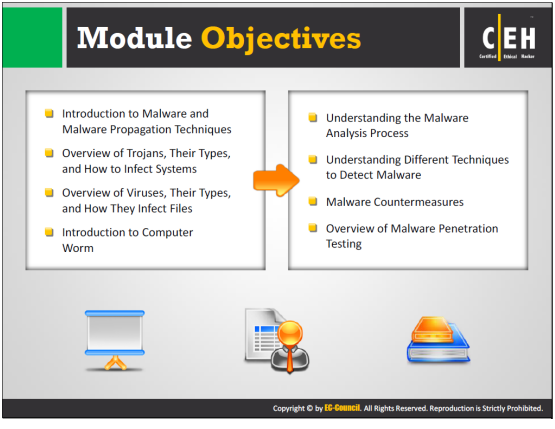
Malware Threats

Module 06

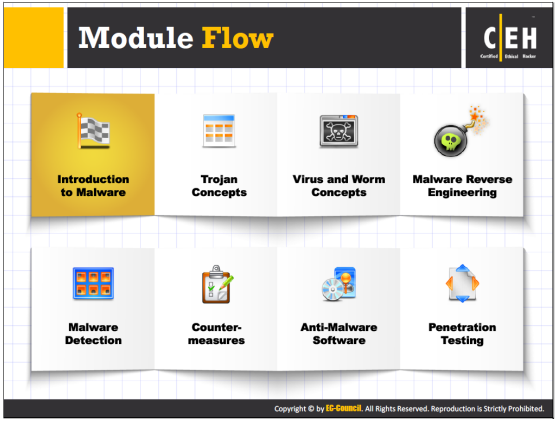
Ethical Hacking and Countermeasures v9

Module 06: Malware Threats

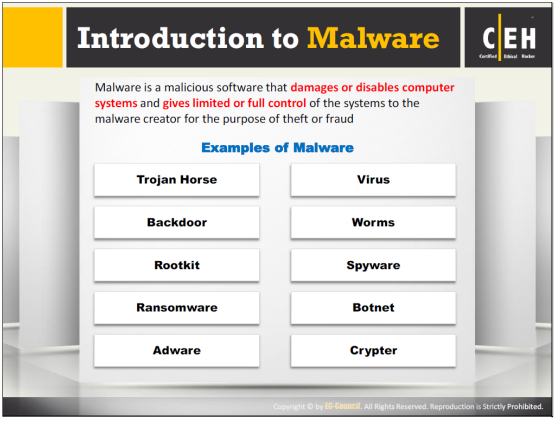
Exam 312-50



The main objective of this module is to provide you with 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.



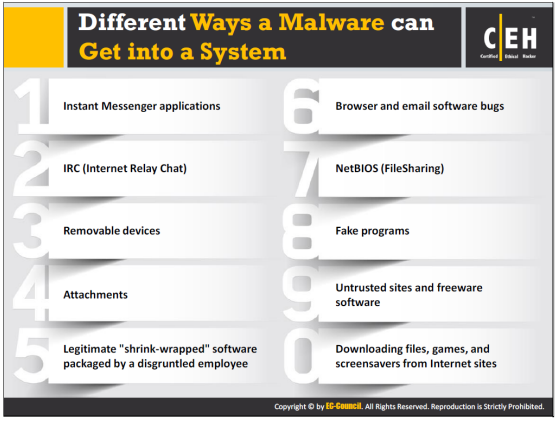
To understand various types of malware and their impact on network and system resources, let us begin with the basic concepts of malware. This section describes malware and highlights the common techniques attackers use to distribute malware on the Web.



Malware is malicious software that damages or disables computer systems and gives limited or full control of the systems to its creator for the purpose of theft or fraud. Malware includes viruses, worms, Trojans, rootkits, spyware, and so on that may delete files, slow down computers, steal personal information, send spam, and commit fraud.

Malware has the ability to 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 important information, resulting in potentially huge data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails



- **Instant Messenger Applications**

  Infection can occur via instant messenger applications such as ICQ or Yahoo Messenger. Users are at high risk while receiving files via instant messengers, no matter from whom or from where. Because there is no file checking utility bundled with instant messengers, 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 example, it could be someone who hacked a messenger ID and password and wants to spread Trojans over a hacked friend's contacts list.

- **IRC (Internet Relay Chat)**

  IRC is another method used for Trojan propagation. **Trojan.exe** can be renamed something like trojan.txt (with 150 spaces).exe. It receives in the DCC (Direct Client to Client) over IRC and appears as **.TXT**. The execution of such files will cause infection. Most people do not notice that an **application (.exe)** file has a text icon. Therefore, before such files are run, even if they have a text icon, it is important to first check their extensions to ascertain that they are really .TXT files.

Removable Devices

- Example: Bob can access Alice's system in her absence and install a Trojan by copying the Trojan software from his disk onto the hard drive
- **Autostart** or Autorun is another way to infect a system while having physical access. Autorun 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 turn off Autostart functionality, follow the instructions given below:

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

Browser and Email Software Bugs

Users do not update their software as often as they should, and many attackers take advantage of this well-known fact. Using an outdated Web browser can pose a risk to the user's computer. A visit to a malicious site 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 browser and e-mail software.

Fake Programs

Attackers can easily lure a victim into downloading free 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 will fail to indicate that the new software is in use. In this situation, an attacker gets e-mail, POP3 account passwords, cached passwords, and keystrokes through email without anyone noticing.
- Attackers thrive on creativity. Consider an example in which an attacker creates a fake Audiogalaxy, 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 simply downloading from other network users. However, the software could act as a backdoor and infect thousands of naive users via ADSL connections.
- 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 site's files with a Trojan. Users who deal with any kind of software or Web application should scan their system on a daily basis. If they detect any new file, it is important 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 taking extra precautions is necessary.

Shrink-wrapped Software

Legitimate "shrink-wrapped" software packaged by a disgruntled employee may contain Trojans.

Attachments

An attachment to e-mails is the medium to transmit the Trojans.

Example: 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 attacker will simply code a program to falsely populate the e-mail "From:" field and send a message with a Trojan attached. The user will check her/his email, see 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.

- **Untrusted Sites and Freeware 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 take the time to scan any files located on these sites before downloading them. Just because a Web site looks professional does not mean that it is safe.
  - Always download Popular software such as mIRC, ICQ, or PGP from its original (or official dedicated mirror) site, and not from third-party sites with links to the (supposedly) same software.

- **NetBIOS (File Sharing)**

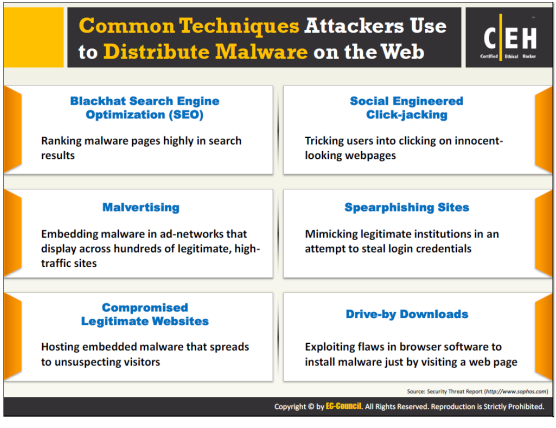
  If port 139 on a system is open (i.e., file sharing is enabled), it can be used by others to access the system, install a Trojan, and modify system files.

  Attackers can also use a DoS attack to shut down the system and force a reboot, so the Trojan can restart itself immediately. To block file sharing in Windows 7,

  Click **Start → Control Panel → Network and Internet → Network and Sharing Center → Change Advanced Sharing Settings → Select a network profile →** Turn off **file and printer sharing**. This will prevent NetBIOS abuse.

- **Downloading**

  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.

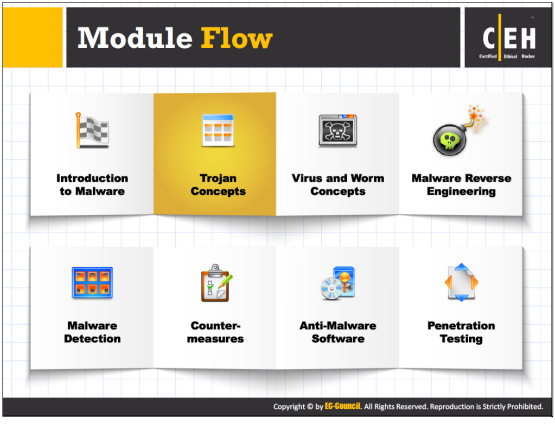


Below are listed some of the common techniques used to distribute malware on the web:

- **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 in an effort to get higher search engine ranking for their malware pages.
- **Social Engineered Click-jacking:** Attackers inject malware into legitimate-looking websites to trick users into 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 Websites:** 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 thereafter carries out malicious activities.

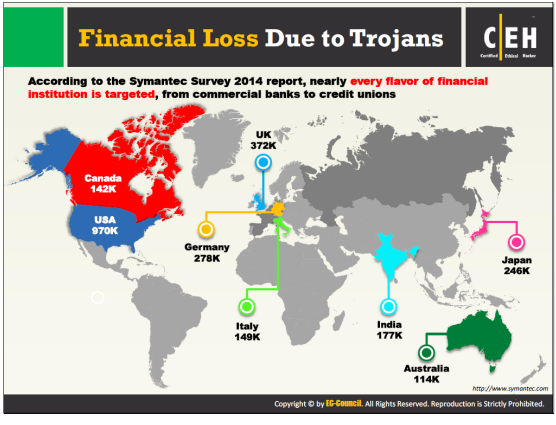
- **Drive-by Downloads:** The unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware just merely by visiting a web site.

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



To understand various Trojans and backdoors and their impact on network and system resources, let us begin with basic concepts of Trojans. 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.



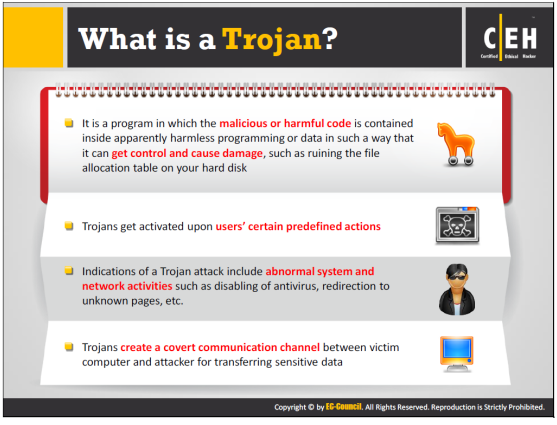
According to the Symantec's threat report, in nearly **95% of** cases of Trojan infection, financial sector institutions were the targets. The remaining 5% accounts for traditional online services like social media, employment websites, auction houses, and webmail.

Key findings of Symantec include:

- About **1,467 financial institutions in 86 countries** were targeted using financial Trojans
- The top nine targeted financial institutions were targeted by more than **40% of all Trojans analyzed**
- Around **95 percent** of the threats focused on the most frequently targeted financial institutions, based in the United States.
- "**Focused attack**" and "**Broader strokes**" were the two dominant attack strategies identified

The United States experienced the most detections of financial Trojans last year, followed by the United Kingdom and Germany. The number of computers compromised by banking Trojans in 2014, by country, is shown in the slide.

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



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 in. The Greeks left it in front of the gates of Troy. The Trojans, who thought it was a gift from the Greeks, which the Greeks had left before apparently withdrawing from the war, 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 "malicious, security-breaking program that is disguised as something benign." Attackers use computer Trojan horses to enter victims' computers undetected, granting attackers unrestricted access to all data stored on them and causing potentially immense damage. Users could download, for example, a file that appears to be a movie, but, when run, 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 does not notify the user.

In addition, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal denial-of-service attacks, such as those that virtually crippled the DALnet IRC network for months. Internet Relay Chat (IRC) is a form of instant text-based communication over the Internet.

Trojan horses work on the same level of privileges that victims have. For example, 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 that level of access, even beyond that of 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 in 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, instant messages.

The following computer malfunctions are symptoms of a Trojan attack:

- The CD-ROM drawer opens and closes automatically. The popular Trojans that exhibit such activities are Netbus and SubSeven.
- The computer screen blinks, flips upside-down, or is inverted, so that everything is displayed backwards.
- The default background or wallpaper settings change automatically. This can be done 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 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.

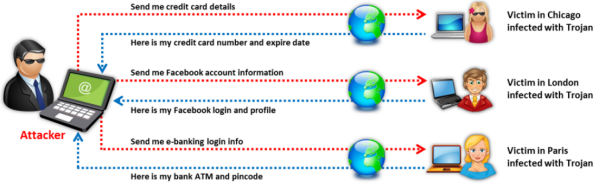


FIGURE 6.1: Screenshot showing how attacker extracts information from the victim system

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.

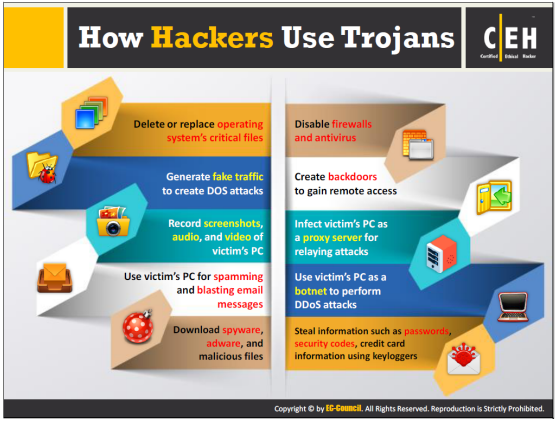
An *overt* channel is a legal channel for the transfer of data or information in a company network and works securely to transfer data and information. On the other hand, a *covert* channel is an illegal, hidden path used to transfer data from a network.

Covert channels are methods attackers can use to hide data in a protocol that is undetectable. They rely on a technique called tunneling, which enables one protocol to transmit over the other. Any process or 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 basic differences between a 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 6.1: Comparison between Overt Channel and Covert Channel



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

- Steal sensitive information, such as:
  - Credit card information, which is useful in domain registration, as well as for shopping
  - Account data such as email passwords, dial-up passwords, and web services passwords
  - Important company projects, including presentations and work-related papers
- Attackers can use the target system:
  - To store archives of illegal materials, such as child pornography. The target continues using their system, having no idea 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

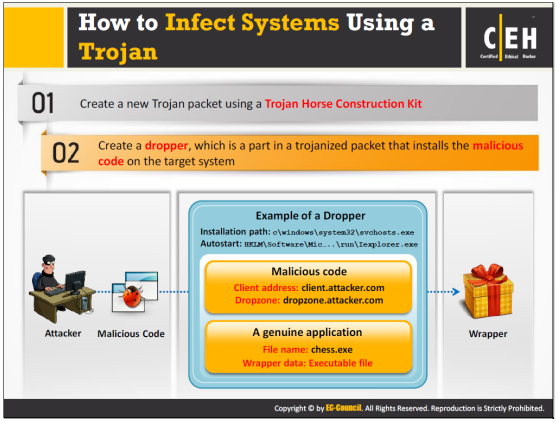
Common Ports used by Trojans

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	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	BackOfrice 2000	31339	NetSpy DK
80	Executor	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			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Ports represent entry and exit points of data traffic. There are two types: hardware ports and software ports. Those within the operating system 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 to have 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.



An attacker can control the hardware as well as software on the system remotely by installing Trojans. Once Trojan installed on the system, not only does the data become vulnerable to threats, chances are that the attacker can perform attacks on the third-party system. Attackers deliver Trojans in many ways to infect target systems:

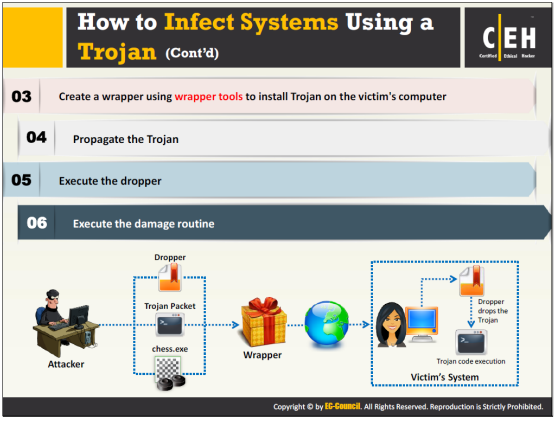
- Trojans are included in bundled shareware or downloadable software. When users download such files, the target systems automatically install the Trojans.
- Different pop-up ads try to trick users. They are programmed by the attacker in such a way that it does not matter whether users click YES or NO; 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 automatically installed.
- 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:

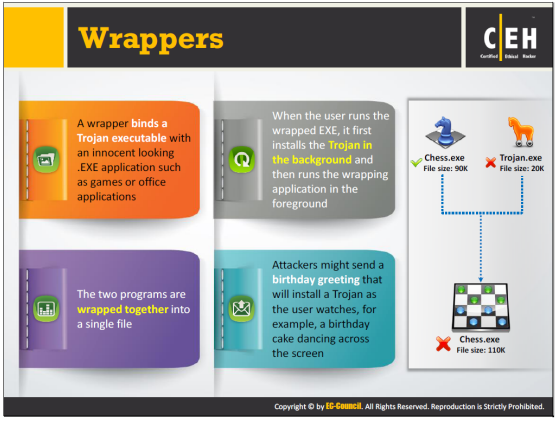
- **Step 1**: Create a **new Trojan packet** using a **Trojan Horse Construction Kit**.

  You can construct new Trojan horses of your choice using various Trojan horse construction Kits such as The Trojan Horse Construction Kit, **The Progenic Mail Trojan Construction Kit (PMT)**, and Pandora's Box. New Trojans have a greater 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, and EliteWrap, to help **bind the Trojan executable** to **legitimate files** in order 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.



Wrappers bind the Trojan executable with a **genuine-looking .EXE application** such as games or office applications. When the user runs the wrapped EXE, 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 executable inside one executable as well. These wrappers may also support functions such as running one file in the background while another one is running 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 game. When the user receives the mail, the description of the game may lead them to install it. Although it may, in fact, be a game, it may also be taking 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 example, 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:

Kriptomatik

Kriptomatik is a wrapper covert program designed to encrypt and protect files against crackers and anti-virus software. It spreads via Bluetooth and allows you to burn CD/DVDs with Autorun.

Features:

- Configure icons
- Gather files
- Posts
- Propagation
- Other features such as autostart, attributes, encryption, etc.

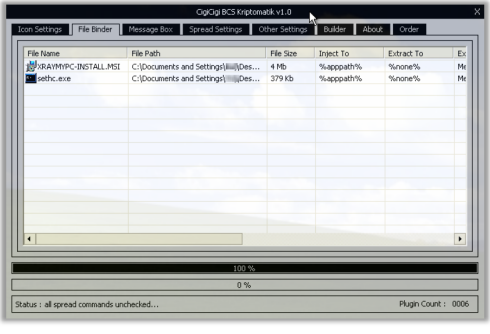


FIGURE 6.2: Screenshot of Kriptomatik wrapper convert program

Advanced File Joiner

Advanced File Joiner is software used to combine and join various files into a single one. If you have downloaded multiple pieces of a large file split into smaller files, you may easily join them together with this tool. For example, you can combine ASCII text files or combine video files such as MPEG files into a single file if and only if they are of the same size, format, and encoding. This tool is not effective to use for joining header file format containing head information such as AVI, BMP, JPEG, and DOC files. Therefore, for each of these types of file formats, you have to use specific software join program.

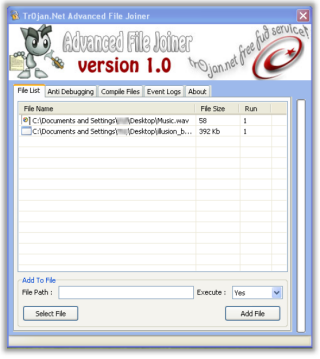


FIGURE 6.3: Screenshot of Advanced File Joiner wrapper

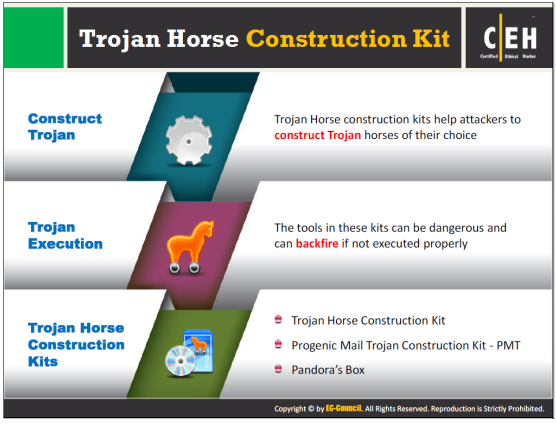
SCB LAB's – Professional Malware Tool

Professional Malware Tool is designed to encrypt (Crypter), join (Binder), download (Downloader), and spread (Spreader) files.

FIGURE 6.4: Screenshot of SCB LAB's – Professional Malware Tool

Dark Horse Trojan Virus Maker creates user-specified Trojans by selecting from various options available. The Trojans created act as per the options selected while creating them. For example, if you choose the option **Disable Process**, the Trojan disables all processes on the target system.

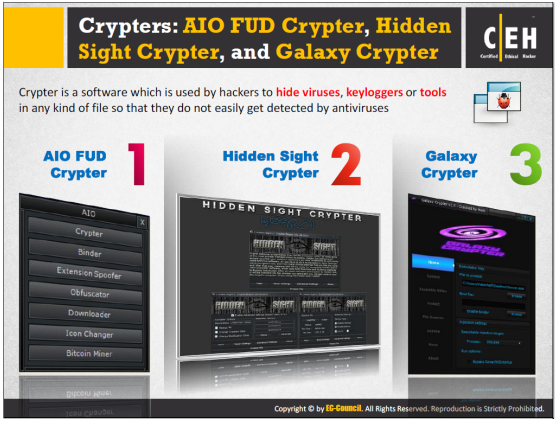
The screenshot shown in the slide is a snapshot of **Dark Horse Trojan Virus Maker** that displays its various available options.



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. Generally, 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.

Below are listed some Trojan horse construction kits:

- **Trojan Horse Construction Kit v2.0** consists of three **EXE files**: Thck-tc.exe, Thck-fp.exe, and Thck-tbc.exe. **Thck.exe** is the actual **Trojan constructor**. With this command-line utility, the attacker can construct a Trojan horse of his or her choice. **Thck-fp.exe** is a **file size manipulator**. With this, the attacker can create files of any length, pad out files to a specific length, or even append a certain number of bytes to a file. **Thck-tbc.exe** will turn any **COM program** into a **Time Bomb**.
- The **Progenic Mail Trojan Construction Kit (PMT)** is a command-line utility that allows an attacker to create an EXE (PM.exe) to be sent to a victim in order to **steal passwords.**
- **Pandora's Box** is a program designed to create **Trojans/time bombs.**



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

AIO FUD Crypter

AIO FUD Crypter can be used to crypt malware such as keyloggers, viruses, and Trojans to bypass anti-virus detection.

Features:

- Crypter
- Binder
- Extension Spoofer
- Obfuscator
- Botnet Bitcoin Miner

Hidden Sight Crypter

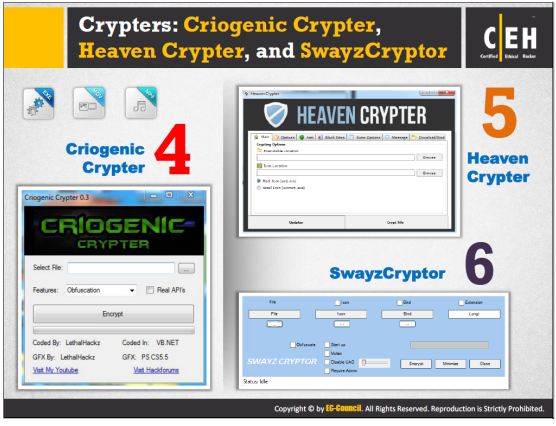
Hidden Sight Crypter crypts files to FUD (fully undetectable), so that most malware-analyzing software, such as McAfee, Norton, AVG, and Avast, fails to detect them.

Features:

- Crypts files fully undetectable
- File binder (.mp3, .pdf, .wmv, JPG, etc.)
- Polymorphic encryption
- Automatic USG (Unique Stub Generator)
- Extension spoofer
- UAC Bypass - Hidden and no popups

Galaxy Crypter

Galaxy Crypter was written in the language C#. It allows attacker to hide malware such as RATs, Keyloggers, HTTP/IRC Bots, Zombies, DDOSers, and Stealers.



Below are listed a few more crypters used to hide malicious files from being detected by an anti-virus program:

Criogenic Crypter

Similar to the ones discussed earlier, Criogenic Crypter can also be used to crypt malicious files such as Trojans, viruses, spyware, etc. to make them undetectable by anti-virus program.

Features:

- Obfuscation
- Real API's selection
- Crypt files
- Supports normal, high, extreme, and max encryption modes

Heaven Crypter

Heaven Crypter also does the same (crypt malicious files to bypass anti-virus detection) as other crypters discussed before.

Features:

- P2P Spreading
- Add any script or source code to Start Up (HK_Current User, HK_Local Machine)

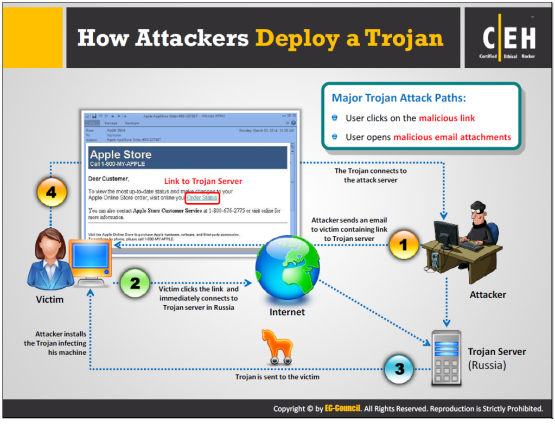
- Custom Process Blacklist
- Assembly code Editor
- Inbuilt Script Compiler
- Hex Code Viewer
- File Binding

SwayzCryptor

SwayzCryptor is a FUD (Fully UnDetectable) Cryptor. It offers various options such as Obfuscate, Start up, Mutex, Disable UAC, and Require Admin. This cryptor displays the status of the cryptor on the bottom left, as shown in the snapshot.

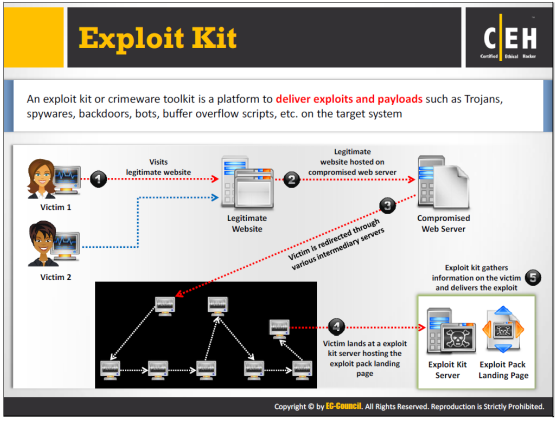
Features:

- Bind other files
- Crypt
- Icon
- Spoof extension, etc.



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 him or her 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 infecting it. As a result, victim 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 action of his/her choosing. If the victim carries out any 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.

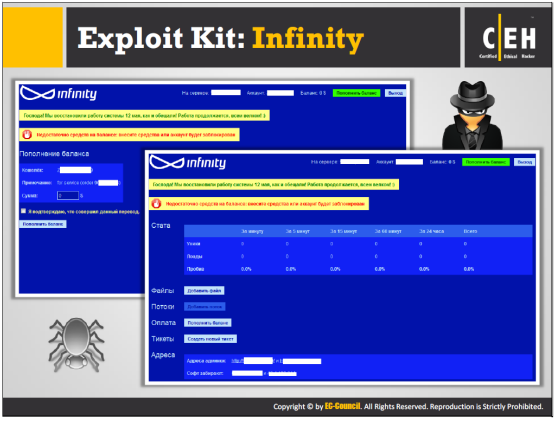
The Trojan may infect the computers when a user clicks on a malicious link or opens an email attachment that installs a Trojan on their computers that might serve as a backdoor for criminals for later access of the system.



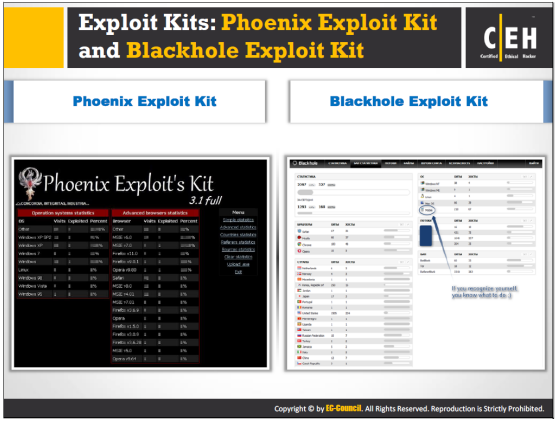
An exploit kit or crimeware toolkit is used to exploit security loopholes found in software applications such as Adobe Reader, Adobe Flash Player, etc. by distributing malware such as spyware, viruses, Trojans, worms, bots, backdoors, buffer overflow scripts, or other payloads to the target system. Exploit kits come with pre-written exploit codes, thus it is easy to use for any user who is not an IT or security expert. They also provide 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 shown in the slide is 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 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 to the victim's system and executed.



The Infinity exploit kit uses vulnerabilities in **Mozilla Firefox**, **Internet Explorer,** and **Opera** to install threats on the victims' computers. The malware analysts also reported that the Infinity Exploit Kit exploits known vulnerabilities in Web browser add-ons and platforms such as Java and Adobe Flash to carry out its attacks. The Infinity Exploit Kit compromises the victims' computers and may be associated with other threats.



Phoenix Exploit Kit

The Phoenix Exploit Kit (PEK) is a configurable set of exploits. Attackers use these exploits on a web server to compromise the security of web browsers that browse to the site. PEK includes different malware including variants of the **PWS:Win32/Zbot** family. There are a number of exploits packaged in PEK, including the following, most of which could allow the execution of arbitrary code:

CVE-2006-5559	ADODB.Connection ActiveX control vulnerability
CVE-2007-0071	—
CVE-2007-5659	Multiple buffer overflows in Adobe Reader and Acrobat via malformed PDF files
CVE-2008-0655	Multiple unspecified vulnerabilities in Adobe Reader and Acrobat versions
CVE-2008-2992	Buffer overflow in Adobe Reader & Acrobat via malformed PDF files
CVE-2008-5353	Vulnerability in Sun Java Runtime Environment versions
CVE-2009-0927	Buffer overflow in Adobe Reader & Acrobat versions
CVE-2009-1869	Vulnerability in Adobe Flash Player
CVE-2009-3867	Stack-based overflow in Sun Java Runtime Environment (JRE) and

	Development Kit (JDK)
CVE-2009-4324	Vulnerability in Adobe Reader and Acrobat via malformed PDF files
CVE-2010-0806	Uninitialized memory corruption vulnerability in Microsoft Internet Explorer

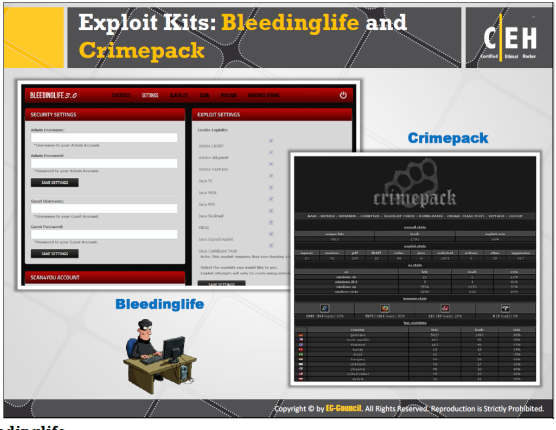
TABLE 6.2: Comparison between Overt Channel and Covert Channel

Blackhole Exploit Kit

The Blackhole exploit kit is another prevalent web threat aiming to deliver a malicious payload to a victim's computer. According to Trend Micro, the majority of infections due to this exploit kit involve a series of high-volume spam runs.

How Blackhole Exploit Kit Works?

- The customer licenses the Blackhole exploit kit from the authors and specifies various options to customize the kit.
- A potential victim loads a compromised web page or opens a malicious link in a spammed email.
- The compromised web page or malicious link in the spammed email sends the user to a Blackhole exploit kit server's landing page.
- This landing page contains obfuscated JavaScript that determines what is on the victim's computer and loads all exploits to which the computer is vulnerable and sometimes a Java applet tag that loads a Java Trojan horse.
- If there is an exploit that is usable, the exploit loads and executes a payload on the victim's computer and informs the Blackhole exploit kit server, which exploit was used to load the payload.



Bleedinglife

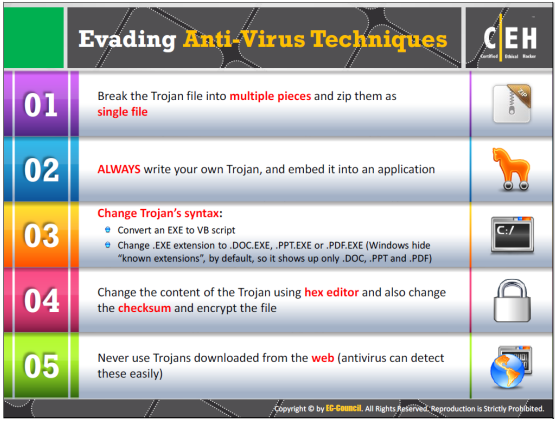
The Bleedinglife exploit kit is a browser exploit kit that allows a remote attacker to compromise a victim's computer by attempting to exploit multiple browser plug-in vulnerabilities. This kit has the feature to exploit vulnerabilities in plug-ins such as Adobe Reader, Oracle, Java, etc. Infection typically occurs when a victim visits a questionable URL that point to the exploit kit or by visiting a compromised website that links to a server hosting the Bleedinglife exploit kit.

Crimepack

Crimepack primarily targets German and South American websites. The kit contains a commercial PHP encoder. It uses PHP and a MySQL backend and has an admin panel that includes a choice of exploits to use and redirection of non-vulnerable traffic. Statistics in this kit shows one table under the MAiN tab and provide such information as overall statistics, exploit statistics, operating system statistics, browser statistics, and referrers and victims' countries. There are several exploits, such as Webstart and vulnerability in Java Runtime Environment, that are particularly associated with the Crimepack Exploit Kit.

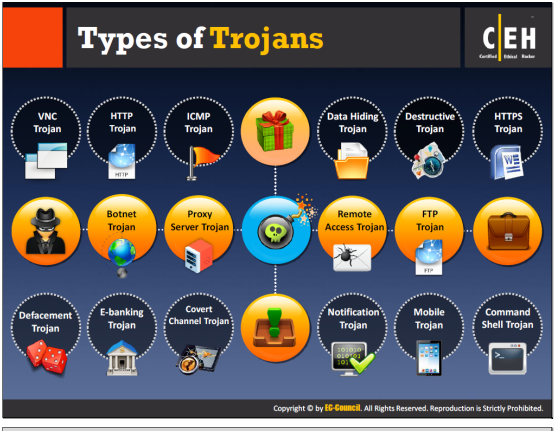
Features:

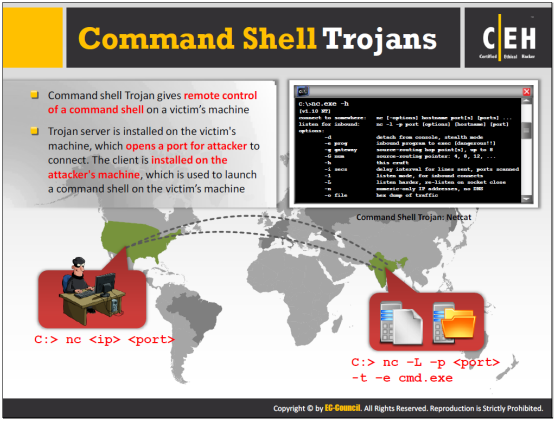
- **iFrame obfuscator** - produces already obfuscated JavaScript code, which can be posted in compromised sites.
- **Blacklist checker** - checks the domain where it is installed against the blacklists of famous security companies.
- **Downloader builder** - takes a URL as an argument and generates a Trojan - Downloader - Rootkit executable.

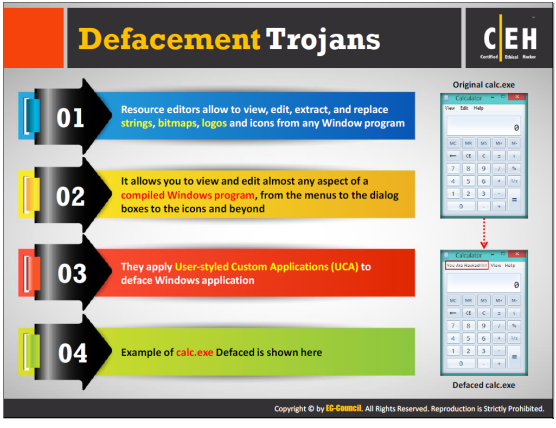


Below are listed various techniques one can use to make malware such as Trojans, viruses, and worms, undetectable by anti-virus applicatons.

1. **Break the Trojan file** into multiple pieces and **zip** them as a single file.
2. Always write your **own 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 hide "known extensions", by default, so it shows up only .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 to change 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.

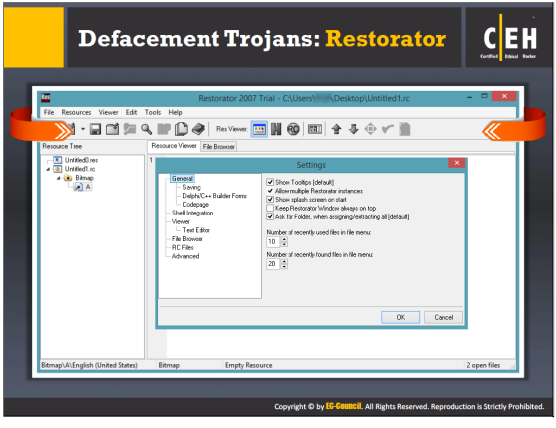






Defacement Trojans, once spread over the system, can destroy or change the entire content present in a database. However, they are more dangerous when attackers target websites, as they physically change their underlying HTML format, resulting in the modification of their content. There is even greater 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.

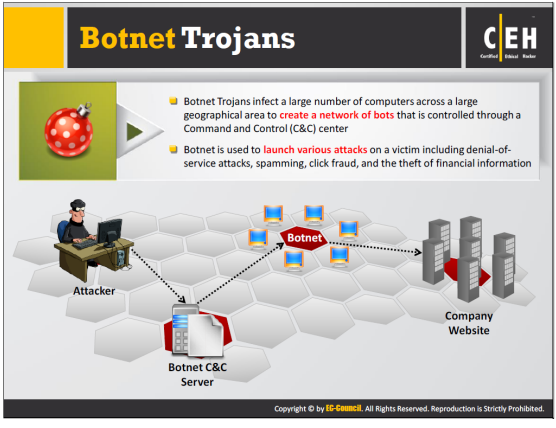


Restorator is a utility for editing Windows resources in applications and their components (e.g., files with .exe, .dll, .res, .rc, and .dcr, extensions). It allows one to change, add, or remove resources such as text, images, icons, sounds, videos, version, dialogs and menus in almost all programs.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

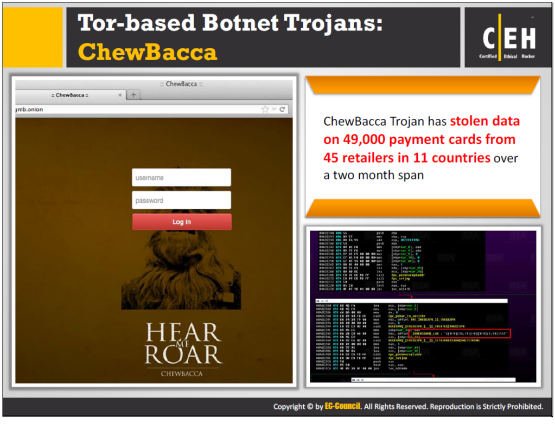
Features:

- 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

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

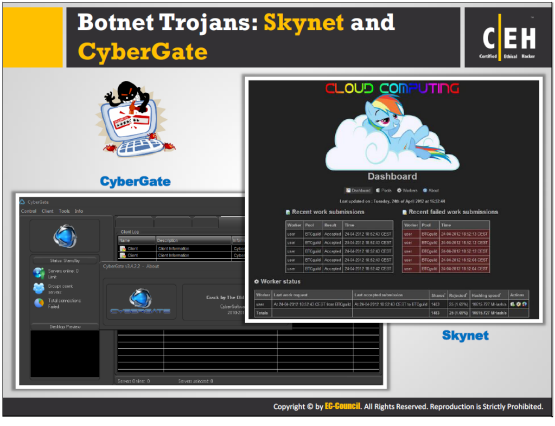


Today, most large information security attacks involve botnets. Attackers (also known as "bot herders") use botnet Trojans to infect a large number of computers throughout a large geographical area to create a network of bots (or a "bot herd") that can control via a Command and Control (C&C) center. They trick normal 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.



ChewBacca is a TOR-based malware program that features two distinct data-stealing mechanisms: a generic keylogger and a memory scanner, designed to specifically target systems that process credit cards, such as Point-of-Sale (POS) systems. The memory scanner dumps a copy of a process's memory and searches it using simple regular expressions for card magnetic stripe data. If it finds a card number, it extracts and logs it using the server.

The TOR network handles the entire communication, concealing the real IP address of the Command and Control (C&C) server(s), encrypting traffic and avoiding network-level detection. The server address uses the pseudo-TLD ".onion" that is not resolvable outside a TOR network and requires a TOR proxy app, which is installed by the bot on the infected machine.

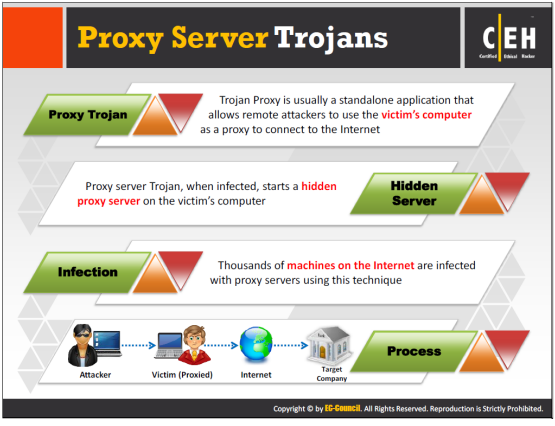


Skynet

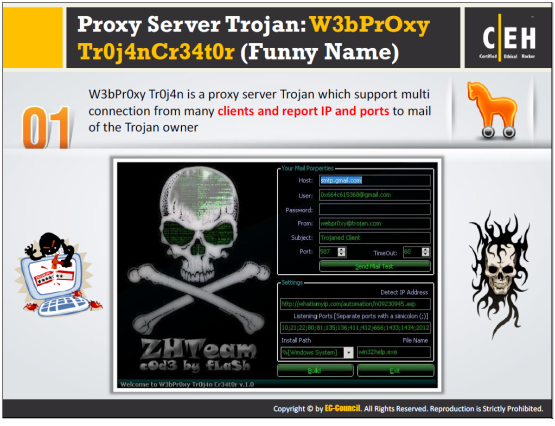
Skynet is a botnet that includes all of the capabilities of Zeus banking Trojan along with other functions, such as Tor-based C&C server anonymity and a Bitcoin mining component. It is a sophisticated Trojan that does not display symptoms while conducting attacks against bank accounts and other sensitive targets. Skynet's main threat lies in its ability to compromise bank accounts. Like Zeus, Skynet is capable of performing Man-in-the-Browser attacks, including stealing confidential bank account data and even making requests for additional information (by disguising the requests as notifications from the bank's website). It is capable of launching DDoS attacks and exploiting security vulnerabilities to allow criminals to make other attacks against target systems.

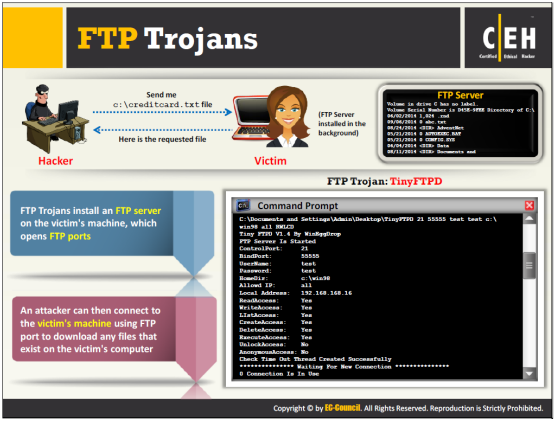
CyberGate

CyberGate is a remote control Trojan. It helps an attacker to control a large number of servers in a target network. CyberGate is only available for now for Windows platforms as a Native application, without requiring any Framework (such as .NET), Virtual Machine (such as Java Virtual Machine) or any Extra Dynamic Link Libraries or shared libraries. Using Cybergate, one can gain a victim's password, a screenshot of the victim's computer screen, and so on.



Proxy Server Trojans convert users' computers into proxy servers, thus making them accessible to specific attackers. Generally, 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 for any attacks launched from it.


Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
C|EH
Certified Ethical Hacker
01
W3bPr0xy Tr0j4n is a proxy server Trojan which support multi connection from many clients and report IP and ports to mail of the Trojan owner
Your Mail Properties
Host:
User:
Password:
From:
Subject:
Port:
TimeOut:
Send Mail Test
Settings
Detect IP Address
Listening Ports [Separate ports with a sinicolon (;)]
Install Path
File Name
Edit
Exit
Welcome to W3bPrOxy Tr0j4n Cr34t0r v 1.0
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

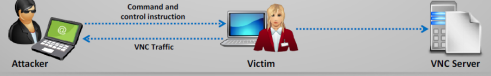

FTP Trojans
C|EH
Certified Ethical Hacker
Send me c:\creditcard.txt file
Here is the requested file
(FTP Server installed in the background)
Hacker
Victim
FTP Server
FTP Trojan: TinyFTPD
FTP Trojans install an FTP server on the victim's machine, which opens FTP ports
An attacker can then connect to the victim's machine using FTP port to download any files that exist on the victim's computer
Command Prompt
C:\Documents and Settings\Admin\Desktop\TinyFTPD 21 55555 test test c:\
win98 all SWLCD
Tiny FTPD V1.4 By WinSpyGroup
FTP Server Is Started
ControlPort: 21
BindPort: 55555
UserName: test
Password: test
HomeDir: c:\win98
Allowed IP: all
Local Address: 192.168.168.16
ReadAccess: Yes
WriteAccess: Yes
ListAccess: Yes
CreateAccess: Yes
DeleteAccess: Yes
ExecuteAccess: Yes
UnlockAccess: No
AnonymousAccess: No
Check Time Out Thread Created Successfully
************** Waiting For New Connection **************
0 Connections Is In Use
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VNC Trojans

VNC Trojan starts a **VNC Server daemon** in the infected system (victim)

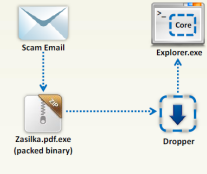
Attacker connects to the victim using any **VNC viewer**

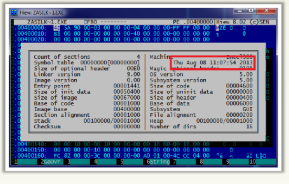
Since VNC program is considered a utility, this Trojan will be difficult to **detect** using anti-viruses

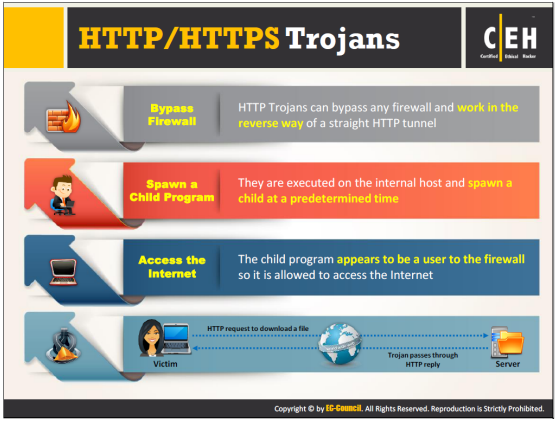


VNC Trojan: Hesperbot

- Hesperbot is a banking Trojan which features common functionalities, such as **keystroke logging, creation of screenshots** and **video capture**, and setting up a remote proxy
- It **creates a hidden VNC server** to which the attacker can remotely connect
- As VNC does not log the user off like RDP, the attacker can connect to the **unsuspecting victim's computer** while they are working







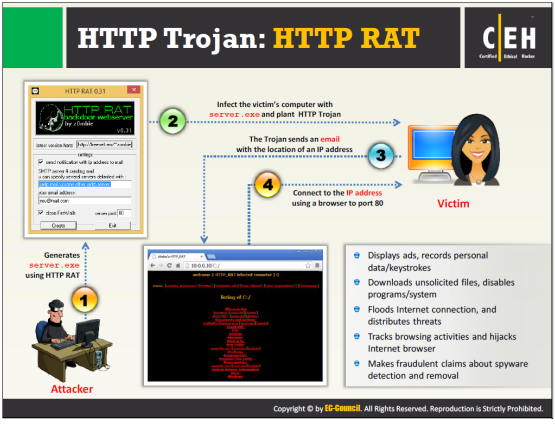
HTTP/HTTPS Trojans can bypass any firewall, and work in reverse, as opposed to a straight HTTP tunnel. They use web-based interfaces and port 80. The execution of these Trojans takes place on the internal host and spawns a child program at a predetermined time. The child program appears to be a user 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`

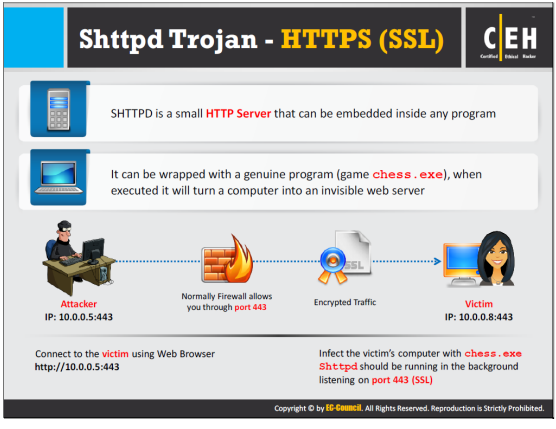
Master replies with: `g5mAlfbknz`

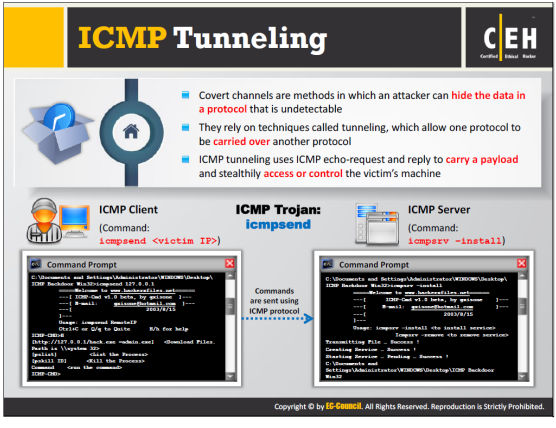
The **GET** of the internal host (SLAVE) is just the command prompt of the shell; the answer is an encoded "`ls`" command from the attacker on the **external server** (MASTER). The SLAVE tries to connect daily at a specified time to the MASTER. If necessary, the child spawn takes place because if the 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.



Remote Access Trojans (RATs) are malicious programs that run invisibly on a host's PC and permit an intruder remote access and control. A RAT can provide a backdoor for administrative control over the target computer. Upon compromising target system, the attacker can use it to distribute RATs to other vulnerable computers and establish a botnet. RAT enables administrative control and makes it possible for the attacker to watch all the target's actions using Keylogger or spyware. An attacker can also implement credit card fraud and identity theft using confidential information. He/she can also remotely access web cams and video recordings, take screenshots, format drives, delete, download, and alter files. It is very hard to detect this Trojan, as it functions like a genuine program.

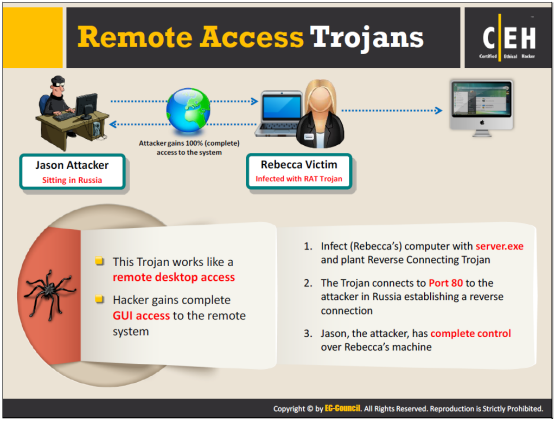




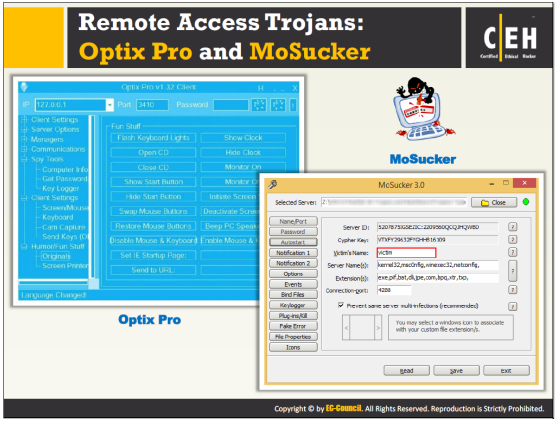
ICMP (Internet Control Message Protocol) is an integral part of IP, and every IP module must implement it. It is a connectionless protocol to provide error messages to unicast addresses. The ICMP protocol encapsulates the packets in IP datagrams.

The concept of ICMP tunneling is simple. 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 them, drop them, or return them. The Trojan packets themselves are masquerading as common **ICMP_ECHO traffic**. The packets can encapsulate (tunnel) any required information.



Remote access Trojans provide attackers with full control over the victim's system, enabling them to remotely access files, private conversations, accounting data, and others on the victim's machine. The remote access Trojan 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. Examples include **Optix Pro**, **BlackHole RAT**, **SSH - R.A.T**.

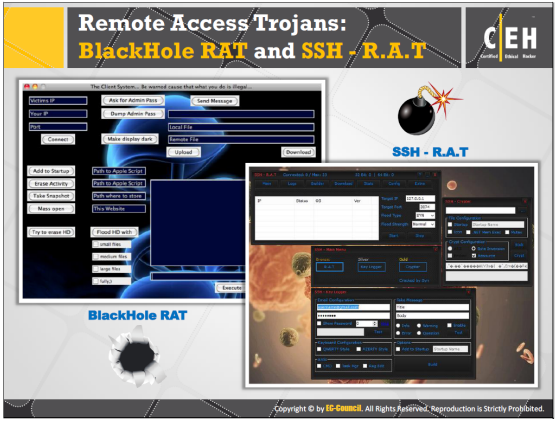


Optix Pro

Optix Pro is a configurable remote access Trojan that has the ability to become untraceable by most of the firewall and anti-virus products. It is also capable of detecting and disabling anti-Trojan products. It allows an attacker to easily control a compromised target system remotely to access or change files, capture the victim's keystrokes, spy on the victim's system through webcam, etc.

MoSucker

MoSucker is a backdoor Trojan written in Visual Basic, affecting most of the versions of Windows operating systems. The backdoor uses a client/server relationship, in which the installation of server component takes place in the victim's system, and the remote attacker has control of the client. The server attempts to open a port to allow the client system to connect. MoSucker contains a keylogger option that captures passwords. The backdoor can disable personal firewalls and anti-virus software. MoSucker could allow an attacker to remotely perform a variety of operations, such as changing the registry, executing commands, starting services, listing files, and uploading or downloading files.

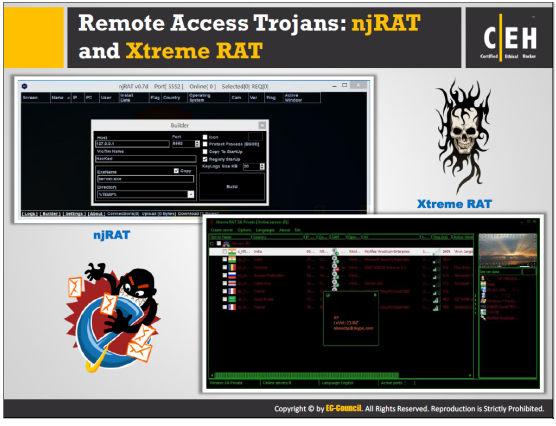


Attackers use Remote Access Trojans (RATs) to infect the target machine in order to gain administrative access. RATs help an attacker to remotely access, control victim's computer without his or her awareness, and are capable to perform screening and camera capture, code execution, key logging, file access, password sniffing, registry management, and so on. Below are listed some Remote Access Trojans.

BlackHole RAT

BlackHole is a remote administration tool (RAT) that, used maliciously, can also serve as a remote access Trojan. The BlackHole RAT works both on Mac OS X and Windows computers, and enables a remote attacker to do the following:

- Remote execution of shell commands (dependent on logged in user's privileges)
- Performs shutdown, restart, or put the computer to sleep
- Displays a message on the victim's computer
- Opens webpage using the user's default browser
- Creates text files on the desktop
- Prompts for admin credentials



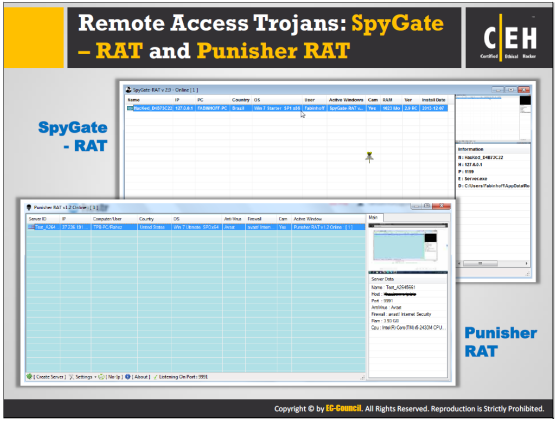
njRAT

njRAT is a Remote Access Trojan (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 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 & Control server software.

Xtreme RAT

Xtreme RAT is a notorious RAT, its activity is associated with spam campaigns that typically distribute Zeus variants, and other banking focused malware. Xtreme RAT can be used for a variety of purposes, including interacting with the victim machine via a remote shell, uploading and downloading files, interacting with the registry and manipulating running processes and services, grabbing passwords from browsers such as Firefox, Chrome, Opera, and Safari, capturing images of the desktop and recording from connected devices such as webcams and microphones.



SpyGate-RAT

SpyGate-RAT is a Remote Access Trojan that helps an attacker control target computers from anywhere in the world.

Features:

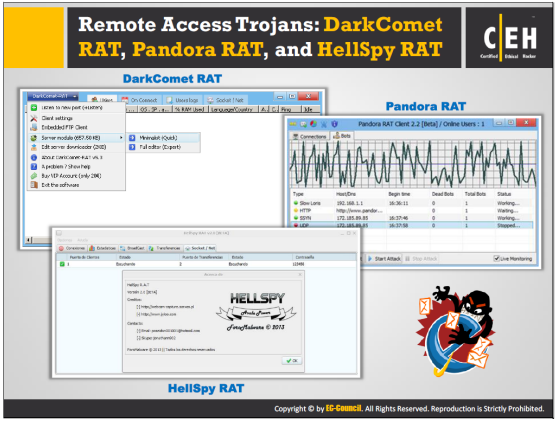
- Captures Keystrokes
- Captures screen activities
- Offers audio recording, which comes with a control period

Punisher RAT

Punisher is another Remote Access Trojan that allows an attacker to perform malicious activities on the target system.

Features:

- Manages files, registers, and processes
- Captures keystrokes and steals passwords
- Operates through Command prompt and remote shell



DarkComet RAT

DarkComet RAT is a Remote Administration Tool, created to remote control any Microsoft Windows machine. It allows an attacker to connect to and control the target system.

Features:

- **System monitors** (Process, Registry, Startup, DNS Manager, etc.)
- **File manager** (Modifies and manages host files)
- **Surveillance** (Micro-capture, Keylogger, screen capture, Webcam capture, etc.)
- **Network functions** (Scan for local computers, monitor network activity, Wi-Fi viewer, download files from the web, etc.)

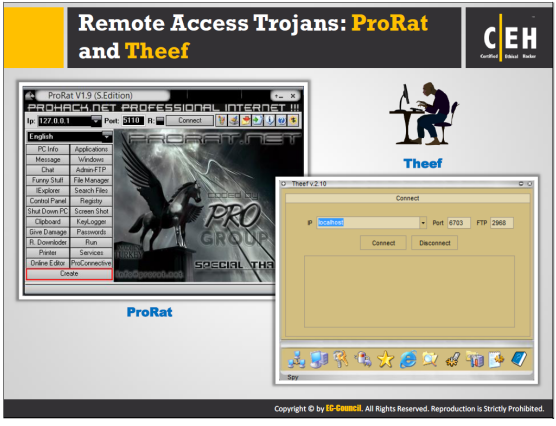
Pandora RAT

Pandora Rat is a professional Remote Administrator Tool developed for the Windows operating system. It uses advanced client and server architecture.

Features:

- File manager (File download and upload, File execute [Hidden or Shown], File Preview, Thumbnail Image (preview photos without downloading), File search, Folder manager [Delete, Rename, Create], etc.)

- Browser decryptor (decrypt passwords for all browsers. [Chrome, Opera, Firefox, Safari, Internet Explorer])
- Registry editor
- Process manager
- Network sniffer
- Screen capture
- Audio streaming, etc.



ProRat

ProRat is a Remote Administration Tool written in **C programming** language and can work in all Windows operating systems. The main purpose of this RAT is accessing one's own computers remotely. As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer, which allows the client to perform numerous operations on the server (the victim machine).

Some of the ProRat's malicious actions on the victim's machine:

- Logging keystrokes
- Stealing passwords
- Full control over files
- Drive formatting
- Open/close CD tray
- Hide taskbar, desktop, and Start button
- Writing on-screen
- Movement of cursor
- Take screenshots
- View system information

- View webcam
- Download and run files
- Password Protect your bound server from being used by anyone else

Theef

Theef is a Remote Access Trojan written in **Delphi** and it allows remote attackers access to the system via **port 9871**. It is a **Windows**-based application on both the client and server ends. The Theef server is a virus installed on the victim's system, and using Theef client, an attacker can control the virus.

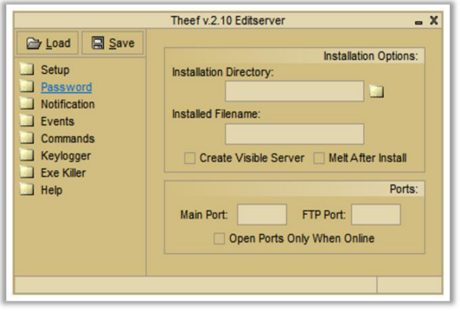
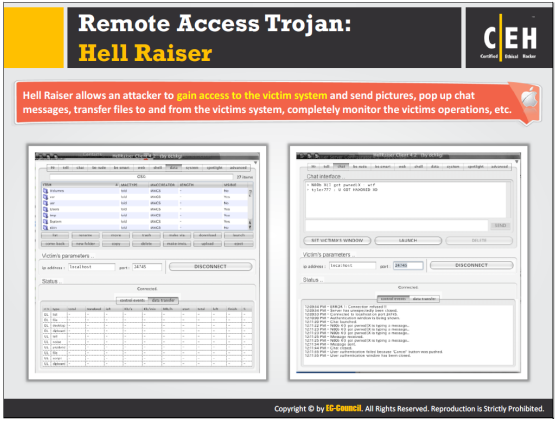


FIGURE 6.5: Screenshot of Remote Access Trojan – Theef

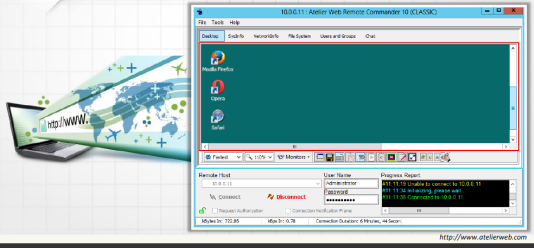


HellRaiser is a Trojan horse that gives control of a Mac OS X system to an attacker. This can include searching through the file system and then transferring files, viewing the clipboard, sending audio, sending chats, viewing the screen, showing pictures, viewing spotlight indexes, controlling mail, rebooting, and even remotely restart or shut down the infected machine.

To become infected, a user must run the server component of the Trojan horse, which can disguise itself as an innocent file. The attacker then uses the client component of the Trojan horse to take control of the infected system.

Remote Access Tool: Atelier Web Remote Commander

Atelier Web Remote Commander (AWRC) allows you to **establish a remote connection to the remote machine** without installing any supporting software on the machine



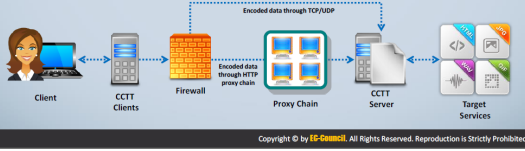
http://www.atelierweb.com

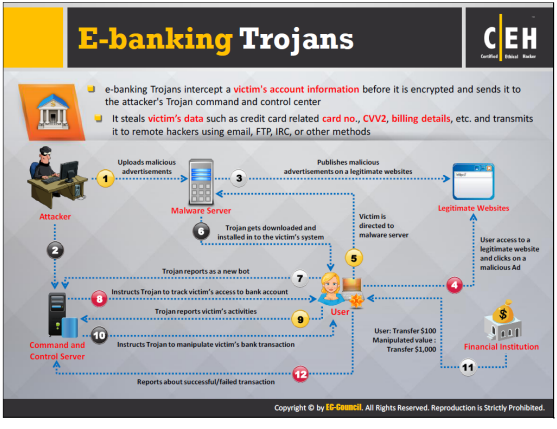
Covert Channel Trojan: CCTT

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

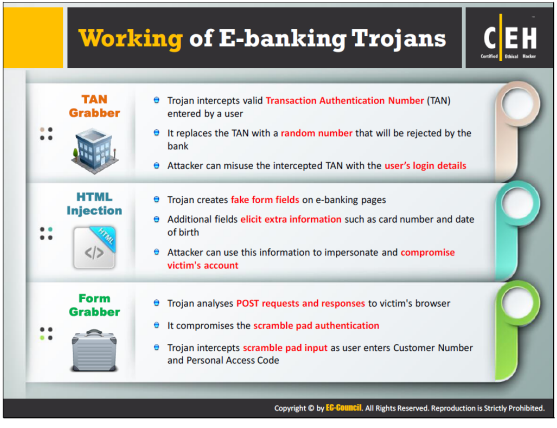
It enables attackers to get an external server shell from within the internal network and vice-versa

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





E-banking Trojans are very dangerous and have become a major threat to online banking. They intercept a 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 generally 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 his/her bank balance and is not aware of this fraud unless he/she checks the balance from another system or from an ATM machine. 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.



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 Transaction Authentication Number (TAN) entered by a user and replaces it with a random number. The Bank will reject this invalid random number. An attacker thereafter 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 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 target's Internet banking information. It analyses POST requests and responses to victim's browser. It compromises the scramble pad authentication. It intercepts scramble pad input as the user enters Customer Number and Personal Access Code.

ZeuS

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

ZeuS is a banking Trojan horse program (or "crimeware"). ZeuS steals data from infected computers via web browsers and protected storage. Once infected, the computer sends the stolen data to a bot command and control (C&C) server, where the data are stored.

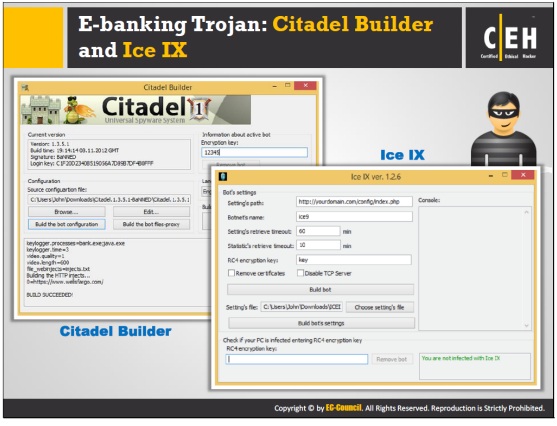
Features:

- 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 hosts file (%systemroot%\system32\drivers\etc\hosts)

- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

SpyEye

SpyEye is malicious software that allows an attacker to steal targets' money from online bank accounts. Actually, this is a botnet with a network of command-and-control servers. This automatically triggers when the target starts his or her transaction and can even block the bank's transactions.



Citadel Builder

The Citadel Trojan is very similar to the Zeus Trojan in terms of logical structure as well as physical data. This means Citadel can steal personal information used in financial transactions, much like ZeuS. Once installed, Citadel steals banking information and allows identity theft. By sending over keystrokes to the botnet operator or using man-in-the-browser technics, the cyber criminals try to gain access to online accounts or to manipulate payment transactions directly. Additionally, Citadel blocks anti-virus programs and its update functionality to prevent users to clean up the infected computers.

Features:

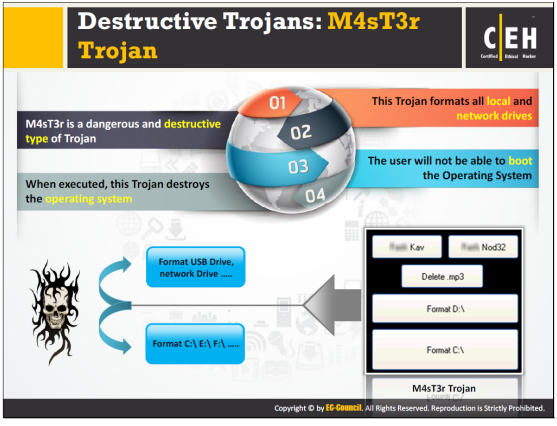
- Offers auto Crypto-protection, that is, data is decrypted in memory
- Possess integrated functionality to export FTP accounts in the API
- Provides a heuristic analysis environment to stop unwanted software
- Stores and transfers data only in the encrypted form
- Offers history software feature that allows to view the Citadel updates in botnet itself
- Delivers an extra layer of protection from trackers (Login Key)
- Blocks or redirects any URL

Ice IX

Ice IX is a new, private form-grabber bot based on Zeus. It has the ability to manipulate the content displayed in browsers used by its victims to inject rogue Web forms into online banking websites. Attackers can use these rogue forms to extract online banking credentials, along with other private information such as secret questions/answer pairs and date of birth. It also displays forms that ask victims for their telephone account numbers and other information used by telephone companies to verify subscriber identity.

Features:

- Keylogging
- HTTP and HTTPS form grabbing, injecting its own code into IE and into IE-based browsers (Maxton, AOL, etc.), as well as Mozilla FireFox
- .sol Cookie Grabbing and scraping info from saved forms
- FTP client credentials grabbing: FlashFXP, Total Commander, WsFTP 12, FileZilla 3, FAR Manager 1, 2, WinSCP 4.2, FTP Commander, CoreFTP, SmartFTP
- Windows Mail, Live Mail, and Outlook grabbing
- Socks with "backconnect" ability
- Real-time screenshots, plus the option to automate taking screenshots while the bot browses to preset URLs
- Grabs certificates from "MY" storage space and clears storage. Once cleared, all new certificates will be sent to the bot master's C&C server
- Upload specific files from the infected machine or perform searches on local disks enabling wildcards.
- TCP protocol traffic sniffer
- Elaborate set of commands to control the infected PCs



The sole purpose of writing destructive Trojans is to delete files on a target system. These Trojans are particularly destructive because they can delete core system files such as .dll, .ini, or .exe files. The attacker can activate these Trojans, or it can be set to initiate at a fixed time and date.

M4sT3r is a multifunctional Trojan for remote computer control written in Visual Basic. For remote control, it opens TCP port 666. When executed, this Trojan destroys the operating system. The user will not be able to boot the operating system. This Trojan formats all local and network drives.

Notification Trojans

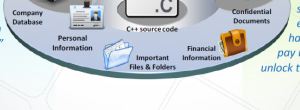
- Notification Trojan sends the location of the **victim's IP address** to the attacker
- Whenever the victim's computer connects to the Internet, the attacker receives the **notification**

Notification Types	
SIN Notification	Directly notifies the attacker's server
ICQ Notification	Notifies the attacker using ICQ channels
PHP Notification	Sends the data by connecting to PHP server on the attacker's server
E-Mail Notification	Sends the notification through email
Net Send	Notification is sent through net send command
CGI Notification	Sends the data by connecting to PHP server on the attacker's server
IRC notification	Notifies the attacker using IRC channels

Data Hiding Trojans (Encrypted Trojans)

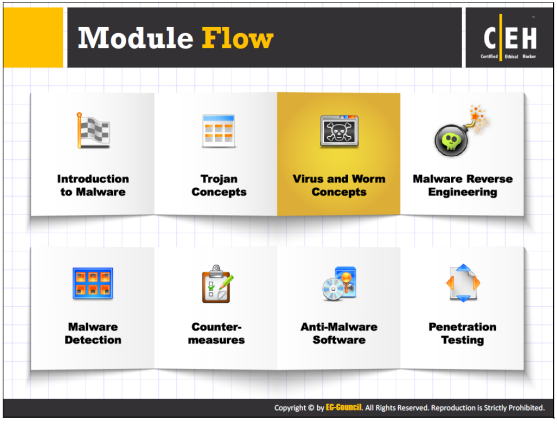
Encryption Trojan encrypts data files in victim's system and renders information unusable

"Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was encrypted with complex password."



Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files

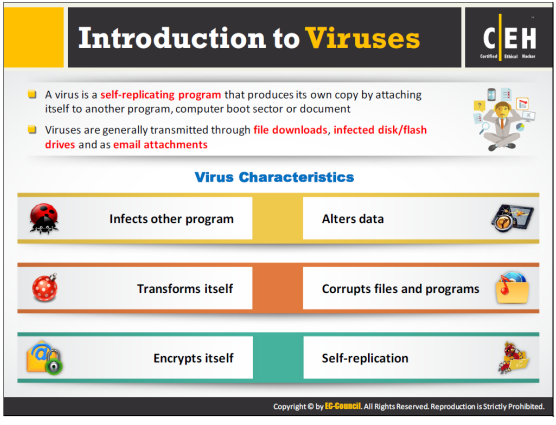
"Do not try to search for a program that encrypted your information – it simply does not exists in your hard disk anymore," pay us the money to unlock the password



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

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 operating system they work on, and so on.

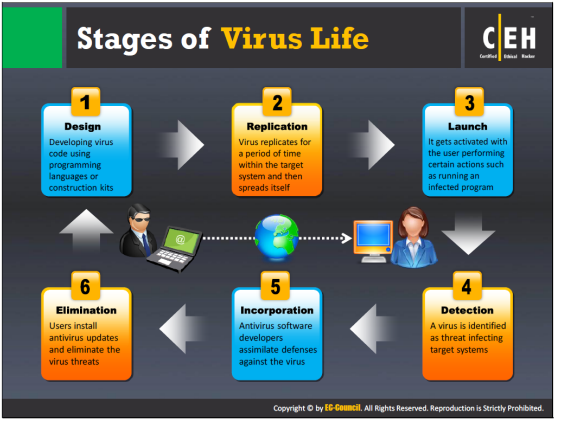
This section also deals with computer worms, and discusses the difference between worms and viruses, worm analysis (Darlloz and Stuxnet), and a worm maker (Internet Worm Maker Thing).

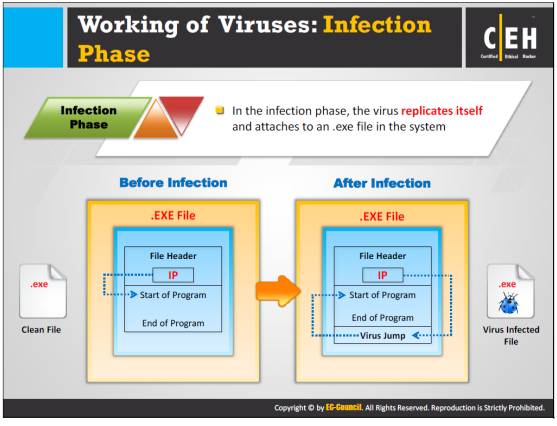


Viruses are the scourge of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce itself. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n*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

A computer virus is a self-replicating program that produces its own 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 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 certain 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, flash cards, and so on. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings among others.

Generally, 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 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 executable on the disk.

- The virus appends malicious code to a legitimate program without the user's permission or knowledge.
- 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.

Obviously, the user unknowingly triggers and executes the virus in order for it to function. There are many ways to execute programs while a computer is running. For example, 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.

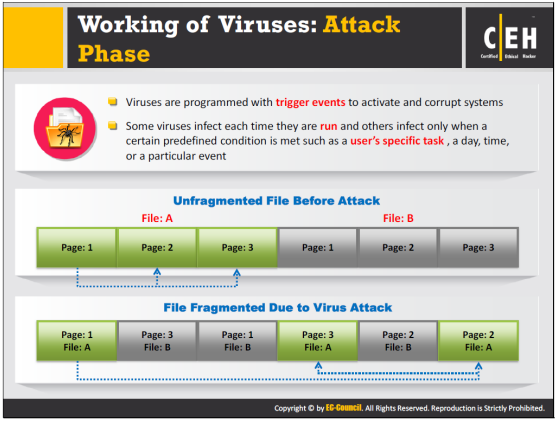
Specific viruses infect in different ways:

- 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 own 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 when the user executes them. Some programs do not infect the programs when first executed. They reside on 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. In the figure given below, 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, Pen 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.



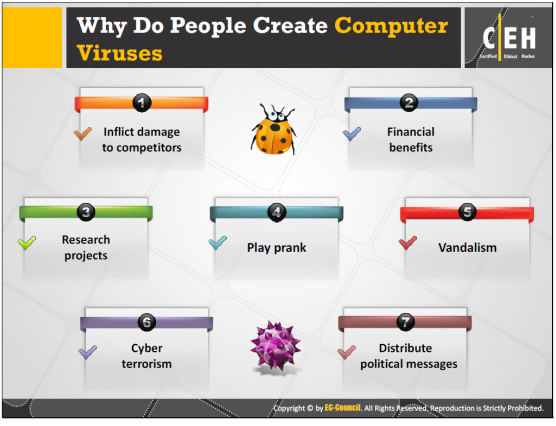
Once viruses spread themselves throughout the target system, they start corrupting the files and programs of the host system. Some viruses have the feature of triggering and corrupt the host system only after activating that triggering event. Some viruses have bugs that replicate themselves, and perform 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, causing the system to slow down
- Performing tasks not related to applications, such as playing music and creating animations

The figure shown 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.

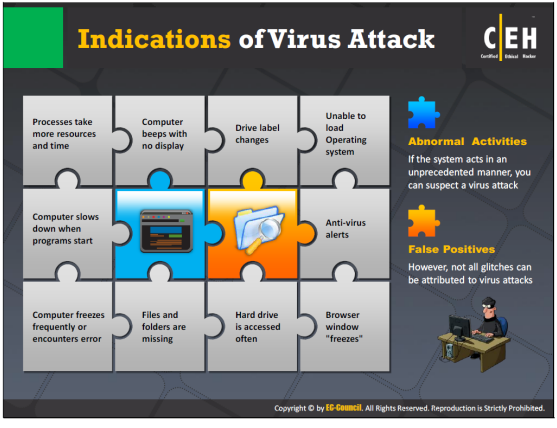
In the attack phase:

- Viruses execute upon triggering certain 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 fully spreading in the host



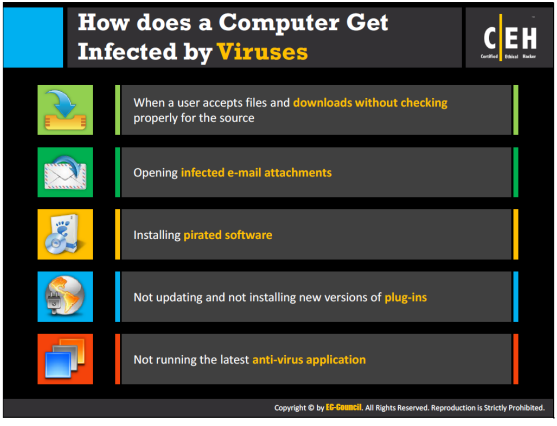
Computer viruses are not self-generated. Generally, attackers create viruses with disreputable motive. Criminals create viruses to destroy a company's data, as an act of vandalism, or to destroy a company's products; however, in some cases, viruses actually aid the system. Typically designed to improve a system's performance by deleting previously embedded viruses from files and they can carry out tasks without causing harm, while self-replicating.

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



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 example, if the system runs slower than usual, one may assume that a virus affected the system, but the reason might actually be program overload.

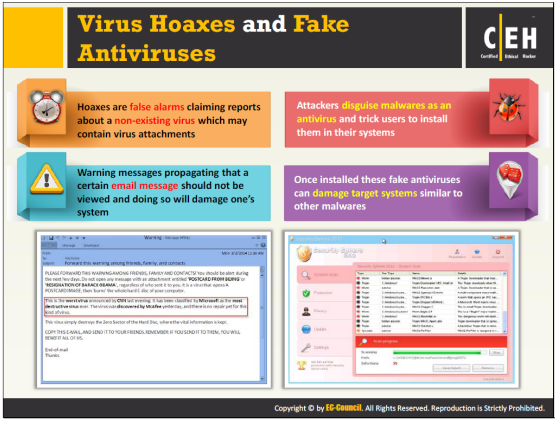
An effective virus tends to multiply rapidly, and may infect a number of machines in a short period. Viruses can infect files on the system which, when transferred, can infect machines of users who receive them. A virus can also make good use of file servers to infect files.



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. The virus then infects the computer in any of various ways, some of which are:

- **Downloads**: Attackers incorporate viruses in popular software programs and upload them on 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 software (OS, Adobe, Microsoft office, etc.) might infect the system as they may contain viruses.
- **Failing to install Security Software**: With the growing technology, 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 attacker to access the system.
- **Browser**: By default, every browser comes with built-in security. If the browser is not configured properly, 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 disk, 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 backup of infected files and restoring them back to a system infects the system again with the same virus.



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

Virus Hoaxes

Virus hoaxes are simply 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, such as the one shown in the slide above.

The following are some important points about hoaxes:

- These warning messages, which can be propagated rapidly, state that a certain 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

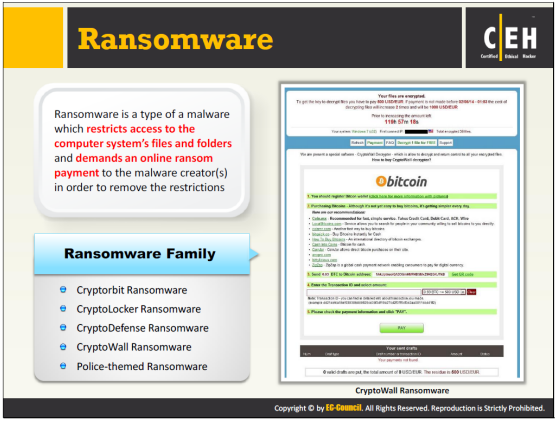
boards on which people actively discuss current community happenings/concerns. Before jumping to conclusions by reading Internet information, first check the following:

- 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.
- If the posting is technical, hunt for sites that would cater to the technicalities, and try to authenticate the information.

Fake Anti-viruses

Fake or rogue anti-virus software is a form of Internet fraud using malware. It appears and performs similar to a real anti-virus program. Fake anti-viruses often display 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 on which they are prompted to buy or subscribe to that anti-virus software and enter their payment details. Fake anti-viruses can further cause a lot of damage to systems, once downloaded and installed; for example, they infect them with malicious software, steal sensitive information (e.g., passwords, bank account numbers, credit card data), and corrupt files.



Ransomware is a type of malware that restricts access to the computer system that it infects, or critical files and documents stored on it, and thereafter demand 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 messages displayed 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.

CryptoWall Ransomware

CryptoWall Ransomware is a ransomware Trojan that carries the same strategy as a number of other encryption ransomware infections, such as Cryptorbit Ransomware or CryptoLocker

Ransomware. CryptoWall Ransomware infects all versions of Windows, including Windows XP, Vista, 7, and 8. As soon as the CryptoWall Ransomware infects a computer, it uses RSA2048 encryption to encrypt crucial files. Effectively, the CryptoWall Ransomware prevents computer users from accessing their data by encrypting and making the data invisible to them. CryptoWall Ransomware claims that it is necessary to pay $500 USD to recover the encrypted data. The software demands payment using TOR and Bitcoins to maintain the recipients' anonymity.

CryptoWall Ransomware is popularly distributed as a fake update for applications such as Adobe Reader, Flash Player, or the Java Runtime Environment. The pop-up window contains these types of updates when you visit unsafe websites, or when a Potentially Unwanted Program is installed on your computer. The CryptoWall Ransomware also may be distributed using spam email attachments and other typical threat delivery methods. Apart from encrypting your software, the CryptoWall Ransomware will also drop the files DECRYPT_INSTRUCTION.txt, DECRYPT_INSTRUCTION.html and DECRYPT_INSTRUCTION.url into directories in which CryptoWall Ransomware has encrypted data.

Given below is the message associated with CryptoWall Ransomware to demand payment:

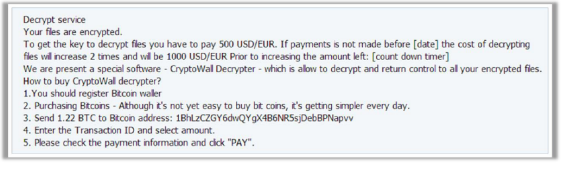


FIGURE 6.6: Screenshot displaying demand message of CryptoWall Ransomware

CryptoDefense Ransomware

CryptoDefense targets text, picture, pdf, MS Office and video files. Attackers use many methods, such as spam email campaigns, web plug-ins, and drive-by-download to inject it into target systems. It targets all versions of Windows, including XP, Vista, 7, and 8. For example, when an end user opens the infected attachment, the program begins encrypting its target files with a strong RSA-2048 key, which is hard to undo. After encryption, the malware places ransom-demand files in every folder containing encrypted files.

Upon opening the files, victims find a CAPTCHA page. If the files are too important and they want to get them back, they accept the terms. Proceeding further, they must complete the CAPTCHA correctly, and then the page redirects them to a payment page. The price of the ransom is predetermined—doubled if the victim fails to comply with the developer's instructions within a defined period of four days. They also demand the purchase of a decryptor within a month; otherwise, their private key will expire and they will no longer be able to decrypt their files. The payment site is located on the Tor network and can only be made in Bitcoins.

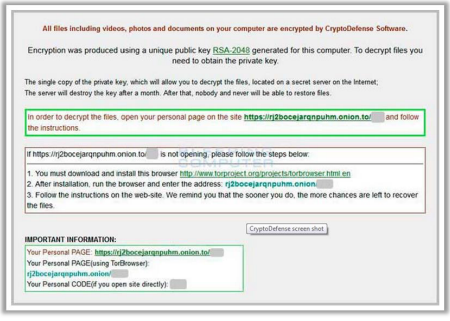


FIGURE 6.7: Screenshot displaying demand message of CryptoDefense Ransomware

Ransomware (Cont'd)

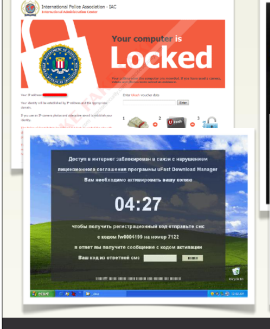
CEH Certified Ethical Hacker

Cryptorbit Ransomware

Police-themed Ransomware

Ransomware (Cont'd)

CEH Certified Ethical Hacker



CryptorBit Ransomware

CryptorBit, or as it is also known, HowDecrypt, is ransomware that has affected a variety of IT consultants, businesses, and end users, and is an increasingly elusive threat. It targets all versions of Windows, including XP, Vista, 7, and 8, and is most likely to spread through email attachments and malicious websites.

CryptorBit scans computers and corrupts any data files it finds, regardless of the file type or extension, by encrypting the first 512 bytes of data and replacing them with illegitimate data.

After it encrypts the files, CryptorBit creates additional files named HowDecrypt.txt file and a HowDecrypt.gif in every folder. The GIF and TXT files advise to pay a ransom and instruct on how to access a payment site to make the payment online. This payment site is located on the TOR network (Anonymity Online project) and only accepts Bitcoins for payment.

CryptorBit also carries a Cryptocoin Miner, a component that utilizes infected computer's CPU to mine digital coins, such as Bitcoin (or other coins), for the malware developer, generating further revenue for them.

Police-Themed Ransomware

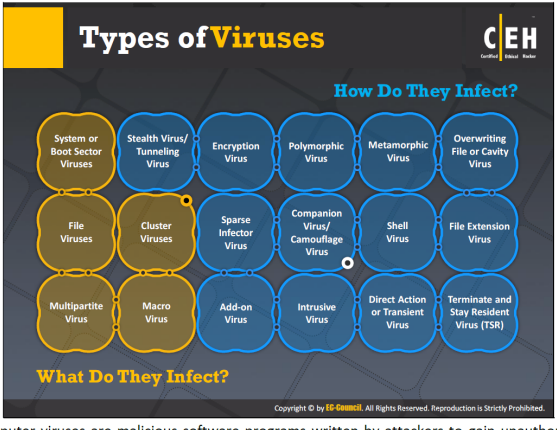
"**Police-themed**" ransomware cunningly disguises its ransom demands as official-looking warning messages from local law enforcement agencies. Most likely, it enters the system when a website containing malicious scripts is browsed. Police-themed ransomware is invisible and hidden in any of the following forms:

- A browser plug-in or extension (typically a toolbar)
- A multimedia codec required to play a certain video clip
- Software shared on peer-to-peer networks
- A free, online malware-scanning service

The language used and the specific authority mentioned vary, depending on the user's geographical location.

The specific text of the ransom messages varies, but generally follows the same pattern: they claim that the user's computer is "**locked**" after the police identified it as being used to visit websites related to terrorism or abuse, and that payment of a "**fine**" is required to settle the "**offense**." The amount of the supposed fine varies, and directions for paying it via anonymous, untraceable disposable cash cards are included.

It is important to note that in almost all cases, payment of the ransom still does not restore the computer to normal use.



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

Virus Forms

For any virus to accomplish its task of corrupting a system, it has to first associate its code with an executable code. Following considerations depicts the forms of the virus:

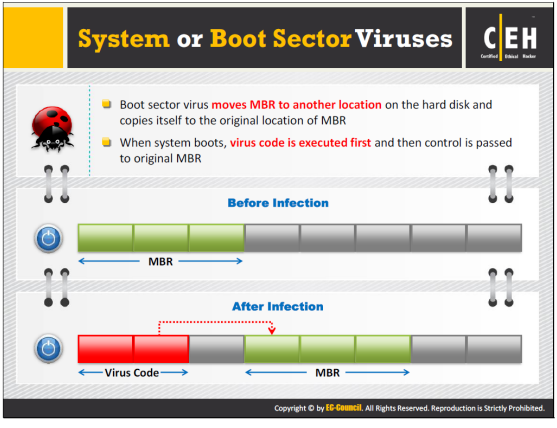
- How they add themselves onto the target host's code
- How they choose to act upon the target system

The following sections describe some of the forms of viruses:

Shell Viruses: This virus code forms a layer around the target host program's code as like an eggshell because it makes itself the original program and the host code its subroutine. Then, the virus code shifts the original code to the new location, and the virus assumes its identity.

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

Intrusive Viruses: This form of virus overwrites its code either by completely removing the target host's program code, or by only overwriting part of it. Therefore, the host executes a part of the original code.



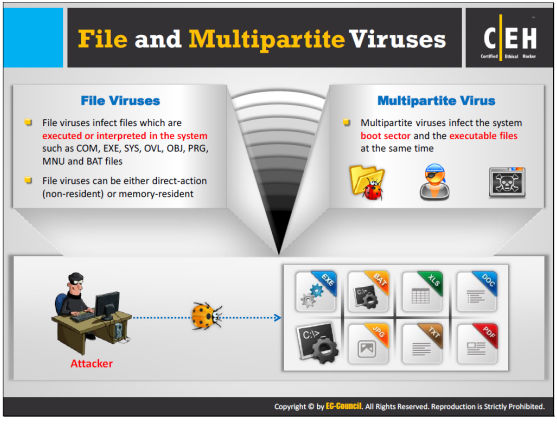
The most common targets for a virus are the system sectors, which are nothing but the master boot record (MBR) and the DOS boot record system sectors. An operating system executes codes in these areas while booting. Every disk has a system sector of some sort. MBRs are the most virus-prone zones, because 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 main carrier of system sector viruses is the floppy disk. These viruses generally 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, the virus code executes first, 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 operating system, 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

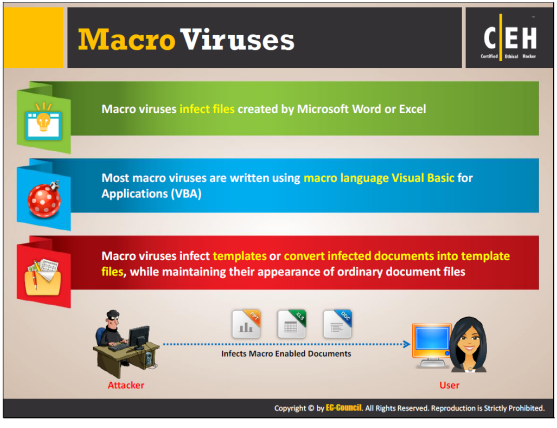
File viruses infect files executed or interpreted in the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU, and BAT files. File viruses can be either direct-action (non-resident) or memory-resident.

File viruses insert their code into the original file and infects executable files. File viruses are large in number, but they found rarely. 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 in a proper manner. These types of viruses tend to found immediately. Before inserting their code into a program, some file viruses save the original instructions and then 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 that 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.

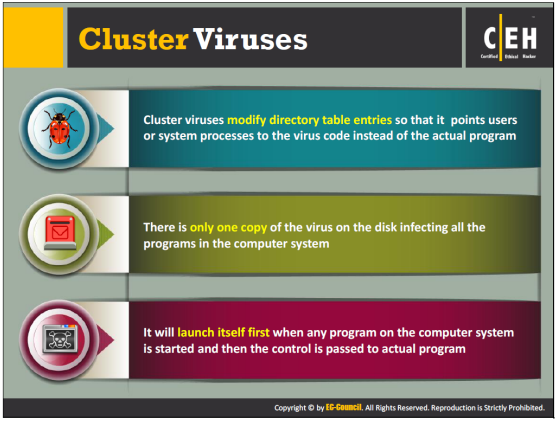
Multipartite Viruses

A multipartite virus (also known as 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 completely rooted out from the target machine. Some of the examples of multipartite viruses include **Invader**, **Flip**, and **Tequila**.



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 ordinary document files.

Macro viruses are somewhat less harmful than other types. 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 common programs with macro capability such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain macrocode.

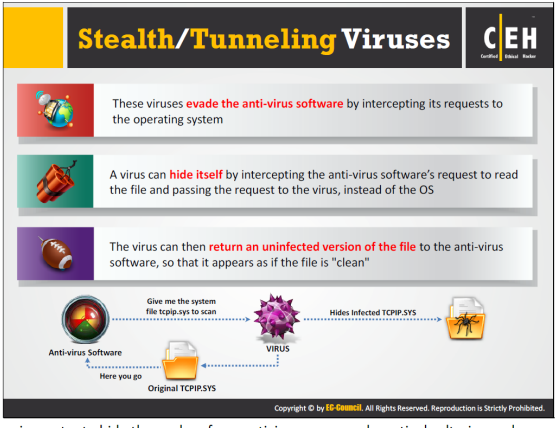


Cluster viruses infect files without changing the file or planting extra files. They save the virus code to the hard drive and overwrite the pointer in the directory entry, directing the disk read point to the virus code instead of the actual program. Even though the changes in the directory entry may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

Cluster virus launches itself first when any program starts on the computer system, and then the control is passed to the actual program. Dir-2 is an example of this type of virus.

This virus infection leads to serious 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 utility such as CHKDSK, the utility reports serious problem with 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.



These viruses try to hide themselves from antivirus programs by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests to perform operations in respect to these service call interrupts. These viruses state false information to hide their presence from antivirus programs. For example, the stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its virus code.

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

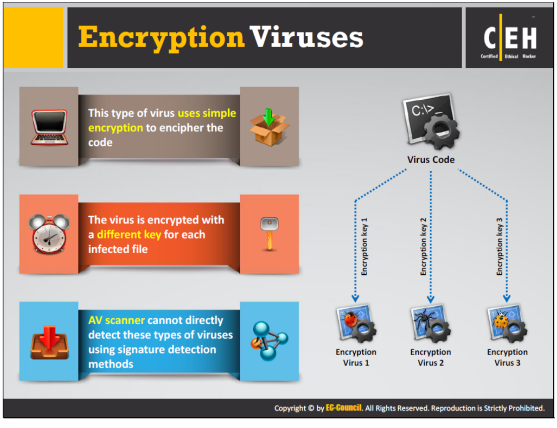
A stealth virus hides the modifications that it makes. It takes control of the system's functions that read files or system sectors and, when another program requests information that had already modified by the virus, the stealth virus reports that information to the requesting program instead. This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

Virus Removal:

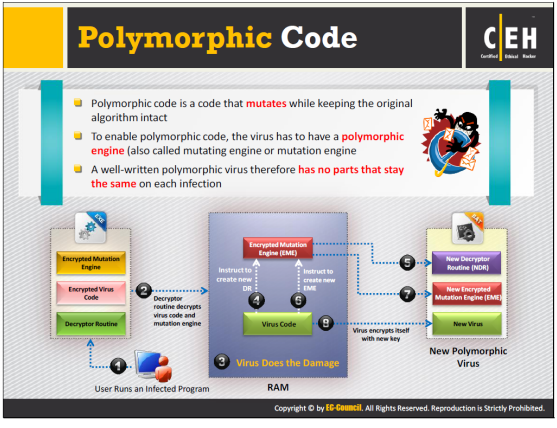
- Always do a cold boot (boot from write-protected CD or DVD).
- Never use DOS commands such as FDISK to fix the virus.
- Use anti-virus software.



Encryption viruses 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 to the target machine, the decryptor will execute first 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 different key for encryption. These viruses generally 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 a limited access to the system. This virus uses encryption to hide itself from virus scanner. It is not possible for the virus scanner to detect the encryption virus by means of signatures, but it can detect the decrypting module.



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.

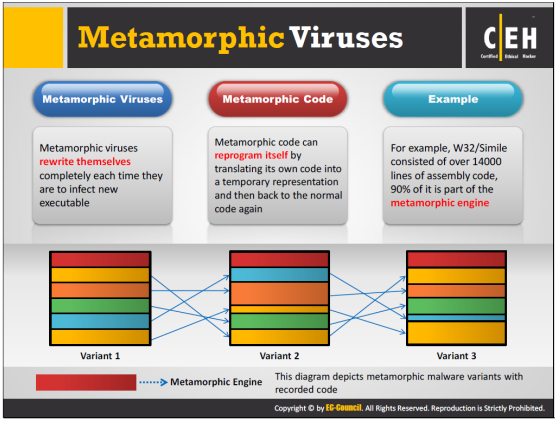
The general use of mutation engine is to enable polymorphic code. The mutator provides a sequence of instructions that a virus scanner can use to optimize an appropriate detection algorithm. Slow polymorphic codes prevent antivirus professionals from accessing the codes. A simple integrity checker detects the presence of a polymorphic virus in the system's disk.

A polymorphic virus consists of three components. They are the encrypted virus code, the decryptor routine, and the mutation engine. The function of the decryptor routine is to decrypt the virus code. It decrypts the code only after taking control over the computer. The mutation engine generates randomized decryption routines. This decryption routine varies every time when 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 RAM (Random Access Memory), the virus makes a replica of itself as well as the mutation engine. Then the virus instructs the encrypted mutation engine to generate a new randomized decryption routine, which has the capability of decrypting virus. Here, 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 are programmed in such a way that they rewrite themselves completely each time they are to infect a new executable file. Such viruses are complex 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 use to avoid pattern recognition of anti-virus software. This 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

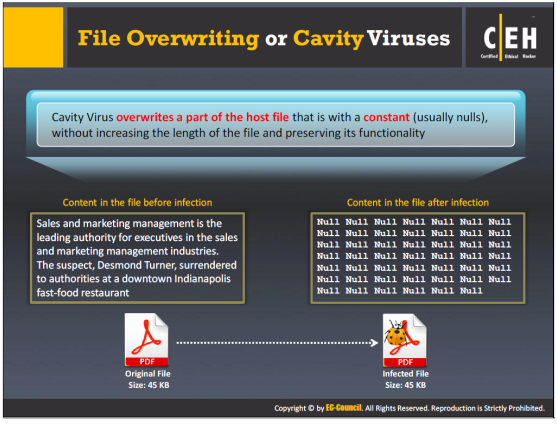
The commonly known metamorphic viruses are:

Win32/Simile

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

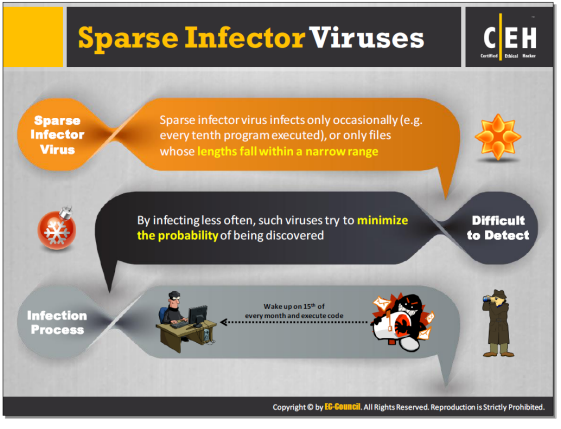
Zmist

Zmist in other sense also 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.



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 found rarely 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 certain 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 of this category is the CIH virus (known as **Chernobyl** or **Spacefiller**).



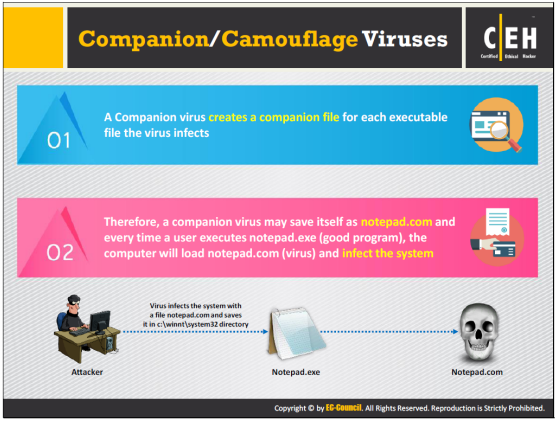
The virus should act smart in order to hide from the antivirus, so that it can spread in a larger extent. Sparse infector viruses infect less often and try to minimize the probability of discovery. Sparse infector viruses infect only occasionally upon satisfying certain conditions or only files whose 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)

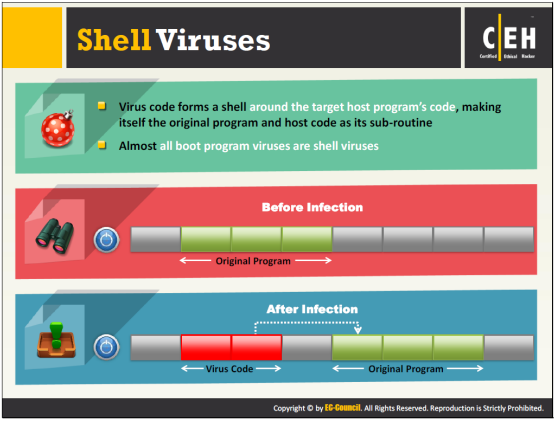
The diagram shown in the slide represents the working of a sparse infector virus.

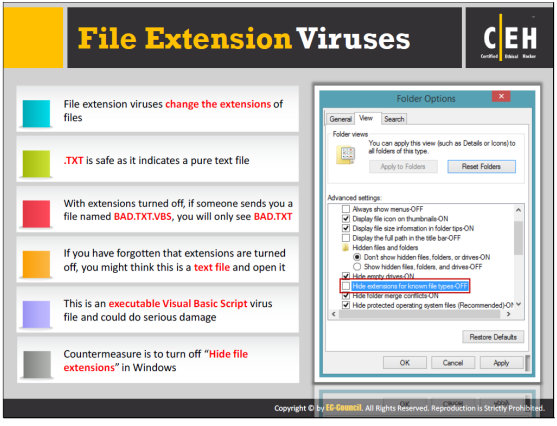
The attacker sends a sparse infector virus to target machine and sets a wakeup call for the virus to execute on the 15th day of every month. This strategy makes it hard for the anti-virus to detect the virus, thus allowing the virus to successfully infect the target machine.



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 your PC and decides it is time to infect a file. It looks around and happens to find a file called PGM.EXE. It now creates a file called PGM.COM, containing the virus. The virus usually plants this file in the same directory as the .EXE file, but it could place it in any directory on your DOS path. If you type PGM and press Enter, DOS executes PGM.COM instead of PGM.EXE. (In 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 PGM.EXE. The user probably would fail to notice anything is wrong. It is easy to detect a companion virus just by the presence of the extra COM file in the system.

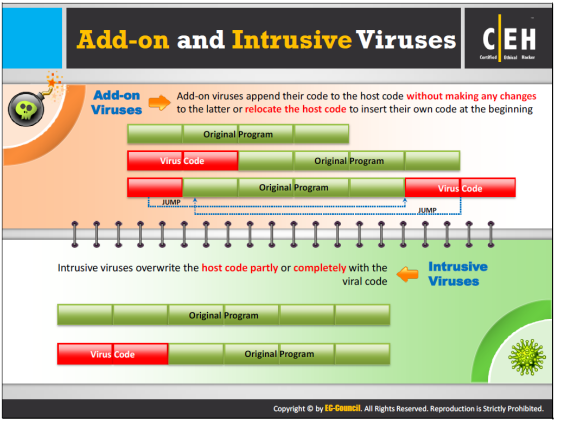


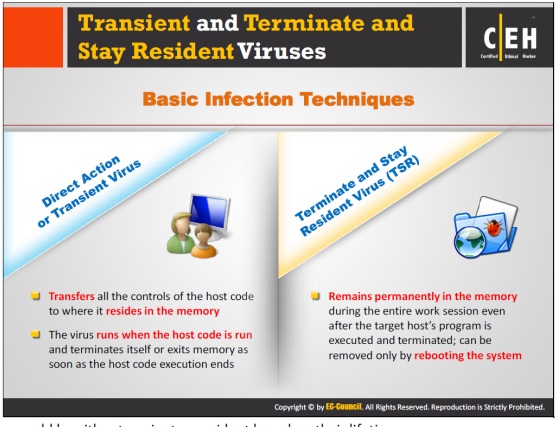


Guidelines to keep files safe from virus infection:

- 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**), as shown in the snapshot in the slide.
- Scan all files in the system with good anti-virus software. To do so takes a substantial amount of time.

Source: *http://www.cknow.com/cms/vtutor/file-extensions.html*





A virus could be either transient or resident based on their lifetime.

Direct or Transient Virus

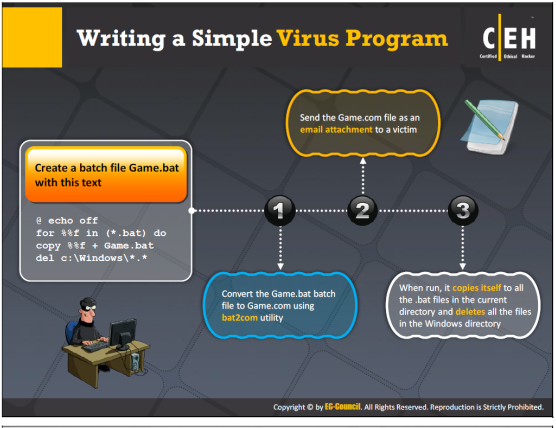
It transfers all controls of the host code to where it resides in the memory. It selects the target program to be modified, and corrupts it. The life of transient virus is directly proportional to the life of its host. This means the transient virus executes only upon the execution of its attached program 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 disk to search for programs to infect.

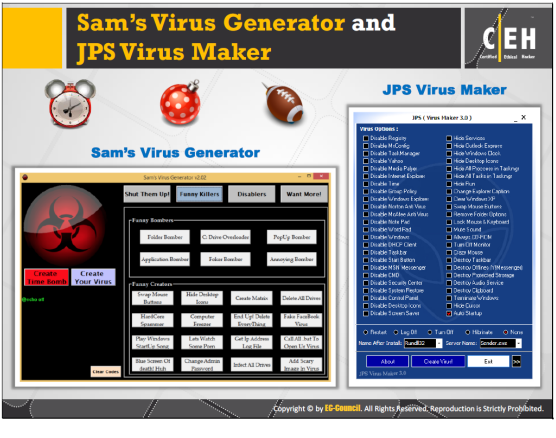
Terminate and Stay Resident Virus (TSR)

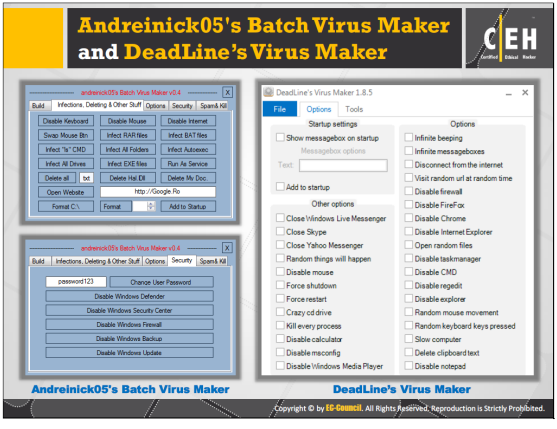
A TSR virus (TSR) remains permanently in the target machine's memory during an entire work session, even after the target host's program is executed and terminated. The TSR remains in memory to have some control over the processes. In general, the TSR takes on interrupt vectors into its code, so that when the interrupt take 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, then user needs to reboot the system to remove the virus.

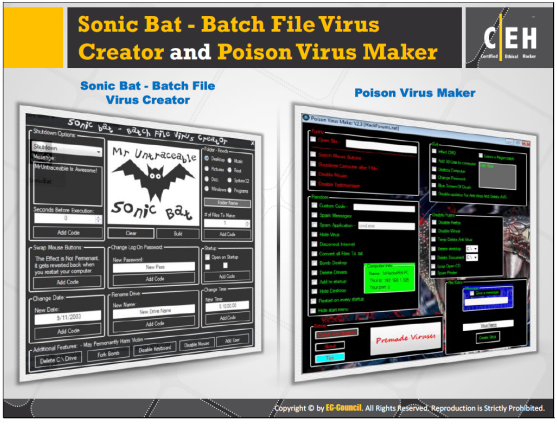
Some of the steps employed by TSR viruses to infect files are as follows:

- 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









Sonic Bat – Batch File Virus Creator

Sonic Bat creates batch (.bat) viruses and has multiple options to ruin the victim computer. One can flood the storage space on victims' computers by making large number of files in different folders by using its "**folder flood**" feature. It also includes a "**bat to exe**" converter to convert batch virus files into .exe virus programs, and an icon changer.

Poison Virus Maker

Poison Virus Maker helps in creating viruses. One can choose various options provided by the tool to create virus of their own interest.

Other Tools to create Viruses

Given below are few more tools that can be used to create viruses:

TeraBIT Virus Maker

Below is a snapshot of TeraBIT Virus Maker that displays various options for creating viruses.

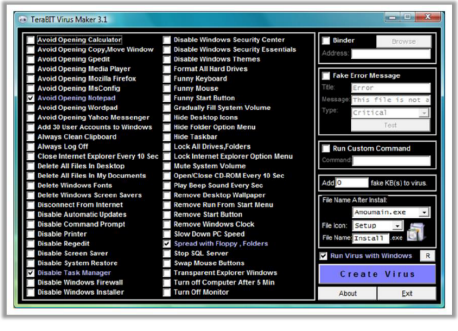


FIGURE 6.8: Snapshot of TeraBIT Virus Maker

DELmE's Batch Virus Maker

DELmE's Batch Virus Maker is a simple tool that allows you to create you own bat file virus to suit different tasks. Below is a snapshot that shows the various features it offers.

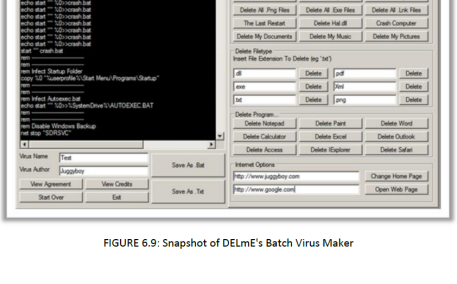
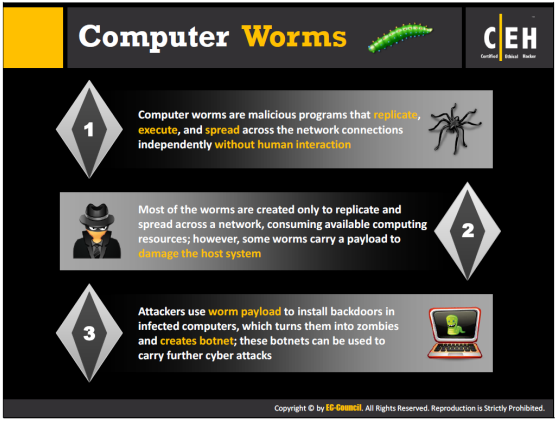


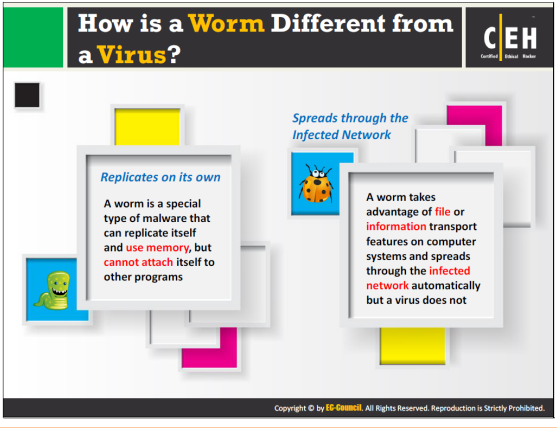
FIGURE 6.9: Snapshot of DELmE's Batch Virus Maker



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 operating systems using the same worms by sharing them in 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.

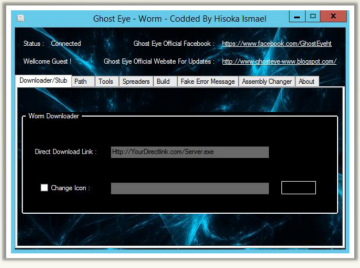


Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not 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 actually sent to the other computer	A worm, after being installed in a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs
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 easily removed from a system

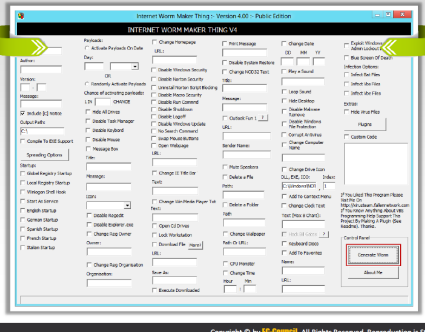
TABLE 6.3: Difference between Virus and Worms

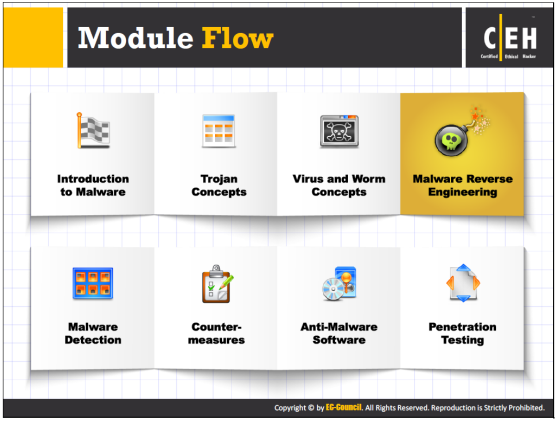
Computer Worms: Ghost Eye Worm

Ghost Eye worm is a hacking program that **spreads random messages** on Facebook or steam or chat websites to get the password



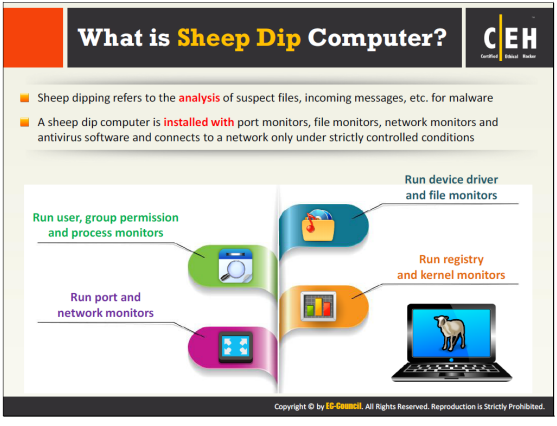
Worm Maker: Internet Worm Maker Thing





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 allows an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future ones from occurring, it is necessary to perform a malware analysis. Many tools and techniques exist to for doing so.

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



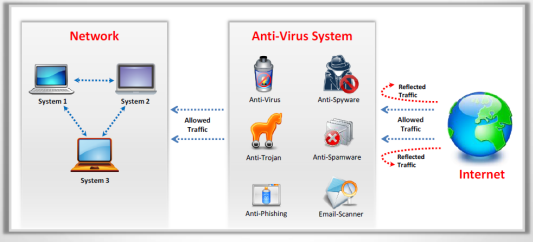
Sheep dipping is a process used in sheep farming which involves dipping of sheep in chemical solutions to make them germ and lice free. A computer sheep dip is the process of running anti-virus checks on one computer connected to a network to detect anomalies.

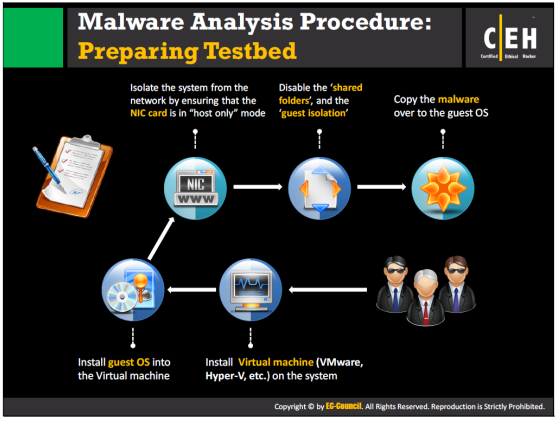
The users isolate the sheep-dipped computer from other computers on the network to block any malware from entering the system. Before performing this process, it is important to save all downloaded programs on external media such as CD-ROMs or DVDs.

A computer used for sheep dipping should have, for example, 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.

Anti-Virus Sensor Systems

- 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





Malware analysis provides in-depth understanding of each individual sample and identifies emerging technical trends from the large collections of malware samples without actually executing them. The samples of malware are mostly compatible with the Windows binary executable. There is 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 on a test bed.

Given below is the procedure for preparing a test bed:

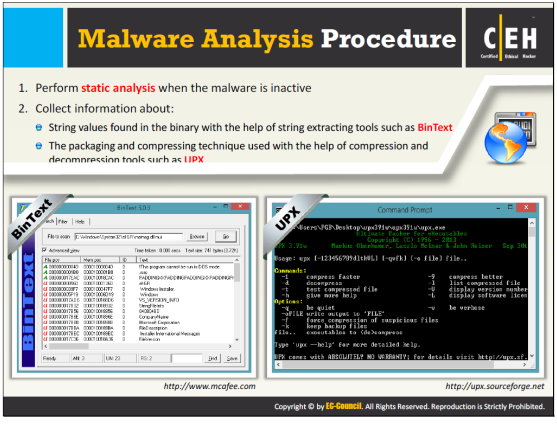
Requirements to build a test bed:

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

- Install Virtual machine (VMware, Hyper-V, etc.) on the system
- Install guest OS on the Virtual machine
- Isolate the system from the network by ensuring that the NIC card is in "**host only**" mode
- Disable the shared folders and the guest isolation
- Copy the malware over to the guest OS



String Extracting Tool: BinText

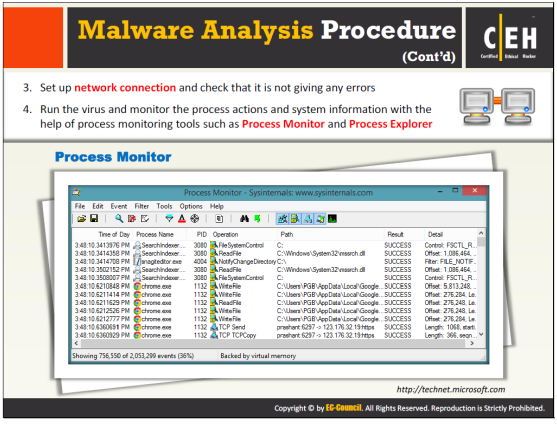
Source: http://www.mcafee.com

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

Compression and Decompression Tool: UPX

Source: http://upx.sourceforge.net

Ultimate Packer for Executables (UPX) is an executable file compression and decompression utility that supports many executable file formats, including Windows and Linux executables and DLLs.



Process Monitoring Tool: Process Monitor

Source: http://technet.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 a 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. Process Monitor's unique features make it a core utility in the system troubleshooting and malware-hunting toolkit.

Process Monitoring Tool: Process Explorer

Source: http://technet.microsoft.com

Process Explorer shows information about which handles and DLLs processes have opened or loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

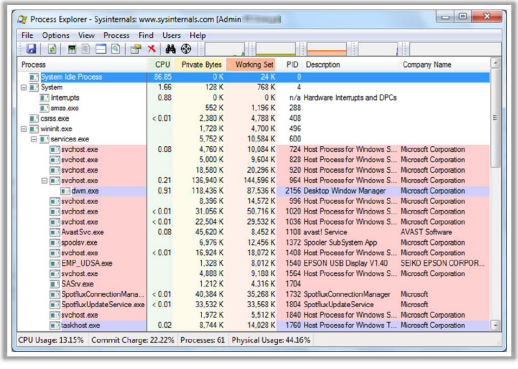
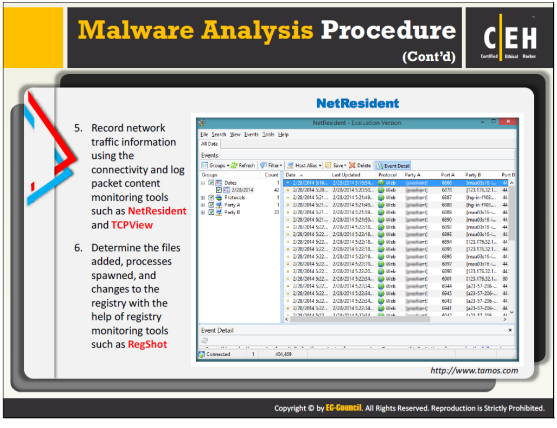


FIGURE 6.10: Screenshot of Process Monitoring Tool - Process Explorer



Connectivity and Log Packet Content Monitoring Tool: NetResident

Source: http://www.tamos.com

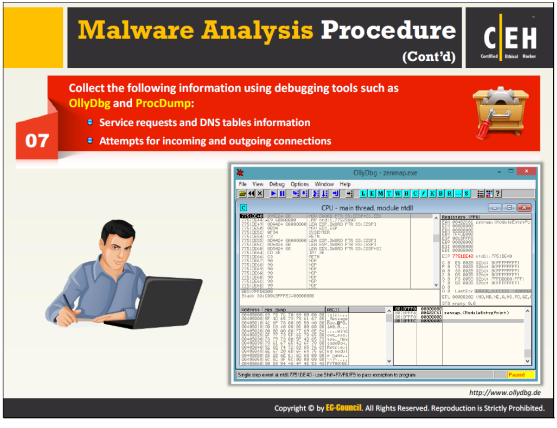
NetResident is a network content analysis application designed to monitor, store, and reconstruct a wide range of network events and activities, such as e-mail messages, Web pages, downloaded files, instant messages, and VoIP conversations. It helps organizations protect sensitive information and enforce security policies as well as adhere to government and industry information protection regulations, by providing event-based network visibility and data leak detection, and reducing the risks associated with uncontrolled information flow.

Connectivity and Log Packet Content Monitoring Tool: TCPView

TCPView is a Windows program that lists details of all TCP and UDP endpoints on the system, including local and remote addresses, and the state of TCP connections.

Registry Monitoring Tool: RegShot

Regshot is an open-source (LGPL) registry compare utility that allows you to take a snapshot of the registry and then compares it to a second one, to be performed after making system changes or installing a new software product.



Debugging Tool: OllyDbg

Source: http://www.ollydbg.de

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

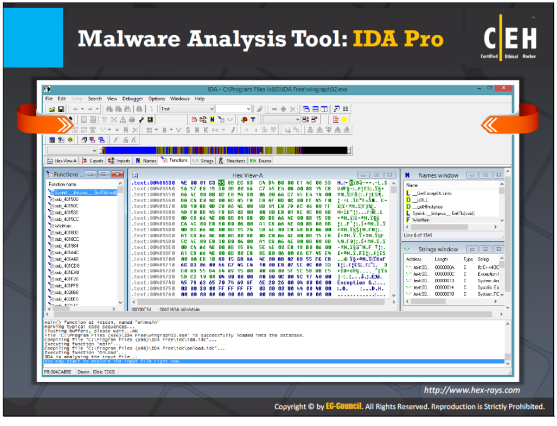
Features:

- Performs code analysis to trace registers, recognizes procedures, loops, API calls, switches, tables, constants, and strings
- Directly loads and debugs DLLs
- Performs object file scanning to locate routines from object files and libraries
- Allows for user-defined labels, comments, and function descriptions
- Understands debugging information in Borland® format
- Saves patches between sessions, writes them back to an executable file, and updates repairs
- Functions as an open architecture, in which many third-party plugins are available

Debugging Tool: ProcDump

Source: *http://technet.microsoft.com*

ProcDump is a command-line utility used to monitor an application for CPU spikes and generate crash dumps during a spike. An administrator or developer can use ProcDump to determine the cause of the spike. ProcDump also includes "**hung window**" monitoring (using the same definition of a "**window hang**" as that of Windows and Task Manager) and unhandled exception monitoring, and can generate dumps according to the values of system performance counters. It also can serve as a general process dump utility that can embed itself in other scripts.



IDA is a Windows, Linux, or Mac OS X hosted multi-processor disassembler and debugger. IDA has become the de facto standard for the analysis of hostile code, vulnerability research, and COTS validation.

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 disembler 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.

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

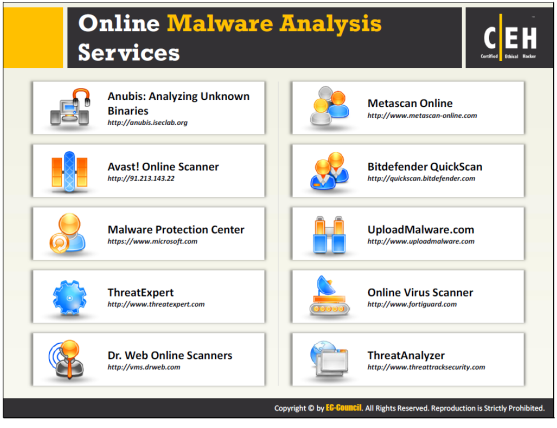
VirusTotal analyzes files and URLs, enabling the identification of viruses, worms, Trojans, and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it can be used to detect false positives (i.e., innocuous resources detected as malicious by one or more scanners).

The mission of VirusTotal is to help improve the antivirus and security industry and make the Internet a safer place through the development of free tools and services.

Features:

- Free and independent service
- Runs multiple antivirus engines and website scanners
- Runs multiple file and URL characterization tools
- Comprised of real-time updates of virus signatures and blacklists
- Gives detailed results from each antivirus engine
- Provides real-time global service operation statistics

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



Malware analysis helps in the understanding of its behavior and the potential severity of the damage it can and does cause. Below is a list of online malware analysis services that one can use to analyze various malware samples.

Anubis: Analyzing Unknown Binaries

Source: *http://anubis.iseclab.org*

Anubis is a tool for analyzing the behavior of Windows PE-executables, with a focus on malware analysis. It generates a report file that contains enough information about the purpose and the actions of the analyzed binary. The generated report includes detailed data about modifications made to the Windows registry or file system, about interactions with the Windows Service Manager or other processes, and of course it logs all generated network traffic.

Avast! Online Scanner

Source: *http://91.213.143.22*

Avast! Online Scanner is an online anti-virus scanner used for malware threats protection. This application tests the file, assesses all the security threats, and provides real time logs of security sweep.

Malware Protection Center

Source: https://www.microsoft.com

The Malware Protection Center is a service provided to protect computers from malware. Users submit the file containing malware or potentially unwanted software, then Microsoft analyzes the file and generates a complete report of its findings.

ThreatExpert

Source: http://www.threatexpert.com

ThreatExpert is an automated threat analysis system designed to analyze and report the behavior of computer viruses, worms, Trojans, adware, spyware, and other security-related risks, in an automated mode.

Dr. Web Online Scanners

Source: http://vms.drweb.com

Dr. Web Online Scanner is an online tool that needs a suspicious file or link to scan. This tool allows file scan, link scan, and virus database search. After the analysis of the suspicious file or links, the tool generates a detailed report of detected viruses, worms, and various kinds of adware, and sends it to the requester.

Metascan Online

Source: http://www.metascan-online.com

Metascan Online is an online file-scanning service powered by OPSWAT's Metascan technology, a multiple engine malware scanning solution.

Bitdefender QuickScan

Source: http://quickscan.bitdefender.com

Bitdefender QuickScan is an online virus scanner that detects hidden threats, malware, and keyloggers. It uses in-the-cloud scanning technology to detect active malware on a system.

UploadMalware.com

Source: http://www.uploadmalware.com

UploadMalware.com is a service that allows you to submit files for analysis by anti-malware and security professionals.

Online Virus Scanner

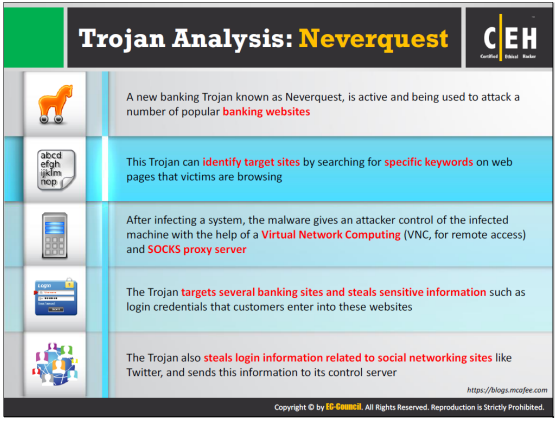
Source: http://www.fortiguard.com

This online tool allows scanning a suspicious file discovered on the machine or a suspicious malicious program downloaded from the Internet.

ThreatAnalyzer

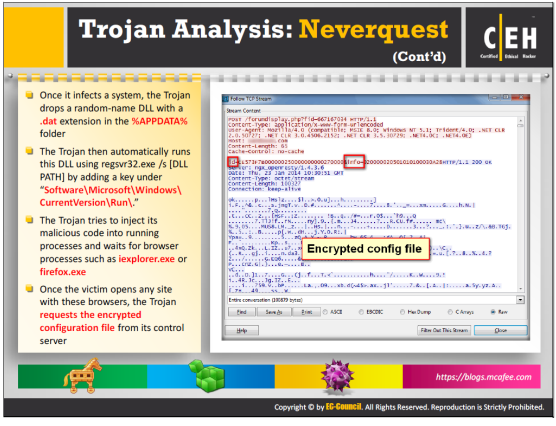
Source: http://www.threattracksecurity.com

ThreatAnalyzer is a malware analysis tool that provides defense against Advanced Persistent Threats (APTs), Zero-days, and custom-targeted attacks. This tool analyzes malware samples, generates report analyses to aid in the understanding of each threat, and improves response time to remediate threats.



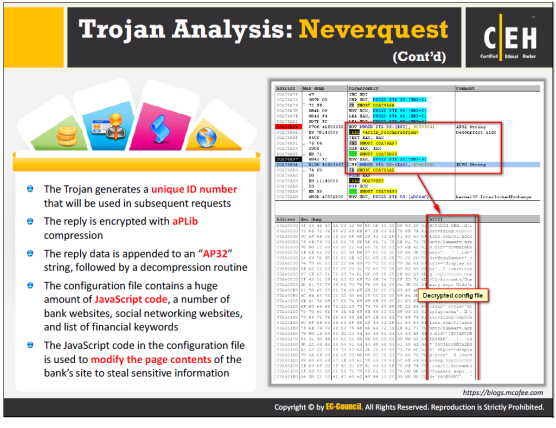
A new banking Trojan, known as Neverquest, is currently active and has attacked a number of popular banking websites. Neverquest can identify target sites by searching for specific keywords on web pages that victims are browsing. After infecting a system, it gives an attacker control of the infected machine with the help of a Virtual Network Computing (VNC, for remote access) and SOCKS proxy server. The Trojan targets several banking sites and steals sensitive information such as login credentials that customers submit to these sites. The Trojan also steals login information related to social networking sites (listed in the configuration file) like Twitter, and sends this information to its control server.

Source: *https://blogs.mcafee.com*



Once it infects a system, the Trojan drops a random-name DLL with a **.dat** extension in the **%APPDATA%** folder. The Trojan then automatically runs this DLL using "regsvr32.exe /s [DLL PATH]" by adding a key under "**Software\Microsoft\Windows\CurrentVersion\Run**." The Trojan tries to inject its malicious code into running processes and waits for browser processes such as **iexplorer.exe** or **firefox.exe**. Once the victim opens any site with these browsers, the Trojan requests the encrypted configuration file from its control server, as shown in the screenshot on the slide above.

Source: *https://blogs.mcafee.com*



The Trojan generates a unique ID number that the system uses in subsequent requests. **aPLib** compression encrypts the reply and it is appended to an "**AP32**" string, followed by a decompression routine, as shown in the slide.

The configuration file contains a huge amount of JavaScript code, a number of bank websites, social networking websites, and list of financial keywords. One can use the JavaScript code in the configuration file to modify the page contents of the bank's site to steal sensitive information.

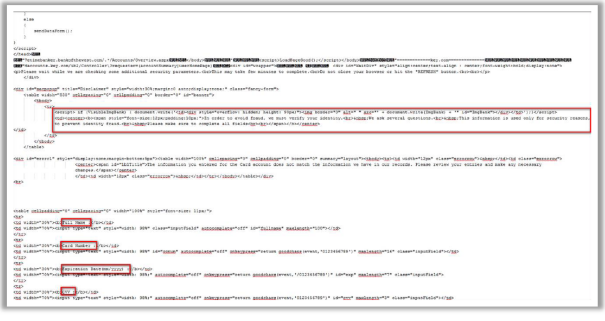


FIGURE 6.11: Screenshot showing JavaScript code in the config file of Neverquest

The Trojan targets financial institutions, including Bank of America, Citibank, and many others. Here is a list of target sites found in the decrypted configuration file:

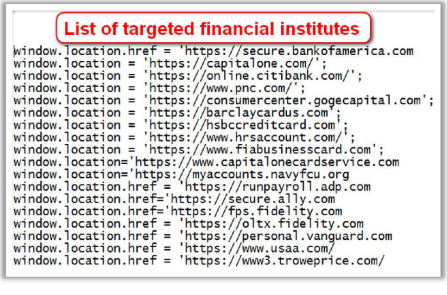
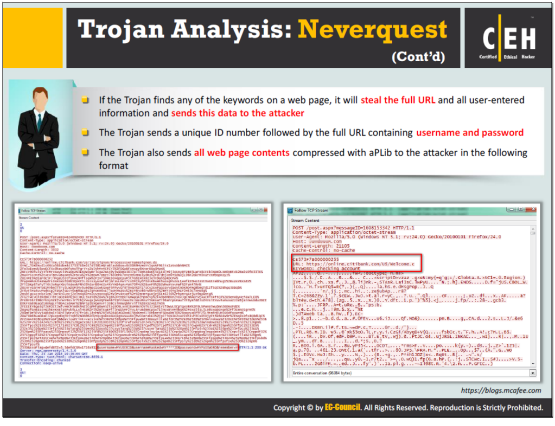


FIGURE 6.12: Screenshot showing the list of websites targeted by Neverquest

The Trojan asks for sensitive information by modifying the page contents that a victim visits. The configuration file also contains a list of social networking sites and a list of keywords related to banking.

FIGURE 6.13: Screenshot highlighting various keywords and websites targeted by Neverquest

Source: *https://blogs.mcafee.com*



If the Trojan finds any of the keywords on a web page, it will steal the full URL and all user-entered information and sends this data to the attacker. The Trojan sends a unique ID number followed by the full URL containing username and password. The Trojan also sends all web page contents compressed with aPLib to the attacker.

The Trojan steals information entered on social networking sites listed in the configuration file and can use that data to further spread the malicious code.

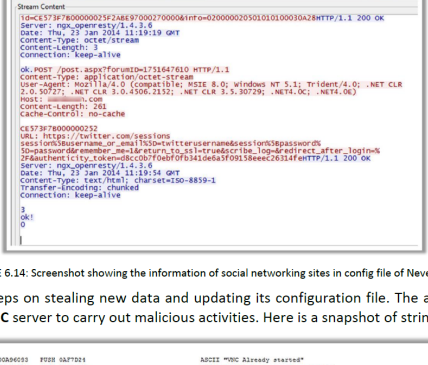


FIGURE 6.14: Screenshot showing the information of social networking sites in config file of Neverquest

The Trojan keeps on stealing new data and updating its configuration file. The attacker uses a **SOCKS** and **VNC** server to carry out malicious activities. Here is a snapshot of strings found:

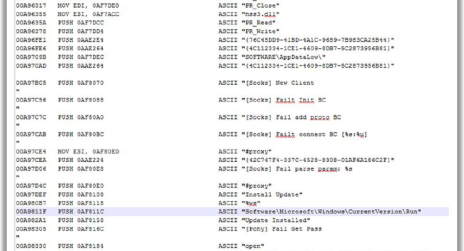


FIGURE 6.15: Screenshot showing information on the attackers VNC Server (1 of 2)

The Trojan can steal **SMTP** (Simple Mail Transfer Protocol) and **POP** (Post Office Protocol) credentials from email clients. It can also steal FTP login credentials from various programs that help to distribute the malicious code.

FIGURE 6.16: Screenshot showing information on the attackers VNC Server (2 of 2)

Also an updated configuration file that contains code to request additional JavaScript files targeting financial sites such as **BMO** (Bank of Montreal), **PayPal**, **RBC** (Royal Bank of Canada), and others from a different malicious server is found. The malicious server has several web panels for collecting sensitive information from different financial sites—which shows that attackers are learning and creating new fake pages for new sites. Given below is a sample JavaScript code.

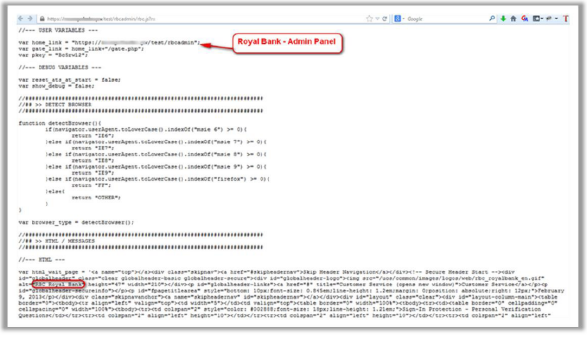


FIGURE 6.17: Screenshot highlighting information about a bank in the JavaScipt code of Neverquest

Victims' browsers display the preceding JavaScript code once they visit these sites. There are many banking Trojans, but Neverquest has more capabilities than most. Attackers can hide their tracks with the help of proxy and remote control and can carry out transactions from the infected machines. The Trojan can search for new banking sites with the help of financial keywords listed in the configuration file. The Trojan can also steal new banking URLs and their page contents, which eventually update its configuration file. In this way, Neverquest can grow its target database to carry out future attacks.

Source: *https://blogs.mcafee.com*

Below is the analysis of some famous Trojans of recent time:

Analysis of Flame Trojan

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

Flame, also known as **Flamer**, **sKyWIper**, or **Skywiper**, is a type of modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. Using Flame, an attacker can engage in cyber-espionage on Middle Eastern targets. It can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity, and network traffic. Flame also records Skype conversations and can turn infected computers into Bluetooth beacons that attempt to download contact information from nearby Bluetooth-enabled devices. The following diagram depicts how an attacker succeeds in installing Flame on a victim's system.

FIGURE 6.18: Screenshot is explaining how attacker installs Flame Trojan on the victim's system

The attacker injects malware (a virus, Trojan horse, etc.) onto the victim's system to gain sensitive data. To perform the attack successfully, the attacker first sets a command and control center and a malware server. Next, the attacker sends a phishing mail to the victim's system and lures him or her to open the link. Once the victim opens the link, it redirects him/her to the malicious server. As a result, the victim's system downloads the malware that infects his/her system. This infected machine infects the other hardware connected in the LAN. The command and control center sends the commands to the infected hardware in LAN. According to the received commands, the infected hardware in LAN sends the data to the command and control center that in turn sends the command to the attacker.

Kaspersky Lab summarizes the results of the analysis about Flame as follows:

- The Flame C&C infrastructure, which had been operating for years, went offline immediately after Kaspersky Lab disclosed the discovery of the malware's existence.
- Currently, there are more than 80 known domains used by Flame for C&C servers and its related domains, which have been registered between 2008 and 2012.
- During the past four years, servers hosting the Flame C&C infrastructure moved between multiple locations, including Hong Kong, Turkey, Germany, Poland, Malaysia, Latvia, the United Kingdom, and Switzerland.

- The Flame C&C domains were registered with an impressive list of fake identities and with a variety of registrars, going back as far as 2008.
- According to Kaspersky Lab's sinkhole, infected users were registered in multiple regions, including the Middle East, Europe, North America, and Asia-Pacific.
- The Flame attackers seem to have a high interest in PDFs, Office, and AutoCad drawings.
- Simple algorithms encrypt the data uploaded to the Flame C&C. Stolen documents are compressed using open source Zlib and modified PPDM compression.

The Windows 7 64-bit OS, which we previously recommended as a good solution to guard against infection from other malware, also seems to be effective in guarding against Flame.

Flame's C&C Server was running on 64-bit Debian 6.0.x OS under OpenVZ and using PHP, Python, and MySQL database on Apache 2.x web server with self-signed certificates. This server configuration was a typical LAMP (Linux, Apache, MySQL, and PHP) setup. It is useful to host a web-based control panel as well as to run some scheduled fully automated scripts in the background.

It was accessible over the HTTPS protocol, ports 443 and 8080. The document root directory was "**/var/www/htdocs/**," which has subdirectories and PHP scripts. While the system installs the PHP5, it generates the code that can run on PHP4 as well. For example, **/var/www/htdocs/newsforyou/Utils.php** has the "**str_split**" function defined that implements the "**str_split**" function logics from PHP5, which was not available in PHP4. The development of the C&C code most likely implemented compatibility with PHP4, because they were not sure which one of two major PHP versions would be installed on the C&Cs.

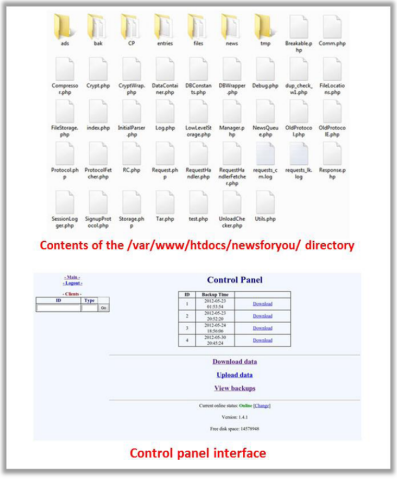


FIGURE 6.19: Screenshot showing root directory contents and Control panel interface of Flame C&C Server

C&C can understand several communication protocols, including **OldProtocol**, **OldProtocolE**, **SignupProtocol**, and **RedProtocol** to talk to different client's codenamed SP, SPE, FL, and IP. A typical client session handled by the C&C started from recognition of the protocol version, then logging of connection information, followed by decoding client request and saving it to the local file storage in encrypted form. All metadata about the files received from the client was kept in a MySQL database. The C&C script encrypts all files received from the client. The C&C uses a PGP-like mechanism to encrypt files. First, the user encrypts file data using the Blowfish algorithm in CBC mode (with static IV). The tool randomly generates the Blowfish key for each file. After file encryption, the tools encrypts Blowfish key with a public key using asymmetric encryption algorithm from the **openssl_public_encrypt PHP** function.

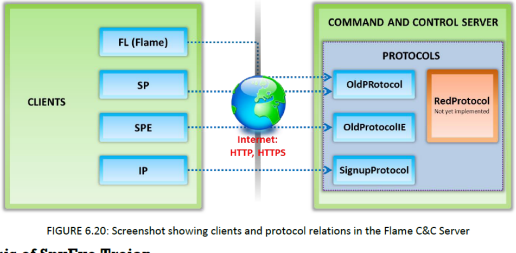


FIGURE 6.20: Screenshot showing clients and protocol relations in the Flame C&C Server

Analysis of SpyEye Trojan

Source: http://techblog.avira.com

The Trojan makes use of user mode rootkit techniques to hide both its registry key located inside **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run** and the folder containing the Trojan executable and the configuration file **config.bin**. The folder is usually located in the root directory of the drive where the operating system is located.

SpyEye is able to inject code in running processes and can perform the following functions:

- Capture network traffic
- Send and receive network packets in order to bypass application firewalls
- Hide and prevent access to the startup registry entry
- Hide and prevent access to the binary code
- Hide the own process on injected processes
- Steal information from Internet Explorer and Mozilla Firefox

The following API functions are hooked by the Trojan within the **winlogon.exe** virtual address space:

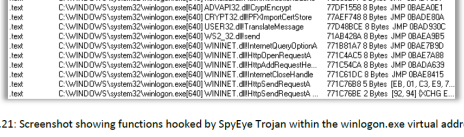


FIGURE 6.21: Screenshot showing functions hooked by SpyEye Trojan within the winlogon.exe virtual address space

After execution, the Trojan connects to a server and sends some information about the system to the server, such as:

- MD5 of the executed sample
- Operating system version
- Computer name
- Internet Explorer version
- User name
- Version number of the malware

FIGURE 6.22: Screenshot showing malware injected code within winlogon.exe virtual address space

Malware contains UPX and a polymorphic decryptor. In the code snippet that follows, you can see a call to another routine after the end of the usual UPX decryption: **call sub_42F851**.

```
push    35417Ah
push    eax
push    4A65474Bh
push    4969h
push    3367h
push    50A7h
lea     ecx, [ebp-1Ch]
push    ecx
push    dword ptr [ebp-0Ch]
push    dword ptr [ebp-10h]
call    sub_42F851
leave
retn
```

FIGURE 6.23: Screenshot showing the malware packed with UPX and a polymorphic decryptor

Analysis of ZeroAccess Trojan

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

ZeroAccess, also known as "**Smiscer**" or "**Max++ rootkit**," is a malicious Windows threat used to generate revenue primarily through pay-per-click fraud. ZeroAccess uses low-level rootkit functionality to remain persistent and stealth. It arrives through various vectors, including web exploit kits and social engineering attacks. Although ZeroAccess contains generic backdoor multiple purpose functionality, it has been observed downloading fake security software, performing click fraud, and searching-engine poisoning.

Click fraud scheme

Upon infection, ZeroAccess will install additional payload modules, downloaded through its back door. Generally, this is an executable that performs click fraud. This click fraud scheme utilizes more than one pay-per-click affiliate network.

Advertisers sign up with ad networks that in turn contract website owners who are willing to display advertisements on their websites in exchange for a small commission. The ad networks charge the advertisers for distributing and displaying their ads and pay the website owners a small commission each time a visitor views (pay-per-view) or clicks (pay-per-click) on the ads.

FIGURE 6.24: Screenshot showing an example advertisement of ClickIce pay-per-click network for ZeroAccess Trojan

In addition to generating revenue through pay-per-click networks, ZeroAccess hijacks users' searches. When an infected user searches in popular search engines (including google.com, bing.com, icq.com, yahoo.com, ask.com, and aol.com), ZeroAccess sends an additional GET request similar to the following:

http://suzukimxm[.]cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&sv=15&os=501.804.x86

This creates an additional pop-up window or tab. The new window or tab will contain search results for the original search query with hijacked links or additional content. The figure below shows an example of returned HTML.

```
1: <jat>

2:  function FormatRedirect(ref,
    title) { body = "<html><head>
    <title>" + title + "</title>
    </head><frameset><frame src=\
    "http://" + ref + "\">
    </frameset></html>";

3:  AddPage("www.google.com.hk/
    search?q=car&hl=zh-CN&source=
    hp&gbv=1",2,null, 0, "HTTP/1.1
    200\r\nConnection: close\r\
    nCache-Control: no-cache\r\
    nPragma: no-cache\r\nContent-
    Length: " + body.length +
    "\r\n\r\n" + body);

4:  }

5:  FormatRedirect("kozenekozasearchsys
    tem.com/?search=car&subid=198&key=4
    15db60c8aa81c
    0bed68", "car");
```

FIGURE 6.25: Screenshot showing an example of returned HTML for a search result

Users can also install ZeroAccess through web exploit kits. The user is often falsely given the impression that they will be installing an update for an application, such as Adobe Flash player. This use of various exploit kits to install ZeroAccess is likely simply a byproduct of its authors attempting to evade IPS rather than an indication of ZeroAccess being sold to other distributors.

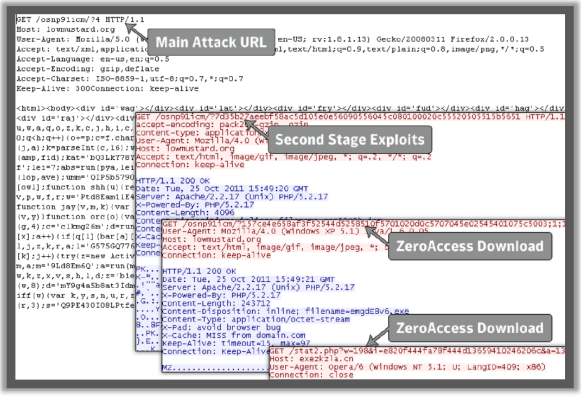


FIGURE 6.26: Screenshot showing exploit kit dropping ZeroAccess Trojan

Upon execution, ZeroAccess selects a random driver alphabetically between `%System%\Drivers\classpnp.sys` and `%System%win32k.sys` and overwrites the driver with its own code.

The original clean driver is stored in a hidden encrypted NTFS volume using the file name `%System%\config\<RANDOM CHARACTERS>`.

The users can use hidden volume to store the original clean driver as well as additional components and downloaded payload modules. The volume is roughly 16 MB in size, and is accessible through the file system device name:

`\\??\ACPI#PNP0303#2&da1a3ff&0`

For example, the original clean driver is stored at:

`\\??\ACPI#PNP0303#2&da1a3ff&0\L\[EIGHT RANDOM CHARACTERS]`

The system uses RC4 algorithm to encrypt the file system of the hidden volume with the following 128-bit key:

`\xFF\x7C\xF1\x64\x12\xE2\x2D\x4D\xB1\xCF\x0F\x5D\x6F\xE5\xA0\x49`

The Trojan then creates the following registry entries to ensure the newly infected driver serves as the main load point for ZeroAccess:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"ImagePath" = "\*"`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Type" = "1"`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Start" = "3"`

The system then injects the Code into services.exe through an APC. The injected code encrypts the data stored in the hidden NTFS volume under `\??\ACPI#PNP0303#2&da1a3ff&0\U` and also creates an alternate data stream file `%SystemDrive%\2385299062:2302268273.exe` and executes it. These main loader components ensure the additional payload files stored in the hidden NTFS volume are loaded and executed.

Analysis of Duqu Trojan

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

Duqu is a sophisticated Trojan that acts as a backdoor and facilitates the theft of private information. The code section of the Payload DLL is common for a binary that was made from several pieces of code. It consists of "**slices**" of code that may have been initially compiled in separate object files before they were linked in a single DLL. Most of them can be found in any C++ program, like the Standard Template Library (STL) functions, run-time library functions, and user-written code, except for the biggest slice, which contains most of the C&C interaction code.

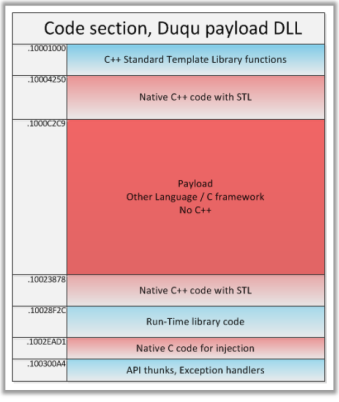


FIGURE 6.27: Screenshot of Duqu Trojan

This slice is different from others, because its compilation does not include C++ sources. It contains no references to any standard or user-written C++ functions, but is definitely object-oriented. It is called the Duqu Framework.

Duqu Framework Code Properties

The code that implements the Duqu Framework has several distinctive properties:

- Everything is wrapped into objects.
- The Function table is placed directly into the class instance and can be modified after construction.
- There is no distinction between utility classes (linked lists, hashes) and user-written code.
- Objects communicate using method calls, deferred execution queues and event-driven callbacks.
- There are no references to run-time library functions; the native Windows API is used instead.

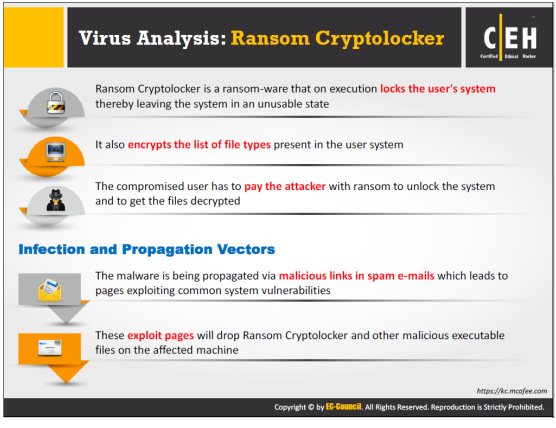
Event-Driven Framework

The layout and implementation of objects in the Duqu Framework is definitely not native to C++ that contributed in programming the rest of the Trojan. There is an even more interesting

feature of the framework that is used extensively throughout the whole code; namely, it is Event-Driven.

There are special objects that implement the event-driven model:

- Event objects based on native Windows API handles
- Thread context objects that hold lists of events and deferred execution queues
- Callback objects linked to events
- Event monitors, created by each thread context for monitoring events and executing callback objects
- Thread context storage manages the list of active threads and provides access to per-thread context objects

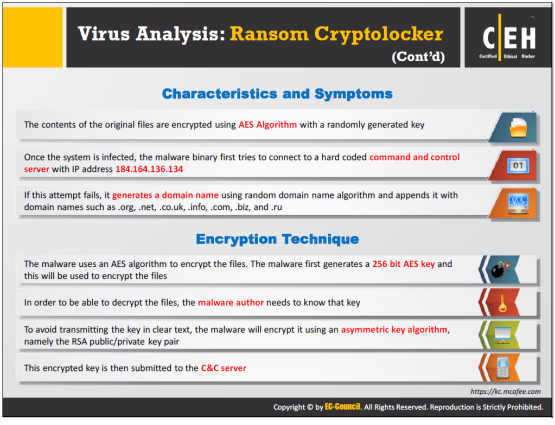


Ransom Cryptolocker is ransomware that, on execution, locks the user's system, thereby leaving the system in an unusable state. It also encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. The compromised user has to pay the attacker with the ransom to unlock the system and get the files decrypted. It targets systems running Microsoft Windows.

Infection and Propagation Vectors

The malware propagates via malicious links in spam emails, which leads to pages exploiting common system vulnerabilities. These exploits pages will drop Ransom Cryptolocker and other malicious executable files on the affected machine.

Source: *https://kc.mcafee.com*



Characteristics and Symptoms

Ransom Cryptolocker belongs to a family of malware that encrypts the compromised user files available in the system and demands the user to pay ransom to retrieve the files. The contents of the original files are encrypted using AES algorithm with a randomly generated key. After the system is infected, the malware binary first tries to connect to a hard-coded command and control server at IP address 184.164.136.134. If this attempt fails, it generates a domain name using a random domain name algorithm and appends it with one of the following domain names: .org, .net, .co.uk, .info, .com, .biz, .ru.

After the system initiates the communication with the remote C&C server, the malware binary proceeds to the next step, which is to encrypt the compromised user files in the system. After generating the AES encryption key and submitting it to the C&C server, the malware binary searches for the below mentioned file types in the user system fixed and removable devices.

*.odt	*.xls	*.pst	img_*.jpg	*.mrf	*.cer
*.ods	*.xlsx	*.dwg	*.dng	*.nef	*.crt
*.odp	*.xlsm	*.dxf	*.arw	*.nrw	*.pem
*.odm	*.xlsb	*.dxg	*.srf	*.orf	*.pfx
*.odc	*.xlk	*.wpd	*.bay	*.raf	*.eps
*.odb	*.ppt	*.rtf	*.crw	*.raw	*.indd
*.doc	*.pptx	*.mdf	*.dcr	*.ptx	*.cdr
*.docx	*.pptm	*.dbf	*.kdc	*.pef	????????.jpg
*.docm	*.mdb	*.psd	*.erf	*.srw	????????.jpe
*.wps	*.accdb	*.pdd	*.mef	*.der	

FIGURE 6.28: Screenshot displaying a list of file types encrypted by Ransom Cryptolocker

Encryption Technique

The malware uses an AES algorithm to encrypt files. The malware first generates a 256-bit AES key that encrypts the files. To be able to decrypt files, the malware author needs to know that key. To avoid transmitting the key in clear text, the malware will encrypt it using an asymmetric key algorithm, namely the RSA public/private key pair. The unique RSA public key created by the malware author and present in the malicious executable encrypts the newly generated AES key. This encrypted key is then submitted to the C&C server. The only way to recover the key after the malware finishes executing is by having the RSA private key associated with the public key used. Only the malware author knew the key, and he never transmits it via the network or present in the infected machine. Hence, it is impossible to recover the user's encrypted files without that key.

Source: *https://kc.mcafee.com*

Ransom Cryptolocker shows the warning to the user and demands ransom to decrypt the files for a compromised system.

It maintains the list of files encrypted by this malware under the following registry entry:

HKEY_CURRENT_USER\Software\CryptoLocker\Files

On execution, this malware binary copies itself to **%AppData%** location and deletes itself using a batch file:

%AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe

NOTE: **%AppData%** refers to the current user's Application data location.

The malware author receives the ransom amount from the compromised user from one of the following payment methods:

- moneypak
- ukash
- cashu
- bitcoin

Network Connections

Cryptolocker uses the DGA (Domain Generation Algorithm) to generate the Random Domain names hourly.

Shown below are some of the observed domains of the C&C servers:

soudpmiyvxmd.org	wxfaxwfotkcp.co.uk	avlpfgiqwdudk.info	irvggrirvsqqy.com
gbpboroxfiep.co.uk	xvaqocjidsht.info	ngmneoxxoisqk.com	jnwsjavtnkvmh.net
ofoauksakmgs.info	soywduppiyvf.com	udsmjlwhfkmeg.net	dyddkwwieairg.biz
crjxtpyytwxf.com	tmtntatjrhbj.net	intkitmowpkrw.biz	euepnfkkvrnnf.ru
qgyvutxttqaj.net	upjsdeujrdpv.biz	vlqtsbjlaojjg.ru	ehbktmjmyefwg.org
estttyesdbrv.biz	vnejtjydblua.ru	jvrrrjysrthwg.org	fdcwwuwoqvkso.co.uk
uwuexnaukgiy.ru	ynnivqvmcyxxr.org	hjxywcvnbotlg.co.uk	fxcyhrpfigvcu.info
vupuoseotond.org	mxoguylttevli.co.uk	ifylakjpsgyhf.info	sidwgwvsyqlxu.com
hdauthcpbwblw.net	oxibtrwnccaej.org	ntmpidpuhvjxm.com	pykluscfamoho.biz
unbssmidrhqhn.biz	dsfyhcdkeiprs.co.uk	opncliitaxswlu.net	qulxxxgkqjcun.ru
bnhdumqalrkij.ru	qdgwghjxusfnj.info	igemsolqdaotb.org	jjrtvxqpkhxem.org
loppindadxdnv.info	mkqclshftuqbu.com	tnfhkwqywydsb.net	hxgfjfggoebgr.biz
uvdotgvjluqgb.ru			

FIGURE 6.29: Screenshot showing some of the domains of the C&C servers

Restart Mechanism:

The following registry entry would enable the Trojan to execute every time Windows starts:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

CryptoLocker "%AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe"

Source: *https://kc.mcafee.com*

Virus Analysis: DNSChanger

DNSChanger, also known as **Alureon**, is a high-profile piece of malware that modifies the DNS settings on the victim PC to divert Internet traffic to malicious websites in order to generate fraudulent ad revenue, sell fake services, or steal personal financial information. It also acts as a robot (or "**bot**") and can be organized into a botnet and controlled from a remote location. DNSChanger has received significant attention due to the large number of affected systems worldwide, and the fact that, as part of the botnet takedown, the FBI took ownership of the rogue DNS servers to ensure that those affected did not immediately lose the ability to resolve DNS names.

The most common vector of malware distribution is email and social engineering. Some of the sources of malware in the market are "**malvertisements**" such as fake codecs to play videos and untrusted free software downloads, both of which are known sources of malware. DNSChanger is available for the MAC OSX platform as well as for Windows (**OSX/Puper** and **OSX/Jahlav**).

In the Network settings of the computer OS is a DNS server entry, which malware modifies; the user resets it after removing the malware. The malicious DNS server fields the resolution request and sends you the IP address of its choosing. Thus, it is now possible to capture internet traffic originating from an infected PC before sending on to the original destination.

On Windows: A regular DNS Changer malware achieves the redirection by modifying the following registry key settings against an interface device, such as a network card:

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

Such malware makes modifications to lower Internet-security settings related to security zones registry keys. This enables unprompted access to malicious sites that would otherwise raise alarm for users through notifications.

On Macintosh: After removal of the malicious binary, the settings can be reverted via network settings.

To verify DNS settings, open the Network Settings GUI, and check the Internet Protocol Version 4 properties. On the "**General**" tab, review the "**Preferred**" and "**Alternate**" DNS server IP addresses. The rogue DNS servers can occur in any of the following ranges:

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

Another means of determining the DNS server IP addresses in use is to open a command prompt via "**Start Menu/All Programs/Accessories/Command Prompt**". When the black box opens, enter "**ipconfig /all**" and scroll through the text to find the section entitled "**DNS Servers**." DNSChanger lists the entire DNS server IP addresses currently in use. If the network is configured using DHCP, DNSChanger also helps in determining the DNS server IP addresses.

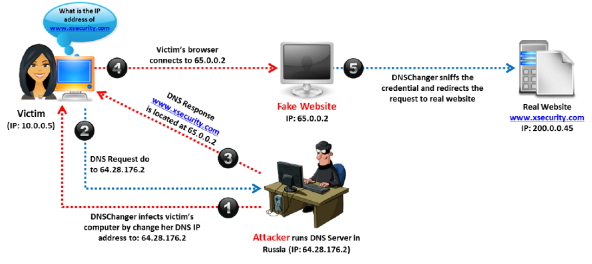
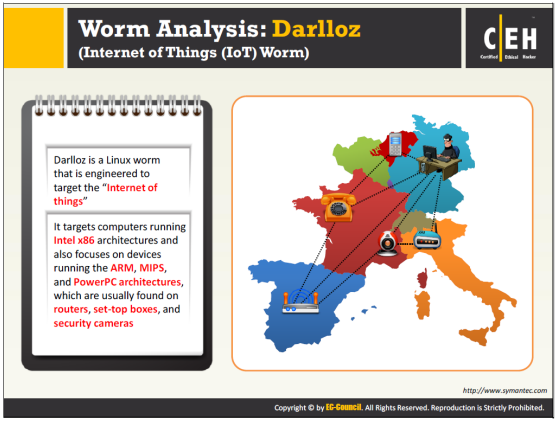


FIGURE 6.30: Snapshot showing the working of DNSChanger

To infect the system and steal credentials, the attacker has to first run DNS server.

In the diagram above, the attacker runs his or her DNSserver in Russia with an IP of, say, 64.28.176.2. Next, the attacker infects the victim's computer with DNSChanger that changes her DNS IP address to 64.28.176.2. Now all DNS requests made by the victim redirected to the DNSserver run by the attacker. Here, the victim sends DNS Request "what is the IP address of www.xsecurity.com" that is directed to the attacker DNS server (64.28.176.2). The attacker then gives response to the request as www.xsecurity.com is located at the IP address 65.0.0.2. When a victim's browser connects to 65.0.0.2, it redirects her to a fake website created by the attacker with IP: 65.0.0.2. Thereafter, DNSChanger sniffs the credentials (user name, passwords) and redirects the request to real website (www.xsecurity.com) at IP: 200.0.0.45.

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



Darlloz worm attacks specially Linux operating systems running on Intel x86 architectures. Not only that, but the worm also focuses on devices running the ARM, MIPS, and PowerPC architectures, which are usually found on routers and set-top boxes.

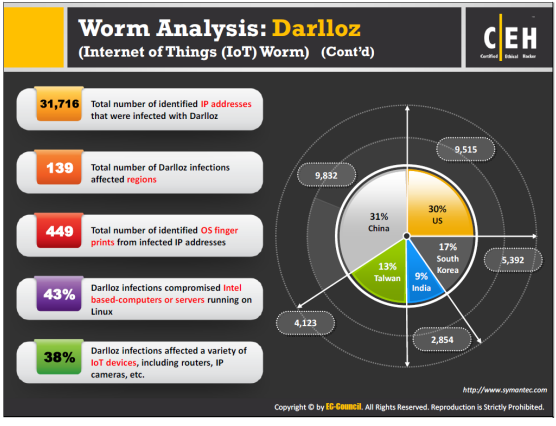
The current purpose of the worm is to mine crypto-currencies. Once the Dalloz worm infects a computer running on Intel architecture, the worm installs cpuminer, an open source coin mining software. The worm then starts mining Mincoins or Dogecoins on infected computers.

The reason for the worm aiming at mining Mincoins and Dogecoins, rather on focusing on the well-known and more valuable crypto-currency Bitcoin is that Mincoin and Dogecoin uses the scrypt algorithm, which can still mine successfully on home PCs whereas Bitcoin requires custom ASIC chips to be profitable.

The **Internet of Things** (IoT) is all about connected devices of all types. Unlike regular computers, a lot of IoT devices ship with a default user name and password and many users may not have changed these. As a result, the use of default user names and passwords is one of the top attack vectors against IoT devices. Many of these devices also contain unpatched vulnerabilities users are unaware of. Although this particular threat focuses on computers, routers, set-top boxes and IP cameras, the worm could be updated to target other IoT devices in the future, such as home automation devices and wearable technology.

Darlloz prevents other attackers or worms from targeting devices already compromised by it. This is by implementing a feature to block the access to the back door port by creating a new firewall rule on infected devices, to ensure that no other attackers can get in through the same back door.

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

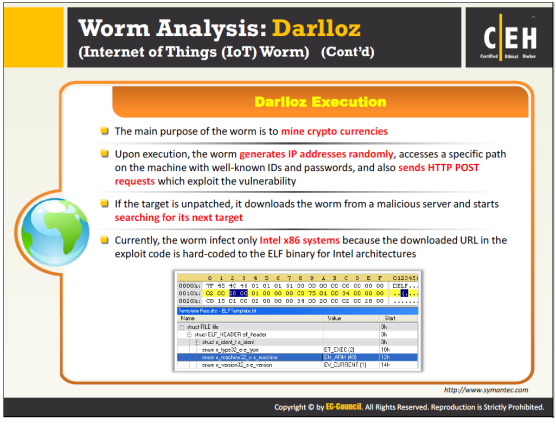


Once a device is infected by Darlloz worm, it starts a HTTP Web server on port 58455 in order to spread. The server hosts worm files and allows anyone to download files through this port by using a HTTP GET request. Symantec searched for IP addresses that open the port and host Darlloz files on static paths. Assuming that the Darlloz worm had already downloaded, Symantec tried to collect some OS fingerprints of the host server. Given below is the statistics that provide an overview of the infection.

- Symantec identified 31,716 IP addresses infected with Darlloz.
- Darlloz infections affected 139 regions. There were 449 identified OS fingerprints from infected IP addresses.
- 43% of Darlloz infections compromised Intel-based computers or servers running on Linux.
- 38% of Darlloz infections seem to have affected a variety of IoT devices, including routers, set-top boxes, IP cameras, and printers.

The five regions that accounted for 50 percent of all Darlloz infections were China (31%), the United States (30%), South Korea (17), Taiwan (13), and India (9%). The reason for the high infections in these regions is most likely because of their large volumes of Internet traffic and users or the penetration of IoT devices.

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



Upon execution, the worm generates IP addresses randomly, accesses a specific path on the machine with well-known IDs and passwords, and sends HTTP POST requests which exploit the vulnerability. If the target is unpatched, it downloads the worm from a malicious server and starts searching for its next target. Currently, the worm seems to infect only Intel x86 systems, because the downloaded URL in the exploit code is hard-coded to the ELF binary for Intel architectures.

Linux is the best-known open-source operating system of any architecture. Linux not only runs on Intel-based computers, but also on small devices with different CPUs, such as home routers, set-top boxes, security cameras, and even industrial control systems. Some of these devices provide a Web-based user interface for settings or monitoring, such as Apache Web servers and PHP servers.

Symantec has also verified that the attacker already hosts some variants for other architectures, including ARM, PPC, MIPS, and MIPSEL on the same server.

Home routers, set-top boxes, security cameras, etc. use this kind of architecture. The attacker is apparently trying to maximize the infection opportunity by expanding coverage to any devices running on Linux. However, attacks against non-PC devices have not yet been confirmed.

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

Worm Analysis: Stuxnet

Stuxnet is a large, complex piece of malware with many different components and functionalities. It is a threat mainly written to target an industrial control system or set of similar systems; for example, Gas pipelines and power plants use industrial control systems. Its final goal is to reprogram **industrial control systems** (ICS) by modifying the code on **programmable logic controllers** (PLCs), to make them work in a manner the attacker intended and hide those changes from the operator of the equipment. To achieve this goal, its creators amassed a vast array of components to increase their chances of success, including zero-day exploits, a Windows rootkit, the first ever PLC rootkit, anti-virus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.

Features:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
- Spreads in a LAN through a vulnerability in the Windows Print Spooler
- Spreads through SMB by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
- Copies and executes itself on remote computers through network shares
- Copies and executes itself on remote computers running a WinCC database server
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded
- Updates itself through a peer-to-peer mechanism in a LAN
- Exploits a total of four unpatched Microsoft vulnerabilities two of which are vulnerabilities for self-replication and the other two are escalation of privilege vulnerabilities
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions
- Contains a Windows rootkit that hide its binaries
- Attempts to bypass security products
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system
- Hides modified code on PLCs, essentially a rootkit for PLCs

The complex architecture of stuxnet is described below:

The heart of Stuxnet consists of a large .dll file that contains many different exports and resources and two encrypted configuration blocks. The dropper component of Stuxnet is a wrapper program that contains all components stored inside itself in a section name “stub.” This stub section is integral to the working of Stuxnet. The wrapper extracts the .dll file from the

stub section, maps it into memory as a module, and calls one of the exports after the execution of the threat. A pointer to the original stub section is passed to this export as a parameter. With reference to the passed parameter, this export in turn extracts the .dll file from the stub section, map it into memory and call another different export from inside the mapped .dll file. The pointer to the original stub section is again passed as a parameter. This occurs continuously throughout the execution of the threat, so the original stub section is continuously passed around between different processes and functions as a parameter to the main payload. In this way every layer of the threat always has access to the main .dll and the configuration blocks.

In addition to loading the .dll file into memory and calling an export directly, Stuxnet also uses another technique to call exports from the main .dll file. This technique is to read an executable template from its own resources, populate the template with appropriate data, such as which .dll file to load and which export to call, and then inject this newly populated executable into another process and execute it. The newly populated executable template will load the original.dll file and call whatever export with which the template was populated.

Exports

As stated earlier, the main .dll file contains all of the code to control the worm. Each export from this .dll file has a different purpose in controlling the threat.

Resources

The main .dll file also contains many different resources that the exports use in the course of controlling the worm. The resources vary from full .dll files to template executables to configuration files and exploit modules.

DLL Exports

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstall Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection
27	RPC server
28	Command and Control routine
29	Command and Control routine
31	Updates itself from infected Step 7 projects
32	Same as 1

DLL Exports and their respective functions in controlling the Threat

DLL Resources

Resource ID	Function
201	MrxNetLnp load driver, signed by RealTek
202	DLL for Step 7 infections
203	Cab file for WinCC infections
205	Data file for resource 201
207	Autorun version of Stuxnet
208	Step 7 replacement DLL
209	Data file (%windows%\help\oem.cfg)
210	Template .tmp file used for injection
221	Exploits MS08-067 to spread via SMB
222	Exploits MS10-061 Print Spooler Vulnerability
231	Internet connection check
240	LNK template file used to build LNK exploit
241	USB Loader DLL "WTR4141.tmp
242	MRxNet.sys rootkit driver
250	Exploits Windows win32k.sys Local Privilege Escalation (MS10-073)

DLL Resources and their respective functions

FIGURE 6.31: Screenshot showing various DLL Exports and DLL Resources along with their respective functions

Bypassing Behavior Blocking When Loading DLLs

Whenever Stuxnet needs to load a DLL, including itself, it uses a special method designed to bypass behavior blocking and host intrusion-protection-based technologies that monitor Load Library calls.

Stuxnet calls Load-Library with a specially crafted file name that does not exist on disk and normally causes Load-Library to fail. However, W32.Stuxnet has hooked Ntdll.dll to monitor for requests to load specially crafted file names.

These specially crafted filenames are mapped to another location instead—a location specified by W32.Stuxnet. That location is generally an area in memory where the threat had decrypted and stored the .dll file.

The filenames used have the pattern of **KERNEL32.DLL.ASLR.[HEXADECIMAL]** or **SHELL32.DLL.ASLR.[HEXADECIMAL]**, where the variable **[HEXADECIMAL]** is a hexadecimal value.

The functions hooked for this purpose in **Ntdll.dll** are:

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

Once a .dll file has been loaded, **GetProcAddress** finds the address of a specific export from the .dll file and recollects that export, handling control to that new .dll file.

Injection Technique

Whenever the programs call an exploit, Stuxnet typically injects the entire DLL into another process and then just calls the particular export. Stuxnet can inject into an existing or newly created arbitrary process or a preselected trusted process. When injecting into a trusted process, Stuxnet may keep the injected code in the trusted process or instruct the trusted process to inject the code into another currently running process.

The trusted process consists of a set of default Windows processes and a variety of security products. Here are some currently running processes:

- Kaspersky KAV (avp.exe)
- McAfee (Mcshield.exe)
- AntiVir (avguard.exe)
- BitDefender (bdagent.exe)
- Etrust (UmxCfg.exe)
- F-Secure (fsdfwd.exe)
- Symantec (rtvscan.exe)
- Symantec Common Client (ccSvcHst.exe)
- Eset NOD32 (ekrn.exe)

- Trend PcCillin (tmpproxy.exe)

In addition, the indicators search for the registry and the following programs are installed:

- KAV v6 to v9
- McAfee
- Trend PcCillin

Upon the detection of any one of the above security product processes, you can extract the main page version information.

Based on the version number, the target process of injection will be determined or the injection process will fail if the threat considers the security product non-bypassable. The potential target processes for the injection are as follows:

- Lsass.exe
- Winlogon.exe
- Svchost.exe
- The installed security product process

The following table describes the process used for that particular injection, depending on the installed security products.

Process Injection	
Security Product Installed	**Injection Target**
KAV v1 to v7	LSASS.exe
KAV v8 to v9	KAV Process
McAfee	Winlogon.exe
Antivir	Lsass.exe
BitDefender	Lsass.exe
ETrust v5 to v6	Fails to inject
ETrust (Other)	Lsass.exe
F-Secure	Lsass.exe
Symantec	Lsass.exe
ESET NOD32	Lsass.exe
Trend PC Cillin	Trend Process

TABLE 6.4: Process injection targets of Stuxnet for different security products

In addition, Stuxnet will determine if it needs to use one of the two currently undisclosed privilege escalation vulnerabilities before injection. Then, Stuxnet executes the target process in suspended mode. A template PE file extract content by itself thereby creating a new section called .verif and kept large enough so that the entry point address of the target process falls within the .verif section. At that address in the template PE file, Stuxnet places a jump to the

actual desired entry point of the injected code. These bytes are then written to the target process and Resume Thread is "called," in turn allowing the process to execute and call the injected code.

This technique may bypass security products that employ behavior-blocking. In addition to creating the new section and patching the entry point, memory of the new process maps the .stub section of the wrapper.dll file (that contains the main .dll file and configuration data) by means of shared sections. Therefore, the new process has access to the original .stub section. After resuming the newly injected process, the injected code unpacks the.dll file from the mapped .stub section and calls the desired export.

Instead of executing the export directly, the injected code also instructs to inject into another arbitrary process instead, and within that secondary process, execute the desired export.

Infection Routine Flow

Installation

Export 15 is the first export called when the .dll file is loaded for the first time. It is responsible for checking that the threat is running on a compatible version of Windows, checking whether the computer is already infected or not, elevating the privilege of the current process to system, checking the installed antivirus products, and determining the best process for injection. It then injects the .dll file into the chosen process using a unique injection technique described in the Injection Technique section, and calls export16.

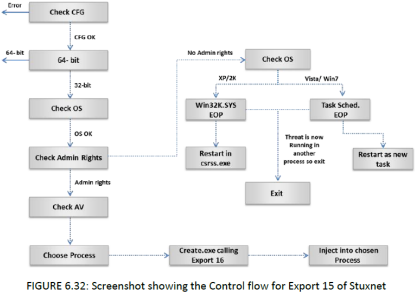


FIGURE 6.32: Screenshot showing the Control flow for Export 15 of Stuxnet

The first task in export 15 is to check if the configuration data is up-to-date. The configuration data can be stored in two locations. Stuxnet checks which is most up-to-date and proceeds with those configuration data. Next, Stuxnet determines if it is running on a 64-bit machine; if the machine is 64-bit, the threat exits. At this point it also checks to see on what operating system it is running. Stuxnet will only run on Windows 2000, XP, 2003, Vista, Server 2008, 7, and Server 2008 R2. If it is not running on one of these operating systems, it will exit.

Next, Stuxnet checks whether it has Administrator rights on the computer. Stuxnet wants to run with the highest privileges possible, so that it will have permission to take whatever actions it likes on the computer. If it does not have Administrator rights, it will execute one of the two zero-day escalation of privilege attacks described below. If the process already has the rights it requires it proceeds to prepare to call export 16 in the main .dll file. It calls export 16 by using the injection techniques described in the Injection Technique section.

When the process does not have Administrator rights on the system, it will try to attain these privileges by using one of two zero-day escalation of privilege attacks. The utilized attack vector depends on the operating system of the compromised computer. If the operating system is Windows Vista, 7, or Server 2008 R2, the currently undisclosed Task Scheduler Escalation of Privilege vulnerability is exploited. If the operating system is Windows XP or 2000, the Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073) is exploited.

If exploited, both of these vulnerabilities result in the main .dll file running as a new process, either within the csrss.exe process, in the case of win32k.sys vulnerability, or as a new task with Administrator rights, in the case of the Task Scheduler vulnerability. The code to exploit the win32k.sys vulnerability is stored in resource 250.

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

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

Infection Routine Flow

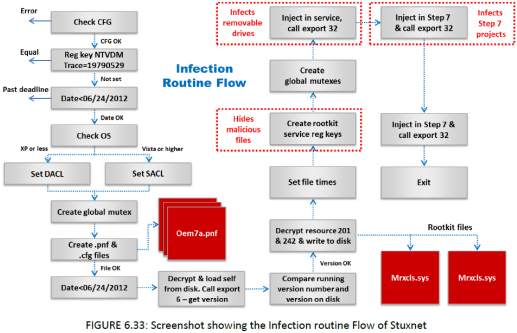


FIGURE 6.33: Screenshot showing the Infection routine Flow of Stuxnet

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

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

If this value is equal to 19790509, the threat will exit. This is thought to be an infection marker or a "**do not infect**" marker. If this is set correctly, infection will not occur. The value may be a random string and represent nothing, but also appears to match the format of date markers used in the threat. As a date, the value may be May 9, 1979. This date could be an arbitrary date, a birth date, or some other significant date. However, on May 9, 1979, although a variety of historical events occurred, according to Wikipedia, "Habib Elghanian was executed by a firing squad in Tehran, sending shock waves through the closely knit Iranian-Jewish community. He was the first Jew and one of the first civilians executed by the new Islamic government. This prompted the mass exodus of the once 100,000 member strong Jewish community of Iran, which continues to this day." Symantec cautions readers on drawing any attribution conclusions. Thus, attackers would have the natural desire to implicate another party.

Next, Stuxnet reads a date from the configuration data (offset 0x8c in the configuration data). If the current date is later than the date in the configuration file, then infection will also not occur and the threat will exit. The date found in the current configuration file is June 24, 2012.

Stuxnet communicates between different components via global mutexes. Stuxnet tries to create such a global matrix, but first it will use SetSecurityDescriptorDacl for computers running Windows XP and also the SetSecurityDescriptorSacl API for computers running Windows Vista or later to reduce the integrity levels of objects, and thus ensure no write actions are denied. Next, Stuxnet creates 3 encrypted files, read from the .stub section of Stuxnet; encrypted and written to disk, the files are: The main Stuxnet payload.

- dll file is saved as Oem7a.pnf
- A 90 byte data file copied to %SystemDrive%\inf\mdmeric3.PNF
- The configuration data for Stuxnet is copied to %SystemDrive%\inf\mdmcpq3.PNF
- A log file is copied to %SystemDrive%\inf\oem6C.PNF

Then Stuxnet checks the date again to ensure the current date is before June 24, 2012.

Subsequently, Stuxnet checks whether it is the latest version, or whether the version encrypted on disk is newer. It does this by reading the encrypted version from the disk, decrypting it, and loading it into memory. Once loaded Stuxnet calls export 6 from the newly loaded file; export 6 returns the version number of the newly loaded file from the configuration data. In this way Stuxnet can read the version number from its own configuration data and compare it with the version number from the file on disk. If the versions match, then Stuxnet continues.

Provided that the version check passed, Stuxnet will extract, decode, and write two files from the resources section to disk, read from resource 201 and 242 and are written to disk as "**Mrxnet.sys**" and "**Mrxcls.sys**," respectively. These are two driver files; one serves as the load point, and the other hides malicious files on the compromised computer and replaces the removed Stuxnet files on the disk. While creating these files, the file time on them

automatically changes to match the times of other files in the system directory to avoid suspicion. Once these files have been dropped, Stuxnet creates the registry entries necessary to load these files as services that will automatically run when Windows starts.

It creates some more global mutexes to signal that the installation has occurred successfully after the establishment of Stuxnet and upon the successful installation of a rootkit.

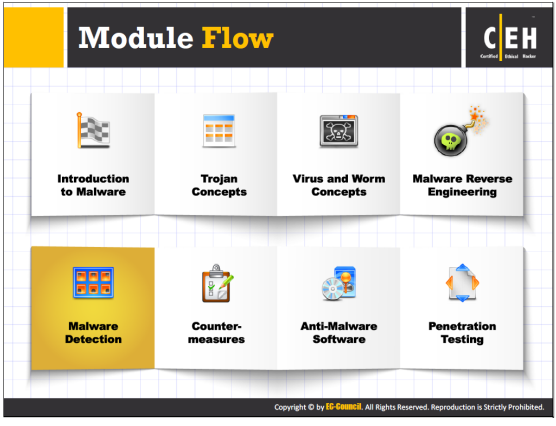
Stuxnet passes control to two other exports to continue the installation and infection routines. Firstly, it injects the payload .dll file into the services.exe process and calls export 32, which is responsible for infecting newly connected removable drives and for starting the RPC server. Secondly, Stuxnet injects the payload .dll file into the Step7 process S7tgtopx.exe and calls export 2. To succeed in this action, Stuxnet may need to kill the explorer.exe and S7tgtopx.exe processes, if they are running.

From this point on, execution of Stuxnet continues via these two injections: via the driver files, and through the created services.

Stuxnet then waits for a short while before trying to connect to the RPC server actually started by the export32 code. It will call function 0 to check that it can successfully connect, and then it makes a request to function 9 to receive some information, storing this data in a log file called oem6c.pnf.

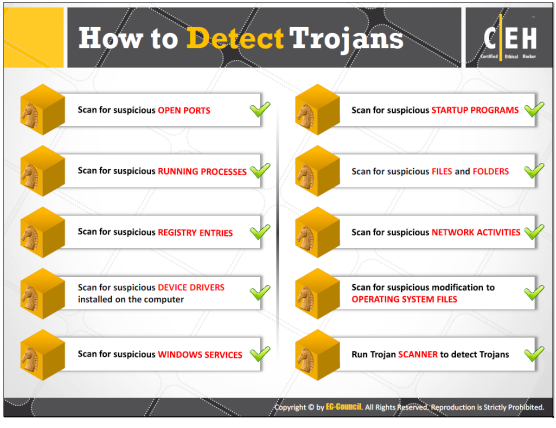
At this point, all the default spreading and payload routines will be in active mode.

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

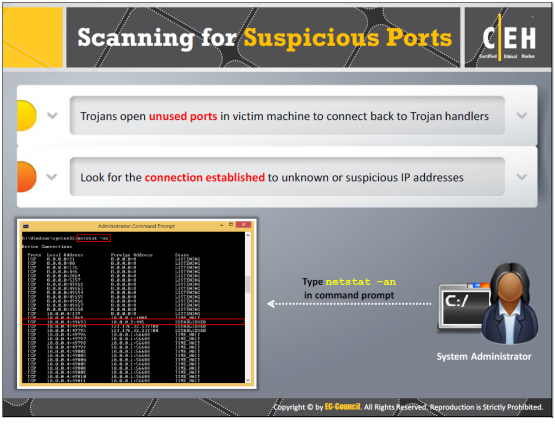


The nature of malware makes it difficult to detect. Unlike viruses, Trojans do not delete or corrupt files or applications that a victim might notice; they do their best to stay out of the victim's sight and escape detection. Malware detection helps protect the system and its resources from further loss.

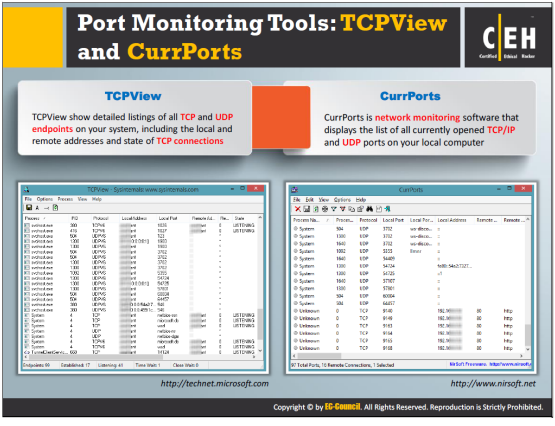
This section focuses on detecting Trojans using various techniques or methods, and tools that helps to accomplish the task. It also highlights various methods to prevent, detect, and eliminate viruses and worms.



Trojans are malicious programs that masquerade as useful or legitimate files, but their actual purpose is to take complete control of computers, thereby accessing files and confidential information. To protect files and personal information from such unauthorized access, it is necessary to use an anti-virus product that automatically scans and detects the presence of Trojans on the system. Alternatively, one can manually detect Trojans installed on systems.



Open ports act as communication channels for Trojans. They open unused ports on the victim's machine to connect back to the Trojan handlers. Scanning for suspicious ports will help the users in identifying these Trojans. By using port scanner utilities such as **TCPView** and **CurrPorts**, it is possible to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses.



TCPView

Source: *http://technet.microsoft.com*

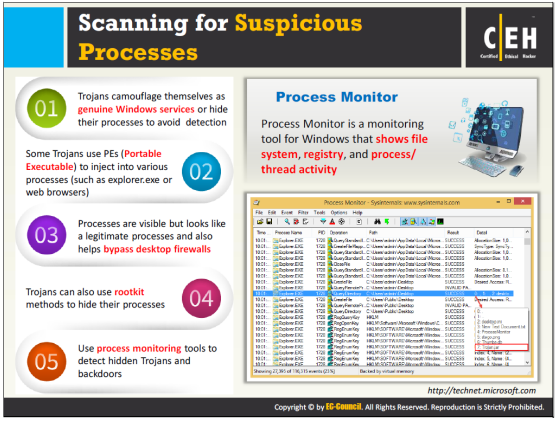
TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses, and the state of TCP connections. It provides a subset of the **Netstat** program that ship with Windows. The TCPView download includes **Tcpvcon**, a command-line 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.

CurrPorts

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

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on the local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user who created it.

It allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file, XML file, or to a tab-delimited text file.



Trojans generally make their entry into the system through pictures, music files, videos, etc. that are downloaded from the Internet. Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection. Some Trojans use PEs (Portable Executable) to inject into various processes (such as explorer.exe or web browsers). Attackers use certain rootkit methods to make the Trojan hide in the system, so that the antivirus software cannot normally detect it. One should scan for suspicious processes in order to detect hidden Trojans and other kinds of vulnerabilities. Use process monitoring tools such as **What's Running**, **Process Explorer**, and **KillProcess** to detect suspicious processes.

Process Monitor

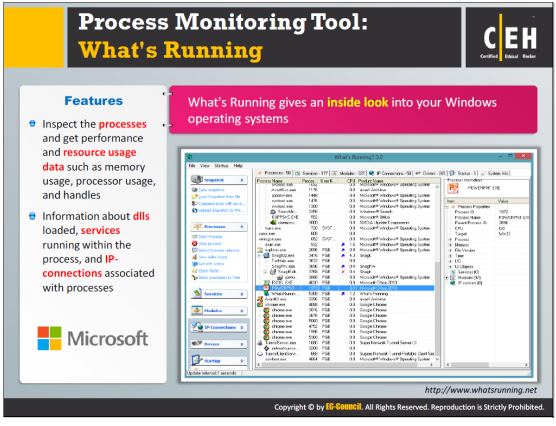
Source: http://technet.microsoft.com

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

- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Filters can be set for any data field, including fields not configured as columns
- Process tree tool shows relationship of all processes referenced in a trace
- Native log format preserves all data for loading in a different Process Monitor instance
- Boot time logging of all operations



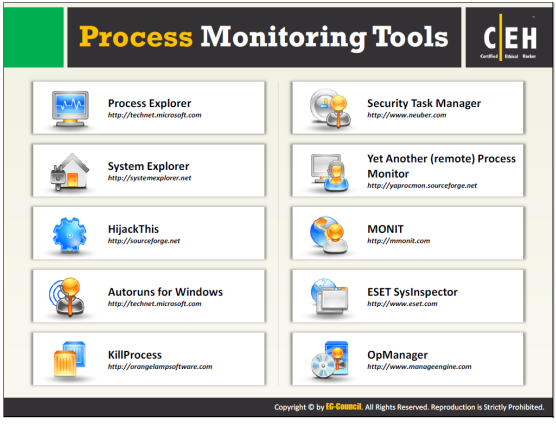
A user can use What's Running to explore processes, services, modules, IP-connections, and drivers, among others. It finds important information such as what modules are involved in a specific process.

Features:

- **Processes:** It inspects the processes and gives performance and resource usage data, such as memory usage, processor usage, and handles. It gives all the details about dll:s that are loaded, services that are running within the process, and the IP connections for each process.
- **IP connections:** Gives information about all active IP-connections in the system. Provides a list of what remote connections each program have and find out what applications are listening for connections.
- **Services:** Inspect services that are running and stopped, find the process for services and inspect its properties.
- **Modules:** Find information about all dll:s and exe:s in use in the system. For each module, one can find all processes that have loaded the module. Also one can find the full path and immediately open the folder where the file is located.
- **Drivers:** Find information about all drivers, for running drivers one can inspect the file version for finding the supplier of the drive.

- **Startup**: Allows management of all startup programs, regardless of source (registry or Startup folder).
- **System information:** Shows important system information about your computer, such as installed memory, processor, registered user, operating system type, and its version.

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



There are many process monitoring tools used to detect Trojans installed on the system. These tools display a list of all the processes running or installed on the system. By analyzing the list of processes, one can identify Trojans. These tools provide a comprehensive monitoring console for the entire network and IT infrastructure. They continuously and proactively monitor the entire IT system, which helps the users to immediately identify and notify any outages or performance degradations. In addition, it kills all the software that threatens the computer, even if it hides in the system. Given below is a list of process monitoring tools:

Process Explorer

Source: *http://technet.microsoft.com*

Process Explorer shows information about which handles and DLLs processes have opened or loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in:

- In handle mode, one can see the handles that the process selected in the top window has opened.
- In DLL mode, one can see the DLLs and memory-mapped files that the process has loaded.

System Explorer

Source: http://systemexplorer.net

System Explorer is software for exploration and management of system Internals. It includes many tools, which help to keep the system under control. With System Explorer, one can get fast access to file database, which helps to determine unwanted processes or threats.

Features:

- Gives information about tasks, processes, modules, startups, IE add-ons, uninstallers, windows, services, drivers, connections, and opened files
- Checks for suspicious files via file database or the virusTotal service
- Monitors processes activities and system changes

HijackThis

Source: http://sourceforge.net

HijackThis is a utility that generates an in depth report of registry and file settings from the computer. It makes no separation between safe and unsafe settings in its scan results giving the ability to selectively remove items from the machine. In addition, HijackThis comes with several tools useful in manually removing malware from a computer.

Autoruns for Windows

Source: http://technet.microsoft.com

Autoruns for Windows has the knowledge of auto-starting locations of any startup monitor, shows what programs are configured to run during system bootup or login, and shows the entries in the order Windows processes them. These programs include ones in the startup folder, Run, RunOnce, and other Registry keys. One can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

KillProcess

Source: http://orangelampsoftware.com

KillProcess can terminate almost any process on a Windows machine, including any service and process running in the system. It can even terminate the protected Microsoft system processes. It can kill multiple processes, either by multi-select or by use of “kill lists.” Using these techniques it is possible to batch-terminate processes. It can also scan the running processes on the computer, and kill them on sight, much like an anti-spyware application would.

Security Task Manager

Source: http://www.neuber.com

Security Task Manager shows comprehensible information about programs and processes running on the computer. For each Windows process, it improves on Windows Task Manager, providing:

- unique security risk rating

- full directory path and file name
- process description
- CPU usage graph
- embedded hidden functions (e.g., keyboard monitoring, browser supervision, or manipulation)
- process type (e.g., visible window, systray program, DLL, IE-plugin, startup service)

Yet Another (remote) Process Monitor

Source: http://yaprocmon.sourceforge.net

Yet Another (remote) Process Monitor (YAPM) is an application that allows to view and manage running tasks, processes, threads, and modules, and the services on a local or on a remote machine.

MONIT

Source: http://mmonit.com

Monit is an open source utility for managing and monitoring UNIX systems. It conducts automatic maintenance and repair and can execute meaningful causal actions in error situations. One can use Monit to:

- Monitor daemon processes or similar programs running on local host, Monit is particularly useful for monitoring daemon processes, such as those started at system boot time from /etc/init/
- Test programs or scripts at certain times, much like cron, but in addition, you can test the exit value of a program and perform an action or send an alert if the exit value indicates an error
- Monitor files, directories, and filesystems on localhost. Monit can monitor these items for changes, such as timestamps changes, checksum changes or size changes
- Monitor general system resources on localhost such as overall CPU usage, Memory, and Load Average

ESET SysInspector

Source: http://www.eset.com

ESET SysInspector is a diagnostic tool that helps troubleshoot a wide range of system issues. It tracks down the presence of malicious code. ESET SysInspector resolves issues related to:

- Running processes and services
- Presence of suspicious and unsigned files
- Software issues
- Hardware incompatibility
- Outdated or malfunctioning drivers

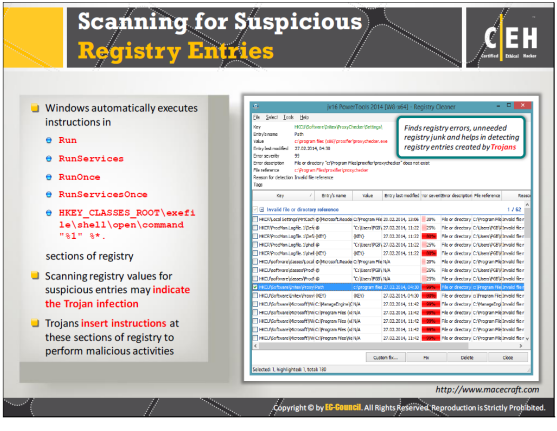
- An unpatched operating system
- Broken registry entries
- Suspicious network connections

OpManager

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

ManageEngine OpManager is a network and data center infrastructure management software that helps large enterprises, service providers and SMEs manage their data centers and IT infrastructure efficiently and cost effectively. Automated workflows, intelligent alerting engines, configurable discovery rules, and extendable templates enable IT teams to setup a "24-7" monitoring system.

Do-it-yourself plug-ins extend the scope of management to include network change and configuration management and IP address management as well as monitoring of networks, applications, databases, virtualization, and NetFlow-based bandwidth.

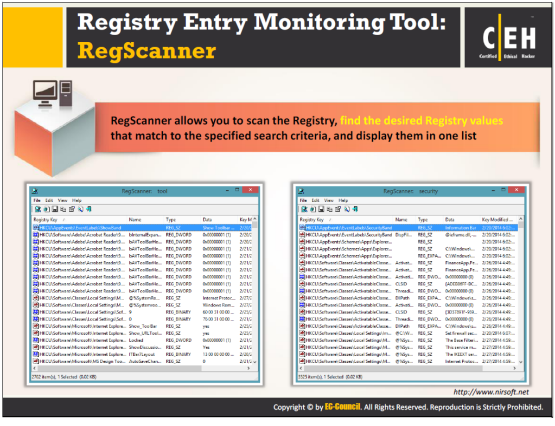


When an attacker installs a Trojan on the victim's machine, it generates a registry entry. We consequently notice various changes: the system gets slower, various advertisements keep popping up, and so on. Thus, scanning for suspicious registries will help to detect Trojans.

jv16 PowerTools 2014 –Registry Cleaner

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

jv16 PowerTools 2012 is the ultimate registry cleaner used to find registry errors and unneeded registry junk and helps in detecting registry entries created by Trojans.

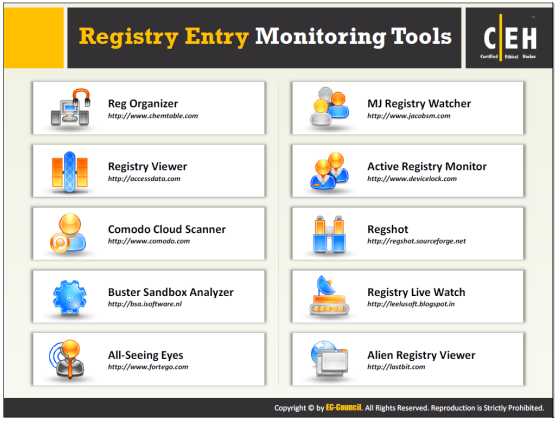


RegScanner is a small utility that allows scanning the Registry, finding the desired Registry values that match to the specified search criteria, and display them in one list. After finding the Registry values, one can jump to the right value in RegEdit by double-clicking the desired Registry item. It also allows exporting the found Registry values into a .reg file that is useful in RegEdit.

Features:

- Displays the entire search result at once, need not press F3 in order to find the next value
- Finds registry values by data length, value type (REG_SZ, REG_DWORD, etc.), and by modified date of the key
- Finds a Unicode string located inside a binary value
- Allows case sensitive search
- While scanning the Registry, RegScanner displays the current scanned Registry key, as opposed to RegEdit, which simply display a rudimentary "searching the registry" dialog box

Source: http://www.nirsoft.net



Below is a list of registry-entry monitoring tools that help in detecting any installed Trojans and cleaning the registry.

Reg Organizer

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

Reg Organizer helps to edit, clean the registry, fix errors in the system, and improve computer performance. The deep registry search feature lets to find all registry keys related to a specific application. The program helps to edit registry files (.reg) and view their content directly from Windows Explorer. It also has a built-in application uninstaller, allowing one to uninstall redundant applications from the system.

Registry Viewer

Source: *http://accessdata.com*

AccessData Registry Viewer allows viewing the contents of Windows operating system registries. Unlike the Windows Registry Editor, which can only display the current computer's registry, Registry Viewer allows to view registry files from any computer. It provides access to a registry's protected storage, which contains passwords, usernames, and other information that is not accessible in Windows Registry Editor. It provides several tools for obtaining and reporting important registry information.

Comodo Cloud Scanner

Source: http://www.comodo.com

Comodo Cloud Scanner scans computer to identify malware, junk files, registry errors, and hidden processes.

Buster Sandbox Analyzer

Source: http://bsa.isoftware.nl

Buster Sandbox Analyzer analyzes the behavior of processes and the changes made to the system and then evaluate if they are malware suspicious. The changes made to the system can be of several types: file system changes, registry changes and port changes. From these changes, one can obtain the necessary information to evaluate the "risk" of some of the actions taken by sandboxed applications.

All-Seeing Eyes

Source: http://www.fortego.com

All-Seeing Eye consists of a collection of tools that monitor important areas of the user's computer, areas in which spyware and other malicious programs practically always leave some kind of trace when they sneak into user's computer. Collection of tools includes: Process Tracker, DLL Tracker, Driver Tracker, Event Log Tracker, Autostart Guard, Service/Driver Guard, ActiveX Object Guard, Browser Helper Object (BHO) Guard, Winsock Layered Security Provider (LSP) Guard, Hosts File Guard, File System Guard, and Registry Guard.

MJ Registry Watcher

Source: http://www.jacobsm.com

MJ Registry Watcher is a registry, file, and directory hooker/poller that safeguard the most important startup files, registry keys and values, and other more exotic registry locations commonly attacked by Trojans.

Active Registry Monitor

Source: http://www.devicelock.com

Active Registry Monitor (ARM) analyzes the changes made to Windows Registry by making the "snapshots" of it and keeping them in the browsable database. User can compare any two snapshots and get the list of keys or data, which are new, deleted or just changed. ARM can do comparing not only in the entire Registry, but also in any key of the Registry. This tool is useful for detecting Trojan viruses and eliminating problems caused by installing/uninstalling software and hardware.

Features:

- Scans different copies of Registry into a special file and browse/search them "off-line"
- Scans Registry on a remote computer
- Compares individual branches of different copies of the Registry

- Perform Undo and Redo Registry changes based on comparison results: directly from the program or by generating the REG-files

Regshot

Source: *http://regshot.sourceforge.net*

Regshot is an open-source (LGPL) registry compare utility that allows to quickly taking a snapshot of the registry and then compares it with a second one—done after doing system changes or installing a new software product.

Registry Live Watch

Source: *http://leelusoft.blogspot.in*

Registry Live Watch monitors activity on a registry key in a read only mode. It can run minimized at the system tray (notification area) and monitor a registry key (sub keys and values) for different kinds of changes.

Alien Registry Viewer

Source: *http://lastbit.com*

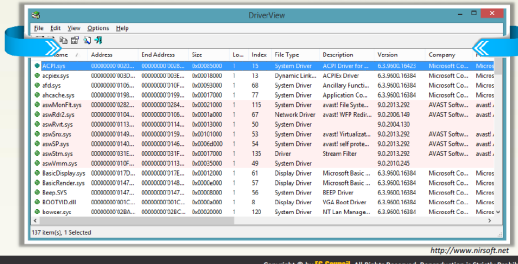
Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. While RegEdit shows the contents of the system registry, Alien Registry Viewer works with registry files copied from other computers. Alien Registry Viewer can be useful for system administration and forensic computer-examination purposes.

The system installs Trojans along with the device drivers, when user downloads infected drivers from untrusted sources; Trojans use these drivers as a shield to avoid their detection. One can scan for suspicious device drivers using tools such as **DriverView**, **Driver Detective**, **DriverGuide Toolkit**, and so on, and verify if they are genuine and downloaded from the publisher's original site. The path to the location of Windows system drivers is:

Run → type **msinfo32** → **Software Environment** → **System Drivers**

Device Drivers Monitoring Tool: DriverView

DriverView utility displays the list of all **device drivers** currently loaded on 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.



http://www.nirsoft.net

Discussed below are some device-driver monitoring tools that help in detecting Trojans:

Driver Detective

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

Driver Detective removes guesswork in resolving driver problems by providing instant access to the most relevant content for your computer's hardware.

Features:

- Scans your PC to determine the manufacturer, family, model, and motherboard
- Easy Migrator will automatically scan your computer's hardware, download all of the latest drivers for any destination operating system that you choose, and then creates a device-driver migration CD
- Ensures that the downloads do not contain viruses
- Possess tools necessary to keep the computer running at its best
- Provides accurate recommendations for user's computer
- Has a built-in wizard that allows you to copy (backup) your downloaded drivers to a CD, network drive, or USB flash drive

Unknown Device Identifier

Source: http://www.zhangduo.com

Unknown Device Identifier enables one to identify the yellow question mark labeled "**Unknown Devices in Device Manager**." It reports a detailed summary for the manufacturer name, OEM name, device type, device model and even the exact name of the unknown devices. With the collected information, one might contact the hardware manufacturer for support or search the Internet for the corresponding driver.

DriverGuide Toolkit

Source: http://www.driverguidetoolkit.com

DriverGuide Toolkit identifies and lists drivers installed on the computer and, when connected to the Internet, allows one to search DriverGuide.com (and other sources) for driver updates and manufacturer sites. In addition, it allows to backup currently installed drivers for safe keeping.

InstalledDriversList

Source: http://www.nirsoft.net

InstalledDriversList is a tool for Windows that lists all device drivers that exists on the system. For every device driver, it displays the following information: Driver Name, Display Name, Description, Startup Type, Driver type, Driver Group, Filename, File Size, Modified/Created Time of the driver file, and version information of the driver file.

If the driver is currently running on Windows kernel, it also displays the following information: Base Memory Address, End Address, Memory Size, and Load Count.

Driver Magician

Source: http://www.drivermagician.com

Driver Magician allows device drivers backup, restoration, update and removal in Windows operating system. It identifies all the hardware in the system, extracts their associated drivers from the hard disk and backs them up to a location of your choice. It has a built-in database of the latest drivers with the ability to go to the Internet to receive the driver updates. If there are unknown devices in the PC, Driver Magician helps to detect them with its built-in hardware identifier database.

Driver Reviver

Source: http://www.reviversoft.com

Driver Reviver restores maximum performance and functionality to the user PC's hardware and its components.

Features:

- Ensures that the user PC and its components are performing at their optimum levels
- It tracks down each driver for each single piece of hardware connected to the PC
- Scans for drivers, downloads them, and installs them correctly

- Prevents users from incorrectly using the wrong driver
- Eliminates the risk of downloading a faulty driver or even malware
- Ensures that if there are any problems with an update, the changes can be reversed to get the system back up and running

ServiWin

Source: http://www.nirsoft.net

ServiWin utility displays the list of installed drivers and services on the system. For some of them, it displays additional useful information: file description, version, product name, company that created the driver file, and so on. In addition, ServiWin allows one to stop, start, restart, pause, and continue service or driver, change the startup type of service or driver (automatic, manual, disabled, boot or system), save the list of services and drivers to file, or view HTML report of installed services/drivers in the default browser.

Double Driver

Source: http://www.boozet.org

Double Driver analyzes the user's system and lists the most important driver details such as version, date, and provider. The application can backup and restore all the drivers found on a system at a later point. It can also list, save, and print all chosen drivers.

My Drivers

Source: http://www.zhangduo.com

My Drivers enables to detect, backup and restore all hardware device drivers currently on the system. In addition, it allows finding the latest drivers for the hardware and installing them onto the computer. One can back up the list of all hardware devices extracted, into a desired folder and restore them after reinstalling or upgrading the system.

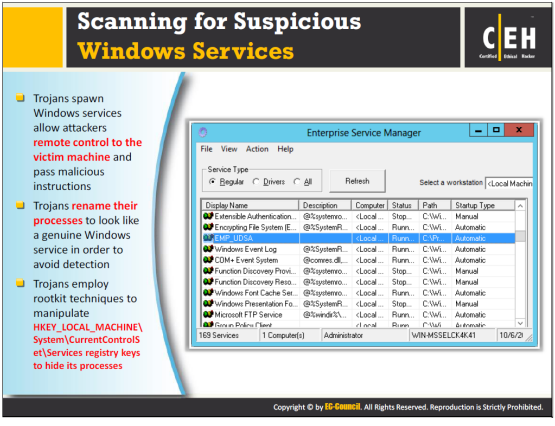
DriverEasy

Source: http://www.drivereasy.com

DriverEasy tool automatically scans and analyses users' systems.

Features:

- Fixes driver issues
- Detects unknown device drivers
- Keeps drivers up-to-date with latest versions
- Secures user's system with backup of Installed drivers, easy to roll back or restore them
- Uninstalls removed device drivers to speed-up booting



Trojans spawn Windows services allow attackers to remotely control the victim machine and pass malicious instructions. Trojans rename their processes to look like a genuine Windows service in order to avoid detection. Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services** registry keys to hide their processes. One can scan for suspicious Windows services using tools such as **Windows Service Manager**, **Netwrix Service Monitor**, and **ServiWin**.

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>
```

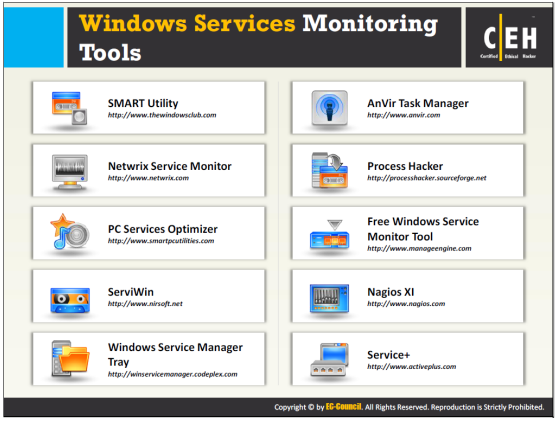
- **Start/stop/restart services**

```
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>]
```

Source: http://tools.sysprogs.org



Windows Services monitoring tools monitor critical Windows services and optionally restart them after failure. Given below is the list of Windows Services monitoring tools:

SMART Utility

Source: http://www.thewindowsclub.com

SMART (Service Management And RealEasy Tweaking) Utility helps to tweak Windows services based on the suggested configurations of BlackVipers. It is useful in portable application to customize Windows services settings to meet the requirements. With judicious tweaking, it can make systems faster, as users can disable services, which they do not require.

One can tweak Windows services manually, but what this utility does is automate the entire process to give users' the desired settings. Based on the recommendations of the BlackVipers Service Configuration Guide, the utility offers three sets of pre-configured tweaks: safe, tweaked, and advanced or BareBones. The utility has set the presets to check for service before applying tweak. There is also a button to re-set services to Windows Default Settings.

Netwrix Service Monitor

Source: http://www.netwrix.com

Netwrix Service Monitor is a tool to monitor critical Windows services and optionally restart them after failure. The tool monitors all automatic startup services on multiple servers at a time and sends e-mail alerts when one or more services stops unexpectedly. The optional automatic restart feature ensures that all monitored services are up and running without down time.

PC Services Optimizer

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

PC Services Optimizer is a tweaking solution that enables to optimize Windows Services automatically. It turns off unneeded Windows services without affecting the normal function, which will make PC to run faster and more securely.

Features:

- **Gaming Mode:** It gives users' systems an immediate performance boost.
- **Services Profiles**: It saves user services settings in profiles, enabling the user to apply different settings in seconds, saving time specially when dealing with multiple computers or users.
- **Services Manager**: It enables advanced users to master Windows services including third party services by providing several tools for performing advanced functions.

ServiWin

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

ServiWin utility displays the list of installed drivers and services on the user's system. For some of them, it displays additional useful information such as file description, version, product name, and the company that created the driver file.

In addition, it allows users to stop, start, restart, pause, and continue service or driver, change the startup type of service or driver (automatic, manual, disabled, boot or system), save the list of services and drivers to file, or view HTML report of installed services/drivers in their default browser.

Windows Service Manager Tray

Source: *http://winservicemanager.codeplex.com*

Windows Service Manager Tray allows selecting the required services and controlling them from the tray. This tool also optimizes the default Windows service manager and permits to start, stop, or restart required services.

AnVir Task Manager

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

AnVir Task Manager controls everything running on the user's computer. It offers all of its features in a single interface instead of releasing multiple packages to perform a family of related tasks.

Features:

- Monitors processes, services, startup programs, etc.
- Replaces Windows Task Manager
- Gets rid of spyware and viruses
- Speeds up the system and Windows startup

Process Hacker

Source: http://processhacker.sourceforge.net

Process Hacker is a multi-purpose tool that helps to monitor system resources, debug software, and detect malware. It is an open source alternative to programs such as Task Manager and Process Explorer.

Features:

- Provides a detailed overview of system activity with highlighting
- Offers graphs and statistics to track down resource hogs and runaway processes
- Allows discovery of which processes are using the file that cannot be edited or deleted
- Permits seeing what programs have active network connections, and close them if necessary
- Provides real-time information on disk access
- Allows viewing of detailed stack traces with kernel-mode, WOW64, and .NET support
- Permits going beyond services.msc: create, edit, and control services

Free Windows Service Monitor Tool

Source: http://www.manageengine.com

Free Windows Service Monitor helps to monitor Exchange Server, SharePoint services, MySQL services, MSSQL services, DHCP services, etc. It allows users to monitor up to five custom services simultaneously.

Features:

- Monitors the Windows services for up to three devices simultaneously
- Allows to know the status and startup type of the Windows services
- Configures the startup type and updates the status of Windows services
- Allows to fetch the status of Windows services by refreshing

Nagios XI

Source: http://www.nagios.com

Nagios XI monitors the state of any Microsoft Windows service such as IIS, Exchange, and DHCP, and alerts whenever the service stops or crashes.

Features:

- Increases server, services, and application availability
- Detects network outages and protocol failures
- Detects failed processes and batch jobs

Service+

Source: http://www.activeplus.com

Service+ provides advanced features to manage Windows services (custom views, specific properties, monitoring, etc.).

Features:

- Implements multiple services such as startup, account, dependencies, name, and path simultaneously
- Monitors services installation and un-installation in real time
- Terminates un-responding services without any reboot
- Allows all authenticated users to start a service
- Prohibits all users, including administrators to stop critical services such as backup and critical applications
- Manages the services on a remote computer
- Sorts services by standard and advanced properties such as name, status, startup, and type
- Imports or exports the configuration of services as an XML file to duplicate them, to backup settings, or to mirror the same configuration on several computers

Trojans, once installed on the computer, run automatically at system startup. Therefore, scanning for suspicious startup programs is very essential for detecting Trojans. Given below are steps to detect hidden Trojans:

Step 1: Check startup program entries in the registry.

The detailed description of this step is available in the next topic.

Step 2: Check device drivers automatically loaded.

`C:\Windows\System32\drivers`

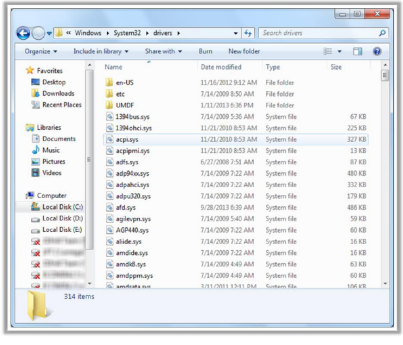


FIGURE 6.34: Snapshot showing automatically loaded device drivers of a system

Step 3: Check `boot.ini`

Check `boot.ini` or `bcd` (bootmgr) entries.

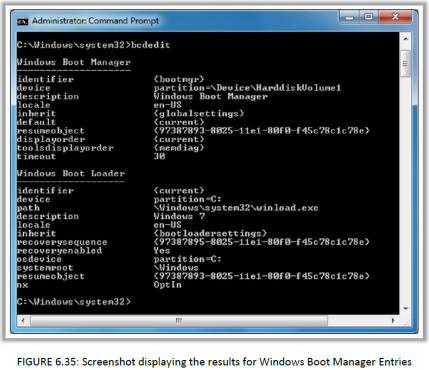


FIGURE 6.35: Screenshot displaying the results for Windows Boot Manager Entries

Step 4: Check that Windows services automatic started.

Go to **Run** → Type **services.msc** → Sort by **Startup Type**.

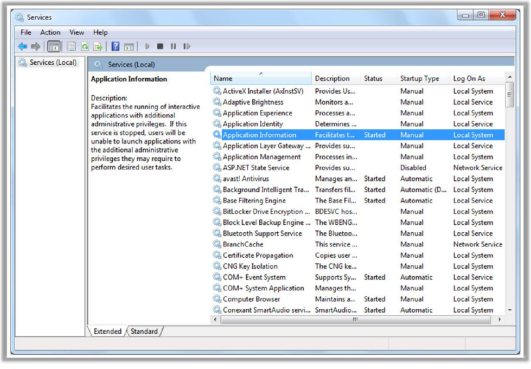
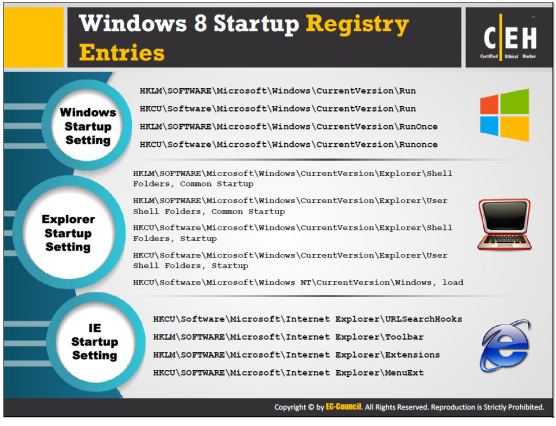


FIGURE 6.36: Screenshot showing the information about services on a local system

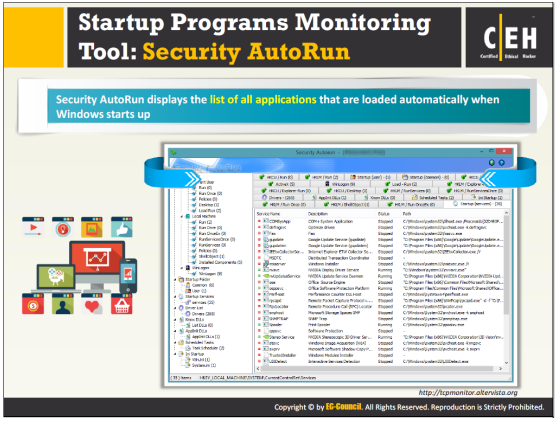
Step 5: Check the **Startup** folder.

`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`

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



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 8). Startup items can be added by either the programs or drivers installed, or manually by the user. Programs that run on Windows 8 startup can be located in these registry entries, such as **IE Startup Setting**, **Windows Startup Setting**, and **Explorer Startup Setting**.

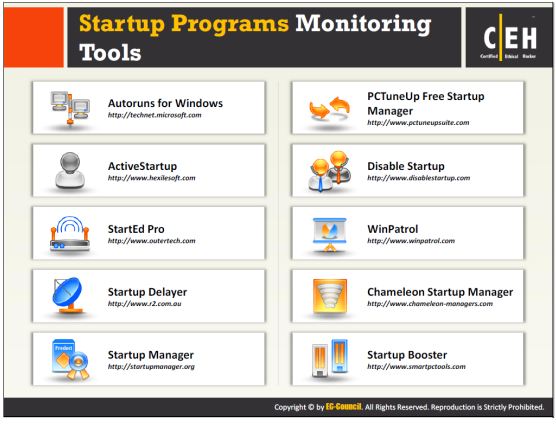


Security AutoRun displays the list of all applications that are loaded automatically when Windows starts up. It also identifies a spyware or adware program that runs at startup.

For each application, it displays the following information:

- Startup type
- Startup registry
- Startup common/user
- Startup services
- Drivers list
- Command-Line String, Product Name, File Version, Company Name, Location in the Registry or file system, etc.

Source: http://tcpmonitor.altervista.org



Below is a list of startup programs monitoring tools that scan for suspicious startup programs to detect Trojans:

Autoruns for Windows

Source: *http://technet.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 user to zoom in on third-party auto-starting images that adds to the users' system and it has support for looking at the auto-starting images configured for other accounts configured on a system.

ActiveStartup

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

ActiveStartup is a program for Windows OSs that allows users to manage programs, which load from Registry, Win.ini, and Startup Menu at Windows Startup.

Features:

- Allows to add, delete, and disable programs from Windows startup list
- Has the ability to backup and restore startup configurations
- Offers open system utilities such as RegEdit and SysEdit
- Monitors the list of programs for updates
- Displays if the program is running or not
- Checks for "dead" files at startup list
- Provides Hotkey to activate ActiveStartup from tray

StartEd Pro

Source: http://www.outertech.com

StartEd is a utility that helps to manage the Windows startup procedure. It recognizes obsolete or memory-hogging startup programs, and enables the option of disabling them to increase the quality of system performance.

Features:

- View, edit, delete, disable, and add entries to the Windows startup configuration
- Backup and Restore startup configurations
- Manage System Services with detailed notes and description
- Filter Service List with keywords
- See new startup items and services since last StartEd use
- Show detailed information about every startup entry
- Create shortcuts on desktop which is useful for temporary disabled items
- Recognize Trojan Horses in startup configuration

Startup Delayer

Source: http://www.r2.com.au

Startup Delayer optimizes startup process by delaying applications from starting up as soon as a user logs into the computer. Because of the delay, the computer becomes usable a lot faster. Startup Delayer will then start launching the delayed applications when the computer is idle.

Features:

- Provides automatic delay engine
- Possess advanced launch options, which let to modify various launch options such as launching on a specific day.
- Monitors running tasks and services
- Creates backups of startup applications and restores them when required

- Recovers deleted applications

Startup Manager

Source: http://startupmanager.org

Startup Manager is a program that manages the Windows startup procedure. It supports Startup folders (all users and current user), the registry section (all the run and services sections and computer sections), and the Win.ini sections (load and run).

Features:

- Makes programs start on logon by adding items
- Allows to rename, delete, enable, or disable existing items
- Creates a batch file with programs that start in a certain order

PCTuneUp Free Startup Manager

Source: http://www.pctuneupsuite.com

PCTuneUp Free Startup Manager is a system startup entry monitor and management tool. It displays the configuration of applications and processes to run automatically during startup or login, and helps to disable or enable startup items from system boot. It displays the detailed information of the exact applications such as the name, type, and arguments, and it makes possible to process some operations of each item in the activated registry editor, such as import/export, modification, renaming, and copy, as needed.

Features:

- Speeds up system boot and Windows login process
- Removes unneeded programs in the startup list
- Allows to set programs to launch at startup
- Allows to acquire more available memory, such as RAM and other system resources

Disable Startup

Source: http://www.disablestartup.com

Disable Startup is a startup manager and monitoring program, it can scan all Windows Startups on the users' computer, and monitor all new startup items. It helps to control, manage, and optimize Windows Startup configuration. Disable Startup can save system memory and resources by disabling unnecessary programs. It also monitors the start page of Internet Explorer and stops any changes in the Windows startup.

WinPatrol

Source: http://www.winpatrol.com

WinPatrol runs on Windows OSs and supports Windows 64-bit features without conflicts with other programs. This tool provides a layered security even if a legitimate program tries to install unwanted toolbars. It also monitors, removes and disables Startup Programs. The startup

commands for these programs are available in the Windows Registry, the WIN.INI file, Windows Startup Folder, within system files, and other internal system areas.

Features:

- It provides additional information on Startup Programs, including the company that created the program file, as well as the program version.
- The Full Report option will create a complete report of the current Startup Programs list and all the information available on each program.
- Sometimes, malicious programs come in pairs or groups that protect each other to prevent from removing them. The Kill feature on the Active Tasks list allows to shut down the malicious programs before removing them from the Startup programs list.
- Sometimes, after trying to remove a suspicious program, it may still persist. In such cases, right-click on the title of the program and select Delete File on Reboot. This action will not take place until the next time you boot, but it deletes the file before Windows starts, as well as any other programs that may attempt to prevent its deletion.

Chameleon Startup Manager

Source: *http://www.chameleon-managers.com*

Chameleon Startup Manager can control the programs that run at Windows startup, which makes Windows start faster, operate with increased stability, and lower the HDD usage. It also offers program launch options with fixed or automatic delayed startup (each program is launched in sequence after the previous one finishes starting), allowing the computer to be started as quickly and smoothly as possible.

Programs run according to various functions including startup order change, priority, consecutive program launch, and day selection. A user can create and select the configurations at Windows startup or applied without restarting Windows.

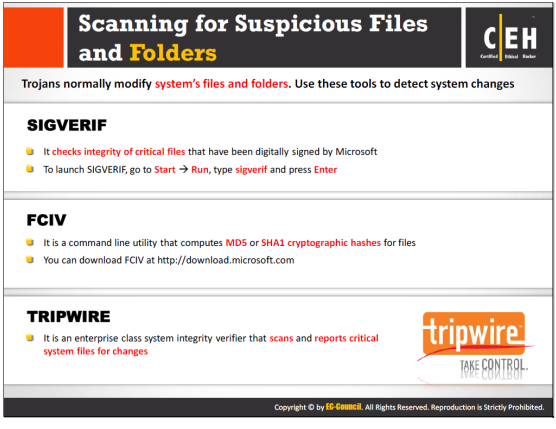
Startup Booster

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

Startup Booster classifies all of programs that are executed at startup as system programs, suspicious applications (such as viruses, etc.), and the unwanted programs for startup. This tool helps to remove programs from startup list or to add them when needed.

Features:

- Configures Windows to perform maximum by simple tweaks that suggest which options are to be activated and deactivated
- Cleans up the registry of outdated data or wrong values
- Instructs on how to configure the BIOS



Usually, when a system becomes infected by a Trojan, it modifies files and folders. One can scan for suspicious files and folders using tools such as FCIV, Tripwire, and SIGVERIF to detect any Trojans installed.

SIGVERIF

SIGVERIF is a built-in Windows tool that searches for unsigned drivers on a system. 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.

FCIV

The **File Checksum Integrity Verifier** (FCIV) is a command-prompt utility that computes and verifies cryptographic hash values of files. FCIV generates MD5 or SHA-1 hash values for files to compare the values against a known good value. It allows saving computed hashes of all the critical files in an XML file database for later use and verification.

With FCIV, you can compute hashes of all your sensitive files. It can compare hash values to make sure that the files do not change. When you suspect that your system has been compromised, you can run a verification to determine which files have been modified. You can also schedule verifications regularly.

Syntax:

Usage: `fciv.exe [Commands] <Options>`

Commands: (Default -add)

`-add <file | dir>`: Compute hash and send to output (default screen).

dir options:

`-r`: recursive.

`-type`: ex: -type *.exe.

`-exc file`: list of directories that should not be computed.

`-wp`: Without full path name. (Default store full path)

`-bp`: base path. The base path is removed from the path name of each entry

`-list`: List entries in the database.

`-v`: Verify hashes.

: Option: -bp basepath.

`-? -h -help` : Extended Help.

Options:

`-md5` | **`-sha1`** | **`-both`**: Specify hash type, default md5.

`-xml db`: Specify database format and name.

To display the MD5 hash of a file, type fciv.exe filename

Compute hashes:

```
fciv.exe c:\mydir\myfile.dll
fciv.exe c:\ -r -exc exceptions.txt -sha1 -xml dbsha.xml
fciv.exe c:\mydir -type *.exe
fciv.exe c:\mydir -wp -both -xml db.xml
```

List hashes stored in database:

```
fciv.exe -list -sha1 -xml db.xml
```

Verifications:

```
fciv.exe -v -sha1 -xml db.xml
fciv.exe -v -bp c:\mydir -sha1 -xml db.xml
```

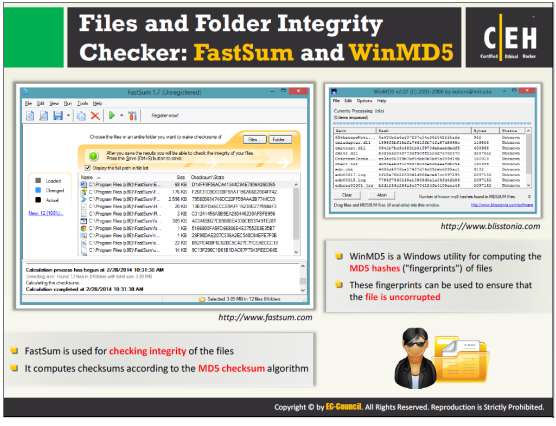
A sample FCIV output:

```
C:\ CIV>fciv.exe –both c:\important.txt
//
// File Checksum Integrity Verifier version 2.05.
//
MD5                                SHA-1
----------------------------------------------------------------------------------------------
e59ff97941044f85df5297e1c302d260 648a6a6ffffdaa0badb23b8baf90b6168dd16b3a important.txt
```

TRIPWIRE

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

Tripwire delivers risk visibility, business context, and security business intelligence, enabling enterprises to protect sensitive data and assets from breaches, vulnerabilities, and threats, through security controls including: security configuration management, vulnerability management, file integrity monitoring, and log and event management. Tripwire's file integrity monitoring finds, assesses, and acts on changes as soon as they occur. It assures the ongoing system integrity and automates detecting, auditing and reconciling changes—even lower profile, obscure ones that reveal advanced hacks and exploits.



One can use file and folder integrity checkers to check for any changes in the critical files, indicating potential intrusion attempts. This accomplishes using a suite of security tools that provide a complete audit and monitoring solution for **OSS** (Open System Services) and Guardian file systems. Discussed below are the two file and folder integrity checkers.

FastSum

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

FastSum checks integrity of files. When the user selects files, FastSum computes their checksums according to the MD5 checksum algorithm, which compares with previously computed checksums or stored for future integrity checking.

WinMD5

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

WinMD5 is a Windows utility for computing the MD5 hashes ("**fingerprints**") of files. It makes easy to compare the fingerprints against the correct fingerprints stored in an MD5SUM file. These fingerprints can be used to ensure that the file is uncorrupted.

Discussed below are file and folder integrity checkers one can use to verify the integrity of files and determine whether any malicious attempts were made on them:

Advanced CheckSum Verifier (ACSV)

Source: http://www.irnis.net

Advanced CheckSum Verifier is a Windows utility for verifying integrity of files by using the CRC32 or MD5 checksum calculation algorithms. It allows users to verify the accuracy of the data after burning a CD or transferring a file over a network. This program is especially effective if a user has many files, many subdirectories, or both.

Fsum Fronted

Source: http://fsumfe.sourceforge.net

Fsum Fronted allows computing message digest, checksums, and HMACs for files and text strings. It supports drag-and-drop and can handle multiple files at once. It generates the checksum to verify the integrity of files.

Features:

- Verifies files using a SFV/MD5/SHA1/SHA2 file and notifies the user if a file is corrupted or missing
- Creates a checksum file
- Verifies whether a file contains a checksum in its name (e.g., readme[b7b9c51e].txt)

- Keeps a checksum in the file name

Verisys

Source: http://www.ionx.co.uk

The Verisys file-integrity monitoring system is a software solution for Windows-based systems, with cross-industry applications, including PCI and SOX compliance, and data integrity assurance.

Features:

- Detects unauthorized changes
- Meets PCI DSS requirements 10.5.5 and 11.5
- Delivers centralized administration
- Schedules automated integrity checks
- Includes comprehensive reporting tools
- Offers templates for common system configurations

AFICK (Another File Integrity Checker)

Source: http://afick.sourceforge.net

AFICK (Another File Integrity Checker) is a security tool that monitors changes to the user's file system and can detect intrusions.

FileVerifier++

Source: http://www.programmingunlimited.net

FileVerifier++ is a Windows application for verifying the integrity of files. This tool supports various algorithms such as CRC, MD, SHA, WHIRLPOOL, and RIPEMD by means of dynamically loadable hash libraries.

Features:

- Hash algorithms can be added through the DLL interface
- Hash verification can load hash results and compare to what is actually on the disk
- Verification considers file size, file attributes, and modification date to be significant
- Recursive directory processing
- Recursive processing using patterns
- Calculates hashes on strings
- Unicode support, which recognizes Unicode file names and writes encoded results in UTF-8 (without BOM)

PA File Sight

Source: http://www.poweradmin.com

PA File Sight is a file monitoring software that helps users to determine who is reading from and writing to important files. It can tell whenever a user creates a new file or rename a folder and when he/she deletes a file or folder. It also intimates who did it and what computer they did it from (IP address and computer name).

Features:

- Monitors files or subsets
- Possess a record of creations, deletions, accesses, changes
- Captures successful actions as well as failure reports
- Includes file auditing compliance
- The ultra-edition Provides centralized management

CSP File Integrity Checker

Source: http://www.tandemsecurity.com

CSP File Integrity Checker monitors, reports and alerts for any changes made to a specified group of files to protect confidential information.

Features:

- Audits database of change history
- Monitors Guardian and OSS files
- Meets PCI DSS regulation 11.5
- Holds unique file fingerprint
- Provides GUI display for file management
- Alerts for unauthorized change

ExactFile

Source: http://www.exactfile.com

ExactFile is a file integrity verification tool that incorporates the functions of programs like fsum, md5sum, sha1sum, and sfv. It is multi-threaded, which means it utilizes extra CPU cores on the computer to make checksum calculation of multiple files much faster. ExactFile (both console and GUI versions) fully supports Unicode.

OSSEC

Source: http://www.ossec.net

OSSEC is an open-source host-based intrusion detection system that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response.

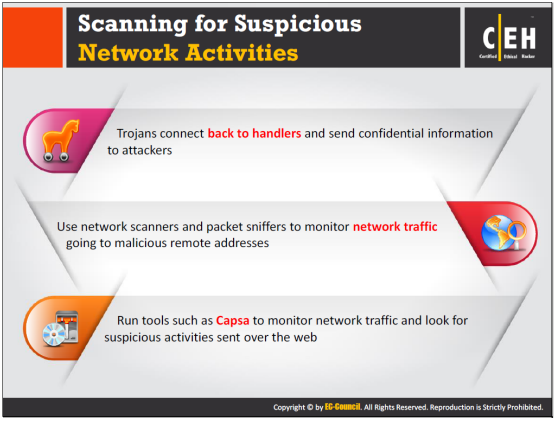
Features:

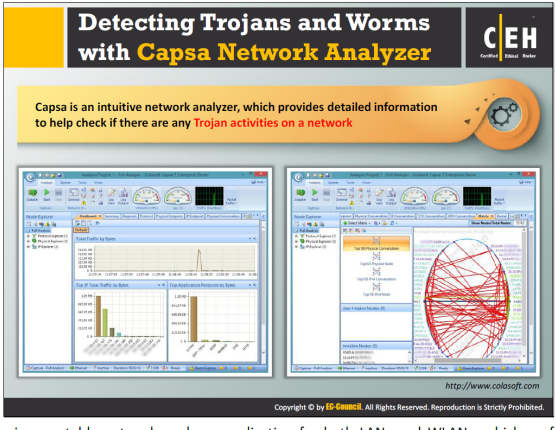
- File Integrity checking: detects and alerts if changes are made to the user system.
- Log Monitoring: collects, analyzes and correlates the logs to let the user know if something wrong is going on.
- Rootkit detection: Notifies when malware (Trojans, viruses, etc.) makes changes to the user system.

Checksum Verifier

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

Quick Checksum Verifier generates and checks file integrity by secure time proven algorithms like MD5 and SHA-1. One can easily create checksums (the digital fingerprints) of files and verify their integrity in the future. The operation comprises two steps: load the file, and paste the predefined checksum. It also supports command-line arguments with error-level output.



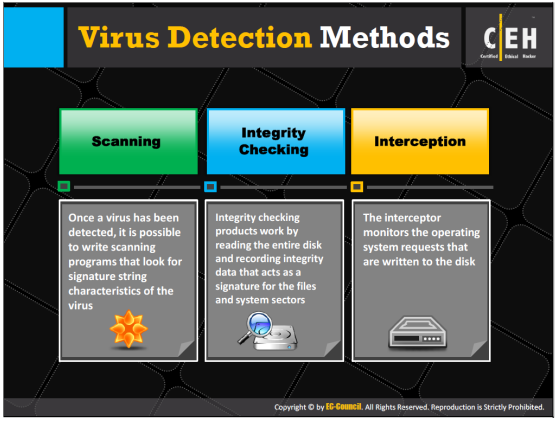


Capsa is a portable network analyzer application for both LANs and WLANs, which performs real-time packet capturing, 24-7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It helps network administrators or network engineers pinpoint and resolve 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 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 each

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



The most basic 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 header looks like something that a known sender would not normally say, the user must be careful about opening the email. This is because 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

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

Scanning

A virus scanner is an important 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 the virus protector regularly and the scan engine and update the virus signature database. 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 important aspects of virus scanning are:

Virus writers often create many new viruses by altering existing ones. What looks like a new virus, may take a little amount of time for creating them. Attackers make these changes frequently to throw off the scanners.

In addition to 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

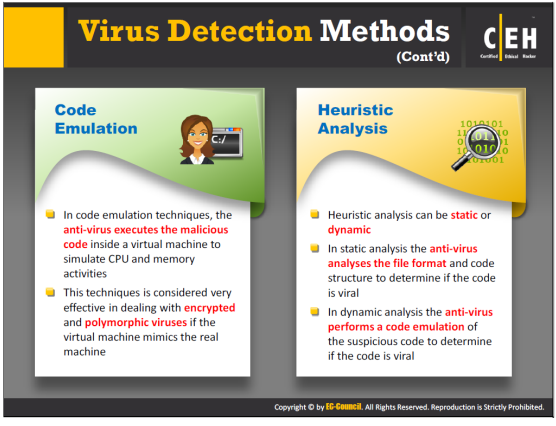
- Old scanners could prove to be unreliable. With the tremendous increase in new viruses, old scanners can quickly become obsolete. It is best to use the latest scanners available on the market.
- Because viruses appear more rapidly than do new scanners to battle them, even new scanners are not equipped 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 main use of an interceptor is for deflecting logic bombs and Trojans.
- The interceptor controls requests to the operating system for network access or actions that cause a threat to the program. If it finds such a request, the interceptor generally pops up and asks if the user wants to allow the request to continue.
- There are no dependable ways to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.
- Some viruses are capable of disabling the monitoring program itself.



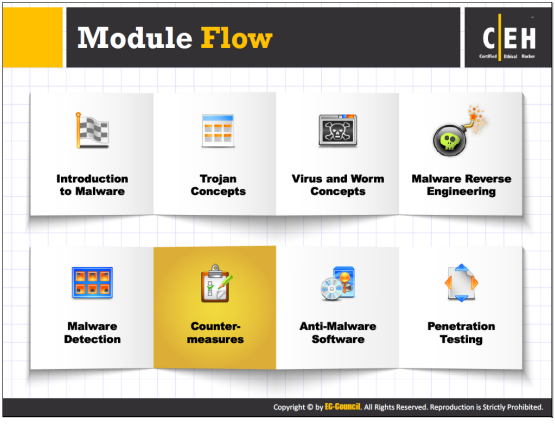
The following are some more methods for detecting viruses:

- **Code Emulation**

  By means of 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 effectively with encrypted and polymorphic virus. After running 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). Drawback of code emulation is that it is too slow, if the decryption loop is very long.

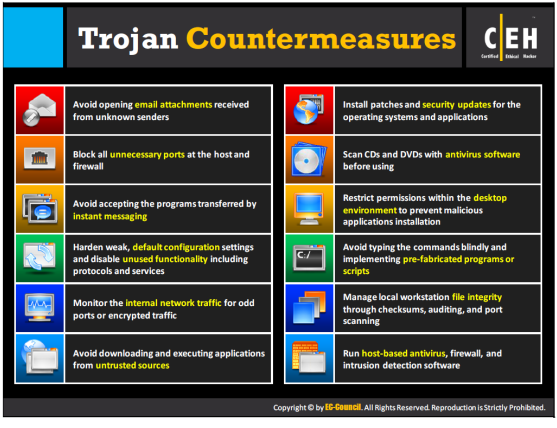
- **Heuristic Analysis**

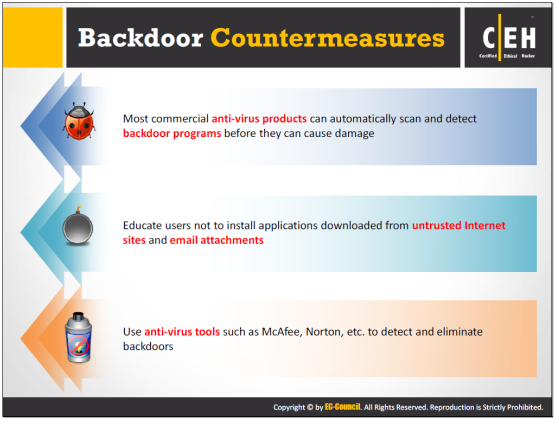
  This method helps in detecting new or unknown viruses that are usually variants of an already existing virus family. Heuristic analysis can be static or dynamic. In static analysis the anti-virus analyzes the file format and code structure to determine if the code is viral. In dynamic analysis the anti-virus 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.

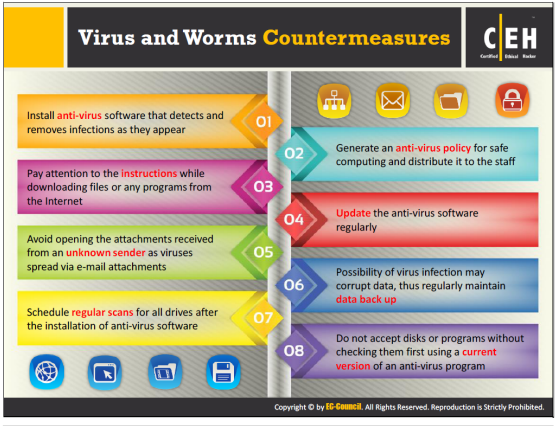


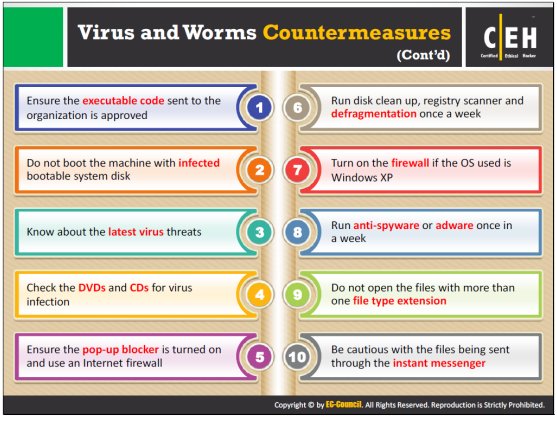
Malware is commonly used by an attacker to compromise target systems. Preventing malware from entering into the system is a far better solution than trying to eliminate it from an infected system, which is a far more difficult task.

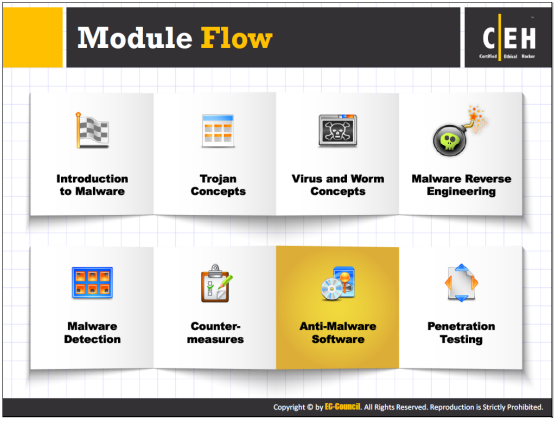
This section deals with various countermeasures that prevent malware from entering a system, and minimizing the risk caused by it upon its entry.





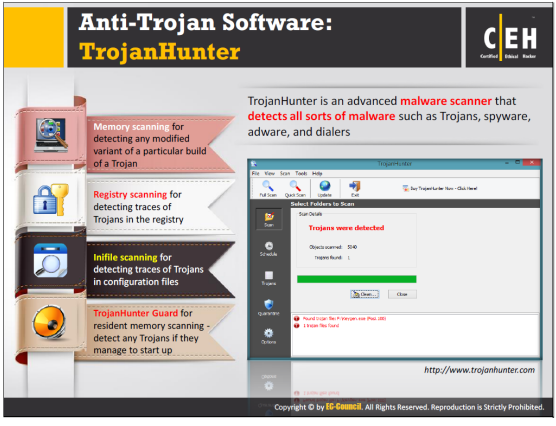






An attacker utilizes malware to commit online fraud or theft. Thus, the recommendation is to use anti-malware software that can help detect malware, remove it, and repair any damage it might cause.

This section lists and describes various anti-malware (anti-Trojan and anti-virus) software programs.



TrojanHunter is a malware scanner that detects and removes all sorts of malware, such as Trojans, spyware, adware, and dialers from the computer.

Features:

- File scan engine capable of detecting modified Trojans
- Memory scanning for detecting any modified variant of a particular build of a Trojan
- Registry scanning for detecting traces of Trojans in the registry
- Inifile scanning for detecting traces of Trojans in configuration files
- Port scanning for detecting open Trojan ports
- An Advanced Trojan Analyzer for finding whole classes of Trojans using advanced scanning techniques
- TrojanHunter Guard for resident memory scanning, to detect any Trojans that might manage to start up
- The Process list provides details about every running process on the system, including the path to the actual executable file

Source: http://www.trojanhunter.com

Below are listed some examples of useful Anti-Trojan software:

Anti Malware BOClean

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

BOClean runs in the background without being bothersome, and monitors the memory for any malware-related activity. When it discovers malware, it deletes it. BOClean has a memory-detection system, which it uses to catch malicious software earlier than most other anti-virus programs.

Features:

- Protects against "Trojan Horse" attacks, spam proxies, and spam relays
- Disconnects the threat without disconnecting you
- Automatic updates for the latest in anti-malware protection

Anti Hacker

Source: *http://www.hide-my-ip.com*

Anti Hacker is an anti-rootkit utility with four functions: keylogger detection, open port scanner, remote connection spy, and suspicious/unwanted program analyzer. This tool uses a variety of system scanning and analytical methods to detect hard-to-find programs that purposely evade anti-spyware tools and firewalls.

Features:

- Scans for three types of keyloggers: system hook-based, timer key capture, and Windows driver based keyloggers
- Finds out who is connecting to the computer without user knowing. It displays the remote computer's IP address, location, etc.
- Reveals all open ports and programs that are using each opened port, and closes unwanted open ports
- Finds invisible programs, spyware, covert desktop monitoring processes, hacking tools, and other possibly unwanted programs

XoftSpySE

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

XoftSpySE is the Spyware detection and removal application on the Internet. It protects from unwanted Spyware, Adware, malware, spybot, keyloggers, unwanted Toolbars, browser hijacking, spyware pop-ups, and so on.

SPYWAREfighter

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

SPYWAREfighter is an anti-spyware program used to detect and remove spyware, malware, Trojans, and other unwanted malicious software that can take over a computer.

Features:

- Registry scanners remove traces of malware from the registry
- Works with computers having multiple user accounts
- Removes malware that hides inside NTFS Alternate Data Streams
- Heuristic analysis helps to detect unknown threats
- Memory scan searches in all active applications of the system for running pests
- Monitors PC with real-time, scheduled, or manual scanners and an analysis tools option

Malwarebytes Anti-Malware Premium

Source: *http://www.malwarebytes.org*

Malwarebytes Anti-Malware Premium detects and removes malicious programs such as worms, rogues, dialers, Trojans, rootkits, spyware, exploits, bots, and other malware from the user's computer. It blocks hacking and phishing attempts, schedules automatic scanning, and offers three flexible scanning modes.

SUPERAntiSpyware

Source: http://www.superantispyware.com

SUPERAntiSpyware identifies potentially unwanted programs and securely removes them. It provides an even easier user interface by putting key tools, such as quarantine management, scan logs, and repair features in one place.

Features:

- Detects and removes spyware, adware and remove malware, Trojans, dialers, worms, keyloggers, hijackers, parasites, rootkits, rogue security products, etc.
- Repairs broken Internet connections, desktops, registry editing, etc.

Trojan Remover

Source: http://www.simplysup.com

Trojan Remover aids in the removal of malware—Trojan horses, worms, adware, and spyware—when standard anti-virus software either fails to detect them or fails to effectively eliminate them. It can disable or remove malware without the user having to manually edit system files or the Registry. It scans all the files loaded at boot time for Adware, Spyware, Remote Access Trojans, Internet Worms, and other malware. Trojan Remover also checks to see if Windows loads Files/Services, which are hidden by Rootkit techniques and warns if it finds any.

Twister Antivirus

Source: http://www.filseclab.com

Twister Antivirus integrates various security technologies such as Proactive Defense, Virtual Machine, Heuristic, iGene, Blackbox, Rollback, and Cloud Security. It defends against viruses, Trojans, spyware, and others.

Features:

- Watches all activities on PC and smartly decides whether they're malware
- Updates several times a day to ensure the safety of information
- Caches info of every scanned files which dramatically improves the performance
- Prevents Blue Screen of Death, and block zero-day exploits
- Provides cloud defense system based on digital neural network

STOPzilla AntiMalware

Source: http://www.stopzilla.com

STOPzilla AntiMalware operates as a primary defense against malware, and other threats, to keep personal data safe.

Features:

- Blocks, detects, and removes malware

- Works cooperatively with other Anti-virus software
- Has an extensive database of Malware Signatures

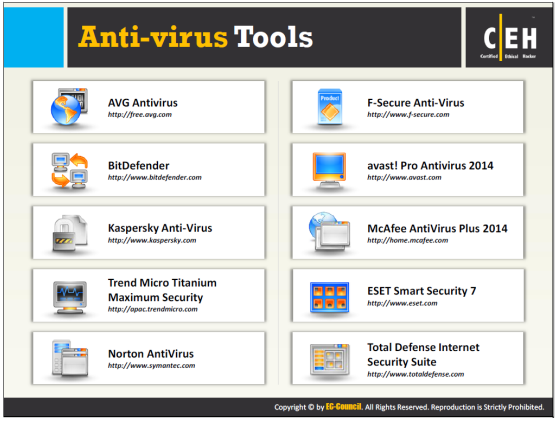
ZeroSpyware

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

ZeroSpyware prevents, detects, and removes spyware and rootkits. It blocks spyware attacks and protects the user's privacy and identity. It can delete a wide range of malware, ranging from old threats, including dialers, keyloggers, Trojans, browser hijackers, and the like, to newer ones such as mutating spyware and rootkits.

Immunet follows the Collective Immunity principle and provides cloud-based protection that is up-to-date against malware, including viruses, spyware, bots, worms, Trojans, and keyloggers without slowing down the PC. Collective Immunity in the sense, the protective resistance gained through community and collaborative intelligence to fight against computer malware infection.

Source: http://www.immunet.com



It is important to update the Antivirus program tools to keep an eye on the data passing through a system. Tools follow Specific or generic methods to detect virus. Generic methods look for a virus like performance, rather than a specific virus. This tool does not specify the virus type, but warns the 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, 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. The following list of anti-virus software defends against viruses:

AVG Antivirus

Source: http://free.avg.com

AVG Antivirus is software that provides protection against viruses, threats and malware.

Features:

- Stops unsecure links and files
- Prevents spying and data theft
- Securely deletes files to prevent snooping

- Protects from harmful downloads
- Encrypts and password-protects private files to keep the data safe

BitDefender

Source: http://www.bitdefender.com

The unique design of Bitdefender Antivirus cleans up the system from viruses and e-threats. It shields online privacy and protects personal identity.

Kaspersky Anti-Virus

Source: http://www.kaspersky.com

Kaspersky Anti-Virus defends against new and emerging viruses, spyware, and so on, without affecting the PC's performance. It allows identifying unknown malware and lets to rollback harmful activities in case of infected computers. It scans and warns about dangerous web links and emails.

Trend Micro Titanium Maximum Security

Source: http://apac.trendmicro.com

Trend Micro Titanium Maximum Security is a PC security suite that covers a variety of security concerns, including the standard firewall and spyware/virus controls, as well as other advanced features, such as data/phishing protection, parental controls and email security.

Features:

- Protection against online threats such as viruses, spyware, worms, and Trojans
- Protects on social networking sites such as Facebook, Google+, and Twitter
- Provides parental controls to safeguard kids online
- Offers online storage for up to 5 GB for digital files
- Protects against new web threats, Identity theft, and detects phishing
- Offers cloud-based protection

Norton Antivirus

Source: http://www.symantec.com

Norton Antivirus is a program that protects you from viruses, identity theft, and social media dangers.

Features:

- Keeps you safe when you surf, shop, and bank online
- Protects you from social media scams
- Stops online threats
- Blocks infected and dangerous downloads

F-Secure Anti-Virus

Source: http://www.f-secure.com

F-Secure Anti-Virus provides protection against viruses, spyware, infected e-mail attachments and other malware. It is a security solution that uses cloud-based technology to protect computer against existing online threats and to respond to new threats effectively as they appear.

avast! Pro Antivirus 2014

Source: http://www.avast.com

It is an anti-virus, anti-spyware, and anti-malware program which has a file-reputation scanning technology to scan an infected file in a virtual environment. It secures credit card or online banking data from being hacked with the SafeZone feature.

McAfee AntiVirus Plus 2014

Source: http://home.mcafee.com

McAfee Antivirus Plus 2014 provides protection against viruses, spyware, and malware. It scans and blocks all malicious contents before reaching the computer. It keeps the personal information safe from cyber criminals by blocking the botnets attempting to connect to your PC.

ESET Smart Security 7

Source: http://www.eset.com

ESET Smart Security is a security solution that combines maximum protection and a minimal system footprint. Its security technologies use artificial intelligence to detect and prevent infiltration by viruses, spyware, Trojan horses, worms, adware, rootkits, and other threats without hindering system performance or disrupting the computer.

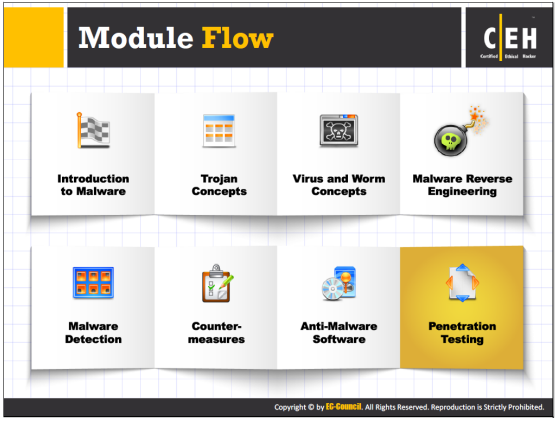
Total Defense Internet Security Suite

Source: http://www.totaldefense.com

Total Defense Internet Security Suite, which now includes Mobile Security, offers virus and spyware protection from emerging threats for desktops, laptops, and mobile devices. Its scanning engine protects against viruses, rootkits, FakeAV, spam, and other online threats.

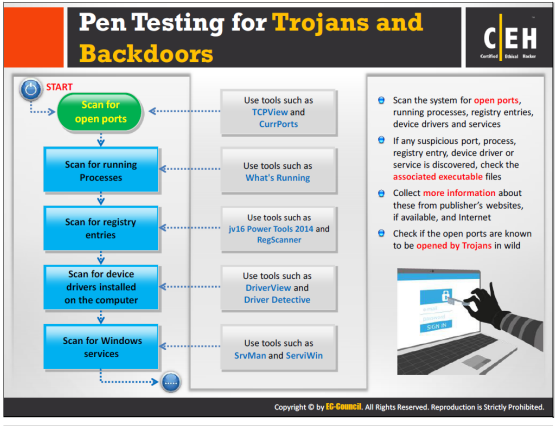
Features:

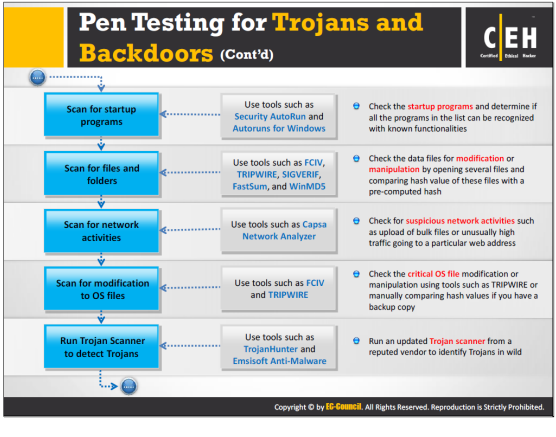
- Multi-layered, cloud-based protection
- Download protection for browsers such as IE, Firefox, and Chrome
- Virus and Spyware protection for Mobile Phones and Tablets
- Social Network Protection
- Antivirus and AntiSpyware
- Anti-spam and anti-phishing
- Parental controls

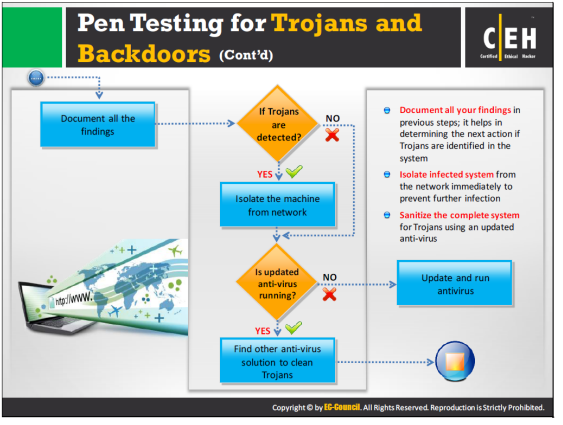


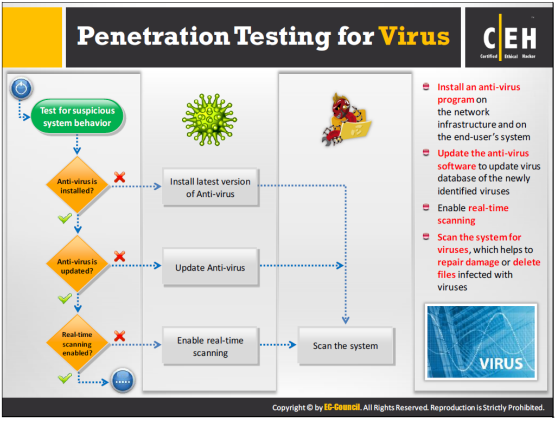
Penetration tester should follow the strategies of an attacker to effectively test the network or system against malware. Pen tester is supposed to perform all the available and newly emerged attacking techniques in order to figure out loopholes or vulnerabilities in the target organization's IT infrastructure and suggest countermeasures to enhance the security.

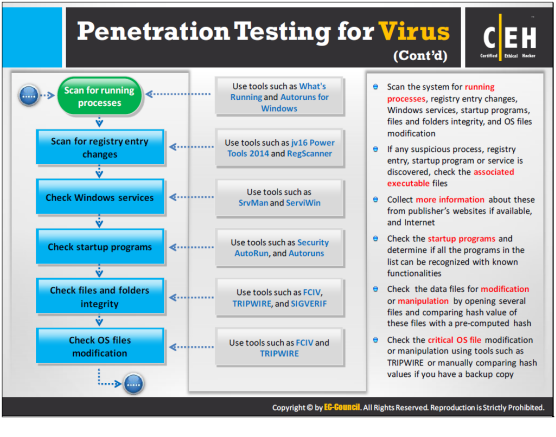
This section describes the steps involved in pen testing the target network for malware attacks.

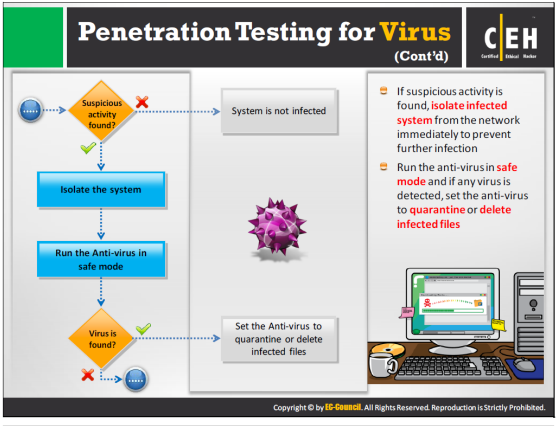


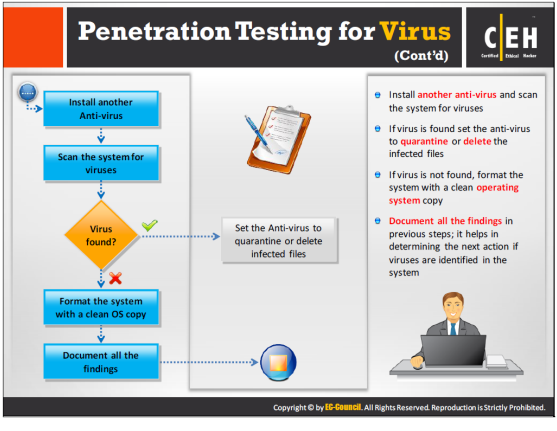


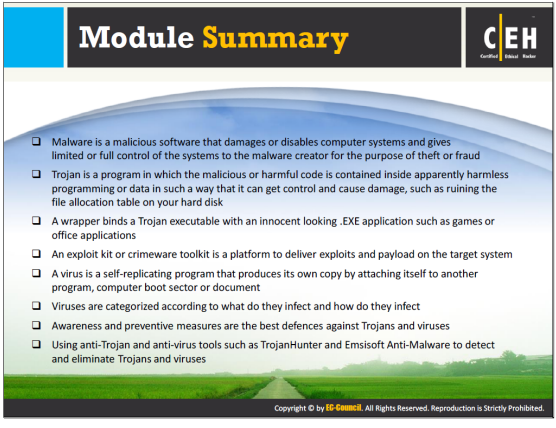












This module ends with an overview discussion on malware and malware propagation techniques, and an overview of Trojans, virus, worms, malware analysis process, techniques to detect malware, malware countermeasures, penetration testing, among others. In the next module, we will see how attackers, as well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