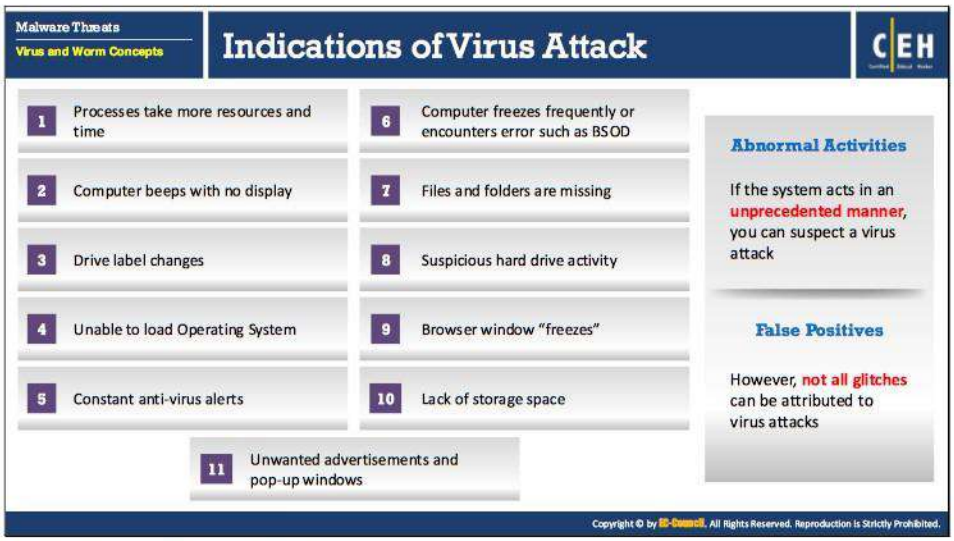
bugs that replicate themselves and perform activities such as deleting files and increasing session time. Viruses corrupt their targets only after spreading as intended by their developers. Most viruses that attack target systems perform actions such as:

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

The figure in the slide shows two files, A and B. Before the attack, the two files are located one after the other in an orderly fashion. Once a virus code infects the file, it alters the position of the files placed consecutively, leading to inaccuracy in file allocations, and causing the system to slow down as users try to retrieve their files.

In the attack phase:

- Viruses execute upon triggering specific events
- Some viruses execute and corrupt via built-in bug programs after being stored in the host's memory.
- The latest and advanced viruses conceal their presence, attacking only after thoroughly spreading in the host



Indications of Virus Attack

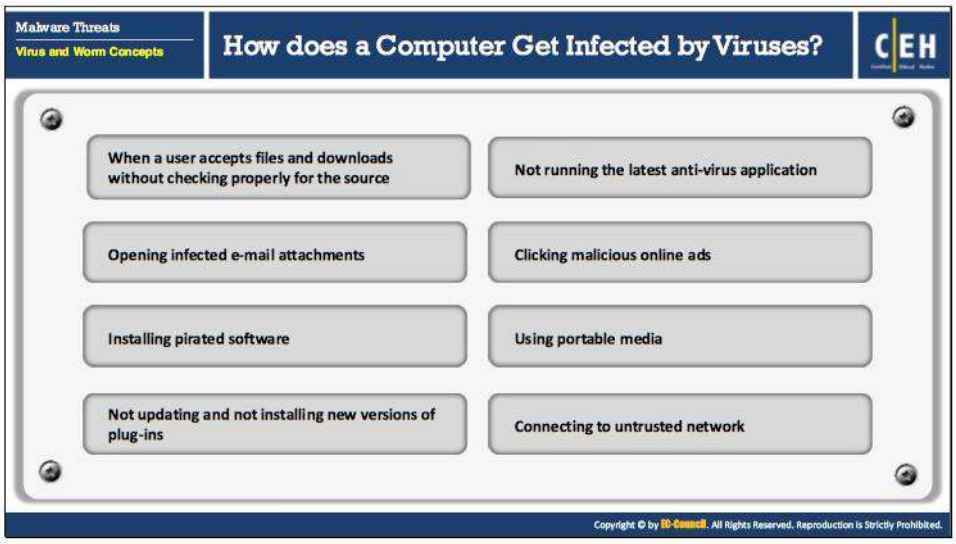
Indications of virus attack arise from abnormal activities. Abnormal activities reflect the nature of a virus by interrupting the regular flow of a process or a program. However, not all bugs created contribute in attacking the system; they may be merely false positives. For e.g., if the system runs slower than usual, one may assume that a virus affected the system, but the reason might be program overload.

An effective virus tends to multiply rapidly and may infect some machines in a short period. Viruses can infect files on the system, which after transferring can infect machines of users who receive them. A virus can also make good use of file servers to infect files.

When a virus infects a computer, the victim or the user will be able to identify some of the indications of the presence of virus infection.

The following are some of the indications of computer virus infection:

- Processes take more resources and time, results in reduced performance
- Computer beeps with no display
- Drive label changes and unable to load OS
- Constant anti-virus alerts
- Computer freezes frequently or encounters error such as BSOD
- Files and folders are missing
- Suspicious hard drive activity
- Browser window "freezes"
- Lack of storage space
- Unwanted advertisements and pop-up windows

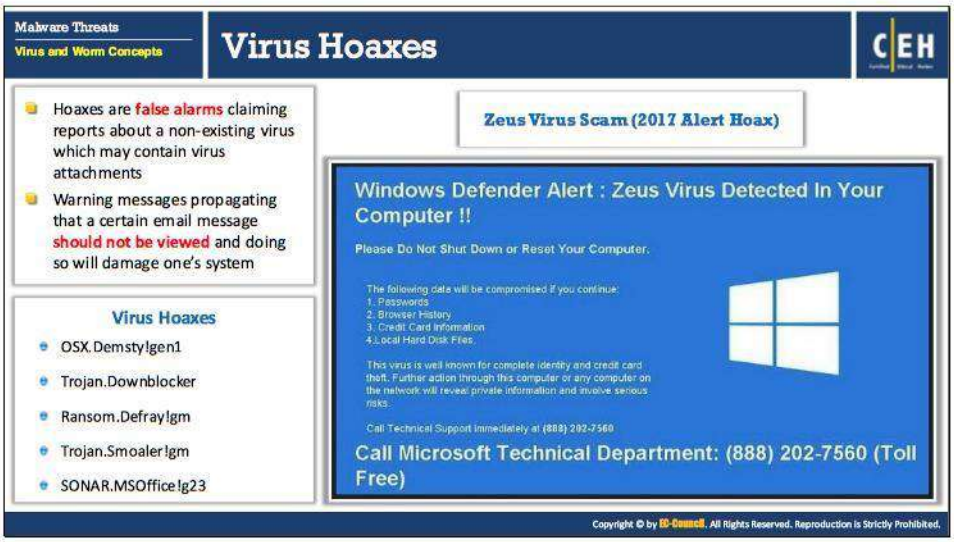


How does a Computer Get Infected by Viruses?

To infect a system, first, a virus has to enter it. Once the user downloads and installs the virus from any source and in any form, it replicates itself to other programs. Then virus can infect the computer in various ways, some of them are listed here:

- **Downloads**: Attackers incorporate viruses in popular software programs and upload them to websites intended for download. When a user unknowingly downloads this infected software and installs it, the system is infected.
- **Email attachments**: Attackers usually send virus-infected files as email attachments to spread the virus on the victim's system. When the victim opens the malicious attachment, the virus automatically infects the system.
- **Pirated software**: Installing a cracked version of the software (OS, Adobe, Microsoft Office, etc.) might infect the system as they may contain viruses.
- **Failing to install Security Software**: With the increase in security parameters, attackers are designing new viruses. Failing to install latest anti-virus software or updating it regularly may expose the computer system to virus attacks.
- **Updating Software**: If patches are not installed regularly when released by vendors, viruses might exploit vulnerabilities allowing an attacker to access the system.
- **Browser**: By default, every browser comes with built-in security. If the browser is not configured correctly, this could result in the automatic running of scripts, which may, in turn, allow viruses to enter the system.
- **Firewall**: Disabling the firewall will compromise the security of network traffic and invite viruses to infect the system.

- **Popups**: When the user clicks any suspicious popups by mistake, the virus hidden behind the popup enters the system. Whenever the user turns on the system, the installed virus code will run in the background.
- **Removable media**: When a healthy system is associated with virus infected removable media (e.g., CD/ DVD, USB drive, card reader), the virus spreads to them.
- **Network access**: Connecting to an untrusted Wi-Fi network, leaving the Bluetooth setting ON or permitting a file sharing program that is accessed openly will allow a virus to take over the device.
- **Backup and Restore**: Taking a backup of infected files and restoring them back to a system infects the system again with the same virus.
- **Malicious Online Ads:** Attackers post malicious online ads by embedding malicious code in the ad, also known as malvertising. Once, the users click these ads, the computer gets infected.
- **Social Media:** People tend to click on social media sites and malicious links shared by their contacts which can infect their systems.



Virus Hoaxes

Techniques such as virus hoaxes and fake anti-viruses are most widely used by attackers to introduce viruses onto victims' systems.

Virus hoaxes are a kind of bluff but can be almost as damaging as real viruses in lost production and loss of bandwidth, while naive users react to them and forward them to other users. Because viruses tend to cause so much fear, they have become a common subject of hoaxes. Virus hoaxes are false alarms claiming reports about nonexistent viruses.

The following are some critical points about hoaxes:

- These warning messages, which can be propagated rapidly, state that a particular e-mail message should not be opened, and that doing so would damage one's system.
- In some cases, these warning messages themselves contain virus attachments.

Try to crosscheck the identity of the person who has posted the warning.

It is a good practice to look for technical details in any message concerning viruses. Also, search for information on the Internet to learn more about hoaxes, especially by scanning bulletin boards on which people actively discuss current community happenings/concerns. Before jumping to conclusions by reading Internet information, first check the following:

- If the information is posted by newsgroups that are suspicious, cross-check 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 anti-virus software vendor sites.

ZeuS Virus Scam: Alert Hoax 2017

Zeus is a devastating Trojan infection. It is an aggressive parasite which is capable of destroying the user's entire online experience. The ZeuS Alert Hoax is the most popular way chosen by hackers to trap their victims into downloading the actual ZeuS malware. Pop-ups of ZeuS infection alerts will be generated on the victim's computer to scare and create a panic situation tricking the victim to click or download the anti-virus or contact the technical support to eliminate the infection from the computer, which leads to the actual ZeuS malware attack. This is how cyber scams worked infecting a large number of computers.
Some of the additional virus hoaxes include:

- OSX.Demsty!gen1
- Trojan.Downblocker
- Ransom.Defray!gm
- Trojan.Smoaler!gm
- SONAR.MSOffice!g23

Fake AntiVirus

Fake or rogue anti-virus software is a form of Internet fraud using malware. It appears and performs similarly to a real anti-virus program. Fake anti-virus software often displays as banner ads, pop-ups, email links, and in search engine results when searching for anti-virus software. A well-designed, fake antivirus looks authentic and often encourages users to install it on their systems, or perform updates, or remove viruses and other malicious programs.

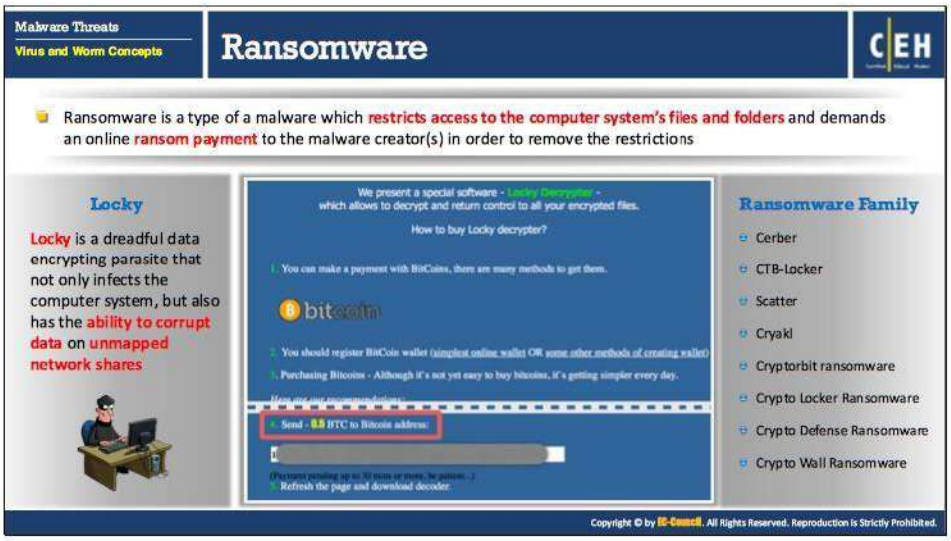
Upon clicking to install it, users are redirected to another page where they are prompted to buy or subscribe to that anti-virus software and enter their payment details. Fake anti-viruses can further cause much damage to systems, once downloaded and installed; for e.g., they infect them with malicious software, steal sensitive information (e.g., passwords, bank account numbers, credit card data), and corrupt files.

- **AntiVirus Pro 2017**

  AntiVirus Pro 2017 is a computer infection from the Rogue.WinPCDefender family of rogue anti-spyware programs. This program is classified as a rogue because it deliberately displays false scan results, fake security alerts, and prevents from running any programs on the computer. Once installed, AntiVirus Pro 2017 will automatically scan the computer and then state that there are numerous infections on the computer. If you attempt to remove any of these so-called infections, it will state to purchase the program to remove anything.

Some of the additional fake anti-virus programs include:

- ScanGuard
- Antivirus 10
- TotalAV



Ransomware

Ransomware is a type of malware that restricts access to the infected computer system or critical files and documents stored on it, and after that demands an online ransom payment to the malware creator(s) to remove user restrictions. Ransomware might encrypt files stored on the system's hard disk, or merely lock the system and display messages meant to trick the user into paying.

Usually, ransomware spreads as a Trojan, entering a system through email attachments, hacked websites, infected programs, app downloads from untrusted sites, vulnerabilities in network services, and so on. After execution, the payload in the ransomware runs and encrypts the victim's data (files and documents), which can be decrypted only by the malware author. In some cases, the user interaction is restricted using a simple payload.

In a web browser, the text file or a webpage displays the Ransomware demands. The displayed messages pretend to be from companies or law enforcement personnel falsely claiming that their system is being used for illegal purposes or contains illegal content (e.g., porn videos, pirated software), or it could be a Microsoft product activation notice falsely claiming that installed Office software is fake and requires product re-activation. These messages entice victims into paying money to undo the restrictions imposed on them. Ransomware leverages victims' fear, trust, surprise, and embarrassment to get them to pay the ransom demanded.

Ransomware Families

Some of the additional ransomware families include:

- Cerber
- CTB-Locker
- Scatter
- Cryakl
- Crysis
- CryptXXX
- Cryptorbit ransomware
- Crypto Locker Ransomware
- Crypto Defense Ransomware
- Crypto Wall Ransomware
- Police-themed Ransomware

Examples of Ransomware

- **Ransomware: Locky**

  Locky is a dreadful data encrypting parasite that not only infects the computer system but also has the ability to corrupt data on unmapped network shares. This ransomware spreads as a malicious Word document named invoice J-[8 random numbers].doc that is attached to spam emails.

  If the macros are enabled, the malicious process starts as soon as the user opens this attachment. In case, the Macros are disabled; the ransomware guides the user to enable macros by displaying a distorted phrase –"Enable macro if data encoding is incorrect," If the user follows this procedure, the malicious code gets triggered which downloads and runs an executable file of Locky virus.

This Ransomware uses **RSA-2048** and **AES-128** encryption algorithms to lock personal files, including audio, video, image files, documents. This virus can also access and encrypt data stored on external drives connected to the target system. After the encryption process, the affected files are renamed with a **".locky extension,"** and this confuses the victim, making it difficult to decrypt particular data. A ransom note is displayed, which explains how the victims are to make a payment towards a ransom.

- **Ransomware: WannaCry**

  WannaCry targets corporate networks without the knowledge of the user by exploiting known vulnerabilities in Microsoft Windows. WannaCry spreads through an exposed, vulnerable **SMB port** instead of phishing or social engineering.

  When the target system is infected, the malware checks for the information ("kill switch" domain name) on the central server to get it activated. Once the attacker gets hold of this information, it begins encrypting files on the infected computer. After all the files are encrypted it posts a message with demand for a ransom of $300 worth of the cryptocurrency Bitcoin to decrypt the files, and if the payment is not made within the stated time frame, it threatens to destroy the encrypted files.

- **Ransomware: Petya –NotPetya**

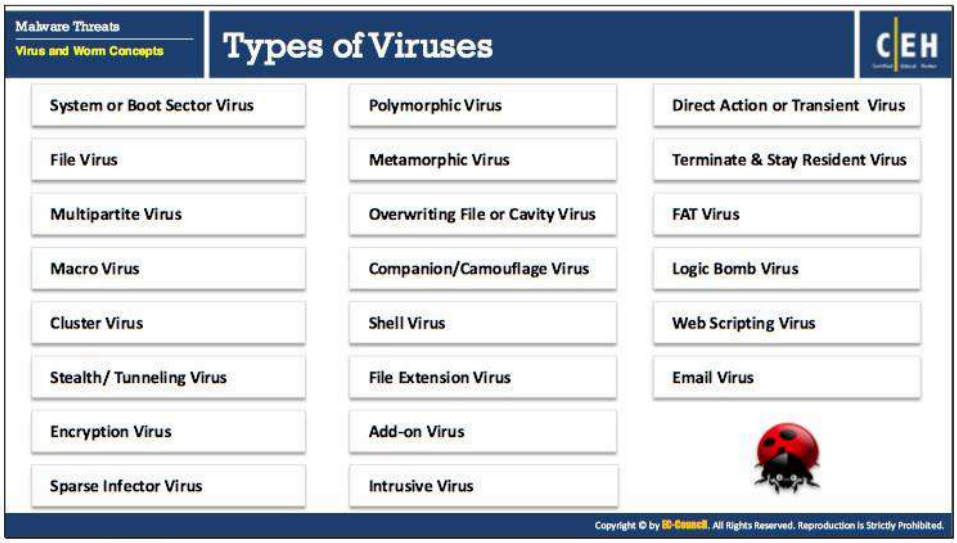
  This ransomware targets all the versions of Windows OSs and can infect the entire network, including known server names.

  The master boot record is infected to execute a payload that encrypts a hard drive's file system table and stops Windows from booting. It can spread over the network using WMIC (Windows Management Instrumentation Command-line) by capturing all credentials from the local machine using Mimikatz.

  This ransomware follows the footsteps of Wannacry that encrypts computer files and demands a ransom of $300 Bitcoins to decrypt the data. This attack had been initiated against an update, used on a third party Ukrainian software called MeDoc, which is used by many government organizations.

Some of the additional ransomware's include:

- GoldenEye
- Chimera
- Hidden Tear & EDA2
- Fantom
- Mischa
- Shark
- HolyCrypt
- CryPy
- Stampado
- zCrypt
- PowerWare
- Hydra Crypt 2016
- RAA ransomware



Types of Virus

Computer viruses are malicious software programs written by attackers to gain unauthorized access to a target system. As a result, they compromise the security of a system and its performance. For any virus to corrupt a system, it has to first associate its code with executable code.

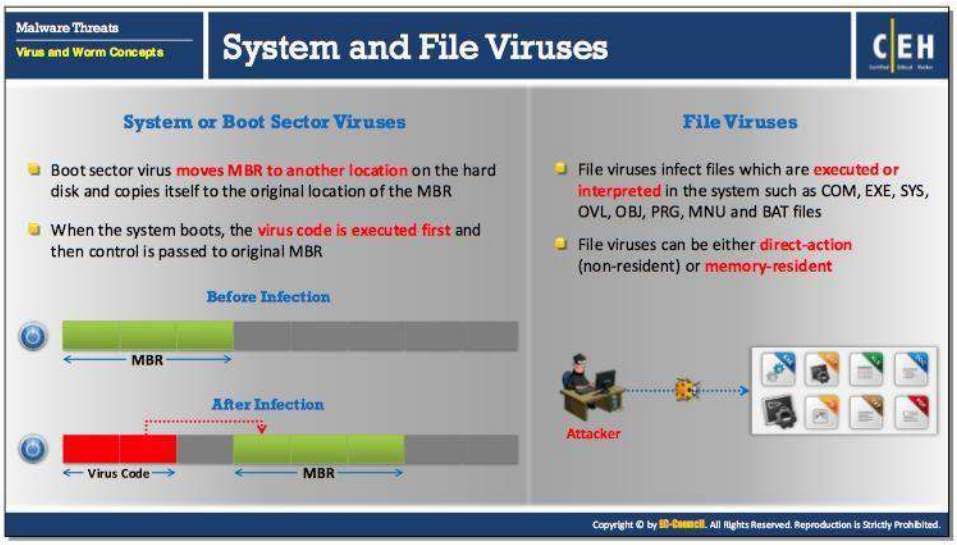
It is important to understand how viruses:

- Add themselves to the target host's code
- Choose to act upon the target system

Some of the most common types of computer viruses that adversely affect the security of the systems are:

1. System or Boot Sector Virus
2. File Virus
3. Multipartite Virus
4. Macro Virus
5. Cluster Virus
6. Stealth Virus/Tunneling Virus
7. Encryption Virus
8. Sparse Infector Virus
9. Polymorphic Virus

10. Metamorphic Virus
11. Overwriting File or Cavity Virus
12. Companion Virus/Camouflage Virus
13. Shell Virus
14. File Extension Virus
15. Add-on Virus
16. Intrusive Virus
17. Direct Action or Transient Virus
18. Terminate and Stay Resident Virus (TSR)
19. FAT Virus
20. Logic Bomb Virus
21. Web Scripting Virus
22. Email Virus



System or Boot Sector Viruses

The most common targets for a virus are the system sectors, which include the master boot record (MBR) and the DOS boot record system sectors. An OS executes codes in these areas while booting. Every disk has some sort of system sector. MBRs are the most virus-prone zones because if the MBR is corrupted, all data will be lost. The DOS boot sector also executes during the system booting. This is the crucial point of attack for viruses.

The system sector consists of 512 bytes of disk space. Because of this, system sector viruses conceal their code in some other disk space. The primary carrier of system or boot sector viruses is the email attachment and removable media (USB drives). These viruses reside in the memory. Some sector viruses also spread through infected files, known as multipartite viruses.

The boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, first the virus code executes and then control passes to the original MBR.

- **Virus Removal**

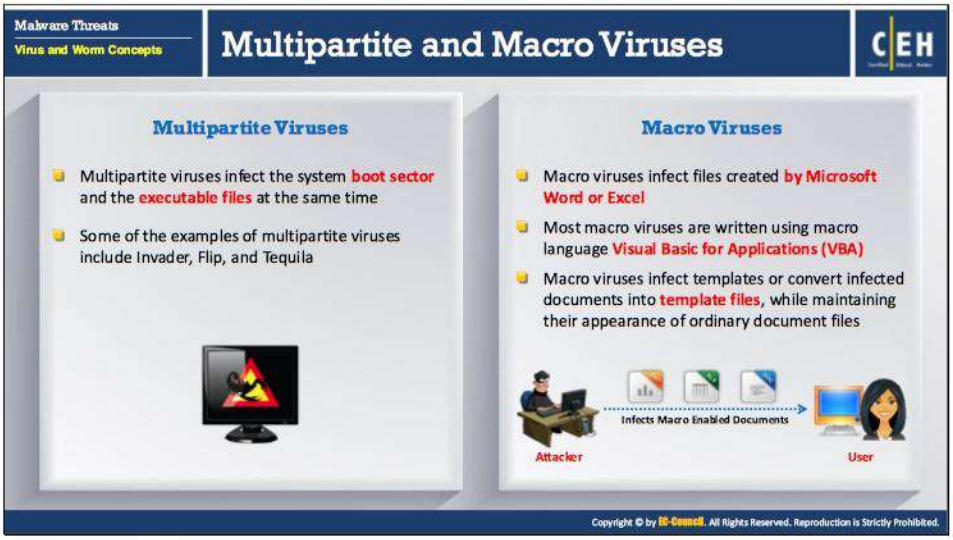
  System sector viruses create the illusion that there is no virus on the system. One way to deal with this virus is to avoid the use of the Windows OS and switch to Linux or Mac because Windows is more prone to these attacks. Linux and Macintosh have a built-in safeguard to protect against these viruses.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

File Viruses

File viruses infect files 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.

File viruses insert their code into the original file and infect executable files. File viruses are large in number, but they are rare. They infect in a variety of ways and found in a large number of file types. The most common type of file virus operates by identifying the file type it can most easily infect, such as file names ending in .COM or .EXE. During program execution, the virus executes along with program files to infect more files. Overwriting a virus is not easy, as the overwritten programs no longer function properly. These types of viruses tend to be found immediately. Before inserting their code into a program, some file viruses save the original instructions and allow the original program to execute, so that everything appears normal.

File viruses hide their presence by using stealth techniques to reside in a computer's memory in the same way as the system sector viruses work. It does not show any increase in file length while performing directory listing. If a user attempts to read the file, the virus intercepts the request, and the user gets back his original file. File viruses can infect a large number of file types, as a wide variety of infection techniques exist.



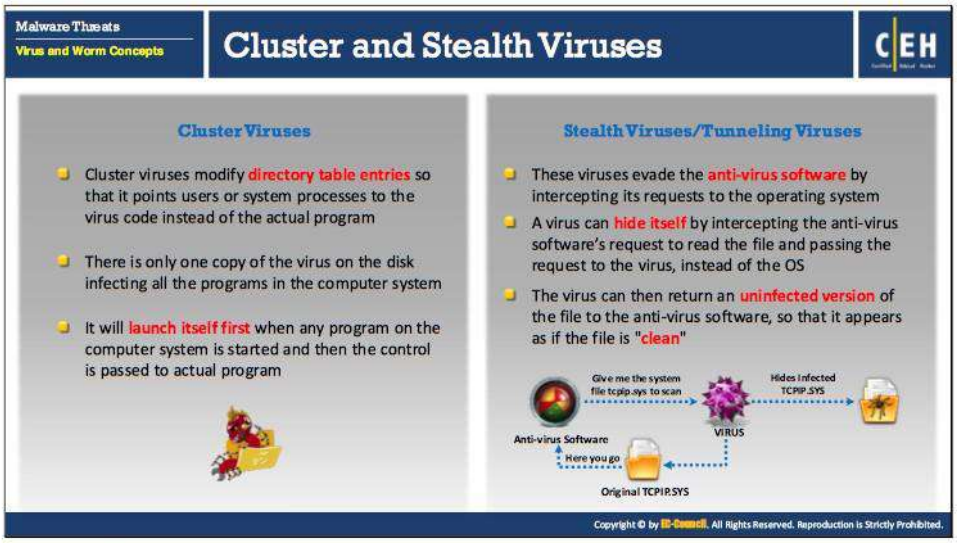
Multipartite Viruses

A multipartite virus (also known as a multipart virus or hybrid virus) combines the approach of file infectors and boot record infectors and attempts to attack both the boot sector and the executable or program files at the same time. When the virus infects the boot sector, it will, in turn, affect the system's file and vice versa. This type of virus re-infects a system repeatedly if the virus is not rooted out entirely from the target machine. Some of the examples of multipartite viruses include Invader, Flip, and Tequila.

Macro Viruses

The macro virus infects Microsoft Word or similar applications, which automatically performs a sequence of actions after triggering an application. Most macro viruses are written using macro language Visual Basic for Applications (VBA), and they infect templates or convert infected documents into template files while maintaining their appearance of common document files.

Macro viruses are somewhat less harmful than other viruses. They usually spread via email. Pure data files do not allow the spreading of viruses, but sometimes the average user due to the extensive macro languages in some programs easily overlooks the line between a data file and an executable file. 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 in which the default macros are set to run automatically every time the data file is loaded. Virus writers can exploit universal programs with macro capability such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain macrocode.



Cluster Viruses

Cluster viruses infect files without changing the file or planting additional files. They save the virus code to the hard drive and overwrite the pointer in the directory entry, directing the disk read point to the virus code instead of the actual program. Even though the changes in the directory entry may affect all the programs, only one copy of the virus exists on the disk.

A cluster virus, for e.g., Dir-2 first launches itself when any program starts on the computer system, and then the control is passed to the actual program.

This virus infection leads to severe problems if the victim does not know its exact location. If it infects memory, it controls access to the directory structure on the disk.

If the victim boots from clean floppy disk and then run a utility such as CHKDSK, the utility reports serious problem with the cross-linked file on the disk. Such utilities usually offer to correct the problems. If the offer is accepted, the virus infects all the executable files and results in the loss of original content, or all files might appear to be of the same size.

Stealth Viruses/Tunneling Viruses

These viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests to perform operations with respect to these service call interrupts. These viruses state false information to hide their presence from antivirus programs. For e.g., 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.

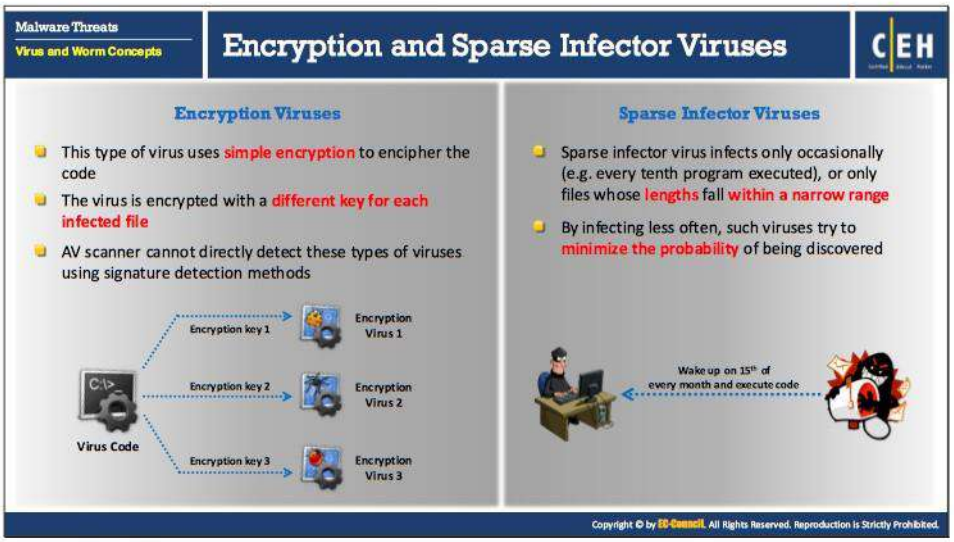
The stealth virus hides from antivirus software by hiding the original size of the file or temporarily placing a copy of itself in some other system drive, thus replacing the infected file with the uninfected file that is stored on the hard drive.

A stealth virus hides the modifications performed by it. It takes control of the system's functions that read files or system sectors and, when another program requests information that had already modified by the virus; the stealth virus reports that information to the requesting program instead. This virus also resides in 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 result in this virus attack because a Trojan installs the rootkits, and thus is capable of hiding any malware.

- **Virus Removal**
  - Always do a cold boot (boot from write-protected CD or DVD)
  - Never use DOS commands such as FDISK to fix the virus
  - Use anti-virus software



Encryption Viruses

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on. This type of virus consists of an encrypted copy of the virus and a decryption module. The decrypting module remains constant, whereas encryption makes use of different keys.

An encryption key consists of a decryption module and an encrypted copy of the code, which enciphers the virus. When the attacker injects the virus into the target machine, the decryptor will first execute and decrypts the virus body. Then the virus body executes and replicates or become resident in the target machine. The replication process accomplishes successfully using encryptor. Each virus infected file makes use of a different key for encryption. These viruses employ XOR on each byte with a randomized key. The decryption technique employed is "*x*," or each byte with a randomized key that is generated and saved by the root virus.

Encryption viruses block the access to target machines or provide victims with limited access to the system. This virus uses encryption to hide from virus scanner. It is not possible for the virus scanner to detect the encryption virus using signatures, but it can detect the decrypting module.

Sparse Infector Viruses

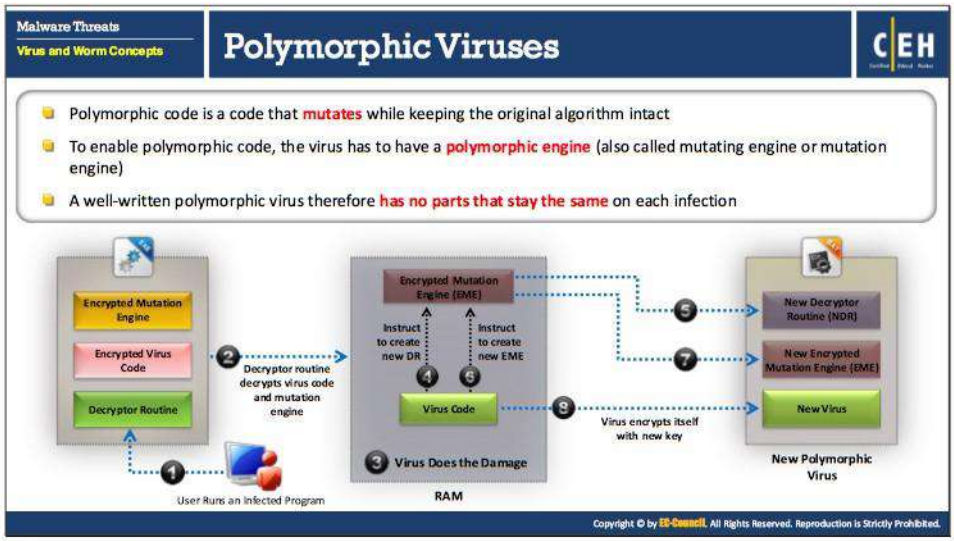
To spread infection, viruses typically attempt to hide from antivirus programs. Sparse infector viruses infect less often and try to minimize the probability of discovery. Sparse infector viruses infect only occasionally upon satisfying certain conditions or only files whose lengths fall within a narrow range.

The sparse infector virus works with two approaches:

- Replicates only occasionally (Example: Every tenth program executed or on a particular day of the week)

- Decides which file to infect based on certain conditions (Example: Infects target files with maximum size of 128 kb)

The diagram shown in the slide represents the working of a sparse infector virus. The attacker sends a sparse infector virus to the target machine and sets a wakeup call for the virus to execute on the 15th day of every month. This strategy makes it hard for the anti-virus to detect the virus, thus allowing the virus to infect the target machine successfully.



Polymorphic Viruses

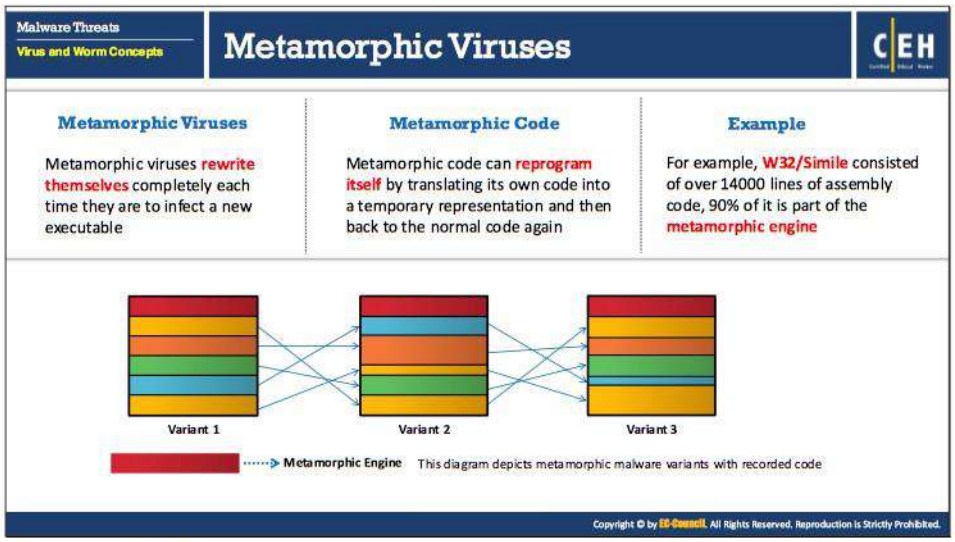
This type of virus infects a file with an encrypted copy of a polymorphic code already decoded by a decryption module. Polymorphic viruses modify their code for each replication to avoid detection. They accomplish this by changing the encryption module and the instruction sequence. Polymorphic mechanisms use random number generators in their implementation.

The general use of mutation engine is 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 prevent antivirus professionals from accessing the codes. A simple integrity checker detects the presence of a polymorphic virus in the system's disk.

A polymorphic virus consists of three components: 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 of the computer. The mutation engine generates randomized decryption routines. This decryption routine varies whenever the virus infects a new program.

Polymorphic virus encrypts both the mutation engine and the virus code. When the user executes a polymorphic virus-infected program, the decryptor routine takes complete control over the system, after which it decrypts the virus code and the mutation engine. Next, the decryption routine transfers the system control of the virus, which locates a new program to infect. In Random Access Memory (RAM), 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, the virus encrypts this new copy of both the virus code and mutation engine. 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 running on the target systems are difficult to detect due to encryption of the virus body and the changes in decryption routine each time these viruses infect. It is difficult for virus scanners to identify these viruses, as no two infections look the same.



Metamorphic Viruses

Metamorphic viruses are programmed in such a way that they rewrite themselves completely each time they infect a new executable file. Such viruses are sophisticated and use metamorphic engines for their execution. Metamorphic code reprograms itself. It is translated into temporary code (a new variant of the same virus but with a different code), and then converted back to the original code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition of anti-virus software. This technique is more effective in comparison to polymorphic code.

The transformation of virus bodies ranges from simple to complex, depending on the technique used. Some techniques used for metamorphosing viruses are:

- Disassembler
- Expander
- Permutator
- Assembler

Sequential flow of transforming virus bodies takes place in the following manner:

1. Inserts dead code
2. Reshapes the expressions
3. Reorders instructions
4. Modifies variable names
5. Encrypts program code
6. Modifies the program control structure

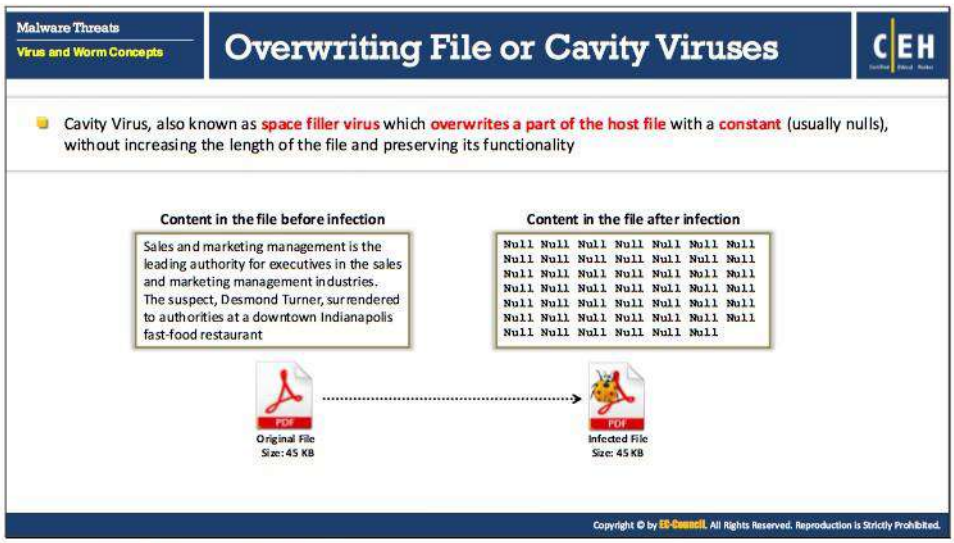
The commonly known metamorphic viruses are:

- **Win32/Simile**

  The intruder programs this virus in assembly language to target Microsoft Windows. This process is complicated and generates almost 90% of virus codes.

- **Zmist**

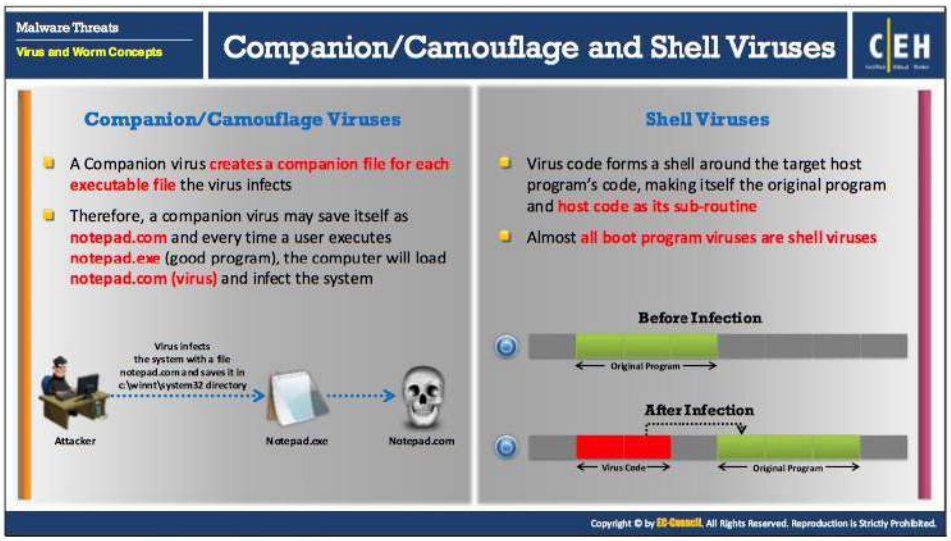
  Zmist also was known as Zombie. Mistfall is the first virus to use the technique called "**code integration**." This code inserts itself into other code, regenerates the code, and rebuilds the executable.



Overwriting File or Cavity Viruses

Some programs have empty spaces in them. Cavity Virus, also known as a space-filler overwrites a part of the host file that is with a constant (usually nulls), without increasing the length of the file but preserving its functionality. Maintaining constant file size when infecting allows it to avoid detection. The cavity viruses are rarely found due to the unavailability of hosts and due to the code complexity in writing.

A new design of Windows file called the Portable Executable improves the loading speed of the programs. However, it leaves a particular gap in the file while it is being executed that can be used by the cavity virus to insert itself. The most popular virus family in this category is the CIH virus (known as Chernobyl or Spacefiller).



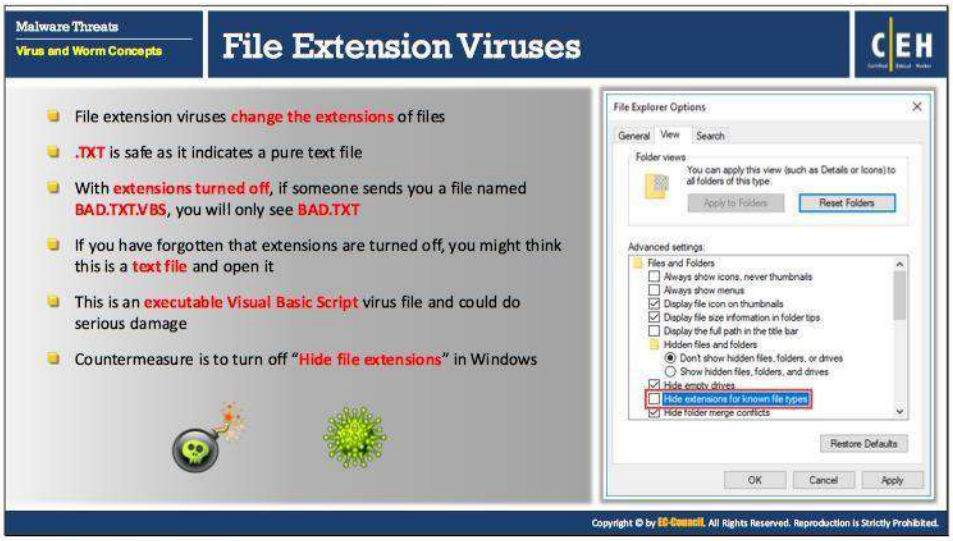
Companion/Camouflage Viruses

The companion virus stores itself by having the identical file name as the targeted program file. The virus infects the computer upon executing the file, and it modifies the hard disk data. Companion viruses use DOS that run COM files before the execution of EXE files. The virus installs an identical COM file and infects EXE files.

This is what happens: Suppose a companion virus is executing on the PC and decides it is time to infect a file. It looks around and happens to find a file called notepad.exe. It now creates a file called notepad.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 the DOS path. If you type notepad and press Enter, DOS executes notepad.com instead of notepad.exe. (In sequence, 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 notepad.exe. The user probably would fail to notice if anything is wrong. It is easy to detect a companion virus just by the presence of the extra COM file in the system.

Shell Viruses

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



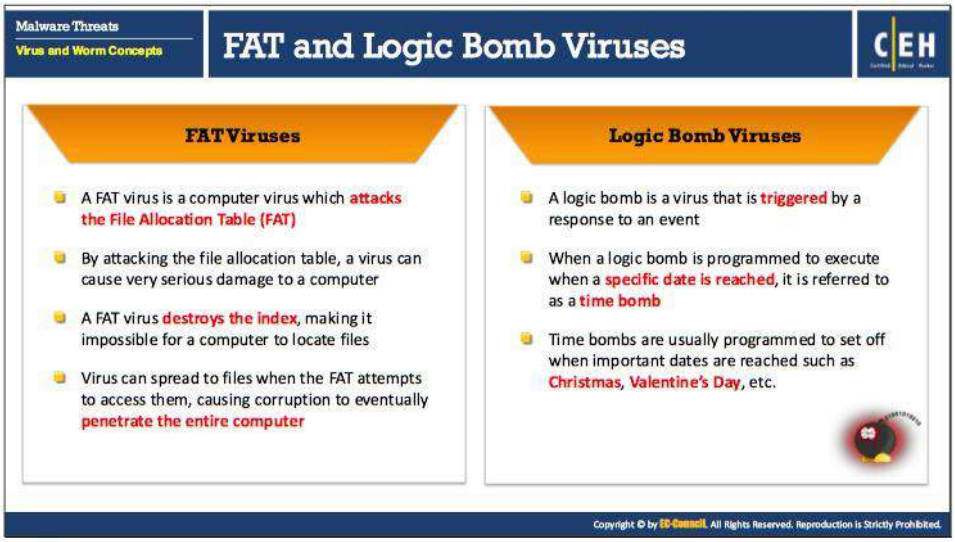
File Extension Viruses

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 severe damage.

The countermeasure is to turn off "Hide file extensions" in Windows.

Guidelines to keep files safe from virus infection:

- Turn off **"Hide file extensions"** in Windows (Go to **Control Panel → Appearance and Personalization → Show hidden files and folders → View tab** → Uncheck **Hide extensions for known files types**).
- Scan all files in the system with good anti-virus software which takes a substantial amount of time.



FAT Viruses

A FAT virus is a computer virus, which attacks the File Allocation Table (FAT), a system used in Microsoft products and some other types of computer systems to access the information stored on a computer. By attacking the file allocation table, a virus can cause severe damage to a computer. FAT viruses can work in a variety of ways. Some are designed to embed themselves into files so that when the FAT accesses the file, the virus is triggered. Others may attack the FAT directly. Many are designed to overwrite files or directories, and material on a computer can lost permanently. If a FAT virus is powerful enough, it can render a computer unusable in addition to destroying data, forcing a user to reformat.

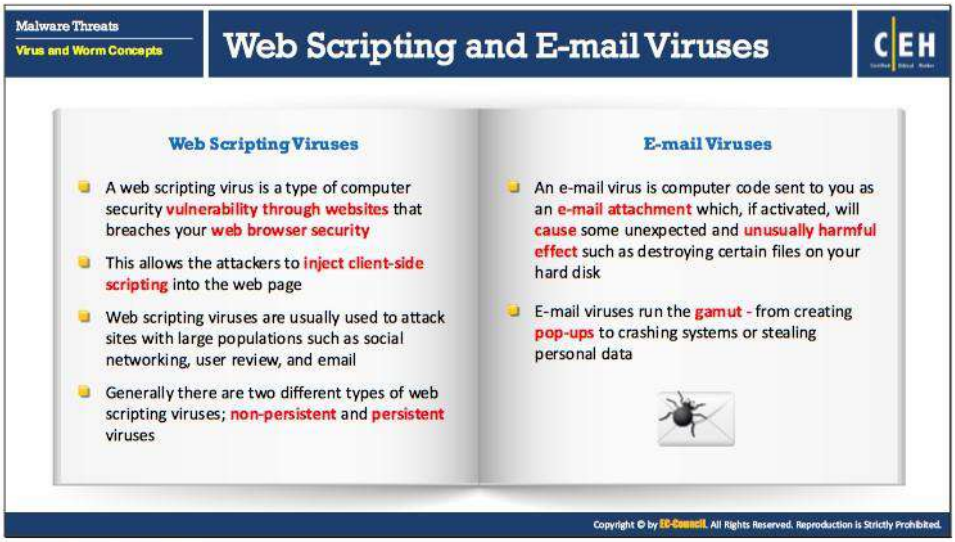
Essentially, a FAT virus destroys the index, making it impossible for a computer to locate files. The virus can spread to files when the FAT attempts to access them, causing corruption to penetrate the entire computer eventually. FAT viruses often manifest in the form of corrupted files, with users noting that files are missing or inaccessible. The FAT architecture itself can also be changed; for e.g., a computer which should be using the FAT32 protocol might abruptly say that it is using FAT12.

Logic Bomb Viruses

A logic bomb is a virus that is triggered by a response to an event, such as launching an application or when a specific date/time is reached, where it involves a logic to execute the trigger.

For e.g., cyber-criminals use spyware to install a keylogger on your computer covertly. The keylogger can capture keystrokes, such as usernames and passwords. The logic bomb is designed to wait until you visit a website that requires to log in with your credentials, such as a banking site or social network. Consequently, this will trigger the logic bomb to execute the keylogger and capture your credentials and send them to a remote attacker.

When a logic bomb is programmed to execute when a specific date is reached, it is referred to as a time bomb. Time bombs are usually programmed to set off when important dates are reached such as Christmas, Valentine's Day, etc.



Web Scripting Viruses

A web scripting virus is a type of computer security vulnerability through websites that breach your web browser security. This allows the attackers to inject client-side scripting into the web page. It can bypass access controls and steal information from the web browser. Web scripting viruses are usually used to attack sites with large populations such as social networking, user review, and email. Web scripting viruses can propagate a bit faster than other viruses. A typical version of web scripting viruses is DDoS. It has the potential to send spam, damage data, and defraud users.

There are two different types of web scripting viruses; non-persistent and persistent attacks. Non-persistent is when you are attacked without knowing. A persistent attack is when you directly get your cookies stolen, and the attacker can hijack your session. This allows the attacker to impersonate you and can lead to much damage.

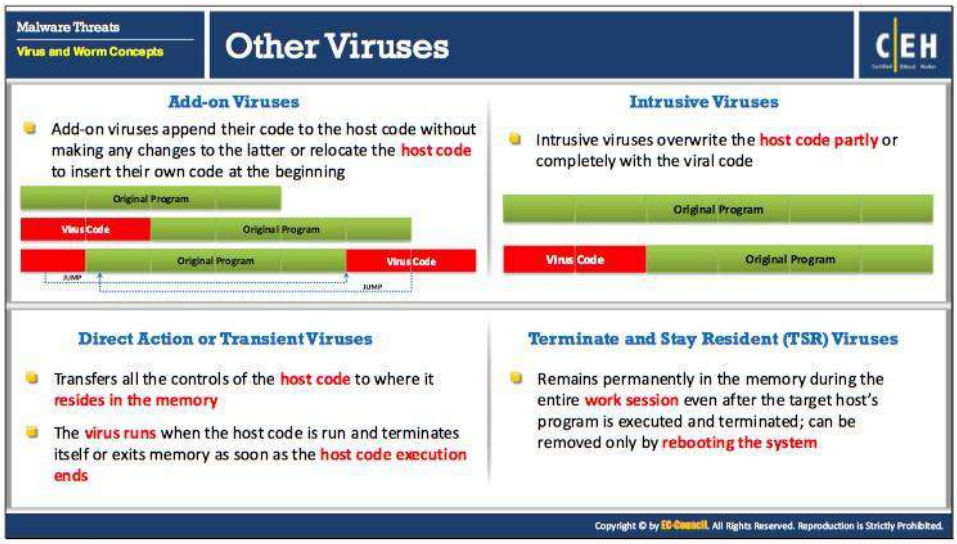
- **Prevention**

  The best ways to prevent these viruses and exploits are by safely validating untrusted HTML input, cookie security, disabling scripts, and using scanning services like an anti-virus which has real-time protection on your web browser. It is also beneficial to not visit unknown websites and using World of Trust to make sure that the site is safe. You would notice if you have a web scripting virus if your searches are linked to elsewhere, the background changed, and homepage changed. The computer would run slow and sluggish, and there would be instances of programs being closed randomly. Modern day browsers have add-ons such as AdBlocker Plus, which allow users to block out scripts from being loaded.

E-mail Viruses

An e-mail virus is computer code sent to you as an e-mail attachment, which if activated, will cause some unexpected and usually harmful effect, such as destroying specific files on your hard disk and causing the attachment to be emailed to everyone in your address book. Email viruses run the gamut - from creating pop-ups to crashing systems or stealing personal data. Email viruses also vary in how they are presented. For e.g., a sender of an email virus may be unknown to a user, or a subject line may be filled with nonsense. In other cases, a hacker may cleverly disguise an email as being from a trusted and known sender.

A policy of never opening (for e.g., double-clicking on) an e-mail attachment unless you know who sent it and what the attachment contains, and installing and using anti-virus software to scan any attachment before you open it can avoid the email virus attack.



Addon 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 code at the beginning.

Intrusive Viruses

Intrusive viruses overwrite the host code wholly or partly with the viral code.

Direct Action or Transient Viruses

Direct action or transient viruses transfer all controls of the host code to where it resides in the memory. It selects the target program to be modified and corrupts it. The life of a transient virus is directly proportional to the life of its host. This means the transient virus executes only upon the execution of its attached program and terminates upon the termination of its attached program. At the time of execution, the virus may spread its infection to other programs. This virus is transient or direct, as it operates only for a short period and goes directly to the disk to search for programs to infect.

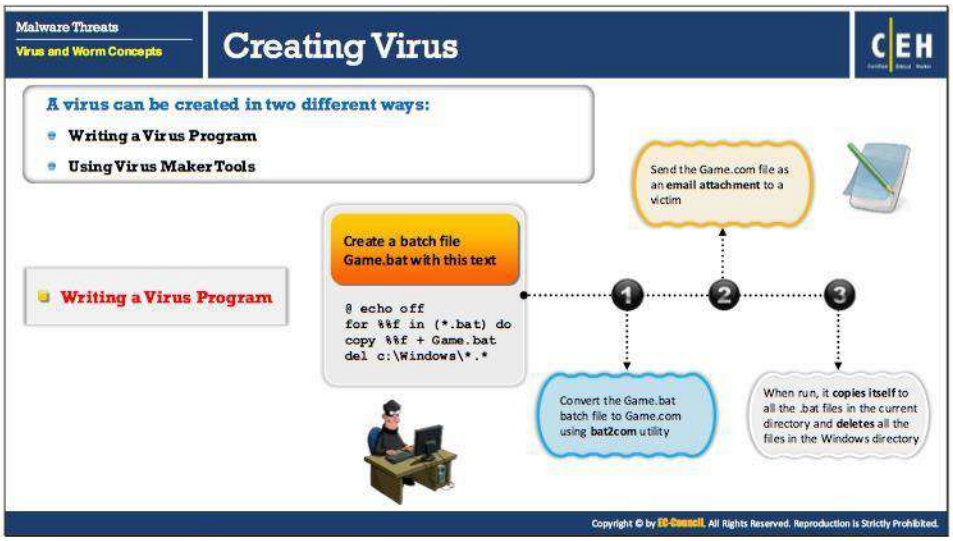
Terminate and Stay Resident (TSR) Viruses

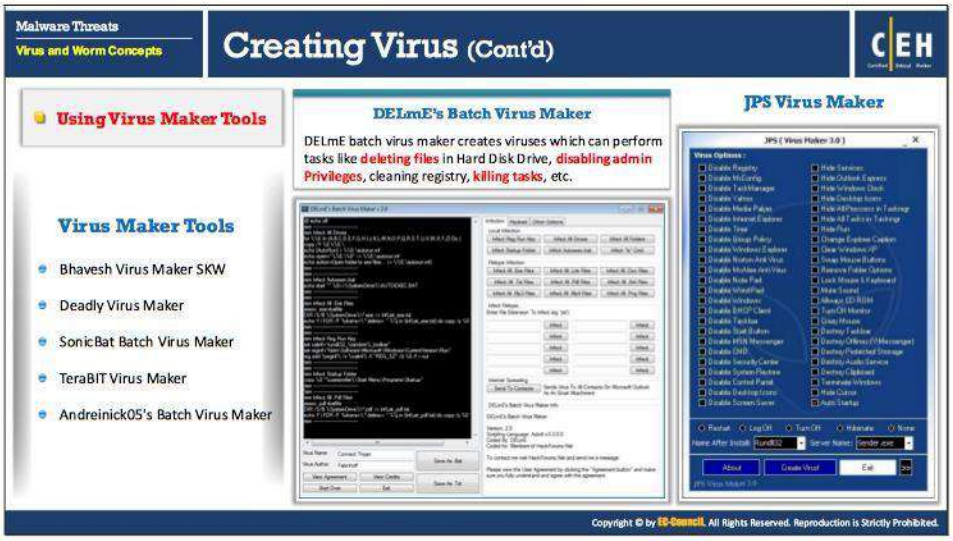
A Terminate and Stay Resident (TSR) virus remains permanently in the target machine's memory during an entire work session, even after the target host's program is executed and terminated. The TSR remains in memory to have some control over the processes. In general, the TSR takes on interrupt vectors into its code, so that when the interrupt takes place, the vector directs execution to TSR code. Rebooting the system completely removes the virus without any traces. If the TSR virus infects the system, the user needs to reboot the system to remove the virus.

Some of the steps employed by TSR viruses to infect files are as follows:

- Gets control of the system

- Assigns a portion of memory for its code
- Transfers and activates itself in the allocated portion of memory
- Hooks the execution of code flow to itself
- Starts replicating to infect files





Creating Virus

A virus can be created in two different ways; writing a virus program and using virus maker tools.

- **Writing a Simple Virus Program**

  Steps involved in writing a simple virus program:

  1. Create a batch file **Game.bat** with the below text

```
@ echo off
for %%f in (*.bat) do copy %%f + Game.bat
del c:\Windows\*.*
```

2. Convert the **Game.bat** batch file to **Game.com** using **bat2com** utility
3. Send the **Game.com** file as an email attachment to the victim
4. When the **Game.com** is executed by the victim, it copies itself to all the .bat files in the current directory on target machine and deletes all the files in the **Windows directory**

- **Using Virus Maker Tools**

  Virus maker tools allow to customize and craft your virus into a single executable file. The nature of the virus depends and relies upon the options that are available in the virus maker tool.

  Once the virus file is built and executed, it can perform all sorts of tasks, including:

  - Disable Windows command prompt and Windows Task Manager
  - Shutdown the system
  - Infect all executable files
  - Inject into the Windows Registry and startup with Windows
  - Perform acts of non-malicious activity such as funny mouse and keyboard actions

  These tools are great if you wish to test the security of your very own antivirus software.

  - **DELmE's Batch Virus Maker**

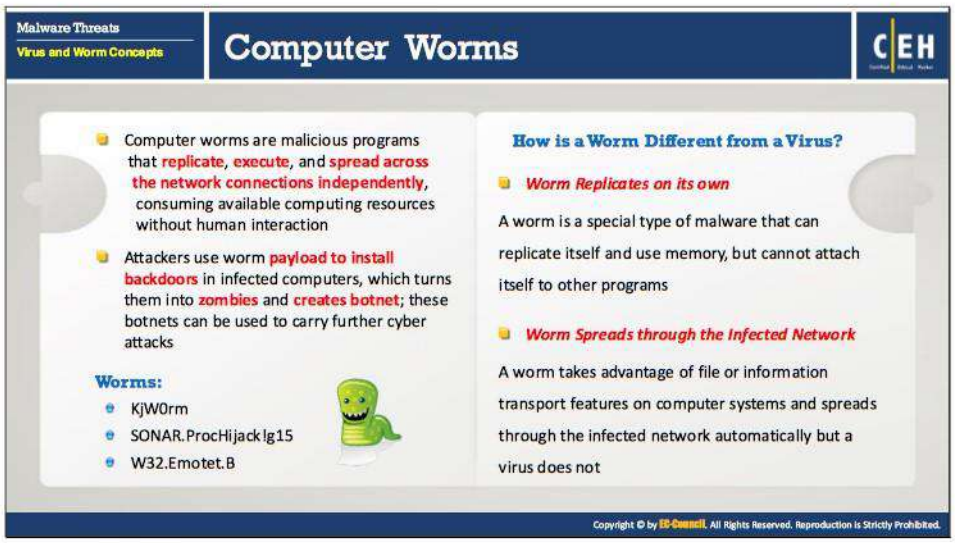
    DELmE's Batch Virus Generator is a virus creation program with lots of options to infect the victim's PC such as formatting C: drive, deleting all files in Hard Disk drive, disabling admin privileges, cleaning registry, changing the home page, killing tasks, disabling/removing antivirus and firewall, etc.

  - **JPS Virus Maker**

    JPS Virus Maker tool is used to create the own customized virus. There are many options in build in this tool which can be used to create the virus. Some of the features of this tool are auto start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.

Some of the additional virus maker tools include:

- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker



Computer Worm

Computer worms are standalone malicious programs that replicate, execute, and spread across network connections independently, without human intervention. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and in turn causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

Worms are a subtype of viruses. A worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they mainly concentrated and targeted on Windows OSs using the same worms by sharing them in an e-mail, IRC, and through other network functions.

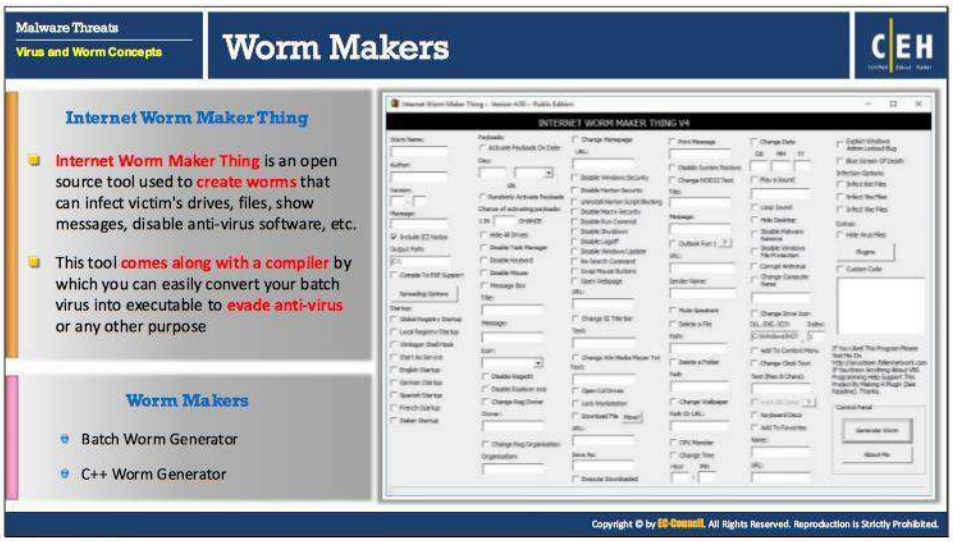
Attackers use worm payloads to install backdoors on infected computers, which turns them into zombies and creates a botnet; an attacker uses these botnets to initiate cyber-attacks. Some of the latest computer worms include:

- KjW0rm
- SONAR.ProcHijack!g15
- W32.Emotet.B

How is a Worm Different from a Virus?

Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates, without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot be spread to other computers unless an infected file is replicated and sent to the other computer	A worm can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs, after being installed in a system
A virus is spread at a uniform speed, as programmed	A worm spreads more rapidly than a virus.
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be removed easily from a system

TABLE 7.4: Difference between virus and worms



Worm Makers

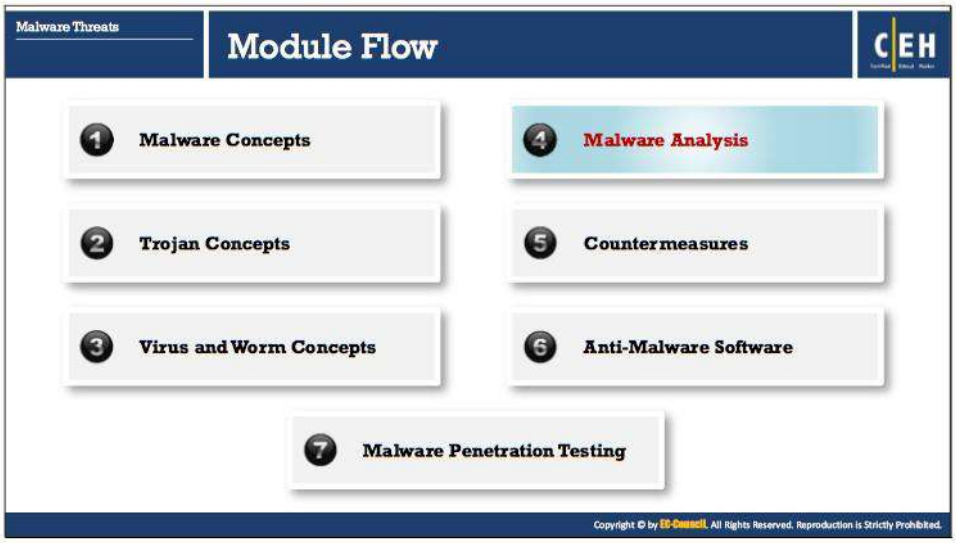
Worm makers are the tools that are used to create and customize computer worms to perform the malicious task. These worms, once created, spread independently over networks and poison the entire networks. With the help of the pre-defined options in the worm makers, the worm can be designed according to the task it is intended to execute.

- **Internet Worm Maker Thing**

  Internet Worm Maker Thing is an open source tool used to create worms that can infect victim's drives, files, show messages, disable anti-virus software, etc. This tool comes along with a compiler by which you can easily convert your batch virus into executable to evade anti-virus or any other purpose.

Some of the worm makers include:

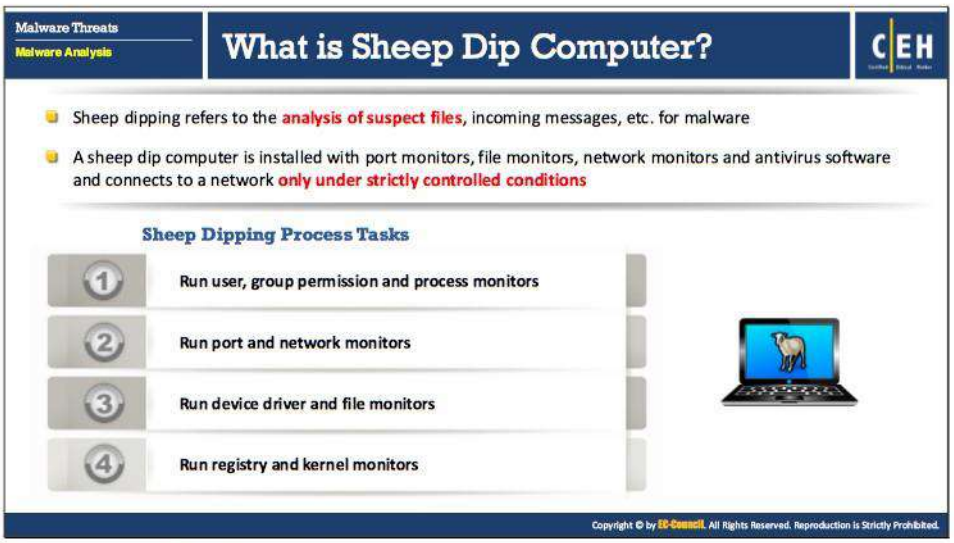
- Batch Worm Generator
- C++ Worm Generator



Malware Analysis

Malware is a program designed to perform malicious acts (The term itself is a contraction of "malicious software"). Malwares such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future, it is necessary to perform a malware analysis. Many tools and techniques exist to perform such tasks.

This section explains malware analysis procedure and discusses the various tools used to accomplish it.



What is Sheep Dip Computer?

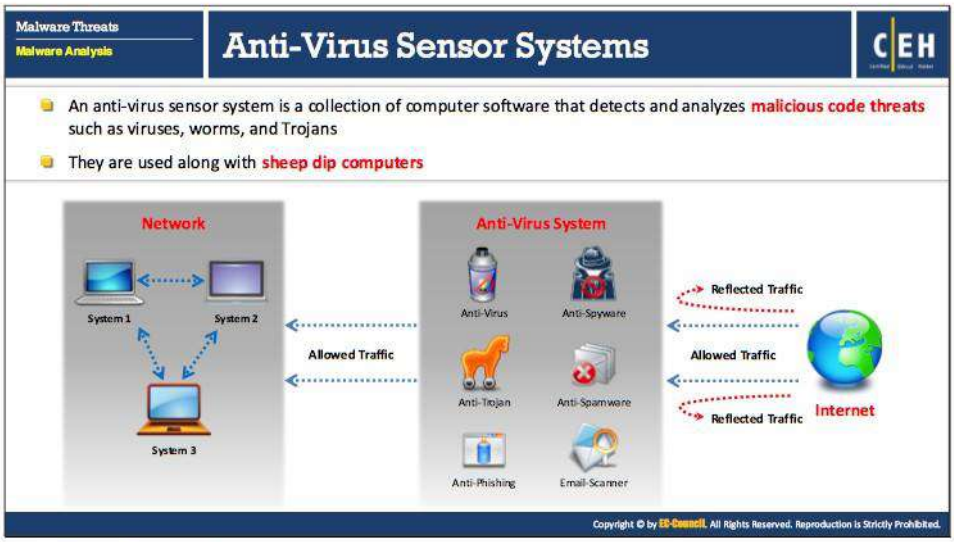
Sheep dipping is a process used in sheep farming which involves dipping of sheep in chemical solutions to make them parasite free. Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware.

The users isolate the sheep-dipped computer from other computers on the network to block any malware from entering the system. Before performing this process, it is important to save all downloaded programs on external media such as CD-ROMs or DVDs.

A computer used for sheep dipping should have tools such as port monitors, files monitors, network monitors, and one or more anti-virus programs for performing malware analysis of files, applications, incoming messages, external hardware devices (such as USB, Pen drive, etc.), and so on.

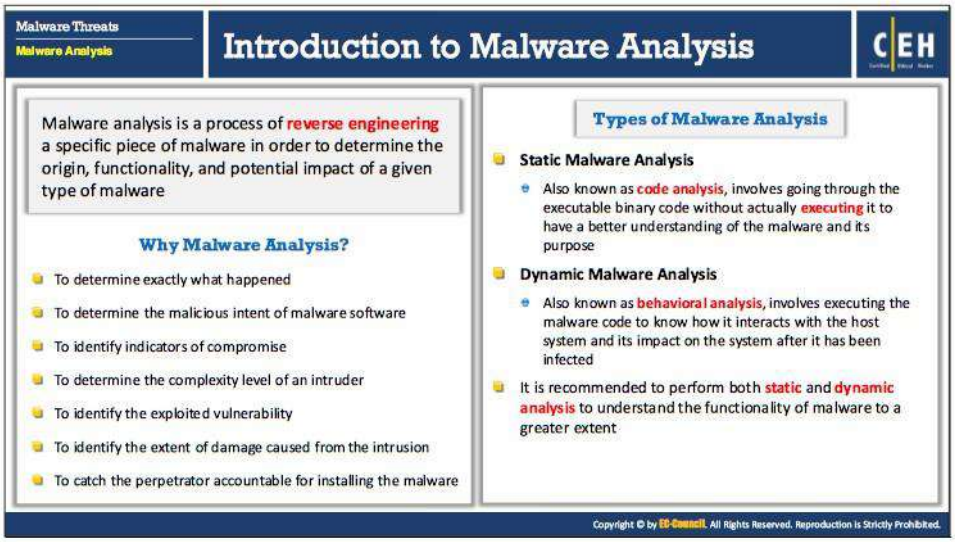
Some of the tasks that are typically run during the sheep dipping process include:

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



Anti-Virus Sensor Systems

An anti-virus sensor 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.



Introduction to Malware Analysis

Attackers are using sophisticated malware techniques as cyber weapons to steal sensitive data. The malware can inflict intellectual and financial losses to the target, whether it be an individual, a group of people or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware analysis is a process of reverse engineering a specific piece of malware to determine the origin, functionality, and potential impact of a given type of malware. By performing malware analysis, the detailed information regarding the malware can be extracted. Malware analysis is an integral part of any penetration testing process.

Why Malware Analysis?

Some of the primary objectives of analyzing a malicious program include:

- Determine what happened exactly
- Determine the malicious intent of malware software
- Identify indicators of compromise
- Determine the complexity level of an intruder
- Identify the exploited vulnerability
- Identify the extent of damage caused by intrusion
- Catch the perpetrator accountable for installing the malware
- Find signatures for host and network-based intrusion detection systems
- Evaluate harm from an intrusion

- List the indicators of compromise for different machines and different malware programs
- Find the system vulnerability malware has exploited
- Distinguish the gatecrasher or insider responsible for the malware entry

Some of the most common business questions answered by malware analysis are:

- What is the intention of the malware?
- How did it get through?
- Who are the perpetrators and how good are they?
- How to abolish it?
- What are the losses?
- How long has the system infected?
- What is the medium of malware?
- What are the preventive measures?

Guidelines for Malware Analysis

Following are some of the guidelines to be remembered while performing malware analysis

- During malware analysis, pay attention to the essential features instead of understanding every detail
- Try different tools and approaches to analyze the malware, as single approach may not be helpful
- Identify, understand, and defeat new malware analysis prevention techniques

Types of Malware Analysis

The two types of malware analysis, based on the approach methodology, include static analysis and dynamic analysis.

- **Static Malware Analysis**

  It also known as code analysis, involves going through the executable binary code without actually executing it to have a better understanding of the malware and its purpose.

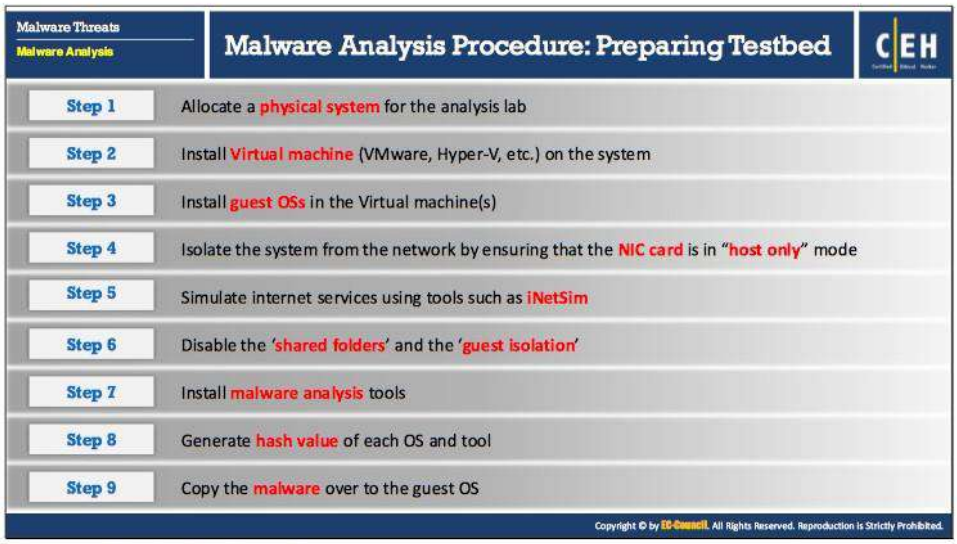
  The general static scrutiny involves analysis of malware without executing the code or instructions. The process includes use of different tools and techniques to determine the malicious part of the program or a file. It also gathers the information about malware functionality and collects technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size.

- **Dynamic Malware Analysis**

  It also known as behavioral analysis, involves executing the malware code to know how it interacts with the host system and its impact on it after infecting the system.

Dynamic analysis involves execution of malware to examine its conduct, operations and identifies technical signatures that confirm the malicious intent. It reveals information, such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, DLL and linked files located on the system or network.

Both techniques are intended to understand how the malware works but differ in the tools used, and the time and skills required for performing the analysis. It is recommended to perform both static and dynamic analysis to understand the functionality of malware to a greater extent.



Malware Analysis Procedure

Malware analysis provides an in-depth understanding of each sample and identifies emerging technical trends from the vast collections of malware samples without actually executing them. The samples of malware are mostly compatible with the Windows binary executable. There are a variety of goals for performing malware analysis.

It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

The following are the procedural steps for malware analysis:

1. Preparing Testbed
2. Static Analysis
3. Dynamic Analysis

Preparing Testbed

Requirements to build a testbed:

- An isolated test network to host your test bed and isolated network services, such as DNS
- Victim machines, installed with a variety of OSs and configuration states (non-patched, patched, etc.)
- Virtualization snapshots and re-imaging tools to wipe and rebuild the victim's machine quickly
- Some tools are required for testing. Following are the more important ones:

- **Imaging tool**: To get a clean image for forensics and prosecution purpose.
- **File/data analysis**: To perform static analysis of potential malware files.
- **Registry/configuration tools**: Malware infects the Windows registry and other configuration variables. These tools help to identify the last saved settings.
- **Sandbox**: To perform dynamic analysis manually.
- **Log analyzers**: The devices under attack record the activities of malware and generate log files. Log analyzers are the tools used to extract log files.
- **Network capture**: To understand how the malware leverages the network.

Steps to prepare the testbed:

- **Step 1**: Allocate a physical system for the analysis lab
- **Step 2**: Install Virtual machine (VMware, Hyper-V, etc.) on the system
- **Step 3**: Install guest OSs on the Virtual machine(s)
- **Step 4**: Isolate the system from the network by ensuring that the NIC card is in "host only" mode
- **Step 5**: Simulate internet services using tools such as iNetSim
- **Step 6**: Disable the 'shared folders' and the 'guest isolation'
- **Step 7**: Install malware analysis tools
- **Step 8**: Generate hash value of each OS and tool
- **Step 9**: Copy the malware over to the guest OS

Supporting Tools for Malware Analysis:

Following are some of the supporting tools required to perform malware analysis:

Virtual Machines Tools:

- Hyper-V (*https://docs.microsoft.com*)
- Parallels Desktop 11 (*http://www.parallels.com*)
- Boot Camp (*https://www.apple.com*)
- VMware vSphere Hypervisor (*http://www.vmware.com*)

Screen Capture and Recording Tools:

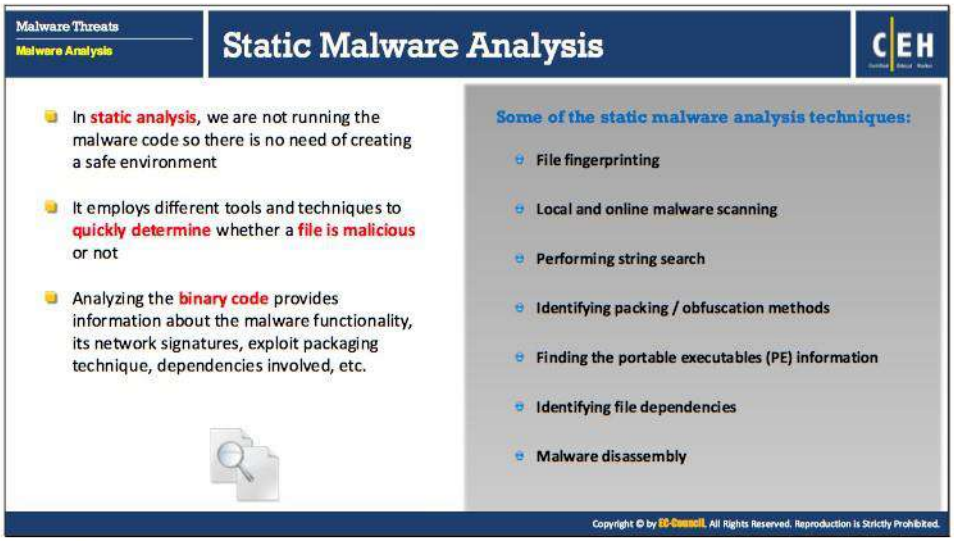
- Snagit (*https://www.techsmith.com*)
- Jing (*https://www.techsmith.com*)
- Camtasia (*https://www.techsmith.com*)
- Ezvid (*http://www.ezvid.com*)

Network and Internet Simulation Tools:

- NetSim (*http://tetcos.com/netsim_gen.html*)
- ns-3 (*https://www.nsnam.org*)
- Riverbed Modeler (*http://www.riverbed.com*)
- QualNet (*http://web.scalable-networks.com*)

OS Backup and Imaging Tools:

- Genie Backup Manager Pro (*http://www.genie9.com*)
- Macrium Reflect Server (*http://www.macrium.com*)
- R-Drive Image (*http://www.drive-image.com*)
- O&O DiskImage 10 (*https://www.oo-software.com*)



Static Analysis

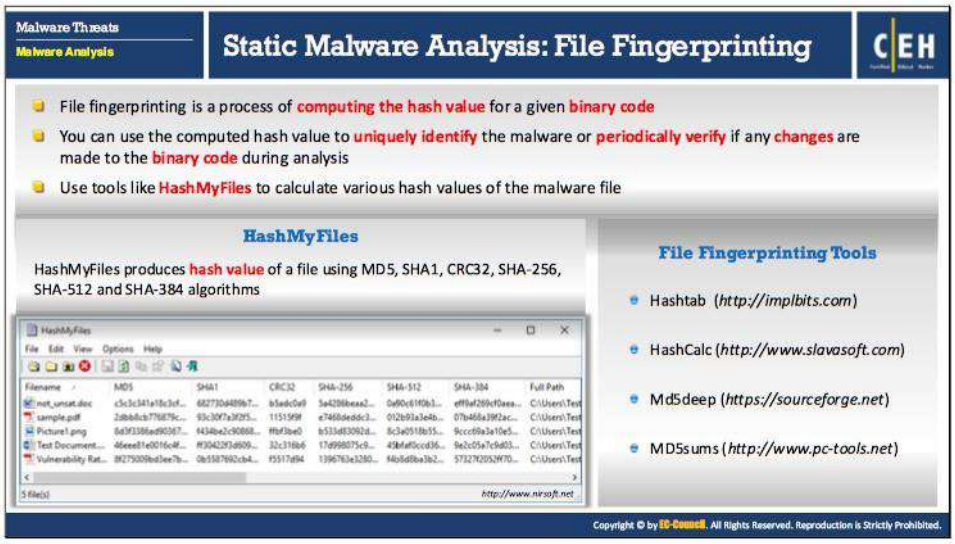
Static analysis is the process of investigating an executable file without running or installing it. It is safe to conduct static analysis because the investigator does not install or execute the suspect file. However, some malware does not need installation for performing malicious activities, so it is better that the investigators perform static analysis in a controlled environment.

Static analysis involves accessing the source code or binary code to find the data structures, function calls, call graphs, etc. that can represent malicious behavior. Investigators can use various tools to analyze binary code to understand file architecture and impact on the system. Compiling the source code of a system into a binary executable will result in data losses, which makes the analysis of the code more difficult. Analyzing the binary code provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, etc.

The procedure of examining a given binary without executing it is mostly manual and requires extraction of intriguing data such as data structures, utilized functions, and call graphs from the malicious file. The investigators cannot see this data after the program compilation.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing/obfuscation methods
- Finding the portable executables (PE) information
- Identifying file dependencies
- Malware disassembly



File Fingerprinting

File fingerprinting is a process of computing the hash value for a given binary code to identify and track data across a network. This process includes calculation of cryptographic hashes of the binary code to recognize its function and compare it to other binary codes and programs faces in the past scenarios. The computed hash value can be used to uniquely identify the malware or periodically verify if any changes are made to the binary code during the analysis process.

These fingerprints are used to track and identify similar programs from a database. Fingerprinting does not work for certain record sorts, including encrypted or password secured files, pictures, audio, and video, which have different content compared to the predefined fingerprint.

The Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are the most commonly used hash functions for malware analysis. Various tools such as HashMyFiles can be used to create a fingerprint of the suspect file as part of the static analysis. HashMyFiles is a GUI-based tool that can calculate various hash values.

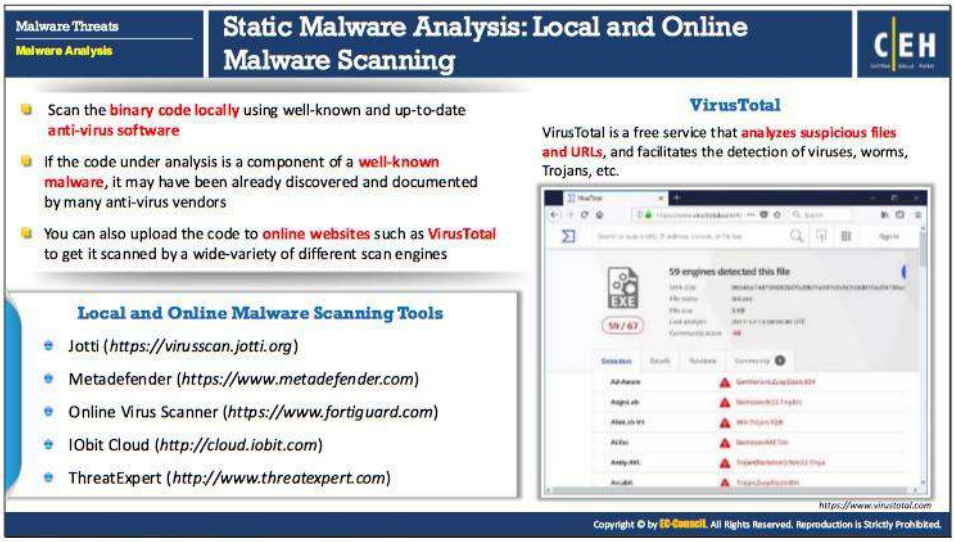
- **HashMyFiles**

  Source: *http://www.nirsoft.net*

  HashMyFiles produces a hash value of a file using MD5, SHA1, CRC32, SHA-256, SHA-512 and SHA-384 algorithms. The program also provides information about the file such as the full path of the file, date of creation, date of modification, file size, file attributes, file version, and extension. This data will help in searching and comparing the similar files them.

Some of the additional file fingerprinting tools include:

- Hashtab (*http://implbits.com*)
- Foundstone's Hash Calculator (*https://www.mcafee.com*)
- md5deep (*https://github.com*)
- MD5sums (*http://www.pc-tools.net*)
- tools4noobs - Online hash calculator (*https://www.tools4noobs.com*)
- Cryptomathic (*http://extranet.cryptomathic.com*)



Local and Online Malware Scanning

You can scan the binary code locally using well-known and up-to-date anti-virus software. If the code under analysis is a component of a well-known malware, it may have been already discovered and documented by many anti-virus vendors. You can also upload the code to online websites such as VirusTotal to get it scanned by a wide-variety of scan engines.

VirusTotal calculates hash values of a suspect file and compares them to online and offline malware databases to find the existence of the recognized malicious code. This process simplifies further investigation by offering better insight into the code, its functionality, and other essential details.

- **VirusTotal**

  Source: *https://www.virustotal.com*

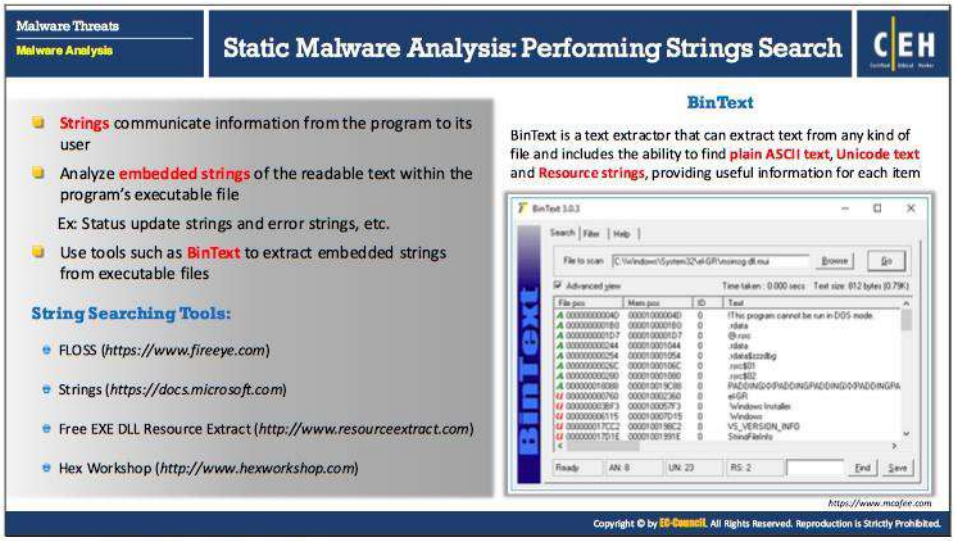
  VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the detection of viruses, worms, Trojans, etc. It generates a report that provides the total number of engines that marked the file as malicious, the malware name, and if available, additional information about the malware.

  It also offers important details of the online file analysis such as target machine, compilation timestamp, type of file, compatible processors, entry point, PE sections, data link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and type of connections established.

Some of the additional local and online malware scanning tools include:

- Jotti (*https://virusscan.jotti.org*)
- Metadefender *(https://www.metadefender.com)*

- Online Virus Scanner (*https://www.fortiguard.com*)
- IObit Cloud (*http://cloud.iobit.com*)
- ThreatExpert (*http://www.threatexpert.com*)
- Malwr (*https://malwr.com*)
- Valkyrie (*https://valkyrie.comodo.com*)
- Dr.Web Online Scanners (*https://vms.drweb.com*)
- UploadMalware.com (*http://www.uploadmalware.com*)
- ThreatAnalyzer (*http://www.threattracksecurity.com)*
- Payload Security (*https://www.payload-security.com*)
- Anubis (*https://sourceforge.net*)
- Windows Defender Security Intelligence (WDSI) (*https://www.microsoft.com*)
- Bitdefender Quickscan (*https://www.bitdefender.com*)

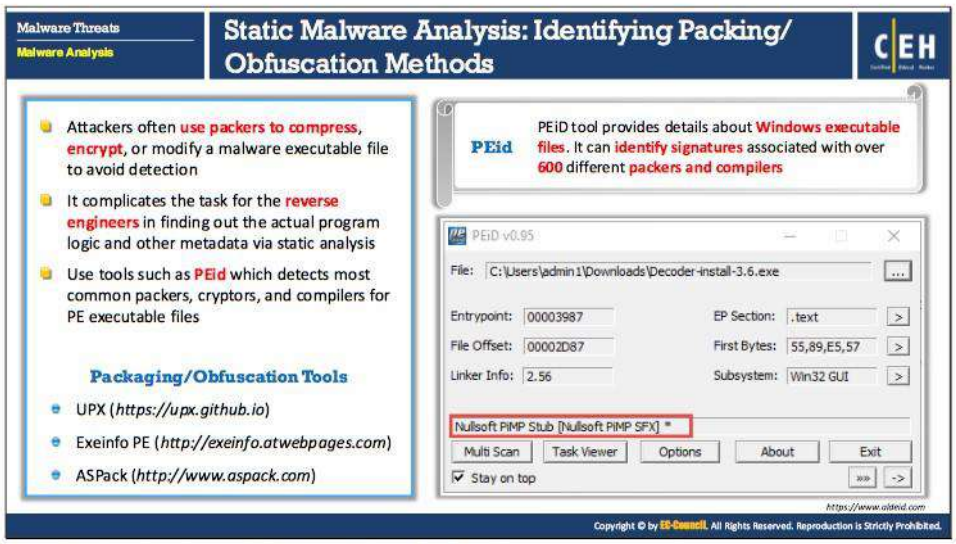


Performing Strings Search

Software programs include some strings that are commands for performing specific functions such as printing output. Strings communicate information from the program to its user. Various strings exist that could represent the malicious intent of a program, such as reading the internal memory or cookie data, etc. embedded in the compiled binary code.

Searching through the strings can provide information about the basic functionality of any program. During malware analysis, search for the malicious string that could determine harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that particular URL string stored in it. You should be attentive while looking for strings and also search for the embedded and encrypted strings to conclude the suspect file.

Use tools such as BinText to extract embedded strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well. Some tools can extract all the strings and copy them to a text or document file. Use such tools to copy the strings to a text file for ease in searching the malicious strings.



Identifying Packing/Obfuscation Methods

Attackers use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file. It complicates the task for the reverse engineers in finding out the actual program logic and other metadata via static analysis.

You should try to determine if the file includes packed elements and also locate the tool or method used for packing it. Use tools such as PEid which detects most common packers, cryptors, and compilers for PE executable files. Finding the packer will ease the task of selecting a tool for unpacking the code.

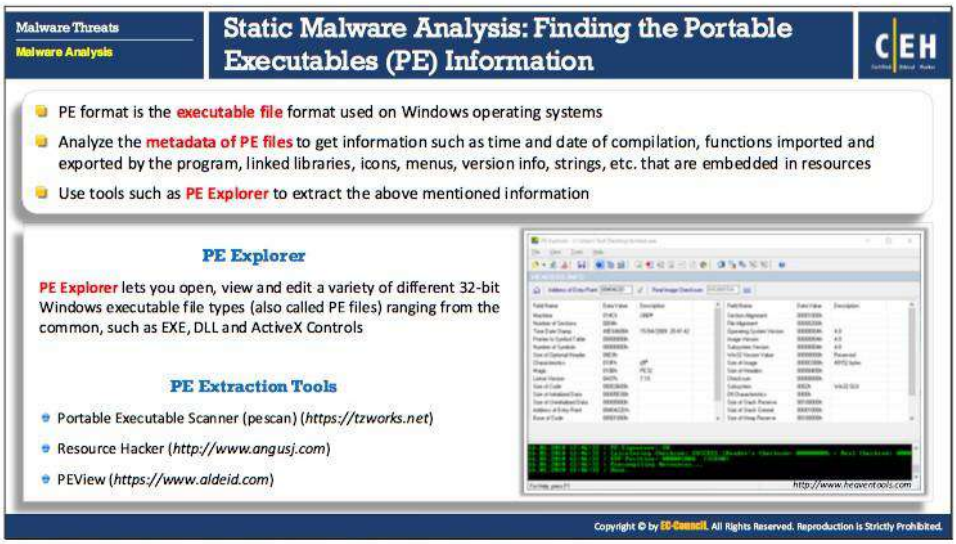
- **PEiD**

  Source: *https://www.aldeid.com*

  PEiD is a free tool that will provide details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packers used in packing the program. Additional details it displays include entry point, file offset, EP Section, and subsystem used for packing.

Some of the additional packaging/obfuscation tools include:

- UPX (*https://upx.github.io*)
- Exeinfo PE (*http://exeinfo.atwebpages.com*)
- ASPack (*http://www.aspack.com*)



Finding the Portable Executables (PE) Information

Portable Executables (PE) format is the executable file format used on Windows OSs, which stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding the additional details of the file. For instance, Windows binary is in PE format that consists of information, such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, as well as strings, menus, and symbols. The PE format contains header and sections, which stores metadata about the file and code mapping in an OS.

The PE of a file contains the sections:

- **.text:** Contains instructions and program codes that the CPU executes.
- **.rdata:** Contains the import and export information as well as other read-only data used by the program.
- **.data:** Contains the program's global data, which the system can access from anywhere.
- **.rsrc:** Comprises of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support.

You can use the header information to gather additional details of a file or program, such as features. You can use tools such as PEView to extract the above-mentioned information.

- **PE Explorer**

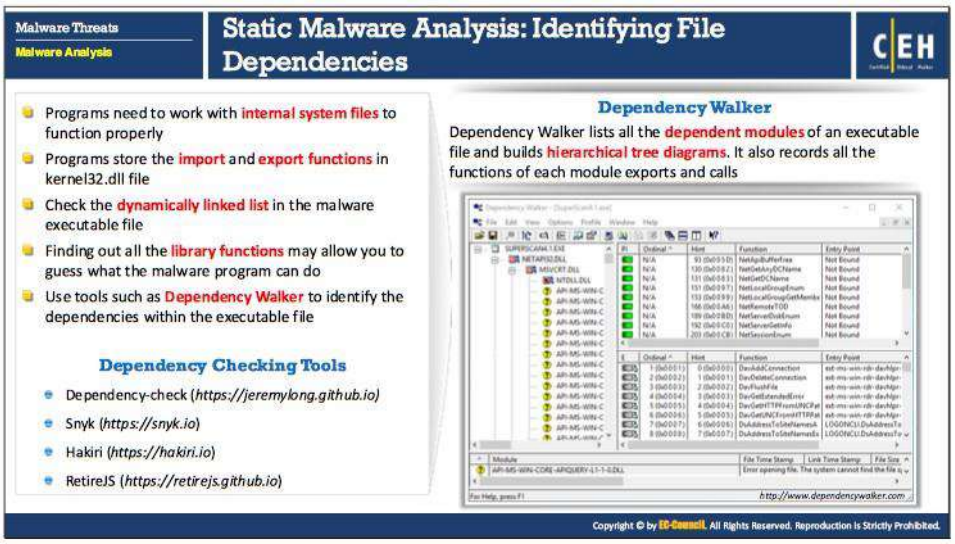
  Source: *http://www.heaventools.com*

  PE Explorer lets you open, view and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from the common, such as EXE, DLL and ActiveX

Controls, to the less familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

Some of the additional PE extraction tools include:

- Portable Executable Scanner (pescan) (*https://tzworks.net*)
- Resource Hacker (*http://www.angusj.com*)
- PEView (*https://www.aldeid.com*)



Identifying File Dependencies

Any software program depends on various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store the import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files the program needs to function properly, the process of registration and location on the machine.

You need to find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Afterthat, it needs to be checked if they can find and analyze these files as they can provide information about malware in a file. File dependencies include linked libraries, functions and function calls. Check the dynamically linked list in the malware executable file. Finding out all the library functions may allow to guess about what the malware program can do. You should know the various dll used to load and run a program.

Some of the standard dlls are:

dll	Description of contents
Kernel32.dll	Core functionality, such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components, such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel

WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

TABLE 7.5: Standard dlls

You can use tools such as Dependency Walker to identify the dependencies within the executable file.

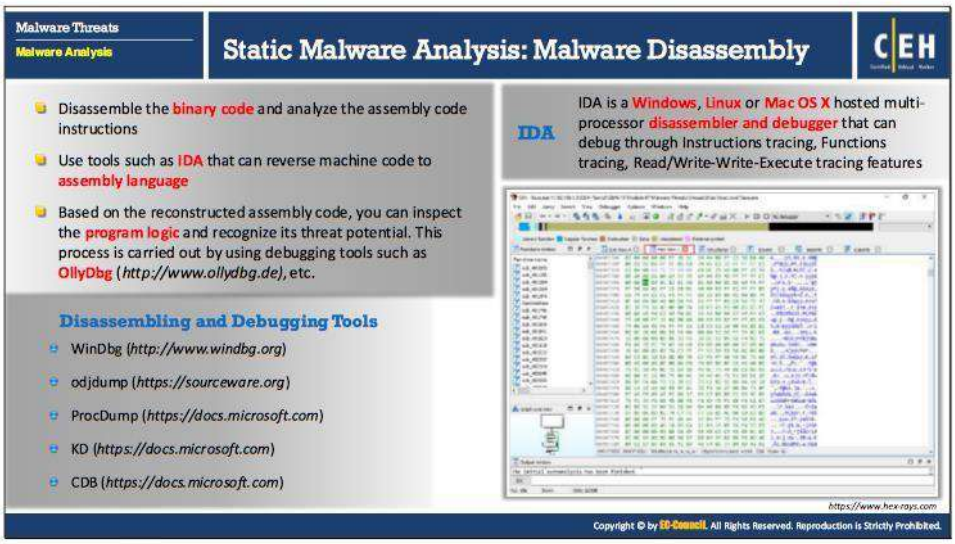
- **Dependency Walker**

  Source: *http://www.dependencywalker.com*

  Dependency Walker lists all the dependent modules of an executable file and builds hierarchical tree diagrams. It also records all the functions of each module exports and calls. It also detects many common application problems such as missing and invalid modules, import/export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

Some of the additional dependency extraction tools include:

- Dependency-check (*https://jeremylong.github.io*)
- Snyk (*https://snyk.io*)
- Hakiri (*https://hakiri.io*)
- Retire.js (*https://retirejs.github.io*)



Malware Disassembly

The static analysis also includes dismantling of a given executable into binary format to study its functionalities and features. This process will help to identify the language used for programming the malware, look for APIs that reveal its function, etc. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process can be carried out by using debugging tools such as IDA Pro, OllyDbg, etc.

- **IDA**

  Source: *https://www.hex-rays.com*

  IDA Pro is a multi-platform disassembler and debugger that explores binary programs, for which source code is not always available, to create maps of their execution. It shows the instructions in the same way as a processor executes them in a symbolic representation called assembly language. Thus, it is easy for you to find the harmful or malicious processes.

  Features:

  - Disassembler

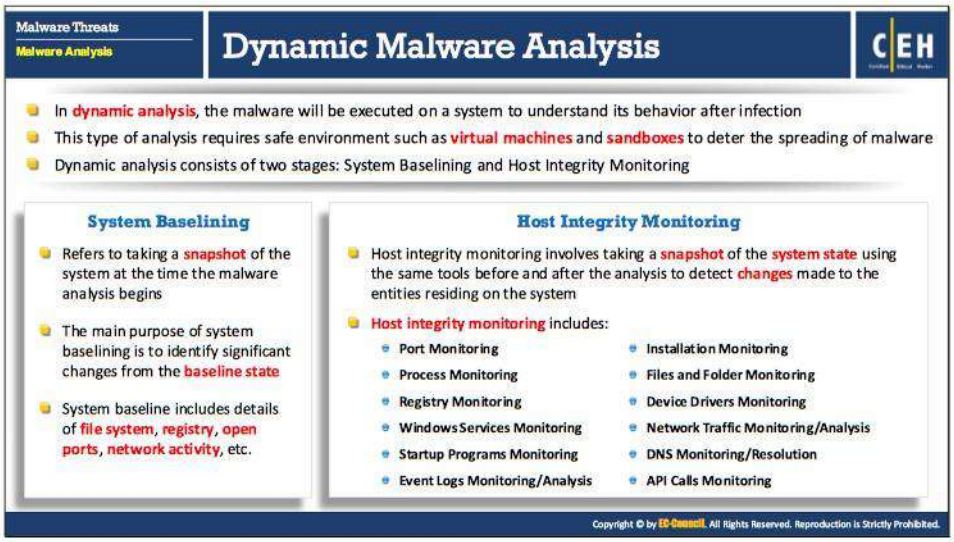
    As a disassembler, IDA Pro explores binary programs for which source code is not always available, to create maps of their execution.

  - Debugger

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

Some of the additional debugging tools include:

- OllyDbg (*http://www.ollydbg.de*)
- WinDbg (*http://www.windbg.org)*
- objdump (*https://sourceware.org*)
- ProcDump (*https://docs.microsoft.com*)
- KD (*https://docs.microsoft.com*)
- CDB (*https://docs.microsoft.com*)
- NTSD (*https://docs.microsoft.com*)



Dynamic Analysis

Dynamic malware analysis is the process of studying the behavior of the malware by running it in a monitored environment. This type of analysis requires safe environment such as virtual machines and sandboxes to deter the spreading of malware. The environment design should include the tools that can capture every movement of the malware in detail and give feedback. Typically, virtual systems act as a base for conducting such experiments.

Dynamic analysis is performed to gather valuable information about malware activity including files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified, processes and services the malware started, etc.

You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network and the testing system is capable of recovering from an earlier set timeframe in case anything goes wrong during the test. To achieve this, the investigator needs to perform the following:

- **System Baselining**

  Baselining refers to the process of capturing system state (taking snapshot of the system) at the time the malware analysis begins that can be used to compare the system's state after executing the malware file. This will help to understand the changes malware has made across the system. System baseline includes recording details of the file system, registry, open ports, network activity, etc.

- **Host Integrity Monitor**

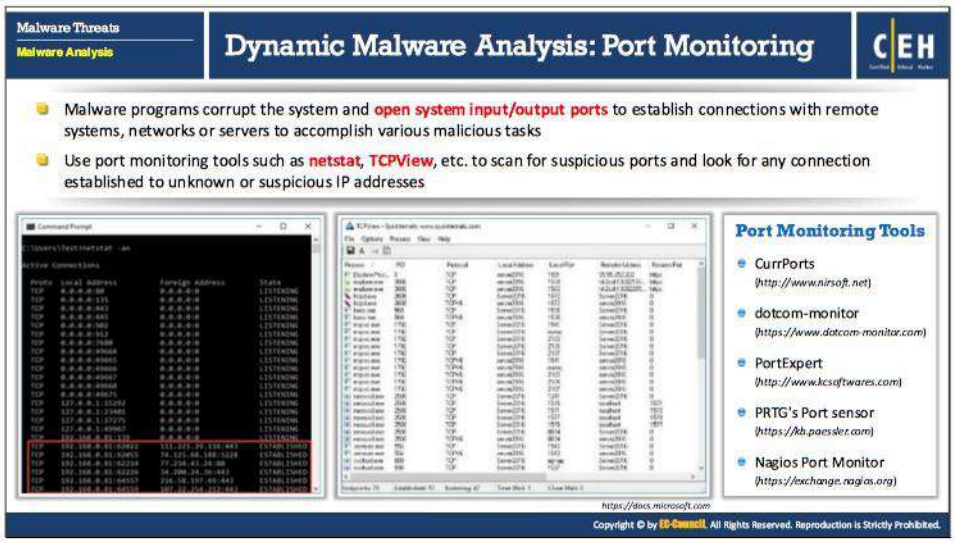
  Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves taking a

snapshot of the system before and after the incident or actions using the same tools and analyzing the changes to evaluate the impact on the system and its properties.

In malware analysis, host integrity monitoring will help to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, etc.

Host integrity monitoring includes:

- Port Monitoring
- Process Monitoring
- Registry Monitoring
- Windows Services Monitoring
- Startup Programs Monitoring
- Event Logs Monitoring/Analysis
- Installation Monitoring
- Files and Folder Monitoring
- Device Drivers Monitoring
- Network Traffic Monitoring/Analysis
- DNS Monitoring/Resolution
- API Calls Monitoring



Port Monitoring

Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks or servers to accomplish various malicious tasks. These open ports can also form backdoors for another type of harmful malware and programs. Open ports act as communication channels for malware. They open unused ports on the victim's machine to connect back to the malware handlers. Scanning for suspicious ports will help in identifying this malware.

You can also find if malware is trying to access a particular port during dynamic analysis by installing port monitoring tools such as TCPView and Windows command line utility tools such as netstat. The port monitoring tools will offer details such as the protocol used, local address, remote address and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

- **Netstat**

  It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

  Syntax

  ```
  netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
  ```

  Parameters

  - **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by the protocol. By default, statistics are shown in the figure for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.

In the image above, the command **netstat -an** displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening along with addresses and port numbers.

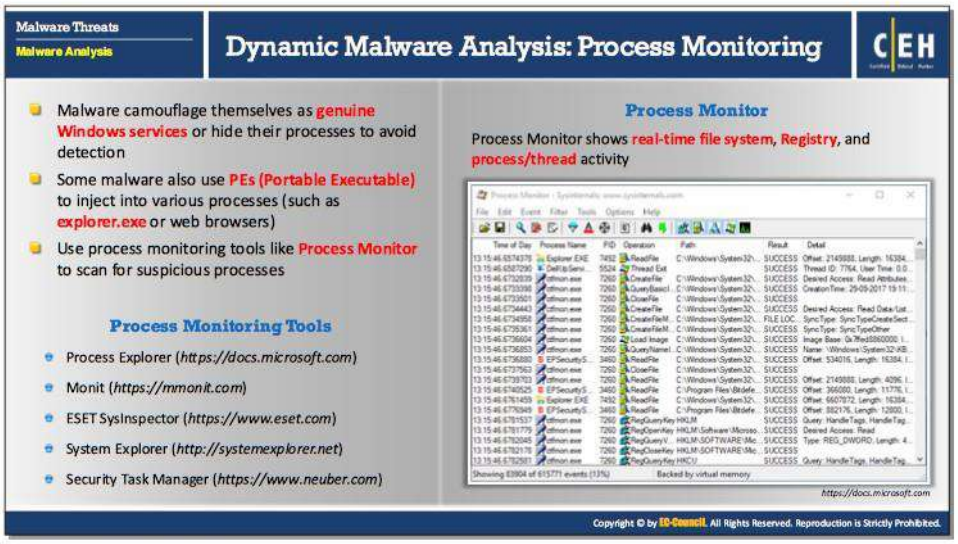
- **TCPView**

  Source: *https://docs.microsoft.com*

  TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses, and the state of TCP connections. It provides a subset of the Netstat program that ship with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain-name versions.

Some of the additional port monitoring tools include:

- CurrPorts (*http://www.nirsoft.net*)
- dotcom-monitor (*https://www.dotcom-monitor.com*)
- PortExpert (*http://www.kcsoftwares.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Nagios Port Monitor (*https://exchange.nagios.org*)



Process Monitoring

Malware makes their entry into the system through pictures, music files, videos, etc. that are downloaded from the Internet and camouflage themselves as genuine Windows services and hide their processes to avoid detection. Some malware use PEs to inject into various processes (such as explorer.exe or web browsers). Malicious processes are visible, but look like legitimate processes and also helps bypass desktop firewalls. Attackers use specific rootkit methods to make the malware hide in the system so that the antivirus software cannot commonly detect it.

Process monitoring will help in understanding the processes malware initiates and takes over after execution. They should also observe the child processes, associated handles, loaded libraries, and functions, to define the entire nature of a file or program, gather information about processes running before execution of the malware, and compare them to the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all the processes malware starts. Use process-monitoring tools such as Process Monitor to detect suspicious processes.

- **Process Monitor**

  Source: *https://docs.microsoft.com*

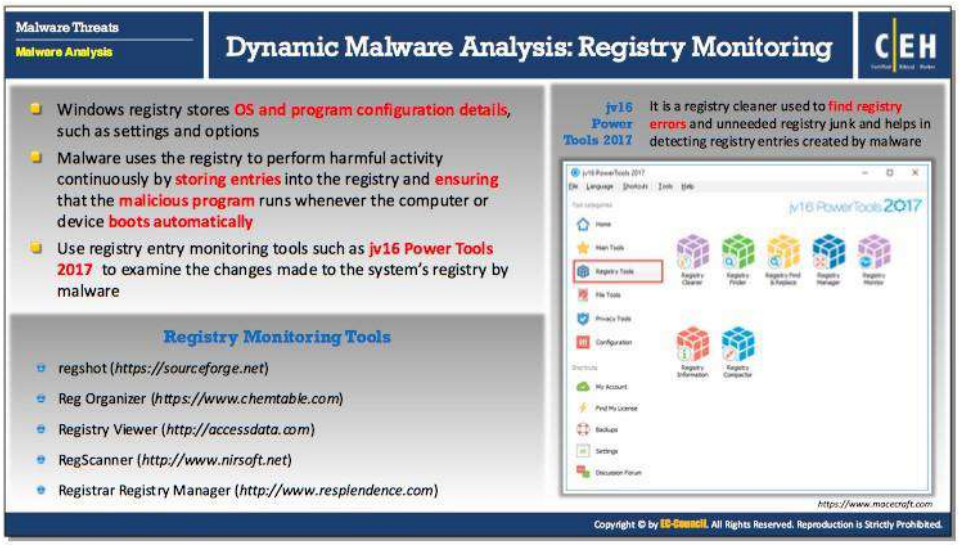
  Process Monitor is a monitoring tool for Windows that shows real-time file system, Registry, and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and so on. Unique features of Process Monitor make it a core utility in system troubleshooting and malware hunting toolkit.

Features:

- More data captured for operation input and output parameters.
- Non-destructive filters allow you to set filters without losing data.
- Capture of thread stacks for each operation makes it possible in many cases to identify the cause of an operation.
- Reliable capture of process details, including image path, command line, user and session ID.
- Configurable and moveable columns for any event property.
- Filters can be set for any data field, including fields not configured as columns.
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
- Process tree tool shows the relationship of all processes referenced in a trace.
- Native log format preserves all data for loading in a different Process Monitor instance.

Some of the additional process monitoring tools include:

- Process Explorer *(https://docs.microsoft.com)*
- Monit *(https://mmonit.com)*
- ESET SysInspector *(https://www.eset.com)*
- System Explorer *(http://systemexplorer.net)*
- Security Task Manager *(https://www.neuber.com)*
- HiJackThis *(https://sourceforge.net)*
- Yet Another (remote) Process Monitor(*http://yaprocmon.sourceforge.net*)
- Proc Net Monitor *(http://securityxploded.com)*
- OpManager *(https://www.manageengine.com)*



Registry Monitoring

Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. The malware uses the registry to perform harmful activity continuously by storing entries into the registry and ensuring that the malicious program run whenever computer or device boots automatically.

When an attacker installs a type of malware on the victim's machine, it generates a registry entry. Consequently, various changes will be noticed such as the system gets slower, various advertisements keep popping up, and so on.

Windows automatically executes instructions in the following sections of registry:

- ***Run***
- ***RunServices***
- ***RunOnce***
- ***RunServicesOnce***
- ***HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.***

Malware inserts instructions in these sections of the registry to perform malicious activities. You should have a fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. Use registry monitoring tools like RegScanner to scan registry values for any suspicious entries that may indicate the malware infection

- **jv16 Power Tools 2017**

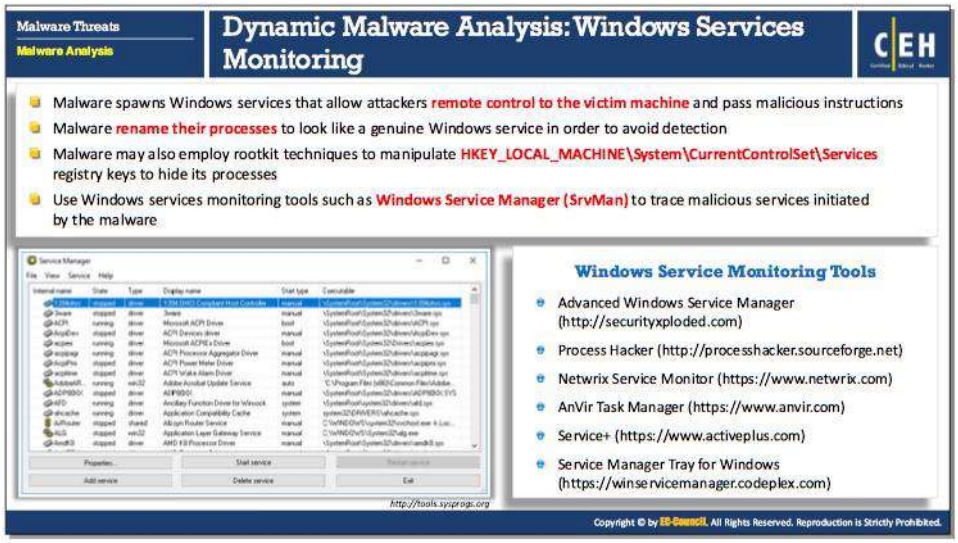
  Source: *https://www.macecraft.com*

Jv16 Power Tools is a PC system utility software that works by cleaning out unneeded files and data, cleaning the Windows registry, automatically fixing system errors and applying optimization to your system. It allows to scan and monitor the Registry.

It helps in detecting registry entries created by malware. "Clean And Speedup My Computer" feature of Registry Cleaner in jv16 Power Tools 2017 is a solution for fixing registry errors and system errors, cleaning registry leftovers, as well as unneeded files such as old log files and temporary files.

Some of the additional registry monitoring tools include:

- regshot *(https://sourceforge.net)*
- Reg Organizer *(https://www.chemtable.com)*
- Registry Viewer *(http://accessdata.com)*
- RegScanner (*http://www.nirsoft.net*)
- Registrar Registry Manager *(http://www.resplendence.com)*
- Active Registry Monitor *(https://www.devicelock.com)*
- MJ Registry Watcher (*http://www.jacobsm.com*)
- Buster Sandbox Analyzer *(http://bsa.isoftware.nl)*



Windows Services Monitoring

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most of the services run in the background to support processes and applications, the malicious services are invisible even when are performing harmful activities on the system and can function even without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

These malicious services run as SYSTEM account or other privileged accounts, which provides more access compared to the user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with manes similar to genuine Windows services to avoid detection.

You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), that can detect changes in services and also scan for suspicious Windows services.

- **Windows Service Manager (SrvMan)**

  Source: *http://tools.sysprogs.org*

  SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such service is stopped, main application window is closed automatically). You can use SrvMan's Command Line interface to perform the following tasks:

- **Create services**

```
srvman.exe add <file.exe/file.sys> [service name] [display name]
[/type:<service type>] [/start:<start mode>] [/interactive:no]
[/overwrite:yes]
```

- **Delete services**

```
srvman.exe delete <service name>
```

- **Start/stop/restart services**

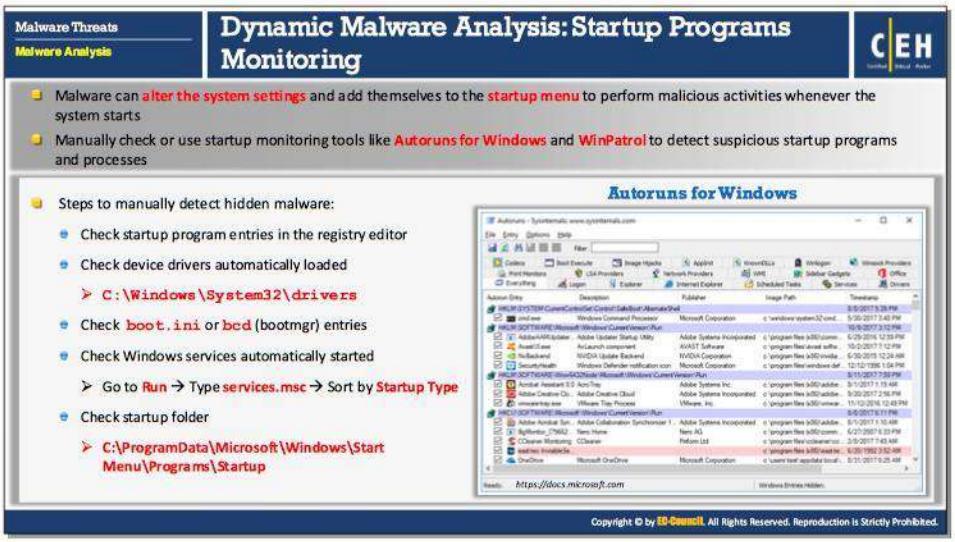
```
srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]
srvman.exe restart <service name> [/delay:<delay in msec>]
```

- **Install and start a legacy driver with a single call**

```
srvman.exe run <driver.sys> [service name] [/copy:yes]
[/overwrite:no] [/stopafter:<msec>]
```

Some of the additional Windows service monitoring tools include:

- Advanced Windows Service Manager (*http://securityxploded.com*)
- Process Hacker *(http://processhacker.sourceforge.net)*
- Netwrix Service Monitor *(https://www.netwrix.com)*
- AnVir Task Manager *(https://www.anvir.com)*
- Service+ (*https://www.activeplus.com*)
- Service Manager Tray for Windows (*https://winservicemanager.codeplex.com*)
- Nagios XI (*https://www.nagios.com*)
- Windows Service Monitor (*https://www.manageengine.com*)
- PC Services Optimizer *(https://www.smartpcutilities.com)*
- SMART Utility *(https://www.volitans-software.com)*



Startup Programs Monitoring

Malware can alter the system settings and add themselves to the startup menu to perform malicious activities whenever the system starts. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows is essential for detecting malware.

Steps to manually detect hidden malware:

- **Step 1: Check startup program entries in the registry**

  Startup items such as programs, shortcuts, folders, and drivers are set to run automatically at startup when users log into a Windows OS (e.g., Windows 10). Startup items can be added by either the programs or drivers installed, or manually by the user. Programs that run on Windows 10 startup can be located in these registry entries, such as Windows startup setting, Explorer startup setting, and IE startup setting.

  - **Windows Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

  - **Explorer Startup Setting**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup`

- **IE Startup Setting**

  `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks`

  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar`

  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions`

  `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\MenuExt`

- **Step 2: Check device drivers automatically loaded**

  Navigate to `C:\Windows\System32\drivers` to check the device drivers.

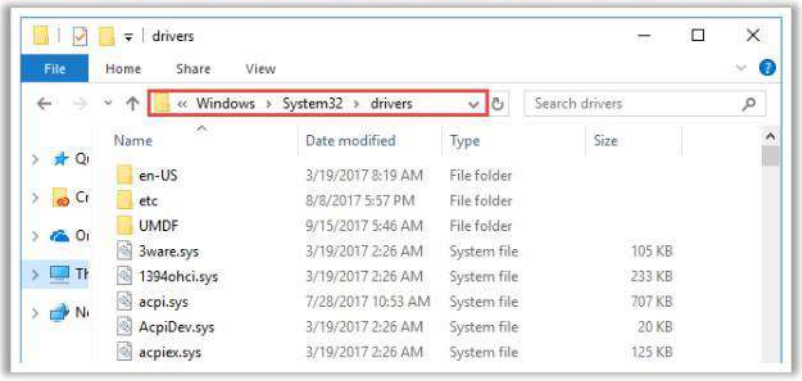


FIGURE 7.4: Screenshot displaying drivers folder

- **Step 3: Check boot. ini or bcd (bootmgr) entries**

  Check **boot.ini** or **bcd** (bootmgr) entries using command prompt. Open **command prompt with administrator,** type **bcdedit** command and press **Enter** button to view all the boot manager entries.

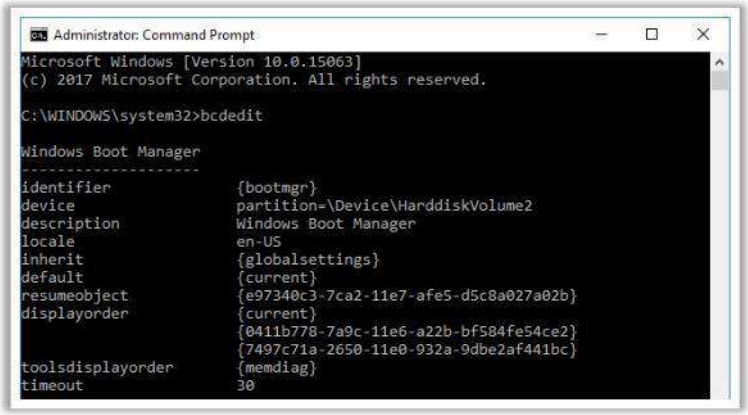


FIGURE 7.5: Screenshot displaying boot info

- **Step 4: Check that Windows services automatic started**

  Go to **Run** → Type **services.msc** and press Enter. Sort the services by **Startup Type** to check the Windows services list for viewing services that start automatically when system boot.

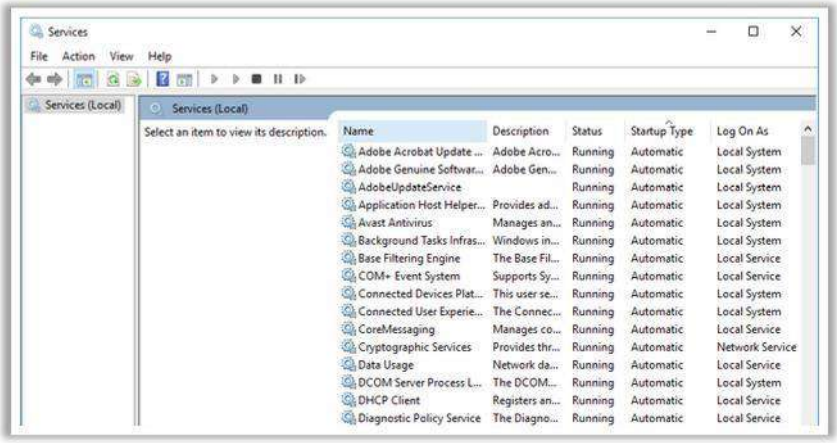


FIGURE 7.6: Screenshot displaying services

- **Step 5: Check the Startup folder**

  Startup folders store the applications or shortcuts for applications that auto-start when the system boots. To check the **Startup** applications, search the following locations on Windows 10:

  - **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup**

- `C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup`

Another method to access startup folders is:

1. Press the **Windows + R** buttons simultaneously to open the **Run** box
2. Type **shell: startup** in the box and click **OK** button to navigate to the startup folder

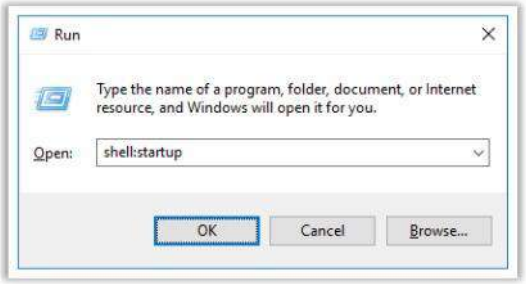


FIGURE 7.7: Screenshot showing shell: startup command in Run box

Startup Program Monitoring Tool: Autoruns for Windows

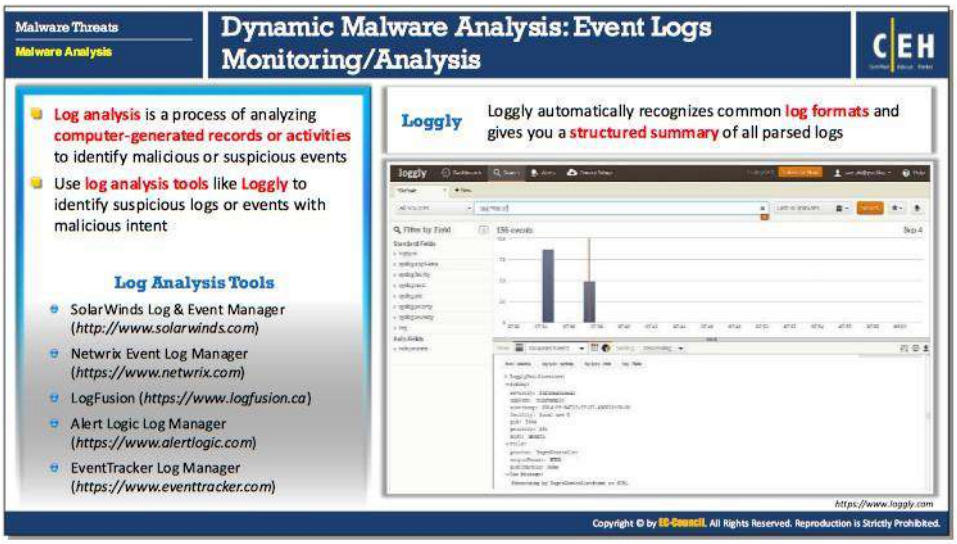
Source: *https://docs.microsoft.com*

This utility can auto-start the location of any startup monitor, display what programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program includes in the startup folder, Run, RunOnce, and other Registry keys; users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user to zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on a system.

Some of the additional startup programs monitoring tools include:

- WinPatrol (*https://www.winpatrol.com*)
- Autorun Organizer (*https://www.chemtable.com*)
- Quick Startup (*http://www.glarysoft.com*)
- StartEd Pro (*http://www.outertech.com*)
- Chameleon Startup Manager (*http://www.chameleon-managers.com*)
- BootRacer (*http://www.greatis.com*)
- WinTools.net: Startup Manager (*http://www.wintools.net*)
- EF StartUp Manager (*http://www.efsoftware.com*)
- PC Startup Master (*https://www.smartpcutilities.com*)
- CCleaner (*https://www.piriform.com*)
- Startup Delayer (*http://www.r2.com.au*)



Event Logs Monitoring/Analysis

Log analysis is a process that provides the details of an activity or an event that can extract possible attacks in the form of Trojans or worms on the system. It serves as a primary source of information and helps in identifying security gaps. This process helps in detecting zero-day backdoor Trojans or any possible attacks (failed authentication/ login attempts) when logs are analyzed on different components. Log monitoring performed on components that perform security operations such as firewall systems, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), web servers, authentication servers, etc. The logs also contain file types, ports, time stamps and registry entries. In Windows, system logs, application logs, and security logs can be analyzed in Event Viewer under the section "Windows Logs."

Logs are located via the following paths:

- **System logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs

- **System Security logs**

  Start → Windows Administrative Tools → Event Viewer → Windows Logs → Security

- **Applications and Services Logs**

  Start → Windows Administrative Tools → Event Viewer → Applications and Services Logs

Log Analysis Tools:

- **Loggly**

  Source: *https://www.loggly.com*

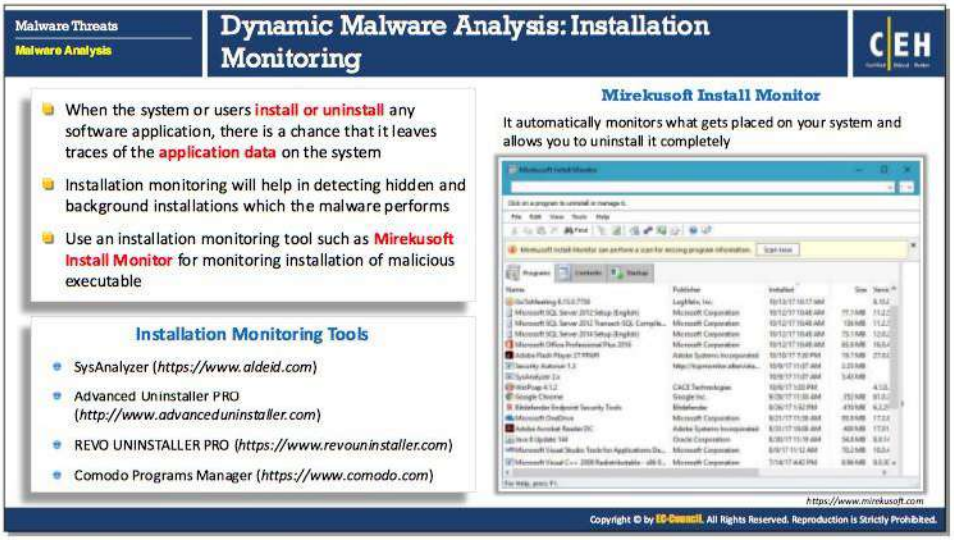
  Loggly automatically recognizes common log formats and gives a structured summary of all your parsed logs. It provides real-time log monitoring, system behavior, and unusual activity. It brings logs from the depths of an organizations infrastructure to track activity and analyze trends. It shows how components interact and identify correlations. Logs can be captured in real-time either on syslog or HTTP.

  Features:

  - Tracks SLA compliance, and identify anomalies and suspicious events
  - Secures log data transmission
  - Generates a real--time, bird's–eye view of logs
  - Monitors proactively

Some of the additional log monitoring/analysis tools include:

- SolarWinds Log & Event Manager (*http://www.solarwinds.com*)
- Netwrix Event Log Manager (*https://www.netwrix.com*)
- LogFusion (*https://www.logfusion.ca*)
- AlertLogic Log Manager (*https://www.alertlogic.com*)
- EventTracker Log Manager (*https://www.eventtracker.com*)
- Process Lasso Pro (*https://bitsum.com*)
- Splunk (*https://www.splunk.com*)



Installation Monitoring

When the system or users install or uninstall any software application, there is a chance that it leaves traces of the application data on the system. To find these traces, you should know the folders modified or created during the installation process as well as the files and folders which have not been modified by the uninstall process. Installation monitoring will help in detecting hidden and background installations which the malware performs. Tools like SysAnalyzer can be used to monitor installation of malicious executables.

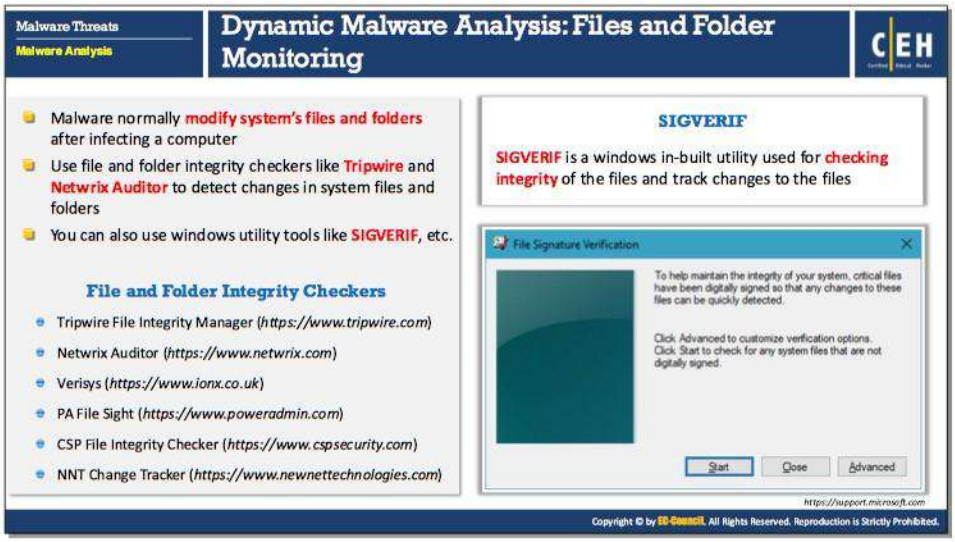
- **Mirekusoft Install Monitor**

  Source: *https://www.mirekusoft.com*

  Mirekusoft Install Monitor automatically monitors what gets placed on your system and allows to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry are created when a program is installed. It provides detailed information about the software installed. You can find out how much disk, CPU, and memory your programs are using. It also provides information about how often you use different programs. The program tree is a useful tool that can show you which programs were installed together.

Some of the additional installation monitoring tools include:

- SysAnalyzer (*https://www.aldeid.com*)
- Advanced Uninstaller PRO (*http://www.advanceduninstaller.com*)
- REVO UNINSTALLER PRO (*https://www.revouninstaller.com*)
- Comodo Programs Manager (*https://www.comodo.com*)



Files and Folder Monitoring

Malware can modify the system files and folders to save some information on them. You should be able to find the files and folders which malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware would schedule for execution on a specific schedule.

Scan for suspicious files and folders using tools such as SIGVERIF, FCIV, Fastsum, WinMD5, Tripwire, etc. to detect any Trojans installed and system file modifications.

- **SIGVERIF**

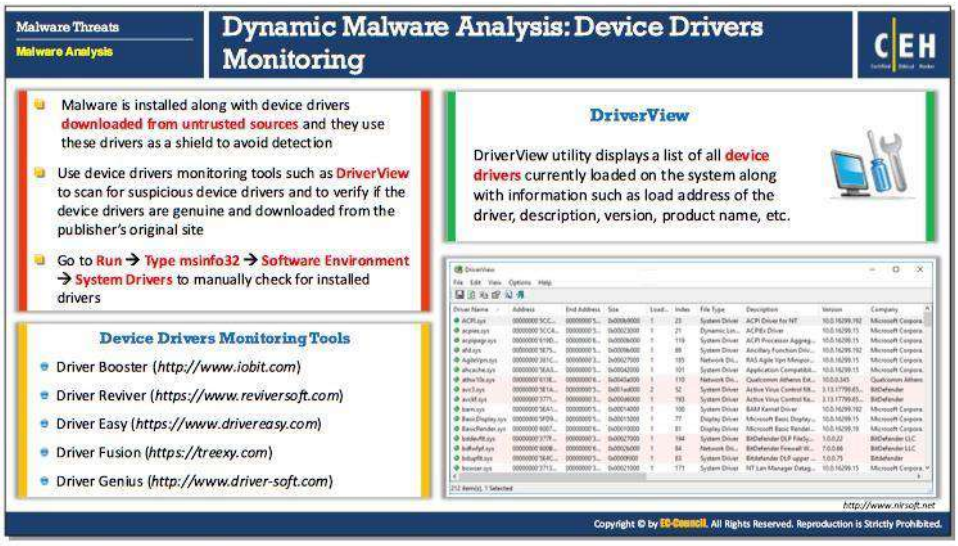
  Source: *https://support.microsoft.com*

  SIGVERIF is a built-in Windows tool that comes inbuilt in Windows 10/8/7 and searches for unsigned drivers on a system. This tool will help to find unsigned drivers. When you observe an unsigned driver, you can move that to a new folder, restart the system, and test the program and its functionality for errors. Below are the steps for identifying unsigned drivers using SIGVERIF:

  - Click **Start → Run**, type **SIGVERIF**, and then click **OK**.
  - Click the **Advanced** button. Click **Look for other files that are not digitally signed**.
  - Navigate to the **Windows\System32\drivers** folder, and then click **OK**.
  - After Sigverif is finished running its check, it displays a list of all unsigned drivers installed on the computer. One can find the list of all signed and unsigned drivers found by Sigverif in the Sigverif.txt file in the %Windir% folder, typically the Windows folder.

Some of the additional File integrity checking Tools include:

- Tripwire File Integrity Manager (*https://www.tripwire.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- Verisys (*https://www.ionx.co.uk*)
- PA File Sight (*https://www.poweradmin.com*)
- CSP File Integrity Checker (*https://www.cspsecurity.com*)
- NNT Change Tracker (*https://www.newnettechnologies.com*)
- AFICK (Another File Integrity Checker) (*https://sourceforge.net*)
- Fsum Frontend (*http://fsumfe.sourceforge.net*)
- OSSEC (*https://ossec.github.io*)
- IgorWare Hasher (*http://www.igorware.com*)



Device Drivers Monitoring

The system installs malware along with the device drivers when user downloads infected drivers from untrusted sources; malware uses these drivers as a shield to avoid their detection. One can scan for suspicious device drivers using tools such as DriverView, Driver Detective, etc. to verify if they are genuine and downloaded from the publisher's original site.

The path to the location of Windows system drivers is:

Goto **Run** → Type **msinfo32** → **Software Environment** → **System Drivers**

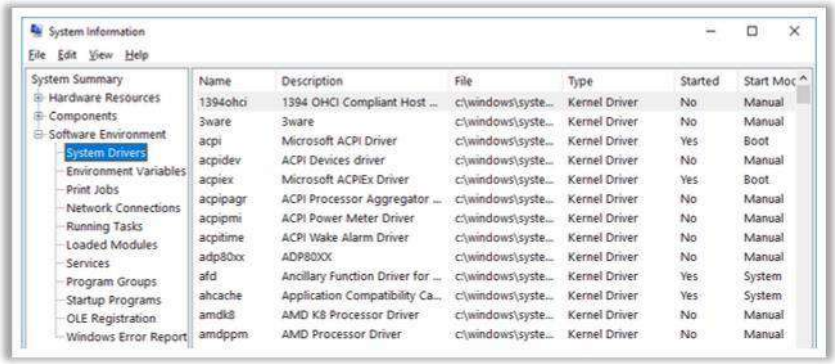


FIGURE 7.8: Screenshot displaying Windows System Drivers

- **DriverView**

  Source: *http://www.nirsoft.net*

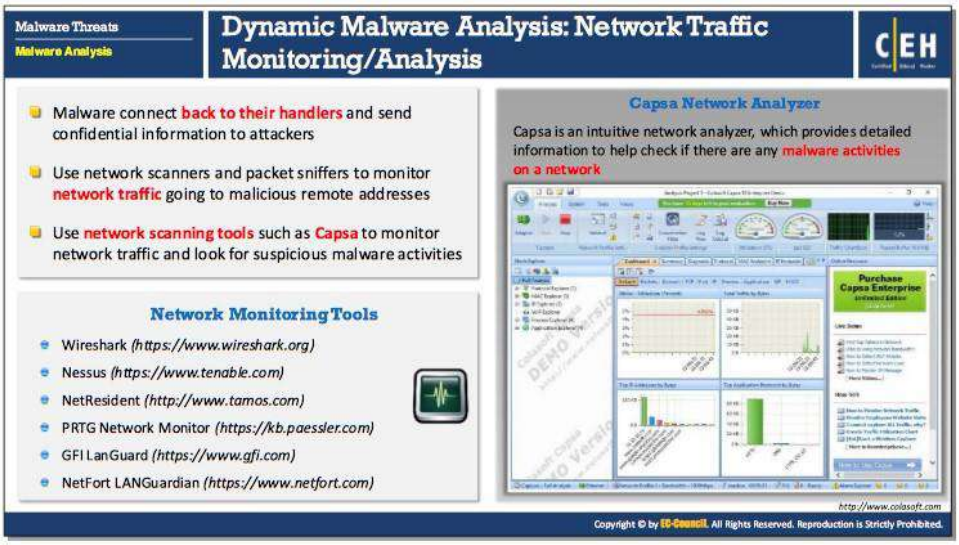
  DriverView utility displays the list of all **device drivers** currently loaded on the system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, company that created the driver, etc.

  Features:

  - Displays the list of all loaded drivers on your system
  - Standalone executable

Some of the additional device driver monitoring tools include:

- Driver Booster (*http://www.iobit.com*)
- Driver Reviver *(https://www.reviversoft.com)*
- Driver Easy *(https://www.drivereasy.com)*
- Driver Fusion (*https://treexy.com*)
- Driver Genius *(http://www.driver-soft.com)*
- Unknown Device Identifier *(http://www.zhangduo.com)*
- Driver Magician *(http://www.drivermagician.com)*
- DriverHive *(http://www.driverhive.com)*
- InstalledDriversList *(https://www.nirsoft.net)*
- My Drivers (*http://www.zhangduo.com*)
- Driver Agent Plus (*http://scan.driverguide.com*)
- DriverPack (*https://drp.su*)



Network Traffic Monitoring/Analysis

Network analysis is the process of capturing the network traffic and investigating it carefully to determine the malware activity. It helps to find the type of traffic/network packets or data transmitted across the network.

Malware depends on the network for various activities such as propagation, downloading malicious content, transmitting sensitive files and information, offering a remote control to attackers, etc. Therefore, you should adopt techniques that can detect the malware artifacts and usage across networks. Some malware connects back to handlers and send confidential information to attackers.

In dynamic analysis, you run a piece of malware in a controlled environment that is installed with various network monitoring tools to trace all the networking activities of malware. Network monitoring tools such as Capsa Network Analyzer, Wireshark, etc. can be used to monitor and capture live network traffic to and from the victim system during execution of the suspect program. This will help to understand the malware's network artifacts, signatures, functions, and other elements.

- **Capsa Network Analyzer**

  Source: *http://www.colasoft.com*

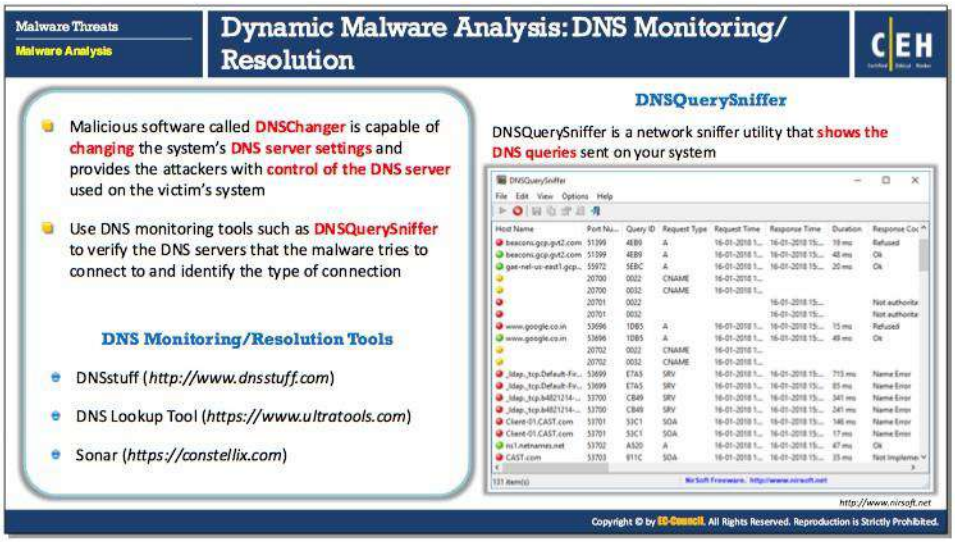
  Capsa is a portable network analyzer application for both LANs and WLANs, which performs real-time packet capturing, 24-7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. Capsa is an intuitive network analyzer, which provides detailed information to help in checking if there are any Trojan activities on a network. It helps network administrators or network engineers pinpoint and resolve application problems.

Features:

- Real-time packet capture, as well as the ability to save data transmitted over local networks, including wired network and wireless network like 802.11a/b/g/n.
- Identifies and analyzes network protocols, as well as network applications based on the protocol analysis.
- Identifies "Top Talkers" by monitoring network bandwidth and usage by capturing data packets transmitted over the network and providing a summary and decoding information about these packets.
- Monitors and saves Internet e-mail and instant messaging traffic, helping identify security and confidential data handling violations.
- Diagnoses and pinpoints network problems by detecting and locating suspicious hosts.
- Maps the traffic, IP address, and MAC of each host on the network, allowing identification of each host and the traffic that passes through.

Some of the additional network activity monitoring tools include:

- Wireshark (*https://www.wireshark.org*)
- Nessus (*https://www.tenable.com*)
- NetResident (*http://www.tamos.com*)
- PRTG Network Monitor (*https://kb.paessler.com*)
- GFI LanGuard (*https://www.gfi.com*)
- NetFort LANGuardian (*https://www.netfort.com*)
- CapMon (*https://www.capmon.dk*)
- Nagios XI (*https://www.nagios.com*)
- Total Network Monitor (*https://www.softinventive.com*)



DNS Monitoring/ Resolution

Malicious software called DNSChanger is capable of changing the system's DNS server settings and provides the attackers with control of the DNS server used on the victim's system. Using this control, the attackers can control the sites the user tries to connect to the Internet and make the victim connect to a fraudulent website or interfere with their online web browsing.

Therefore, you should identify if the malware is capable of changing any DNS server settings while performing dynamic analysis. You can use tools such as DNSQuerySniffer, DNSstuff, etc. to verify the DNS servers' that the malware tries to connect to and identify the type of connection.

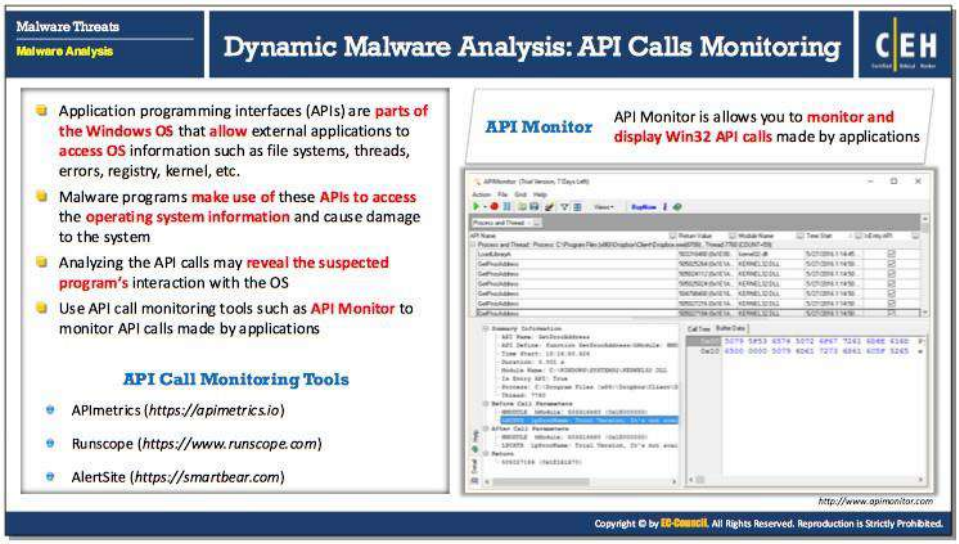
- **DNSQuerySniffer**

  Source: *http://www.nirsoft.net*

  DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and so on), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS queries information to CSV/tab-delimited/XML/HTML file, or copy the DNS queries to the clipboard, and then paste them into Excel or other spreadsheet application.

Some of the additional DNS monitoring/resolution tools include:

- DNSstuff (*http://www.dnsstuff.com*)
- DNS Lookup Tool (*https://www.ultratools.com*)
- Sonar (*https://constellix.com*)



API Calls Monitoring

Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access OS information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the internet, etc. Malware programs also make use of these APIs to access the OS information and cause damage to the system.

You need to gather the APIs related to the malware programs and analyze them to reveal its interaction with the OS as well as the activities it has been performing over the system. Use API call monitoring tools such as API Monitor to monitor API calls made by applications.

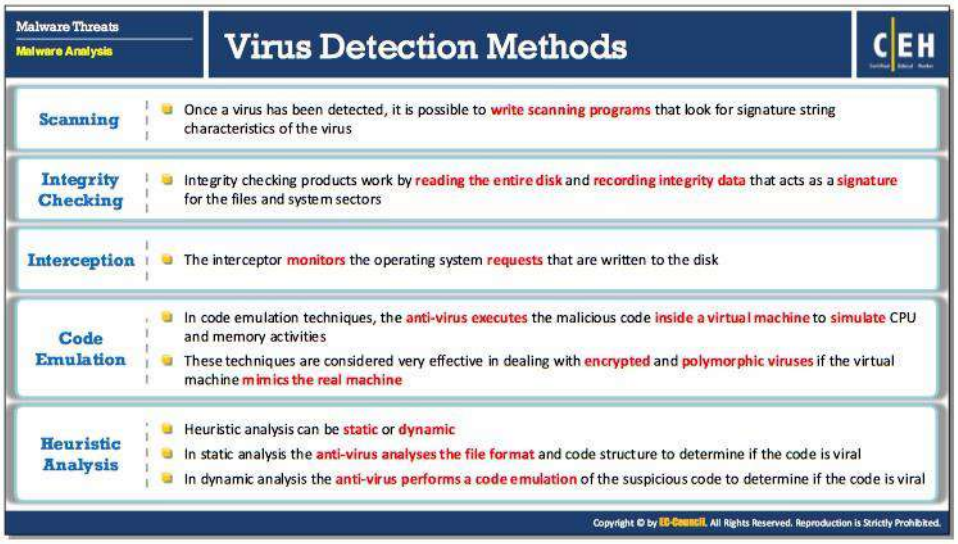
- **API Monitor**

  Source: *http://www.apimonitor.com*

  API Monitor is a software that allows you to monitor and display Win32 API calls made by applications. It can trace any exported APIs and displays a wide range of information, including function name, call sequence, input and output parameters, function return value and more. It is a useful developer tool for seeing how win32 applications work and learn their tricks.

Some of the additional API monitoring tools include:

- APImetrics (*https://apimetrics.io*)
- Runscope (*https://www.runscope.com*)
- AlertSite (*https://smartbear.com*)



Virus Detection Methods

The rule of thumb for virus and worm detection is that if an email looks suspicious (i.e., if the user is not expecting an e-mail from the sender and does not know the sender), or if the email header looks like something that a known sender would not usually say, the user must be careful about opening the email. There might be a risk of virus infection.

The **MyDoom** and **W32.Novarg.A@mm** worms infected the systems of many Internet users, mostly through e-mail.

The best methods for virus detection are:

- Scanning
- Integrity checking
- Interception
- Code Emulation
- Heuristic Analysis

Also, a combination of these techniques can be even more effective.

- **Scanning**

  A virus scanner is an essential piece of software for detecting viruses. If there is no scanner, there is a high probability that the system will be hit by and suffer from a virus. Run antivirus continuously and the scan engine and virus signature database regularly. Antivirus software is of no use if it does not know what to look for. Virus detection follows scanning according to the following series of steps:

- The moment a virus is detected in the wild, antivirus vendors across the globe identify the signature strings (characteristics) of the virus.
- The vendors start writing scanning programs that look for the virus's signature strings.
- 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 predefined viruses can be detected.

Some critical aspects of virus scanning are:

Virus writers often create many new viruses by altering existing ones. It may only take a short time to create a virus that looks new but is just a modification of an existing virus. Attackers make these changes frequently to throw off the scanners.

In addition, to enhance signature recognition, new scanners make use of 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.

Some scanners set up a virtual computer in a machine's RAM and test the programs by executing them in this virtual space. This technique, called heuristic scanning, can also check and remove messages that might contain a computer virus or other unwanted content.

Advantages of scanners

- They can check programs before the execution.
- They are the easiest way to check new software for any known or malicious viruses.

Drawbacks to scanners

- 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 in the market.
- Because viruses appear more rapidly than do new scanners to battle them, even new scanners are not equipped to handle every new challenge.

- **Integrity Checking**
  - Integrity checking products perform their functions by reading and recording integrated data to develop a signature or baseline for those files and system sectors.
  - A disadvantage of a basic integrity checker is that it cannot differentiate file corruption caused by a bug from corruption caused by a virus.
  - There are some advanced integrity checkers available that are capable of analyzing and identifying the types of changes that viruses make.
  - Some integrity checkers combine antivirus techniques with integrity checking to create a hybrid. This simplifies the virus checking process.

- **Interception**
  - The primary use of an interceptor is for deflecting logic bombs and Trojans.
  - The interceptor controls request to the OS for network access or actions that cause a threat to the program. If it finds such a request, the interceptor pops up and asks if the user wants to allow the request to continue.
  - There are no reliable ways to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.
  - Some viruses are capable of disabling the monitoring program itself.
- **Code Emulation**

  Using code emulation, anti-virus software executes a virtual machine to mimic CPU and memory activities. Here virus code is executed on the virtual machine instead of the real processor. Code emulation deals efficiently with the encrypted and polymorphic virus. After running the emulator for a long time, the decrypted virus body eventually presents itself to a scanner for detection. It also detects metamorphic viruses (use single or multiple encryptions). A drawback of code emulation is that it is too slow if the decryption loop is very long.
- **Heuristic Analysis**

  This method helps in detecting new or unknown viruses that are usually variants of an already existing virus family. Heuristic analysis can be static or dynamic. In the static analysis, the anti-virus analyzes the file format and code structure to determine if the code is viral. In the dynamic analysis, the anti-virus performs a code emulation of the suspicious code to determine if the code is viral. The drawback of heuristic analysis is that it is prone to too many false positives (tags benign code as viral); thus, a user might mistrust a positive test result and mistakenly assume a false alarm when it is a real attack.

Malware Threats
Malware Analysis

Trojan Analysis: ZeuS/Zbot

- Zeus, also known as Zbot, is a banking Trojan that specifically attempts to steal confidential information like system information, online credentials, and banking details, etc.
- Detecting ZeuS malware is considered to be difficult due to its stealth techniques

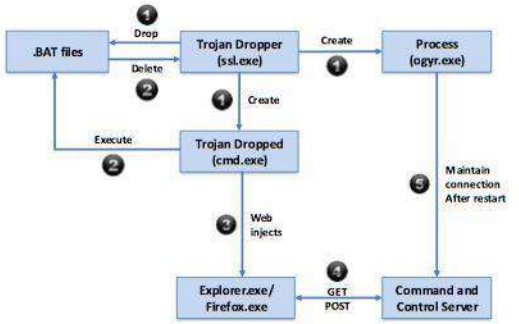
Propagation

- Zeus is spread through drive-by downloads and phishing schemes

Structure

- A ZeuS trojan consists of three .dll files:
  - Kernel32.dll - To access/manipulate memory files and hardware
  - Advapi32.dll - To access/manipulate Service Manager and Registry
  - User32.dll - To display and manipulate graphics

Stages in ZeuS/Zbot Attack



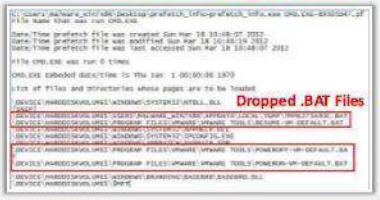
http://sysforensics.org

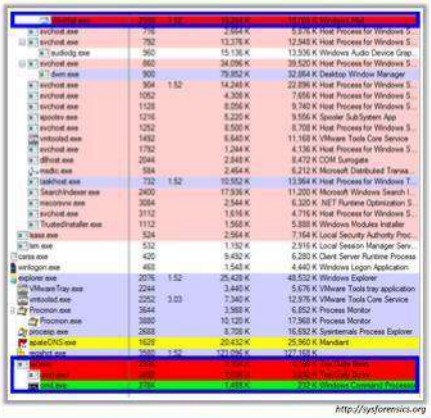
Malware Threats
Malware Analysis

Trojan Analysis: ZeuS/Zbot (Cont'd)

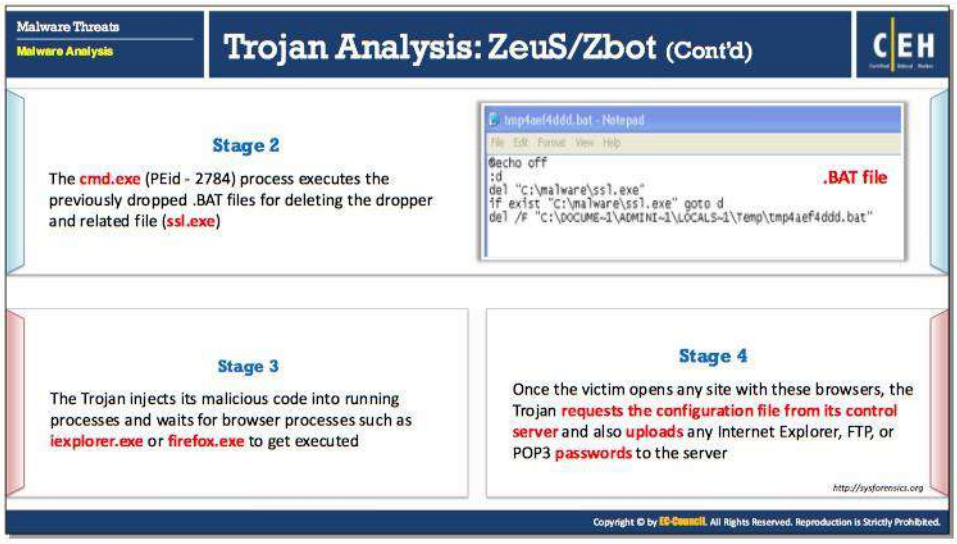
Stage 1

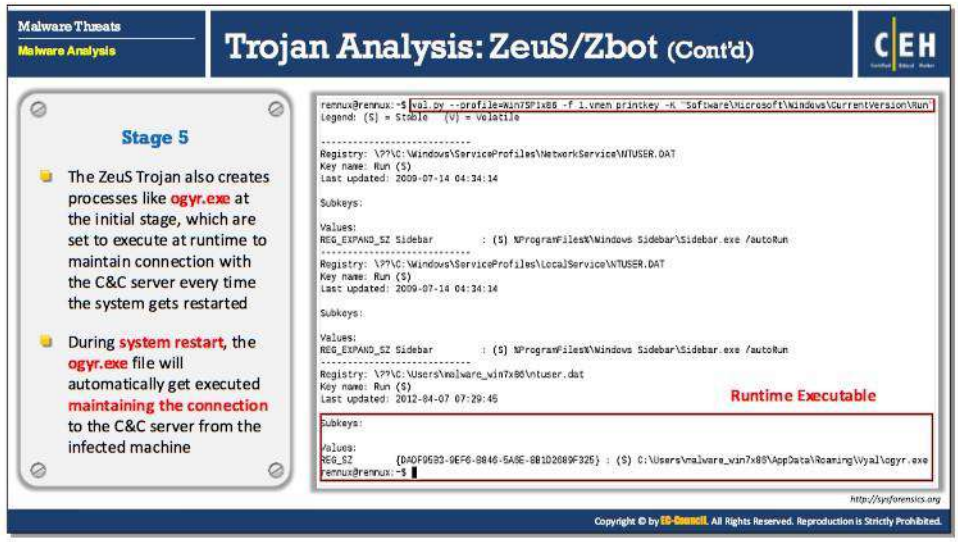
- A ZeuS trojan is packed with UPX and contains executable code in compressed or encrypted form or both
- When a Trojan dropper (ssl.exe) drops the Trojan into a system, it unpacks and creates multiple random-name process objects like uron.exe, WinMail.exe, cmd.exe, etc. You can view information about handles and DLLs processes that have opened or loaded using Microsoft inbuilt tools such as Process Explorer
- Simultaneously, the Trojan dropper drops random-named batch files with .BAT extension in the %APPDATA% and %PROGRAM FILES% folders





http://sysforensics.org





Trojan Analysis: ZeuS/Zbot

Source: *http://sysforensics.org*

ZeuS, also known as Zbot, is a powerful banking trojan that explicitly attempts to steal confidential information like system information, online credentials, and banking details, etc. Zeus is spread mainly through drive-by downloads and phishing schemes. Detecting ZeuS malware is considered to be difficult due to its stealth techniques. This malware creates a

network of infected machines, and all the machines are connected to a Command and Control Server. The owners of the infected machines are not aware of the critical situation since the trojan runs silently in the background of the infected computer.

Some of the attack features of ZeuS Trojan include:

- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows protected storage
- Steals client-side X.509 public key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies
- Modifies the HTML pages of target websites for information stealing purposes
- Redirects victims from target web pages to attacker-controlled ones
- Takes screenshots and scrapes HTML from target sites
- Searches for and uploads files from the infected computer
- Modifies the local host's file (%systemroot%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

Structure:

A ZeuS trojan consists of three main .dll files packed in UPX format, namely Kernel32.dll, Advapi32.dll, and user32.dll. These three .dll files are required by the trojan to perform the following actions:

- **Kernel32.dll** – To access/manipulate memory files and hardware
- **Advapi32.dll** – To access/manipulate Service Manager and Registry
- **User32.dll** – To display and manipulate graphics

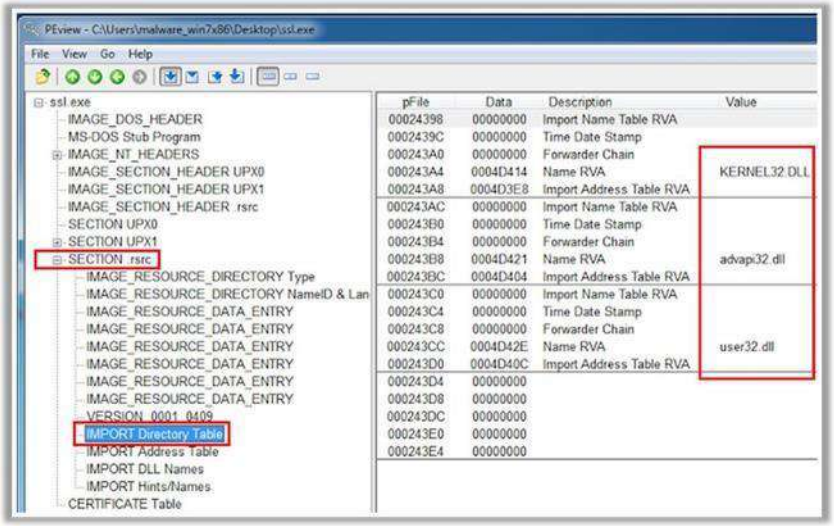


FIGURE 7.9: Screenshot displaying .dll files of Zeus Trojan

Stages in ZeuS Trojan Attack

ZeuS performs stolen data exfiltration and remote commands via encrypted HTTP POST requests to a Command and Control web server. The ZeuS Trojan uses RC4 encryption with a key that is embedded in the binary. ZeuS can re-encrypt itself each time it infects a victim, thus making each infection unique.

There are five stages in the ZeuS infection process:

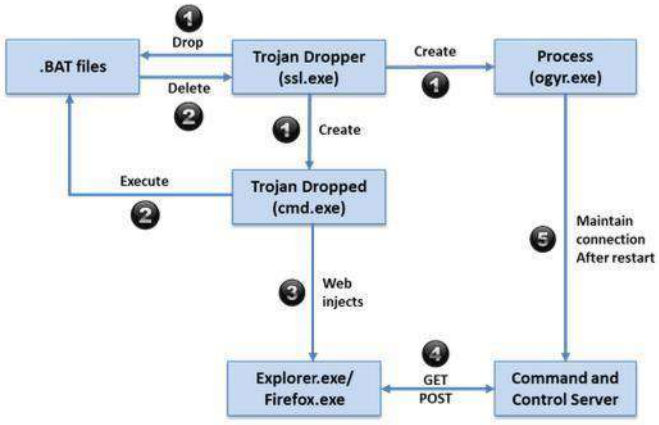


FIGURE 7.10: Screenshot displaying stages of Zeus Trojan attack

- **Stage 1**

  A ZeuS trojan dropper contains executable code in the compressed form, encrypted form, or both. When a trojan dropper (ssl.exe) drops into a system, it unpacks and creates multiple random-name process objects like uron.exe, WinMail.exe, cmd.exe, etc. and also simultaneously drops random-named batch files (with .BAT extension) in the %APPDATA% and %PROGRAM FILES% folders. The names of the processes and the exe files may vary based on time.

  You can view information about handles and DLLs processes that have opened or loaded using Microsoft inbuilt tools such as Process Explorer.

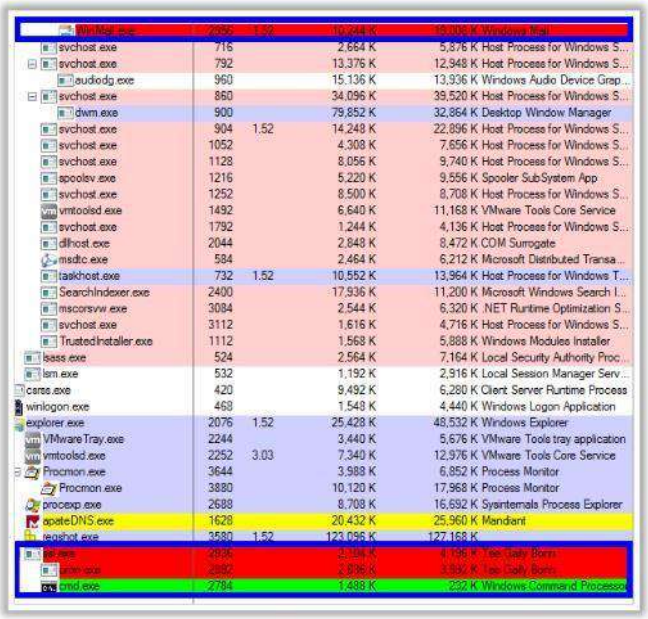


FIGURE 7.11: Screenshot displaying processes in Process Explorer

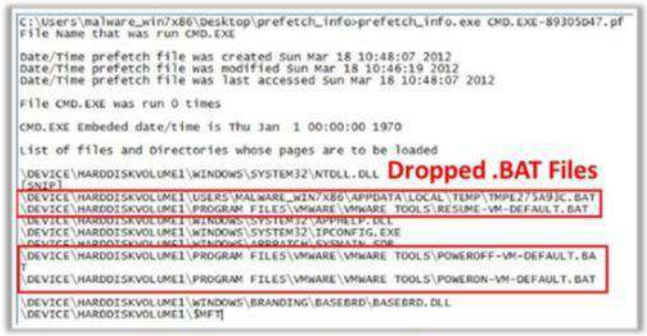


FIGURE 7.12: Screenshot displaying .BAT files location

- **Stage 2**

  In this stage, the dropped trojan **cmd.exe** will execute the previously dropped batch files for deleting the dropper file (**ssl.exe**). The following is the image showing the code in a .BAT file. The content of the .bat files can be grabbed using tools like **OllyDbg**. The .BAT file deletes itself after execution.

FIGURE 7.13: Screenshot displaying ogyr.exe process as Runtime executable

- **Stage 3**

  The **cmd.exe** injects its malicious code into running processes and waits for browser processes such as **iexplorer.exe** or **firefox.exe** to execute.

- **Stage 4**

  Without the user's knowledge, the Trojan requests the C&C Server to download a configuration file in the background. Following is the snapshot showing the requests sent to C&C Server (**http://dns1.nsdnsrv.com**) for downloading **static.htmls** files.

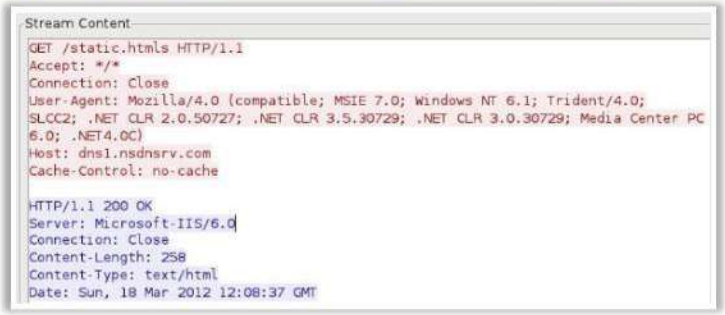


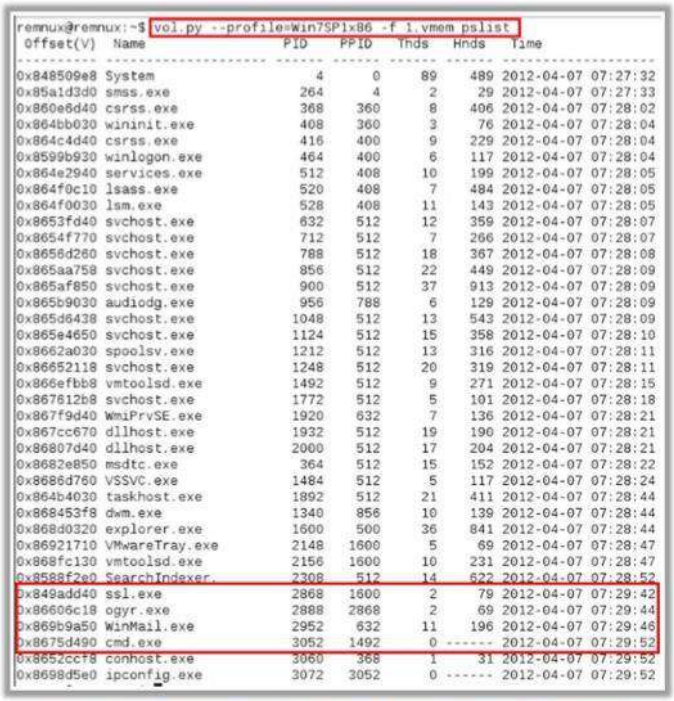
FIGURE 7.14: Screenshot displaying the requests sent to C&C Server for downloading static.htmls files

After establishing a successful connection with the C&C Server, the attacker has full control over the infected machine and can access any Internet Explorer, FTP, or POP3 passwords.

- **Stage 5**

  The ZeuS trojan dropper (**ssl.exe**) also creates processes like **ogyr.exe** at the initial stage, which are set to execute at runtime to maintain a connection with the C&C server every time the system gets restarted.

You can view information about processes that have opened or loaded using tools such as **vol.py**.



```
remnux@remnux:~$ vol.py --profile=Win7SP1x86 -f 1.vmem pslist
 Offset(V)  Name                    PID   PPID   Thds     Hnds   Time
---------- -------------------- ------ ------ ------ -------- -----------------
0x848509e8 System                    4      0     89      489 2012-04-07 07:27:32
0x85a1d3d0 smss.exe                264      4      2       29 2012-04-07 07:27:33
0x860e6d40 csrss.exe               368    360      8      406 2012-04-07 07:28:02
0x864bb030 wininit.exe             408    360      3       76 2012-04-07 07:28:04
0x864c4d40 csrss.exe               416    400      9      229 2012-04-07 07:28:04
0x8599b930 winlogon.exe            464    400      6      117 2012-04-07 07:28:04
0x864e2940 services.exe            512    408     10      199 2012-04-07 07:28:05
0x864f0c10 lsass.exe               520    408      7      484 2012-04-07 07:28:05
0x864f0030 lsm.exe                 528    408     11      143 2012-04-07 07:28:05
0x8653fd40 svchost.exe             632    512     12      359 2012-04-07 07:28:07
0x8654f770 svchost.exe             712    512      7      266 2012-04-07 07:28:07
0x8656d260 svchost.exe             788    512     18      367 2012-04-07 07:28:08
0x865aa758 svchost.exe             856    512     22      449 2012-04-07 07:28:09
0x865af850 svchost.exe             900    512     37      913 2012-04-07 07:28:09
0x865b9030 audiodg.exe             956    788      6      129 2012-04-07 07:28:09
0x865d6438 svchost.exe            1048    512     13      543 2012-04-07 07:28:09
0x865e4650 svchost.exe            1124    512     15      358 2012-04-07 07:28:10
0x8662a030 spoolsv.exe            1212    512     13      316 2012-04-07 07:28:11
0x86652118 svchost.exe            1248    512     20      319 2012-04-07 07:28:11
0x866efbb8 vmtoolsd.exe           1492    512      9      271 2012-04-07 07:28:15
0x867612b8 svchost.exe            1772    512      5      101 2012-04-07 07:28:18
0x867f9d40 WmiPrvSE.exe           1920    632      7      136 2012-04-07 07:28:21
0x867cc670 dllhost.exe            1932    512     19      190 2012-04-07 07:28:21
0x86807d40 dllhost.exe            2000    512     17      204 2012-04-07 07:28:21
0x8682e850 msdtc.exe               364    512     15      152 2012-04-07 07:28:22
0x8686d760 VSSVC.exe              1484    512      5      117 2012-04-07 07:28:24
0x864b4030 taskhost.exe           1892    512     21      411 2012-04-07 07:28:44
0x868453f8 dwm.exe                1340    856     10      139 2012-04-07 07:28:44
0x868d0320 explorer.exe           1600    500     36      841 2012-04-07 07:28:44
0x86921710 VMwareTray.exe         2148   1600      5       69 2012-04-07 07:28:47
0x868fc130 vmtoolsd.exe           2156   1600     10      231 2012-04-07 07:28:47
0x8588f2e0 SearchIndexer.         2308    512     14      622 2012-04-07 07:28:52
0x849add40 ssl.exe                2868   1600      2       79 2012-04-07 07:29:42
0x86606c18 ogyr.exe               2888   2868      2       69 2012-04-07 07:29:44
0x869b9a50 WinMail.exe            2952    632     11      196 2012-04-07 07:29:46
0x8675d490 cmd.exe                3052   1492      0 ------ 2012-04-07 07:29:52
0x8652ccf8 conhost.exe            3060    368      1       31 2012-04-07 07:29:52
0x8698d5e0 ipconfig.exe           3072   3052      0 ------ 2012-04-07 07:29:52
```

FIGURE 7.15: Screenshot displaying ogyr.exe process along with other process

During system restart, the **ogyr.exe** file will automatically get executed maintaining the connection to the C&C server from the infected machine.

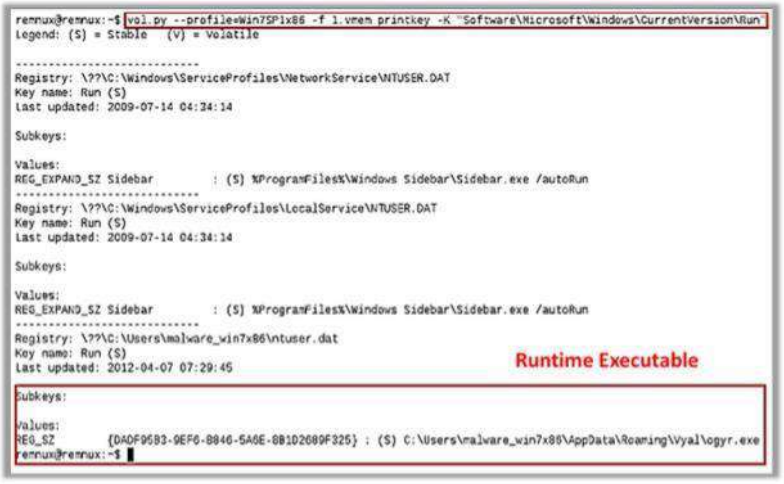


FIGURE 7.16: Screenshot displaying ogyr.exe process as Runtime executable

Malware Threats
Malware Analysis

Virus Analysis: WannaCry

WannaCry	WannaCry is a ransomware that on execution encrypts the files and **locks the user's system**, thereby leaving the system in an unusable state. The compromised user has to **pay ransom in bitcoins to the attacker** to unlock the system and get the files decrypted
Propagation	This ransomware spreads through malicious **email attachments** and also spreads across the same LAN by using a **Windows SMB (Server Message Block) vulnerability** via **port 445** (Microsoft Security Bulletin **MS17-010**)
Encryption	It uses the **RSA AES encryption** algorithm to encrypt content on infected systems
Symptoms	A **Ransomware wallpaper** appears on the screen **demanding ransom in bitcoins** within a **limited time**
Structure	WannaCry ransomware has two key components: • A ransomware package called **ETERNALBLUE** to perform the **SMB exploitation** • A backdoor called **DOUBLEPULSAR** to perform **remote code execution** and further propagation

Malware Threats
Malware Analysis

Virus Analysis: WannaCry (Cont'd)

The malware enters a system through an email attachment or through internal LAN. **Diskpart.exe** is the **dropped EXE** file by the malware

Dropped EXE file details

File Name	File Type	Architecture	File Size
File MD5 Hash	File MD5 Import Hash		Compile Time
Diskpart.exe	PE.EXE	X86	3,514,368
84c82835a5d21bbcf75a61706d8ab549	68f013d7437aa653a8a98a05807afeb1		2010-11-20 09:05:05

Stage 1

- Once the malware is executed on the system, the malware searches for **Mutex** in memory
- Mutex is created when a system is attacked by WannaCry ransomware and the **diskpart.exe** file will not be executed on a system that already contains this Mutex
- Existence of this Mutex in memory can suggest that a system is already infected with WannaCry

Mutex

Mutant	\Sessions\1\BaseNamedObjects\MsWinZonesCacheCounterMutexA
Mutant	\BaseNamedObjects\MsWinZonesCacheCounterMutexA0

https://deceive.trapx.com

Malware Threats
Malware Analysis

Virus Analysis: WannaCry (Cont'd)

Stage 2

Once this executable file is executed on the system it attempts to gather information about the infected system, such as the **hostname**

System Hostname

```
Stack[00000318]:0012F657 db   0
Stack[00000318]:0012F658 db  57h ; W
Stack[00000318]:0012F659 db   0
Stack[00000318]:0012F65A db  49h ; I
Stack[00000318]:0012F65B db   0
Stack[00000318]:0012F65C db  4Eh ; N
Stack[00000318]:0012F65D db   0
Stack[00000318]:0012F65E db  2Dh ; -
Stack[00000318]:0012F65F db   0
Stack[00000318]:0012F660 db  41h ; A
Stack[00000318]:0012F661 db   0
Stack[00000318]:0012F662 db  33h ; 3
```

Stage 3

Once the hostname information has been recorded, this file then proceeds to set the following registry key value on the affected system:

[HKEY_CURRENT_USER\Software\WanaCrypt0r]
"wd"="C:\\Users\\<username>\\Desktop"

Tools like **Microsoft Sysinternal Process Explorer** can be used to capture the process instances

Registry Key Creation

Time ...	Process Name	PID	Operation	Path
10:25:...	diskpart.exe	3612	RegCreateKey	HKLM\Software\WanaCrypt0r
10:26:...	diskpart.exe	3612	RegSetValue	HKLM\SOFTWARE\WanaCrypt0r\wd
10:27:...	diskpart.exe	3612	RegCloseKey	HKLM\SOFTWARE\WanaCrypt0r

https://deceive.trapx.com

Malware Threats
Malware Analysis

Virus Analysis: WannaCry (Cont'd)

Stage 4

- Next, the PE file proceeds to extract additional password protected malware component files stored inside its resource section. The PE file uses a hardcoded password (value ***WNcry@2ol7***) to extract these component files
- An **XOR** operation process is used to decode the loaded resource section. When this process is completed, the files are extracted one-by-one via a loop

Extracted files into the affected system

Filename	MD5 Hash
(00000000.eky)	7c423aa8025bc05ed3e326cd6d29e04
(00000000.pky)	81d0a1e7fb92114bb1882bbb7b073164
(@Please_Read_Me@.txt)	f97d2e6f9d820dbd3b66f21137de4f09
(b.wnry)	c5bbb7b89196ad97b7581242ae03ead5
(b.wnry.bmp)	c5bbb7b89196ad97b7581242ae03ead5
(c.wnry)	383a85eab4ecda313bfddd82416fc6c2
(f.wnry)	2939a6adf172e5dc0aaa9ba36e6f26a4
(m_bulgarian.wnry)	95673b0f968c0f55b32204361940d184
(m_chinese (simplified).wnry)	0252d45ca21c6e43c9742285c44e91a4
(m_chinese (traditional).wnry)	2efc3690d67cd073a9406a2585f7cea
(m_croatian.wnry)	171940037a70ce477326ce2f6deeb270
(m_czech.wnry)	537efeecdfa94cc421e55fd82a58ba9e
(m_danish.wnry)	2e5a3b81d5c4715b7bea01033367fcb3

PE file password

```
4010FD          ; Call Procedure
+6F4h+Str], offset Str ; "WNcry@2ol7"
```

Extracting c.wnry

https://deceive.trapx.com

Malware Threats
Malware Analysis

Virus Analysis: WannaCry (Cont'd)

CEH

Stage 5

Once the files are extracted successfully on the affected system, the PE file proceeds to grab the following hardcoded Bitcoin addresses

- *13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94*
- *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*
- *115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn*

Stage 6

- Next, the PE file extracts the content of c.wnry file
- These extracted strings show at least one bitcoin address, several onion domains likely used for communication by the PE file, and a full URL for downloading a Windows ZIP file for a TOR client

Extracted content from c.wnry

https://deceive.trapx.com

Malware Threats
Malware Analysis

Virus Analysis: WannaCry (Cont'd)

CEH

Stage 7

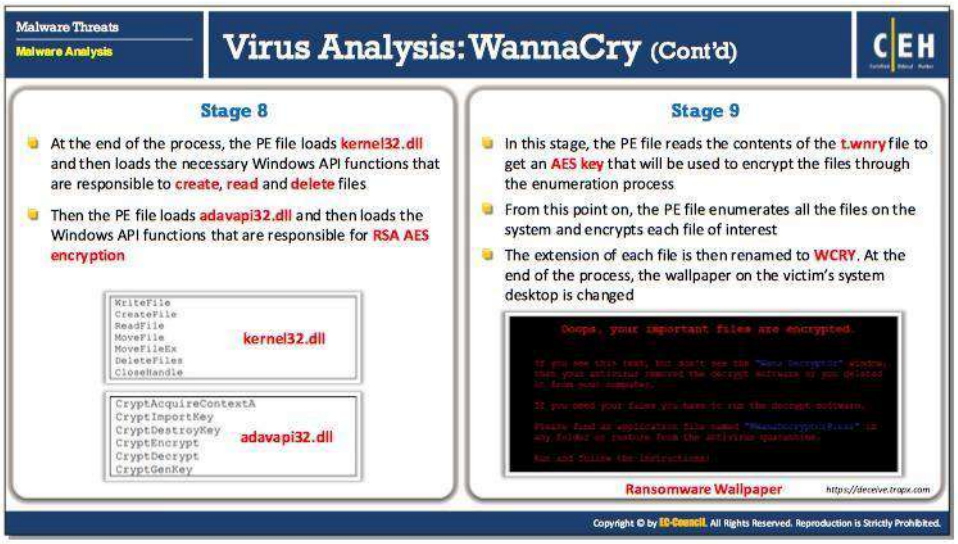
- The next step of the process is to change the attributes and permissions of files in the same folder and any subfolders. To accomplish this the PE file executes a process that runs two hardcoded strings
- The first file changes file attributes to hidden and the icacls command grants global permission for all files
- The PE file runs these two Windows commands to hide itself and all the additional malware components from the user. As a result, the user can no longer see the file in which diskpart.exe was executed, including any dropped files

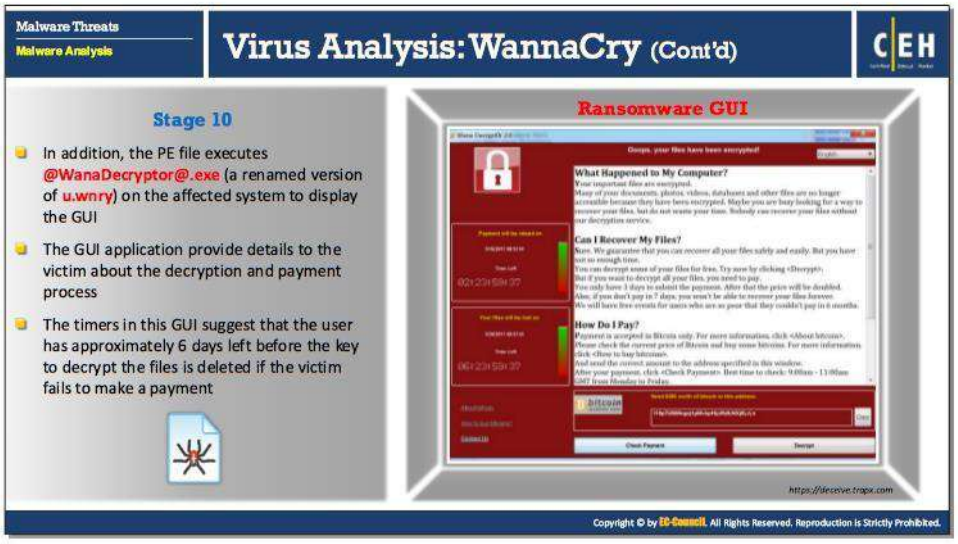
Hardcoded Strings

```
attrib +h .
icacls . /grant Everyone:F /T /C /Q
```

Execute Windows Files

https://deceive.trapx.com





Virus Analysis: WannaCry

Source: *https://deceive.trapx.com*

WannaCry is ransomware that on execution encrypts the files and locks the user's system thereby leaving the system in an unusable state. The compromised user has to pay ransom in bitcoins to the attacker to unlock the system and get the files decrypted. This ransomware spreads through malicious email attachments and also spreads across the same LAN by using a Windows SMB

(Server Message Block) vulnerability via port 445 (Microsoft Security Bulletin MS17-010). WannaCry uses the RSA AES encryption algorithm to encrypt contents on infected systems and change the wallpaper of the system desktop demanding payment in bitcoins.

After infecting a machine, the file extensions that the ransomware is targeting are:

- Commonly used Microsoft Office file extensions (.ppt, .doc, .docx, .xlsx, .sxi, .sxw, .odt, .hwp)
- Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
- Emails and email databases (.eml, .msg, .ost, .pst, .edb)
- Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd)
- Developers' source code and project files (.php, .java, .cpp, .pas, .asm)
- Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes)
- Virtual machine files (.vmx, .vmdk, .vdi)

WannaCry has two key components:

- A ransomware package called **ETERNALBLUE** to perform the **SMB exploitation**
- A backdoor called **DOUBLEPULSAR** to perform remote code execution and further propagation

Stages in WannaCry Ransomware Attack

The malware enters into a system through an email attachment or internal LAN. **Diskpart.exe** is the **dropped EXE** file by the malware.

File Name	File Type	Architecture	File Size
File MD5 Hash	File MD5 Import Hash		Compile Time
Diskpart.exe	PE.EXE	X86	3,514,368
84c82835a5d21bbcf75a61706d8ab549	68f013d7437aa653a8a98a05807afeb1		2010-11-20 09:05:05

FIGURE 7.17: Screenshot displaying Dispart.exe

The following are the stages involved in WannaCry ransomware attack:

- **Stage 1**

  Once the malware is executed on the system, the malware searches for the **Mutex** in memory. The mutex is created when a system is attacked by WannaCry ransomware, and the diskpart.exe file will not be executed on a system that already contains this Mutex. The existence of this Mutex in memory can suggest that a system is already infected with WannaCry.

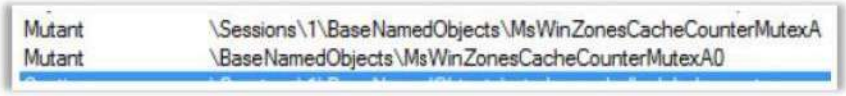


FIGURE 7.18: Screenshot displaying Mutex process

- **Stage 2**

  Once this executable file is executed on the system, it attempts to gather information about the infected system, such as the hostname. The following figure shows an example of the hostname of the system this ransomware was running on.

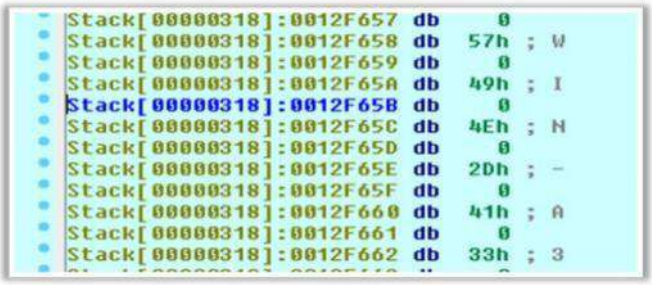


FIGURE 7.19: Screenshot displaying System Hostname

- **Stage 3**

  Once the hostname information has been recorded, this file then proceeds to set the following registry key value on the affected system:

  `[HKEY_CURRENT_USER\Software\WanaCrypt0r]"wd"="C:\\Users\\<username>\\Desktop"`

  Tools like **Microsoft Sysinternal Process Explorer** can be used to capture the process instances.

Time ...	Process Name	PID	Operation	Path
10:25:...	diskpart.exe	3612	RegCreateKey	HKLM\Software\WanaCrypt0r
10:26:...	diskpart.exe	3612	RegSetValue	HKLM\SOFTWARE\WanaCrypt0r\wd
10:27:...	diskpart.exe	3612	RegCloseKey	HKLM\SOFTWARE\WanaCrypt0r

FIGURE 7.20: Screenshot displaying Registry Key Creation

- **Stage 4**

  Next, the PE file proceeds to extract additional password protected malware component files stored in its resource section. The PE file uses a hardcoded password (value **`WNcry@2o17`**) to extract these component files.

FIGURE 7.21: Screenshot displaying hardcoded password

The extraction process is performed inside the subroutine **`sub_401DAB`**, and the PE file calls the **`FindResourceA`** Windows API function whereas the **`lpName 2058`** value is the index value inside the resource section as shown in the following figure.

```
00401DB6 138 push    offset lpType      ; lpType
00401DBB 13C push    2058               ; lpName
00401DC0 140 push    [ebp+hModule]      ; hModule
00401DC3 144 call    ds:FindResourceA ; Indirect Call Near Procedure
00401DC9 138 mov     esi, eax
```

FIGURE 7.22: Screenshot displaying Call to FindResourceA

The following list contains the next Windows API functions that are called by the PE file after the call to the FindResource is completed:

- **FindResourceA**
- **LoadResource**
- **LockResource**
- **SizeofResource**

At the end of the process, this subroutine uses an **XOR** operation process to decode the loaded resource section. When this process is completed, the files are extracted one-by-one via a loop. The following figure shows an example of the process for extracting the file **c.wnry**.

```
00401E0E     loc_401E0E:             ; Logical AND
00401E0E 138 and     [ebp+var_12C], 0
00401E15 138 push    ebx
00401E16 13C push    74
00401E18 140 xor     eax, eax        ; Logical Exclusive OR
00401E1A 140 pop     ecx
00401E1B 13C lea     edi, [ebp+Str1] ; Load Effective Address
00401E21 13C rep stosd               ; Store String
00401E23 13C lea     eax, [ebp+var_12C] ; Load Effective Address
00401E29 13C push    eax
00401E2A 140 push    0FFFFFFFFh
00401E2C 144 push    esi
00401E2D 148 call    sub_4075C4      ; Call Procedure
00401E32 148 mov     ebx, [ebp+var_12C]
00401E38 148 add     esp, 0Ch        ; Add
00401E3B 13C xor     edi, edi        ; Logical Exclusive OR
00401E3D 13C test    ebx, ebx        ; Logical Compare
00401E3F 13C jle     short loc_401E8F ; Jump if Less or Equal (ZF=1 | SF!=OF)

00401E41
00401E41     loc_401E41:             ; Load Effective Address
00401E41 13C lea     eax, [ebp+var_12C]
00401E47 13C push    eax
00401E48 140 push    edi
00401E49 144 push    esi
00401E4A 148 call    sub_4075C4      ; Call Procedure
00401E4F 148 lea     eax, [ebp+Str1] ; Load Effective Address
00401E55 148 push    offset Str2     ; "c.wnry"
00401E5A 14C push    eax             ; Str1
00401E5B 150 call    strcmp          ; Call Procedure
00401E60 150 add     esp, 14h        ; Add
00401E63 13C test    eax, eax        ; Logical Compare
00401E65 13C jnz     short loc_401E79 ; Jump if Not Zero (ZF=0)
```

FIGURE 7.23: Screenshot displaying Extraction of c.wnry

Once this process is completed, the following files (and their relative MD5 hash value) are extracted into the affected system:

Filename	MD5 Hash
(00000000.eky)	7c423aa8025bc05ed3e326cd6d283e04
(00000000.pky)	81d0a1e7fb92114bb1882bbb7b073164
(@Please_Read_Me@.txt)	f97d2e6f8d820dbd3b66f21137de4f09
(b.wnry)	c5bbb7b89196ad97b7581242ae03ead5
(b.wnry.bmp)	c5bbb7b89196ad97b7581242ae03ead5
(c.wnry)	383a85eab6ecda319bfddd82416fc6c2
(f.wnry)	2939adadf172e5dc0aaa9ba38e6f26ad
(m_bulgarian.wnry)	95673b0f968c0f55b32204361940d184
(m_chinese (simplified).wnry)	0252d45ca21c8e43c9742285c48e91ad
(m_chinese (traditional).wnry)	2efc3690d67cd073a9406a25005f7cea
(m_croatian.wnry)	17194003fa70ce477326ce2f6deeb270
(m_czech.wnry)	537efeecdfa94cc421e58fd82a58ba9e
(m_danish.wnry)	2c5a3b81d5c4715b7bea01033367fcb5
(m_dutch.wnry)	7a8d499407c6a647c03c4471a67eaad7
(m_english.wnry)	fe68c2dc0d2419b38f44d83f2fcf232e
(m_filipino.wnry)	08b9e69b57e4c9b966664f8e1c27ab09
(m_finnish.wnry)	35c2f97eea8819b1caebd23fee732d8f
(m_french.wnry)	4e57113a6bf6b88fdd32782a4a381274
(m_german.wnry)	3d59bbb5553fe03a89f817819540f469
(m_greek.wnry)	fb4e8718fea95bb7479727fde80cb424
(m_indonesian.wnry)	3788f91c694dfc48e12417ce93356b0f
(m_italian.wnry)	30a200f78498990095b36f574b6e8690
(m_japanese.wnry)	b77e1221f7ecd0b5d696cb66cda1609e
(m_korean.wnry)	6735cb43fe44832b061eeb3f5956b099
(m_latvian.wnry)	c33afb4ecc04ee1bcc6975bea49abe40
(m_norwegian.wnry)	ff70cc7c00951084175d12128ce02399
(m_polish.wnry)	e79d7f2833a9c2e2553c7fe04a1b63f4
(m_portuguese.wnry)	fa948f7d8dfb21ceddd6794f2d56b44f
(m_romanian.wnry)	313e0ececd24f4fa1504118a11bc7986
(m_russian.wnry)	452615db2336d60af7e2057481e4cab5
(m_slovak.wnry)	c911aba4ab1da6c28cf86338ab2ab6cc
(m_spanish.wnry)	8d61648d34cba8ae9d1e2a219019add1
(m_swedish.wnry)	c7a19984eb9f37198652eaf2fd1ee25c
(m_turkish.wnry)	531ba6b1a5460fc9446946f91cc8c94b
(m_vietnamese.wnry)	8419be28a0dcec3f55823620922b00fa
(r.wnry)	3e0020fc529b1c2a061016dd2469ba96
(s.wnry)	ad4c9de7c8c40813f200ba1c2fa33083
(t.wnry)	5dcaac857e695a65f5c3ef1441a73a8f
(u.wnry)	7bf2b57f2a205768755c07f238fb32cc

TABLE 6.6: Table displaying extracted files and their MD5 hash values from c.wnry

The following table describes the functionality associated with each file:

Filename	Description
(00000000.eky)	ransomware Encrypted with private key
(00000000.pky)	Public key for encrypting files
(@Please_Read_Me@.txt)	Questions & Answers Text file
(b.wnry)	Desktop Wallpaper
(c.wnry)	TOR configurration file
(m_bulgarian.wnry)	ransomware instructions in differnet language
(m_chinese (simplified).wnry)	ransomware instructions in differnet language
(m_chinese (traditional).wnry)	ransomware instructions in differnet language
(m_croatian.wnry)	ransomware instructions in differnet language
(m_czech.wnry)	ransomware instructions in differnet language
(m_danish.wnry)	ransomware instructions in differnet language
(m_dutch.wnry)	ransomware instructions in differnet language
(m_english.wnry)	ransomware instructions in differnet language
(m_filipino.wnry)	ransomware instructions in differnet language
(m_finnish.wnry)	ransomware instructions in differnet language
(m_french.wnry)	ransomware instructions in differnet language
(m_german.wnry)	ransomware instructions in differnet language
(m_greek.wnry)	ransomware instructions in differnet language
(m_indonesian.wnry)	ransomware instructions in differnet language
(m_italian.wnry)	ransomware instructions in differnet language
(m_japanese.wnry)	ransomware instructions in differnet language
(m_korean.wnry)	ransomware instructions in differnet language
(m_latvian.wnry)	ransomware instructions in differnet language
(m_norwegian.wnry)	ransomware instructions in differnet language
(m_polish.wnry)	ransomware instructions in differnet language
(m_portuguese.wnry)	ransomware instructions in differnet language
(m_romanian.wnry)	ransomware instructions in differnet language
(m_russian.wnry)	ransomware instructions in differnet language
(m_slovak.wnry)	ransomware instructions in differnet language
(m_spanish.wnry)	ransomware instructions in differnet language
(m_swedish.wnry)	ransomware instructions in differnet language
(m_turkish.wnry)	ransomware instructions in differnet language
(m_vietnamese.wnry)	ransomware instructions in differnet language
(r.wnry)	Questions & Answers Text file
(s.wnry)	ZIP file for the TOR client

TABLE 6.7: Table displaying extracted files and their functionality from c.wnry

- **Stage 5**

  Once the files are extracted successfully on the affected system, the PE file proceeds to grab the following hardcoded Bitcoin addresses.

  - **13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**
  - **12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw**
  - **115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn**

  The following figure shows these Bitcoin addresses inside this subroutine:

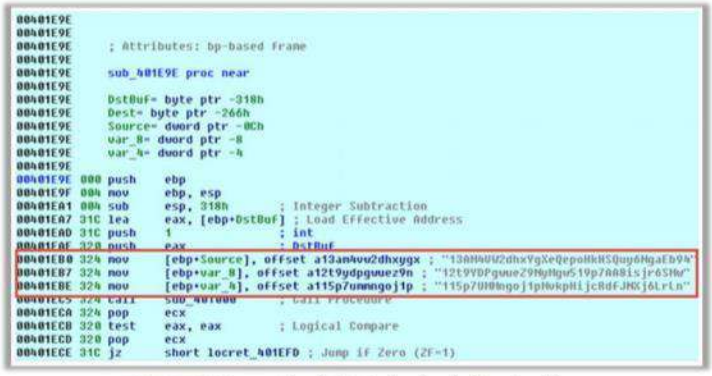


FIGURE 7.24: Screenshot displaying hardcoded bitcoin address

- **Stage 6**

Next, the PE file calls the subroutine **sub_401000**. This subroutine is responsible for reading the content of the file **c.wnry** as shown in the figure.

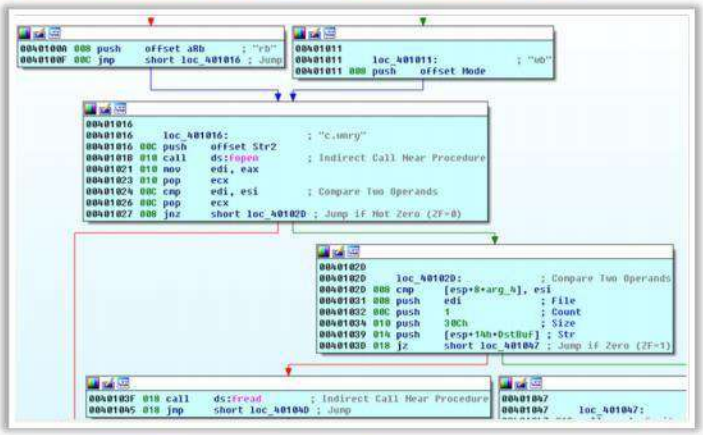


FIGURE 7.25: Screenshot displaying the extraction of c.wnry contents

The following figure contains the strings extracted from the **c.wnry** file.

```
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
gx7ekbenv2riucmf.onion;57g7spgrzlojinas.onion;xxlvbrloxvriy2c5.onion;76jdd2ir2e
mbyv47.onion;cwwnhwhlz52maqm7.onion;
hXXps://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
```

FIGURE 7.26: Screenshot displaying the extracted content of c.wnry file

These strings show at least one bitcoin address, several onion domains likely used for communication by the PE file and a full URL for downloading a Windows ZIP file for a TOR client.

- **Stage 7**

The next step of the process is to change the attributes and permissions of files in the same folder and any subfolders. To accomplish this, the PE file executes a process that runs two hardcoded strings.

```
attrib +h .
icacls . /grant Everyone:F /T /C /Q
```

FIGURE 7.27: Screenshot displaying the Hardcoded Strings

These strings belong to two legitimate Windows binary files. The first file changes file attributes to hidden, and the icacls command grants global permission for all files. Once each string is pushed into the stack, the PE file calls subroutine **sub_401064** for running each one of these files as shown in the figure below.

```
004020DC 704 push    offset CommandLine ; "attrib +h ."
004020E1 708 call    sub_401064         ; Call Procedure
004020E6 708 push    ebx                ; lpExitCode
004020E7 70C push    ebx                ; dwMilliseconds
004020E8 710 push    offset aIcacls_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
004020ED 714 call    sub_401064         ; Call Procedure
004020F2 714 add     esp, 20h           ; Add
004020F5 6F4 call    sub_40170A         ; Call Procedure
004020FA 6F4 test    eax, eax           ; Logical Compare
004020FC 6F4 jz      short loc_402165 ; Jump if Zero (ZF=1)
```

FIGURE 7.28: Screenshot displaying Execution of Windows Files

The PE file runs these two Windows commands to hide and all the additional malware components from the user. As a result, the user can no longer see the file in which diskpart.exe was executed, including any dropped files.

- **Stage 8**

At the end of the process, the PE file calls subroutine **sub_40170A**. This subroutine is responsible for calling **LoadLibrary** to load **kernel32.dll** and then load the following Windows API functions using the **GetProcAddress** Windows API function.

These Windows API functions are responsible for creating, reading and deleting files. Inside this subroutine, the PE file calls another subroutine named **sub_401A45**. This subroutine calls the **LoadLibrary** to load **adavapi32.dll** and then use the same **GetProcAddress** Windows API function to call the following Windows API functions:

FIGURE 7.29: Screenshot displaying kernel32.dll and adavapi32.dll

These Windows API functions, as their name implies, are used by RSA AES encryption. It should be noted that typically some malware variants use the LoadLibrary and GetProcAddress Windows API functions to call other Windows API functions during runtime to avoid exposing these Windows API functions within the import section.

- **Stage 9**

  In this stage, the PE file reads the content of the **t.wnry** file to get an **AES** key that will be used to encrypt the files through the enumeration process. The subroutine responsible for this process is **sub_4014A6**. From this point on, the PE file enumerates all the files on the system and encrypts each file of interest. The extension of each file is then renamed to **WCRY**. At the end of the process, the wallpaper on the victim's system desktop is changed.

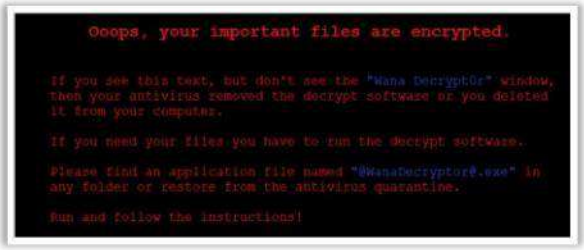


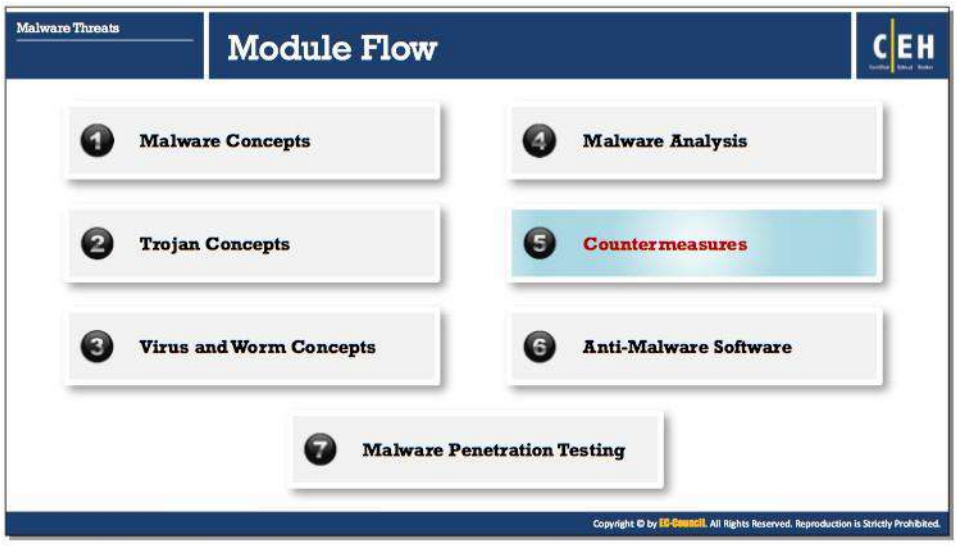
FIGURE 7.30: Screenshot displaying Ransomware Wallpaper

- **Stage 10**

  Also, the PE file executes the GUI file **@WanaDecryptor@.exe** (a renamed version of **u.wnry**) on the affected system as shown in the figure.

FIGURE 7.31: Screenshot displaying Ransomware GUI

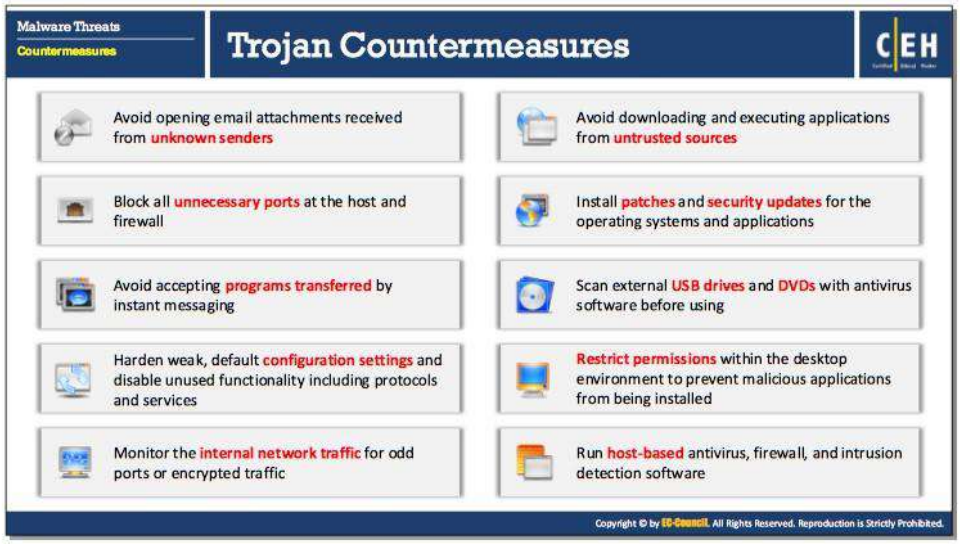
The GUI application provides details to the victim about the decryption and payment process. The timers in this GUI suggest that the user has approximately six days left before the key to decrypt the files is deleted if the victim fails to make a payment.



Countermeasures

Malware is commonly used by an attacker to compromise target systems. Preventing malware from entering into the system is a far better solution than trying to eliminate it from an infected system, which is a far more difficult task.

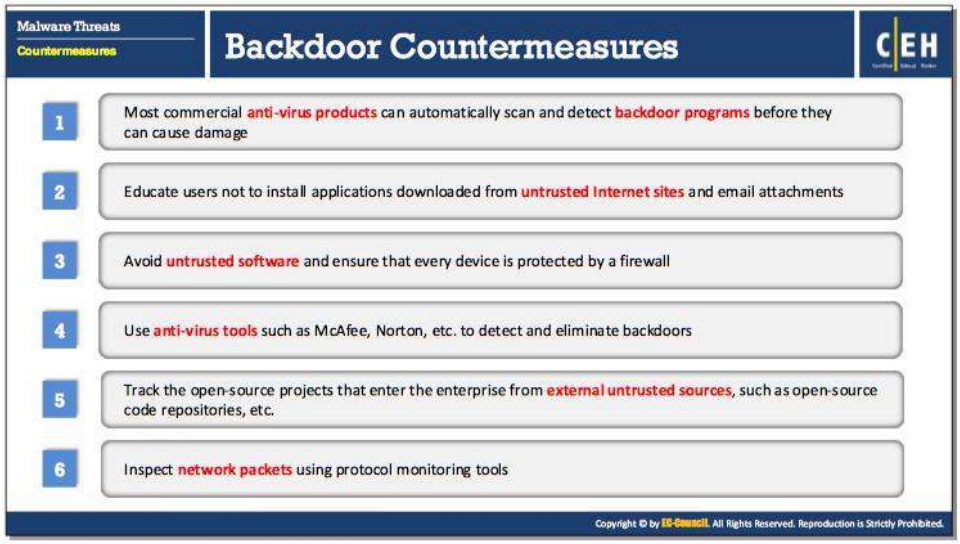
This section deals with various countermeasures that prevent malware from entering a system, and minimizing the risk caused by it upon its entry.



Trojan Countermeasures

The following are some of the Trojan countermeasures

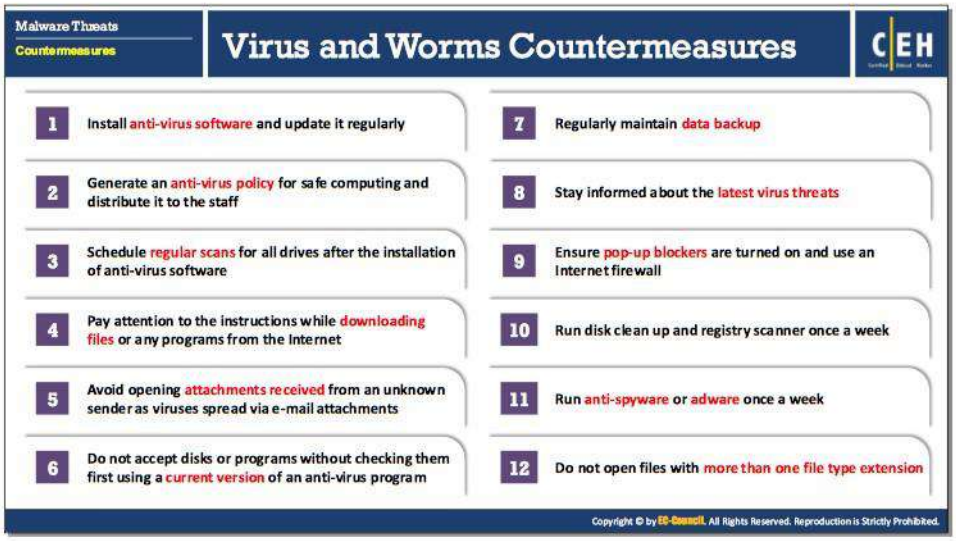
- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and firewall
- Avoid accepting programs transferred by instant messaging
- Harden weak, default configuration settings and disable unused functionality including protocols and services
- Monitor the internal network traffic for odd ports or encrypted traffic
- Avoid downloading and executing applications from untrusted sources
- Install patches and security updates for the OSs and applications
- Scan external USB drives, CDs and DVDs with antivirus software before using
- Restrict permissions within the desktop environment to prevent malicious applications installation
- Avoid typing the commands blindly and implementing pre-fabricated programs or scripts
- Manage local workstation file integrity through checksums, auditing, and port scanning
- Run host-based antivirus, firewall, and intrusion detection software



Backdoor Countermeasures

The following are some common backdoor countermeasures

- Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage
- Educate users not to install applications downloaded from untrusted Internet sites and email attachments
- Avoid untrusted software and ensure that a firewall protects every device
- Use anti-virus tools such as McAfee, Norton, etc. to detect and eliminate backdoors
- Track the open-source projects that enter the enterprise from untrusted external sources, such as open-source code repositories, etc.
- Inspect network packets using protocol monitoring tools
- If a computer is found to be infected by backdoors, restart the infected computer into safe mode with networking
- Run registry monitoring tools to find malicious registry entries added by the backdoor
- Remove or uninstall the program or application installed by the backdoor Trojan or virus
- Remove the malicious registry entries added by the backdoor Trojan
- Delete malicious files related to the backdoor Trojan

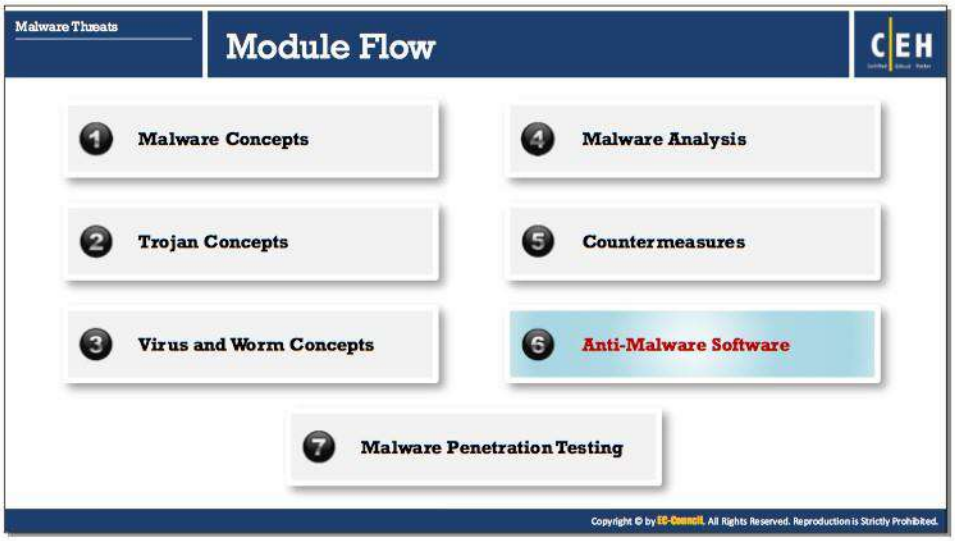


Virus and Worms Countermeasures

The following are some virus and worm countermeasures:

- Install anti-virus software that detects and removes infections as they appear
- Generate an anti-virus policy for safe computing and distribute it to the staff
- Pay attention to the instructions while downloading files or any programs from the Internet
- Update anti-virus software regularly
- Avoid opening attachments received from an unknown sender as viruses spread via e-mail attachments
- Since virus infections can corrupt data, ensure you are performing regular data backups
- Schedule regular scans for all drives after the installation of anti-virus software
- Do not accept disks or programs without checking them first using a current version of an anti-virus program
- Ensure that any executable code used within the organization has been approved
- Do not boot the machine with infected bootable system disk
- Stay informed about the latest virus threats
- Check DVDs and CDs for virus infection
- Ensure pop-up blockers are turned on and use an Internet firewall
- Run disk clean up and registry scanner once a week

- Run anti-spyware or adware once a week
- Do not open files with more than one file type extension
- Be cautious with files being sent through instant messenger applications



Anti-Malware Software

An attacker utilizes malware to commit online fraud or theft. Thus, the recommendation is to use anti-malware software that can help detect malware, remove it, and repair any damage it might cause. This section lists and describes various anti-malware (anti-Trojan and anti-virus) software programs.

Anti-Trojan Software

Anti-Trojan software is a tool or program, that is designed to identify and prevent malicious trojans, or malware, from infecting computer systems or electronic devices. Anti-trojan tools may employ scanning, strategies, freeware or licensed tools to detect Trojans, rootkits, backdoors and other types of potentially damaging software.

- **Kaspersky Internet Security**

  Source: *https://www.kaspersky.com*

  Kaspersky Internet Security protects against Trojans, viruses, spyware, ransomware, phishing and dangerous websites. It protects devices from various types of intrusions. It securely stores passwords for easy access from PC, Mac, and Mobile. It makes backup copies of photos, music, and files and also encrypts data on PC. It automatically blocks inappropriate content and helps you manage the use of social networks. It adds extra security when you shop or bank online on PC or Mac.

Some of the additional anti-trojan software include:

- McAfee® LiveSafe™ (*https://www.mcafee.com*)
- Symantec Norton Security Premium (*http://www.symantec-norton.com*)
- Bitdefender Internet Security (*https://bitdefender.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Malwarebytes (*https://www.malwarebytes.org*)
- Zemana Antimalware (*https://www.zemana.com*)

- Emsisoft Anti-Malware (*https://www.emsisoft.com*)
- Malicious Software Removal Tool (*https://www.microsoft.com*)
- SUPERAntiSpyware (*http://www.superantispyware.com*)
- Plumbytes Anti-Malware (*https://plumbytes.com*)
- Comodo Cleaning Essential (*https://www.comodo.com*)
- Twister Antivirus (*http://www.filseclab.com*)
- SPYWAREfighter (*http://www.spamfighter.com*)
- STOPzilla AntiMalware (*http://www.stopzilla.com*)
- Anti Malware BOClean (*https://www.comodo.com*)
- Trojan Remover (*https://www.simplysup.com*)
- ZeroSpyware (*http://www.fbmsoftware.com*)

Antivirus Software

It is essential to update the Antivirus program tools to keep an eye on the data passing through a system. Tools may follow specific or generic methods to detect viruses. Generic methods look for a virus like performance, rather than a specific virus. This tool does not specify the virus type but warns the user of a possible virus infection. The generic method can raise false alarms, so this tool does not perform well for detecting precise virus forms. Specific methods look for known virus signatures in the anti-virus database and ask the user to choose the necessary action to be taken, such as repair and delete.

It is a good practice for organizations to install the most recent version of the anti-virus software and update it on a regular basis as the arrival of new viruses in the market and updating anti-virus software by the respective vendors is an ongoing process.

- **Bitdefender Antivirus Plus 2018**

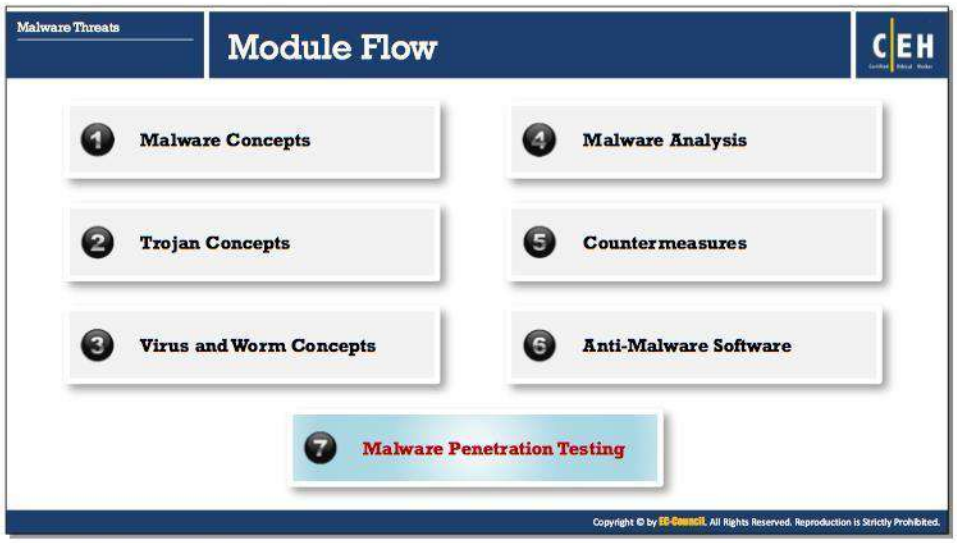
  Source: *https://www.bitdefender.com*

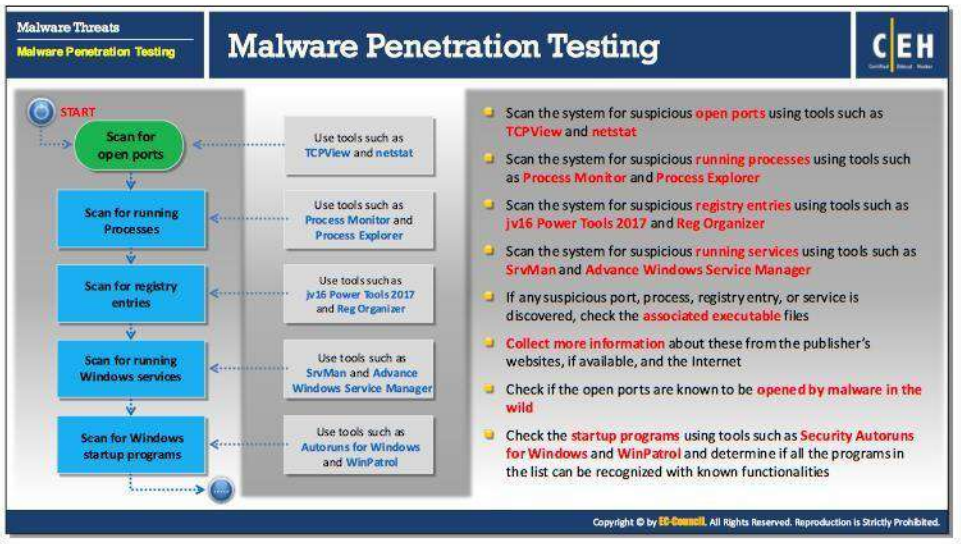
  Bitdefender Antivirus Plus 2018 works against all threats – from viruses, worms, and Trojans, to ransomware, zero-day exploits, rootkits and spyware. It uses a technique called behavioral detection to monitor active apps closely. The moment it detects anything suspicious, it takes instant action to prevent infections. It sniffs and blocks websites that masquerade as trustworthy to steal financial data such as passwords or credit card numbers.

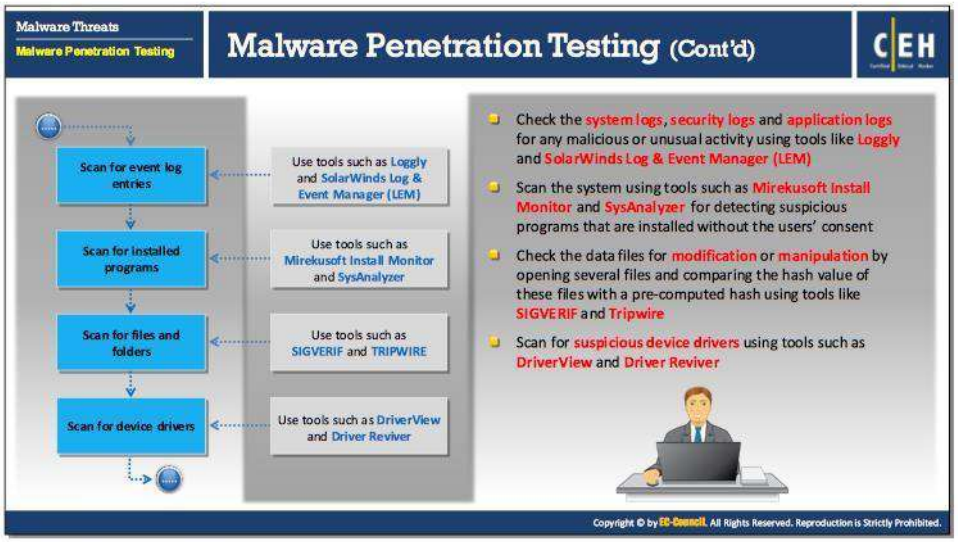
Some of the additional antivirus software is listed below:

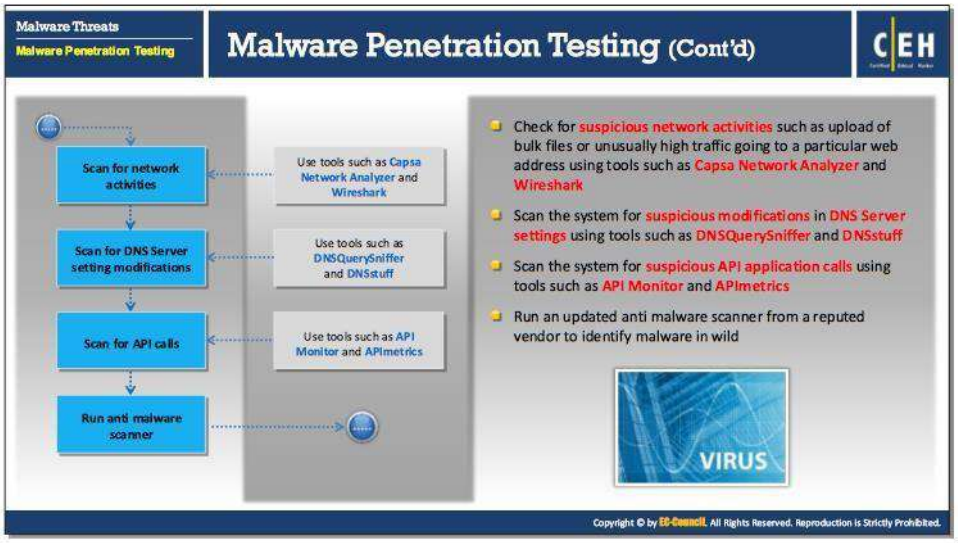
- ClamWin (*http://www.clamwin.com*)
- Kaspersky Anti-Virus (*https://www.kaspersky.com*)

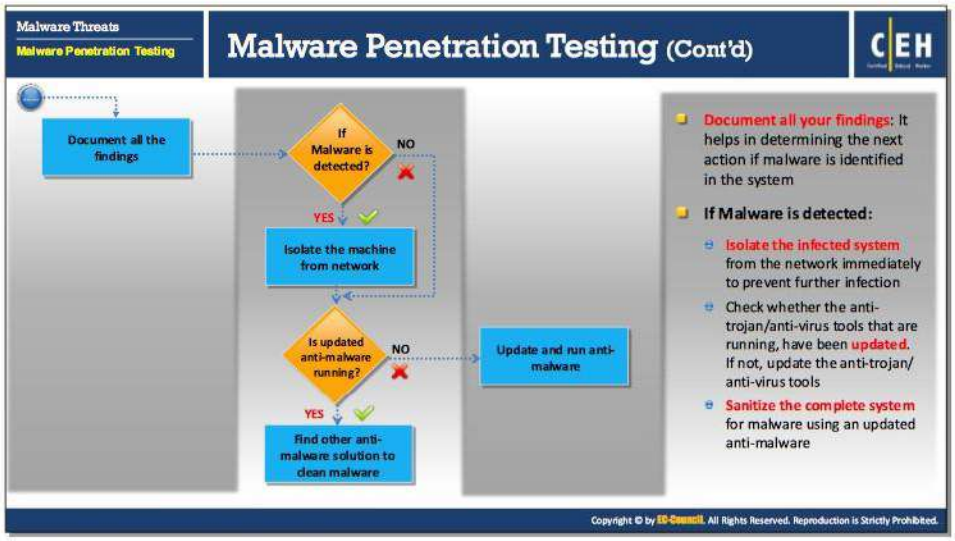
- McAfee AntiVirus Plus (*https://home.mcafee.com*)
- Norton AntiVirus (*https://in.norton.com*)
- Avast Premier Antivirus (*https://www.avast.com*)
- ESET Smart Security (*https://www.eset.com*)
- AVG Antivirus FREE (*https://free.avg.com*)
- Avira Antivirus Pro (*https://www.avira.com*)
- Trend Micro Maximum Security (*http://apac.trendmicro.com*)
- Panda Antivirus Pro (*http://www.pandasecurity.com*)
- Webroot SecureAnywhere Antivirus (*https://www.webroot.com*)
- BullGuard Antivirus (*https://www.bullguard.com*)
- ZoneAlarm® PRO ANTIVIRUS+ 2017 (*https://www.zonealarm.com*)
- F-Secure Anti-Virus (*https://www.f-secure.com*)
- Immunet (*http://www.immunet.com*)
- Total Defense Internet Security Suite (*https://www.totaldefense.com*)
- Spybot (*https://www.safer-networking.org*)





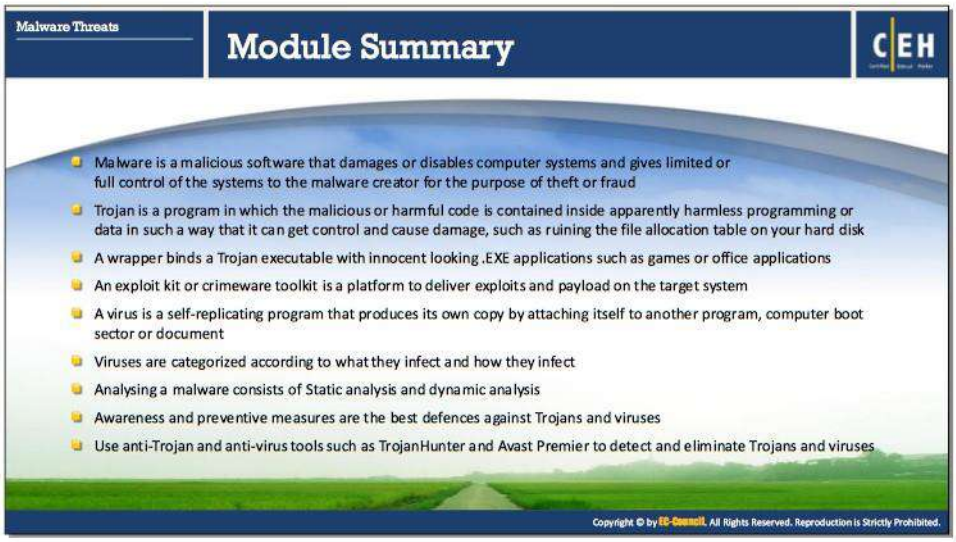






Malware Penetration Testing

Penetration testers should follow the strategies of an attacker to test the network or system efficiently against malware. A penetration tester performs a wide range of available and emerging attack to find loopholes or vulnerabilities in the target organization's IT infrastructure and suggest countermeasures to enhance the security.



Module Summary

This module ends with an overview discussion on malware and their propagation techniques. Further, it provides an overview of Trojans, virus, worms, malware analysis process, techniques to detect malware, malware countermeasures, penetration testing, among others. In the next module, we will see how attackers, as well as ethical hackers and pen testers, use sniffing to collect information about a target of evaluation.