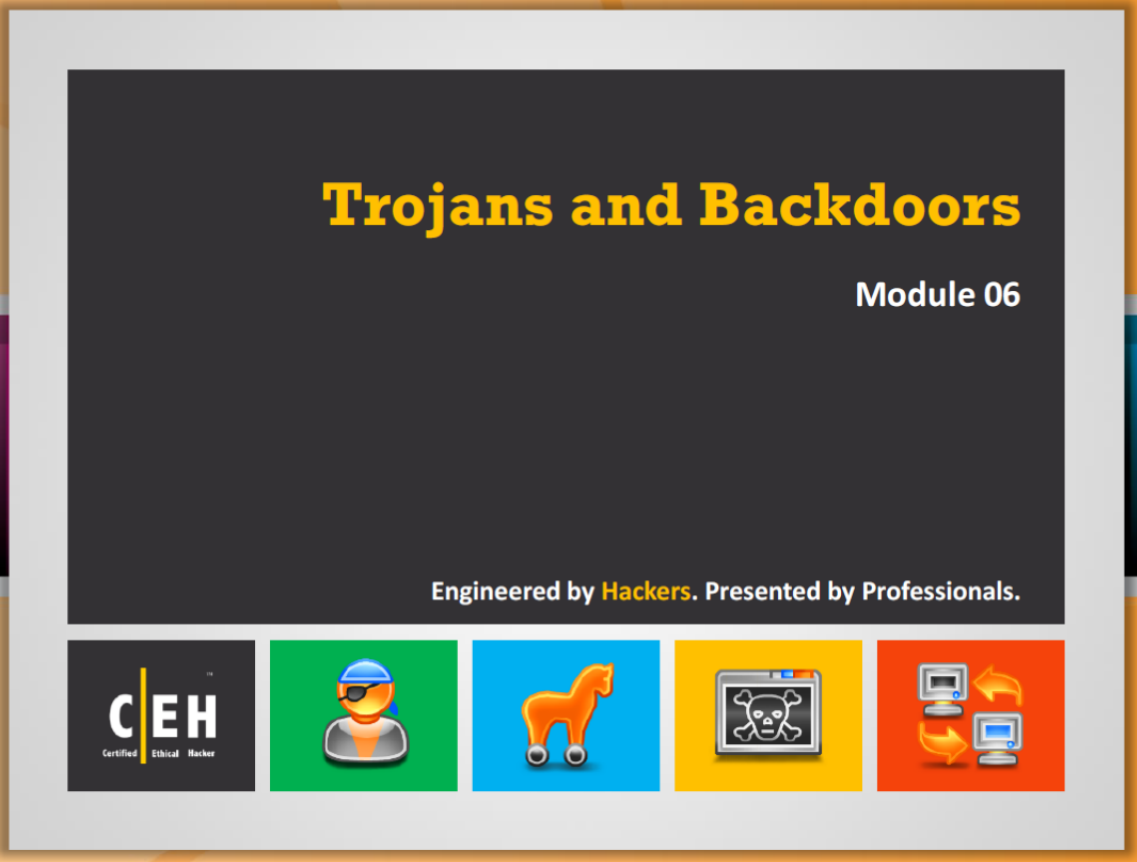
Trojans and Backdoors

Module 06



Ethical Hacking and Countermeasures v8

Module 06: Trojans and Backdoors

Exam 312-50

Security News

Cyber-Criminals Plan Massive Trojan Attack on 30 Banks

Source: http://securitywatch.pcmag.com

A large-scale coordinated **Trojan attack** to launch fraudulent wire transfers may be headed your way. And it has nothing to do with the recent wave of denial-of-service attacks.

A group of cybercriminals appears to be actively recruiting up to **100 botmasters** to participate in a complicated man-in-the-middle hijacking scam using a variant of the Gozi Trojan, RSA's **FraudAction** research team said in a blog post recently. The team put together the warning after weeks of monitoring underground chatter.

As many as 30 financial institutions in the United States may be targeted in this "blitzkrieg-like" series, said Mor Ahuvia, a **cyber-crime communications** specialist at RSA FraudAction. It's possible these well-known and high-profile institutions were selected, not because of "anti-American motives," but simply because American banks are less likely to have deployed two-factor authentication for private banking consumers, Ahuvia said. European banks generally require all consumers to use two-factor for wire transfers, making it harder to launch a man-in-the-middle session hijacking attack.

"A cyber gang has recently communicated its plans to launch a Trojan attack spree on 30 American banks as part of a large-scale orchestrated crimeware campaign," Ahuvia said.

Potential targets and relevant law enforcement agencies have already been notified, RSA said.

RSA FraudAction was not sure how far along the recruitment campaign has gone, or when the attacks are expected. While it's possible revealing the gang's plans may cause the criminals to scuttle their operation, it may just cause the group to modify the attack.

"There are so many Trojans available and so many points of failure in security that could go wrong, that they'd still have some chance of success," Ahuvia said.

Anatomy of the Attack

The proposed cyber-attack consists of several parts. The first part involves infecting victim computers with the variant of the Gozi Trojan, which RSA has dubbed **Gozi Prinimalka**, Once the computer has been compromised, it will communicate with the botmaster's computer, which has a "virtual machine syncing module," capable of duplicating the victim's PC settings, such as the time zone, screen resolution, cookies, browser type, and installed software IDs, into a virtual machine, RSA said.

When the attacker accesses victim accounts using the cloned system, the virtual machine appears to be a legitimate system using the last-known IP address for the victim's computer, RSA said. This cloning module would make it easy for the attackers to log in and initiate wire transfers. The attackers also plan to use VoIP phone flooding software to prevent victims from receiving confirmation calls or texts verifying online account transfers and activity, RSA said.

The recruits have to make an initial investment in hardware and agree to training on how to deploy the Gozi Trojan, Ahuvia wrote. They will receive executable files, but not the compilers used to create the Trojan. In return, the new partners in this venture will receive a cut of the profits.

Trojan Behind Previous Attacks

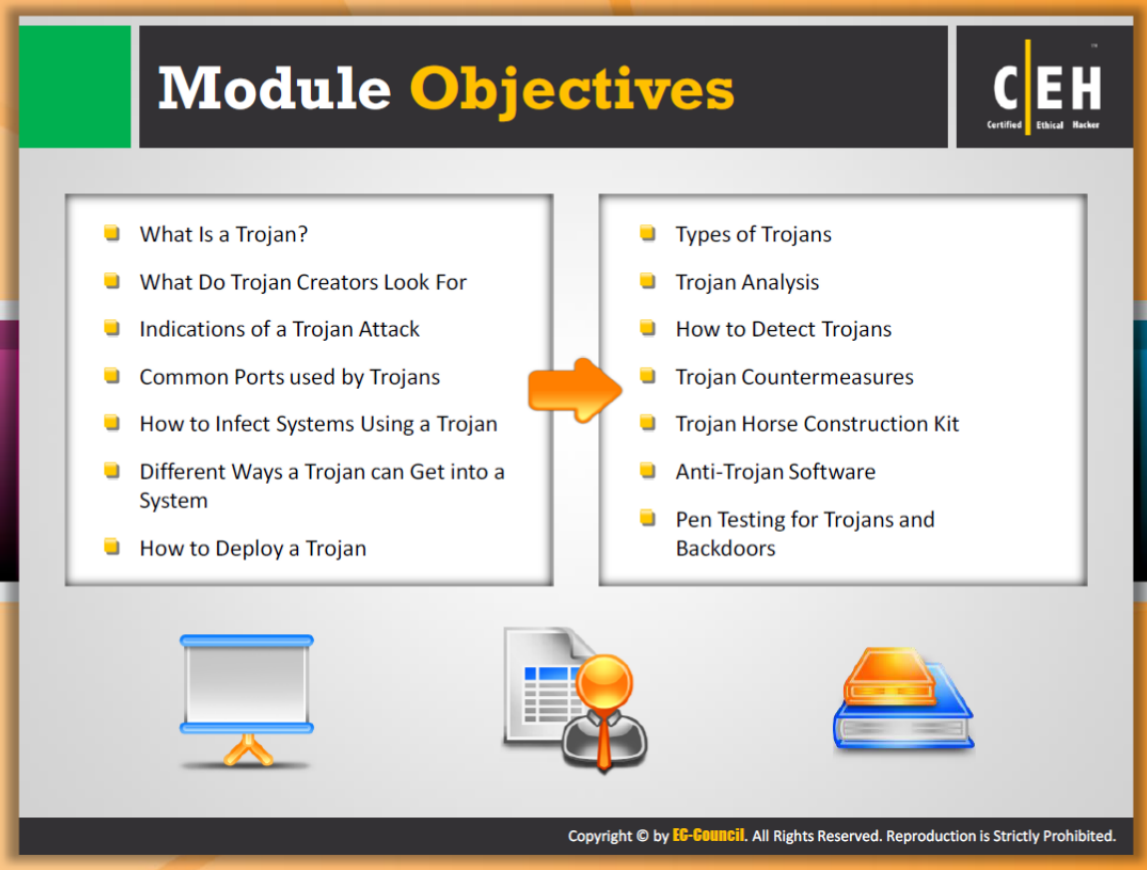
The Trojan is not as well-known as others, such as **SpyEye** or **Citadel**, nor is it as widely available, Ahuvia said. Its relative obscurity means antivirus and security tools are less likely to flag it as malicious.

RSA has linked the Gozi Trojan to previous attacks responsible for more than **$5 million** in losses in the United States in 2008. The researchers have linked the Trojan to a group called the HangUp Team, and speculated the same group was behind this latest campaign.

The way the attack is structured, it is very likely the targeted institutions won't even realize they'd been affected till at least a month or two after the attacks. "The gang will set a pre-scheduled D-day to launch its spree, and attempt to cash out as many compromised accounts as possible before its operations are ground to a halt by security systems," Ahuvia said.

By Author: Fahmida Y. Rashid

http://securitywatch.pcmag.com/none/303577-cyber-criminals-plan-massive-trojan-attack-on-30-banks

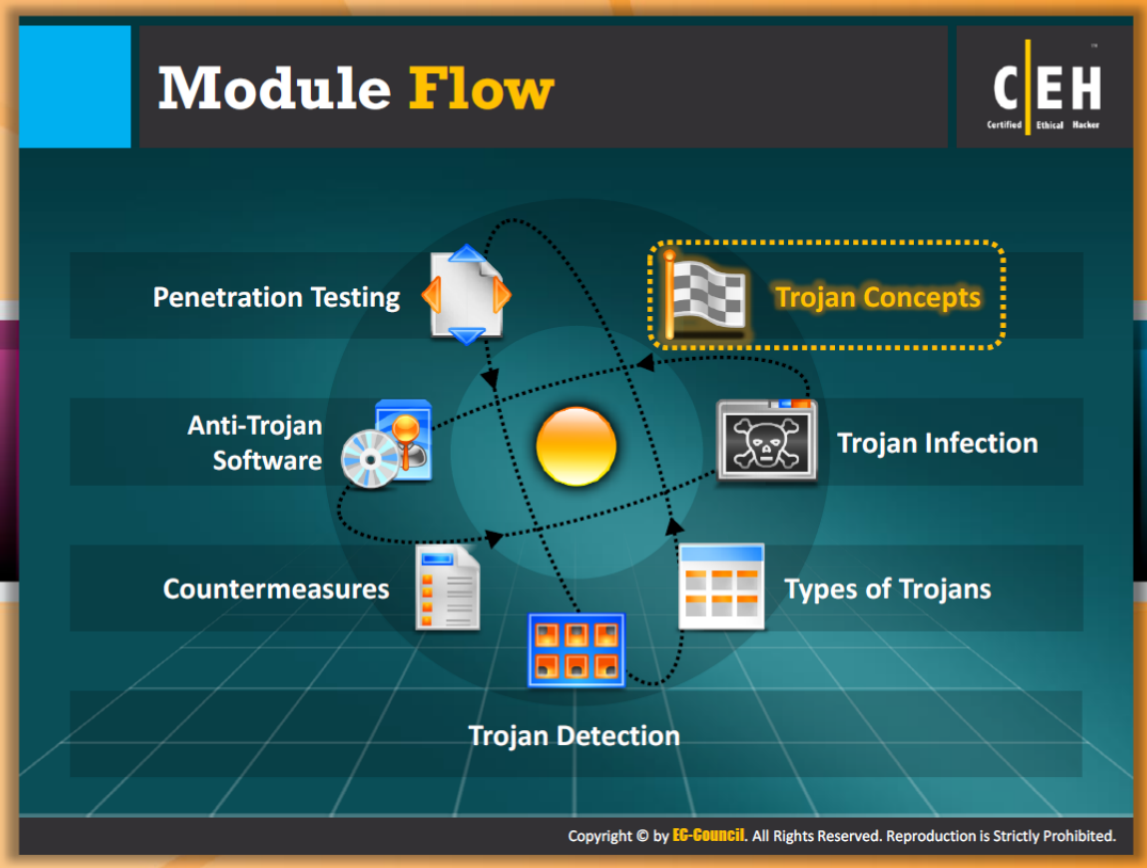


Module Objectives

The main objective of this module is to provide you with knowledge about various kinds of **Trojans** and **backdoors**, the way they propagate or spread on the Internet, symptoms of these attacks, consequences of Trojan attacks, and various ways to protect network or system resources from Trojans and backdoor. This module also describes the penetration testing process to enhance your security against Trojans and backdoors.

This module makes you familiarize with:

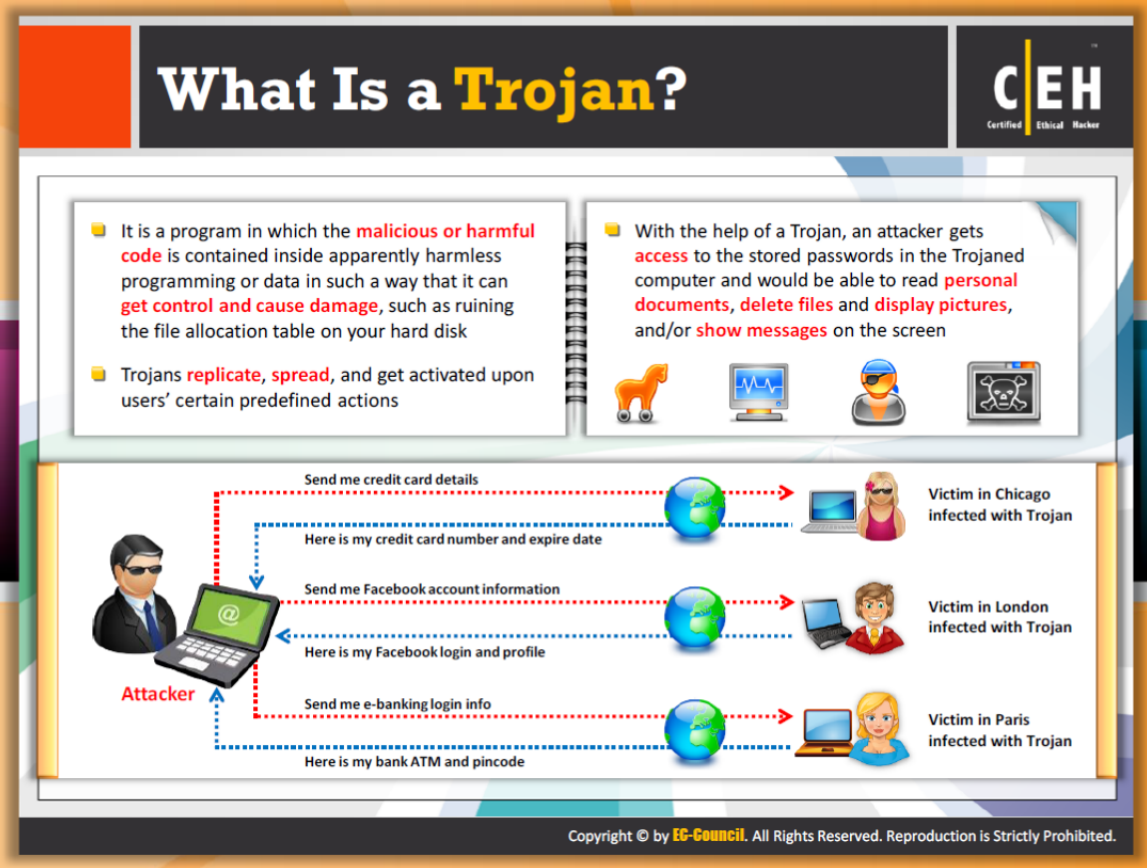
- What Is a Trojan?
- What Do Trojan Creators Look For?
- Indications of a Trojan Attack
- Common Ports Used by Trojans
- How to Infect Systems Using a Trojan
- Different Ways a Trojan Can Get into a System
- How to Deploy a Trojan
- Types of Trojans
- Trojan Analysis
- How to Detect Trojans
- Trojan Countermeasures
- Trojan Horse Construction Kit
- Anti-Trojan Software
- Pen Testing for Trojans and Backdoors



Module Flow

To understand various **Trojans** and **backdoors** and their impact on network and system resources, let's begin with basic concepts of Trojans. This section describes Trojans and highlights the purpose of Trojans, the symptoms of **Trojan attacks**, and the common ports used by Trojans.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	



What Is a Trojan?

According to **Greek mythology**, the Greeks won the **Trojan War** by entering in to the fortified city of Troy hiding in a huge, hollow wooden horse. The Greeks built a huge wooden horse for their soldiers to hide in. They left the horse in front of the gates of Troy. The Trojans thought it to be a gift from the Greeks, who had withdrawn from the war, and so they transported the horse into their city. At night, the Spartan soldiers broke through the wooden horse, and opened the gates for their soldiers who eventually destroyed the city of Troy.

Taking a cue from Greek mythology, a computer Trojan is defined as a "**malicious, security-breaking program** that is disguised as something benign." A computer Trojan horse is used to enter a **victim's computer undetected**, granting the attacker unrestricted access to the data stored on that computer and causing immense damage to the victim. For example, a user downloads what appears to be a movie or a music file, but when he or she runs it, it unleashes a dangerous program that may erase the **unsuspecting user's disk** and send his or her credit card numbers and passwords to a stranger. A Trojan can also be wrapped into a legitimate program, meaning that this program may have hidden functionality that the user is unaware of.

In another scenario, a victim may also be used as an intermediary to attack others—without his or her knowledge. Attackers can use the victim's computer to commit illegal denial-of-service attacks such as those that virtually crippled the **DALnet IRC** network for months on end.

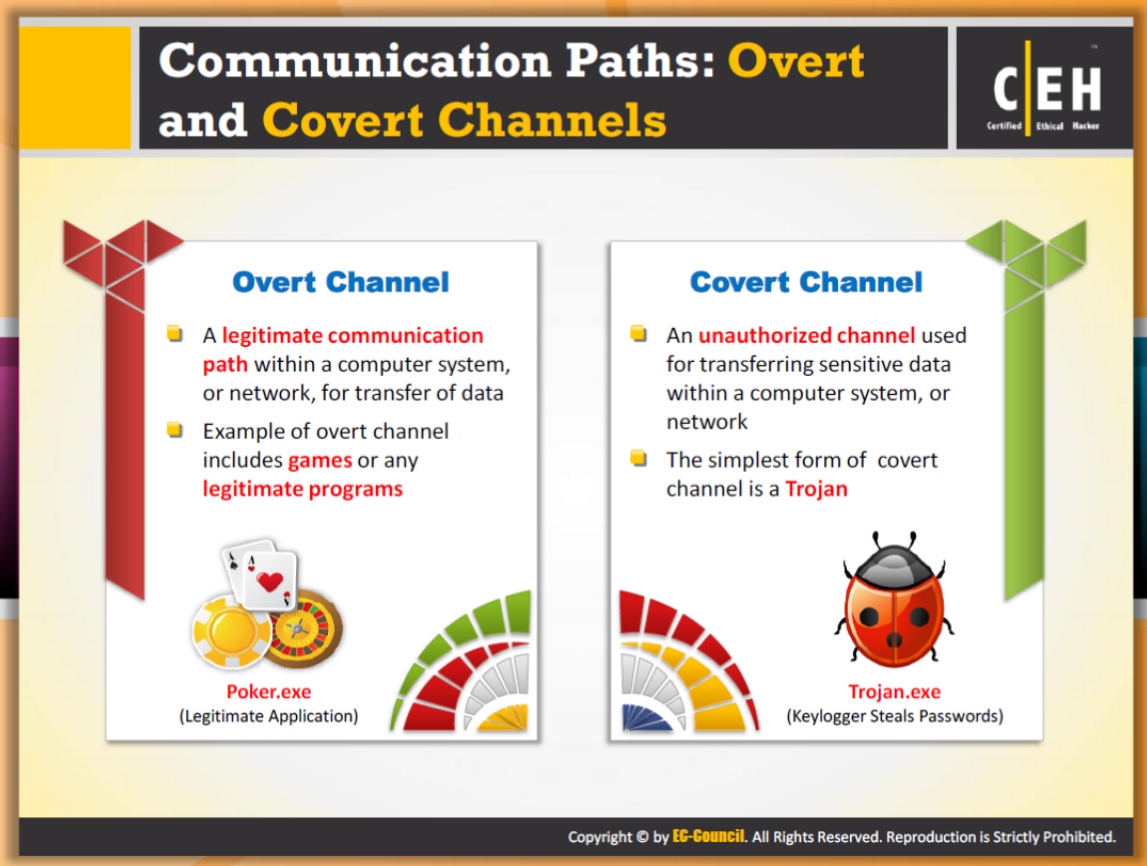
(DALnet is an Internet relay chat (IRC) network that is a form of instant communication over the network.)

Trojan horses work on the same level of privileges that the victim user has. If the victim had the privileges, Trojan can delete files, transmit information, modify existing files, and install other programs (such as programs that provide **unauthorized network access** and execute privilege-elevation attacks). The Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If successful, the Trojan horse can operate with increased privileges and may install other malicious codes on the victim's machine.

A compromise of any system on a network may affect the other systems on the network. Systems that **transmit authentication credentials** such as passwords over shared networks in clear text or in a trivially encrypted form are particularly vulnerable. If a system on such a network is compromised, the intruder may be able to record user names 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 and, thereby, cause the remote system to incur liabilities.

FIGURE 6.1: Attacker extracting sensitive information from the system's infected with Trojan



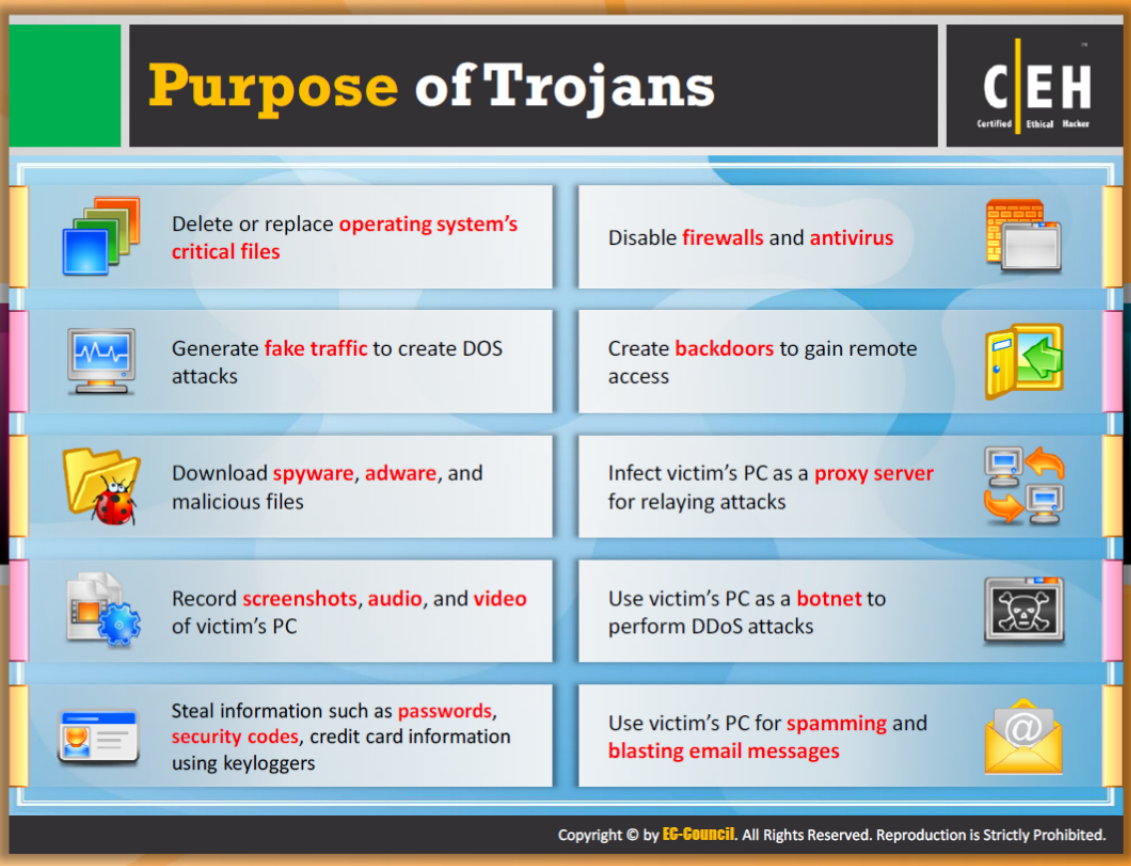
Communication Paths: Overt and Covert Channels

Overt means something that is explicit, obvious, or evident, whereas covert means something that is secret, concealed, or hidden. An overt channel is a legal, secure channel for the **transfer of data** or **information** within the network of a company. This channel is within the **secure environment** of the company and works securely for the transfer of 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 by which an attacker can hide data in a protocol that is undetectable. They rely on a technique called tunneling, which allows one protocol to be carried over another protocol. Covert channels are generally not used for information exchanges, so they cannot be detected by using standard **system security methods**. Any process or bit of data can be a covert channel. This makes it an attractive mode of transmission for a Trojan, since an attacker can use the covert channel to install the backdoor on the target machine.

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 the presence of a covert channel by selecting components of the overt channels with care that are idle or not related	The simplest form of covert channel is a Trojan

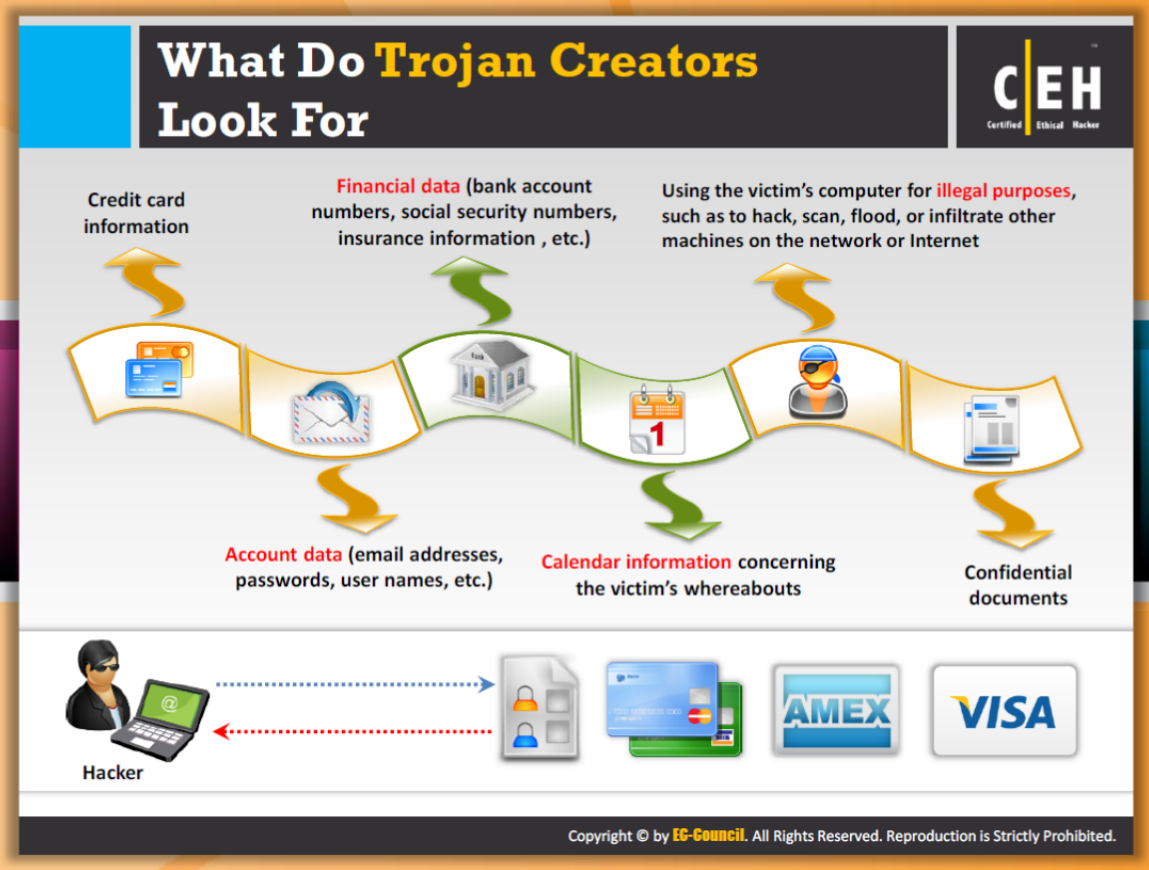
TABLE 6.1: Comparison between Overt Channel and Covert Channel



Purpose of Trojans

Trojan horses are the dangerous malicious programs that affect computer systems without the **victim's knowledge**. The purpose of Trojan is to:

- Delete or replace the operating system's critical files
- Generate fake traffic to create DOS attacks
- Download spyware, adware, and malicious files
- Record screenshots, and audio and video of the victim's PC
- Steal information such as passwords, security codes, and credit card information using keyloggers
- Disable firewalls and antivirus software
- Create backdoors to gain remote access
- Infect a victim's PC as a proxy server for relaying attacks
- Use a victim's PC as a botnet to perform **DDoS attacks**
- Use a victim's PC for spamming and blasting email messages



What Do Trojan Creators Look For?

Trojans are written to **steal information** from other systems and to exercise control over them. Trojans look for the **target's personal information** and, if found, return it to the Trojan writer (attacker). They can also allow attackers to take **full control over a system**.

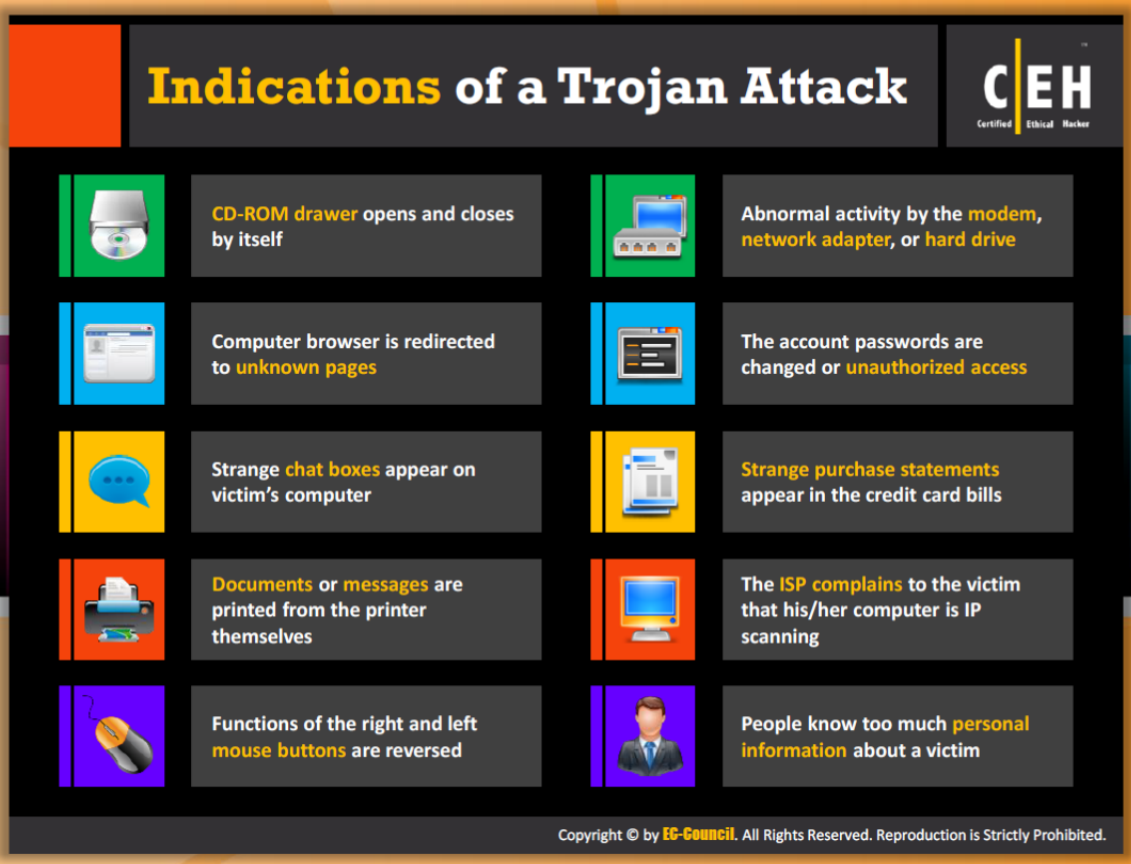
Trojans are not solely used for **destructive purposes**; they can also be used for spying on someone's machine and accessing private and/or sensitive information.

Trojans are created for the following reasons:

- To steal sensitive information, such as:
  - Credit card information, which can be used for domain registration, as well as for shopping.
  - Account data such as email passwords, dial-up passwords, and web services passwords. Email addresses also help attackers to spam.
  - Important company projects including presentations and **work-related papers** could be the targets of these attackers, who may be working for rival companies.

- Attackers can use the target's computers for storing archives of **illegal materials**, such as child pornography. The target can continue to use their computer, and have no idea about the illegal activities for which their computer is being used.
- Attackers can use the target computer as an **FTP Server** for pirated software.
- **Script kiddies** may just want to have fun with the target's system. They might plant a Trojan in the system, which then starts acting strangely: the CD tray opens and closes frequently, the mouse functions improperly, etc.
- The compromised system might be used for other illegal purposes, and the target would be held responsible for all illegal activities, if the authorities discover them.

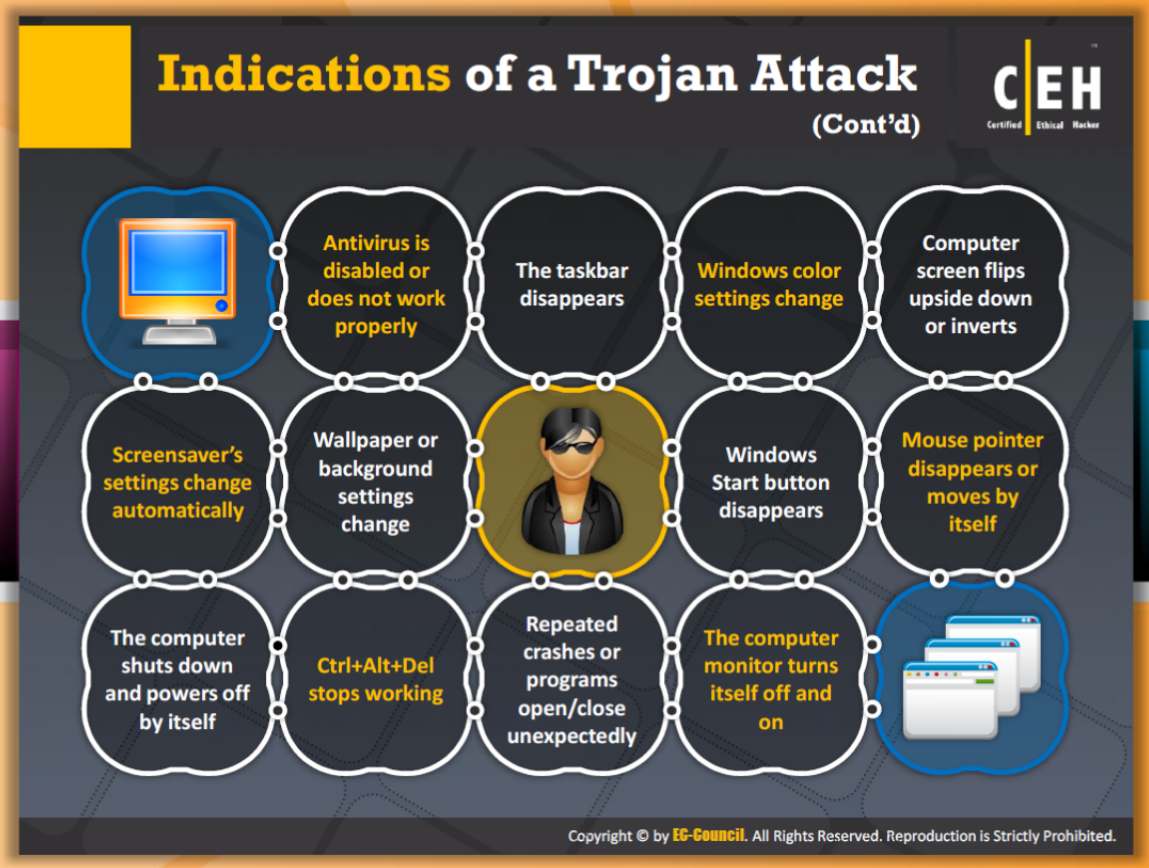
FIGURE 6.2: Hacker stealing credit card information from victim



Indications of a Trojan Attack

A Trojan is software designed to **steal data** and **demolish** your system. It creates a **backdoor** to attackers to intrude into your system in **stealth mode**. The system becomes vulnerable to the Trojan and attackers can easily launch their attack on the system if it is not **safeguarded**. Trojans can enter your system using various means such as email attachments, downloads, instant messages, open ports, etc. The following are some of the indications that you may notice on your system when it is attacked by the Trojan:

- CD-ROM drawer opens and closes by itself
- Computer browser is redirected to unknown pages
- Strange chat boxes appear on target's computer
- Documents or messages are printed from the printer
- Functions of the right and left mouse buttons are reversed
- Abnormal activity by the modem, network adapter, or hard drive
- The account passwords are changed or unauthorized access
- Strange purchase statements appear in the credit card bills
- The ISP complains to the target that his or her computer is IP scanning
- People know too much personal information about a target



Indications of a Trojan Attack (Cont'd)

Though Trojans run in **stealth mode**, they exhibit some characteristics, observing which; you can determine the existence of Trojans on your computer. The following are typical symptoms of a Trojan horse virus infection:

- **Antivirus** software is disabled or does not work properly
- The taskbar disappears
- Windows color settings change
- Computer screen flips upside down or inverts
- Screensaver's settings change automatically
- Wallpaper or background settings change
- Windows Start button disappears
- Mouse pointer disappears or moves by itself
- The computer shuts down and powers off by itself
- **Ctrl+Alt+Del** stops working
- Repeated crashes or programs open/close unexpectedly
- The computer monitor turns itself off and on

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

Common Ports Used by Trojans

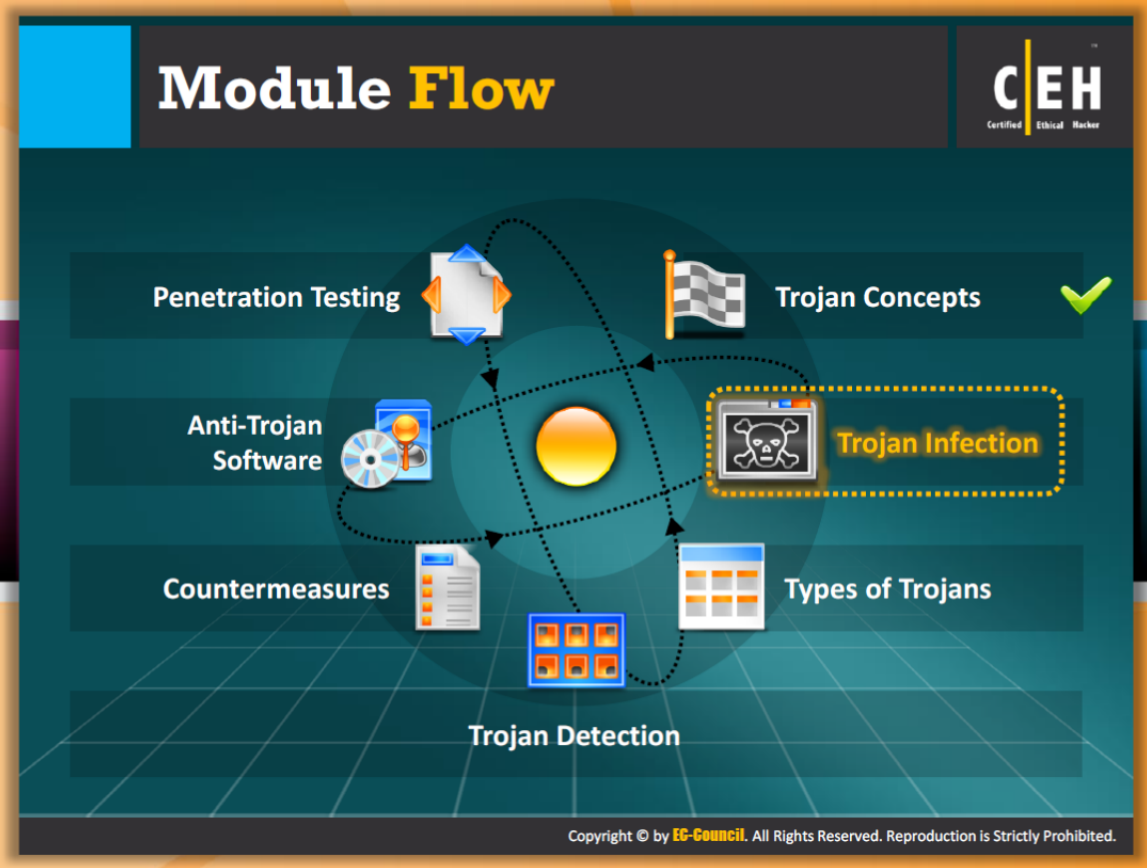
IP ports play an important role in **connecting your computer** to the Internet and surfing the web, downloading information and files, running software updates, and sending and receiving emails and messages so that you can connect to the world. Each computer has unique sending and receiving ports for each function.

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

There are different states, but the "**listening**" state is the important one in this context. This state is generated when a system listens for a port number when it is waiting to make a connection with another system. Trojans are in a listening state when a **system is rebooted**. Some Trojans use more than one port as one port may be used for "listening" and the other(s) for data transfer.

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

TABLE 6.2: Common ports used by Trojans

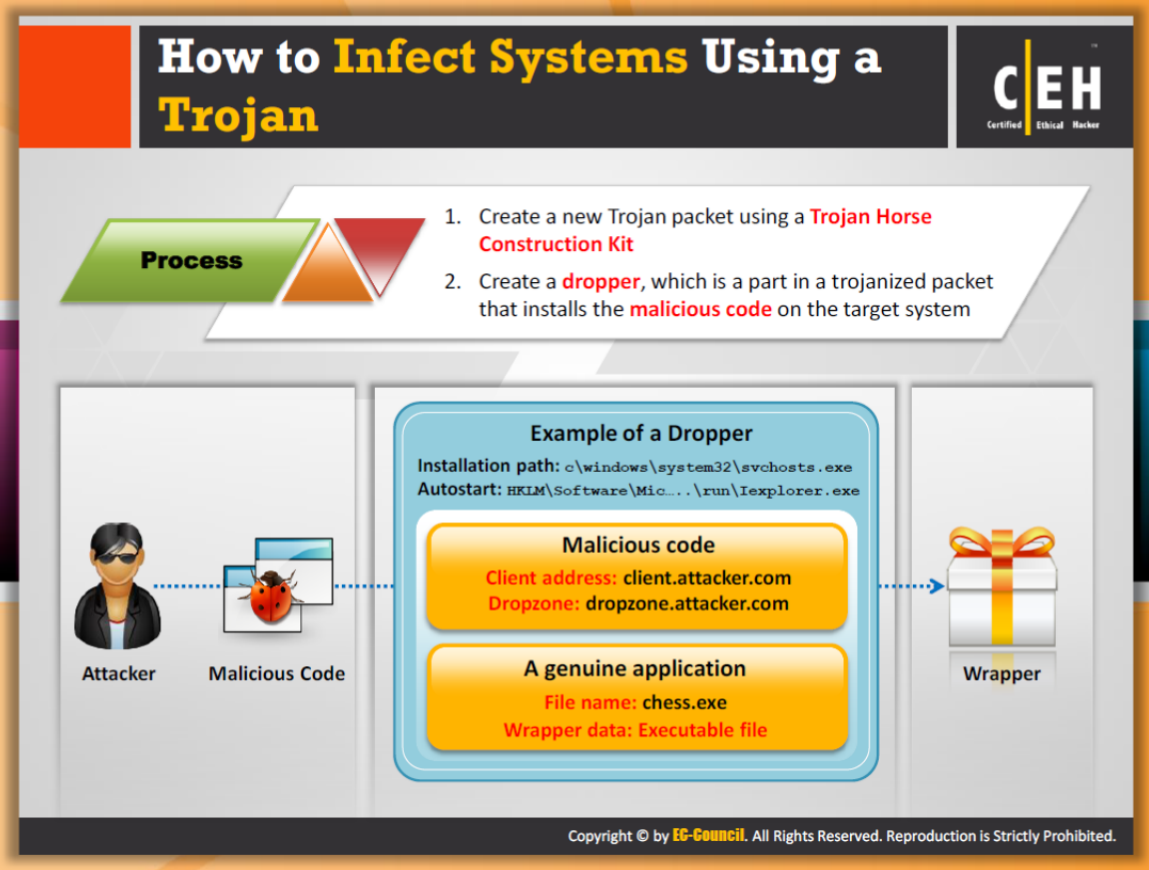


Module Flow

So far we have discussed various Trojan concepts. Now we will discuss Trojan infections.

Trojan Concepts	Countermeasures
Trojan Infection	Anti-Trojan Softwares
Types of Trojans	Penetration Testing
Trojan Detection	

In this section, we will discuss the different methods adopted by the attacker for installing Trojans on the victim's system and infecting their system with this malware.



How to Infect Systems Using a Trojan

An attacker can **control** the **hardware as well as software** on the system remotely by installing Trojans. When a Trojan is 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 infect the system using Trojans in many ways:

- Trojans are included in bundled shareware or downloadable software. When a user downloads those files, Trojans are installed onto the systems automatically.
- Users are tricked with the **different pop-up ads**. It is programmed by the attacker in such a way that it doesn't matter if is the user clicks YES or NO; a download starts and the Trojan is installed onto the system automatically.
- Attackers send Trojans through email attachments. When those attachments are opened, the Trojan is installed on the system.
- Users are sometimes tempted to click on different kinds of files such as greeting cards, porn videos, images, etc., where Trojans are silently installed one the system.

The step-by-step process for infecting machines using a Trojan is as follows:

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

Step 2: Create a dropper, which is a part in a Trojanized packet that installs the malicious code on the target system.

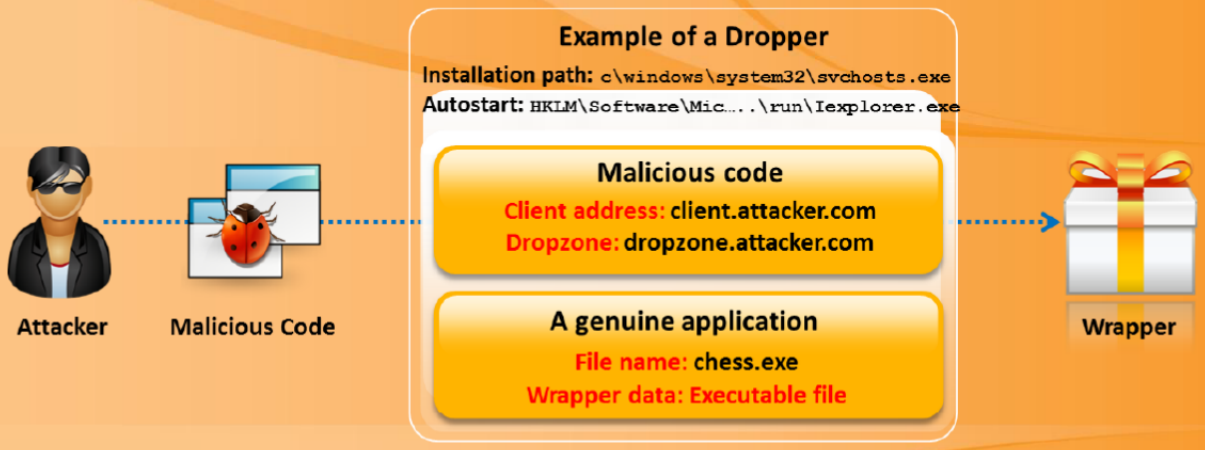
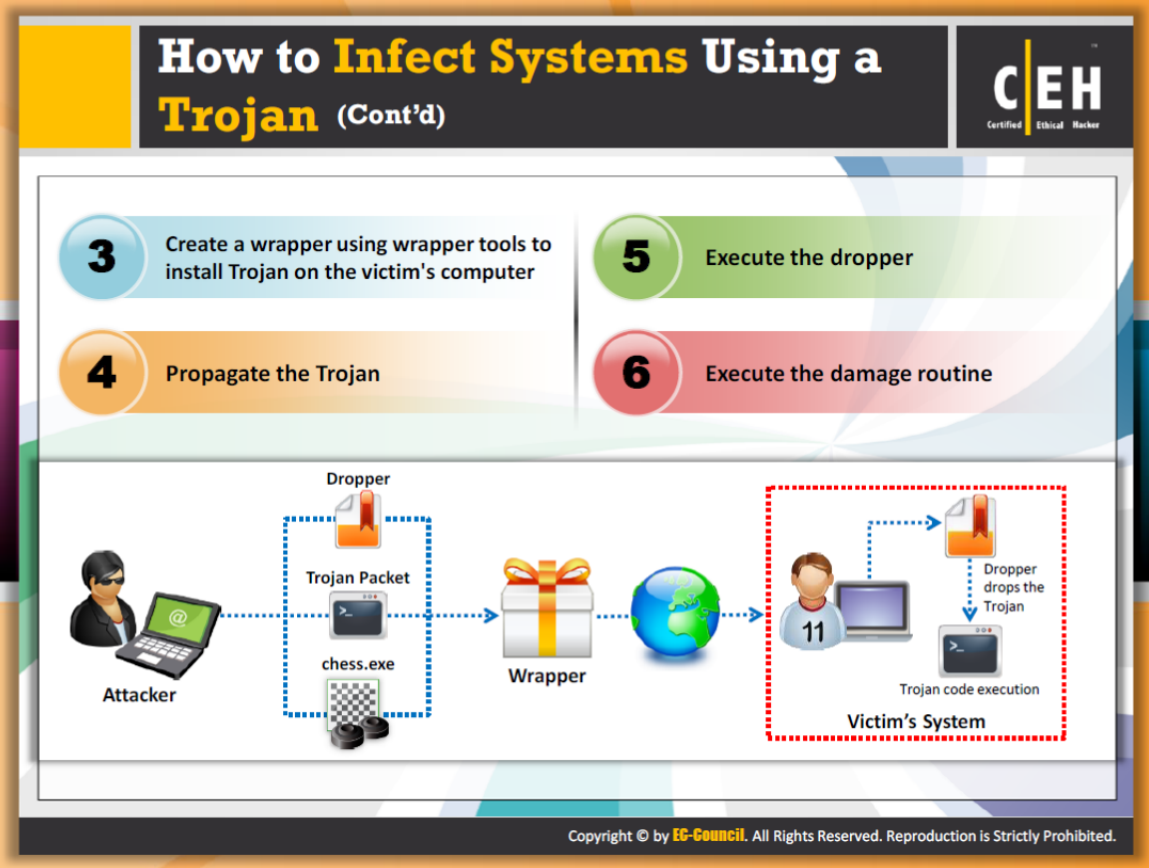


FIGURE 6.3: Illustrating the process of infecting machines using Trojans (1 of 2)



How to Infect Systems Using a Trojan (Cont'd)

Step 3: Create a wrapper using tools to install the Trojan on the **victim's computer**. By using various tools like petite.exe, Graffiti.exe, EliteWrap, etc., a wrapper is created to install the Trojan on the victim's computer.

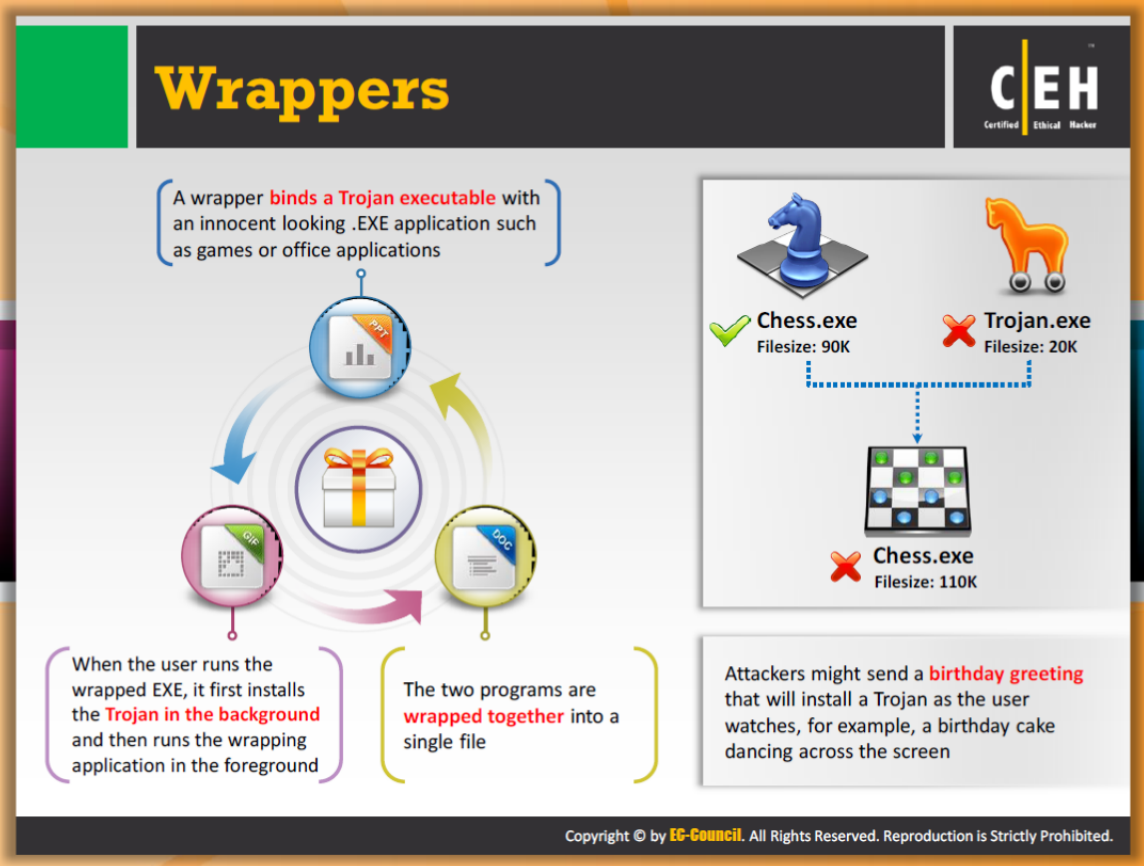
Step 4: Propagate the Trojan. **Computer virus propagation** (spreading) can be done through various methods:

- An automatic execution mechanism is one method where traditionally it was spread through floppy disks and is now spread through various external devices. Once the computer is booted, the virus automatically spreads over the computer.
- Even viruses can be propagated through emails, Internet chats, network sharing, P2P file sharing, network redirecting, or hijacking.

Step 5: Execute the Dropper. **Dropper** is used by attackers to **disguise their malware**. The user is confused and believes that all the files are genuine or known files. Once it gets loaded into the host computer, it helps other malware to get loaded and perform the task.

Step 6: Execute the damage routine. Most computer viruses contain a **Damage Routine** that delivers payloads. A payload sometimes just displays some images or messages whereas other payloads can even delete files, reformat hard drives, or cause other damage.

FIGURE 6.4: Illustrating the process of infecting machines using Trojans (2 of 2)



Wrappers

Source: http://www.objs.com

Wrappers are used to 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, since most antivirus software is not able to detect the signatures in the file.

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

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

Users can be tricked into installing **Trojan horses** by being enticed or frightened. 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 entice him or her to install it. Although it may, in fact, be a game, it may also be taking other action that is not readily apparent to the user, such as

deleting files or mailing sensitive information to the attacker. In another instance, wan attacker sends a birthday greeting that will install a Trojan as the user watches, such as a birthday cake dancing across the screen.

FIGURE 6.5: Wrappers

Wrapper Covert Programs

Kriptomatik

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

It has the following features:

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

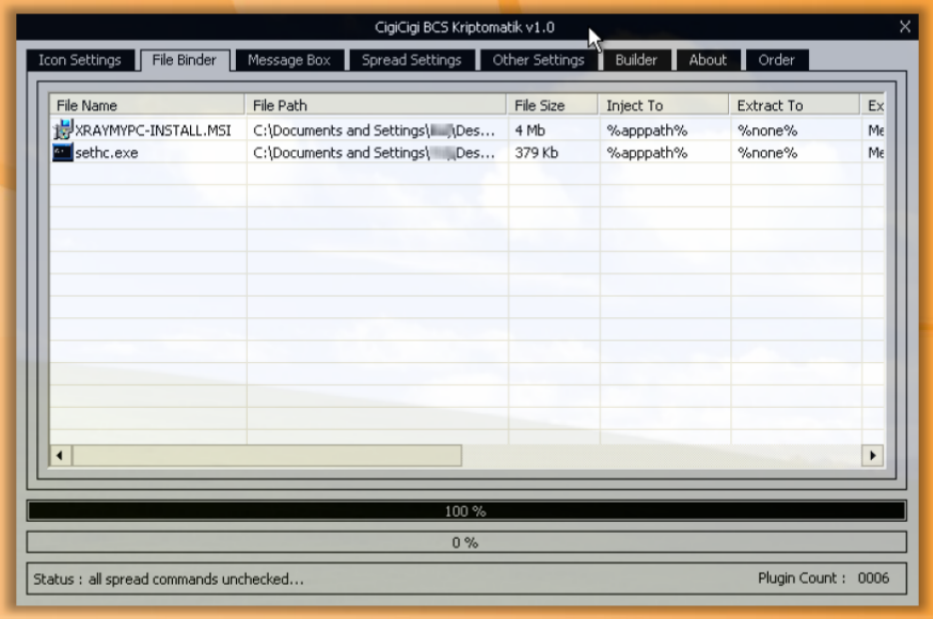


FIGURE 6.6: Kriptomatik screenshot

Advanced File Joiner

Advanced File Joiner is software that is used to **combine** and **join** various files into a single file. 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 same size, format, and encoding. This tool cannot be used effectively for joining a file format containing head information such as AVI, BMP, JPEG, and DOC files. So, for each of these types of file formats, you have to use specific software join program.

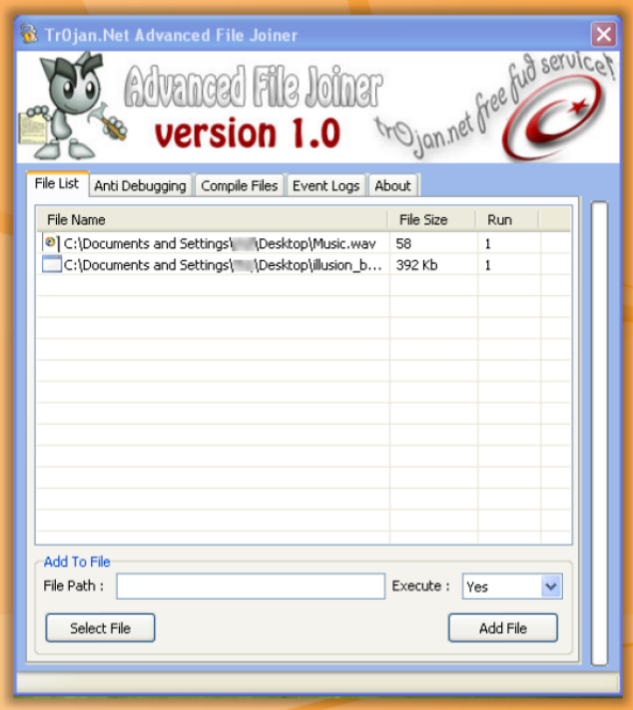


FIGURE 6.7: Advanced File Joiner Screenshot

SCB LAB's – Professional Malware Tool

Professional Malware Tool is designed to encrypt (crypter), together (binder), download (downloader), and files spread (spread).

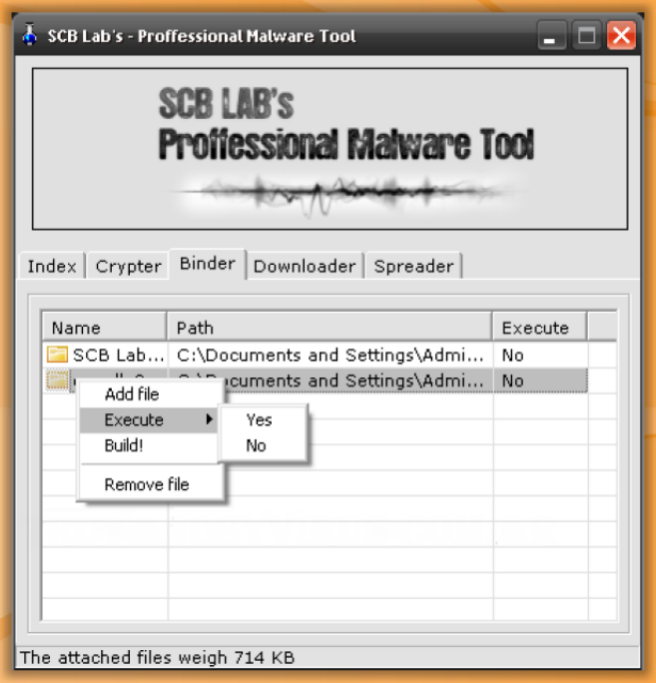
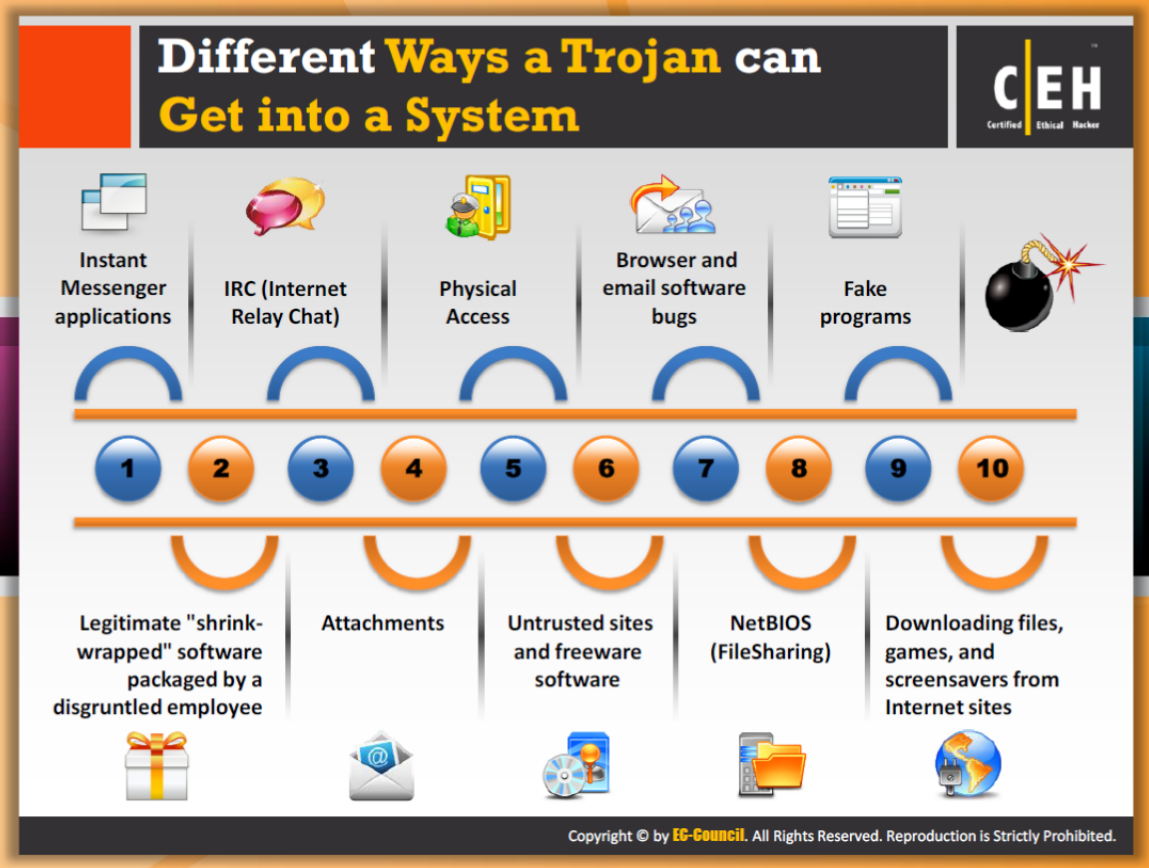


FIGURE 6.8: SCB LAB's – Professional Malware Tool Screenshot



Different Ways a Trojan Can Get into a System

Different access points are used by Trojans to infect the victim's system. With the help of these points, the Trojan attacks the target system and takes **complete control** over the system. They are as follows:

Instant Messenger Applications

The system can get infected via **instant messenger applications** such as ICQ or Yahoo Messenger. The user is at high risk while receiving files via the messenger, no matter from whom or from where. Since there is no file checking **utility bundled** with instant messengers, there is always a risk of infection by a Trojan. The user can never be 100% sure who is on the other side of the computer at any particular moment. It could be someone who hacked a messenger **ID** and **password** and wants to spread Trojans over the hacked friends 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 can be received over IRC and, in the DCC (Direct Client to Client), it will appear as **.TXT**. The execution of such files will cause infection. Most people do not notice that an **application (.exe)** file has a text icon. So before

such things are run, even if it is with a text icon; the extensions must be checked to ascertain that they are really .TXT files.

- Do not download any files that appear to be free porn or **Internet software**. Novice computer users are often targets of these false offers, and many people on IRC are unaware of security. Users get infected from porn-trade channels, as they are not thinking about the risks involved—just how to get **free porn** and **free programs**.

Physical Access

Restricting physical access is important for a computer's security.

- Example:
  - A user's friend wants to have **physical access** to his system. The user might sneak into his friend's computer room in his absence and install a Trojan by copying the Trojan software from his disk onto the hard drive.
  - **Autostart** is another way to infect a system while having physical access. When a CD is placed in the CD-ROM tray, it automatically starts with a setup interface. An example of the Autorun.inf file that is placed on such CDs:

[autorun]

open=setup.exe

icon=setup.exe

  - Trojan could be run easily by running a real setup program.
  - Since many people do not know about this CD function, their machine might get infected, and they would not understand what happened or how it was done.
  - The Autostart functionality should be turned off by doing the following:

Start → Settings → Control Panel → System → Device Manager → CDROM → Properties → Settings

Once there, a reference to Auto Insert Notification will be seen. (It checks approximately once per second whether a CD-ROM has been inserted, or changed, or not changed.) To avoid any problems with this function, it should be turned off.

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. Imagine an old version of Internet Explorer being used. A visit to a malicious site will automatically infect the machine without downloading or executing any program. The same scenario occurs while checking email with Outlook Express or some other software with well-known problems. Again, the user's system will be infected without even downloading an attachment. The latest version of the browser and email software should be used, because it reduces the risk of these variations.

- Check the following sites to understand how dangerous these bugs are, all due to the use of an old version of the software:
  - http://www.guninski.com/browsers.html
  - http://www.guninski.com/netscape.html

Fake Programs

- Attackers can easily lure a victim into downloading free programs that are suitable for their needs, and loaded with features such as an address book, access to check several POP3 accounts, and many other functions that make it even better than the currently used email client.
- The victim downloads the program and marks it as **TRUSTED**, so that the protection software fails to alert him or her of the new software being used. The email and POP3 account passwords are mailed directly to the attacker's mailbox without anyone noticing. Cached passwords and keystrokes can also be mailed. The aim is to gather ample information and send it to the attacker.
- In some cases, an attacker may have complete access to a system, but what the attacker does depends on his or her ideas about how to use the hidden program's functions. While sending email and using port 25 or 110 for POP3, these could be used for connections from the attacker's machine (not at home, of course, but from another hacked machine) to connect and use the hidden functions they implemented in the freeware program. The idea here is to offer a program that requires a connection with a server be established.
- Attackers thrive on creativity. Consider an example where a **fake audio galaxy**, which is a site for downloading MP3, is given. An attacker generates such a site by using **15-gb space** on his system to place a larger archive there for the MP3. In addition, some other systems are also configured in the same fashion. This is done to fool users into thinking that they are downloading from other people who are spread across the network. The software acts as a **backdoor** and will infect thousands of naïve users using ADSL connections.
- Some fake programs have **hidden codes**, but still maintain a professional look. These websites link to anti-Trojan software, thus fooling users into trusting them. Included in the setup is readme.txt. This can deceive almost any user, so proper attention needs to be given to any freeware before it is downloaded. This is important because this dangerous method is an easy way to infect a machine via Trojans hidden in the freeware.

Shrink-Wrapped Software

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

Via Attachments

When unaware web users receive an email saying they will get free porn or free Internet access if they run an attached .exe file, they might run it without completely understanding the risk to their machines.

- Example:
  - A user has a good friend who is carrying out some research and wants to know about a topic related to his friend's field of research. He sends an email to his friend asking about the topic and waits for a reply. The attacker targeting the user also knows his friend's email address. The attacker will simply code a program to fake the email From: field and make it appear to be the friend's email address, but it will include the **TROJANED** attachment. The user will check his email, and see that his friend has answered his query in an attachment, and download and run it without thinking that it might be a Trojan. The end result is an infection.
  - Trash email with the subject line, "Microsoft IE Update," without viewing it.
  - Some email clients, such as Outlook Express, have bugs that automatically execute the attached files.

Untrusted Sites and Freeware Software

- A site located at a free web space provider or one just offering programs for illegal activities can be considered suspicious.
- There are many underground sites such as **NeuroticKat Software**. It is highly risky to download any program or tool located on such a suspicious site that can serve as a
- conduit for a Trojan attack on a victim's computer. No matter what software you use, are you ready to take that risk?
- Many sites are available that have a professional look and contain huge archives. These sites are full of feedback forms and links to other popular sites. Users must take the time to scan such files before downloading them, so that it can be determined whether or not they are coming from a genuine site or a suspicious one.
- Software such as mIRC, ICQ, PGP, or any other popular software must be downloaded from its original (or official dedicated mirror) site, and not from any other websites that may have links to download supposedly the same software.
- Webmasters of well-known security portals, who have vast archives with various "hacking" programs, should be responsible for the files they provide and scan them often with anti-virus and anti-Trojan software to guarantee the site to be "free of Trojans and viruses." Suppose an attacker submits a program infected with a Trojan,

- e.g., a UDP flooder, to the webmaster for the archive; if the webmaster is not alert, the attacker may use the webmaster's irresponsibility to infect the site's files with a Trojan.
- Users who deal with any kind of software or **web application** should scan their systems on a daily basis. If they detect any new file, it should be examined. If any suspicion arises regarding the file, it must be forwarded to software detection labs for further analysis.
- It is easy to infect machines using freeware programs. "Free is not always the best" and hence these programs are hazardous for systems.

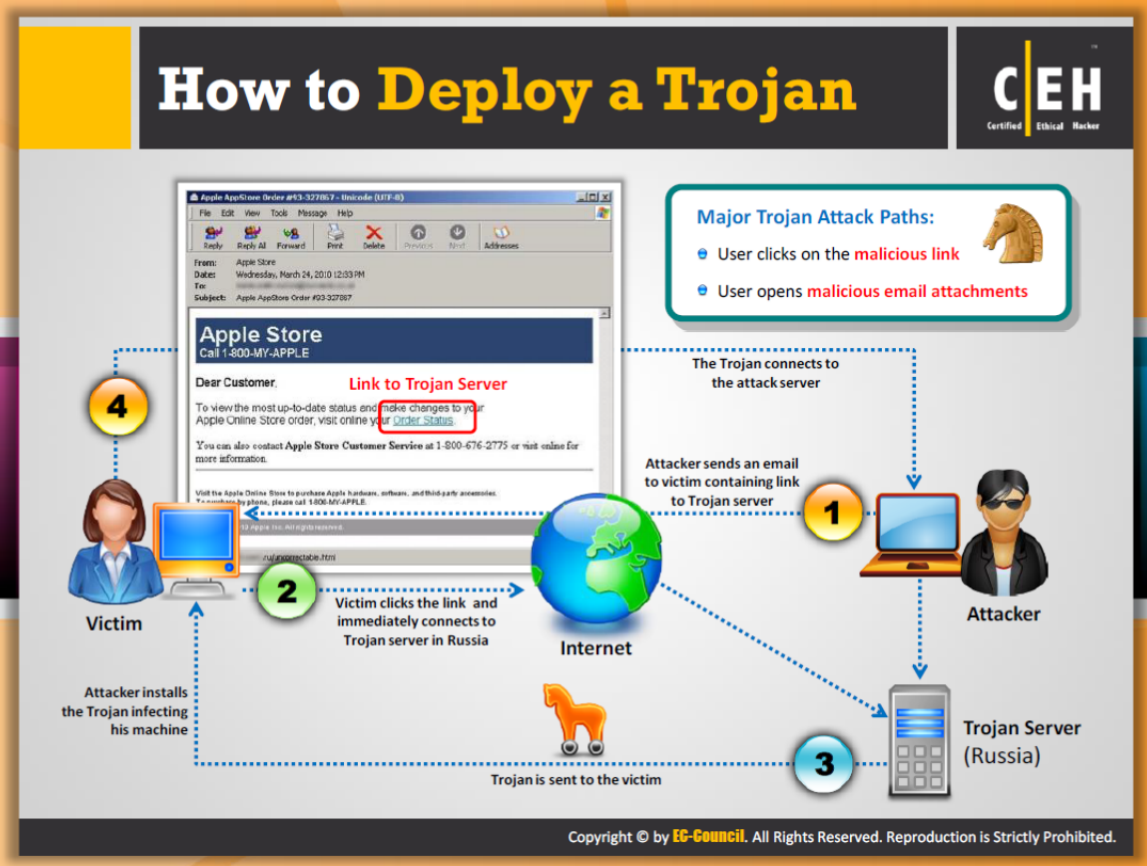
NetBIOS (File Sharing)

If port 139 on the system is open, i.e., file sharing is enabled, it can be used by others to access the system, install trojan.exe, and modify a system's file.

- The attacker 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 the WinME version, go to:
  - **Start → Settings → Control Panel → Network → File and Print Sharing**
  - Uncheck the boxes there. This will prevent NetBIOS abuse.

Downloading

Downloading files, games, and screensavers from Internet sites can be dangerous.



How to Deploy a Trojan

A Trojan is the means by which an attacker can gain access to the **victim's system**. In order to gain control over the victim's machine, an attacker creates a **Trojan server**, and then sends an email to a victim containing a link to the Trojan server. Once the victim clicks on the link sent by the attacker, it connects him or her directly to the Trojan server. The Trojan server sends a **Trojan** to the victim system. The attacker installs the Trojan, infecting the victim's machine. As a result, victim is **connected** to the attack server unknowingly. Once the victim connects to an attacker server, the attacker takes complete control over the victim's system and performs any action the **attacker chooses**. If the victim carries out any online transaction or purchase, then the attacker can easily steal sensitive information such as credit card details, account information, etc. In addition, attackers can also use the victim's machine as the source for launching attacks on other systems.

Computers typically get infected by users clicking on a malicious link or opening an email attachment that installs a Trojan on their computers that serves as a back door to criminals who can then command the computer to send spam email.

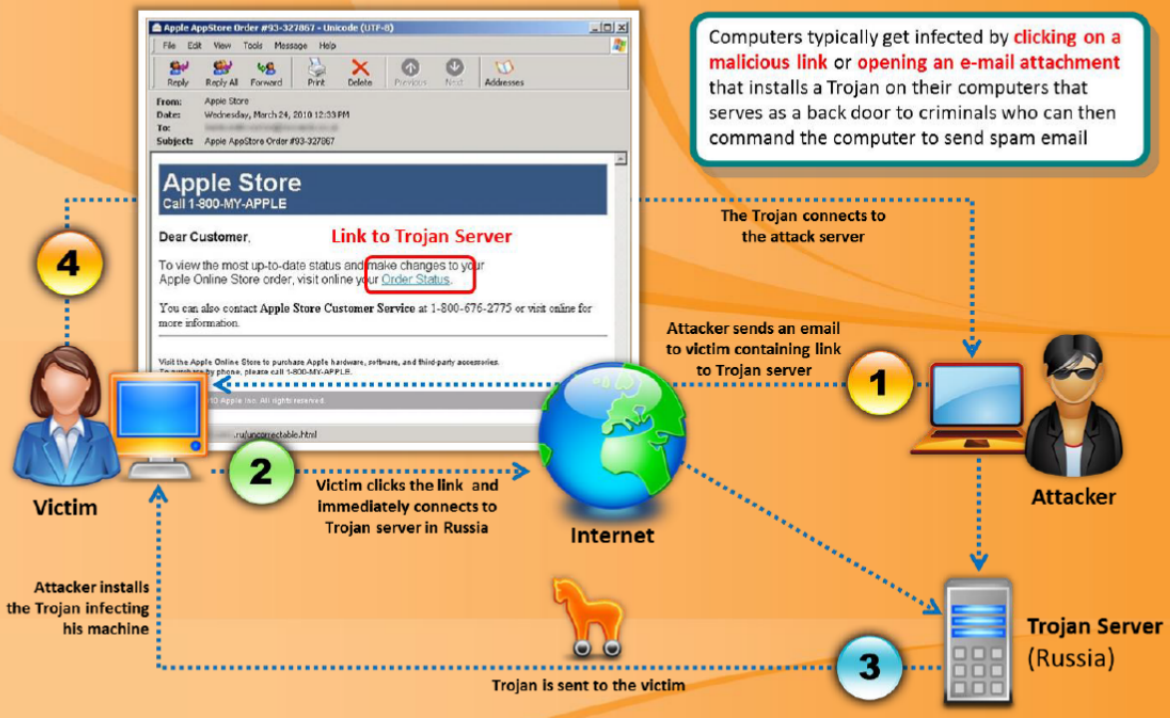
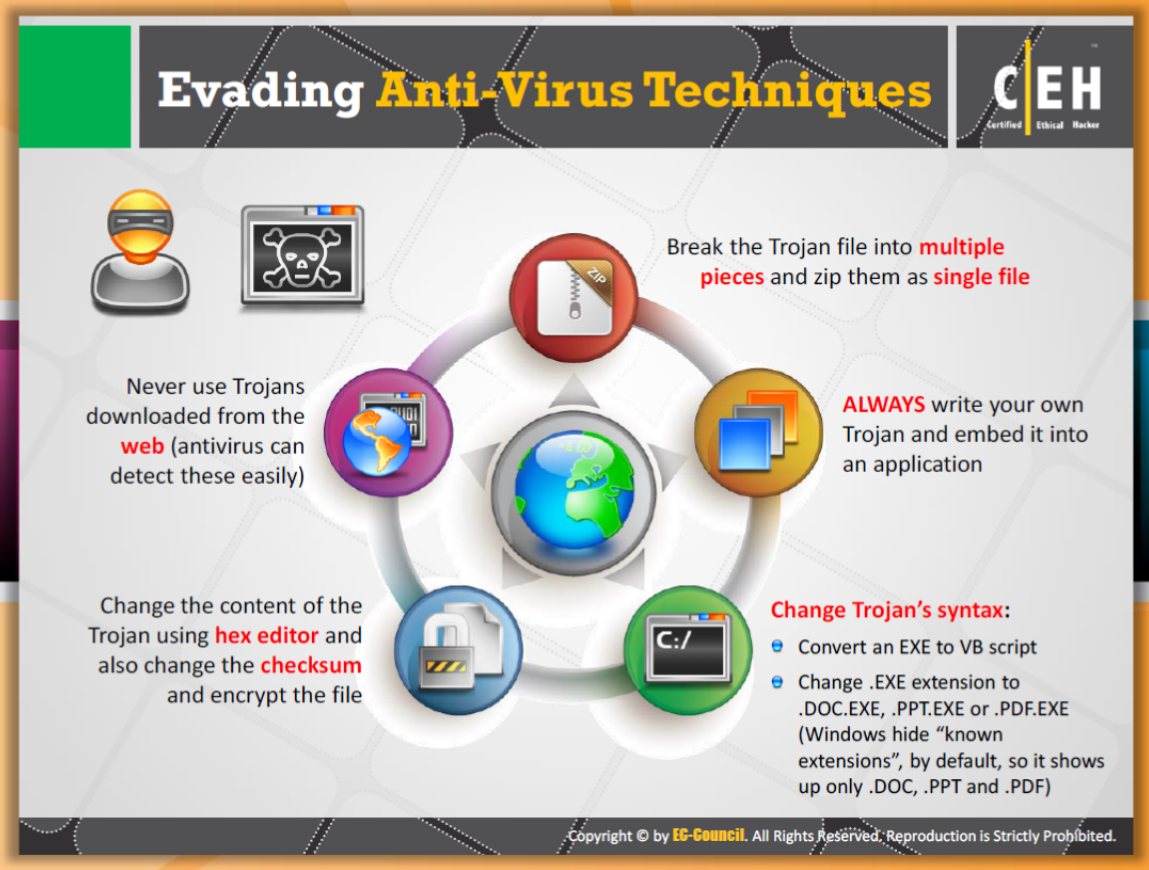


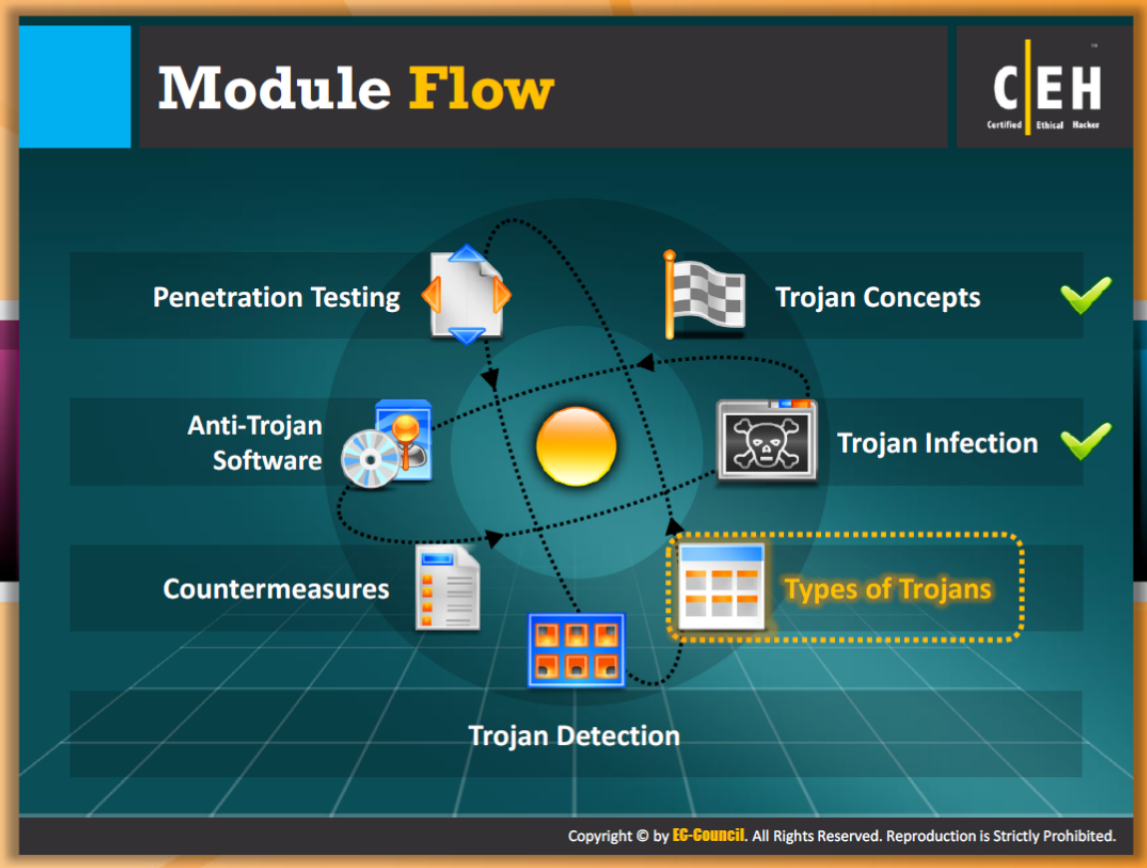
FIGURE 6.9: Diagrammatical representation of deploying a Trojan in victims system



Evading Antivirus Techniques

The following are the **various techniques** used by Trojans, viruses, and worms to evade most of antivirus software:

1. Never use Trojans downloaded from the web (antivirus detects these easily).
2. Write your own Trojan and embed it into an application.
3. Change the Trojan's syntax:
   - Convert an EXE to VB script
   - Convert an EXE to a DOC file
   - Convert an EXE to a PPT file
4. Change the checksum.
5. Change the content of the Trojan using a hex editor.
6. Break the Trojan file into multiple pieces.

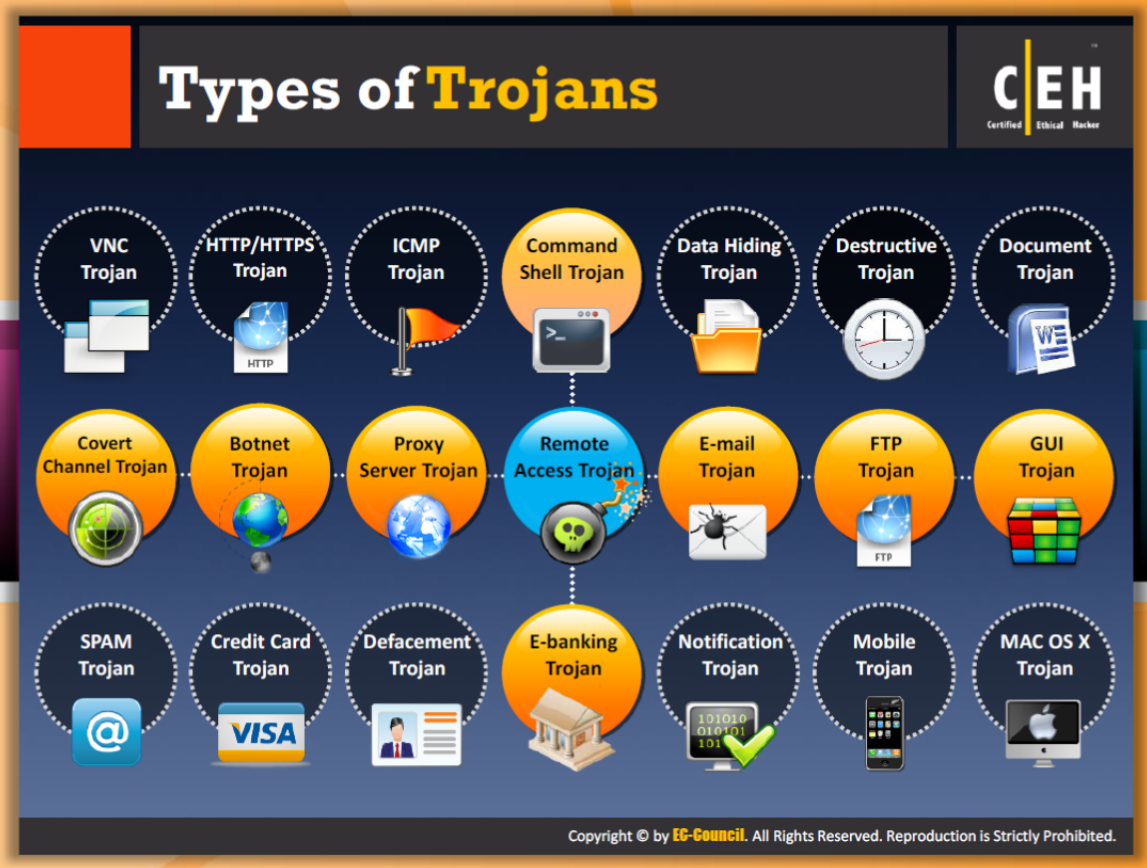


Module Flow

So far, we have discussed various concepts of Trojans and the way they infect the system. Now we will discuss various types of Trojans that are used by attackers for gaining sensitive information through various means.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

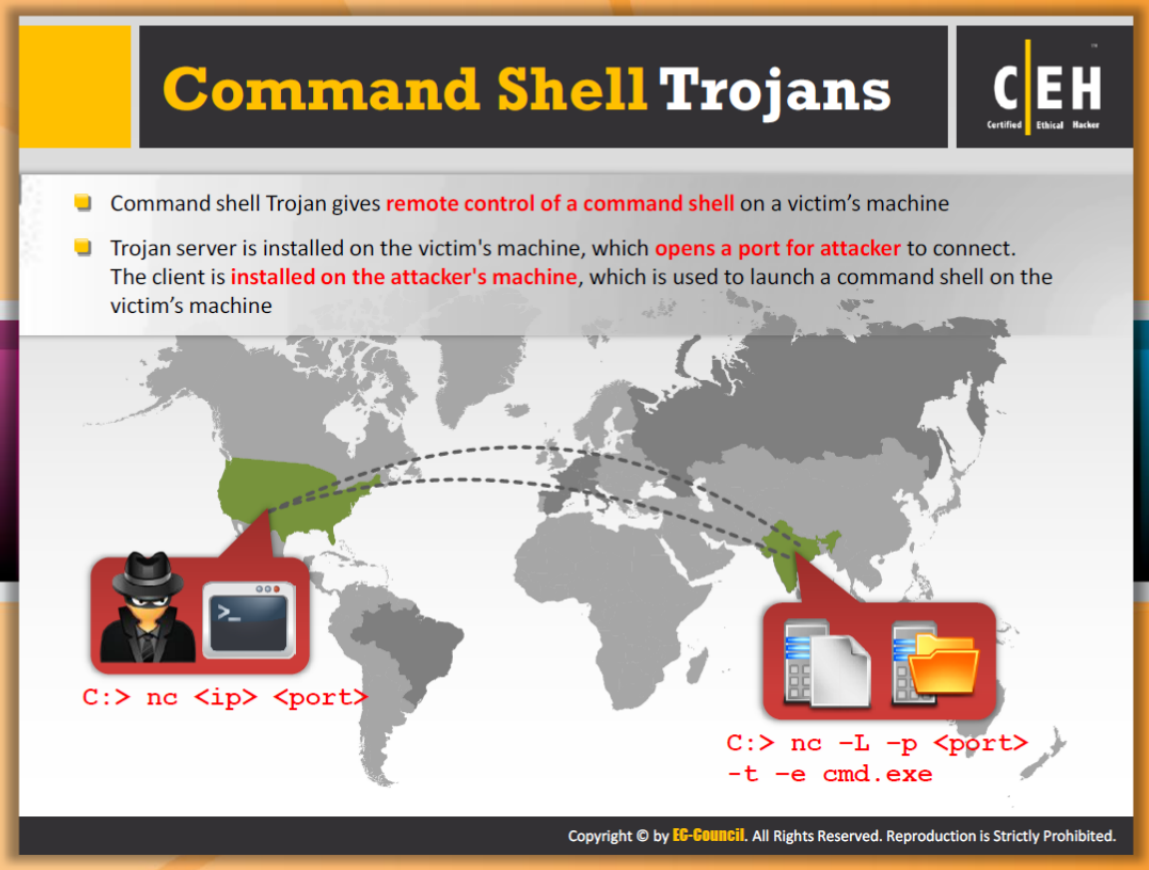
This section covers various types of Trojans such as command-shell Trojans, document Trojans, email Trojans, botnet Trojans, proxy server Trojans, and so on.



Types of Trojans

Various types of Trojans that are intended for various purposes are available. The following is a list of types of Trojans:

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- GUI Trojan
- FTP Trojan
- E-mail Trojan
- Remote Access Trojan
- Proxy Server Trojan
- Botnet Trojan
- Covert Channel Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan



Command Shell Trojans

The command shell Trojan gives remote control of a **command shell** on a victim's machine. The Trojan server is installed on the victim's machine, which opens a port for the attacker to connect. The client is installed on the **attacker's machine**, which is used to launch a command shell on the victim's machine.

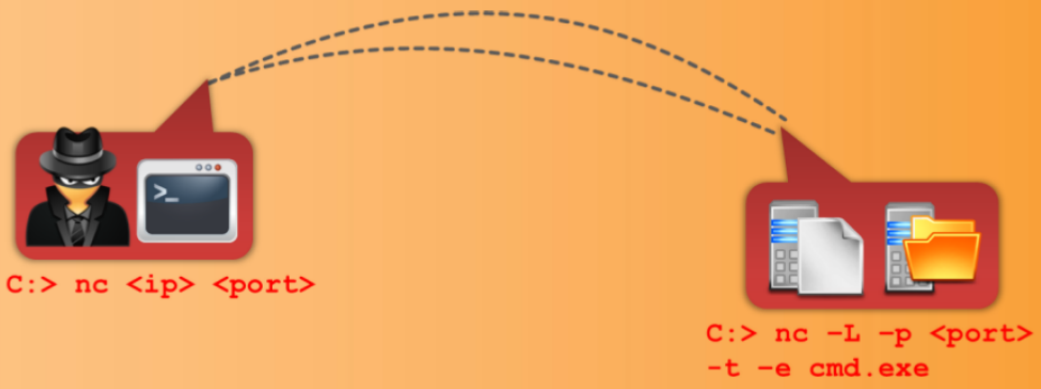


FIGURE 6.10: Attacker launching command shell Trojan in victim's machine

Command Shell Trojan: Netcat

Using Netcat, an attacker can set up a **port or a backdoor** that will allow him or her to telnet into a DOS shell. With a simple command such as **C:\>nc -L -p 5000 -t -e cmd.exe**, the attacker can **bind port 5000**. With Netcat, the user can create outbound or inbound connections, TCP or UDP, to or from any port. It provides for full DNS forward/reverse checking, with appropriate warnings. Additionally, it provides the ability to use any local source port, any locally configured network source address, and it comes with built-in port-scanning capabilities. It has a **built-in loose source-routing capability** and can read command-line arguments from standard input. Another feature is the ability to let another program respond to inbound connections (another program service established connections).

In the simplest usage, "nc host port" creates a TCP connection to the given port on the given target host. The standard input is then sent to the host, and anything that comes back across the connection is sent to the standard output. This continues indefinitely, until the network side of the connection shuts down. This behavior is different from most other applications, which shut everything down and exit after an end-of-file on the standard input. Netcat can also function as a server by listening for inbound connections on arbitrary ports, and then doing the same reading and writing. With minor limitations, Netcat does not really care if it runs in client or server mode; it still moves data back and forth until there is none left. In either mode, shutdown can be forced after a configurable time of inactivity on the network side.

Features:

- Outbound or inbound connections, TCP or UDP, to or from any port
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally configured network source address
- Built-in port-scanning capabilities, with randomizer
- Built-in loose source-routing capability
- Can read command-line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service establish connections
- Optional telnet-options responder using the command nc -l -p 23 -t -e cmd.exe
- Where 23 is the port for telnet, -l option is to listen, -e option is to execute, -t option tells Netcat to handle any telnet negotiation the client might expect

Netcat is a utility used for **reading and writing the networks** that support TCP and UDP protocols. It is a Trojan that is used to open either the TCP or UDP port on a target system and hackers with the help of Telnet gain the access over the system.

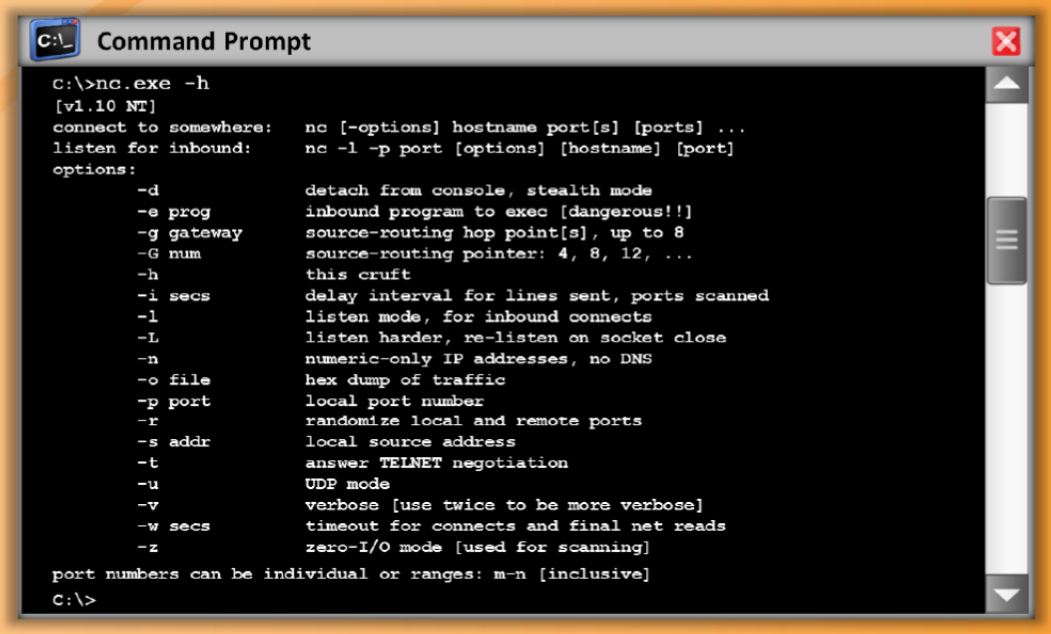
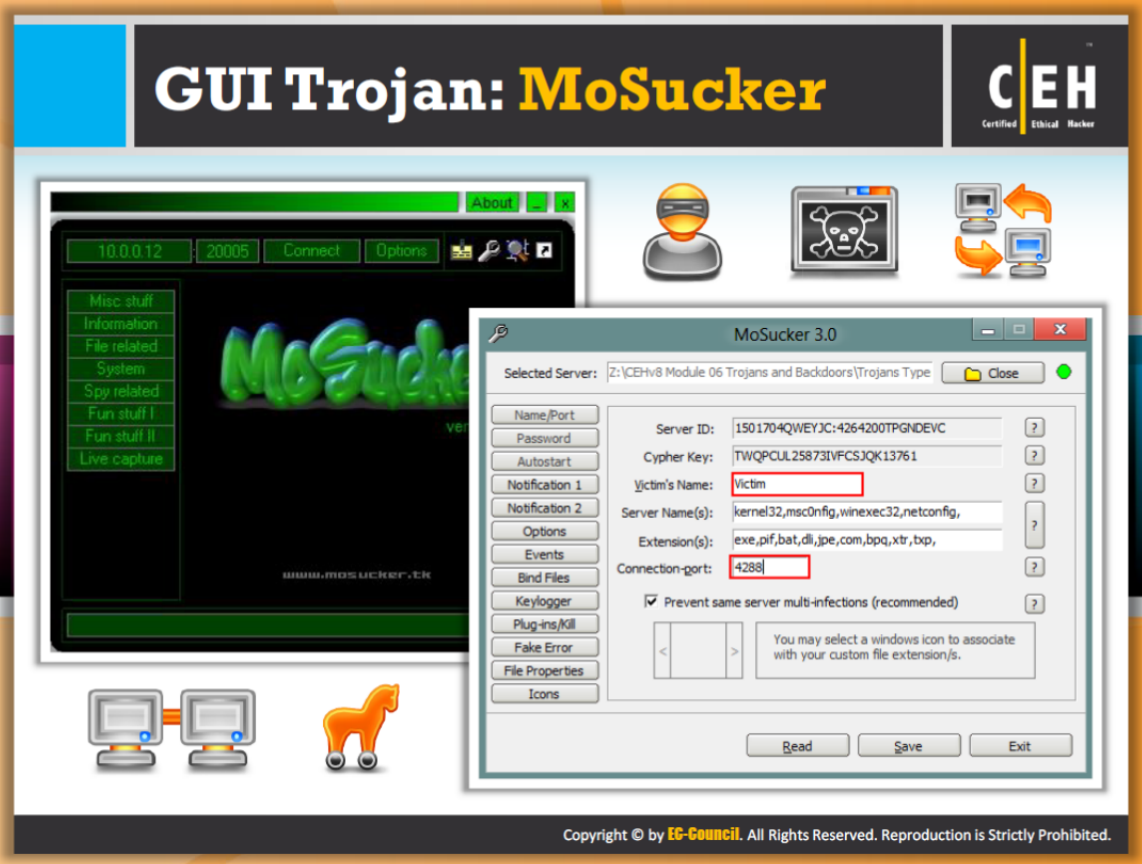


FIGURE 6.11: Netcat screenshot



GUI Trojan: MoSucker

Source: http://www.dark-e.com

MoSucker is a **Visual Basic Trojan**. MoSucker's edit **server program** lets the infection routine be changed and **notification information** set. MoSucker can auto load with the system.ini and/or the registry. Unlike any other Trojan, MoSucker can be set to randomly choose which method to auto load. It can notify cell **phones via SMS** in Germany only. MuSucker's edit server can gain X number of kilobytes (X is either a static number or it is random each time). The standard error message for MoSucker is "**Zip file is damaged**, truncated, or has been changed since it was created. If you downloaded this file, try downloading again." Here is a list of file names MoSucker suggests to name the server: MSNETCFG.exe, unin0686.exe, Calc.exe, HTTP.exe, MSWINUPD.exe, Ars.exe, NETUPDATE.exe, and Register.exe.

Server Features:

- Chat with victim
- Clipboard manager
- Close/remove server
- Control mouse
- Crash System File Manager

- Get passwords entered by user, system info
- Hide/Show start button, system tray, taskbar
- Keylogger
- Minimize all windows
- Open/close CD-ROM drive
- Ping server
- Pop-up startmenu
- Process manger
- Shutdown/Reboot/Standby/Logoff/Dos mode server
- System keys on/off
- Window manager

FIGURE 6.12: MoSucker screenshot

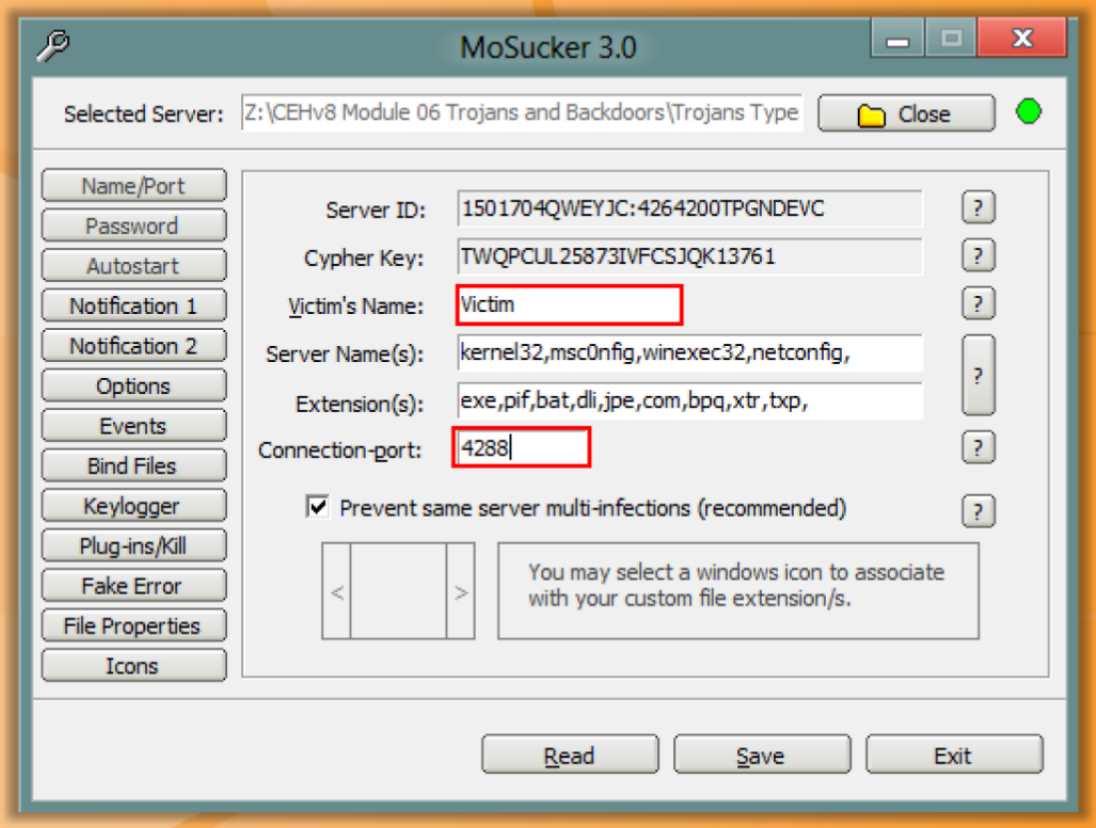
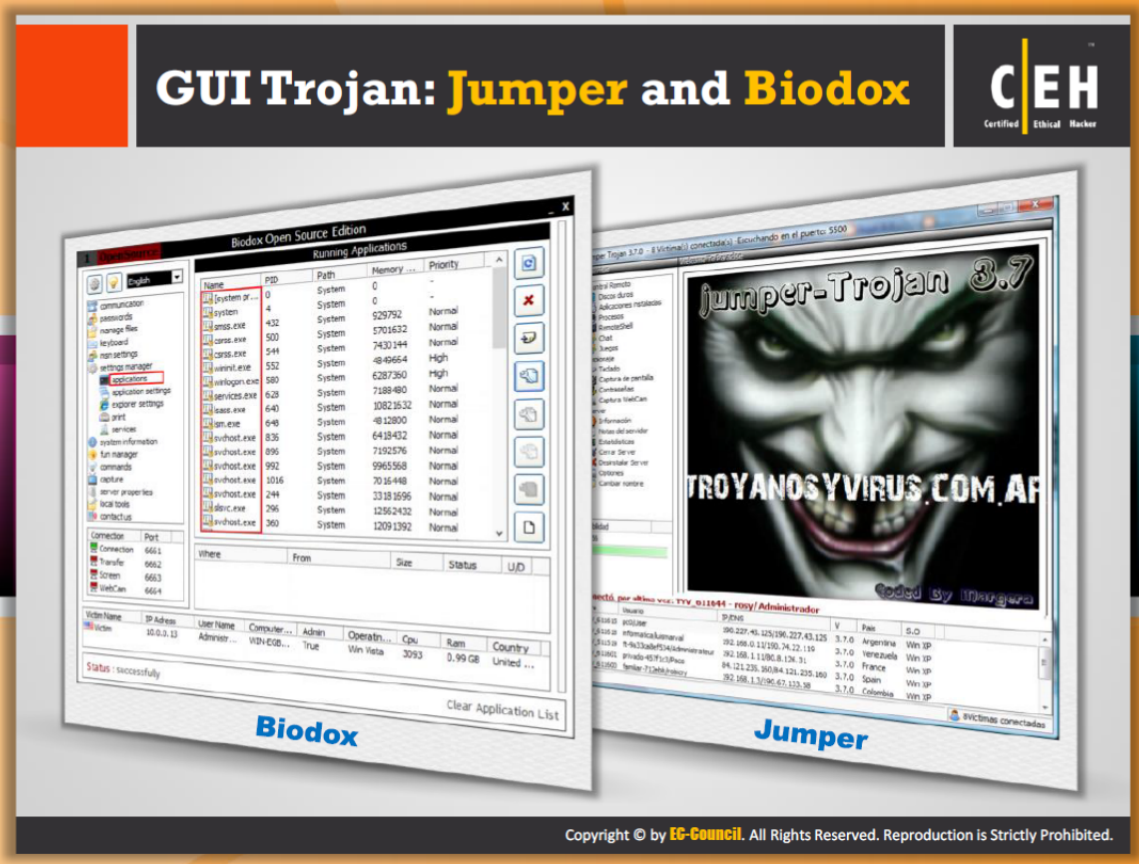


FIGURE 6.13: MoSucker showing victim's name and connection port



GUI Trojan: Jumper and Biodox

Jumper is a **malicious malware** program that performs many functions to download malicious malware from the Internet. Attackers use this **jumper Trojan** to get sensitive data like **financial information** from the user's system. It also downloads additional downloads for the attacker to be able to access the system remotely.

Generally, the **BIODOX OE Edition.exe** file should be in the **C:\Windows\System32 folder**; if it has been found elsewhere, then it is a Trojan. Once the computer gets infected by the Biodox, the system performance decreases. The screensaver gets changed automatically. Continuous annoying advertisement pop-ups appearing on the computer can be treated as one of the symptoms of this Trojan.

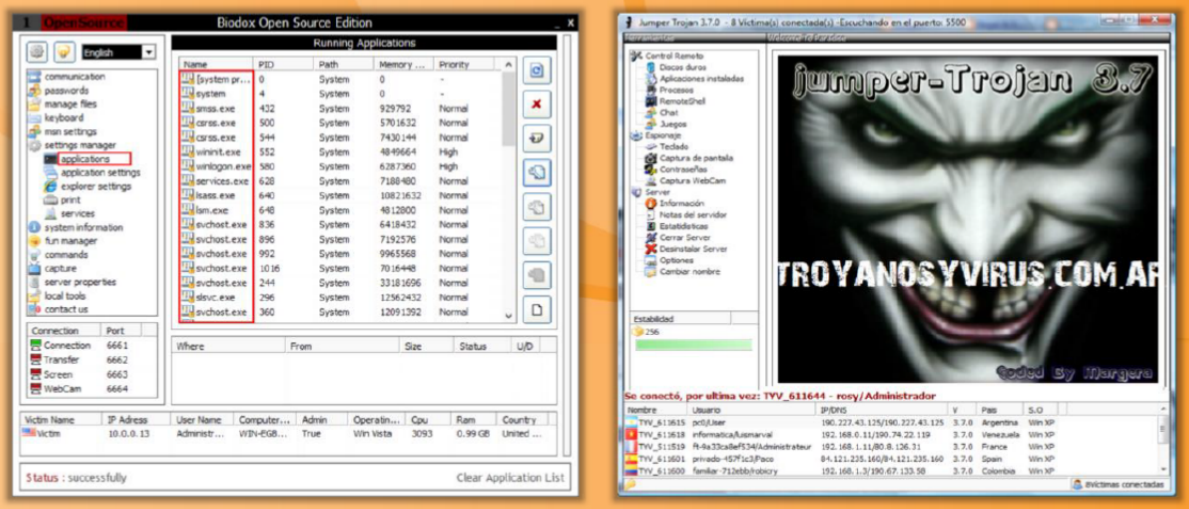
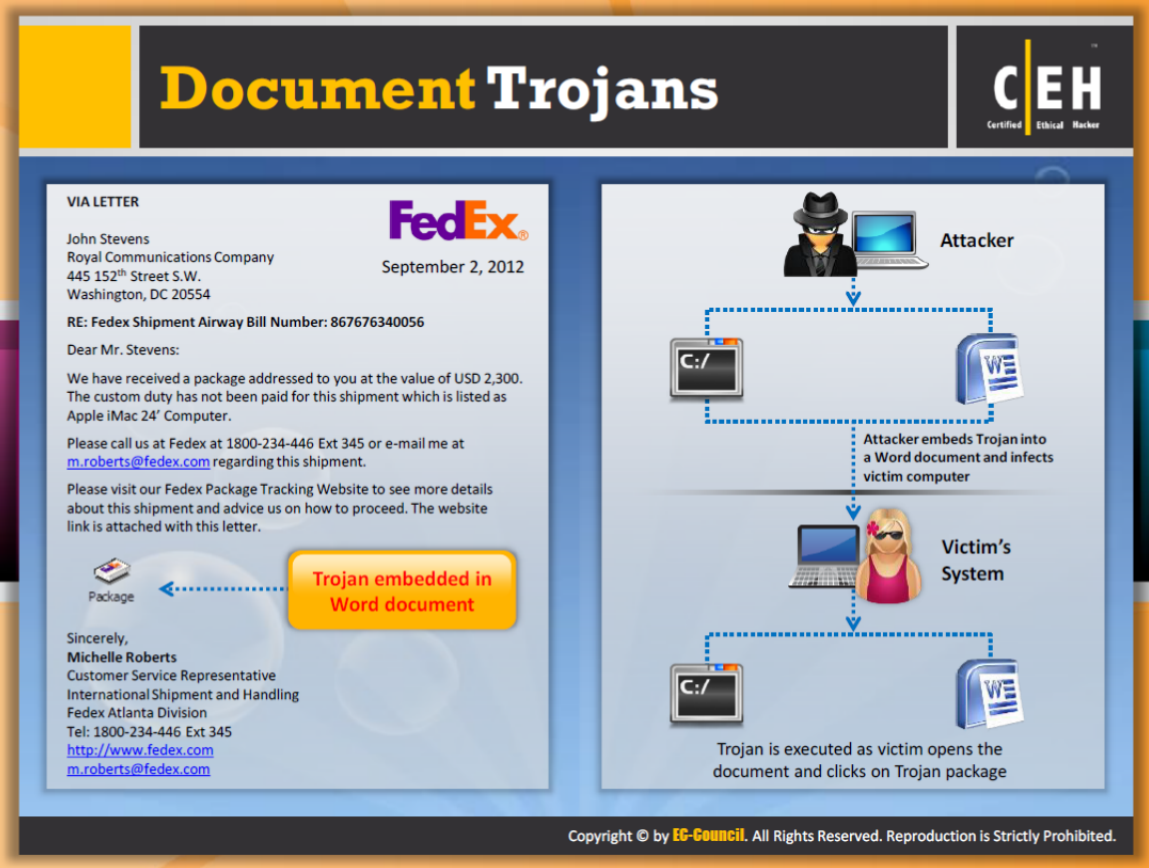


FIGURE 6.13: Screenshots showing Biodox and Jumper



Document Trojans

Most users usually have the tendency to update their operating system but not the application they use regularly. Attackers take this opportunity to install document Trojans. Attackers usually **embed a Trojan** into a document and transfer it in the form of an attachment in emails, office documents, web pages, or media files such as flash and PDFs. When a user opens the document with the embedded Trojan assuming it is a legitimate one, the Trojan is installed on the victim's machine. This exploits the application used to open the document. Attackers can then access sensitive data and perform malicious actions.

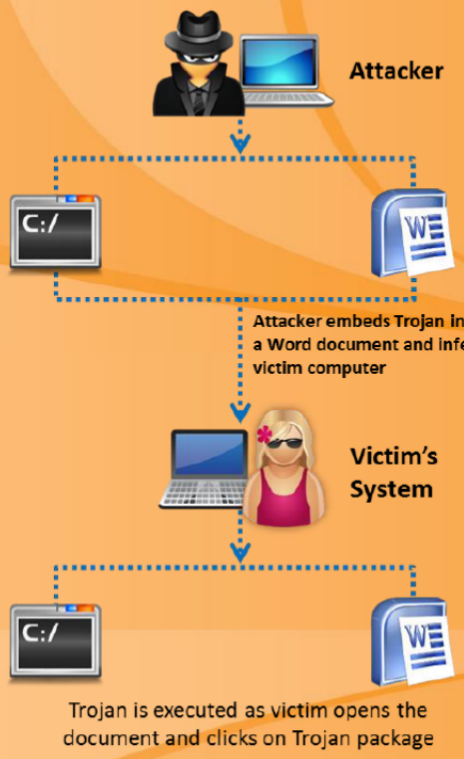


FIGURE 6.13: Attacker infecting victim's machine using Document Trojan

An example of a Trojan embedded in a Word document is as follows:

VIA LETTER

John Stevens
Royal Communications Company
445 152th Street S.W.
Washington, DC 20554

September 2, 2012

RE: Fedex Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24' Computer.

Please call us at Fedex at 1800-234-446 Ext 345 or e-mail me at m.roberts@fedex.com regarding this shipment.

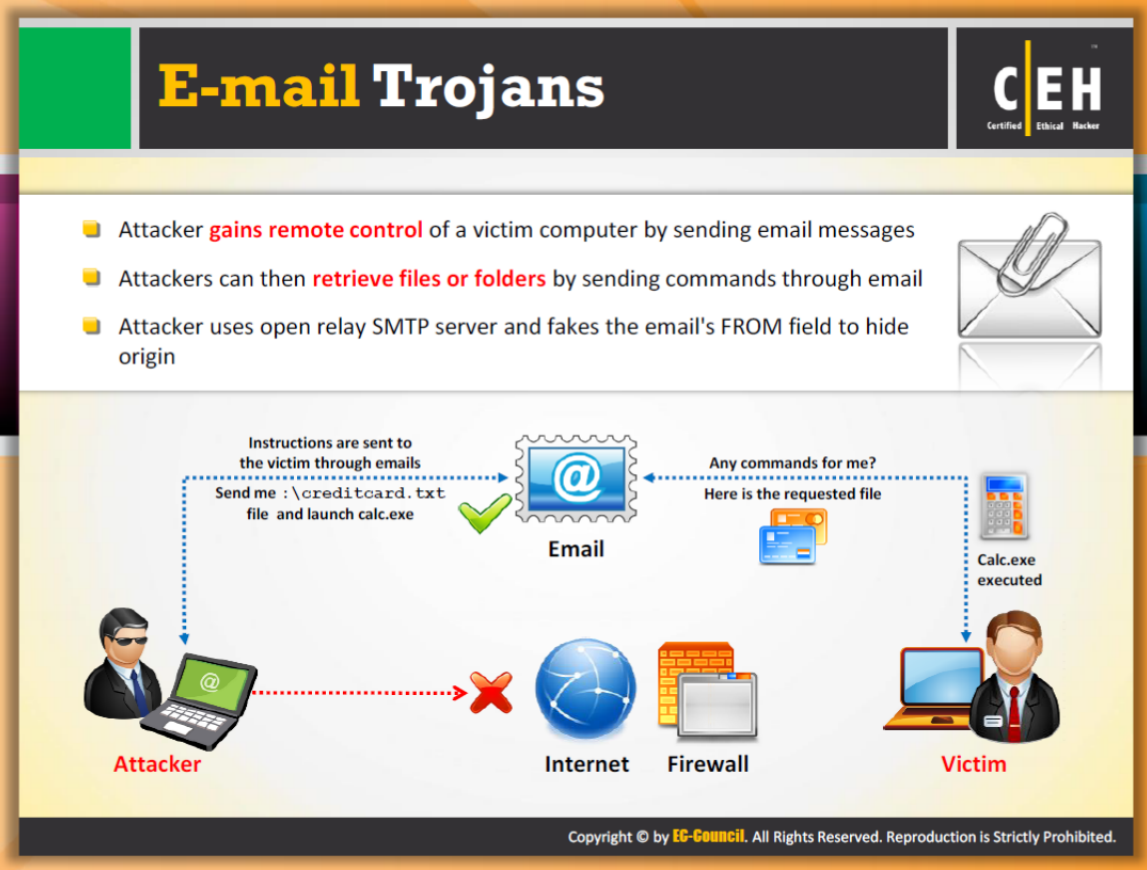
Please visit our Fedex Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.

Package

Trojan embedded in Word document

Sincerely,
Michelle Roberts
Customer Service Representative
International Shipment and Handling
Fedex Atlanta Division
Tel: 1800-234-446 Ext 345
http://www.fedex.com
m.roberts@fedex.com

FIGURE 6.14: An example of Trojan embedded in a Word document



Email Trojans

Email Trojans spread through **bulk emails**. Trojan viruses are sent through attachments. The moment the user opens the email, the **virus enters the system** and spreads and causes a lot of damage to the data in the system. It is always recommended that users not open emails from unknown users. Sometimes email Trojans may even generate automatic mail and send it to all the contacts present in the **victim's address book**. Thus, it is spread through the contact list of the infected victim.

Attackers send instructions to the victim through email. When the victim opens the email, the instructions will be **executed automatically**. Thus, attackers can retrieve files or folders by sending commands through email.

The following figure explains how an attack can be performed using email Trojans.

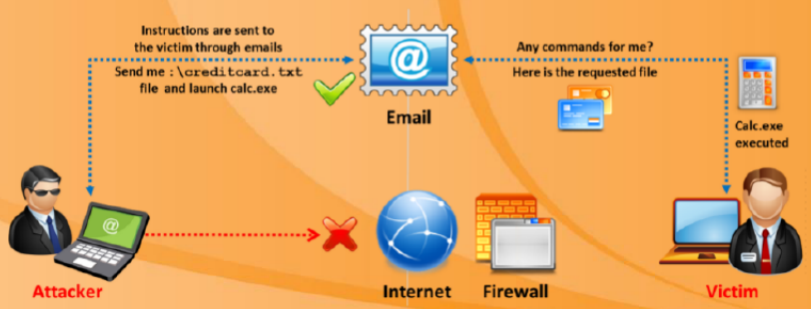
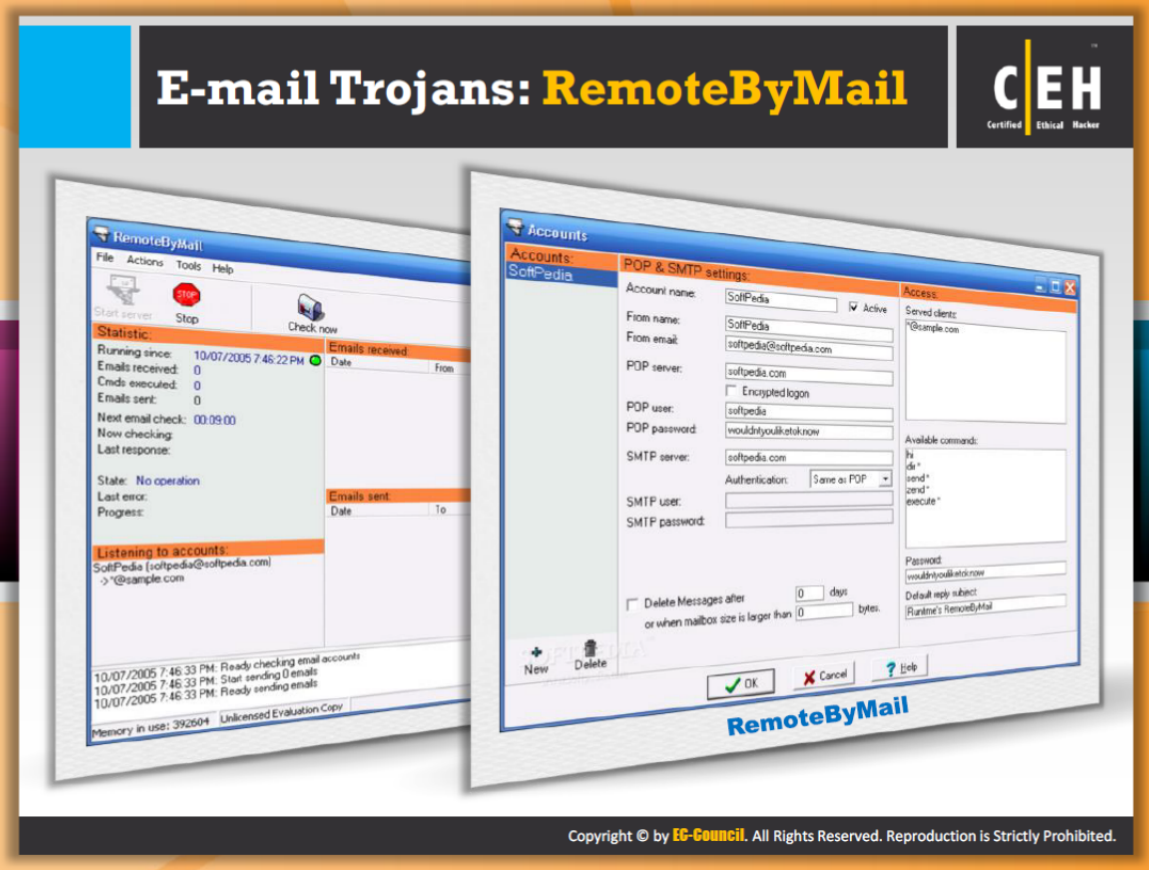


FIGURE 6.15: Illustrating the attack process using email Trojans



Email Trojans: RemoteByMail

RemoteByMail is used to **control** and **access** a computer, irrespective of its location, simply by sending email. With simple commands sent by email to a computer at work or at home, it can perform the following tasks:

- Retrieves list of files and folders easily
- Zips files automatically that are to be transferred
- Helps to execute programs, batch files, or opens files

This is an easier way to access files or to execute programs on a computer remotely. The main screen displays information that the program has received and processed:

- **Start Server**: Click the Start Server icon for RemoteByMail to begin the process and receive email
- **Stop**: Click the Stop icon to stop the application at any time
- **Check now**: Checks for next scheduled email
- **Statistics**: Displays program information
- **Listening to Accounts**: Displays accounts and associated email addresses

- **Emails received**: Displays email list containing commands the program has received
- **Command queue**: Displays commands the program has received but not yet processed
- **Outgoing emails**: Checks for processing email
- **Emails send**: Displays list of email sent by RemoteByMail

RemoteByMail accepts and executes the following commands:

- **HI**: Used to send email with the content "Hi" to your email address
- **SEND**: Sends files located on the host computer to your email address
- **ZEND**: Zips and then sends files or folders located on the host computer to your email address. To open a Zip attachment after you receive, enter the password you chose when you created the account
- **EXECUTE**: Executes programs or batch files on the host's computer
- **DIR**: Sends the directory of a drive or folder to your email address

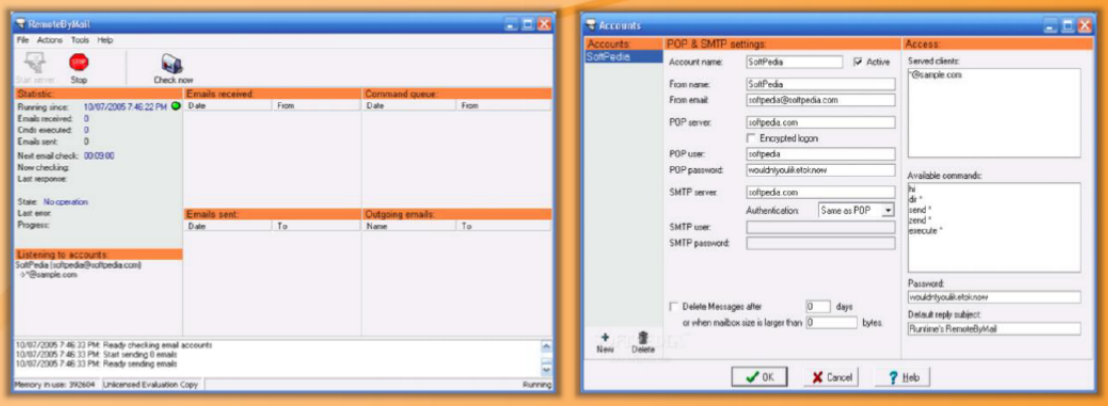
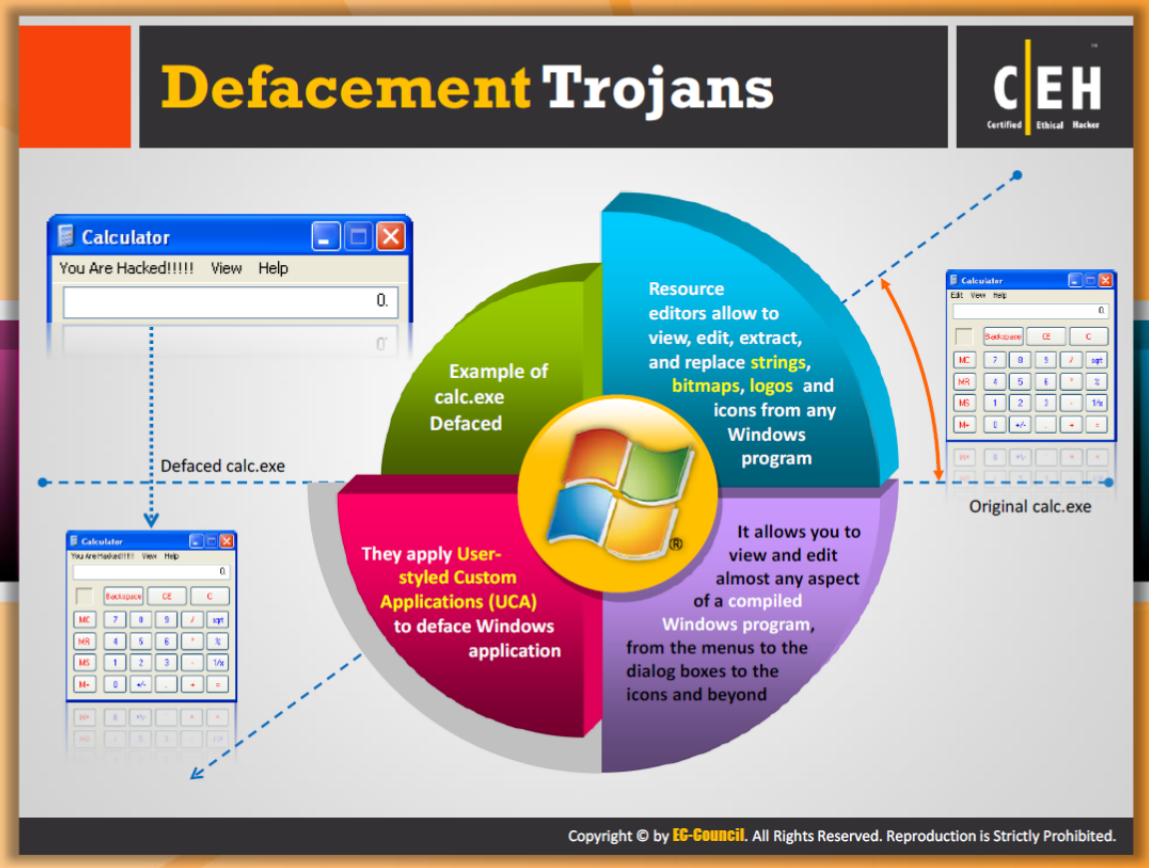


FIGURE 6.16: RemoteByMail screenshots



Defacement Trojans

Defacement Trojans, once spread over the system, can destroy or change the entire content present in the **database**. This defacement Trojan is more dangerous when attackers target websites; they physically change the entire **HTML format**, resulting in the changes of content of the website, and even more loss occurs when this defacement targets e-business activities. It allows you to view and edit almost any aspect of a compiled **Windows program**, from the menus to the dialog boxes to the icons and beyond. Resource editors allow you to view, edit, extract, and replace strings, bitmaps, logos, and icons from any Windows program. They apply **target-styled Custom Applications (UCAs)** to deface Windows applications. Example of calc.exe defaced:

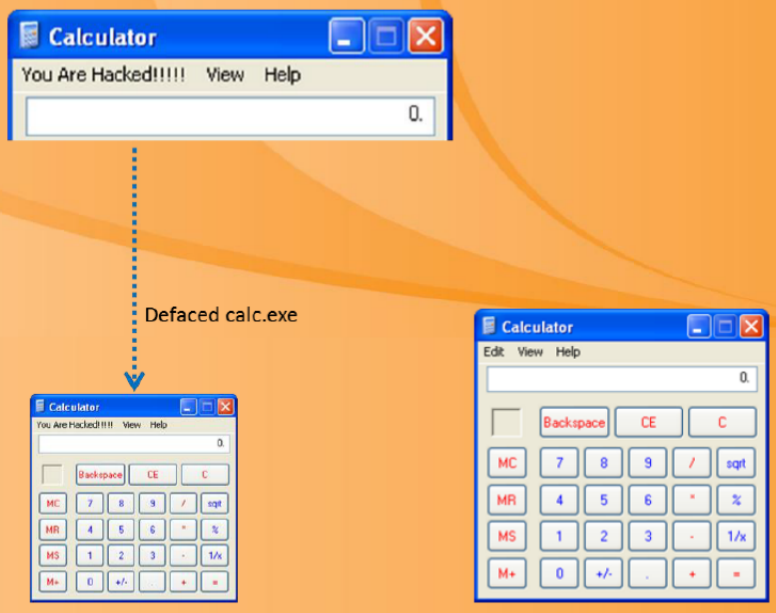
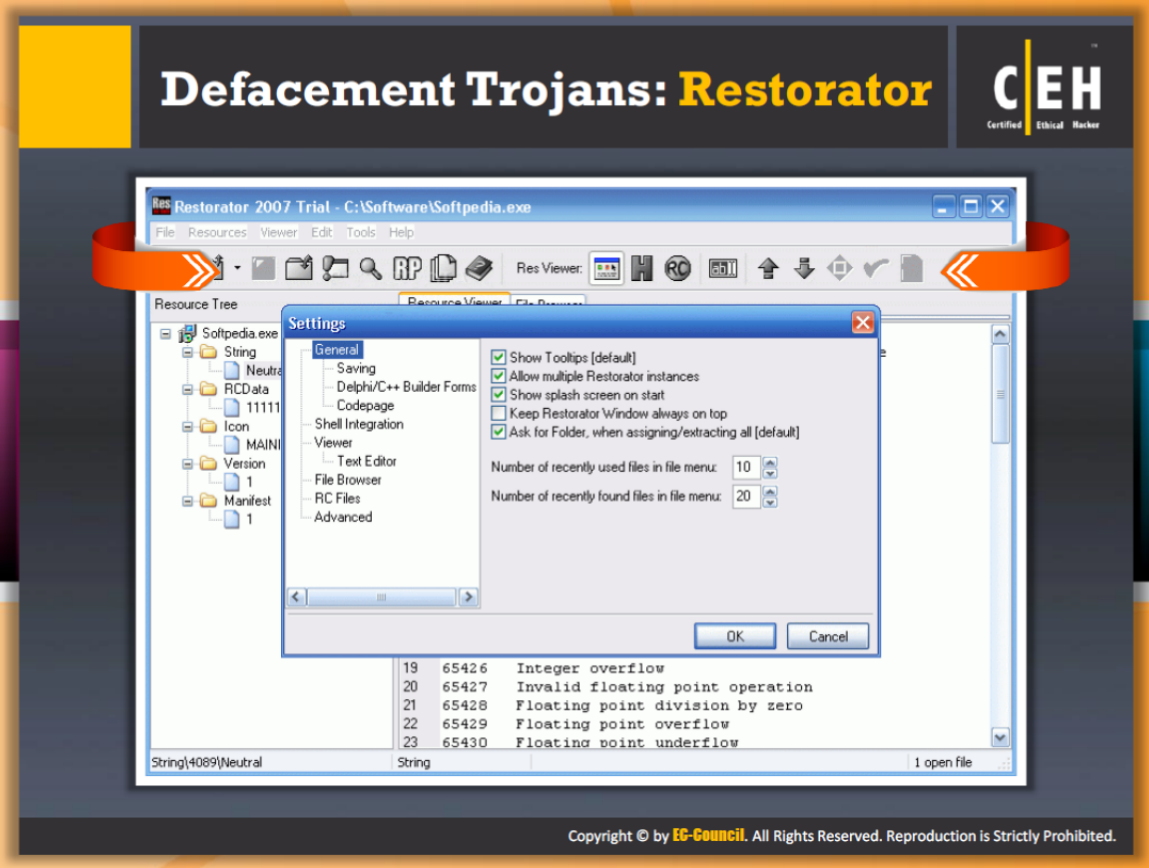


FIGURE 6.16: An example of calc.exe defaced



Defacement Trojans: Restorator

Source: http://www.bome.com

Restorator is a versatile skin editor for any **Win32 programs**. The tool can modify the target interface of any Windows 32-bit program and thus create target-styled Custom Applications (UCAs). You can view, extract, add, remove, and change images, icons, text, dialogs, sounds, videos, version, dialogs, and menus in almost all programs.

Technically speaking, it allows you to edit the resources in many file types, for example .ocx (Active X), .scr (Screen Saver), and others. The attacker can distribute modifications in a small, self-executing file. It is a standalone program that redoes the modifications made to a program. Its Grab function allows you to retrieve resources from files on a target's disk.

Restorator is the **Bome flagship** product that allows you to do resource (resources are application-dependent data that the respective programmer includes in the program) editing. It is a utility for editing Windows resources in applications and their components, e.g., files with .exe, .dll, .res, .rc, and .dcr extensions. You can use this for translation/localization, customization, design improvement, and development. This resource editor comes with an intuitive target-interface. You can replace logos and can control resource files in the software development process. It can intrude into the target's system and its working programs.

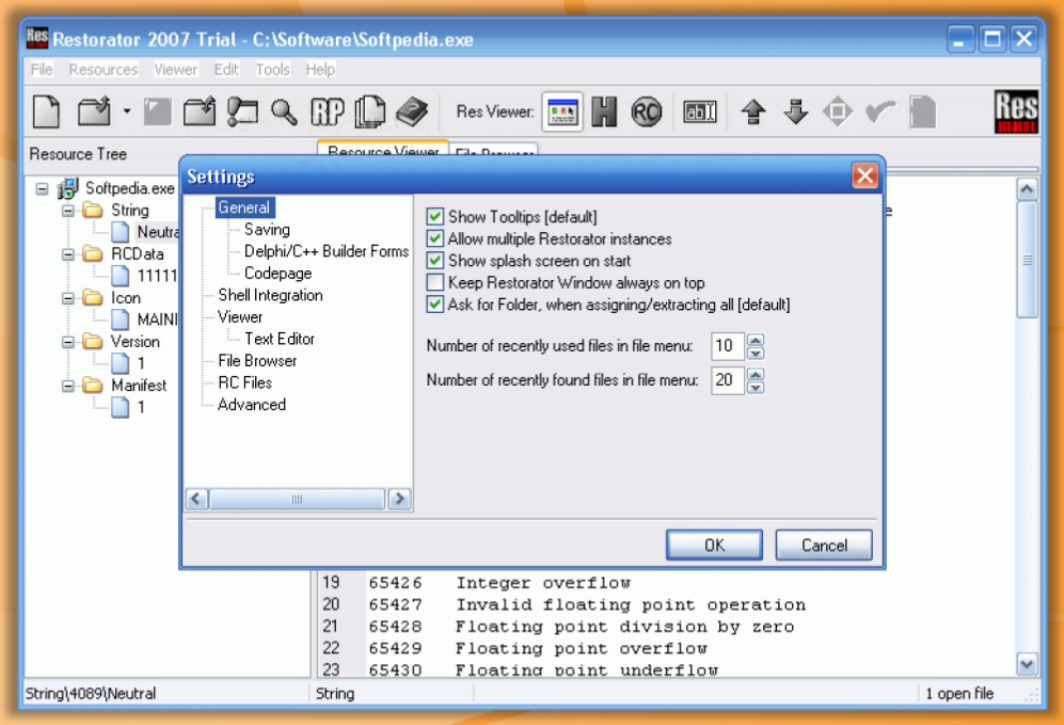
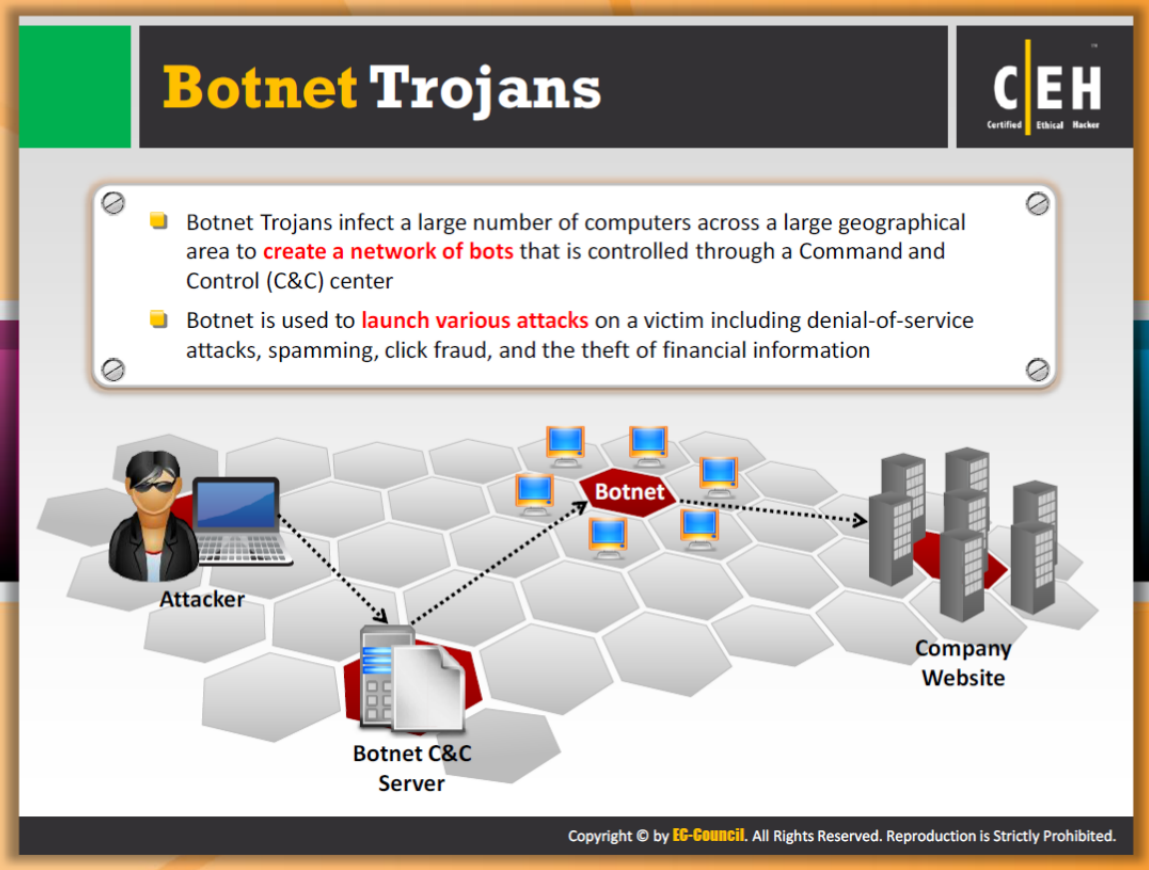


FIGURE 6.17: Restorator Screenshot



Botnet Trojans

A botnet is a collection of **software robots** (worms, Trojan horses, and backdoors) that run automatically. It refers to a collection of compromised machines running programs under a common command and control infrastructure. A botnet's originator (attacker) can control the group remotely. These are computers (a group of **zombie computers**) infected by worms or Trojans and taken over **surreptitiously** by attackers and brought into networks to send spam, more viruses, or launch denial of service attacks. This is a computer that has been infected and taken over by an attacker by using a **virus/Trojan/malware**.

Botnet owners usually target educational, government, military, and other networks. With the help of botnets, attacks like denial of service, creation or misuse of SMTP mails, click fraud, theft of application serial numbers, login IDs, credit card numbers, etc. are performed.

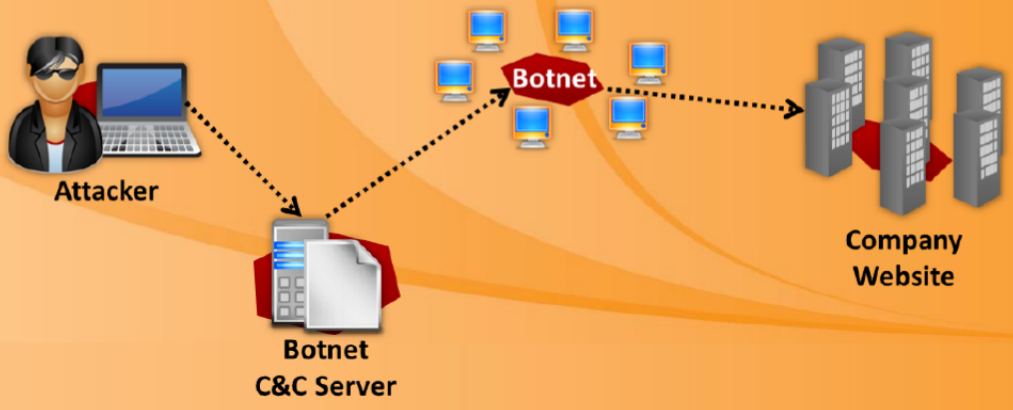


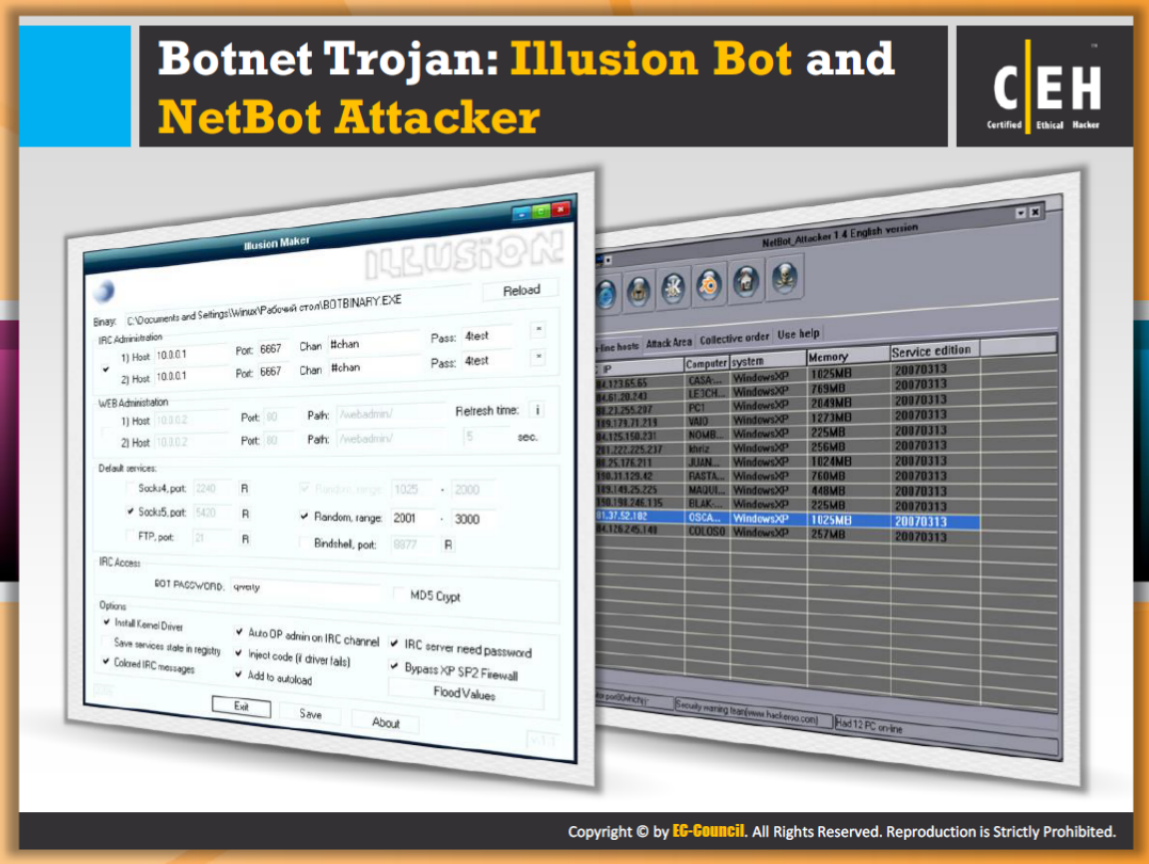
FIGURE 6.18: Illustrating the process of infecting company's website using Botnet Trojans

It has two main components:

- Botnet
- Botmaster

They target both businesses as well as individual systems to steal valuable information. There are four botnet topologies.

- Hierarchal
- Multi Server
- Star
- Random (Mesh)



Botnet Trojan: Illusion Bot and NetBot Attacker

Illusion Bot is a clear GUI tool for configuration. When this bot starts, it checks the OS version and if it detects **Win98**, it calls the **Register Service Process API** to hide the process from the Task Manager. The bot then proceeds to install the rootkit component. If the installation fails, the bot tries to inject its code inside the explorer.exe process.

Illusion Bot is a GUI tool.

Features:

- C&C can be managed over IRC and HTTP
- Proxy functionality (Socks4, Socks5)
- FTP service
- MD5 support for passwords
- Rootkit
- Code injection
- Colored IRC messages
- XP SP2 Firewall bypass
- DDOS capabilities

NetBot Attacker provides a simple **Windows UI** for controlling a botnet, reporting and managing the network, and commanding attacks. It installs in to the system in a very simple way such as **RAR file** with **two pieces**: an INI file (see the following, partially edited and obscured) and a simple EXE. The original NetBot Attacker is a backdoor; this tool retains that capability and lets you update the bot and be a part of the rest of the botnet.

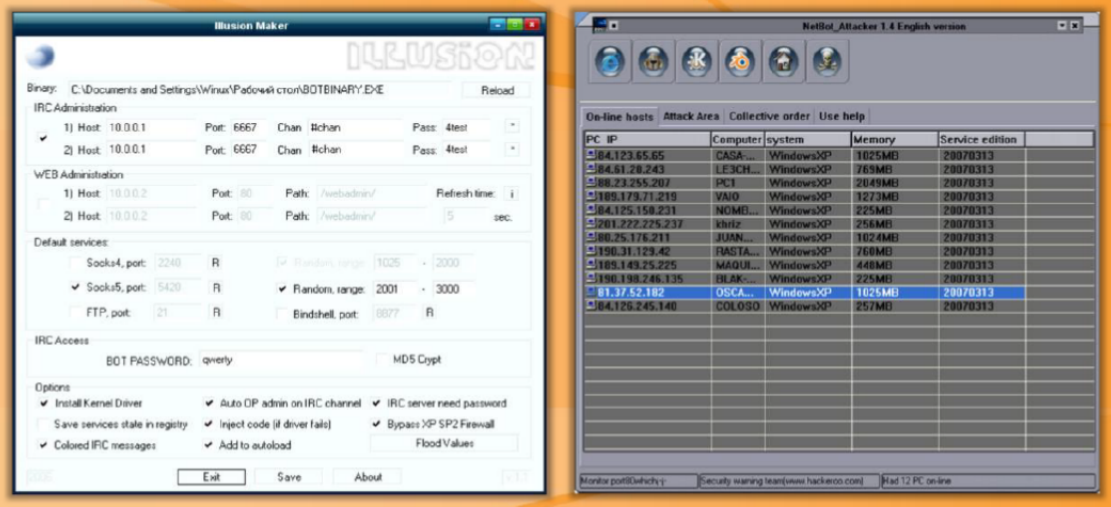
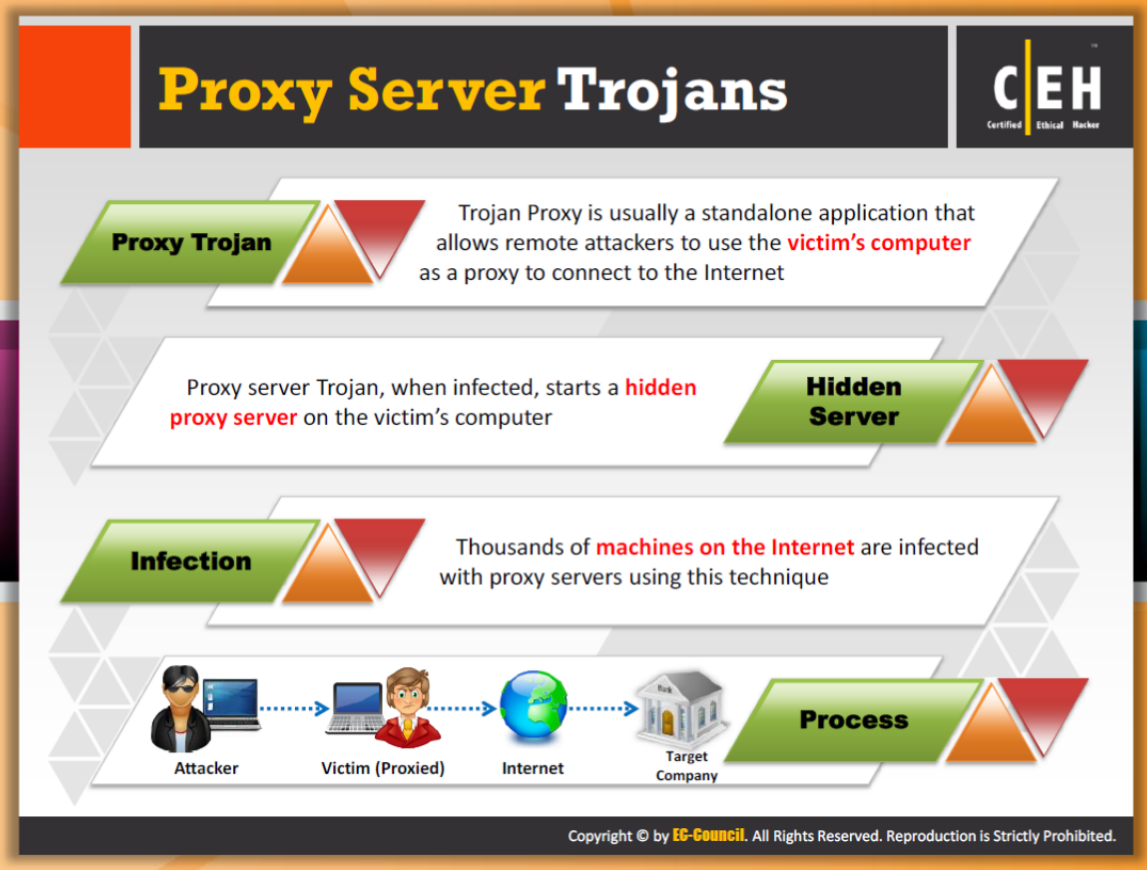


FIGURE 6.18: Illusion Bot and NetBot Attacker Screenshots



Proxy Server Trojans

A proxy server Trojan is a type of **Trojan** that customizes the target's system to act as a proxy server. A proxy server Trojan, when infected, starts a **hidden proxy server** on the **victim's computer**. The attacker can use this to carry out any **illegal activities** such as credit card fraud, identity theft, and can even launch malicious attacks against other networks. This can communicate to other proxy servers and can also send an email that contains the related information.

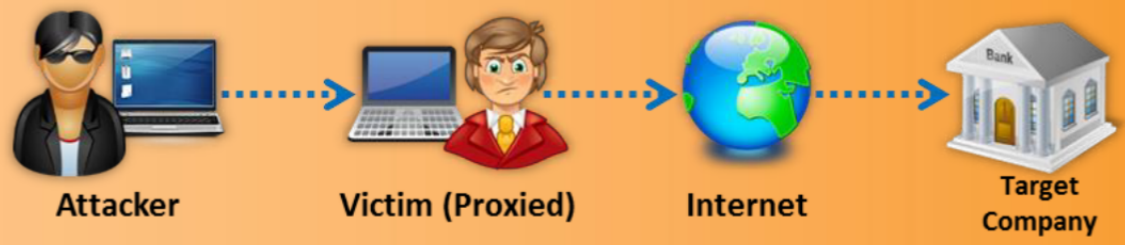
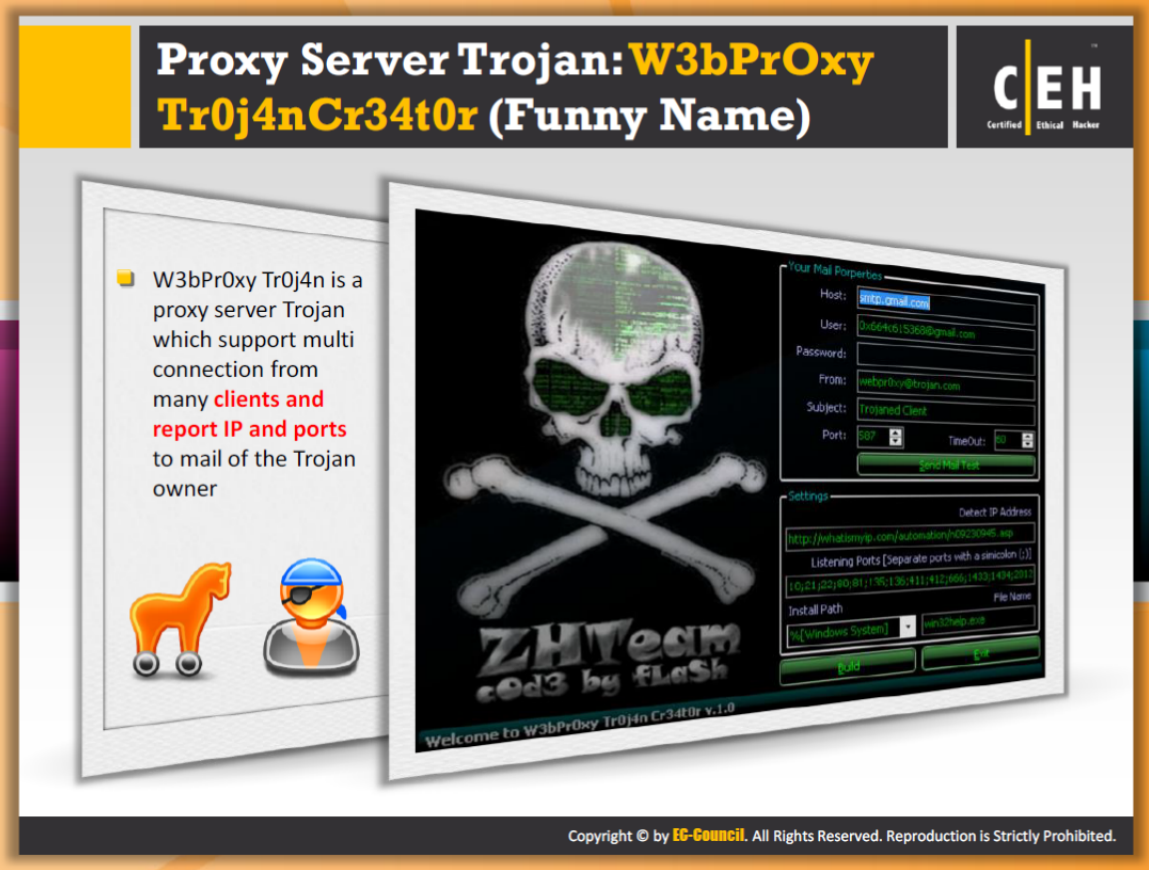


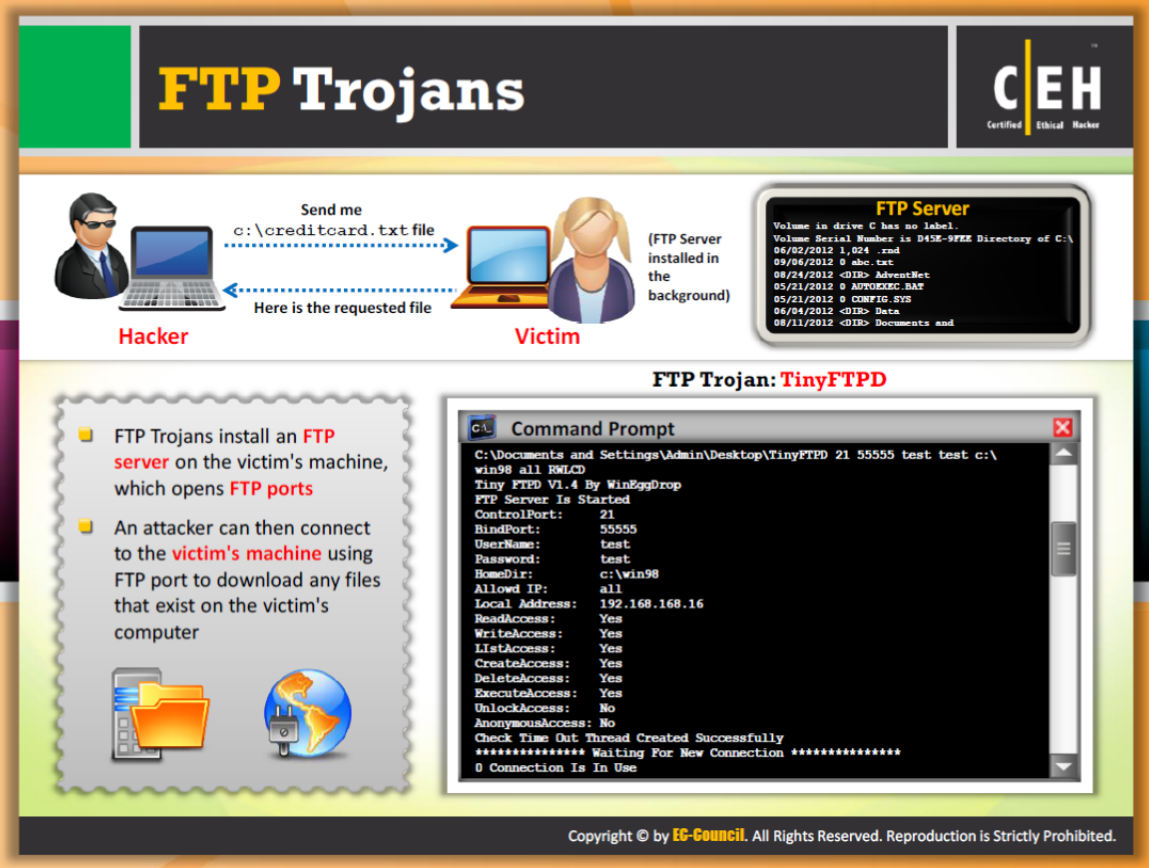
FIGURE 6.19: Attacker infecting Target company's system using Proxy Server Trojans



Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

W3bPrOxy Tr0j4nCr34t0r is a **proxy server Trojan** developed in order to access systems remotely. It supports multi-connections from many clients and reports IP and ports to the email of the Trojan owner.

FIGURE 6.20: W3bPrOxy Tr0j4nCr34t0r detecting IP address



FTP Trojans

An FTP Trojan is a type of Trojan that is designed to open **port 21** and make the target's system accessible to the attacker. It Installs an FTP server on the target's machine, allowing the attacker to gain access to sensitive **data** and **download/upload files/programs** through the **FTP Protocol**. Further, it also installs malware on the targets system. Credit card information, confidential data, email addresses, and password attacks can also be employed where only the attacker gains access to the system.

FIGURE 6.21: Attacker infecting victim's system using FTP Trojans

FTP Trojan: TinyFTPD.

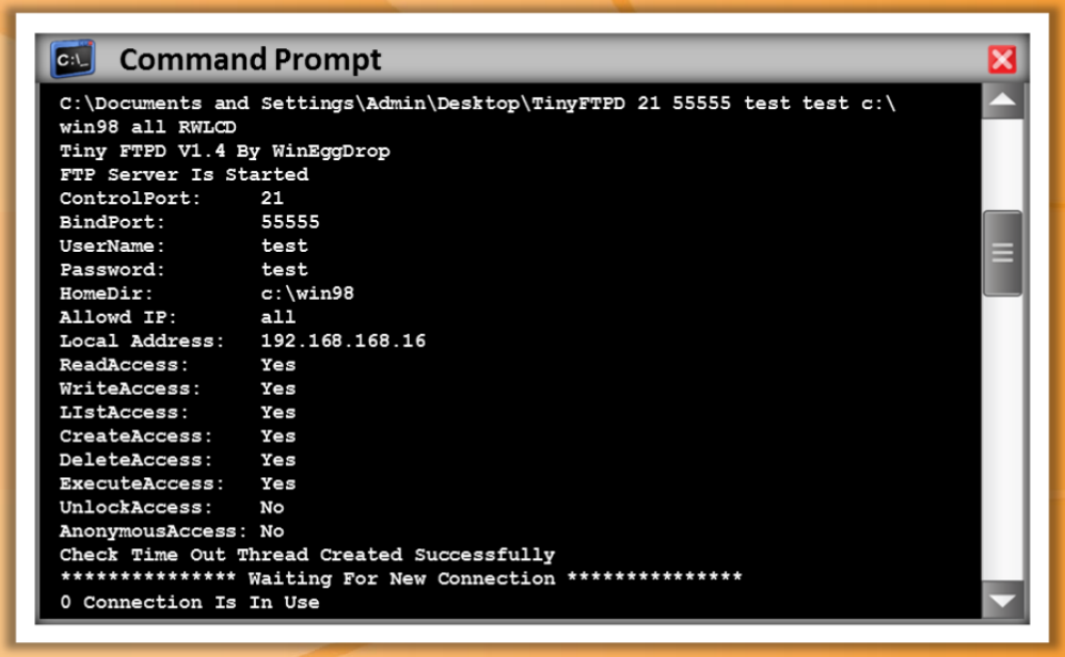
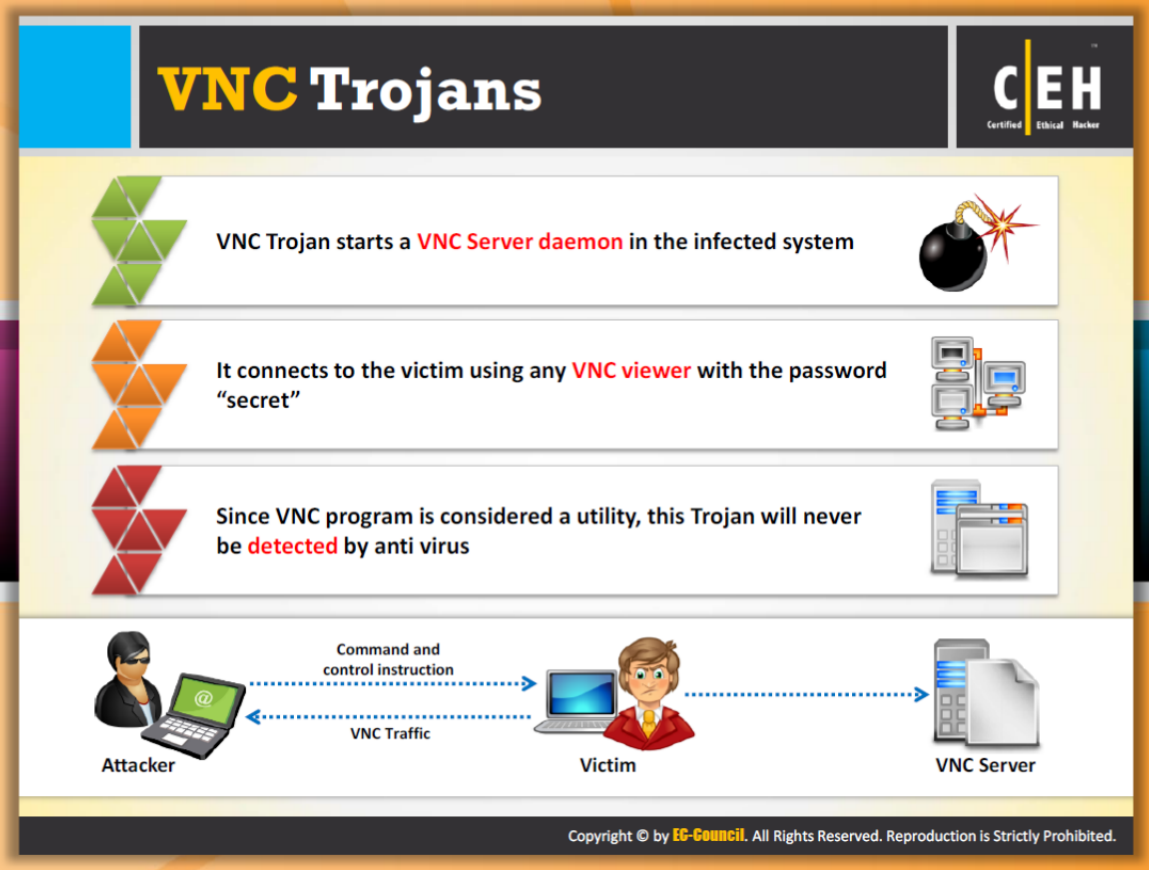


FIGURE 6.22: TinyFTPD Screenshot



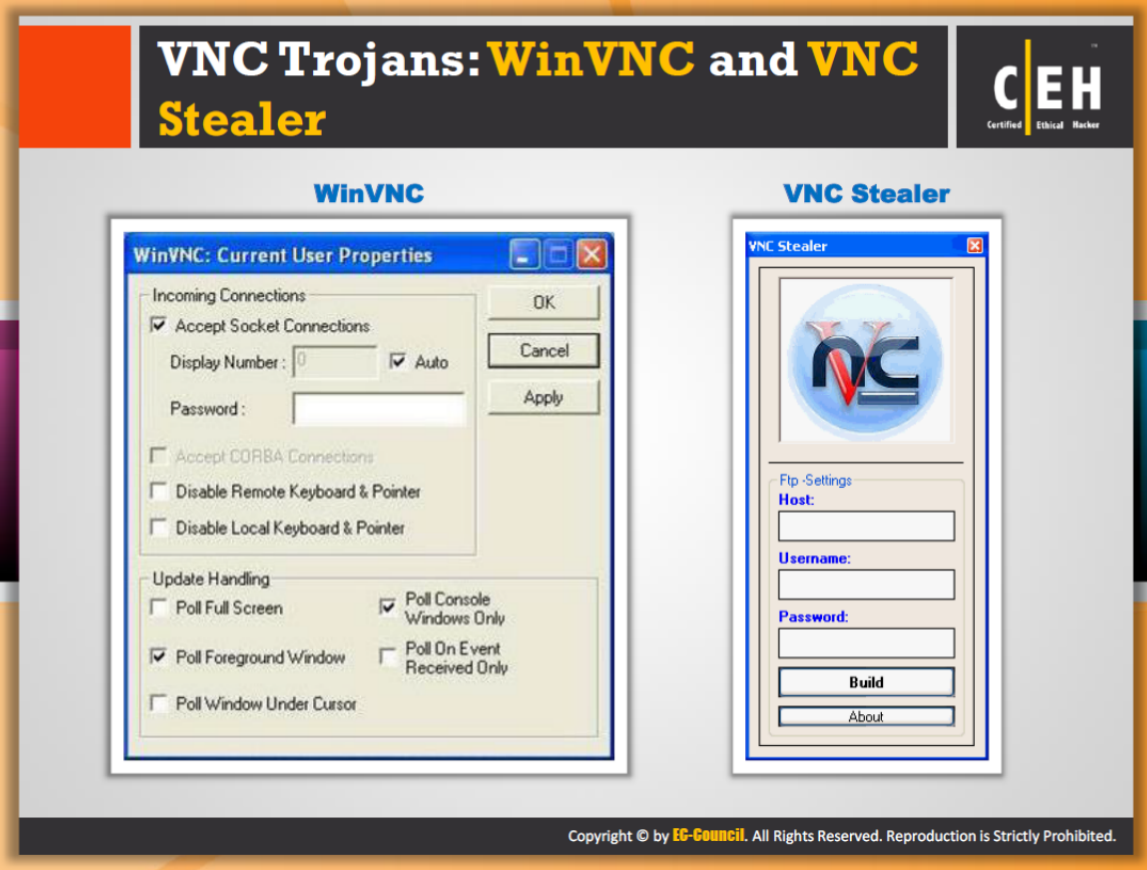
VNC Trojans

VNC Trojans allow attackers to use the target's computer as a **VNC server**. These Trojans won't be detected by antiviruses after they are run, because VNC Server is considered a utility.

Performs the following functions when it infects the system:

- Starts VNC Server daemon in the background when infected
- Connects to the target using any VNC viewer with the password "secret"

FIGURE 6.23: Attacker uses victim's computer as VNC server using VNC Trojans



VNC Trojans: WinVNC and VNC Stealer

WinVNC and VNC Stealer are two VNC Trojans.

WinVNC

WinVNC is used for a **remote view** or to control a Windows machine so this becomes a threat as attackers are able to inject a Trojan into the system and then they are able to access the target's system remotely.

VNC Stealer

VNC Stealer is a Trojan written in Visual Basic. **VNC.EXE** has been used to perform the following behavior:

- The process is packed and/or encrypted using a software packing process
- Creates system tray pop-ups, messages, errors, and security warnings
- Adds products to the system registry
- Writes to another Process's Virtual Memory (process hijacking)
- Executes a process
- Creates new folders on the system

- This process deletes other processes from a disk
- The process hooks code into all running processes, which could allow it to take control of the system or record keyboard input, mouse activity, and screen contents
- Registers a Dynamic Link Library File

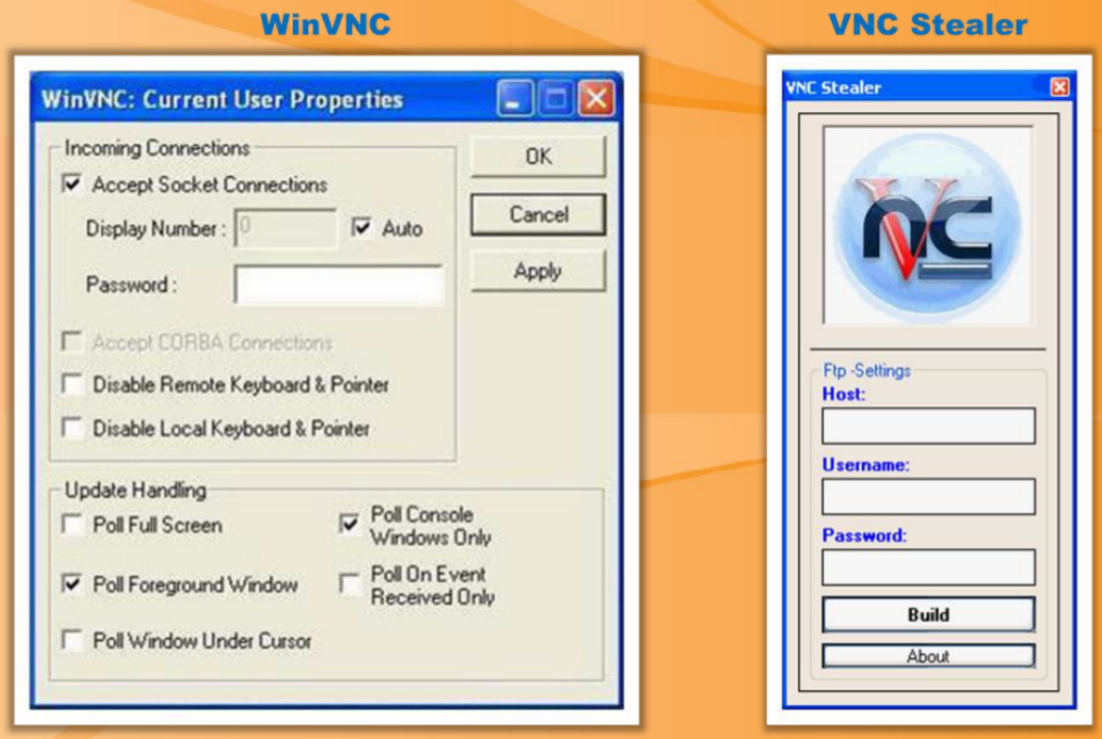
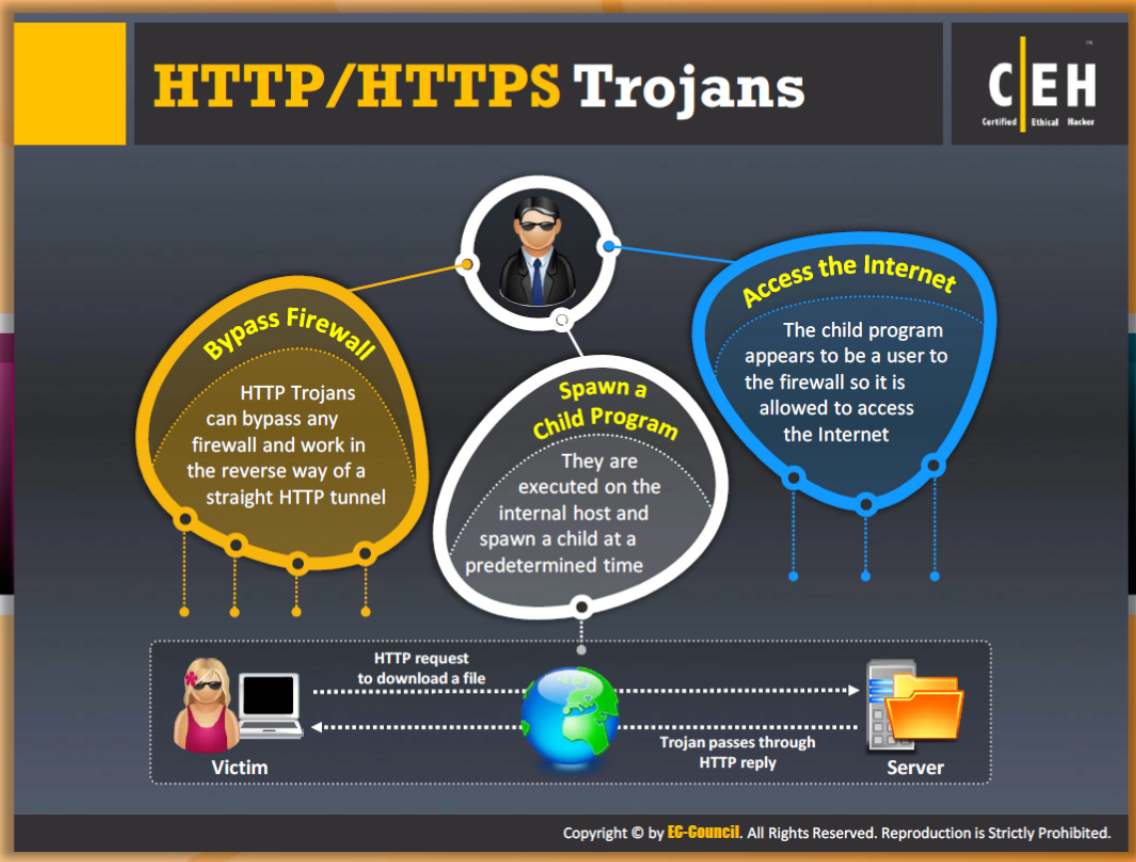


FIGURE 6.23: Screenshots showing WinVNC and VNC Stealer



HTTP/HTTPS Trojans

HTTP/HTTPS Trojans can bypass any firewall, and work in the reverse way of a straight HTTP tunnel. They use **web-based interfaces** and **port 80**. These Trojans are executed on the internal host and spawn a child every day at a certain time. The child program appears to be a target to the firewall which, in turn, allows it to access the Internet. However, this child program executes a local shell, connects to the web server that the attacker owns on the Internet through a legitimate-looking HTTP request, and sends it a ready signal. The legitimate-looking 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. All traffic is converted into a **Base64-like** structure and given as a value for a **cgi-string**, so the attacker can avoid detection. The following is an example of a connection:

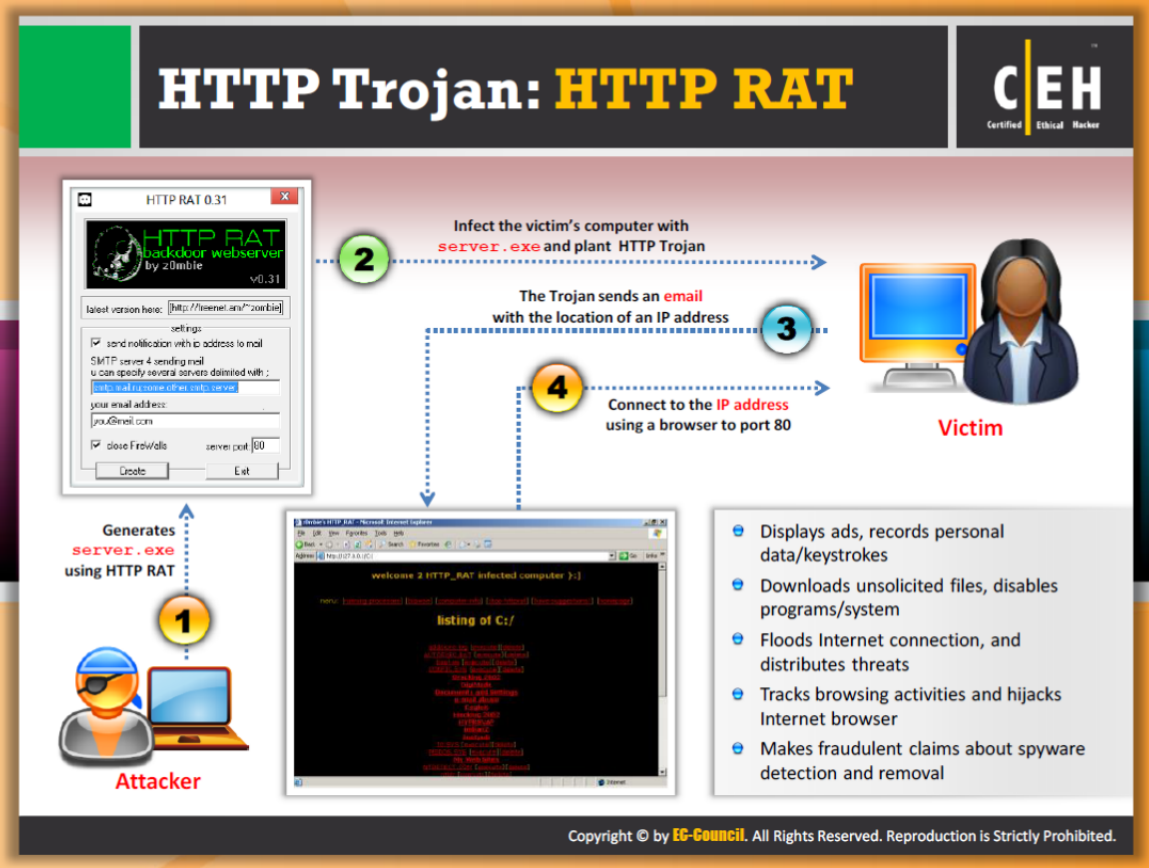
Slave: `GET/cgi-bin/order? M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdb1He7krj HTTP/1.0`

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 needed, the child is spawned 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 himself, 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) are supported. The program masks its name in the process listing. The programs are reasonably small with the master and slave programs, just 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.

FIGURE 6.24: Victim's system infected with HTTP Trojans



HTTP Trojan: HTTP RAT

RATs are malicious programs that run **invisibly** on host **PCs** and permit an intruder remote access and control. A RAT can provide a **back door** for administrative control over the target computer. Once the target system is compromised, the attacker can use it to distribute RATs to other vulnerable computers and establish a botnet. The **RAT** enables administrative control and makes it possible for the attacker to watch all the target's actions using keyloggers or any other **spywares**. An attacker can also implement **credit card fraud**, identity theft using confidential information, and can **remotely access web cams** and video recordings, take screenshots, format drives, and delete, download, and alter files. It can't be detected as it works like genuine programs and it is not easily noticed.

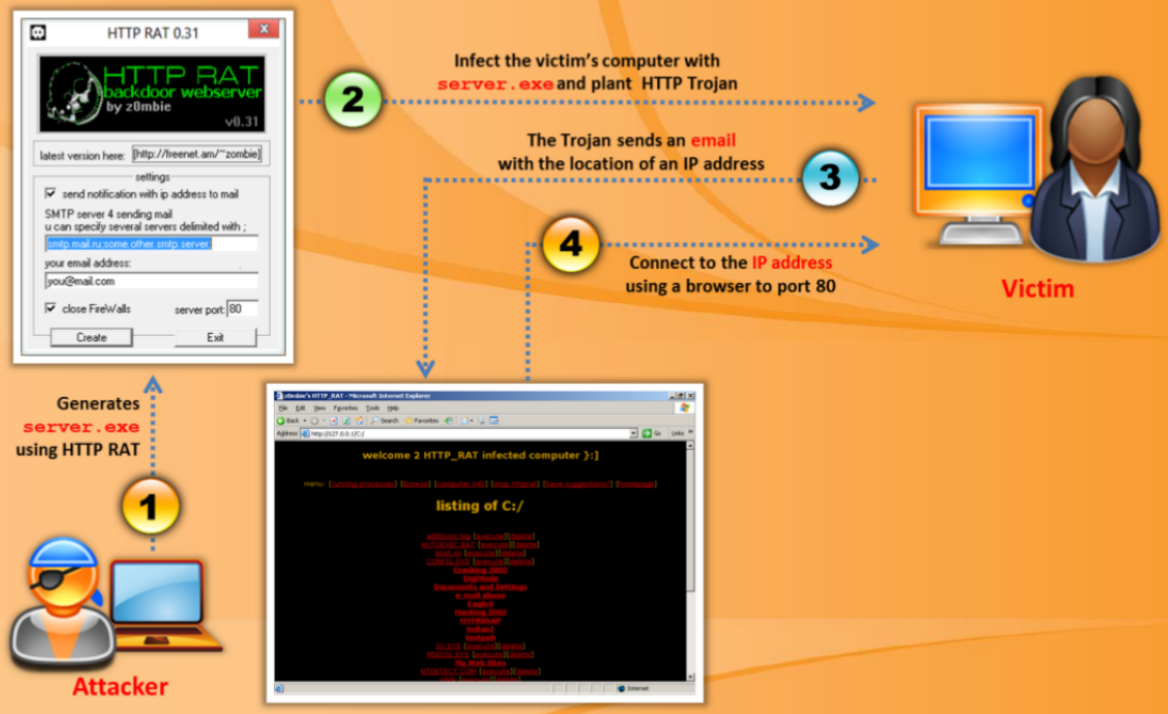
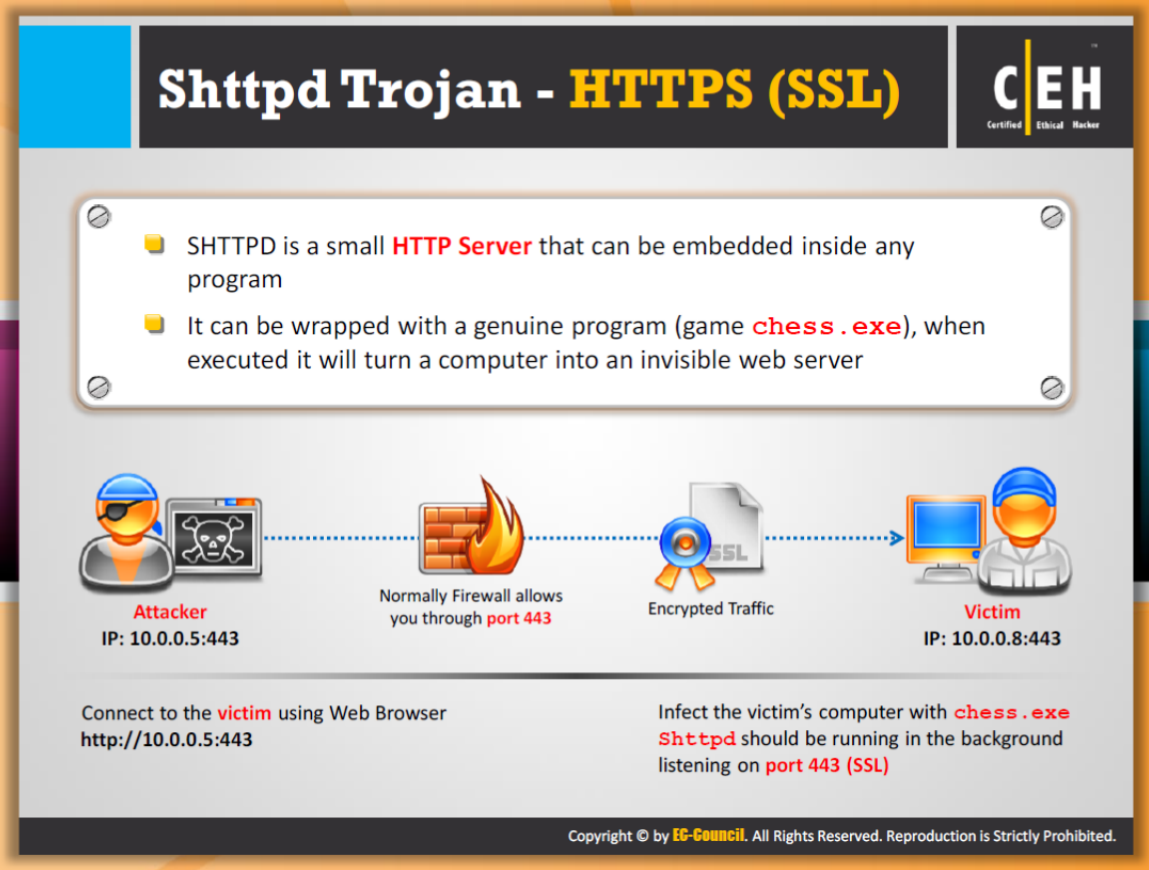


FIGURE 6.25: Attacker infecting Victim's system using HTTP RAT

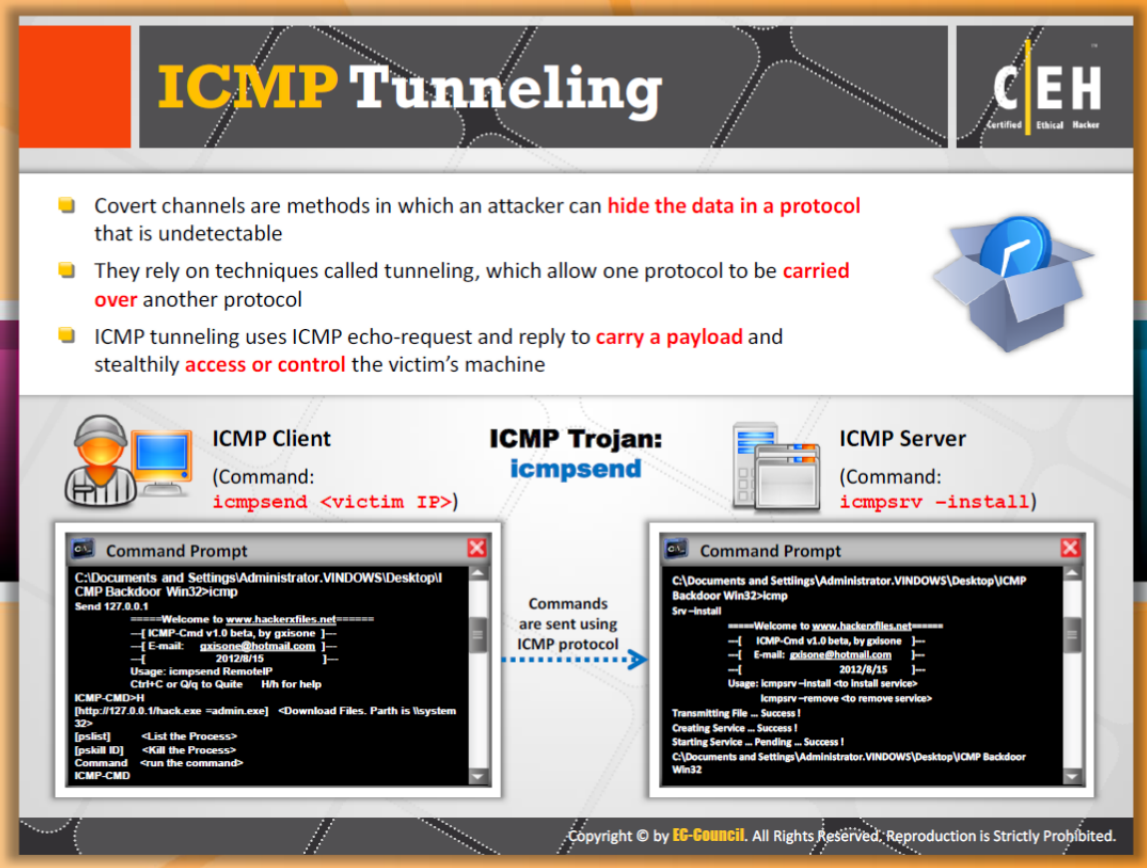


Shttpd Trojan - HTTPS (SSL)

Shttpd is a **small HTTP server** that can easily be embedded inside any program. **C++ source code** is provided. Even though shttpd is not a Trojan, it can easily be wrapped with a chess.exe file and it can turn a computer into an invisible web server.

- Infect the target's computer with chess.exe.
- Shttpd should be running in the background listening on port 443 (SSL).
- Connect to the target using a web browser: http://10.0.0.5:443.

FIGURE 6.26: Attacker infecting Victim's system using Shttpd Trojan



ICMP Tunneling

The concept of ICMP tunneling is simple since arbitrary information tunneling in the data portion of **ICMP_ECHO** and **ICMP_ECHOREPLY** packets is possible. ICMP_ECHO traffic contains a covert channel that can be destroyed due to tunneling. Network devices do not filter 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.

Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable. They rely on techniques called tunneling, which allow one protocol to be carried over another protocol. A covert channel is defined as a vessel through which the information can pass, and it is generally not used for information exchanges. Therefore, covert channels cannot be detected by using standard system security methods. Any process or bit of data can be a covert channel. This makes it an attractive mode of transmission for a Trojan, since an attacker can use the covert channel to install the backdoor on the target machine.

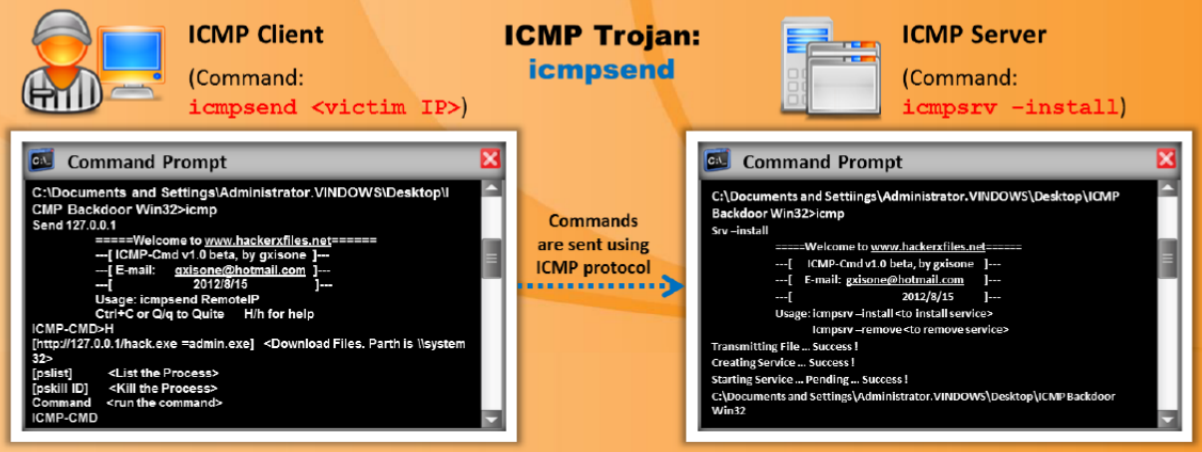
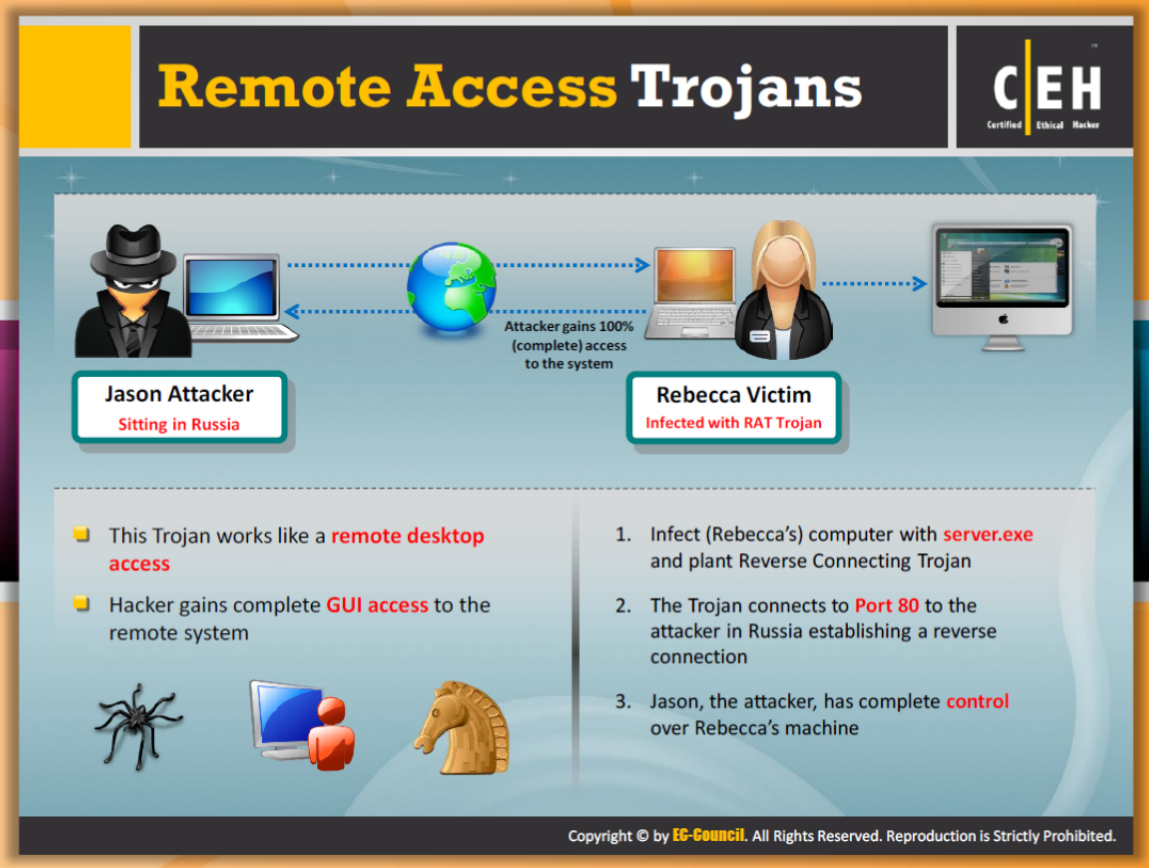


FIGURE 6.27: ICMP Tunneling



Remote Access Trojans

Remote access Trojans provide **full control** over the **target's system** to attackers and enables them to remotely access files, private conversations, accounting data, and so on in the target'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 target is behind a firewall on the network, there is less chance that a remote attacker would be able to connect to the Trojan. Attackers on the same network located behind the firewall can easily access the Trojans.

Examples include the **Back Orifice** and **NetBus Trojans**. Another example, the Bugbear virus that hit the Internet in September 2002, installed a Trojan horse on targets' systems, giving access to sensitive data to the remote attackers.

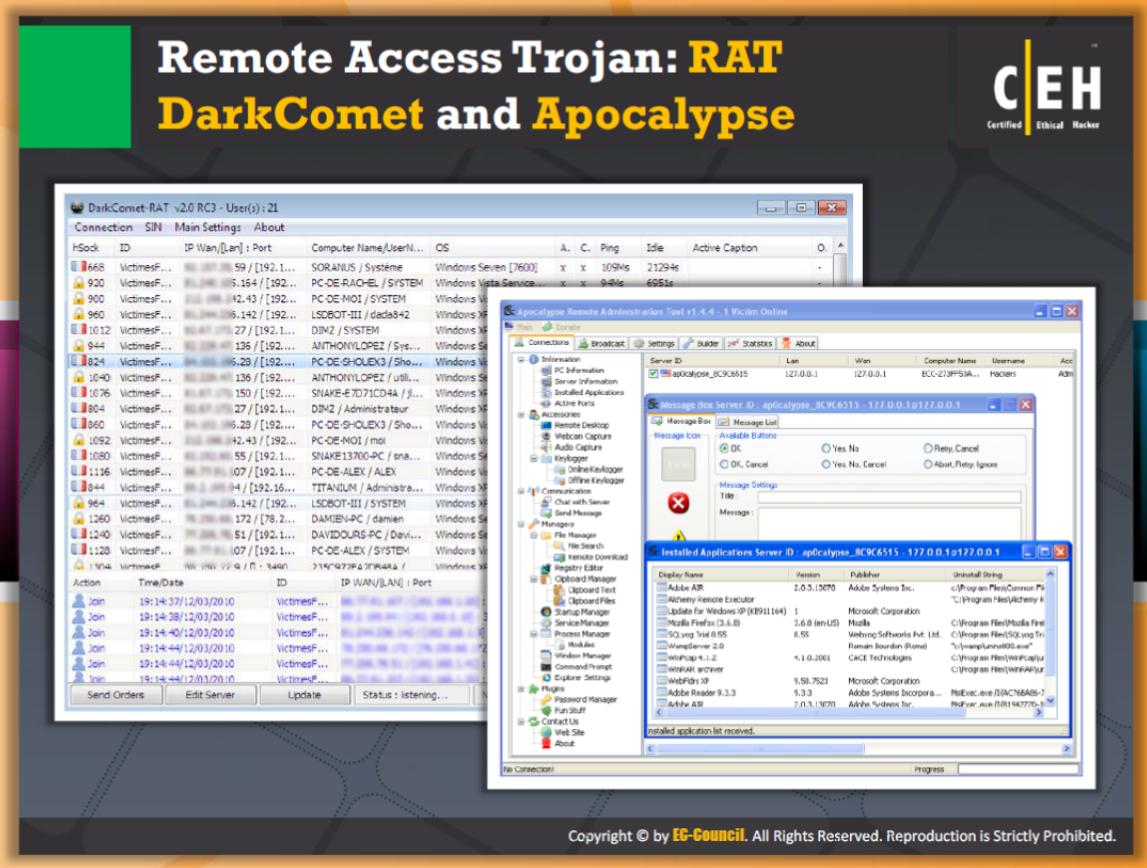
This Trojan works like a remote desktop access. The attacker gains complete GUI access to the remote system.

The process is as as follows:

1. Infects (Rebecca's) computer with server.exe and plants Reverse Connecting Trojan.
2. The Trojan connects to Port 80 to the attacker in Russia establishing a reverse connection.

3. Jason, the attacker, has complete control over Rebecca's machine.

FIGURE 6.28: Attacker infecting victim's machine using Remote access Trojans



Remote Access Trojan: RAT DarkComet and Apocalypse

DarkComet is a tool that allows you to **remotely access** the administrative controls and privileges of an infected machine without the user's knowledge or permission. It provides you with access to processes, registry, command prompts, webcams, microphones, applications and can even provide a **keylogger** whenever you use the system.

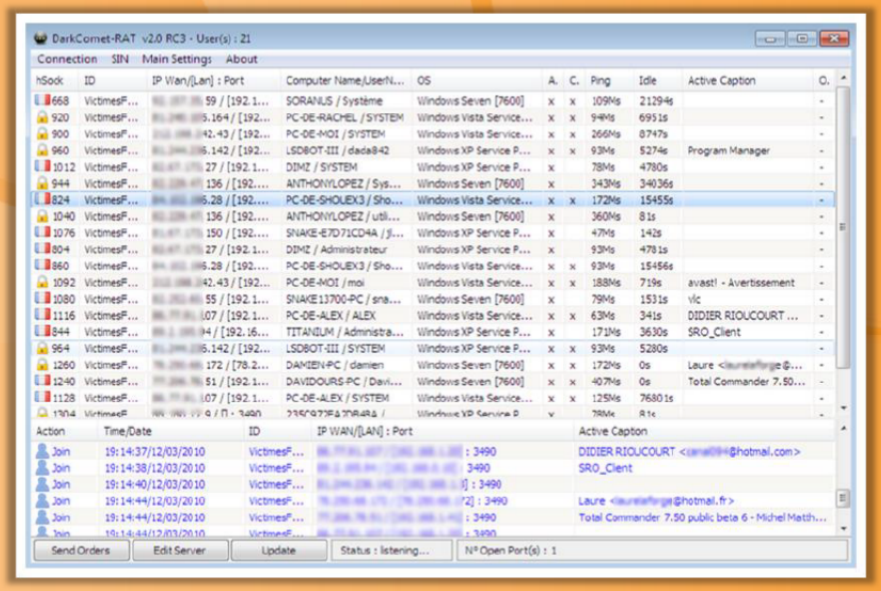


FIGURE 6.29: RAT DarkComet Screenshot

Apocalypse Remote Access Trojan is a tool that allows you to modify the entire registry and allow .dl files to run executables. This runs in invisible mode when it is executed.

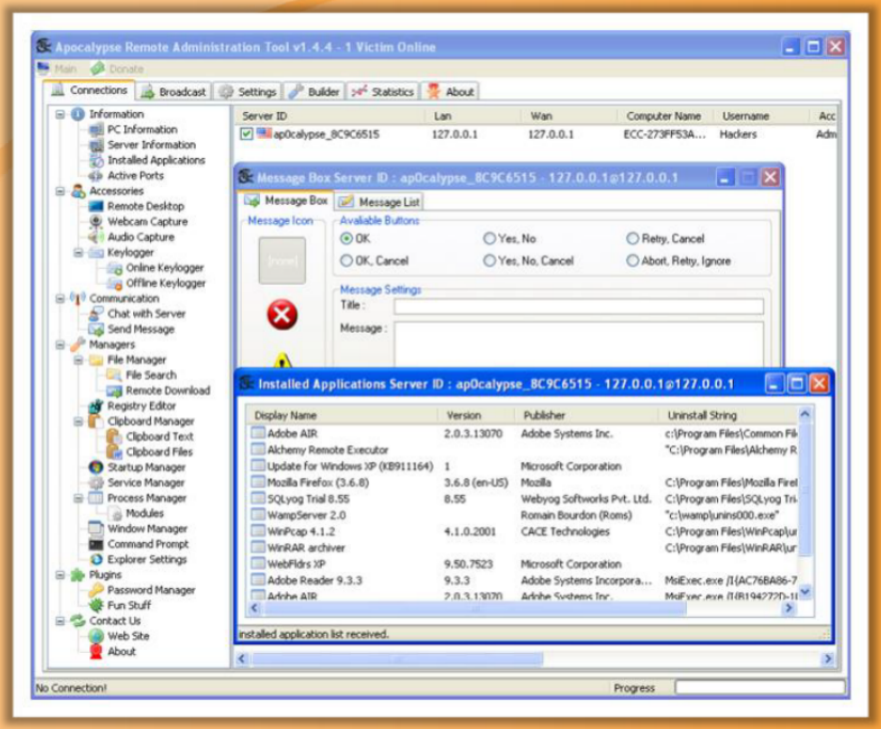
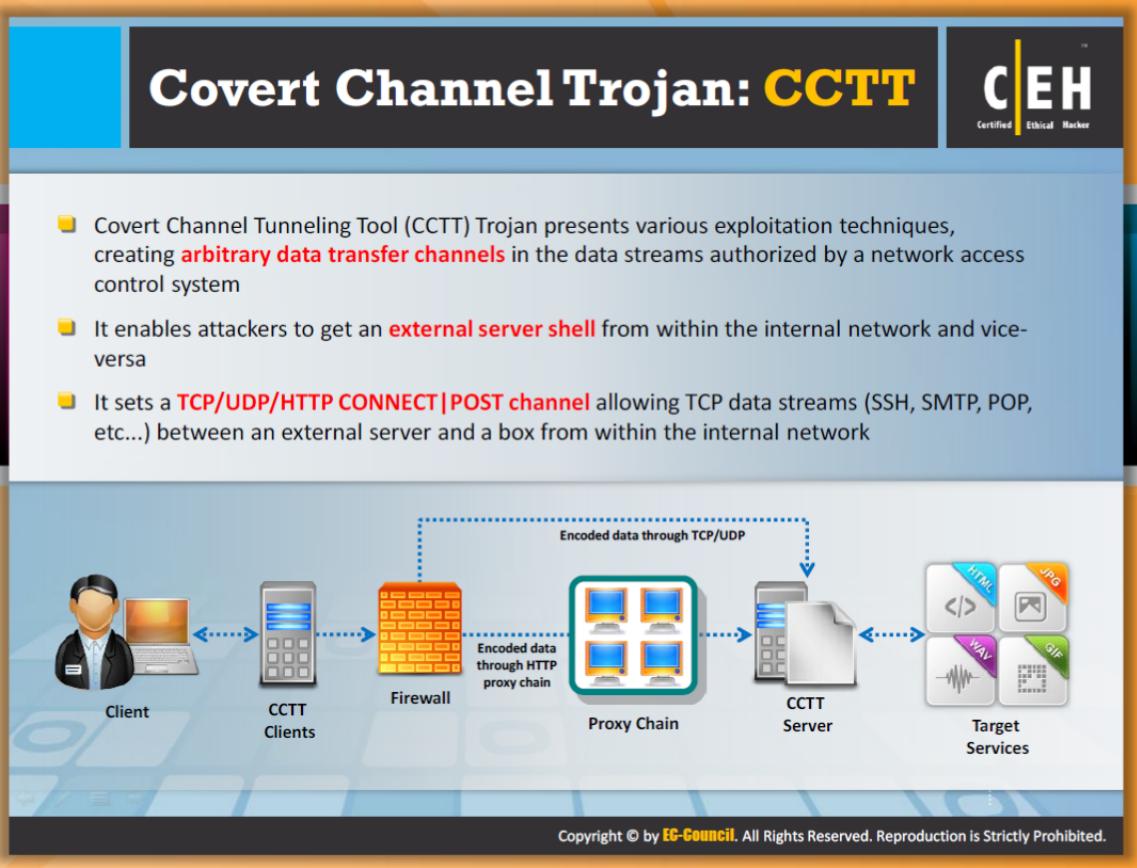


FIGURE 6.30: Apocalypse Screenshot



Covert Channel Trojan: CCTT

The Covert Channel Tunneling Tool is a **hidden channel tool**. It provides you with many probable ways to achieve and allow arbitrary **data transfer channels** in the data streams (TCP, UDP, HTTP) authorized by a **network access control system**. A 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.

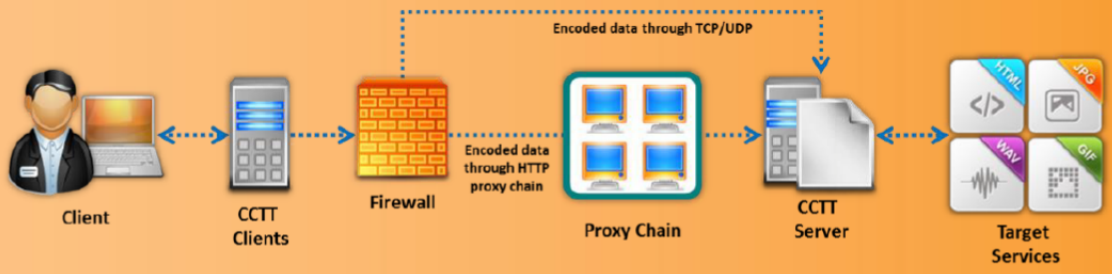
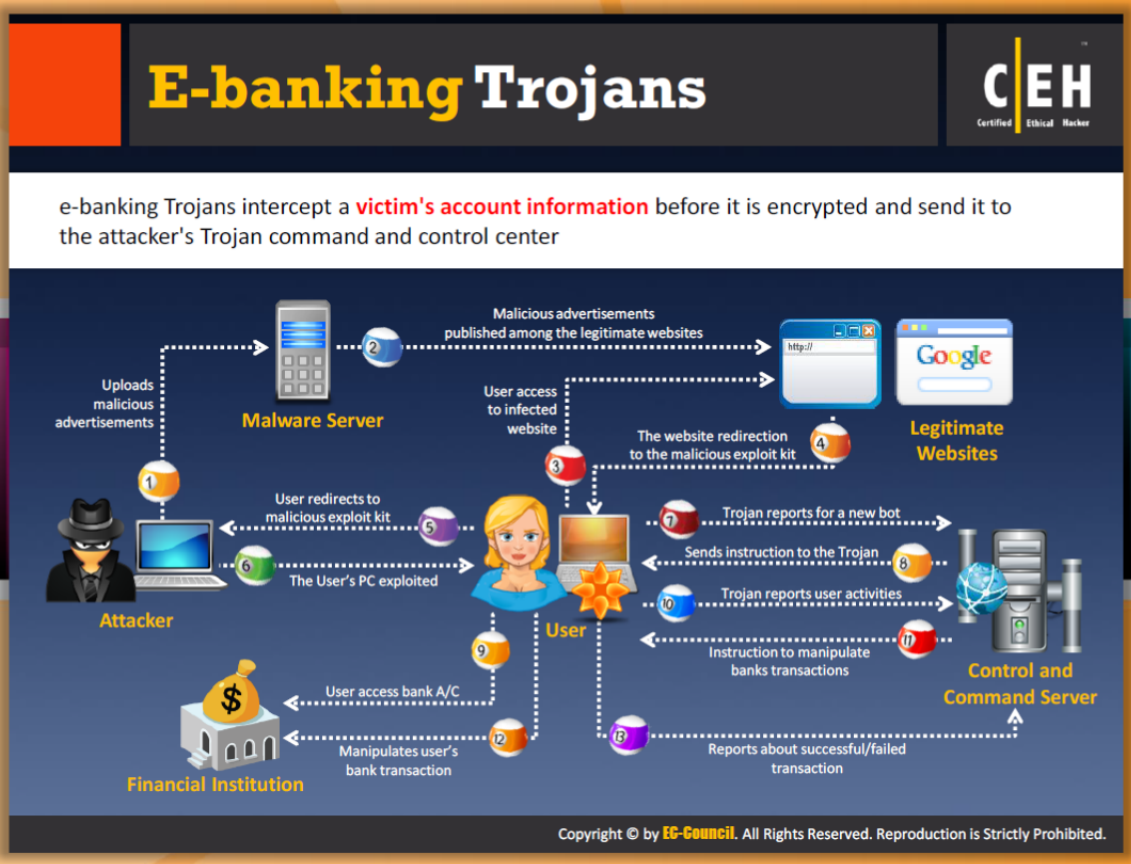


FIGURE 6.31: Covert Channel Trojan



E-banking Trojans

E-banking Trojans are **very dangerous** and have become a major threat to the banking transactions performed online. This **Trojan** is installed on the victim's computer when he or she clicks the email attachment or clicks on some advertisement once the target logins in to the banking site. The Trojan is **preprogrammed** with a minimum range and maximum range to steal. So it doesn't withdraw all the money from the bank. Then the Trojan creates screenshots of the bank account statement; the victims aren't aware of this type of fraud and thinks that there is no variation in their bank balance unless they check the balance from other systems or from **ATM machines**. Only when they check the balance will the differences be noticed.

The following diagram explains how the attack is carried out using E-banking Trojans.

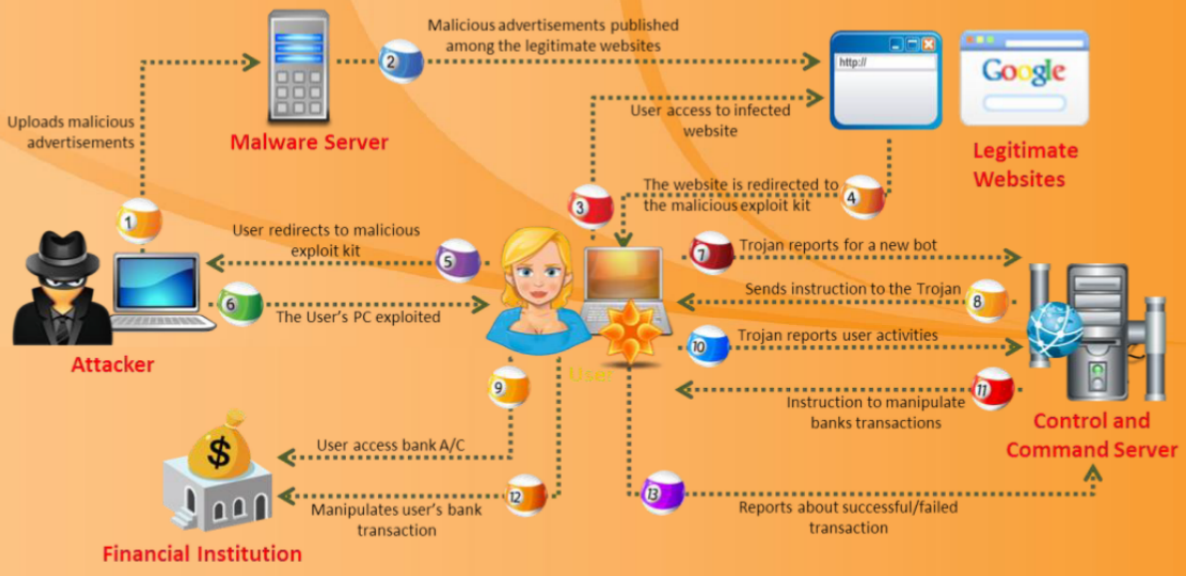
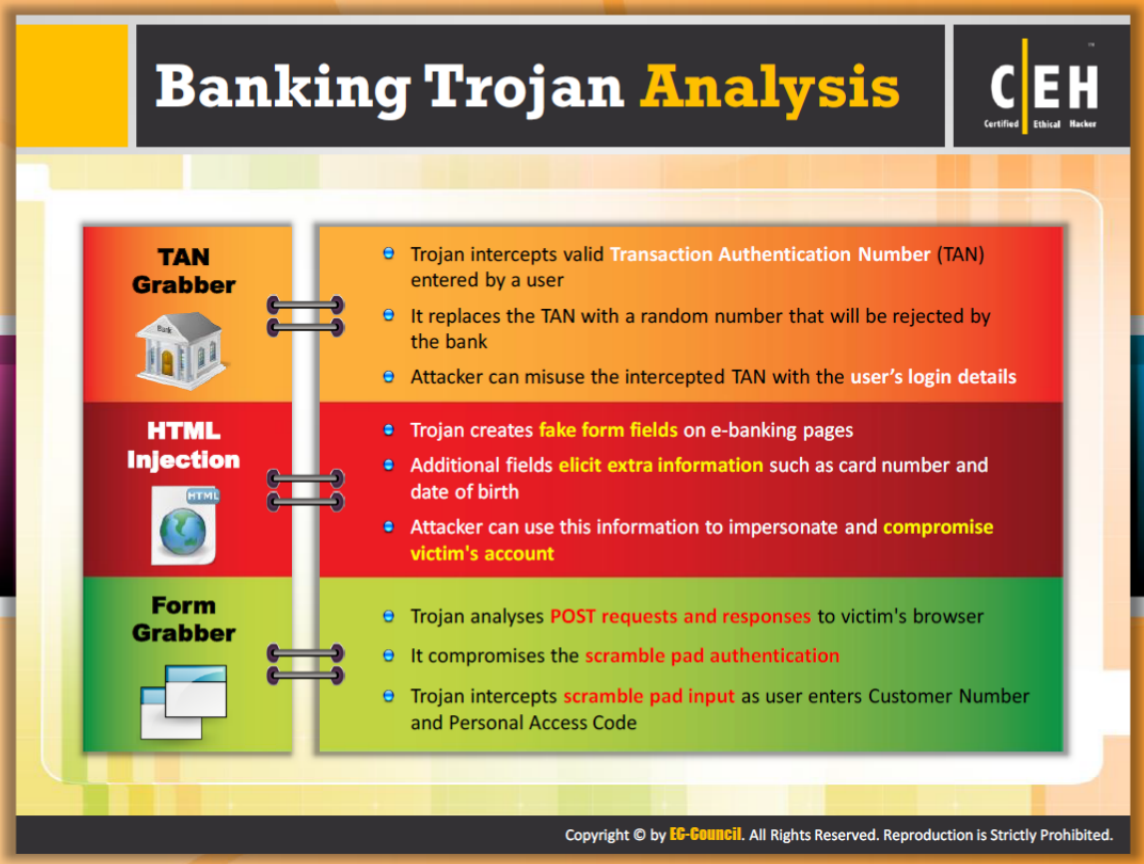


FIGURE 6.32: illustrating the attack using E-banking Trojans

Here the attacker first infects the malicious advertisements and publishes these advertisements among genuine websites. When the victims access the **infected website**, it automatically redirects him or her to a website from where the exploit kit gets loaded onto the victim's system. Thus, the exploit kit allows the attacker to control what is loaded in the victim's system and used for installing a Trojan horse. This malware is **highly obfuscated** and can only be detected by few **anti-virus systems**. The system of the victim is now a botnet from where the Trojan easily sends and receives instruction from the control and command server without the knowledge of the victim. When a victim access his or her bank account from the infected system, all the sensitive information, i.e., used by the victim in accessing account information such as login credentials (**user name password**), phone number, security number, date of birth, etc. are sent to the Control and Command Server by the Trojan. If the victim is accessing the transaction section of the banking website for performing online transactions, then the data that is entered by the victim on the transaction form is sent to the Control and Command Server instead of to the bank website. The control and command server system analyzes and decodes the information and **identifies suitable** money mule bank accounts. The Trojan receives instructions from the control and command server to send the latest transaction form that is updated by the control and command server to the bank for transferring money to the mule account. Confirmation from the bank about successful/failed transaction of the money that was transferred is also reported by the Trojan to the control and command server .



Banking Trojan Analysis

A banker Trojan is a malicious program that allows obtaining personal information about users and clients using online banking and payment systems.

A banking Trojan analysis involves the following three basic types:

Tan Gabbler: A **Transaction Authentication Number (TAN)** is used for authenticating the online banking transaction, which is a single-use password. The banking Trojan explicitly attacks the target's online banking services that depend on the TAN. When the TAN is entered, the Trojan grabs that number and changes that number with any random number that is incorrect and rejected by the bank. The content is filtered by the Trojan and the incorrect number is replaced in order to satisfy the target. An attacker can misuse the intercepted TAN with the target's login details.

HTML Injection: This type of Trojan creates duplicate fields on the **online banking sites** and these extra fields are used by the attacker to collect the targets account details, credit card number, date of birth, etc. Attackers can use this information to impersonate and compromise the target's account.

Form Grabber: This is an advanced method of collecting data from the Internet available on the various browsers. This is highly effective in collecting the target IDs, passwords, and other sensitive information.

E-banking Trojan: ZeuS and SpyEye

ZeuS

Source: http://www.secureworks.com

ZeuS is a latest threat for online banking transactions as it uses both form **grabber** as well as **keystroke logging**. It is mainly spread through drive-by downloads and phishing schemes. The ZeuS botnet targets only Windows. New version of ZeuS even affects Windows Vista. It has evolved over time and includes a full arsenal of information stealing capabilities:

- 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 targets 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 (%system root%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

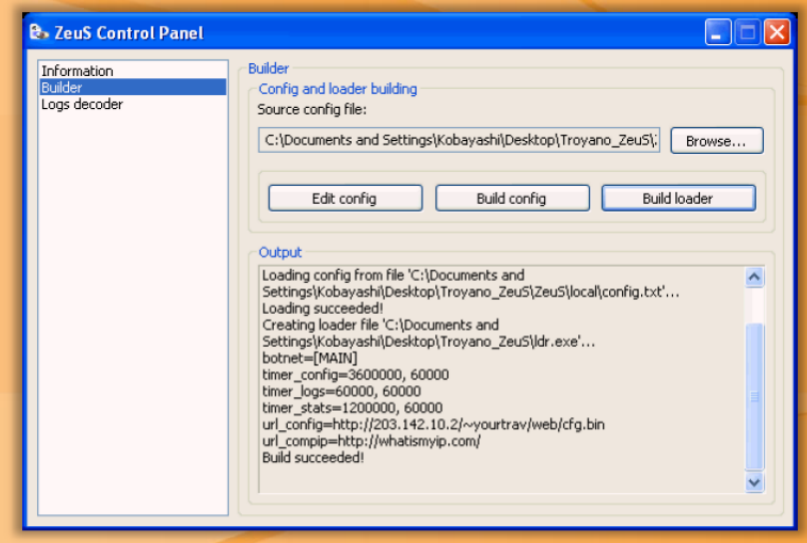
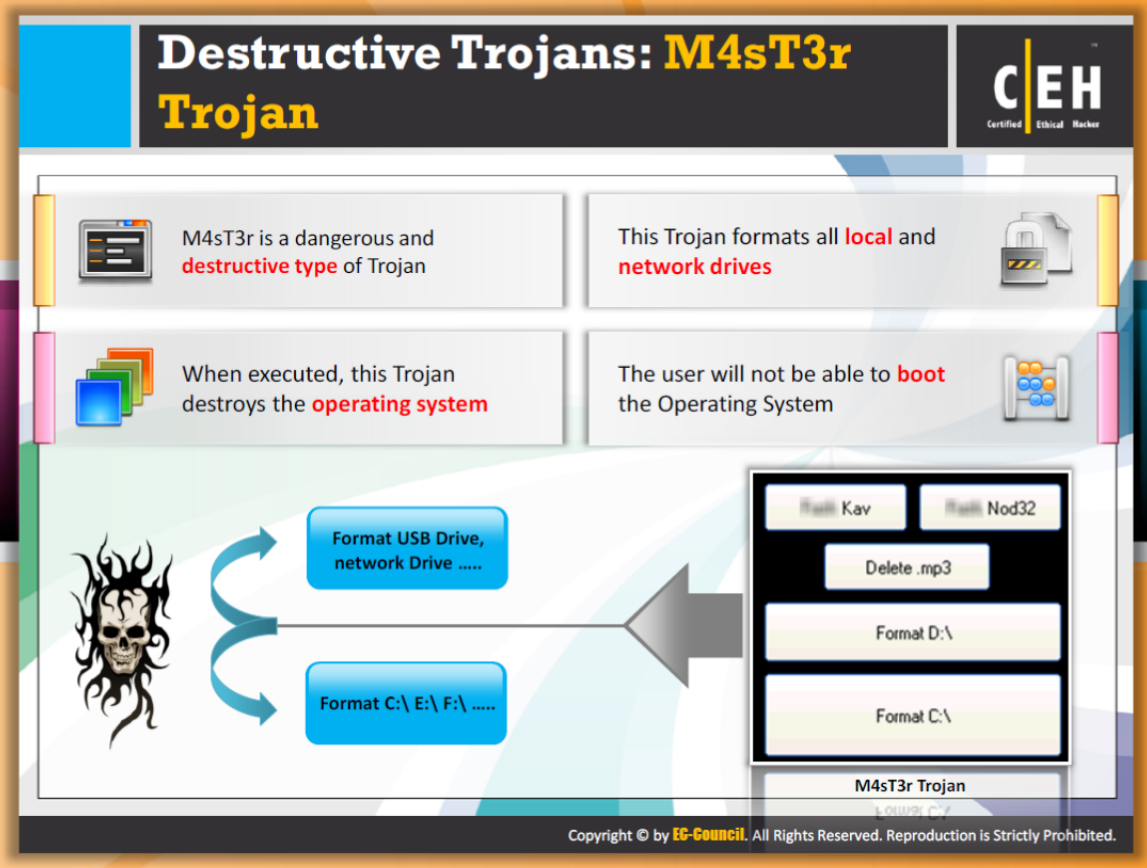


FIGURE 6.33: ZeuS Screenshot

SpyEye

SpyEye is malicious software that is used by the 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.

FIGURE 6.34: SpyEyeScreenshot



Destructive Trojans: M4sT3r Trojan

The M4sT3r Trojan is exclusively designed to **destroy or delete files** from the victim's computer. Files are automatically deleted by the Trojans, which can be controlled by the attacker or can be preprogrammed like a **logic bomb** to perform a particular task on a given time and date.

When executed, this Trojan destroys the operating system. The victim cannot boot the operating system. This Trojan formats all local and network drives.

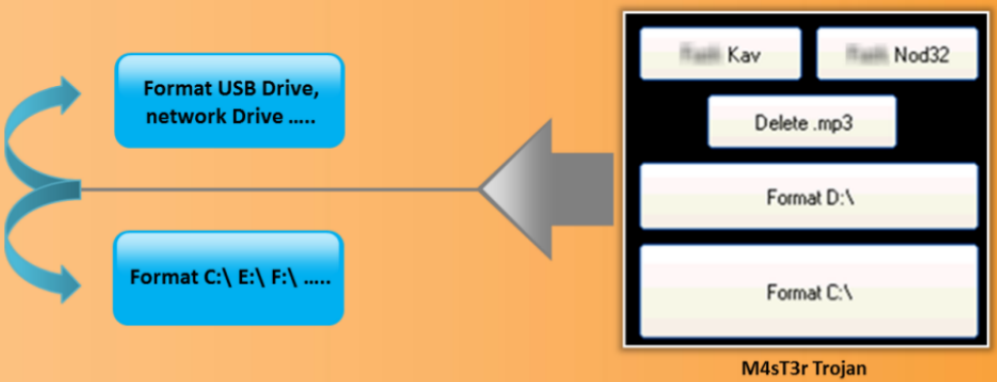
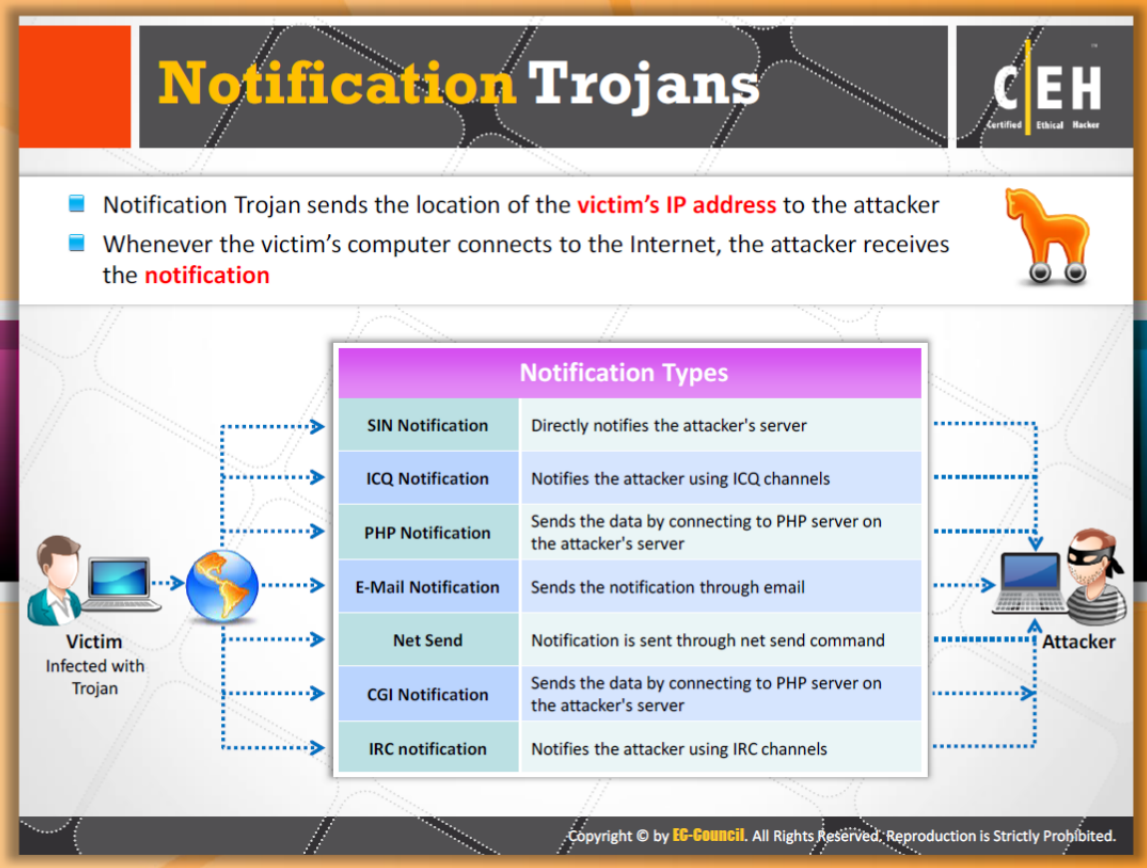


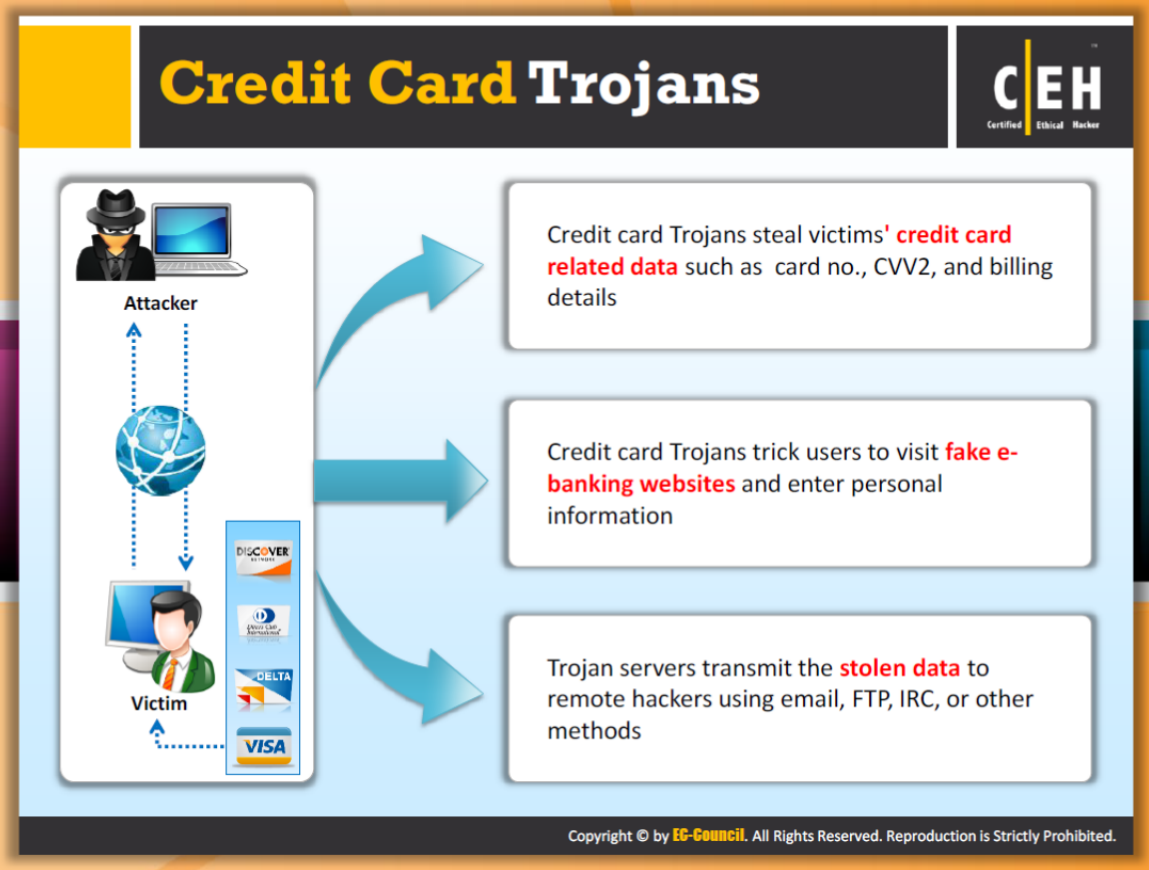
FIGURE 6.35: Attacker using M4sT3r Trojan for deleting or destroying files



Notification Trojans

Notification Trojans send the IP address of the **victim's computer** to the attacker. Whenever the victim operates the system, the notification Trojan notifies the attacker. Some of the notifications include:

- 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
- Email 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

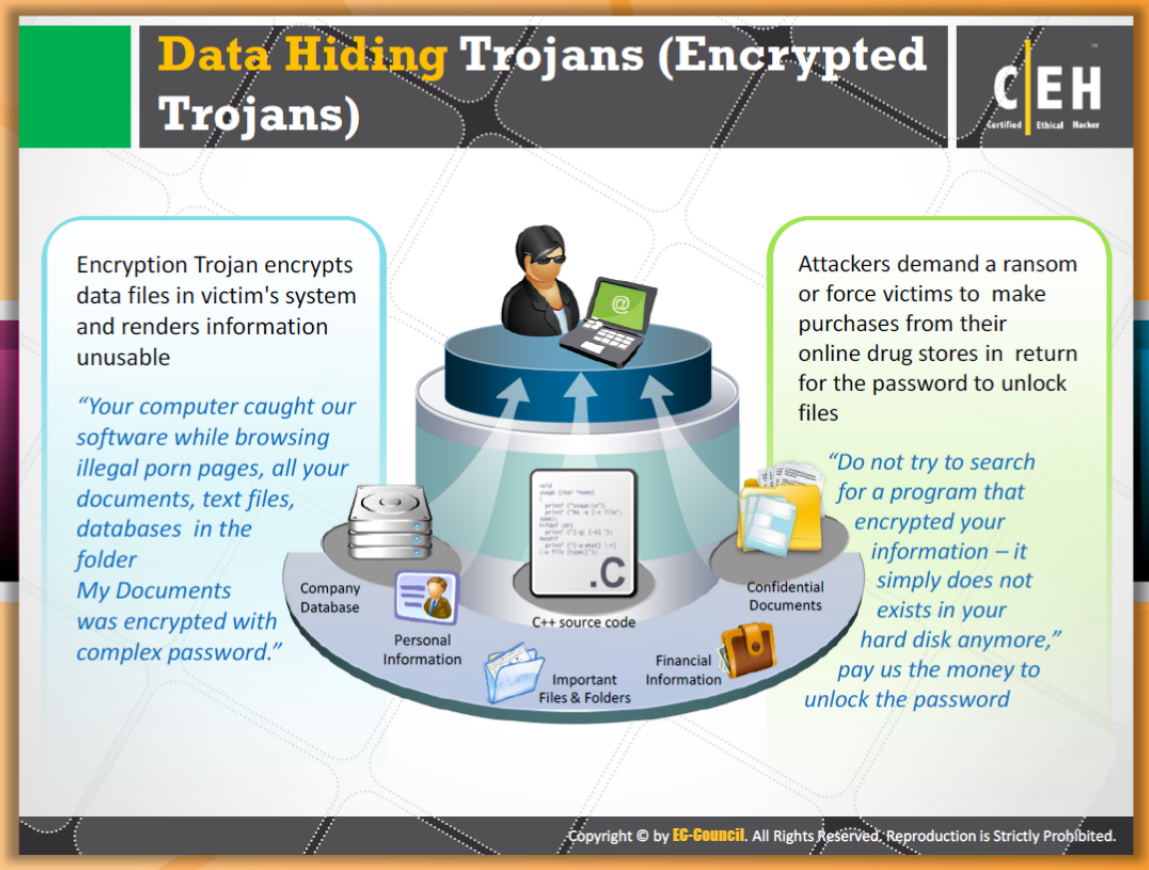


Credit Card Trojans

Credit card Trojans, once they are installed on the victim's system, collect various details such as credit card numbers, latest billing details, etc. Then, a **fake online banking registration** form is created and they make the credit card user believe that it is genuine information from the bank. Once the user enters the required information, attackers collect the information and use the credit card for personal use without the knowledge of the victim.

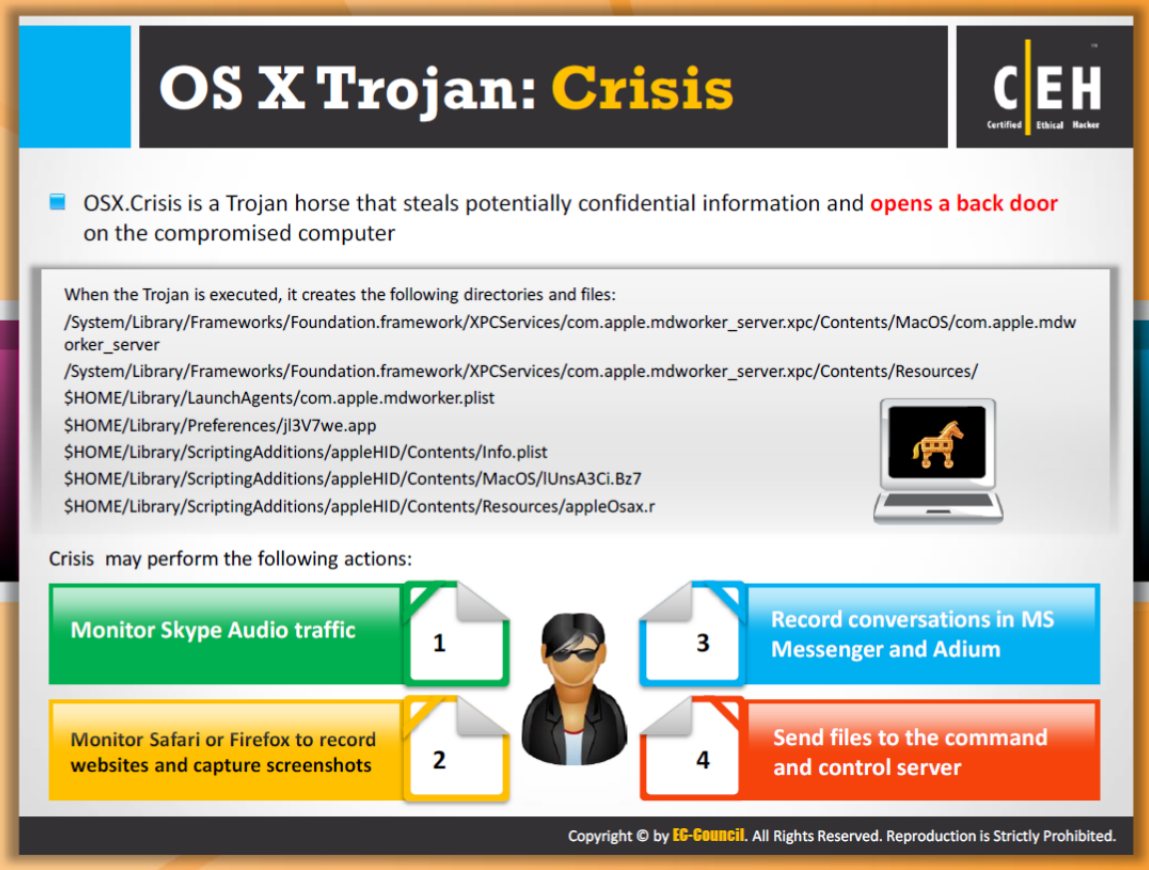
Credit card Trojans steal victims' **credit-card-related data** such as card number, CVV2s, and billing details. These Trojans trick users into visit fake e-banking websites and entering personal information. The Trojan servers transmit the stolen data to remote hackers using email, FTP, IRC, or other methods.

FIGURE 6.36: Attacker stealing credit card information of victim's using credit card Trojan



Data Hiding Trojans (Encrypted Trojans)

Encryption Trojans encrypt the data present on the victim's computer and renders the complete data 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 drugstores 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 can be decrypted only by the attacker, who demands money, or they can force the user buy from a few websites for decryption.



OS X Trojan: Crisis

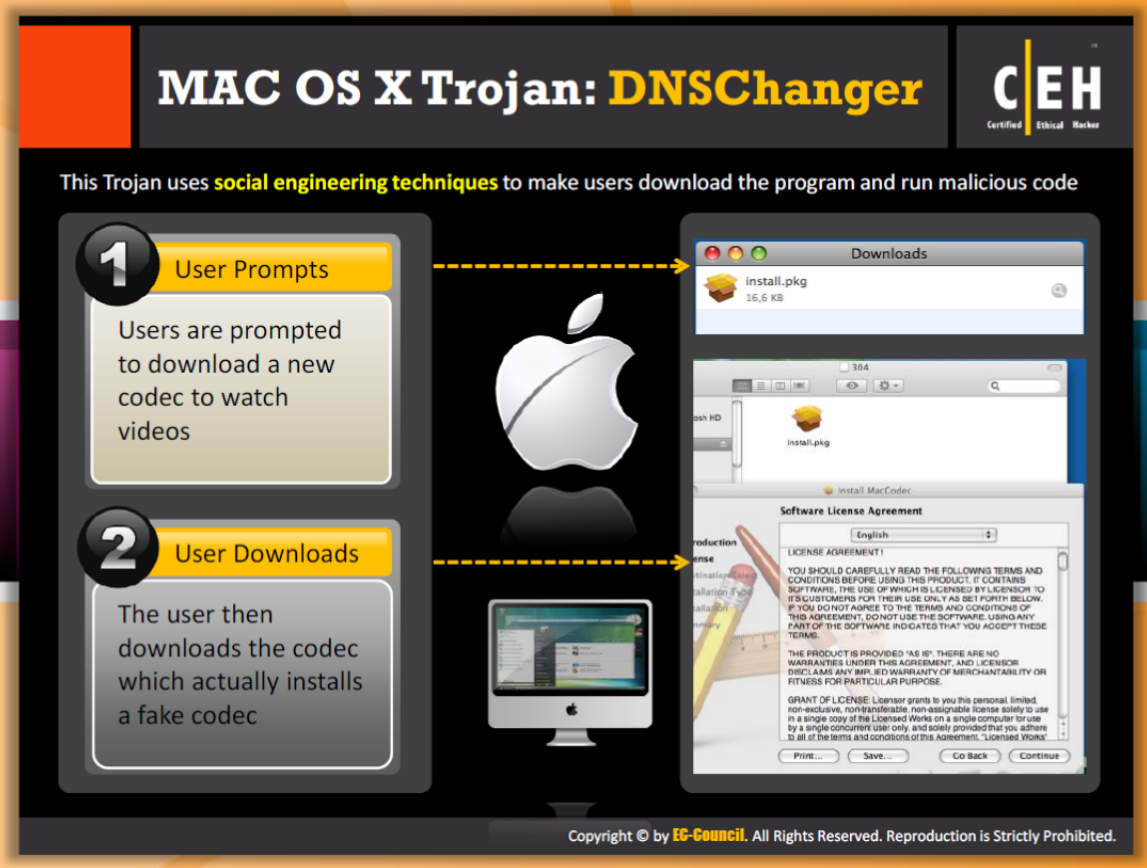
OSX.Crisis is a **Trojan horse** that steals potentially sensitive information that is on the victim's system and opens a back door on the compromised computer (victim's system) for future attacks.

When the Trojan is executed, it creates the following directories and files:

```
/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/MacOS/com.apple.mdworker_server
/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/Resources/
$HOME/Library/LaunchAgents/com.apple.mdworker.plist
$HOME/Library/Preferences/jl3V7we.app
$HOME/Library/ScriptingAdditions/appleHID/Contents/Info.plist
$HOME/Library/ScriptingAdditions/appleHID/Contents/MacOS/lUnsA3Ci.Bz7
$HOME/Library/ScriptingAdditions/appleHID/Contents/Resources/appleOsax.r
```

The following are the actions performed by the OSX.Crisis:

- Monitor Skype audio traffic
- Monitor Safari or Firefox to record websites and capture screenshots
- Record conversations in MS Messenger and Adium
- Send files to the command and control server



MAC OS X Trojan: DNSChanger

The malware modifies the DNS settings of the **active network**. The users are forced to download codecs or other movie downloads through **QuickTime**, etc. Once the download is finished, then the Trojan is attacked, resulting in slow access to the Internet, unnecessary ads popping up on the screen of the computer, etc. This Trojan uses social engineering techniques to make users download the program and run malicious code.

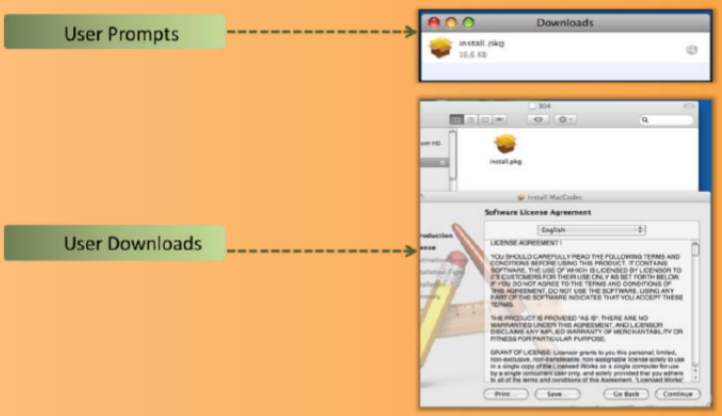
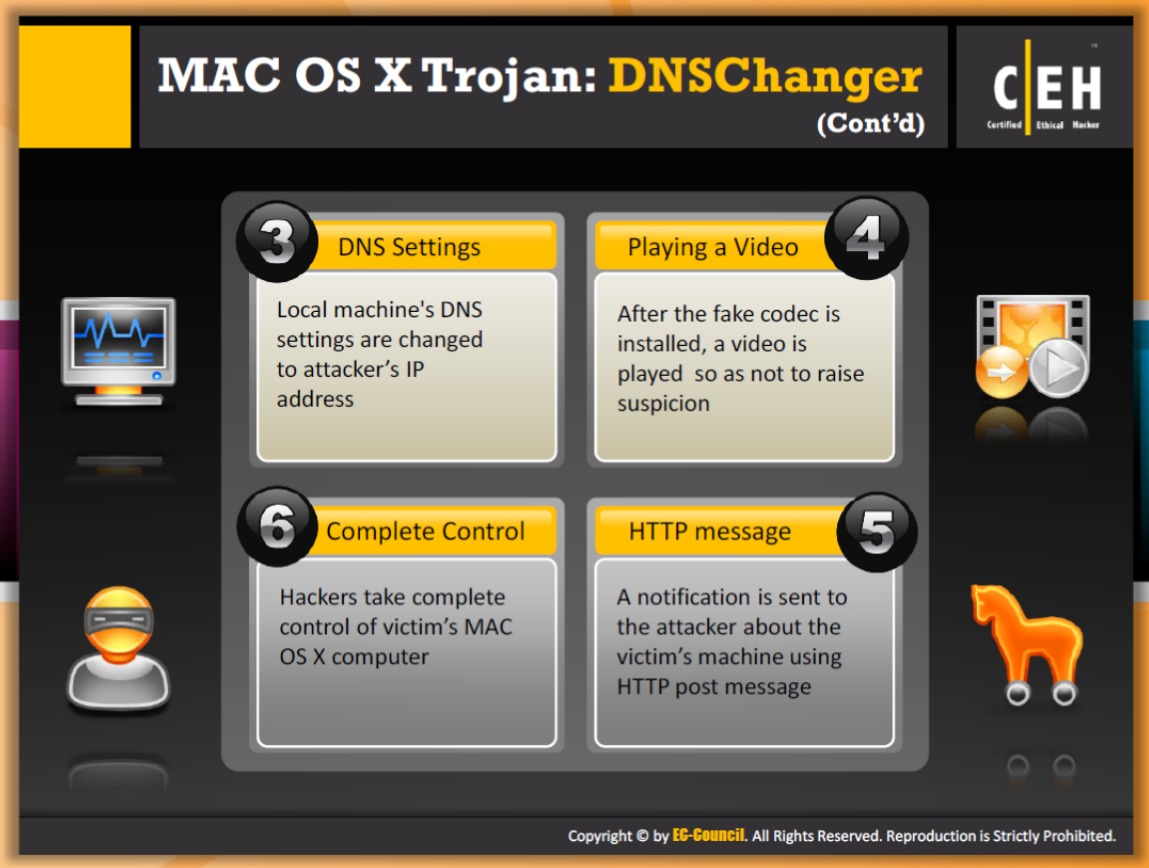


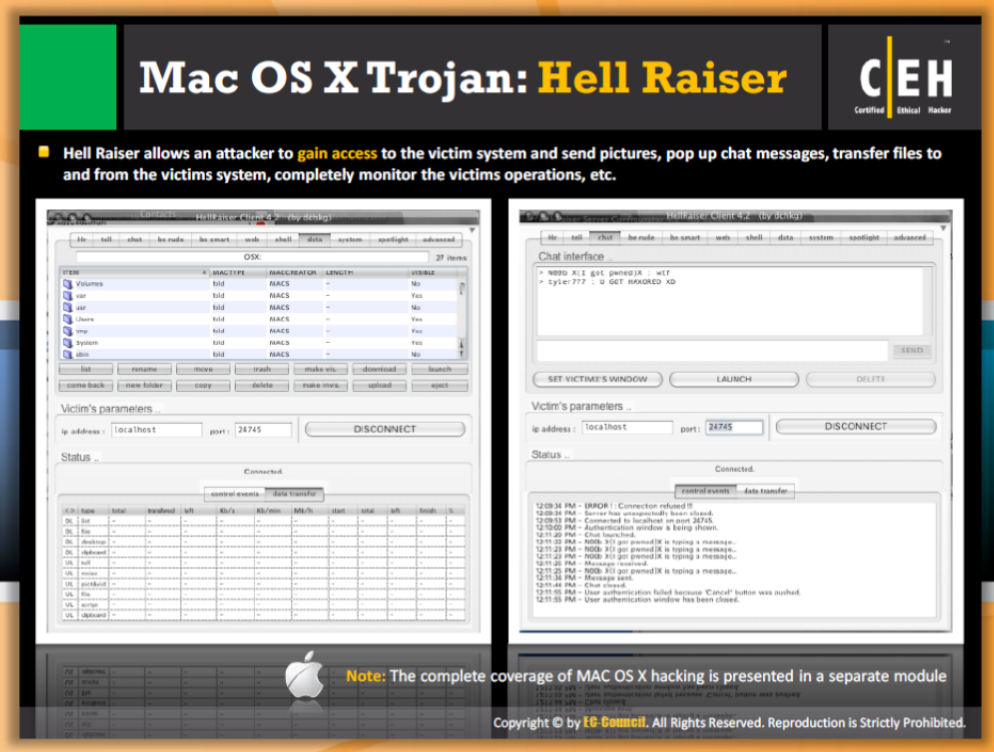
FIGURE 6.37: Attacker injecting MAC OS X Trojan in victim's system through downloads and prompt



MAC OS X Trojan: DNSChanger (Cont'd)

After the user downloads the false codec, the process of tricking and retrieving the user's information continues as follows:

- **DNS settings:** Local machine's DNS settings are changed to attacker's IP address
- **Playing a video:** After the fake codec is installed, a video is played so as not to raise suspicions
- **HTTP message:** A notification is sent to the attacker about the victim's machine using an HTTP post message
- **Complete control:** Hackers take complete control of the victim's MAC OS X computer



Mac OS X Trojan: Hell Raiser

Hell Raiser is **malware** that gets onto the victim's system when clicked on, the user it is an innocent file. Once access has been gained to the victim's system, the attacker can send pictures, pop-up chat messages, can **transfer files** to and from the victim's computer, and even can turn ON and turn OFF the system from a remote location. Finally, victim operations can be completely monitored.

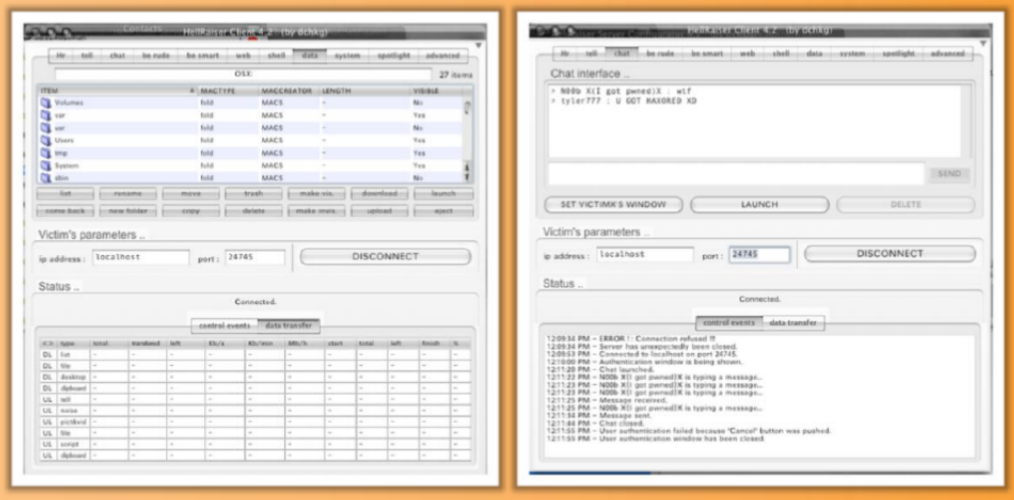
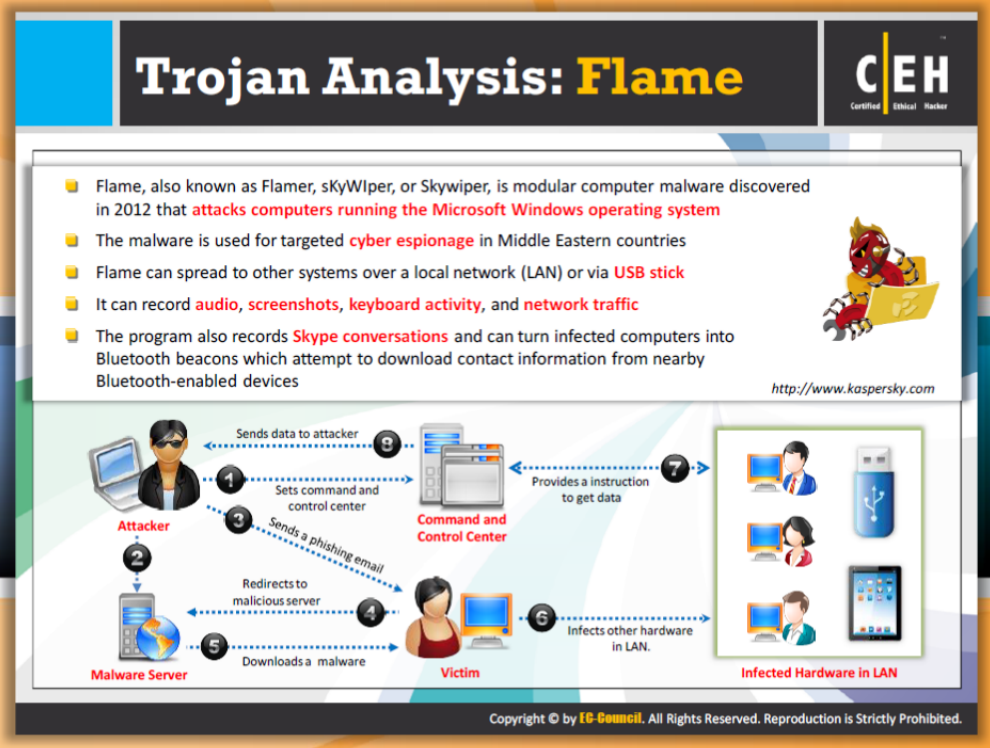


FIGURE 6.38: Hell Raiser Screenshots



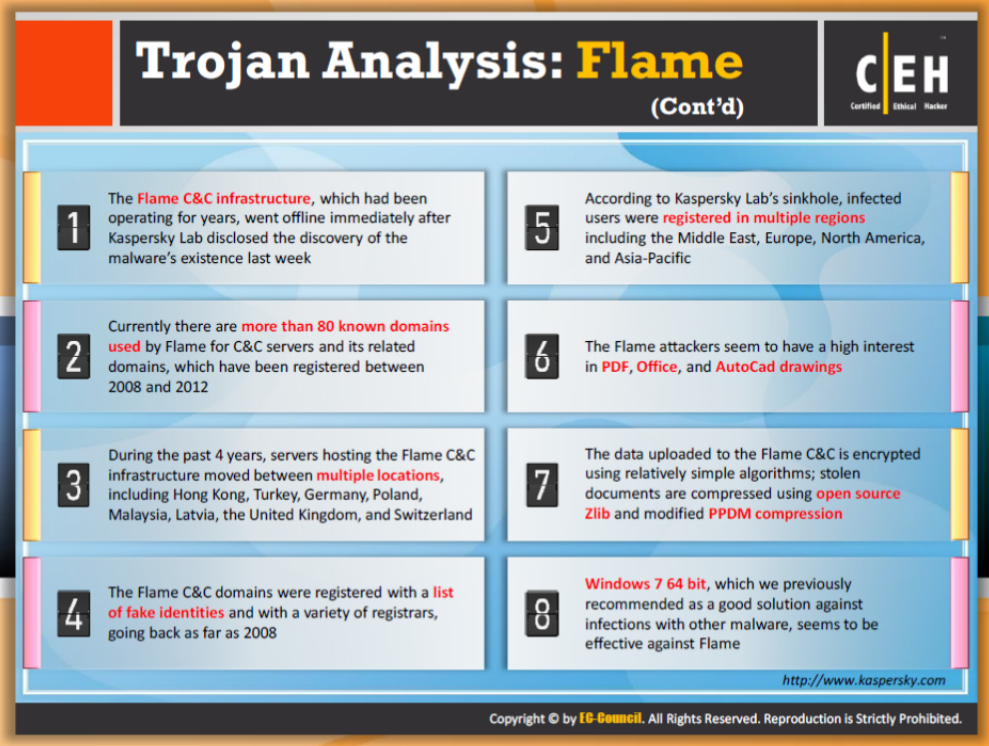
Trojan Analysis: Flame

Source: http://www.kaspersky.com

Flame, also known as Flamer, sKyWIper or Skywiper, is modular computer malware that attacks computers running the **Microsoft Windows** operating system. This malware is used for targeted cyber espionage. 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. It 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.

In order to inject a Trojan onto the victim's system and to gain sensitive information, attackers first set a command and control center and a malware server. Next, the attacker sends a

phishing email to the victim's system and lures him or her to open the link. Once the attacker opens the link, he or she is redirected to the malicious server. As a result, the malware gets downloaded onto the victim's system and the system is infected. This infected machine infects the other hardware connected on the LAN. Thus, the commands from the control and command center are sent to and received from the infected hardware LAN. According to the received commands, the infected hardware LANs send the data to the control and command center.



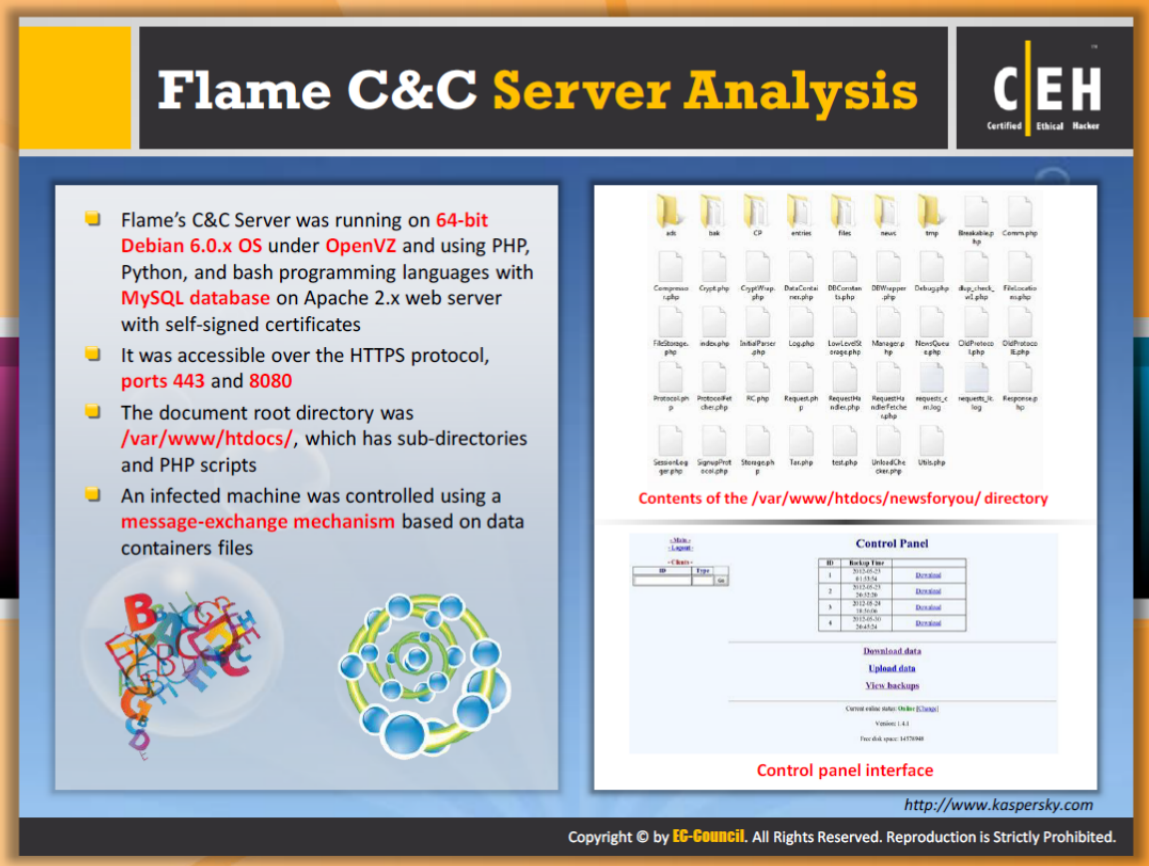
Trojan Analysis: Flame (Cont'd)

Source: http://www.kaspersky.com

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 recently.
- 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.
- The data uploaded to the Flame C&C is encrypted using relatively simple algorithms. Stolen documents are compressed using open source Zlib and modified PPDM compression.

Windows 7 64 bit, which we previously recommended as a good solution against infections with other malware, seems to be effective against Flame.



Flame C&C Server Analysis

Source: http://www.kaspersky.com

Flame's C&C Server was running on **64-bit Debian 6.0.x OS** under OpenVZ and using PHP, Python, and bash programming languages with MySQL database on Apache 2.x web server with self-signed certificates. This server configuration was a typical LAMP (Linux, Apache, MySQL, PHP) setup. It was used 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 sub-directories and PHP scripts. While the systems had PHP5 installed, the code was made to 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 developers 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.

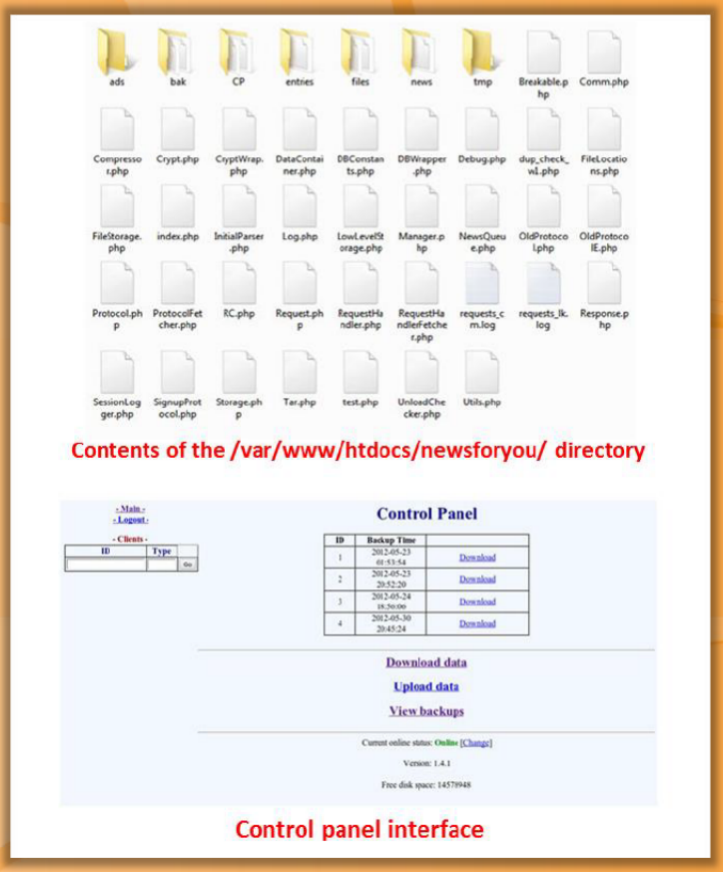
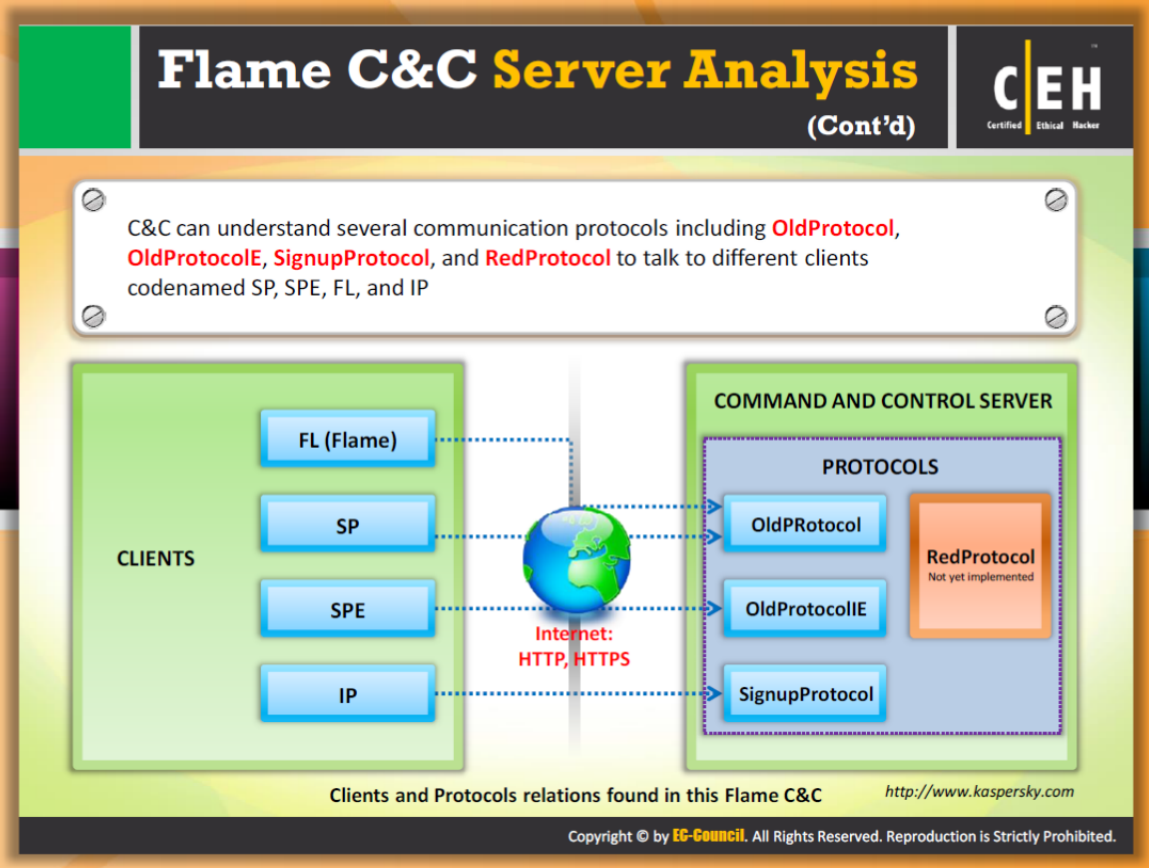


FIGURE 6.39: Flame C&C Server Screenshot



Flame C&C Server Analysis (Cont'd)

Source: http://www.kaspersky.com

C&C can understand several communication protocols including OldProtocol, OldProtocolE, SignupProtocol, and RedProtocol to talk to different clients 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 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 file data is encrypted using the Blowfish algorithm in CBC mode (with static IV). The Blowfish key is generated randomly for each file. After file encryption, the Blowfish key is encrypted with a public key using asymmetric encryption algorithm from the openssl_public_encrypt PHP function.

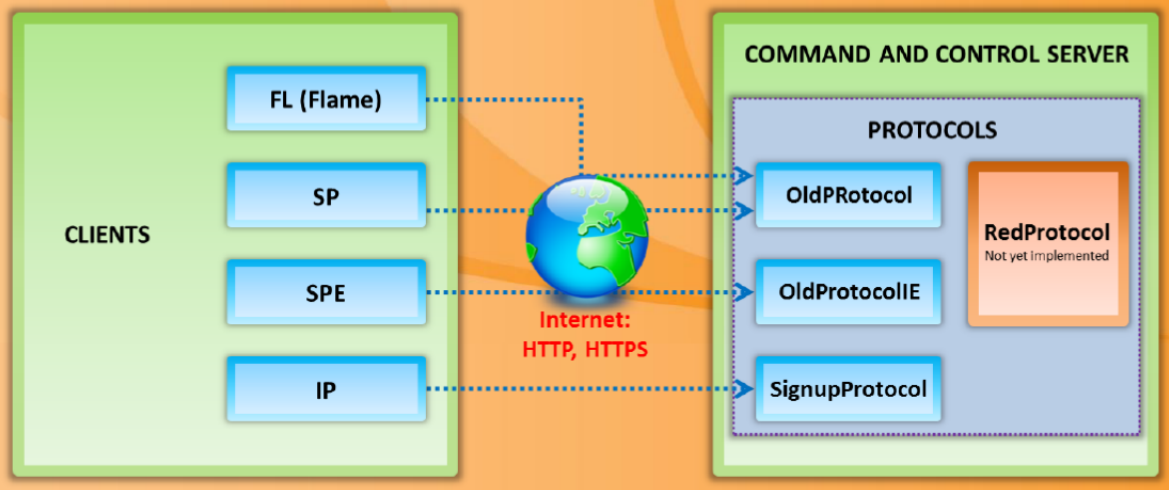
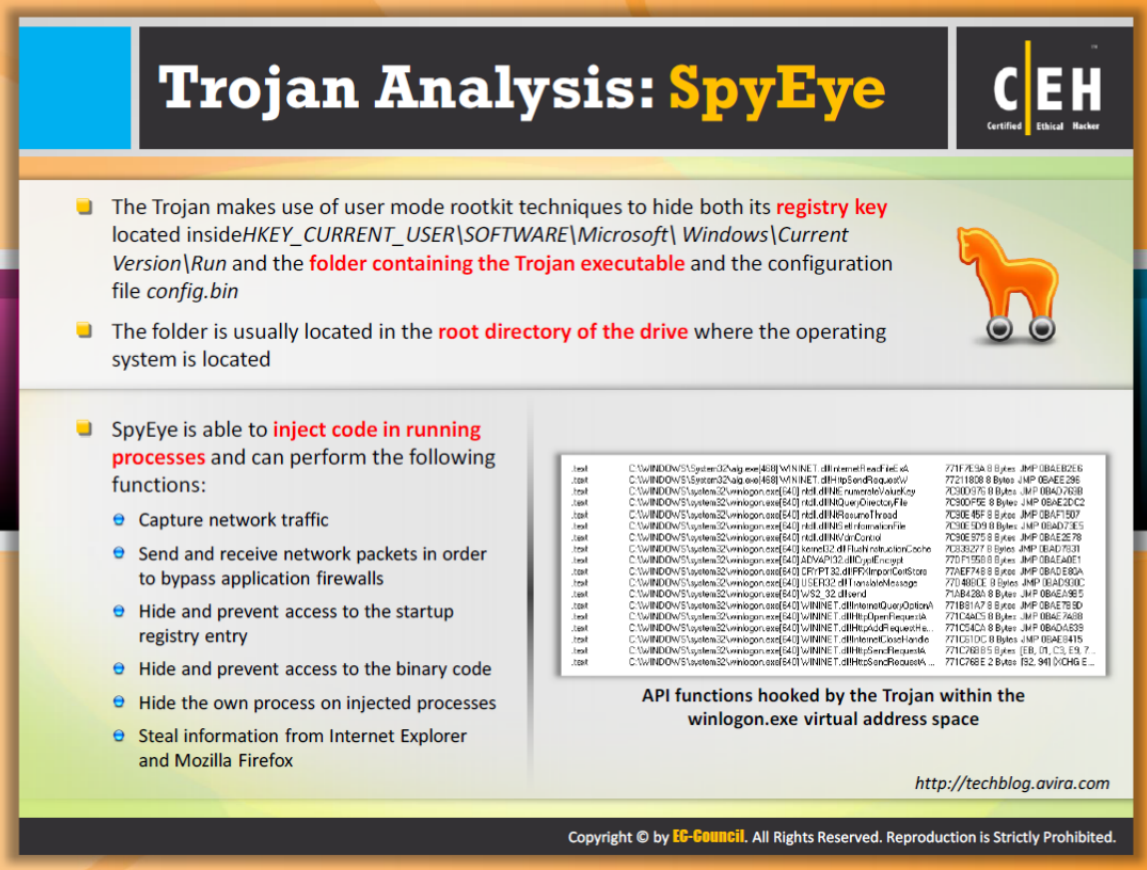


FIGURE 6.39: Clients and protocol relations found in this Flame C&C



Trojan Analysis: SpyEye

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.

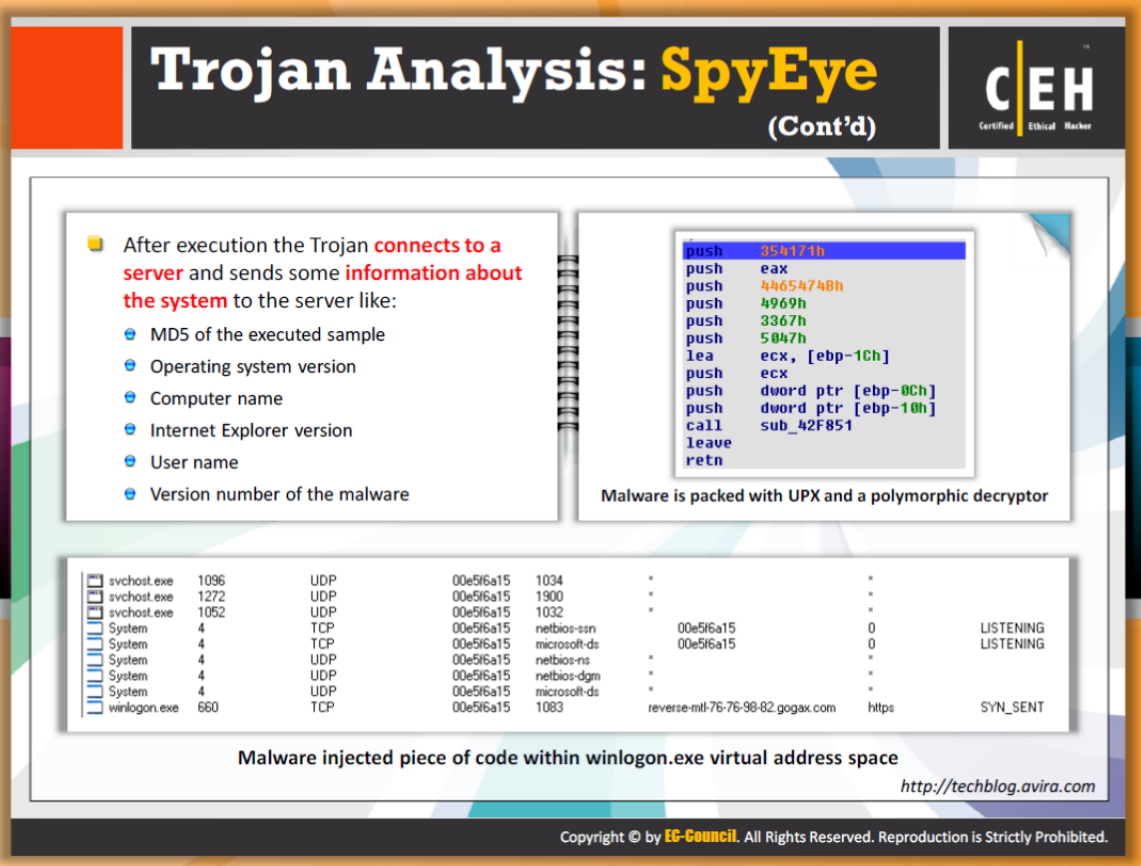
SpyEye is able to inject code in running processes and can perform the following functions:

- 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:

.text	C:\WINDOWS\System32\alg.exe[468] WININET.dll!InternetReadFileExA	771F7E9A	8 Bytes JMP 0BAEB2E6
.text	C:\WINDOWS\System32\alg.exe[468] WININET.dll!HttpSendRequestW	77211808	8 Bytes JMP 0BAEE296
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtEnumerateValueKey	7C90D976	8 Bytes JMP 0BAD769B
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtQueryDirectoryFile	7C90DF5E	8 Bytes JMP 0BAE2DC2
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtResumeThread	7C90E45F	8 Bytes JMP 0BAF1507
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtSetInformationFile	7C90E5D9	8 Bytes JMP 0BAD73E5
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtVdmControl	7C90E975	8 Bytes JMP 0BAE2E78
.text	C:\WINDOWS\system32\winlogon.exe[640] kernel32.dll!FlushInstructionCache	7C839277	8 Bytes JMP 0BAD7831
.text	C:\WINDOWS\system32\winlogon.exe[640] ADVAPI32.dll!CryptEncrypt	77DF1558	8 Bytes JMP 0BAEA0E1
.text	C:\WINDOWS\system32\winlogon.exe[640] CRYPT32.dll!PFXImportCertStore	77AEF748	8 Bytes JMP 0BADE80A
.text	C:\WINDOWS\system32\winlogon.exe[640] USER32.dll!TranslateMessage	77D48BCE	8 Bytes JMP 0BAD930C
.text	C:\WINDOWS\system32\winlogon.exe[640] WS2_32.dll!send	71AB428A	8 Bytes JMP 0BAEA9B5
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryOptionA	771B81A7	8 Bytes JMP 0BAE7B9D
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpOpenRequestA	771C4AC5	8 Bytes JMP 0BAE7A88
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpAddRequestHe...	771C54CA	8 Bytes JMP 0BADA639
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetCloseHandle	771C61DC	8 Bytes JMP 0BAE8415
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA	771C76B8	5 Bytes [EB, 01, C3, E9, 7...
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA ...	771C76BE	2 Bytes [92, 94] (XCHG E...

FIGURE 6.40: API functions hooked by the Trojan within the winlogon.exe virtual address space



Trojan Analysis: SpyEye (Cont'd)

Source: http://techblog.avira.com

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

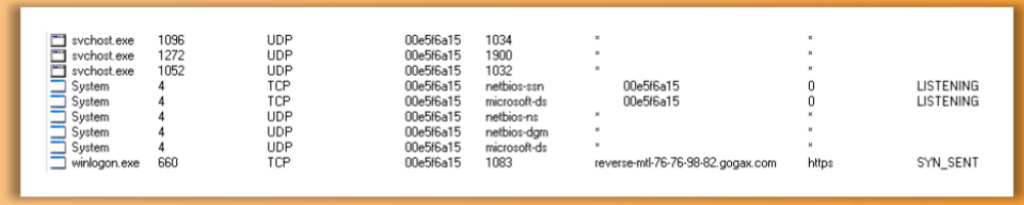


FIGURE 6.41: Malware injected piece of code within winlogon.exe virtual address space

Malware is packed with **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    354171h
push    eax
push    4465474Bh
push    4969h
push    3367h
push    5047h
lea     ecx, [ebp-1Ch]
push    ecx
push    dword ptr [ebp-0Ch]
push    dword ptr [ebp-10h]
call    sub_42F851
leave
retn
```

FIGURE 6.42: Malware is packed with UPX and a polymorphic decryptor

Trojan Analysis: ZeroAccess

Source: http://www.symantec.com

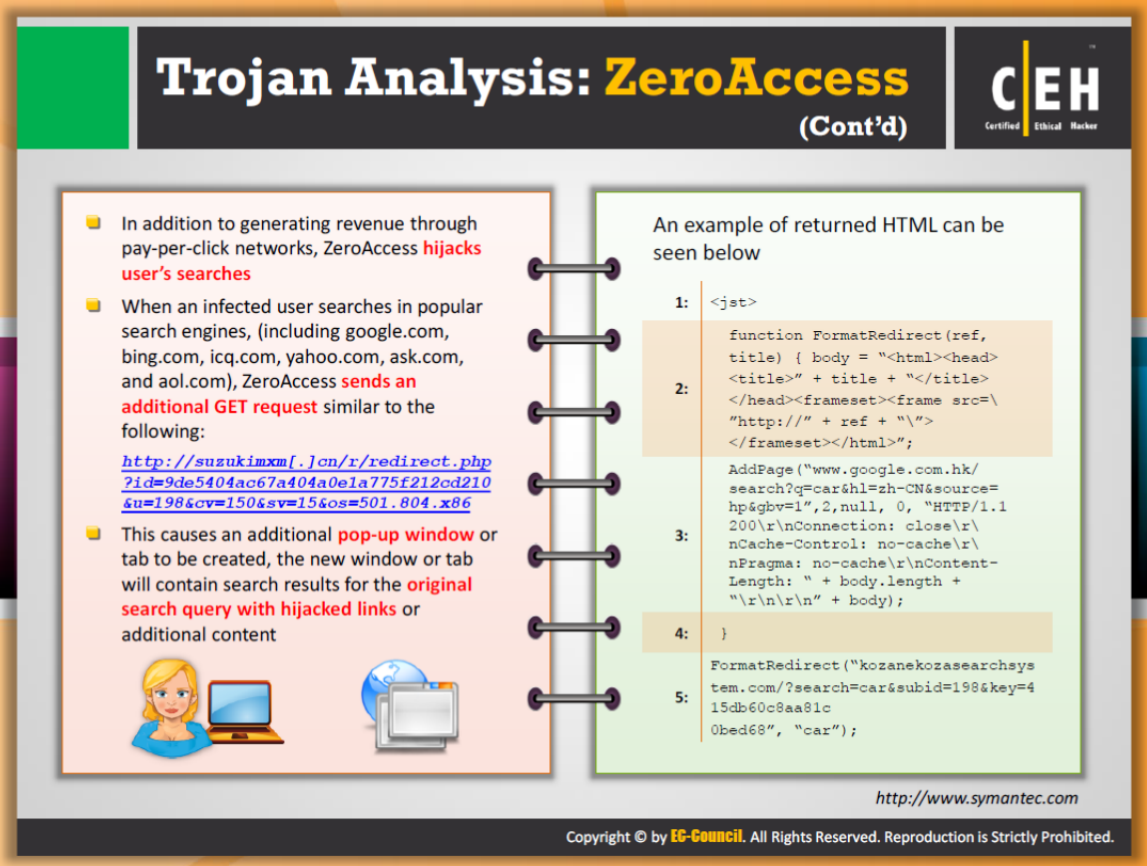
ZeroAccess, also known as "**Smiscer**" or "**Max++ rootkit**," is a malicious Windows threat used to generate revenue primarily through **pay-per-click fraud**. ZeroAccess uses **low-level rootkit** functionality to remain persistent and stealth. It arrives through various vectors, including web exploit kits and social engineering attacks. Although ZeroAccess contains generic backdoor functionality that could be used for multiple purposes, 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 has been observed to utilize 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 6.43: Example advertisement for the ClickIce pay-per-click network



Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

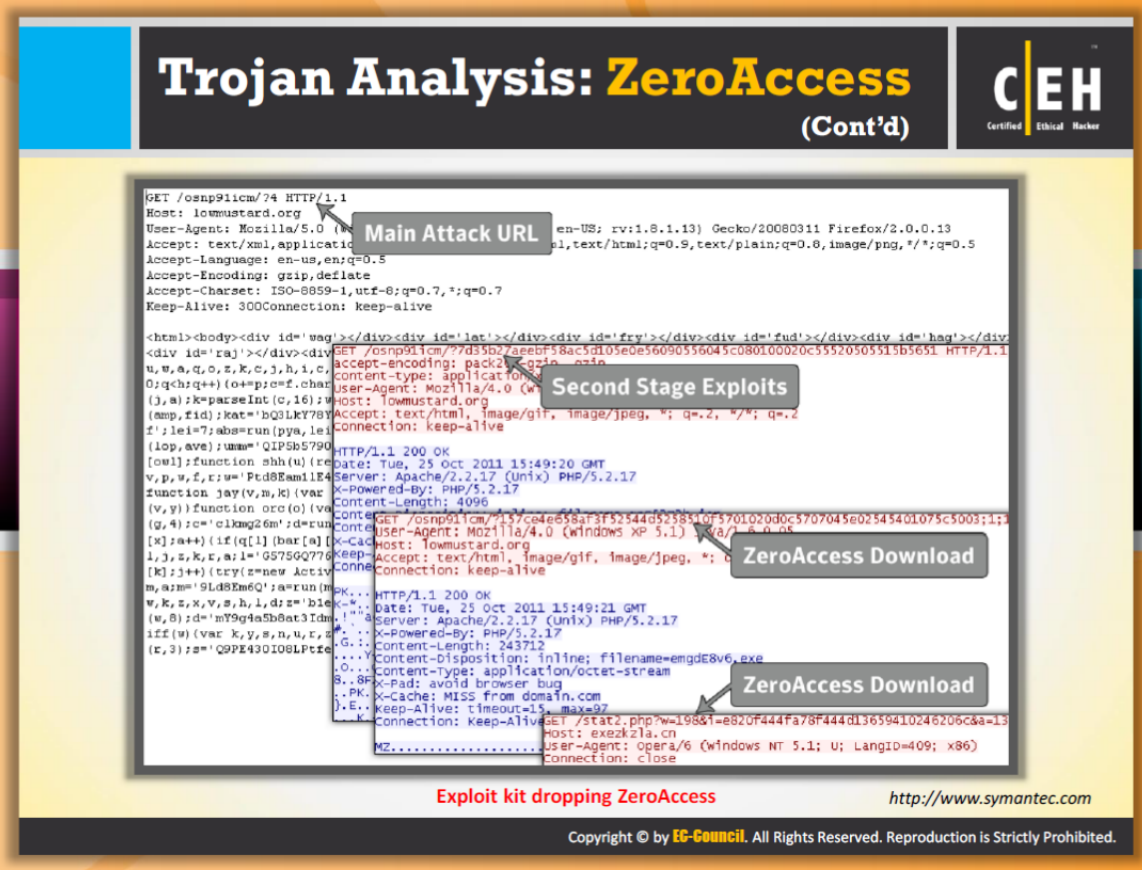
In addition to generating revenue through **pay-per-click** networks, **ZeroAccess hijacks** users' searches. When an infected user searches in popular search engines (including google.com, bing.com, icq.com, yahoo.com, ask.com, and aol.com), ZeroAccess sends an additional GET request similar to the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

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

This causes an additional pop-up window or tab to be created. The new window or tab will contain search results for the original search query with hijacked links or additional content. An example of returned HTML can be seen as follows.

```
1: <jst>
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("kozanekozasearchsys
   tem.com/?search=car&subid=198&key=4
   15db60c8aa81c
   0bed68", "car");
```

FIGURE 6.44: An example of returned HTML

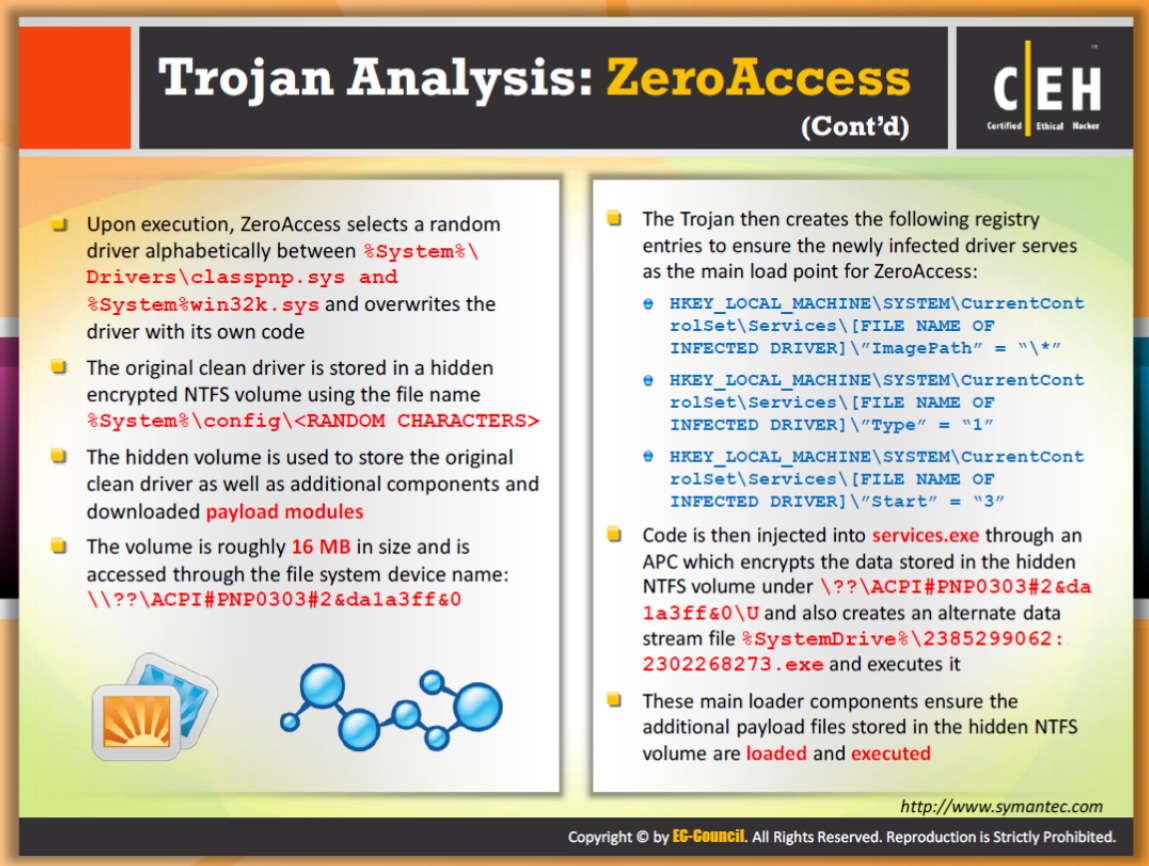


Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

ZeroAccess can also be installed through **web exploit kits**. The user is often falsely given the impression 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 6.45: Exploit kit dropping ZeroAccess



Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

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 hidden volume is used 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 accessed 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].
```

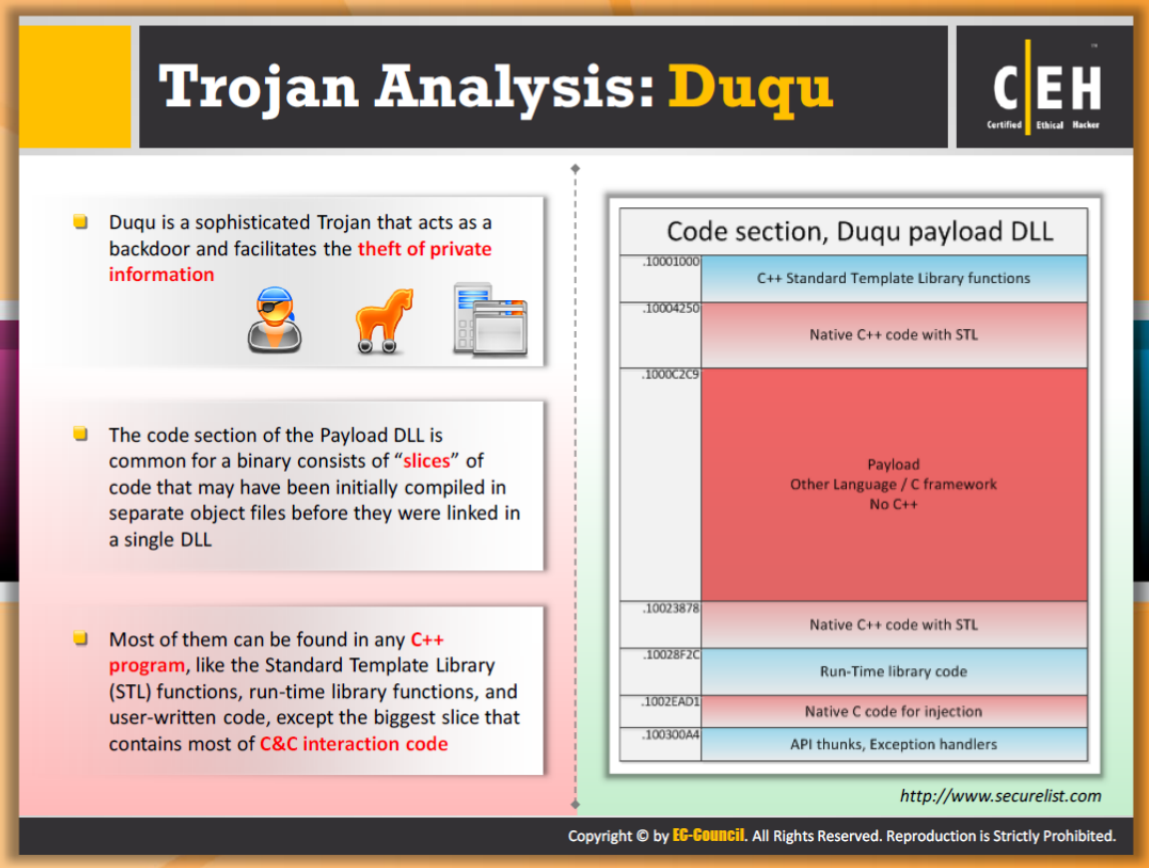
This file system of the hidden volume is encrypted using RC4 with the following 128-bit key:

```
\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"`

Code is then injected 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.



Trojan Analysis: Duqu

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 the biggest slice that contains most of C&C interaction code.

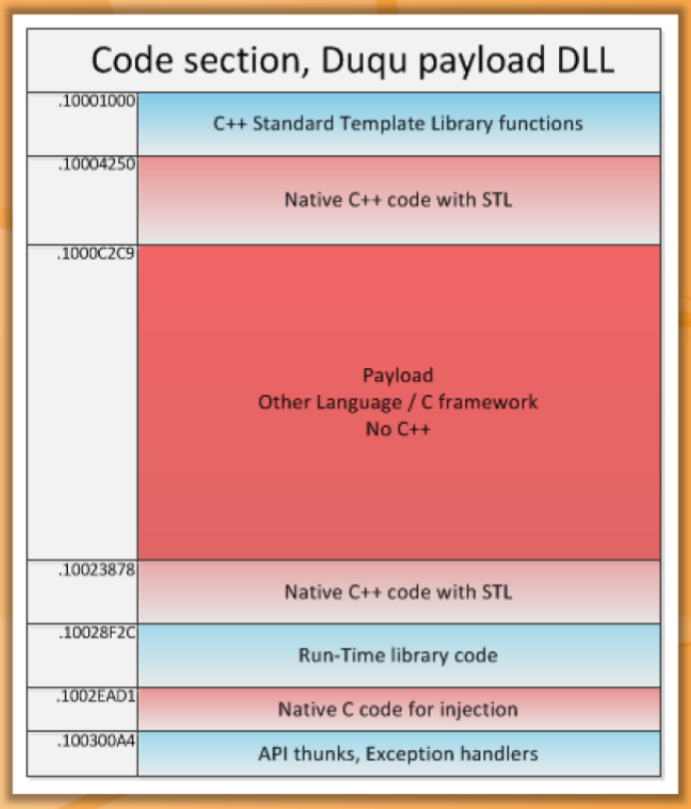
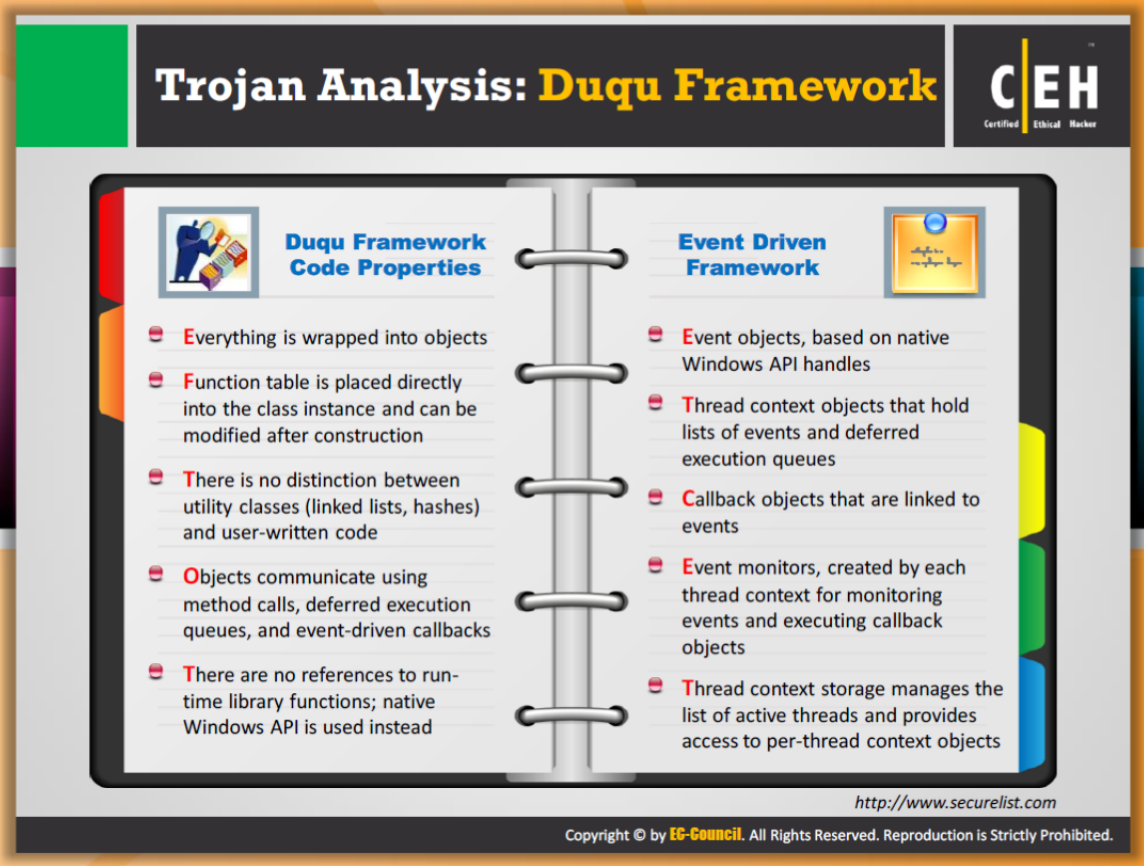


FIGURE 6.46: Duqu Tool Screenshot



Trojan Analysis: Duqu Framework

Source: http://www.securelist.com

This slice is different from others, because it was not compiled from **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
- 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

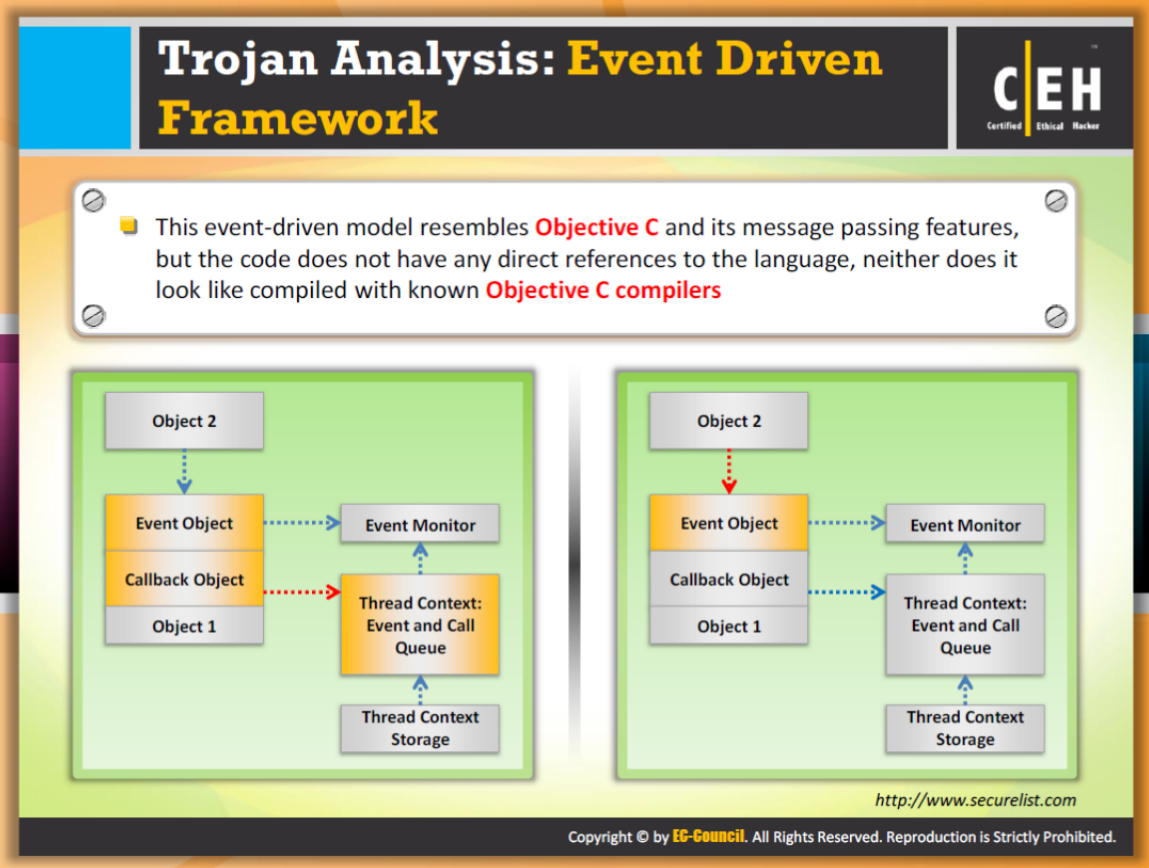
- There are no references to **run-time library functions**; native Windows API is used instead

Event-Driven Framework

The layout and implementation of objects in the Duqu Framework is definitely not native to C++ that was used to program the rest of the Trojan. There is an even more interesting feature of the framework that is used extensively throughout the whole code: 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 that are 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



Trojan Analysis: Event Driven Framework

Source: http://www.securelist.com

The event-driven model resembles **Objective C** and its message passing features, but the code does not have any direct references to the language, neither does it look like it is compiled with known objective **C compilers**.

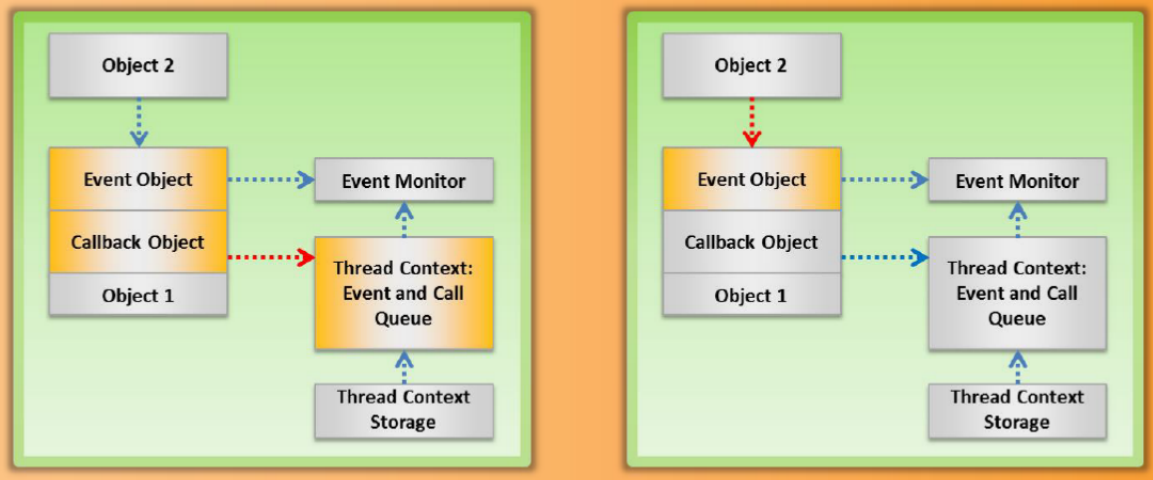
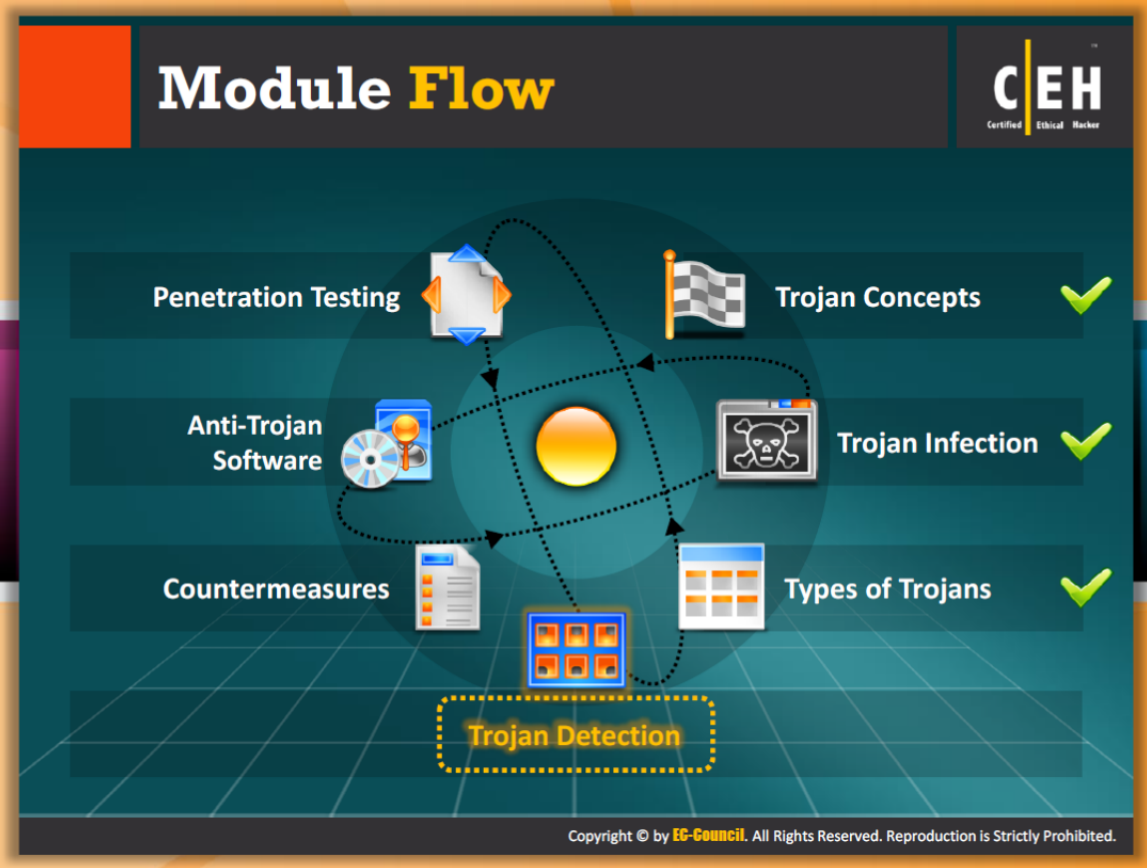


FIGURE 6.47: Event Driven Framework

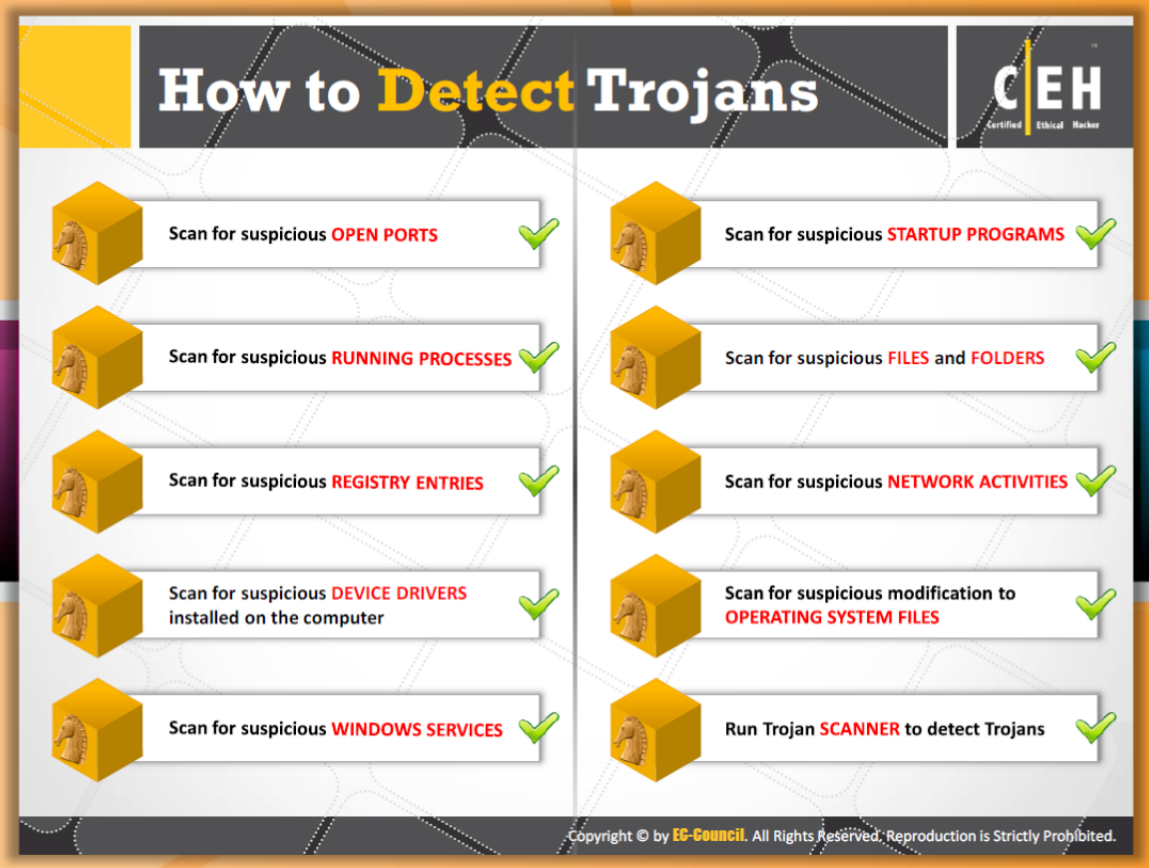


Module Flow

So far, we have discussed how a Trojan infects a system and the types of Trojans available. Now we will discuss how to conduct Trojan detection. Trojan detection helps in detecting the presence of Trojans on an infected system and thus helps you in protecting the system and its resources from further loss.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

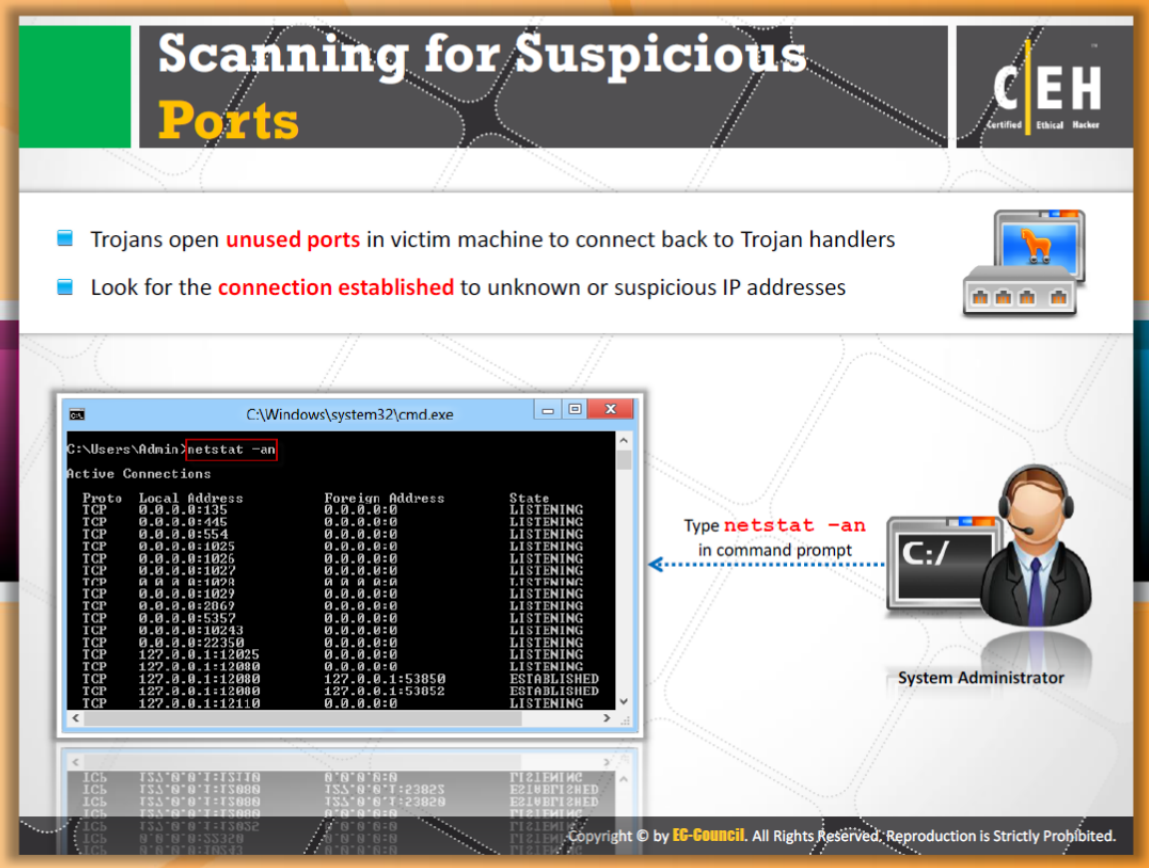
This section focuses on Trojan detection using various techniques or methods.



How to Detect Trojans

Trojans are **malicious programs** that masquerade as a useful or legitimate file but their actual purpose is to take complete control over your computer, thereby accessing your files and **confidential information**. In order to avoid such **unauthorized access** and to protect your files and personal information, an antivirus product has to be used, which automatically scans and detects the presence of Trojans on your system or you can also detect the Trojans installed on your system manually. The following are the steps for detecting Trojans:

1. Scan for suspicious OPEN PORTS
2. Scan for suspicious RUNNING PROCESSES
3. Scan for suspicious REGISTRY ENTRIES
4. Scan for suspicious DEVICE DRIVERS installed on the computer
5. Scan for suspicious WINDOWS SERVICES
6. Scan for suspicious STARTUP PROGRAMS
7. Scan for suspicious FILES and FOLDERS
8. Scan for suspicious NETWORK ACTIVITIES
9. Scan for suspicious modification to OPERATING SYSTEM FILES
10. Run Trojan SCANNER to detect Trojans



Scanning for Suspicious Ports

Trojans open **unused ports** on the victim's machine to connect back to the Trojan handlers. These Trojans can be identified by scanning for suspicious ports. Scan for suspicious ports and look for the connection established to unknown or suspicious IP addresses.

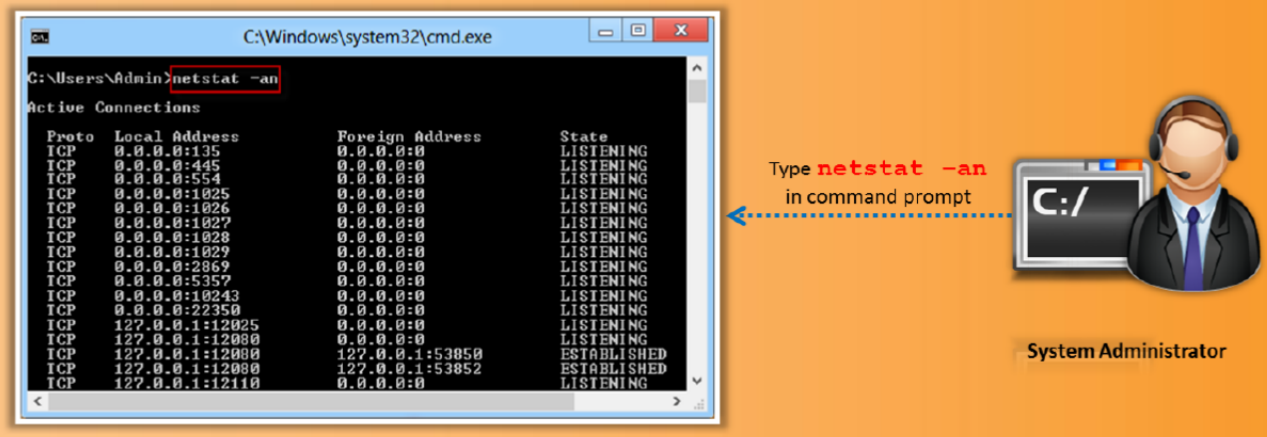
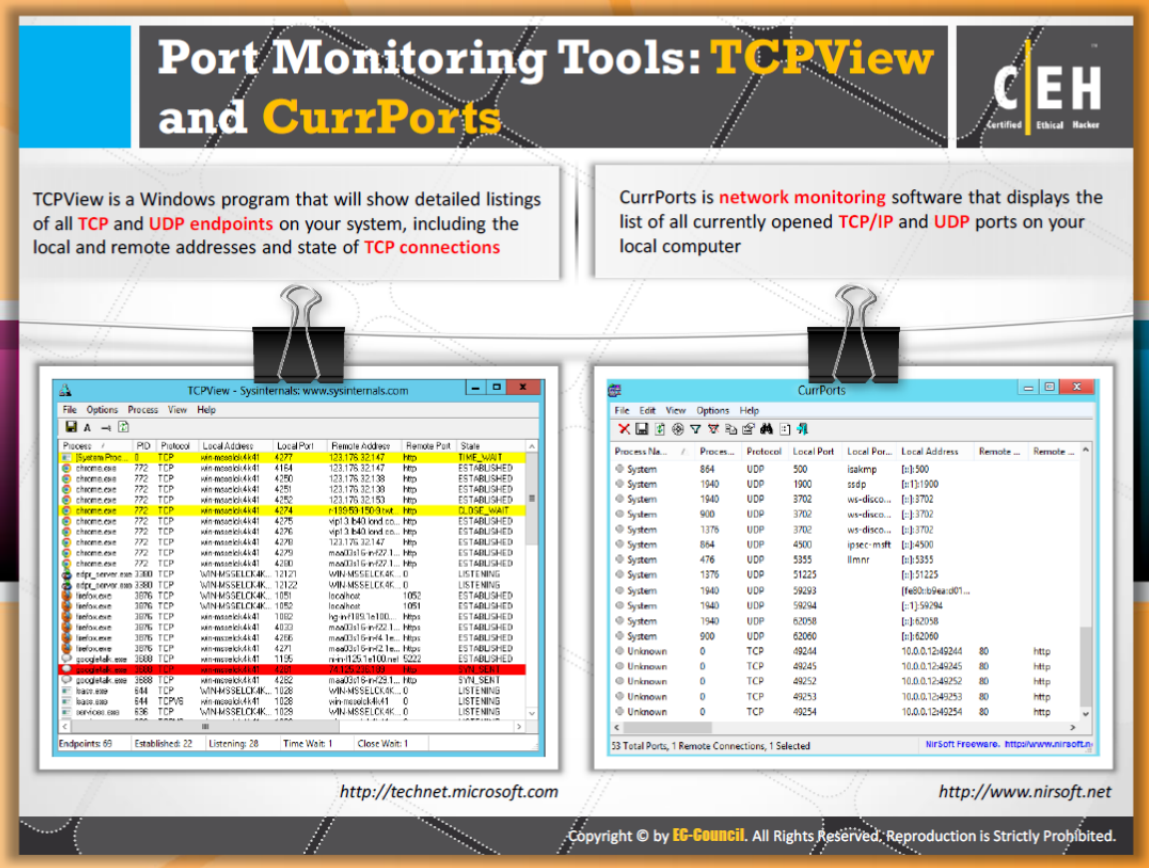


FIGURE 6.48: Scanning for Suspicious Ports



Port Monitoring Tools: TCPView and CurrPorts

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. On Windows NT, 2000, and XP, TCPView also reports the name of the process that owns the endpoint. It provides a more informative and conveniently presented subset of the Netstat program that is shipped with Windows. It works on **Windows NT/2000/XP** and Windows 98/ME.

When **TCPView runs**, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. On **Windows XP** systems, TCPView shows the name of the process that owns each endpoint. By default, TCPView is updated every second. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green. The user can close established TCP/IP connections (those labeled with a state of ESTABLISHED) and save TCPView's output window to a file as well.

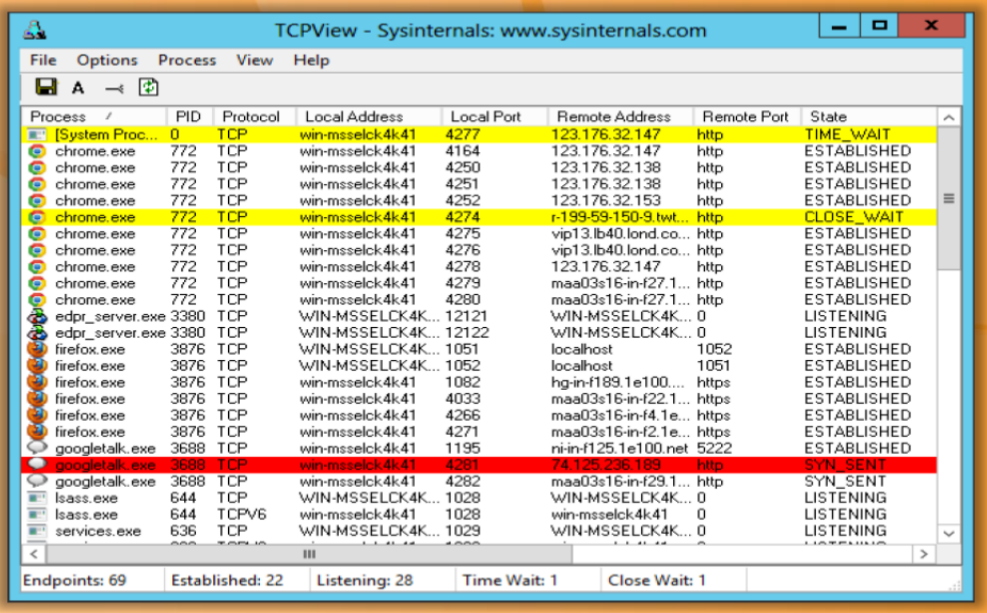


FIGURE 6.49: TCPView Tool Screenshot

CurrPorts Tool

Source: http://www.nirsoft.net

CurrPorts allows you to view a list of ports that are currently in use and the application that is using the ports. You can close a selected connection and also terminate the process using it, and export all or selected items to **an HTML or text report**. It displays the list of all currently opened **TCP/IP** and **UDP ports** on the system. 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 tab-delimited text file.

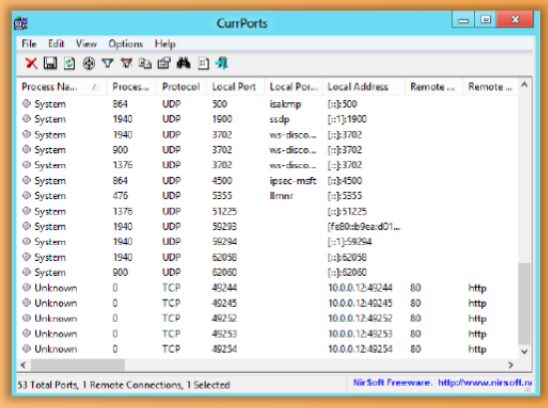
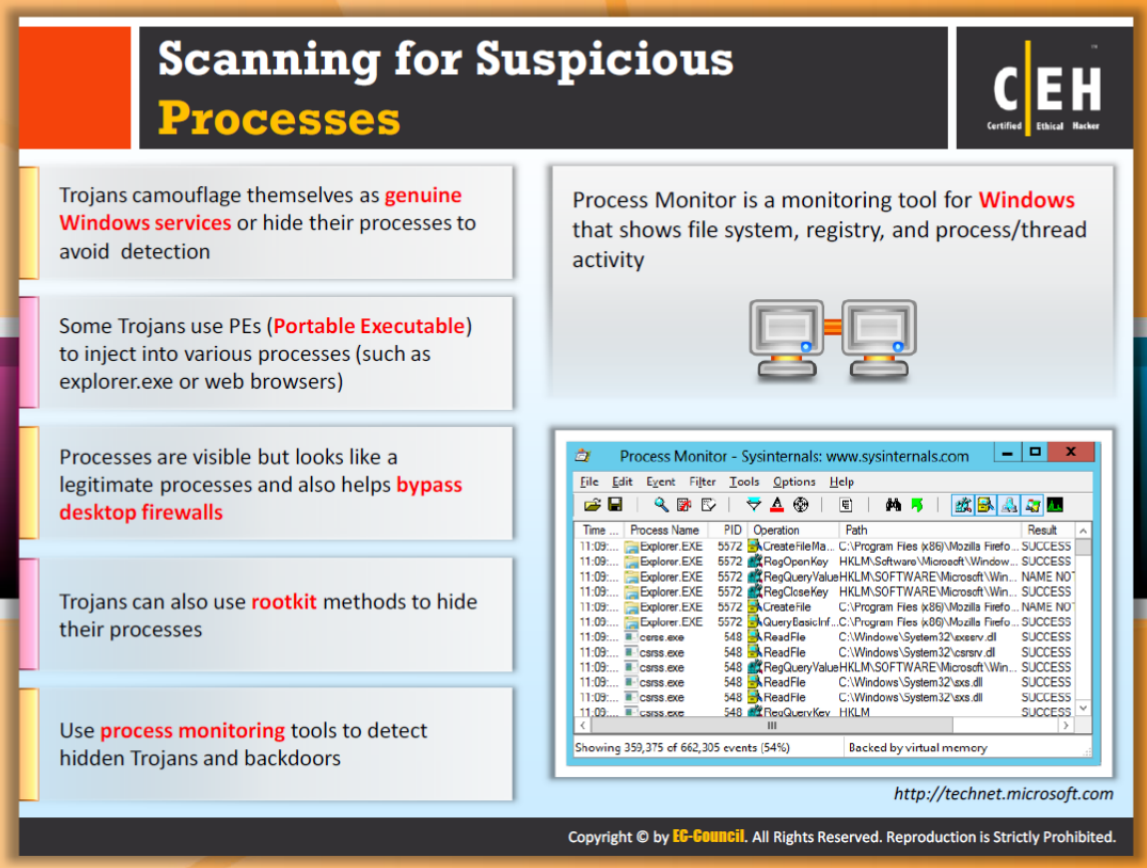


FIGURE 6.50: CurrPorts Tool Screenshot



Scanning for Suspicious Processes

There are various symptoms that can indicate that our system has been **infected**. The system suddenly becomes slow, downloading speed becomes slow, and the Internet's speed also comes down drastically.

Attackers use certain **rootkit methods** to make the Trojan hide in the system where it can't be normally detected by antivirus software. These **Trojans** and **worms** usually enter into the system through pictures, music files, videos, etc. that are downloaded into the system. Initially, everything seems to be good but slowly they show effect in various ways. By using process monitoring tools, we can easily **detect hidden Trojans**, worms, and backdoors. Hidden Trojans and other kinds of vulnerabilities or viruses can be detected by scanning for 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 is used to analyze the behavior of spyware and dubious programs. Its features include rich and **non-destructive filtering**, comprehensive event

properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, etc.

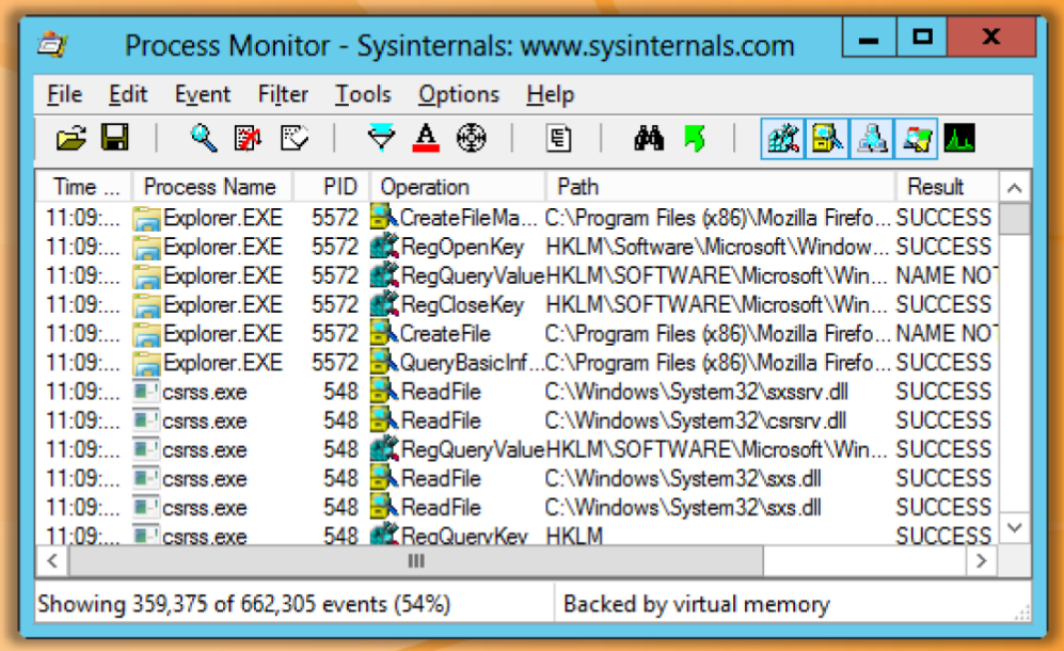
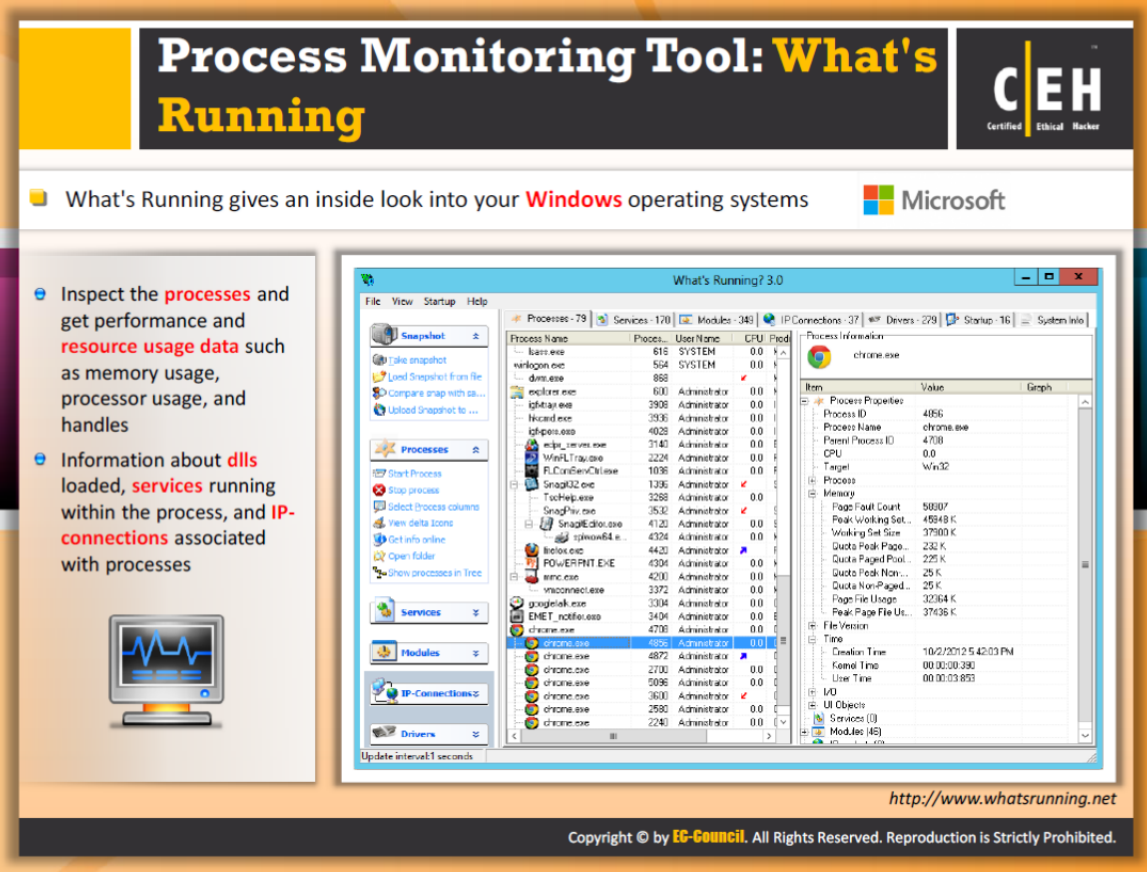


FIGURE 6.51: Process Monitor



Process Monitoring Tool: What's Running

Source: http://www.whatsrunning.net

What's Running gives you an inside look into your Windows system, such as **2000/XP/2003/Vista/Windows7**. It explores processes, services, modules, IP-connections, drivers, etc. through a simple-to-use application.

- **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 each process has
- **IP connections:** It gives all the active IP connections in your system
- **Services:** Inspects the services that are running and stopped
- **Modules:** Finds out the information about all dll:s and exe:s that are in use on your system

- **Drivers:** It finds out the information about all drivers, for running drivers you can inspect the file version for finding the supplier of the drive
- **System information:** It shows crucial system information about your system such as installed memory, processor, registered user, and operating system and its version

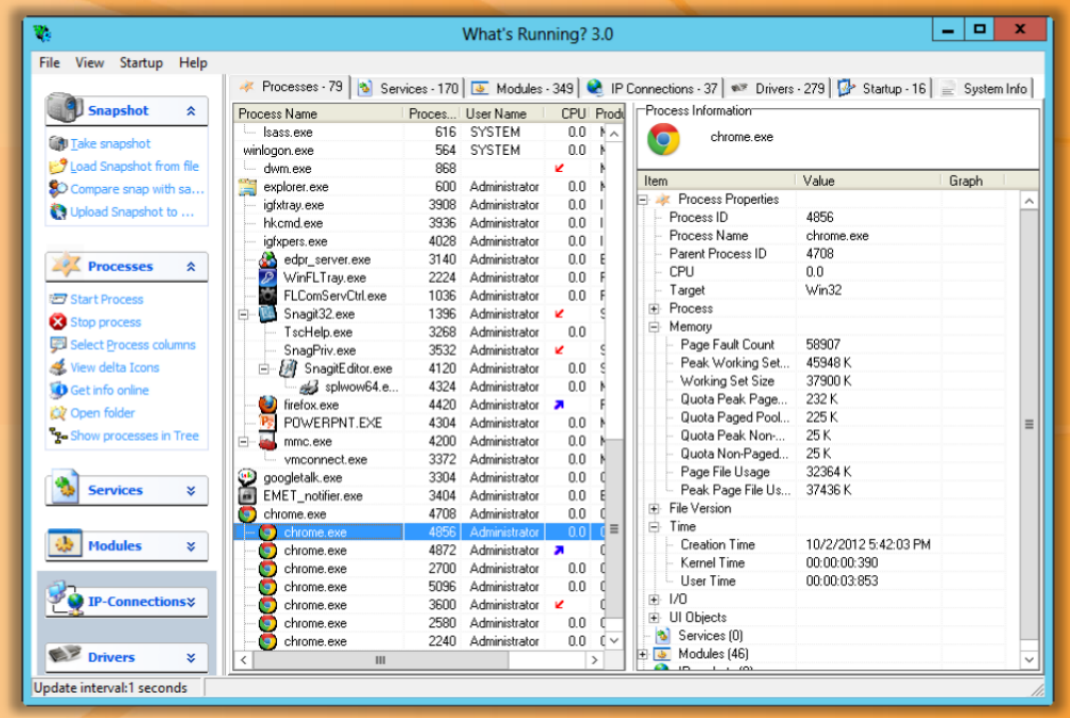
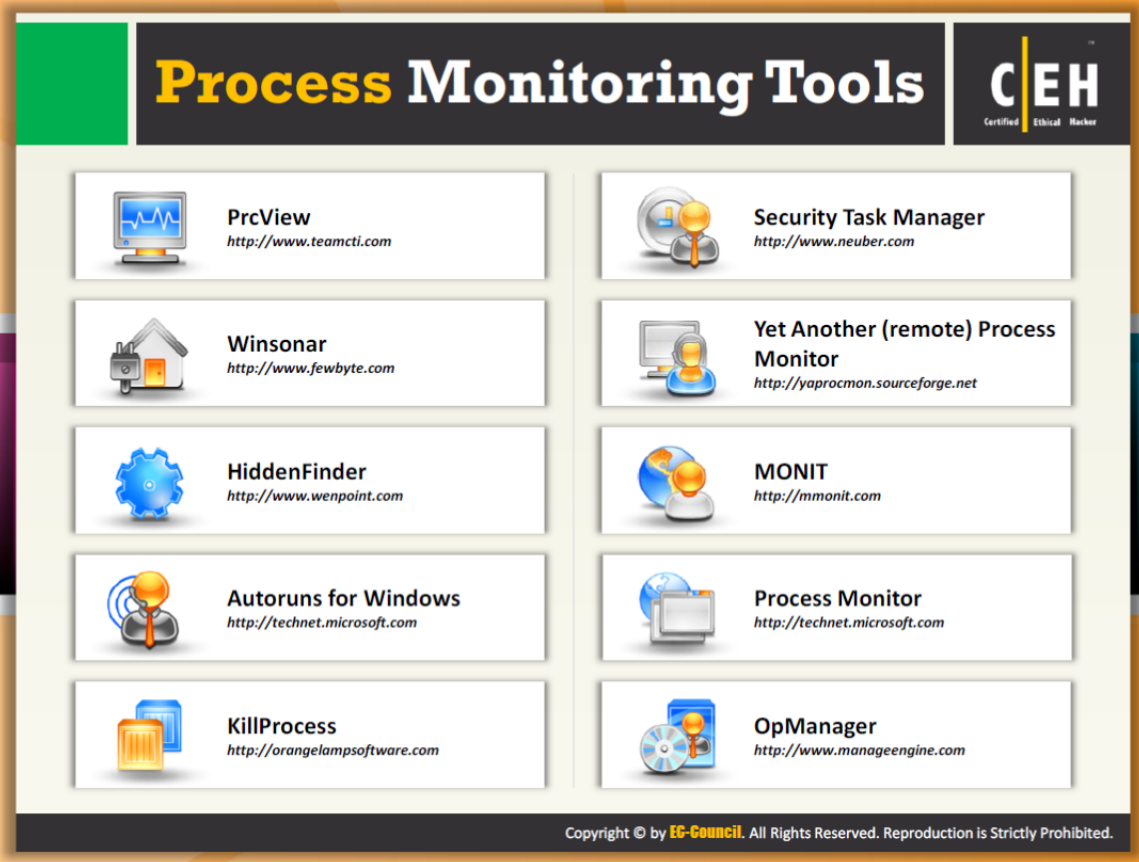


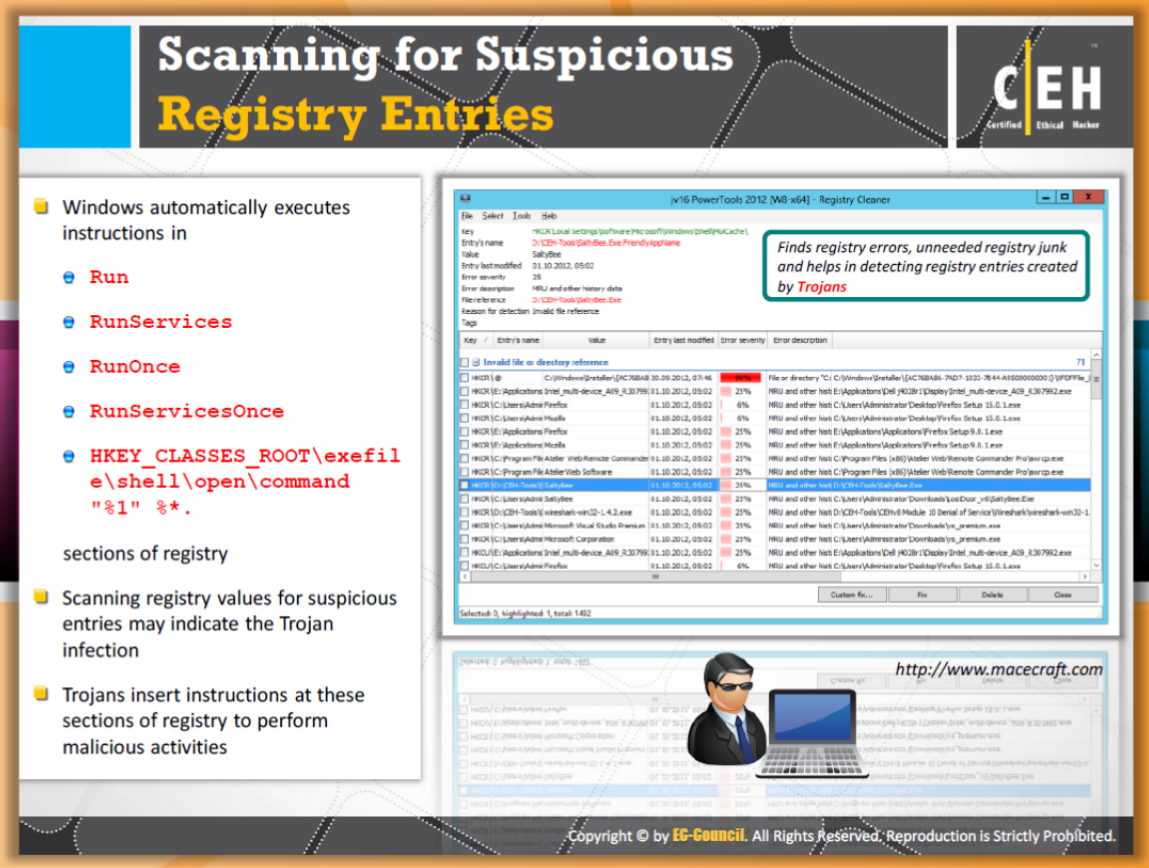
FIGURE 6.52: What's Running Tool Screenshot



Process Monitoring Tools

There are many process monitoring tools that you can use for the detection of **Trojans** installed on your system. These tools display a list of all the processes running or installed on your system. By analyzing the list you can identify the Trojans. These tools provide a comprehensive monitoring console for your **entire network** and **IT infrastructure**. They continuously and proactively monitor the entire IT system because of which any outages or performance degradations can be immediately **identified and notified**. In addition, it kills all the software that threatenss your computer, even if it is hidden. A few process monitoring tools are listed as follows:

- PrcView available at http://www.teamcti.com
- Winsonar available at http://www.fewbyte.com
- HiddenFinder available at http://www.wenpoint.com
- Autoruns for Windows available at http://technet.microsoft.com
- KillProcess available at http://orangelampsoftware.com
- Security Task Manager available at http://www.neuber.com
- Yet Another (remote) Process Monitor available at http://yaprocmon.sourceforge.net
- MONIT available at http://mmonit.com
- Process Monitor available at http://technet.microsoft.com
- OpManager available at http://www.manageengine.com



Scanning for Suspicious Registry Entries

When a Trojan gets installed on the victim's machine, it generates a **registry entry**. We can notice various changes; the first symptom is the **system gets slower**. Various advertisements keep popping up. So, **scanning suspicious registries** will help in detecting Trojans. Windows automatically executes instructions in the following sections of the registry:

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

Scanning registry values for suspicious entries may indicate a Trojan infection. Trojans insert instructions at these sections of the registry to perform malicious activities.

jv16 PowerTools 2012 –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.

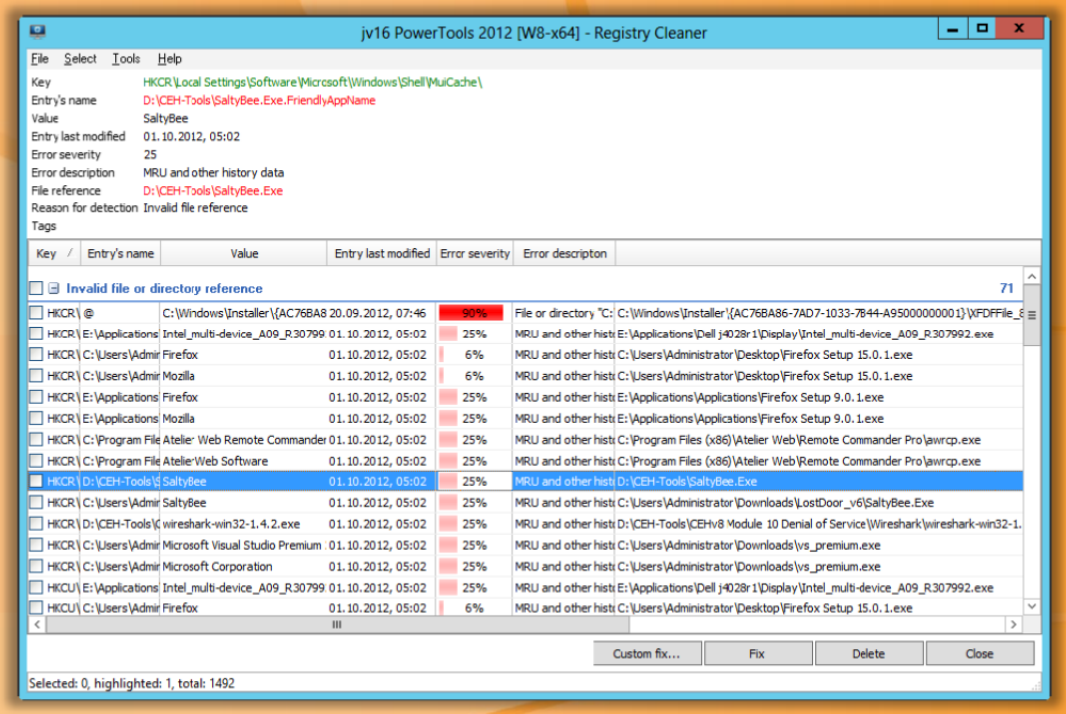


FIGURE 6.53: jv16 PowerTools 2012 –Registry Cleaner

Registry Entry Monitoring Tool: PC Tools Registry Mechanic

Source: http://www.pctools.com

PC Tools Registry Mechanic is an **advanced registry cleaner** that scans the registry values for suspicious entries created by **Trojan infections**. It fixes the Windows error and improves your system speed and **maximizes software performance**. It cleans up your system and secures your personal privacy. It keeps all your Internet and PC activities private and erases sensitive information permanently.

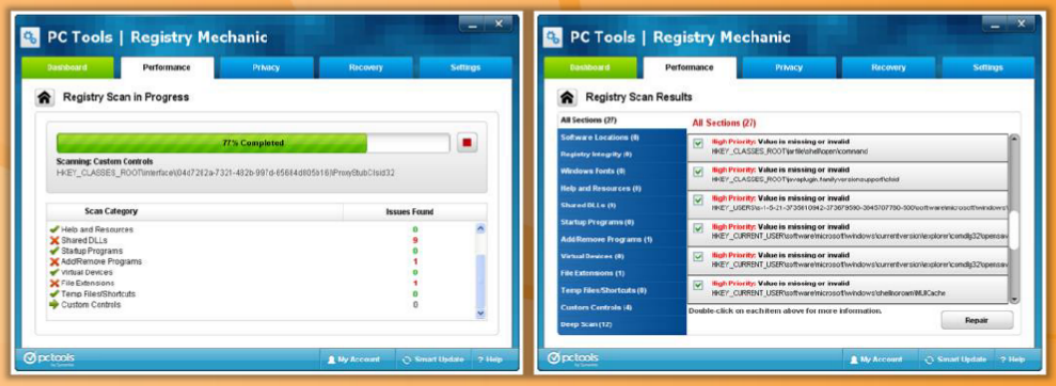
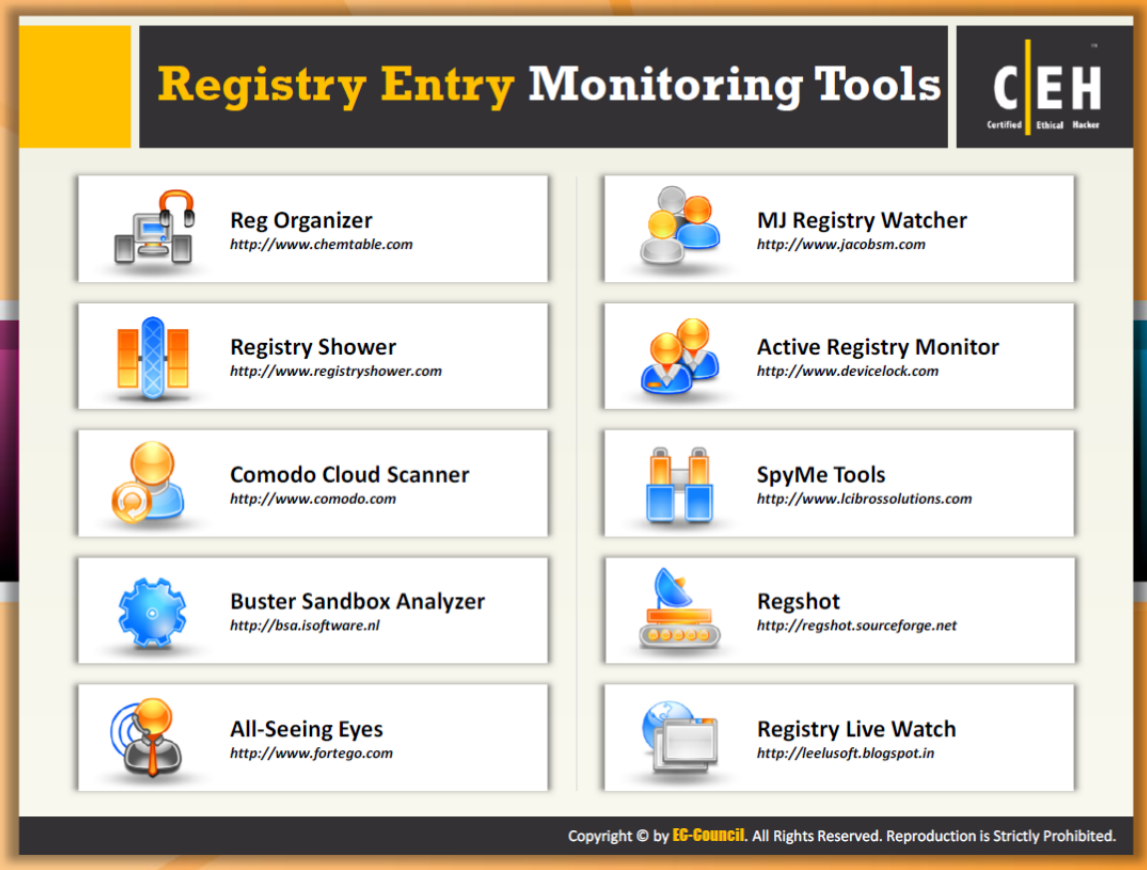


FIGURE 6.54: PC Tools Registry Mechanic Tool Screenshot



Registry Entry Monitoring Tools

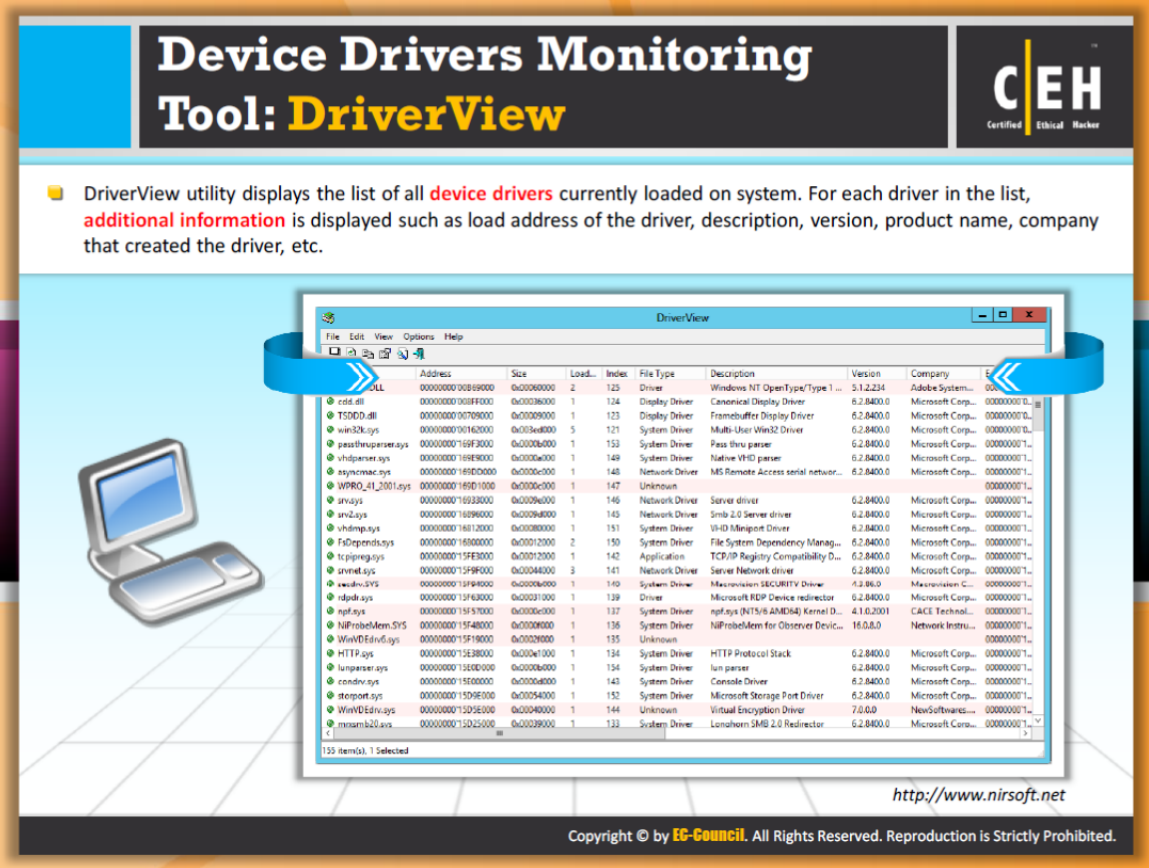
In addition to **jv16 PowerTools 2012** – Registry Cleaner and PC Tools Registry Mechanic, there are many other tools that allow you to monitor registry entries and thus help detect Trojans installed, if any. A few of the registry entry monitoring tools that are mainly used for the purpose of cleaning the registry are listed as follows:

- Reg Organizer available at http://www.chemtable.com
- Registry Shower available at http://www.registryshower.com
- Comodo Cloud Scanner available at http://www.comodo.com
- Buster Sandbox Analyzer available at http://bsa.isoftware.nl
- All-Seeing Eyes available at http://www.fortego.com
- MJ Registry Watcher available at http://www.jacobsm.com
- Active Registry Monitor available at http://www.devicelock.com
- SpyMe Tools available at http://www.lcibrossolutions.com
- Regshot available at http://regshot.sourceforge.net
- Registry Live Watch available at http://leelusoft.blogspot.in

Scanning for Suspicious Device Drivers

When device drivers are downloaded from various sources that are **not trustworthy** Trojans may also get installed on the system. Trojans use these **devices as covers** to hide but by using device driver monitoring tools, we can identify if there is any Trojan present. Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection. Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.

FIGURE 6.55: Scanning for Suspicious Device Drivers



Device Drivers Monitoring Tool: DriverView

Source: http://www.nirsoft.net

The DriverView utility displays the entire currently loaded **device drivers** list in your system. Additional information is displayed for each and every driver in the list such as load address of the driver, description, version, product name, company that created the driver, etc. Instead of browsing for **system components** separately in **Control Panel**, just by running this application on your system you can easily know all the drivers on your system. This application displays the list of drivers that are on your system quickly and easily. It can create **HTML reports**.

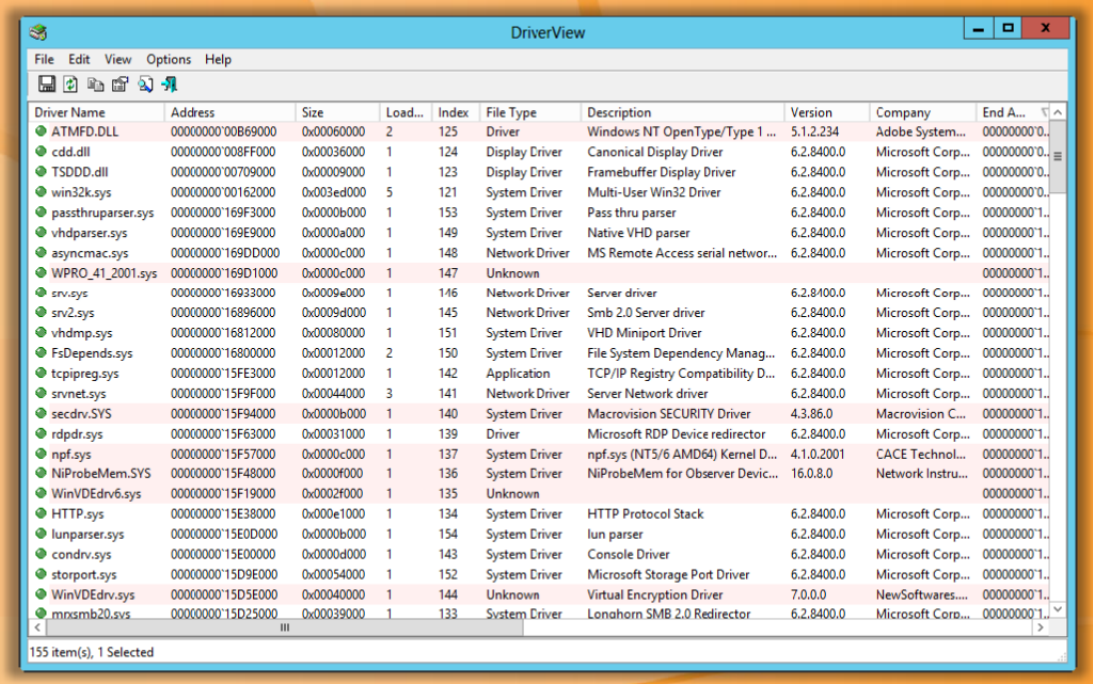
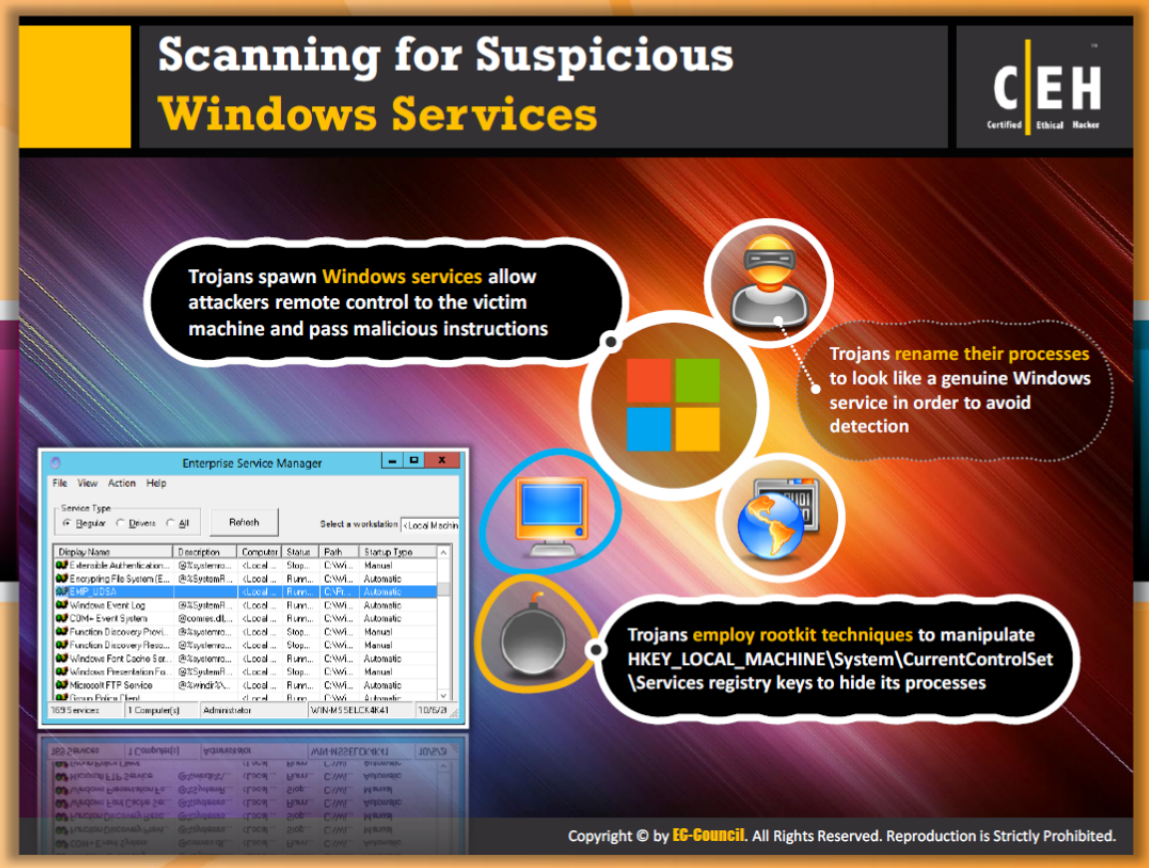


FIGURE 6.56: DriverView Screenshot

Device Drivers Monitoring Tools

A few of the device driver monitoring tools that help in detecting Trojans are listed as follows:

- Driver Detective available at http://www.drivershq.com
- Unknown Device Identifier available at http://www.zhangduo.com
- DriverGuide Toolkit available at http://www.driverguidetoolkit.com
- DriverMax available at http://www.innovative-sol.com
- Driver Magician available at http://www.drivermagician.com
- Driver Reviver available at http://www.reviversoft.com
- DriverScanner available at http://www.uniblue.com
- Double Driver available at http://www.boozet.org
- My Drivers available at http://www.zhangduo.com
- DriverEasy available at http://www.drivereasy.com



Scanning for Suspicious Windows Services

Once the Trojans are installed on **Windows services**, it becomes easy for an attacker to operate the system from a remote location. Trojans also create their processes to look like genuine Windows services in order to **avoid detection**. With the help of Windows services monitoring tools, you can detect the Trojans.

Trojans that spawn Windows services allow attackers remote control to the target 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.

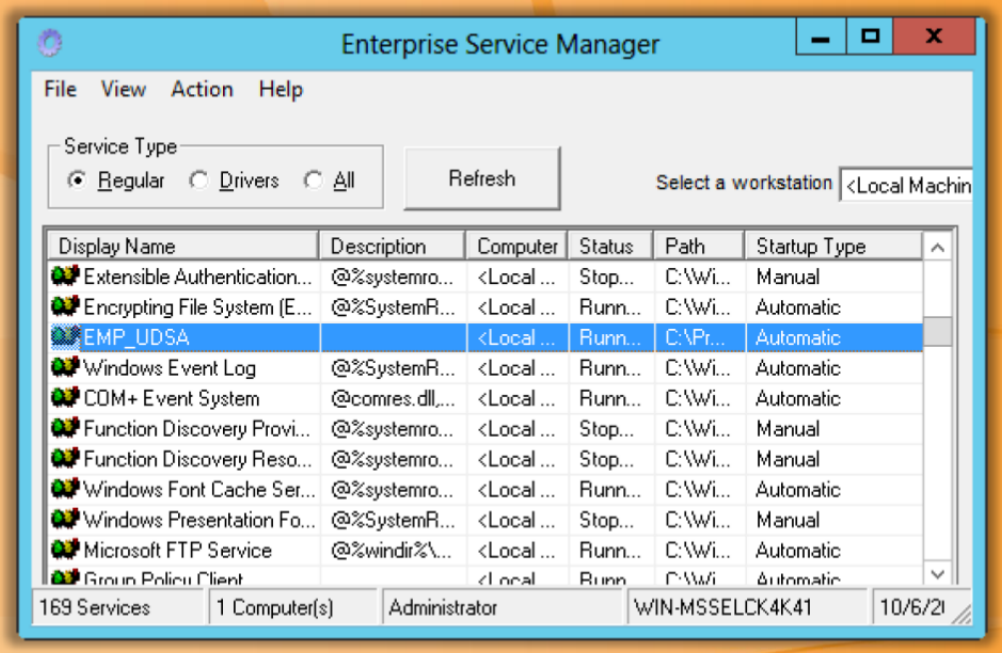
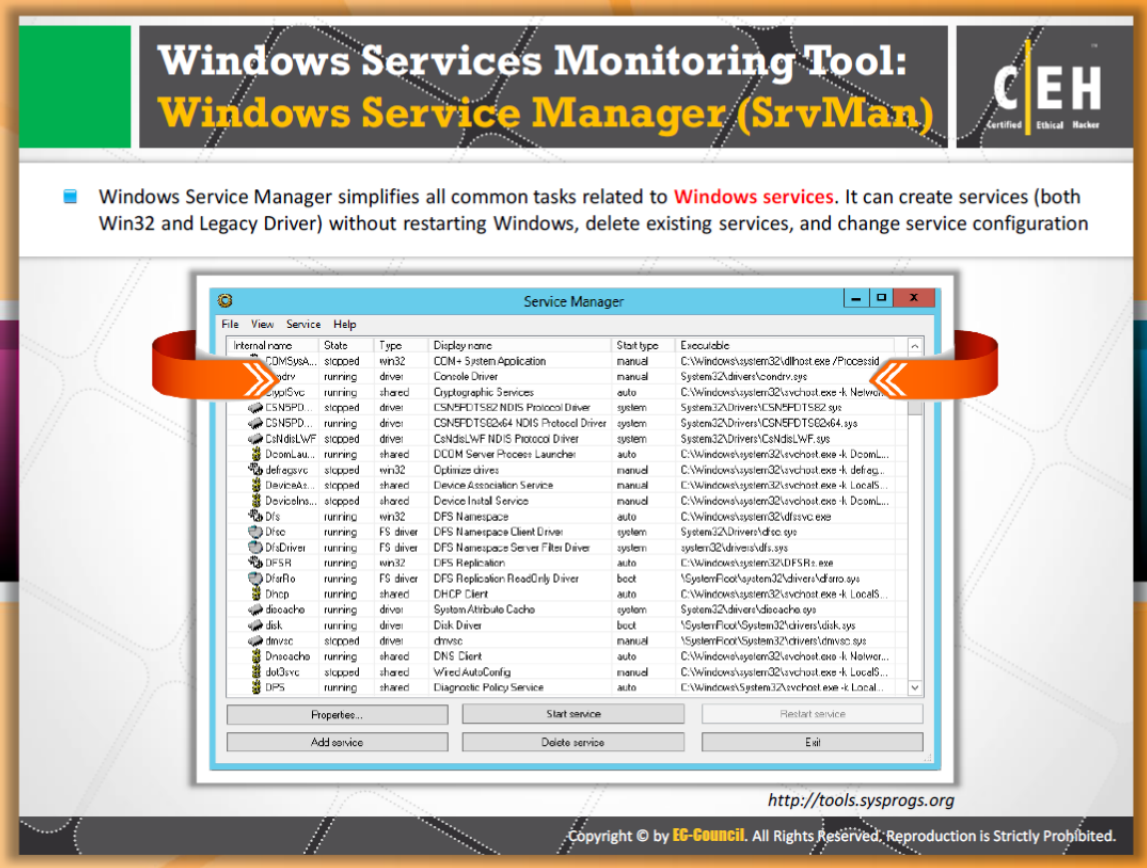


FIGURE 6.57: Scanning for Suspicious Windows Services



Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

Source: http://tools.sysprogs.org

Windows Service Manager is a tool that allows you to **shorten** all **public tasks** linked to Windows services. This can generate different services for Win32 and Legacy drivers without shutting down and restarting Windows. It can also cancel existing services and manipulate other configuration services. It has both **GUI and ccommand-line** modes. It can also be used to run arbitrary Win32 applications as services. It supports all modern **32-bit and 64-bit** versions of Windows.

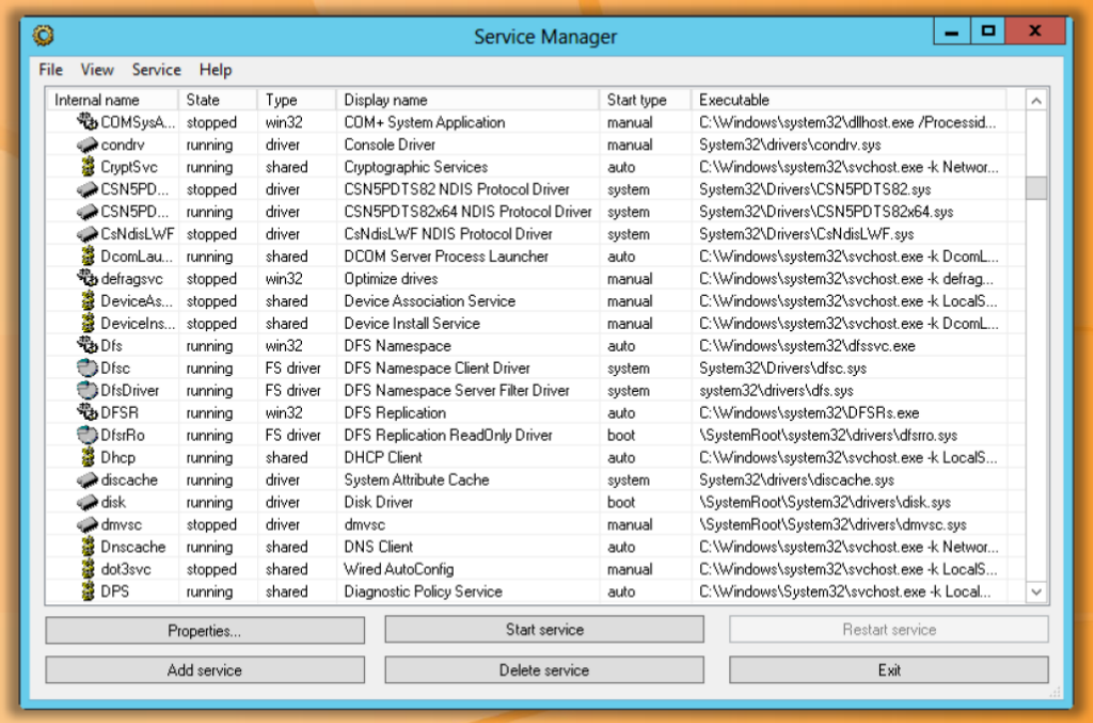
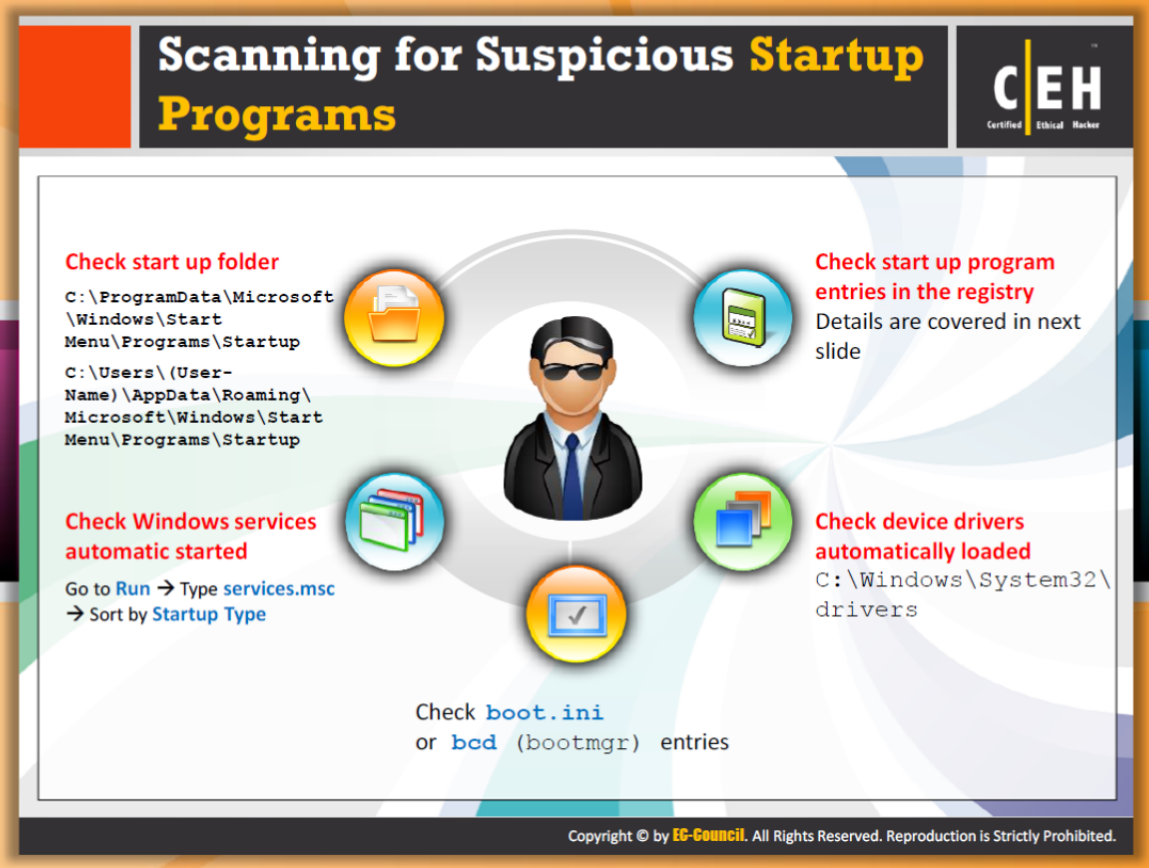


FIGURE 6.58: Windows Service Manager (SrvMan) Tool Screenshot

Windows Services Monitoring Tools

Windows Services monitoring tools monitor critical **Windows services** and optionally restart them after failure. A few of the Windows service monitoring tools that are readily available in the market are listed as follows:

- Smart Utility available at http://www.thewindowsclub.com
- Netwrix Service Monitor available at http://www.netwrix.com
- Vista Services Optimizer available at http://www.smartpcutilities.com
- ServiWin available at http://www.nirsoft.net
- Windows Service Manager Tray available at http://winservicemanager.codeplex.com
- AnVir Task Manager available at http://www.anvir.com
- Process Hacker available at http://processhacker.sourceforge.net
- Free Windows Service Monitor Tool available at http://www.manageengine.com
- Overseer Network Monitor available at http://www.overseer-network-monitor.com
- Total Network Monitor available at http://www.softinventive.com



Scanning for Suspicious Startup Programs

Trojans, once installed on the computer, start automatically at **system startup**. Therefore, scanning for suspicious **startup programs** is very essential for detecting Trojans. By following these simple steps, you can identify if there are any hidden Trojans:

Step 1: Check the Startup folder

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

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

Step 2: Check Windows services automatic started

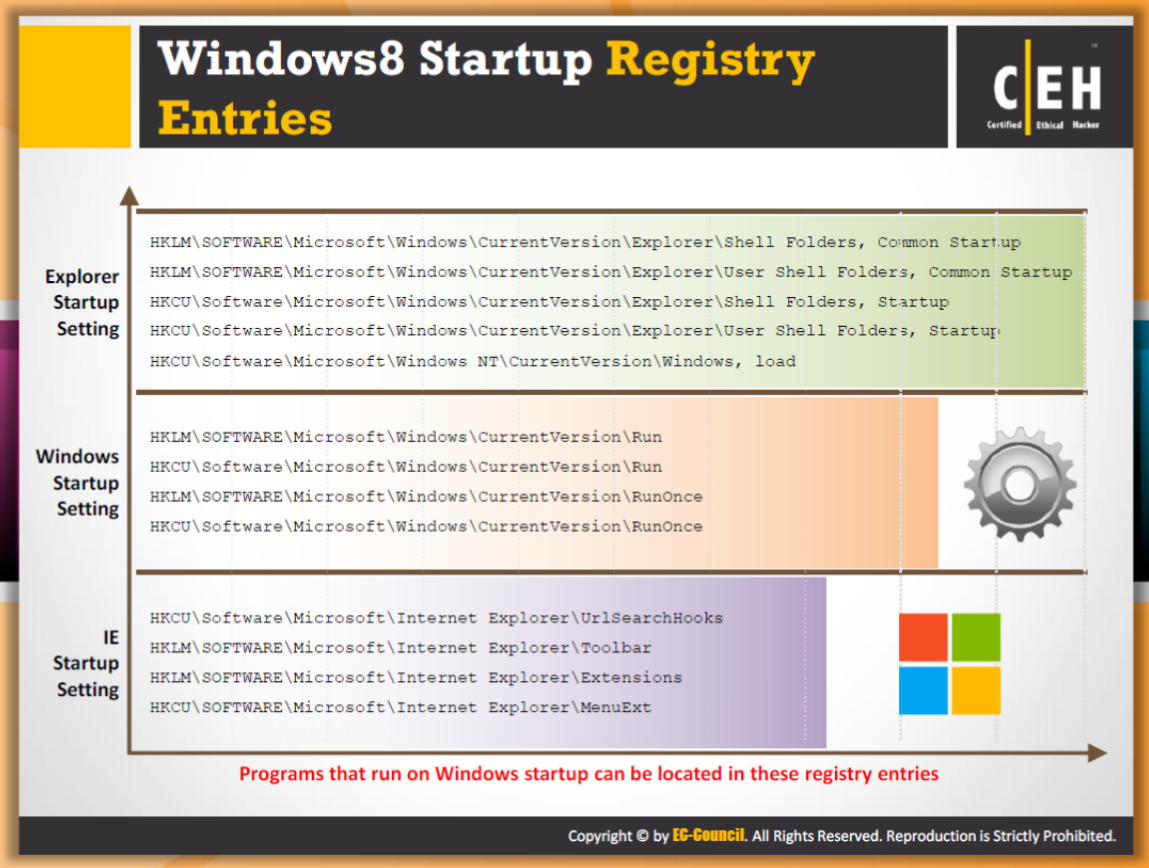
Go to **Run**, type services.msc, and click **Sort by Startup Type**

Step 3: Check startup program entries in the registry

Step 4: Check that device drivers are automatically loaded:

`C:\Windows\System32\drivers`

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



Windows8 Startup Registry Entries

Programs that run on Windows startup can be located in these registry entries:

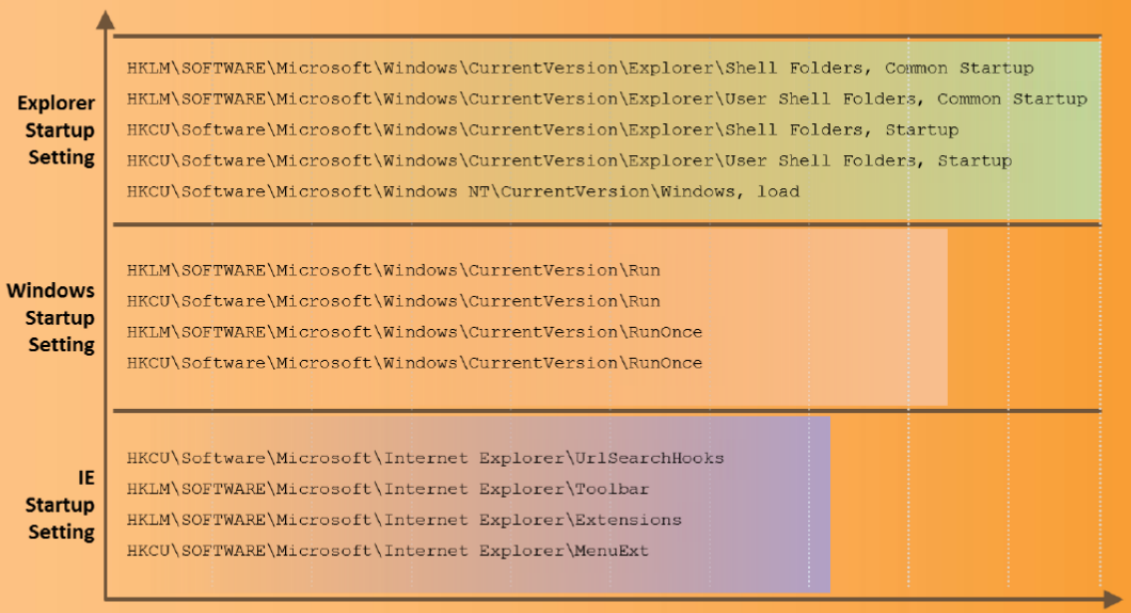
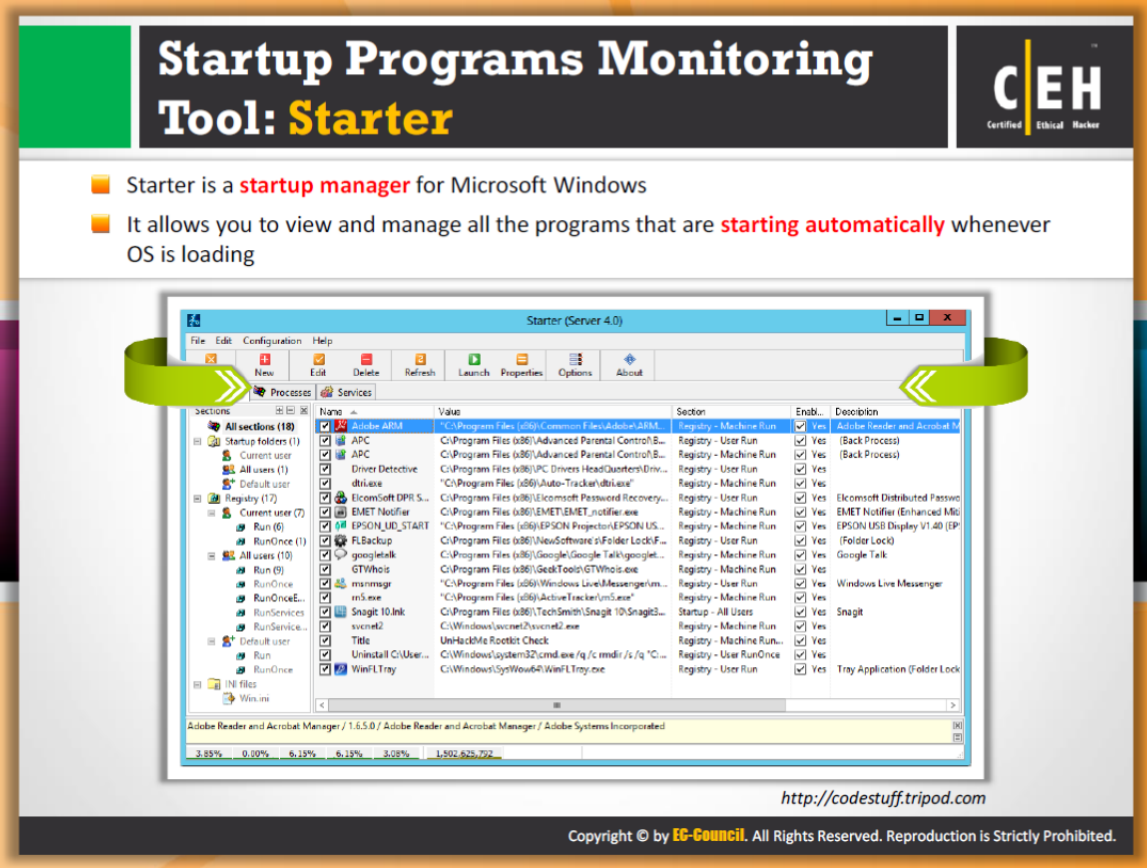


FIGURE 6.59: Windows8 Startup Registry Entries



Startup Programs Monitoring Tool: Starter

Source: http://codestuff.tripod.com

Starter allows you to view and manage all the programs that **start automatically** whenever the operating system is loaded. It enumerates all the **hidden registry entries**, startup folders' items and some of the initialization files, so that the user could choose to temporarily disable selected entries, edit them, create new, or delete them **permanently**.

Starter can also list all the processes running and with a change to view extended process' information (such as used DLLs, memory usage, thread count, priorities, etc.), and to terminate selected process. It supports Microsoft Windows 9x, Me, NT, 2000, XP, 2003, and Vista. There are no specific requirements except one: **registry operations** on a Windows-NT-based operating system may require special access rights. As a rule, members of **Administrators** and Power Users groups have nothing to worry about.

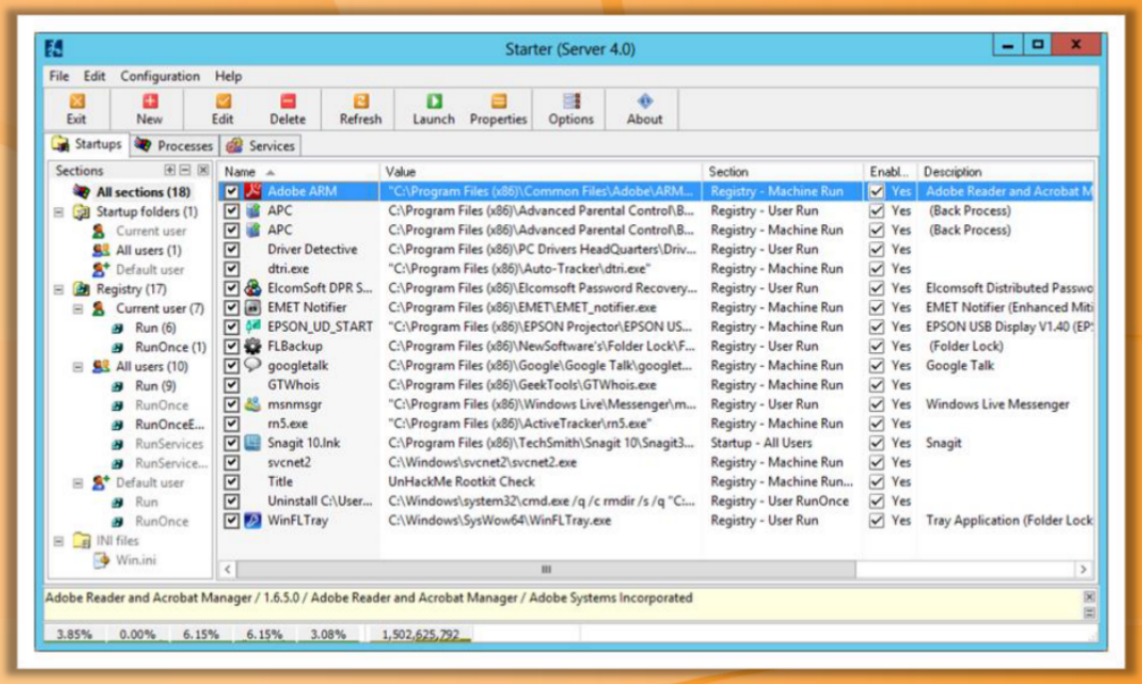


FIGURE 6.60: Starter Tool Screenshot

Startup Programs Monitoring Tool: Security AutoRun

Source: http://tcpmonitor.altervista.org

Security AutoRun allows you to view the **list of all applications** that are loaded automatically when **Windows starts up**. Each application is listed with the details of its type, registry, common/user, services, drivers list, command-line string, product name, file version, company name, location in the registry or file system, and more. It identifies a spyware or adware program that runs at startup. Compatible operating systems of Windows are **9x/ME/NT/2000/XP/Vista/7**.

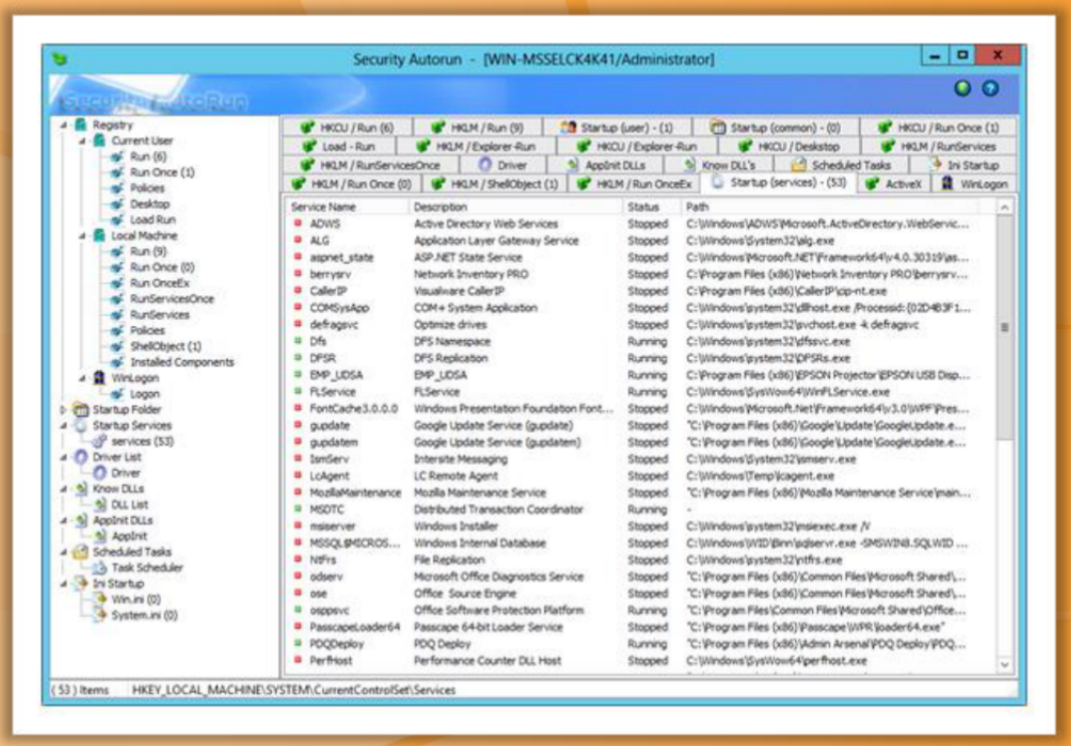
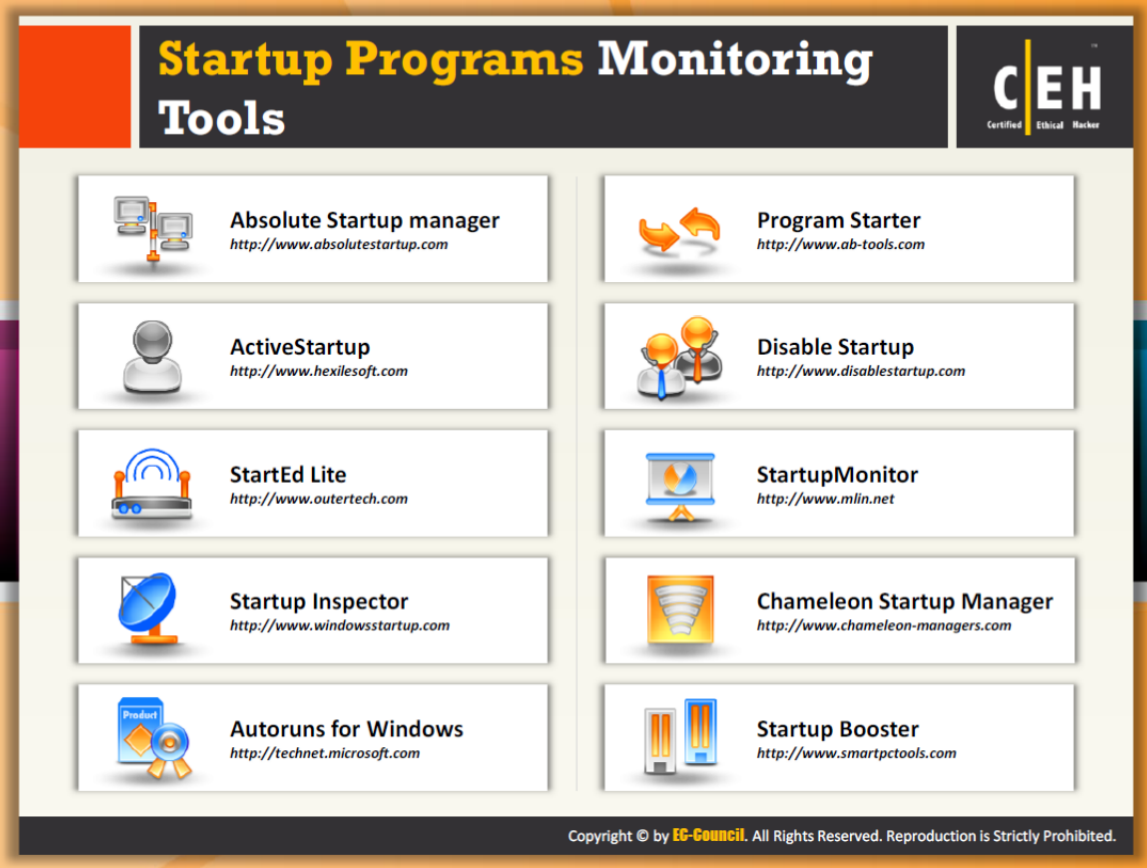


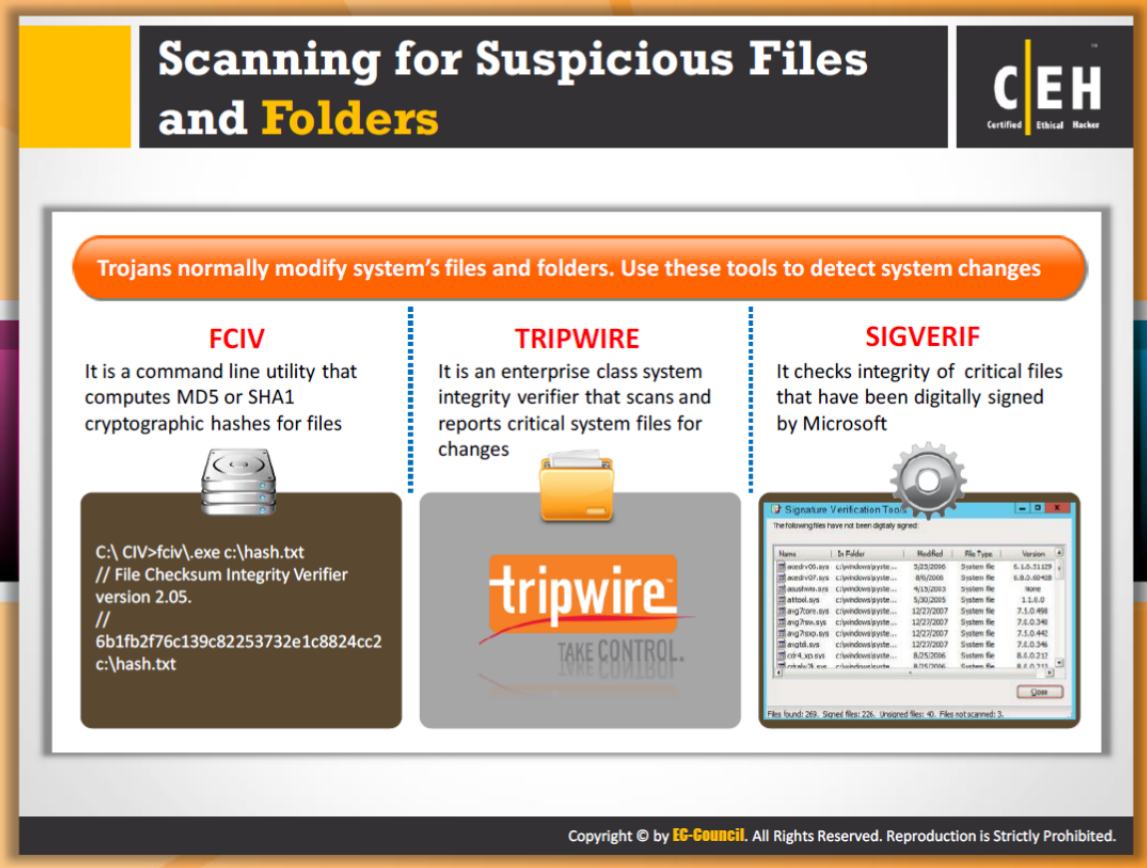
FIGURE 6.61: Security AutoRun Tool Screenshot



Startup Programs Monitoring Tools

A list of Startup programs' monitoring tools are as follows:

- Absolute Startup manager available at http://www.absolutestartup.com
- ActiveStartup available at http://www.hexilesoft.com
- StartEd Lite available at http://www.outertech.com
- Startup Inspector available at http://www.windowsstartup.com
- Autoruns for Windows available at http://technet.microsoft.com
- Program Starter available at http://www.ab-tools.com
- Disable Startup available at http://www.disablestartup.com
- StartupMonitor available at http://www.mlin.net
- Chameleon Startup Manager available at http://www.chameleon-managers.com
- Startup Booster available at http://www.smartpctools.com



Scanning for Suspicious Files and Folders

Usually when a system gets infected by a Trojan, it modifies the files and folders; you can scan the files and folders with the following tools in order to detect the **Trojans installed**.

FCIV

File Checksum Integrity Verifier (FCIV) is a utility that can allow you to generate **MD5** or **SHA-1** hash values for files that can be verified with the standard values to determine any change in them; if found, you can run a verification of the file system files against the XML database to determine which files have been modified. It is a command-prompt utility that computes and verifies **cryptographic** hash values of all your critical files and saves the values in an XML file database.

```
C:\ CIV>fciv\.exe c:\hash.txt
// File Checksum Integrity Verifier version 2.05.
//
6b1fb2f76c139c82253732e1c8824cc2 c:\hash.txt
```

Tripwire

Source: http://www.tripwire.com

Tripwire Enterprise provides the configuration control capabilities organizations need to proactively secure the entire infrastructure and ensure compliance with internal policies, regulations, and industry standards and benchmarks.

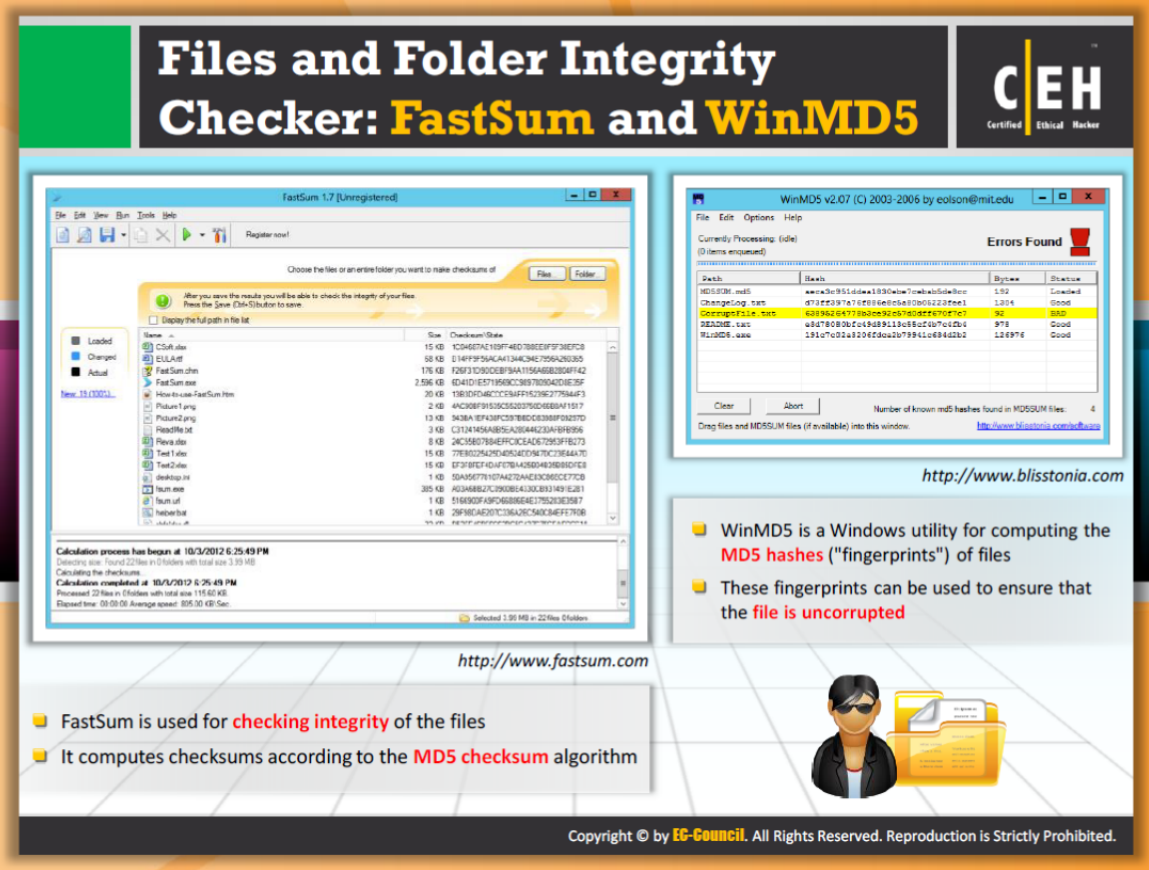
SIGVERIF

Source: http://books.google.co.in

SIGVERIF is a signature **verification tool** that allows you to find signed and **unsigned drivers** connected to the system. When you find any unsigned driver, you can move that to a new folder and restart the system and test the program and functionality for errors. The following are the steps to identify unsigned drivers:

- Click **Start**, click **Run**, type **SIGVERIF**, and then click **OK**.
- Click the **Advanced** button.
- Click the other files that are not digitally signed.
- Navigate to winnt\system32\driversfolder and then click **OK**.

After SIGVERIF finishes, it checks all the unsigned drivers and lists are displayed on the computer. The investigator can find the list of all signed and unsigned drivers found by SIGVERIF in `sigverif.txt` in the `%windir%` folder, typically the winnt or windows folder.



Files and Folder Integrity Checker: FastSum and WinMD5

A files and folder integrity checker allows you to **monitor the integrity of files** and **folders** and **check** for any **changes** in the critical files, indicating potential intrusion attempts. These work with a suite of security tools to provide a complete audit and monitoring solution for OSS and Guardian file systems.

FastSum

Source: http://www.fastsum.com

FastSum is built on the well-proven **MD5 checksum algorithm**, which is used worldwide for checking the integrity of the files. You can take control of your data with FastSum. **Fingerprint** your important files now and check the integrity after a network transfer or a **CD burning** simply by taking the fingerprints again and comparing them with the previously made ones. In the same way, you can also find out whether your files had been damaged by viruses, network issues, or **CD/ DVD burning failures**.

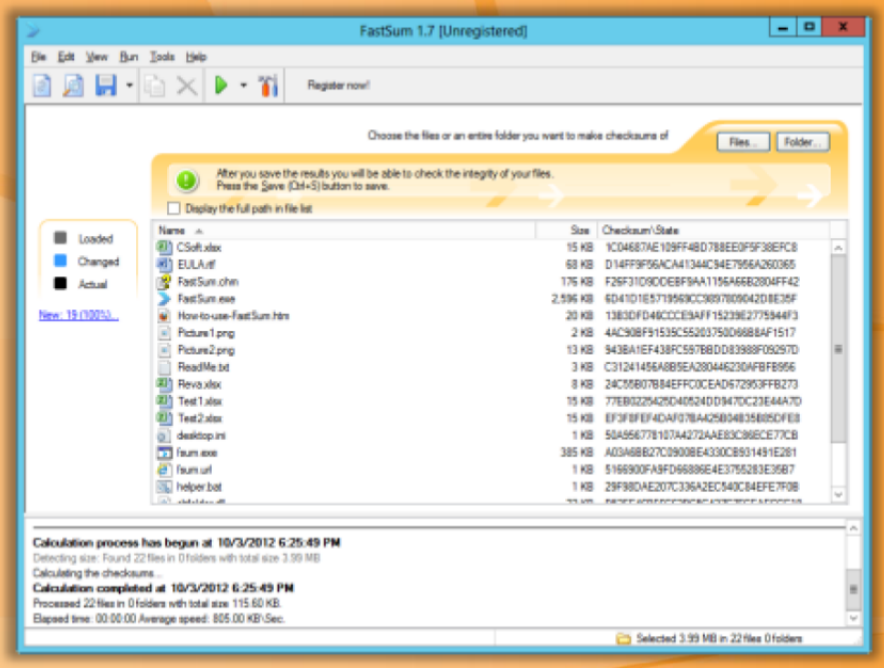


FIGURE 6.62: FastSum

WinMD5

Source: http://www.blisstonia.com

WinMD5 v2.0 is a Windows (98, 2000, XP, Vista, 7) utility for computing the **MD5 hashes** ("fingerprints") of files. It also makes it very easy to compare the fingerprints against the correct fingerprints stored in an **MD5SUM** file. RedHat, for example, provides MD5SUM files for all of its large downloadable files. These fingerprints can be used to ensure that your file is uncorrupted.

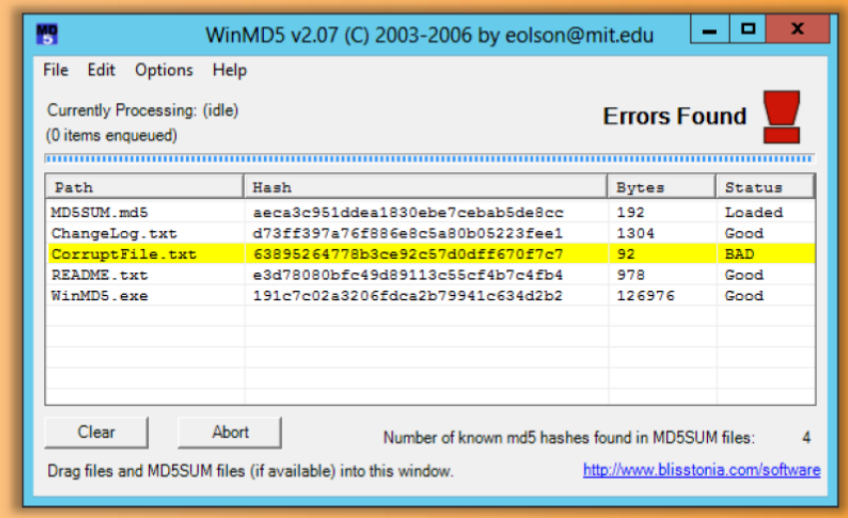
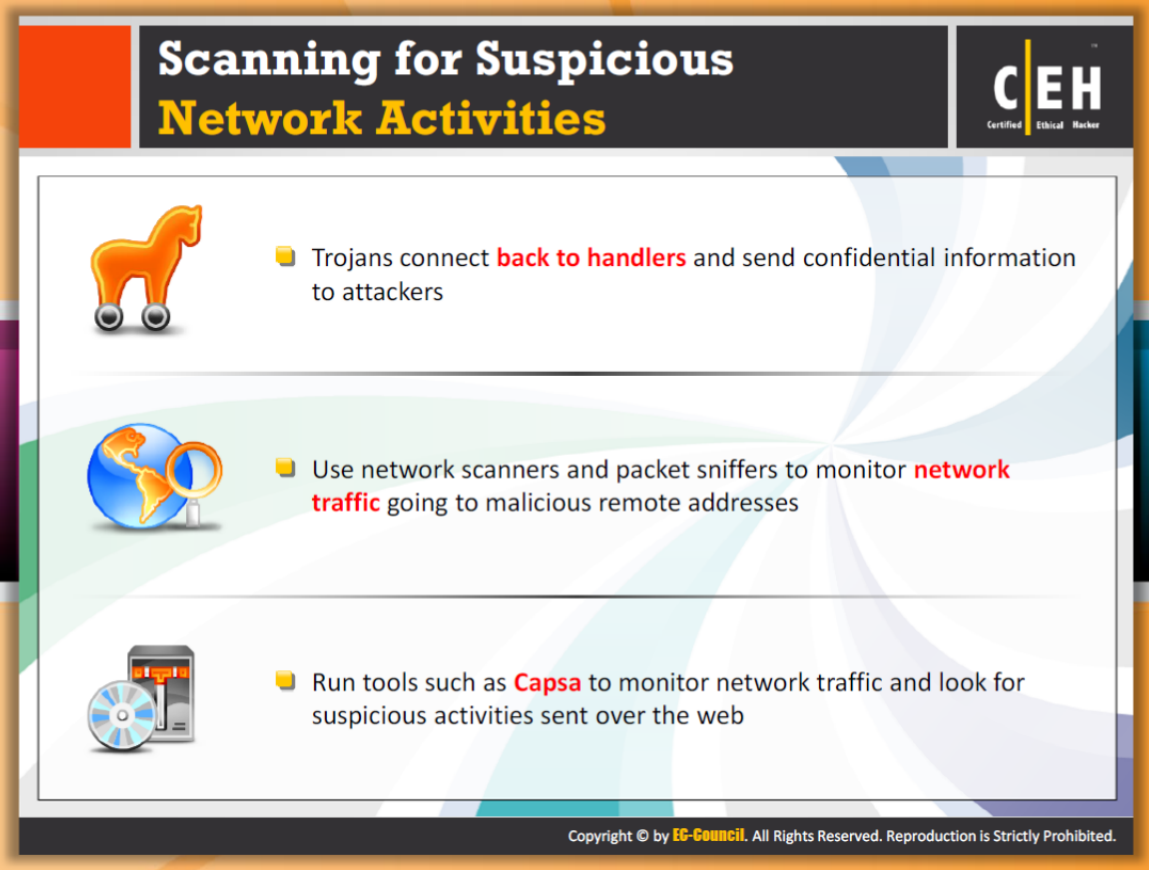


FIGURE 6.63: WinMD5

Files and Folder Integrity Checkers

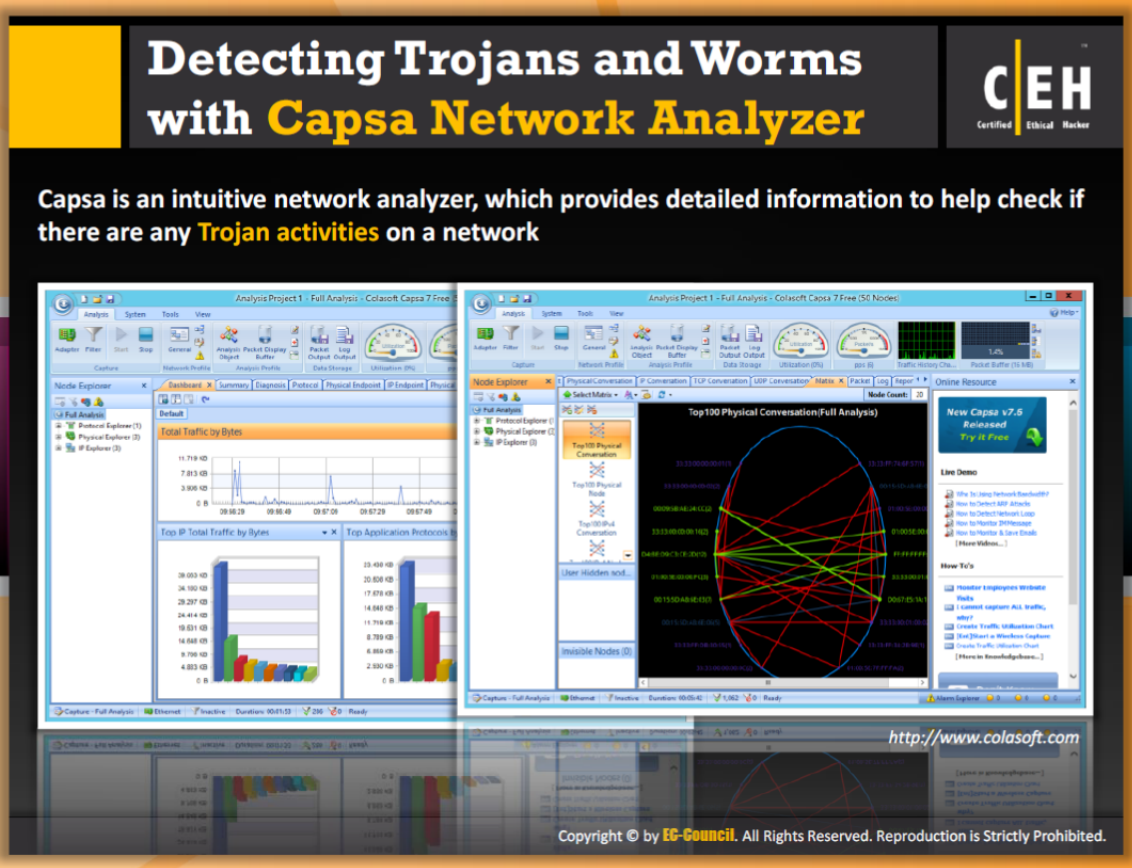
Files and Folder Integrity **Checkers monitor** file integrity and identify the changes in the critical files that intimate any **potential intrusion** attempts A few files and folder integrity checkers are listed as follows:

- Advanced CheckSum Verifier (ACSV) available at http://www.irnis.net
- Fsum Fronted available at http://fsumfe.sourceforge.net
- Verisys available at http://www.ionx.co.uk
- AFICK (Another File Integrity Checker) available at http://afick.sourceforge.net
- File Integrity Monitoring available at http://www.ncircle.com
- Attribute Manager available at http://www.miklsoft.com
- PA File Sight available at http://www.poweradmin.com
- CSP File Integrity Checker available at http://www.tandemsecurity.com
- ExactFile available at http://www.exactfile.com
- OSSEC available at http://www.ossec.net



Scanning for Suspicious Network Activities

After a **malicious attack**, the Trojans start sending the **confidential data** present on the system to the attackers. Trojans connect back to handlers and send confidential information to attackers. Use **network scanners** and **packet sniffers** to monitor network traffic going to malicious remote addresses. In order to avoid these situations, it's always better to scan the networks for suspicious activities. With the help of **scanning utilities**, you can know if the data is being transferred to a malicious remote source. By using network scanning tools like Capsa, you can identify such activities.



Detecting Trojans and Worms with Capsa Network Analyzer

Source: http://www.colasoft.com

Capsa is a network analyzer that provides enough information to help check if there is any **Trojan activity on a network**. It is a portable network analyzer for **LANs/WLANs** that performs packet capturing, network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis.

Features of Capsa Network Analyzer include:

- Real-time capture and save data transmitted over local networks, including wired network and wireless network like **802.11a/b/g/n**
- Monitor network bandwidth and usage by capturing **data packets transmitted** over the network and providing summary and decoding information about these packets
- View network statistics, allowing easy capture and interpretation of network utilization data
- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum

- Diagnose and **pinpoint network problems** in seconds by detecting and locating suspicious hosts
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the **entire network** in an ellipse that shows the connections and traffic between each host

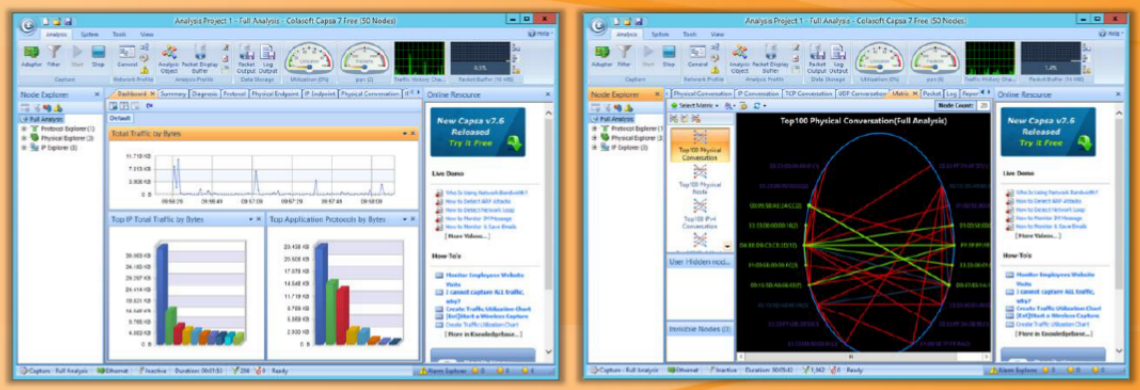
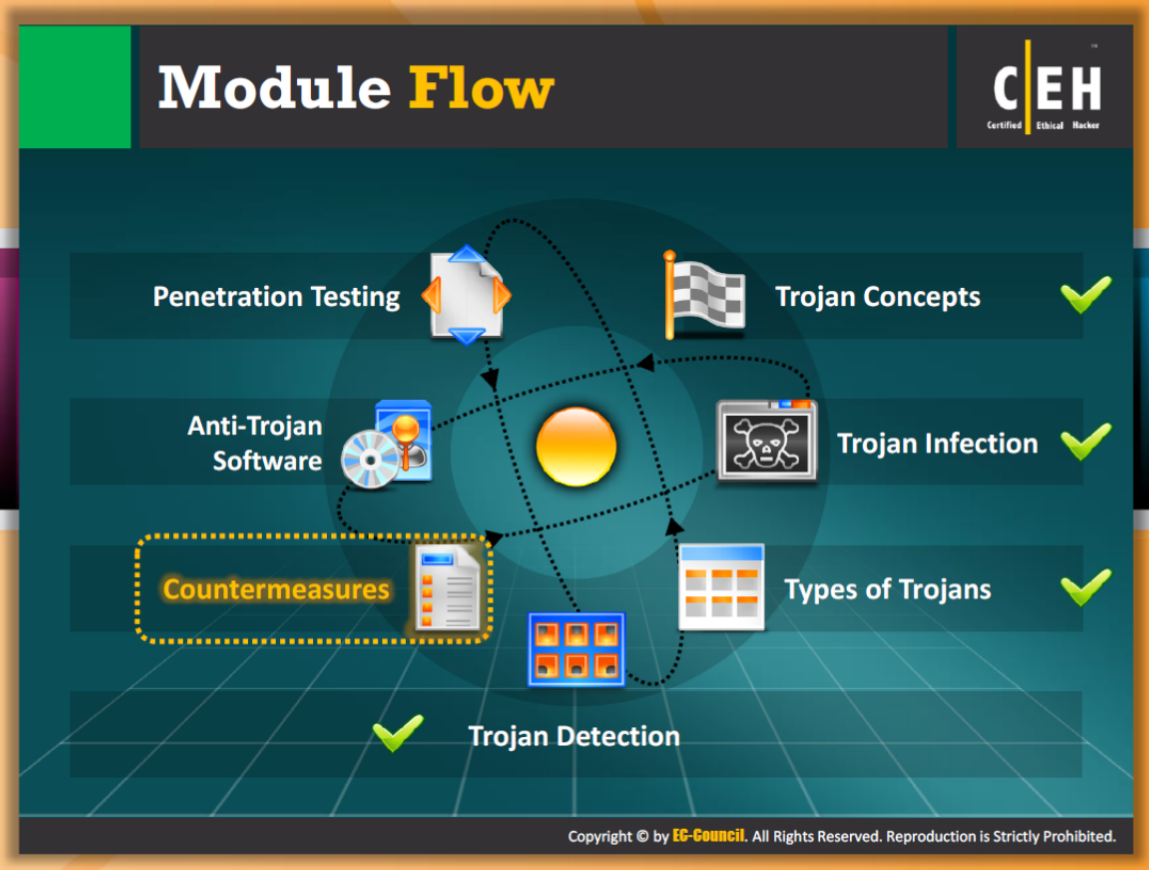


FIGURE 6.64: Detecting Trojans and Worms with Capsa Network Analyzer

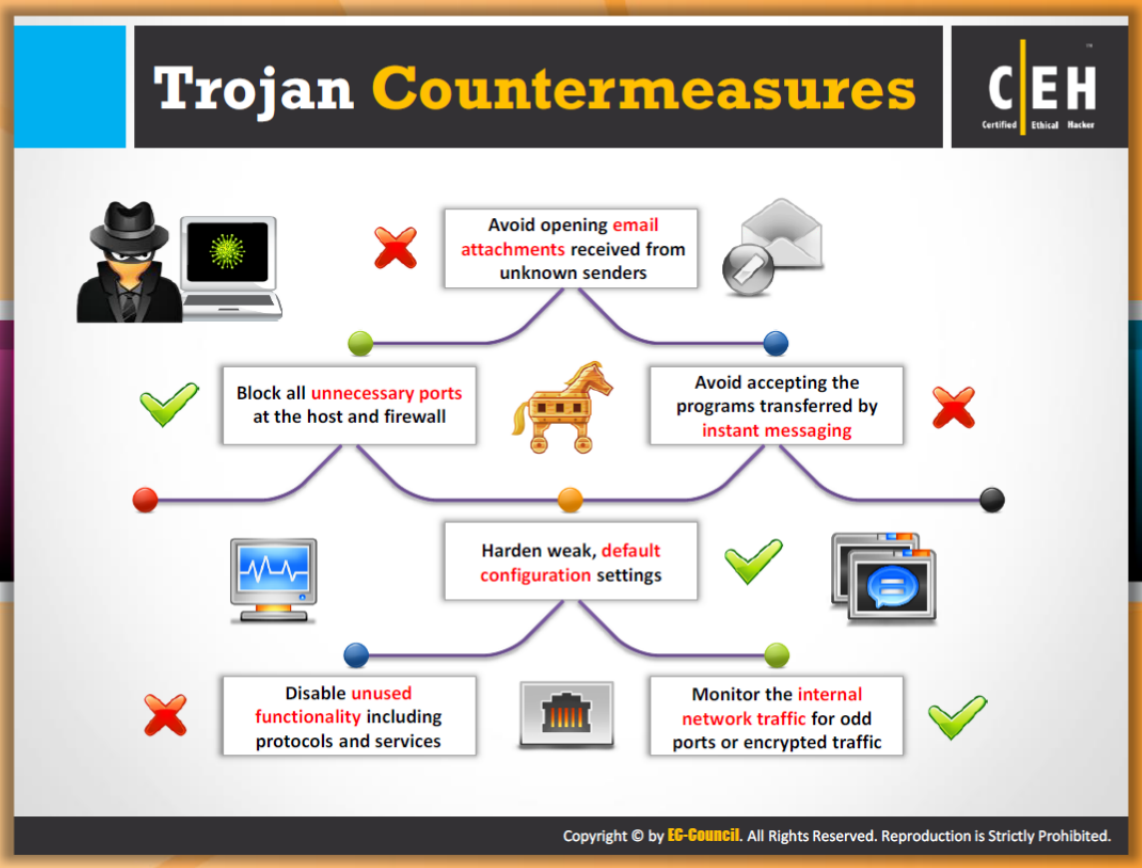


Module Flow

So far, we have discussed various Trojans and the ways they **infect the system resources** or information stored on the computer, as well as ways to detect Trojans on a computer. Once you detect a **Trojan**, you should immediately delete it and apply countermeasures that offer protection against Trojans and backdoors. These countermeasures minimize risk and provide complete protection to the user's system.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

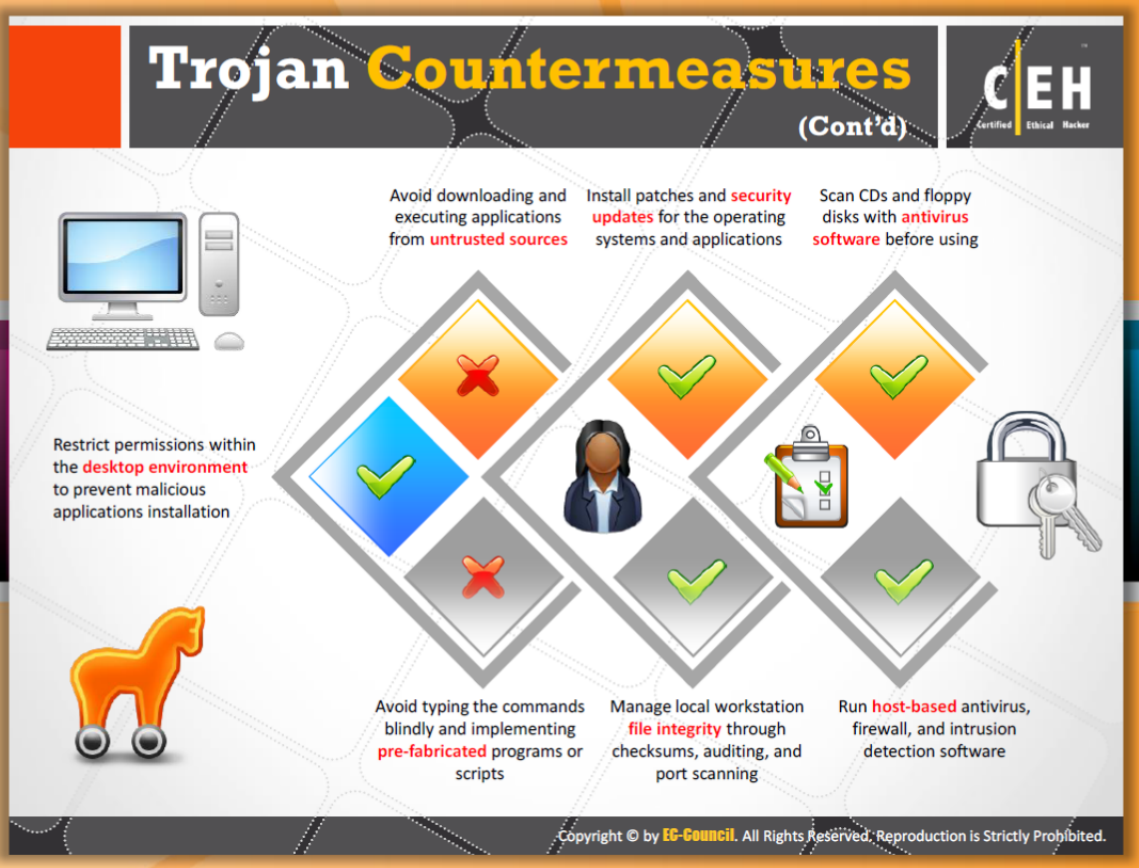
This section highlights various countermeasures that prevent Trojans and backdoors from entering into your system.



Trojan Countermeasures

A Trojan is a malicious program that masquerades as a **genuine application**. When these Trojans are activated, they lead to many issues such as erasing data, replacing data on a victim's computer, corrupting files, spreading viruses, and spying on the **victim's system** and secretly reporting the data, recording keystrokes to steal sensitive information such as credit card number, user names, passwords etc. and **opening a backdoor** on the victim's system for carrying out precarious activities in the future. In order to prevent such activities and reduce the risks against Trojans, the following countermeasure should be adopted:

- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and firewall
- Avoid accepting the programs transferred by instant messaging
- Harden weak, default configuration settings
- Disable unused functionality including protocols and services
- Monitor the internal network traffic for odd ports or encrypted traffic



Trojan Countermeasures (Cont'd)

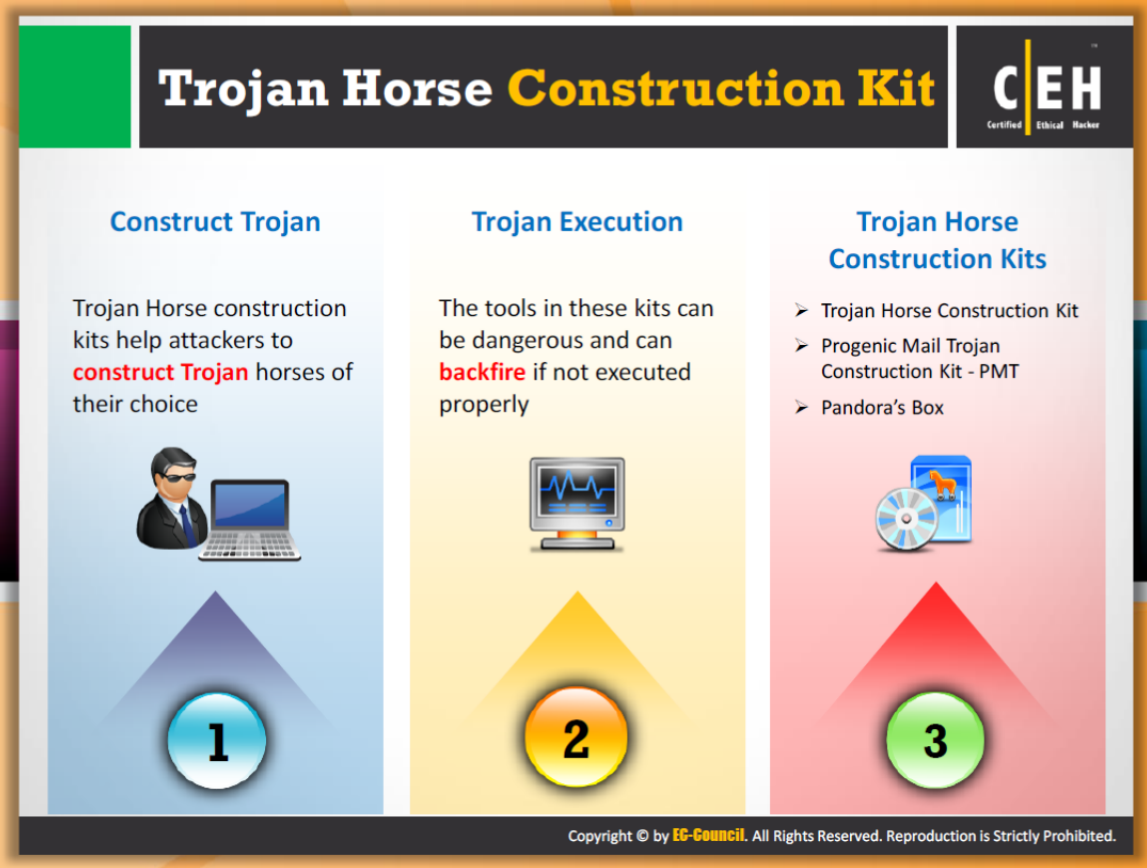
- Avoid downloading and executing applications from untrusted sources
- Install patches and security updates for the operating systems and applications
- Scan CDs and floppy disks with antivirus software before using
- Restrict permissions within the desktop environment to prevent malicious applications installation
- Avoid typing the commands blindly and implementing pre-fabricated programs or scripts
- Manage local workstation file integrity through checksums, auditing, and port scanning
- Run local versions of antivirus, firewall, and intrusion detection software on the desktop

Backdoor Countermeasures

Perhaps the old adage "**anounce of prevention is worth a pound of cure**" is relevant here. Some backdoor countermeasures are:

- The first line of defense is to educate users regarding the dangers of installing applications downloaded from the Internet, and to be cautious if they have to open email attachments.
- The second line of defense can be antivirus products that are capable of recognizing Trojan signatures. The updates should be regularly applied over the network.
- The third line of defense comes from keeping application versions updated by the following security patches and vulnerability announcements.

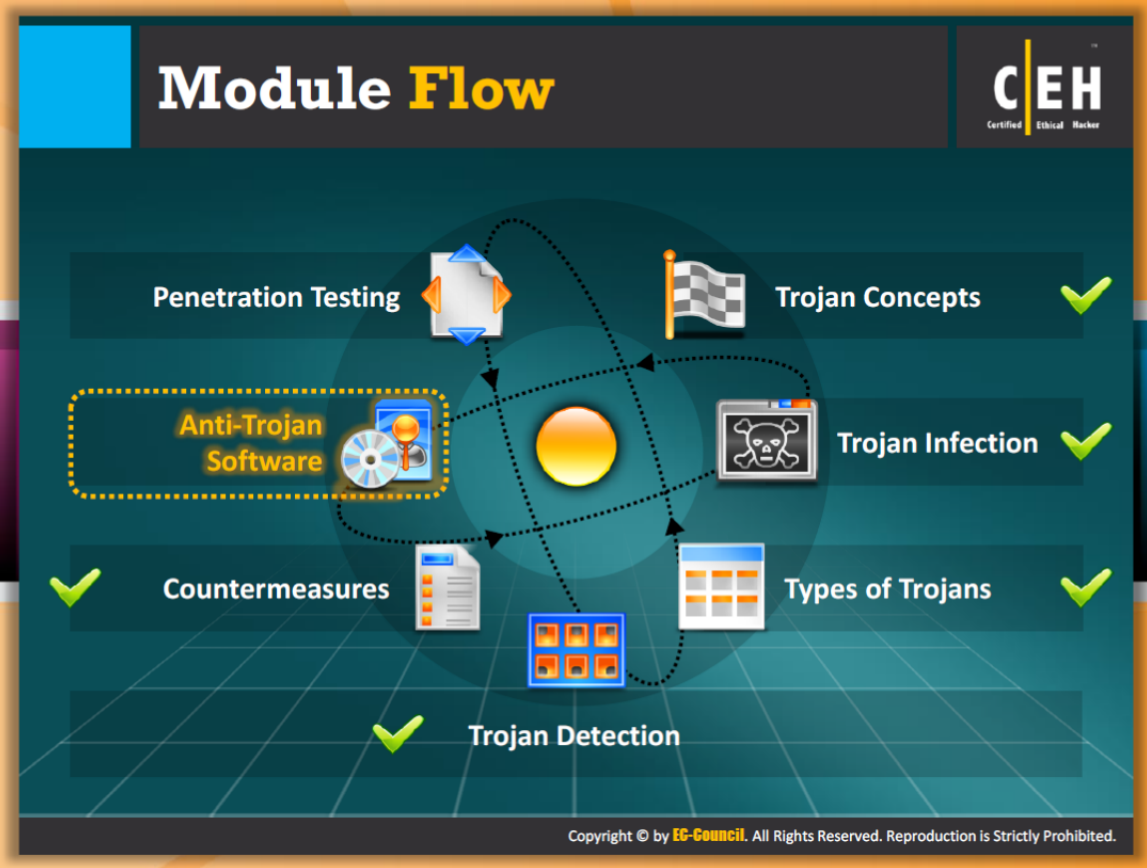
Use antivirus tools such as Windows Defender, McAfee, and Norton to detect and eliminate backdoors.



Trojan Horse Construction Kits

These kits help attackers construct **Trojan horses** of their choice. The tools in these kits can be dangerous and can backfire if not executed properly. Some of the Trojan kits available in the wild are as follows:

- The **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 send to a victim.
- Pandora's Box is a program designed to create **Trojans/time bombs**.

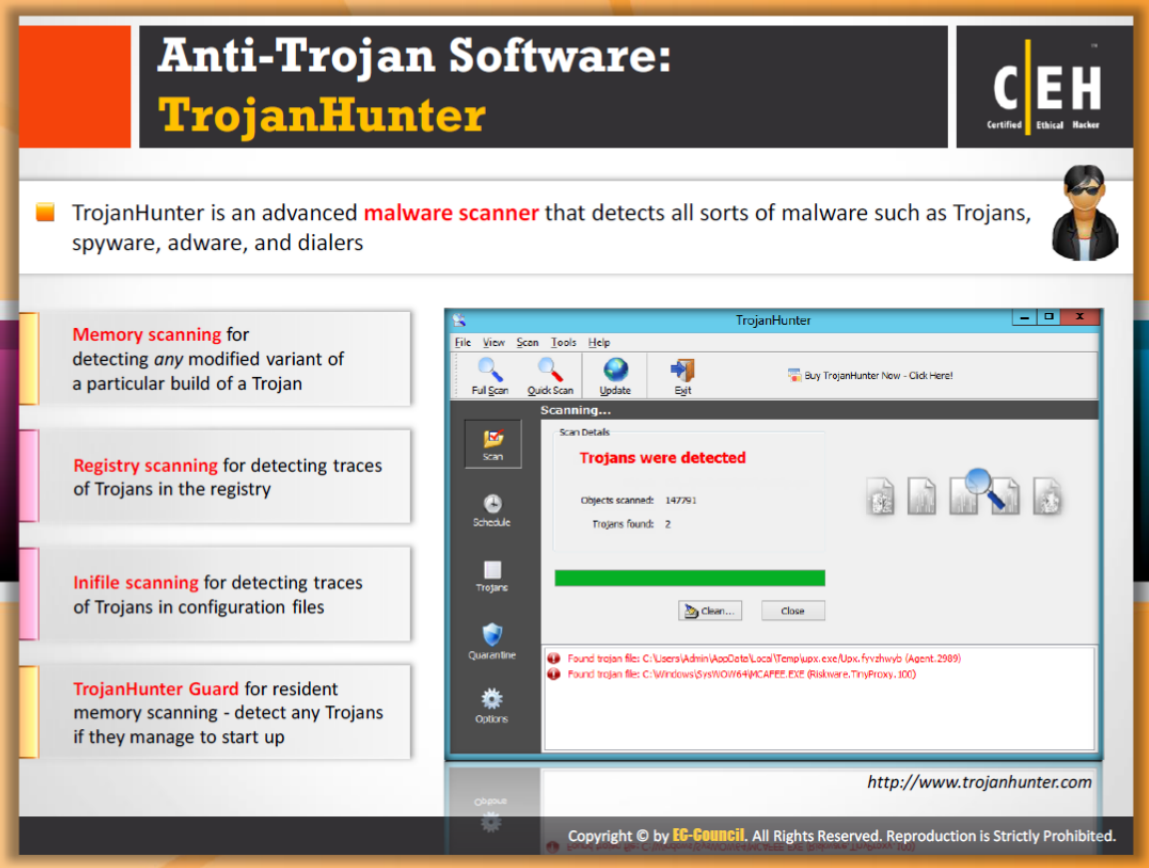


Module Flow

Prior to this, we have discussed various **countermeasures** that offer protection to your computer system and the information stored on it against various malware such as **Trojans and backdoors**. In addition to these, there is **anti-Trojan software** that can protect your computer systems and other information assets against Trojans and backdoors. Anti-Trojan software deals with removing or deactivating malware.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

This section lists and describes various anti-Trojan software programs.



Anti-Trojan Software: TrojanHunter

Source: http://www.trojanhunter.com

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

Some of TrojanHunter's features include:

- High-speed 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
- The Advanced Trojan Analyzer, an exclusive feature of **TrojanHunter**, is able to find whole classes of Trojans using advanced scanning techniques
- TrojanHunter Guard for resident memory **scanning - detect** any Trojans if they manage to start up
- LiveUpdate utility for effortless ruleset updating via the Internet

- Process list giving details about every running process on the system, including the path to the actual executable file
- Accurate removal of all detected Trojans - even if they are running or if the Trojan has injected itself into another process

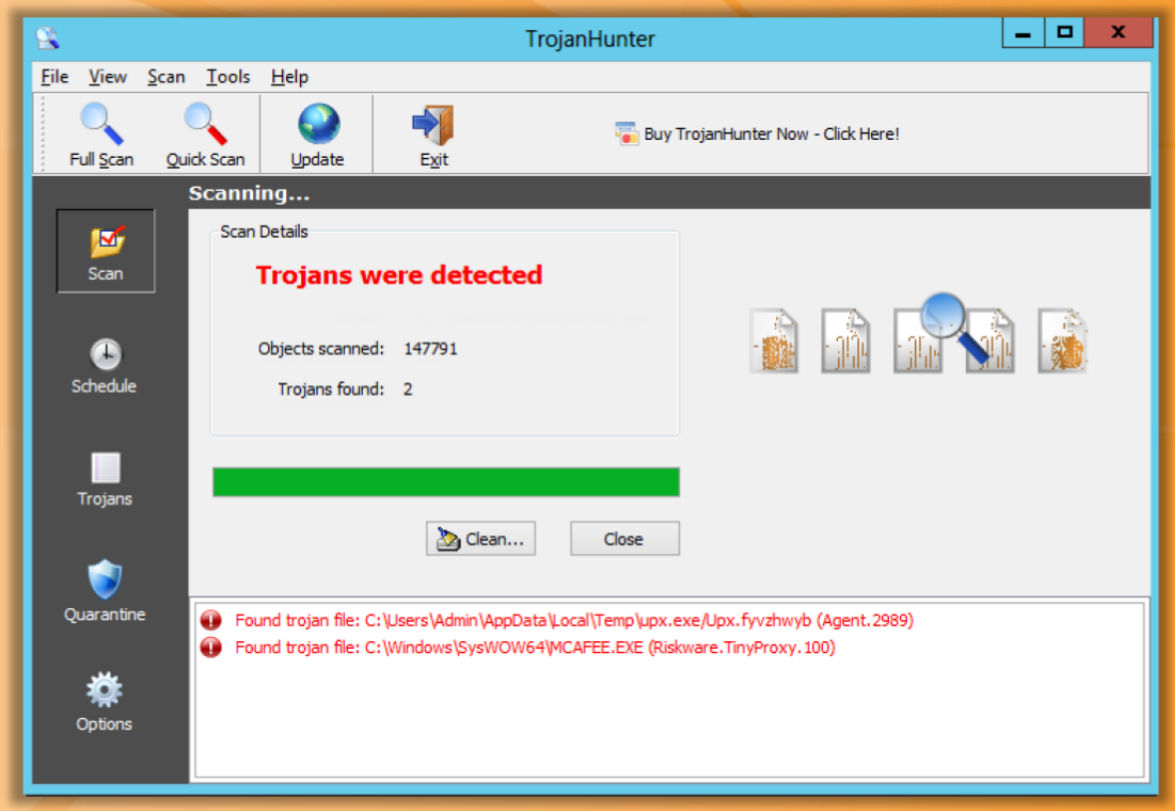


FIGURE 6.65: TrojanHunter Anti-Trojan Software

Anti-Trojan Software: Emsisoft Anti-Malware

Source: http://www.emsisoft.com

Emsisoft Anti-Malware provides reliable **protection of your system** against various threats such as viruses, Trojans, spyware, adware, worms, bots, keyloggers, and rootkits. It has two combined scanners (antivirus and anti-malware) for cleaning infection and three guards against new infections: file guard, behavior blocker, and surf protection.

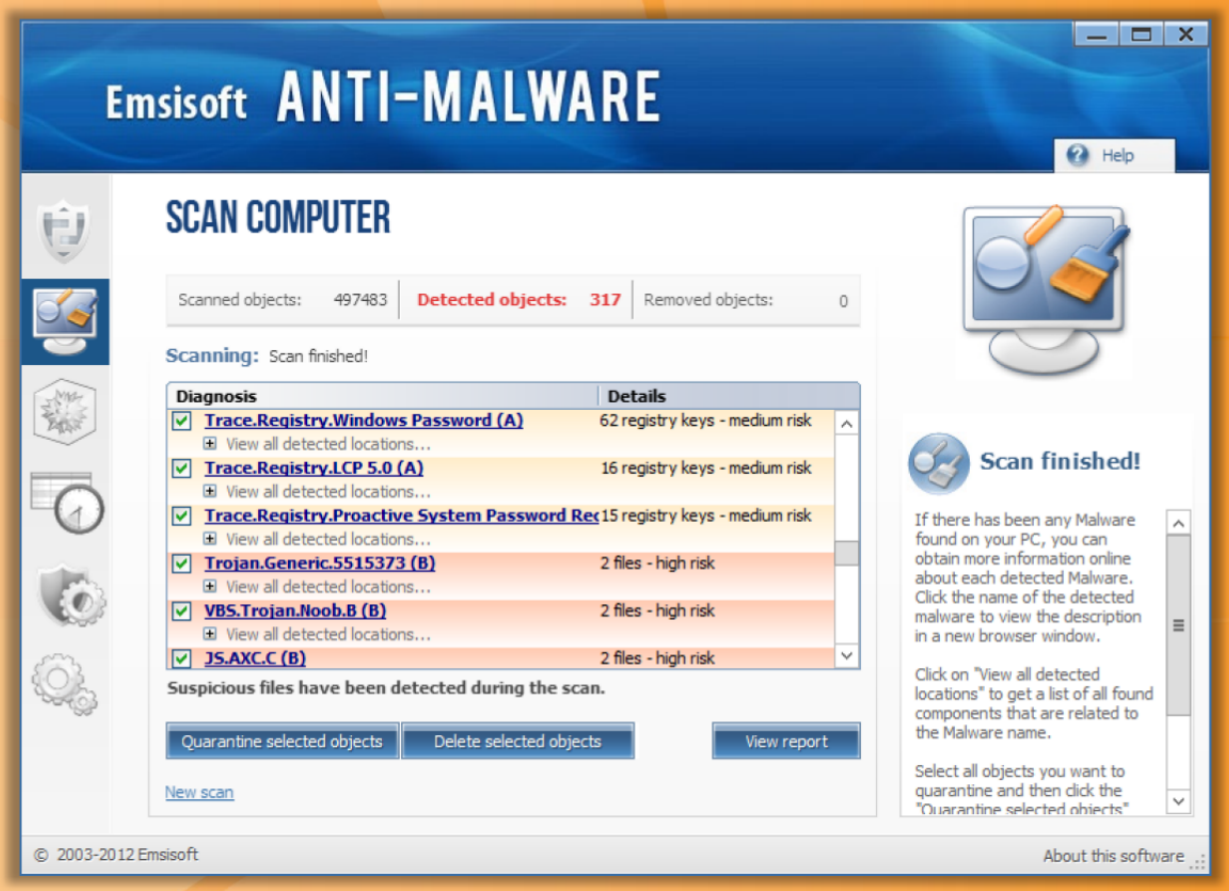
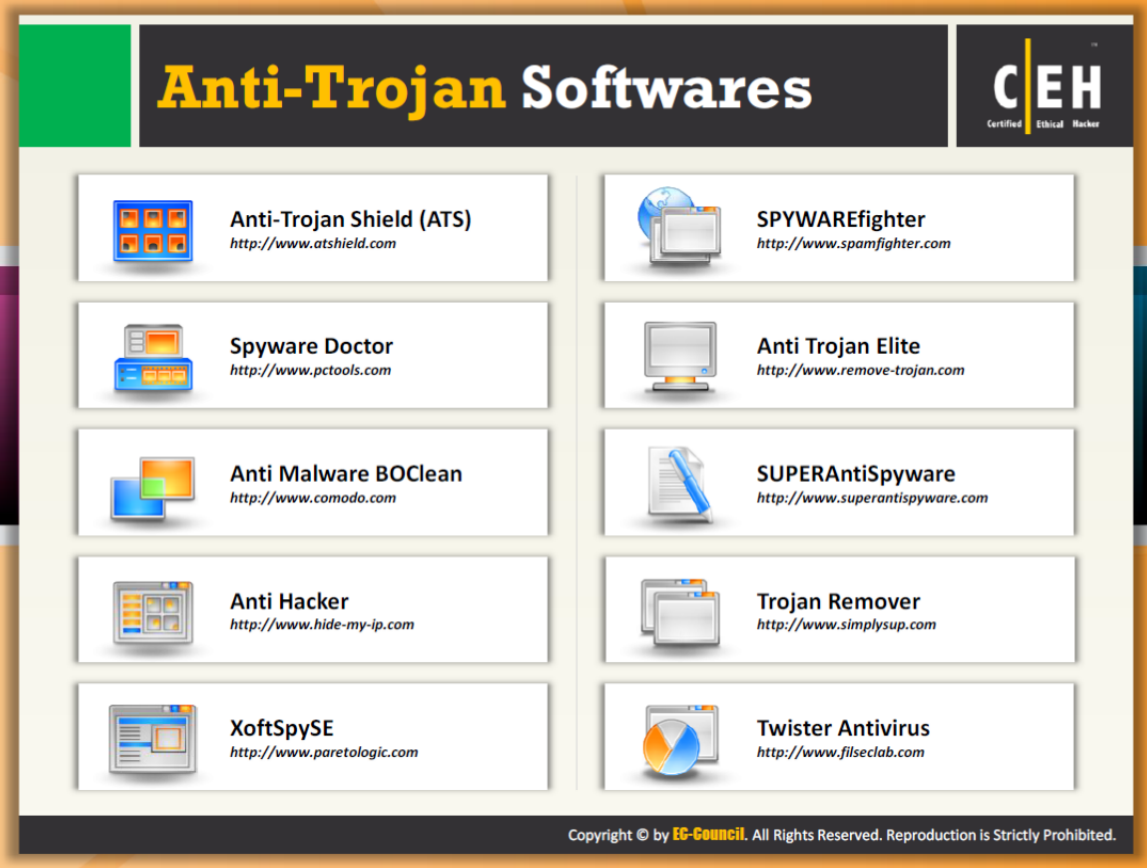


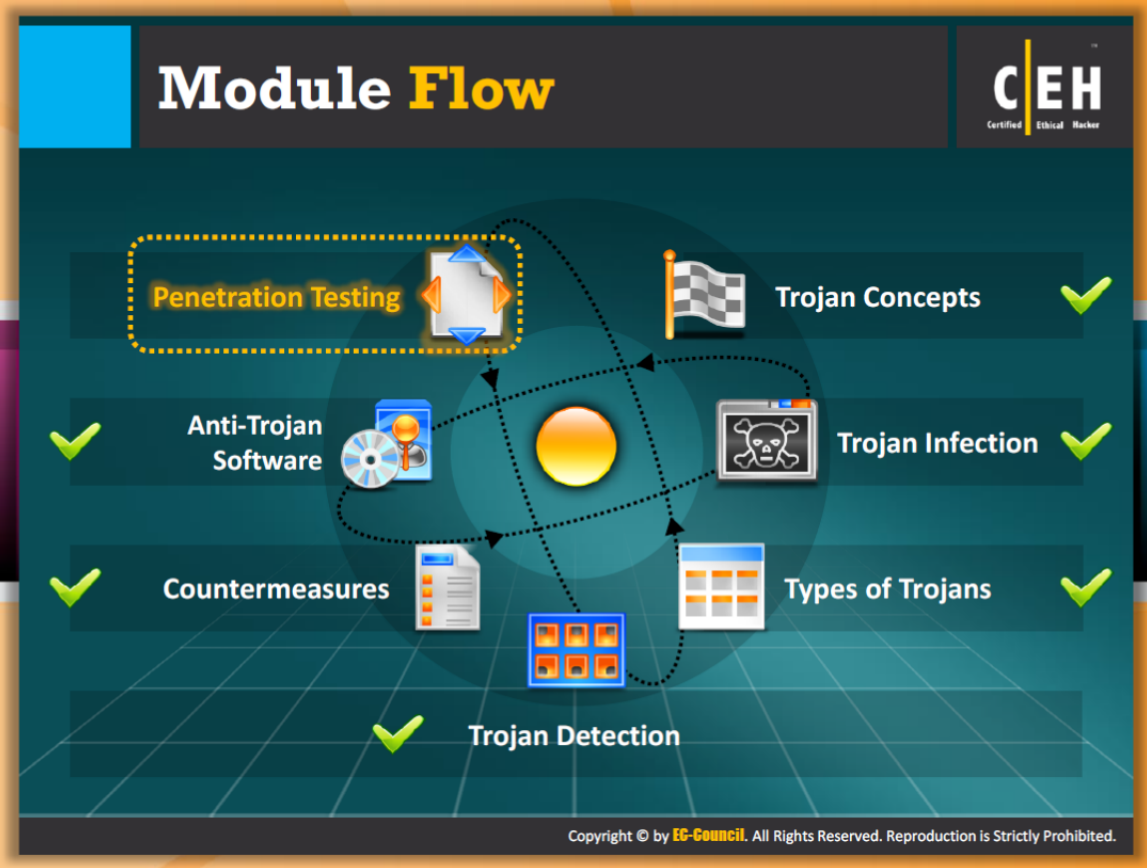
FIGURE 6.66: Emsisoft Anti-Malware



Anti-Trojan Software

Anti-Trojan software provides protection to your **computer system** and the information stored on it by blocking various malicious threats such as Trojans, worms, viruses, backdoors, malicious ActiveX controls, and Java applets to enter your system. A few of the anti-Trojan software programs that are used for the purpose of killing malware are listed as follows:

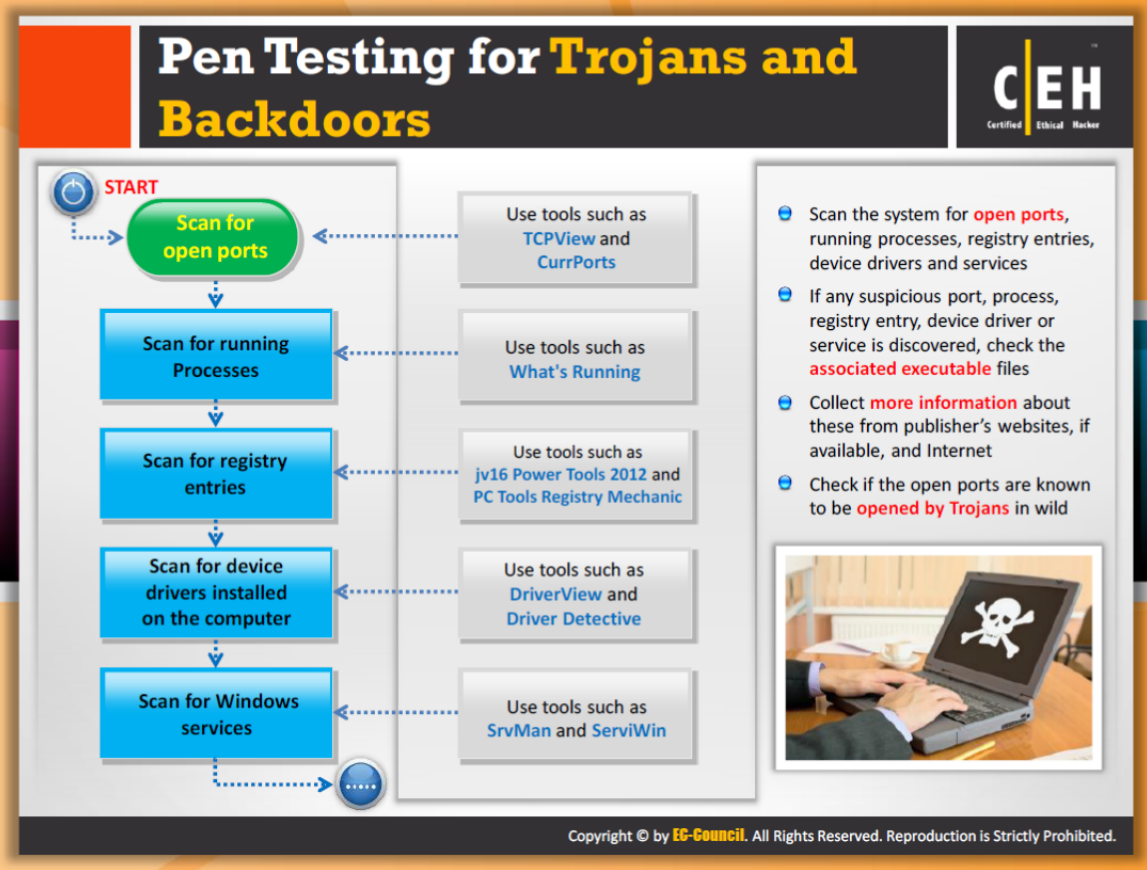
- Anti-Trojan Shield (ATS) available at http://www.atshield.com
- Spyware Doctor available at http://www.pctools.com
- Anti Malware BOClean available at http://www.comodo.com
- Anti Hacker available at http://www.hide-my-ip.com
- XoftSpySE available at http://www.paretologic.com
- SPYWAREfighter available at http://www.spamfighter.com
- Anti Trojan Elite available at http://www.remove-trojan.com
- SUPERAntiSpyware available at http://www.superantispyware.com
- Trojan Remover available at http://www.simplysup.com
- Twister Antivirus available at http://www.filseclab.com



Module Flow

As a penetration tester, you should follow the same strategies as that of an attacker to test your network or system against **Trojan and backdoor attacks**. You should perform all the available attacking techniques including the newly emerged attacking techniques. This allows you to figure out the loopholes or vulnerabilities in the target organization's security. If you find any vulnerabilities or loopholes, you should suggest countermeasures that can make the organization's security better and stronger.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	



Pen Testing for Trojans and Backdoors

Step 1: Scan for open ports

Open ports are the **primary sources** to launch attacks. Therefore, in an attempt to make your network secure by conducting pen testing, you should find the open ports and protect them. You can find the unnecessary open ports by scanning for open ports. For this purpose, you can use the tools such as **TCPView** and **CurrPorts**.

Step 2: Scan for running processes

Most Trojans don't require the user to **start the process**. They start automatically and don't even notify the user. This kind of Trojan can be detected by **scanning for running processes**. In order to scan for running processes, you can use tools such as What's Running, which scans your system and lists all currently active programs, processes, services, modules, and network connections. It also includes special areas to display **startup programs**.

Step 3: Scan for registry entries

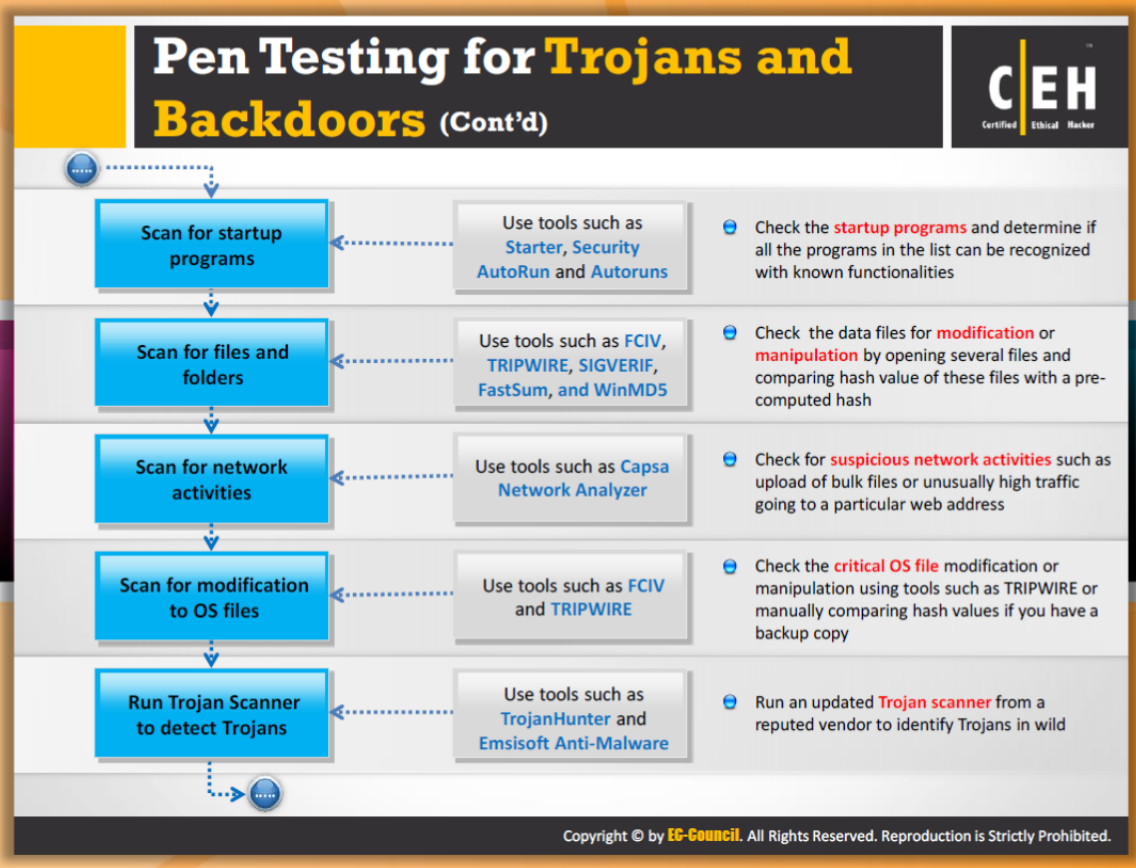
A few Trojans run in the **background** without any notification to the system's user. If you want to test for such Trojans, then you should scan for registry entries. This can be done with the help of tools such as JV Power Tools and PC Tools Registry Mechanic.

Step 4: Scan for device drivers installed on the computer

In order to control the hardware, most modern **OSes** use their own device drivers. Attackers can take advantage of this situation to spread **Trojans** and **backdoors** through device driver files. Trojans spread through device drivers infect the device driver files and other processes.

Step 5: Scan for Windows services

If you find any of the Windows services suspicious, then check the associated executable files. To scan Windows services, you can use the tools such as SrvMan and ServiWin.



Pen Testing for Trojans and Backdoors (Cont'd)

Step 6: Scan for startup programs

Some Trojans run automatically when you start **Windows**. Therefore, scan for Startup programs using tools such as Starter, Security AutoRun, and Autoruns and check the listed startup programs and determine if all the programs in the list can be recognized with known functionalities.

Step 7: Scan for files and folders

The easy way for an attacker to hack a system is with the use of files embedded with Trojan packages. Firewalls, IDSes, and other security mechanisms may fail to prevent this kind of attack. Therefore, you need to scan all files and folders for **Trojans and backdoors**. You can scan files and folders using tools such as FCIV, TRIPWIRE, SIGVERIF, FastSum, and WinMD5.

Step 8: Scan for network activities

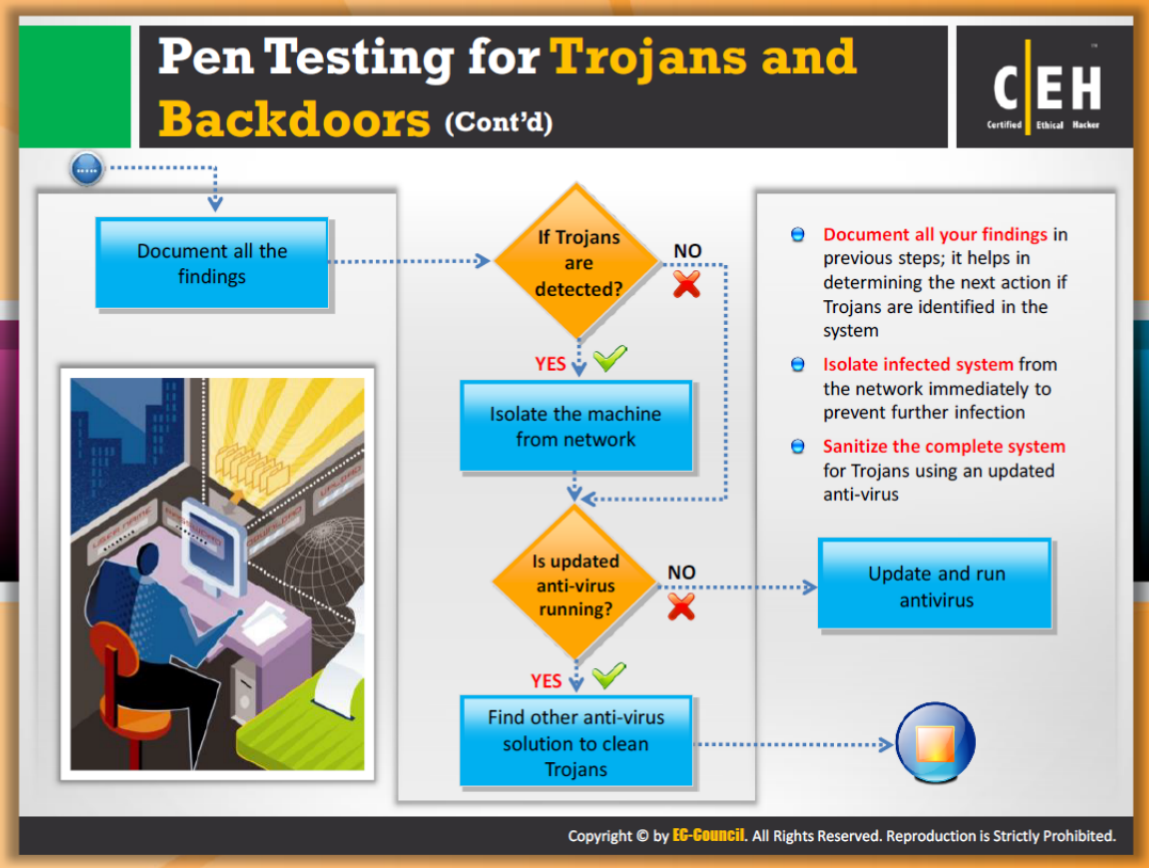
Network activities such as upload of **bulk files** or unusually high traffic going to a particular web address may sometimes represent a sign of Trojan. You should scan for such **network activities**. Tools such as Capsa Network Analyzer can be used for this purpose.

Step 9: Scan for modification to OS files

Check the critical OS file modification or manipulation using tools such as **TRIPWIRE** or manually compare hash values if you have a backup copy.

Step 10: Run Trojan Scanner to detect Trojans

Trojan scanners such as **Trojan Hunter** and **Emsisoft Anti-Malware** are readily available in the market. You can install and run those Trojan scanners to detect Trojans on your system.



Pen Testing for Trojans and Backdoors (Cont'd)

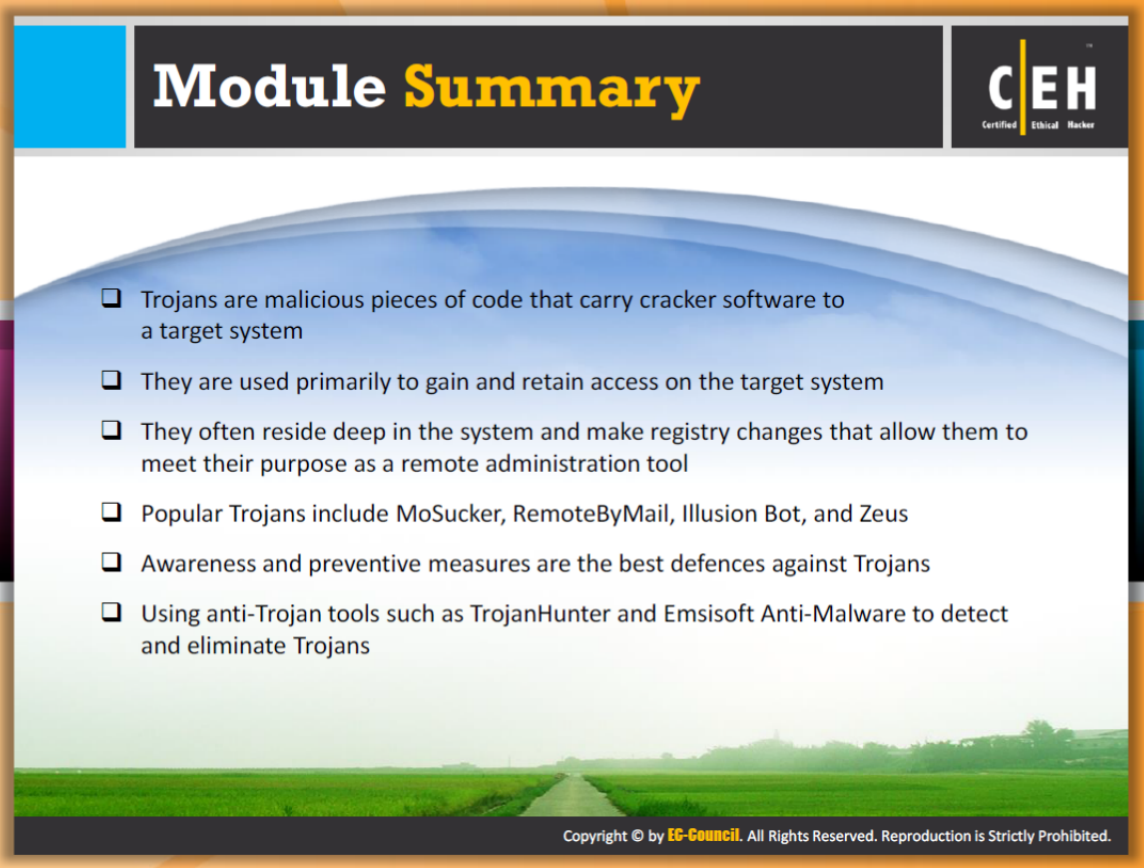
Step 11: Document all the findings

Once you conduct all possible tests to find the **Trojans**, document all the findings that you obtain at each **test for analysis** and check if there is any sign of a Trojan.

Step 12: Isolate the machine from the network

When you find a **Trojan on a machine**, you should isolate the machine immediately from the network before it takes control over other systems in the network. Check whether the antivirus software is updated or not.

If the antivirus is not updated, then update it and then run it to scan the system. If the antivirus is already updated, then find other antivirus solutions to **clean Trojans**.



Module Summary

- Trojans are malicious pieces of code that carry cracker software to a target system.
- They are used primarily to gain and retain access on the target system.
- They often reside deep in the system and make registry changes that allow them to meet their purpose as a remote administration tool.
- Popular Trojans include MoSucker, RemoteByMail, Illusion Bot, and Zeus.
- Awareness and preventive measures are the best defences against Trojans.
- Using anti-Trojan tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans.