4.6. Malware Threats

Trojans and backdoors are two ways a hacker can gain access to a target system. They come in many different varieties, but they all have one thing in common: they must be installed by another program, or the user must be tricked into installing the Trojan or backdoor on their system. Trojans and backdoors are potentially harmful tools in the ethical hacker's toolkit and should be used judiciously to test the security of a system or network.

Viruses and worms can be just as destructive to systems and networks as Trojans and backdoors. In fact, many viruses carry Trojan executables and can infect a system, then create a backdoor for hackers. This chapter will discuss the similarities and differences among Trojans, backdoors, viruses, and worms. All of these types of malicious code or malware are important to ethical hackers because they are commonly used by hackers to attack and compromise systems.

Trojans and Backdoors

Trojans and backdoors are types of malware used to infect and compromise computer systems. A ***Trojan*** is a malicious program disguised as something benign. In many cases the Trojan appears to perform a desirable function for the user but actually allows a hacker access to the user's computer system. Trojans are often downloaded along with another program or software package. Once installed on a system, they can cause data theft and loss, as well as system crashes or slowdowns. Trojans can also be used as launching points for other attacks, such as distributed denial of service (DDoS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts. Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel.

Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge. A Trojan can be sent to a victim system in many ways, such as the following:

- An instant messenger (IM) attachment
- IRC
- An email attachment
- NetBIOS file sharing
- A downloaded Internet program

Many fake programs purporting to be legitimate software such as freeware, spyware removal tools, system optimizers, screensavers, music, pictures, games, and videos can install a Trojan on a system just by being downloaded. Advertisements on Internet sites for free programs, music files, or video files lure a victim into installing the Trojan program; the program then has system-level access on the target system, where it can be destructive and insidious.

Common Trojan programs are,

Trojan	**Protocol**	**Port**
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-Mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Master's Paradise	TCP	3129, 40421, 40422, 40423, and 40426

A ***backdoor*** is a program or a set of related programs that a hacker installs on a target system to allow access to the system at a later time. A backdoor can be embedded in a malicious Trojan. The objective of installing a backdoor on a system is to give hackers access into the system at a time of their choosing. The key is that the hacker knows how to get into the backdoor undetected and is able to use it to hack the system further and look for important information.

Adding a new service is the most common technique to disguise backdoors in the Windows operating system. Before the installation of a backdoor, a hacker must investigate the system to find services that are running. Again the use of good information-gathering techniques is critical to knowing what services or programs are already running on the target system. In most cases the hacker installs the backdoor, which adds a new service and gives it an inconspicuous name or, better yet, chooses a service that's never used and that is either activated manually or completely disabled.

This technique is effective because when a hacking attempt occurs the system administrator usually focuses on looking for something odd in the system, leaving all existing services unchecked. The backdoor technique is simple but efficient: the hacker can get back into the machine with the least amount of visibility in the server logs. The backdoored service lets the hacker use higher privileges—in most cases, as a System account.

Remote Access Trojans *(RATs)* are a class of backdoors used to enable remote control over a compromised machine. They provide apparently useful functions to the user and, at the same time, open a network port on the victim computer. Once the RAT is started, it behaves as an executable file, interacting with certain Registry keys responsible for starting processes and sometimes creating its own system services. Unlike common backdoors, RATs hook themselves into the victim operating system and always come packaged with two files: the client file and the server file. The server is installed in the infected machine, and the client is used by the intruder to control the compromised system.

RATs allow a hacker to take control of the target system at any time. In fact one of the indications that a system has been exploited is unusual behavior on the system, such as the mouse moving on its own or pop-up windows appearing on an idle system.

Overt and Covert Channels

An ***overt channel*** is the normal and legitimate way that programs communicate within a computer system or network. A *covert channel* uses programs or communications paths in ways that were not intended.

Trojans can use covert channels to communicate. Some client Trojans use covert channels to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand. An unsuspecting intrusion detection system (IDS) sniffing the transmission between the Trojan client and server would not flag it as anything unusual. By using the covert channel, the Trojan can communicate or "phone home" undetected, and the hacker can send commands to the client component undetected.

Some covert channels rely on a technique called *tunneling*, which lets one protocol be carried over another protocol. **Internet Control Message Protocol** (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system. The ping command is a generally accepted troubleshooting tool, and it uses the ICMP protocol. For that reason, many router, switches, firewalls, and other packet filtering devices allow the ICMP protocol to be passed through the device. Therefore, ICMP is an excellent choice of tunneling protocols.

Types of Trojans

Trojans can be created and used to perform different attacks. Here are some of the most common types of Trojans:

Remote Access Trojans (RATs) Used to gain remote access to a system.

Data-Sending Trojans Used to find data on a system and deliver data to a hacker.

Destructive Trojans Used to delete or corrupt files on a system.

Denial-of-Service Trojans Used to launch a denial-of-service attack.

Proxy Trojans Used to tunnel traffic or launch hacking attacks via other systems.

FTP Trojans Used to create an FTP server in order to copy files onto a system.

Security Software Disabler Trojans Used to stop antivirus software.

How Reverse-Connecting Trojans Work

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network,

such as the reverse WWW shell server. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. The reverse WWW shell server uses standard HTTP. It's dangerous because it's difficult to detect: it looks like a client is browsing the Web from the internal network.

Wrappers are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run.

Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn't notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.

Trojan Construction Kit and Trojan Makers

Several Trojan-generator tools enable hackers to create their own Trojans. Such toolkits help hackers construct Trojans that can be customized. These tools can be dangerous and can backfire if not executed properly. New Trojans created by hackers usually have the added benefit of passing undetected through virus-scanning and Trojan-scanning tools because they don't match any known signatures.

Some of the Trojan kits available in the wild are Senna Spy Generator, the Trojan Horse Construction Kit v2.0, Progenic Mail Trojan Construction Kit, and Pandora's Box.

Trojan Countermeasures

Most commercial antivirus program have anti-Trojan capabilities as well as spyware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before they can cause damage. Once a system is infected, it's more difficult to clean, but you can do so with commercially available tools.

Although several commercially antivirus or Trojan removal tools are available, my personal recommendation is Norton Internet Security (Figure below). Norton Internet Security includes a

personal firewall, intrusion detection system, antivirus, antispyware, antiphishing, and email scanning. Norton Internet Security will clean most Trojans from a system as well.

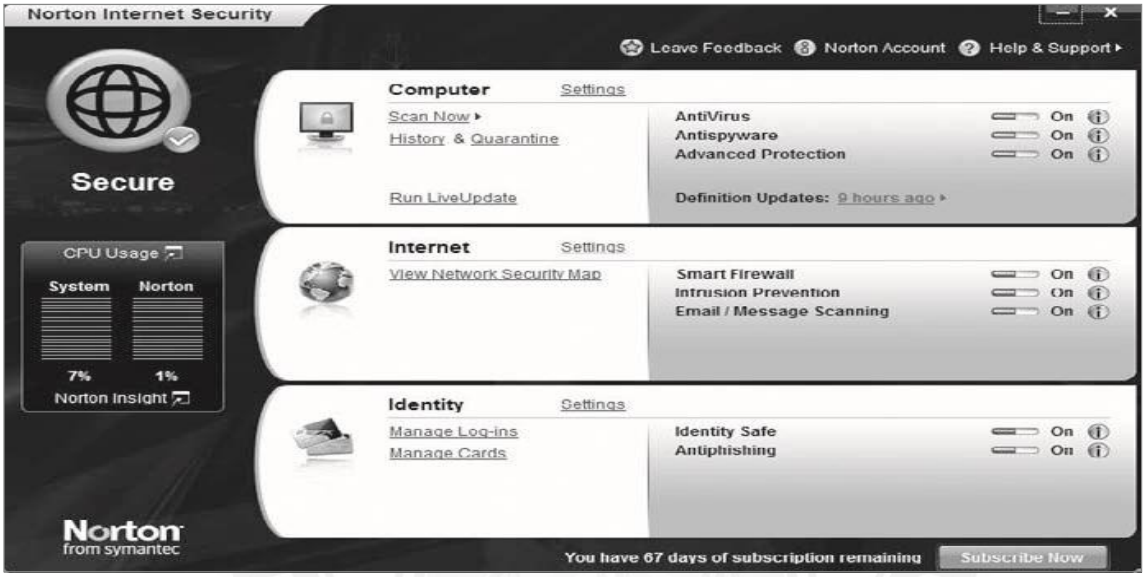
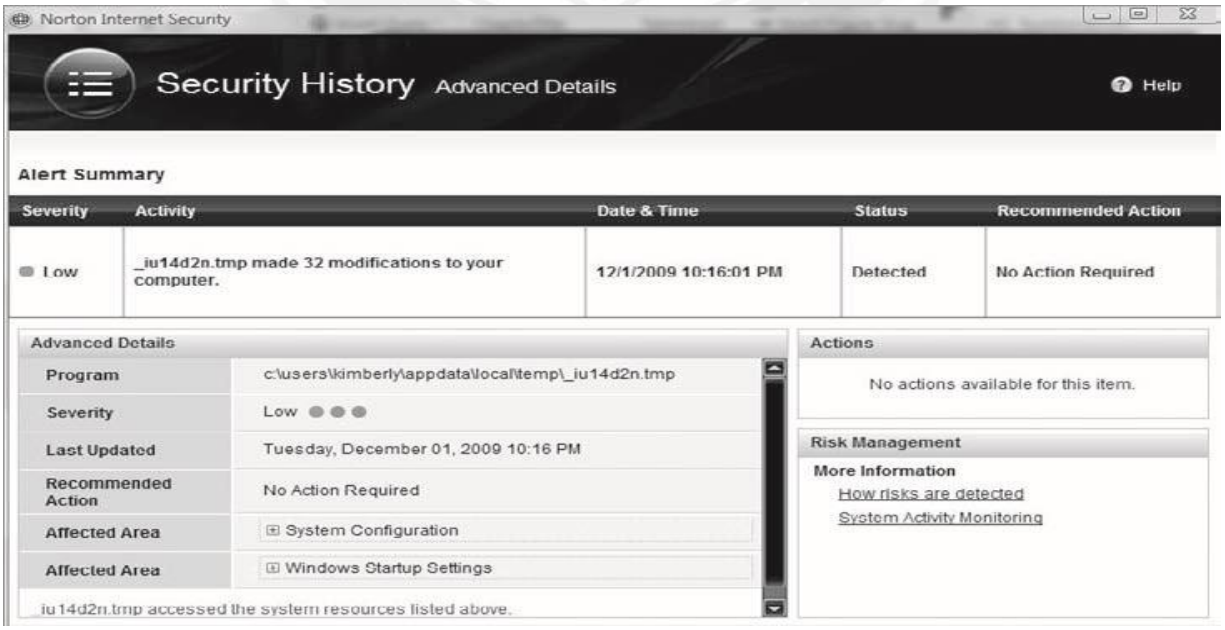


Fig: Norton Internet Security



The security software works by having known signatures of malware, such as Trojans and viruses. The repair for the malware is made through the use of definitions of the malware. When installing and using any personal security software or antivirus and anti-Trojan software, you must make sure that the software has all the current definitions. To ensure the latest patches and fixes are available, you should connect the system to the Internet so the software can continually update the malware definitions and fixes.

It's important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, a lot of commercial security software includes an intrusion detection component that will perform port monitoring and can identify ports that have been opened or files that have changed.

The key to preventing Trojans and backdoors from being installed on a system is to educate users not to install applications downloaded from the Internet or open email attachments from parties they don't know. Many system administrators don't give users the system permissions necessary to install programs on their system for that very reason. Proper use of Internet technologies should be included in regular employee security awareness training.

Checking a System with System File Verification

Windows 2003 includes a feature called Windows File Protection (WFP) that prevents the replacement of protected files. WFP checks the file integrity when an attempt is made to overwrite a SYS, DLL, OCX, TTF, or EXE file. This ensures that only Microsoft-verified files are used to replace system files.

Viruses and Worms

Viruses and worms can be used to infect a system and modify a system to allow a hacker to gain access. Many viruses and worms carry Trojans and backdoors. In this way, a virus or worm is a carrier and allows malicious code such as Trojans and backdoors to be transferred from system to system much in the way that contact between people allows germs to spread.

A *virus* and a *worm* are similar in that they're both forms of malicious software (*malware*). A virus infects another executable and uses this carrier program to spread itself. The virus code is

injected into the previously benign program and is spread when the program is run. Examples of virus carrier programs are macros, games, email attachments, Visual Basic scripts, and animations.

A worm is similar to a virus in many ways but does not need a carrier program. A worm can self-replicate and move from infected host to another host. A worm spreads from system to system automatically, but a virus needs another program in order to spread. Viruses and worms both execute without the knowledge or desire of the end user.

Types of Viruses

Viruses are classified according to two factors: what they infect and how they infect. A virus can infect the following components of a system:

- ✓ System sectors
- ✓ Files
- ✓ Macros (such as Microsoft Word macros)
- ✓ Companion files (supporting system files like DLL and INI files)
- ✓ Disk clusters
- ✓ Batch files (BAT files)
- ✓ Source code

A virus infects through interaction with an outside system. Viruses need to be carried by another executable program. By attaching itself to the benign executable a virus can spread fairly quickly as users or the system runs the executable. Viruses are categorized according to their infection technique, as follows:

Polymorphic Viruses These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.

Stealth Viruses These viruses hide the normal virus characteristics, such as modifying the original time and date stamp of the file so as to prevent the virus from being noticed as a new file on the system.

Fast and Slow Infectors These viruses can evade detection by infecting very quickly or very slowly. This can sometimes allow the program to infect a system without detection by an antivirus program.

Sparse Infectors These viruses infect only a few systems or applications.

Armored Viruses These viruses are encrypted to prevent detection.

Multipartite Viruses These advanced viruses create multiple infections.

Cavity (Space-Filler) Viruses These viruses attach to empty areas of files.

Tunneling Viruses These viruses are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.

Camouflage Viruses These viruses appear to be another program.

NTFS and Active Directory Viruses These viruses specifically attack the NT file system or Active Directory on Windows systems.

An attacker can write a custom script or virus that won't be detected by antivirus programs. Because virus detection and removal is based on a signature of the program, a hacker just needs to change the signature or look of the virus to prevent detection. The virus signature or definition is the way an antivirus program is able to determine if a system is infected by a virus. Until the virus is detected and antivirus companies have a chance to update virus definitions, the virus goes undetected. Additional time may elapse before a user updates the antivirus program, allowing the system to be vulnerable to an infection. This allows an attacker to evade antivirus detection and removal for a period of time. A critical countermeasure to virus infection is to maintain up-to-date virus definitions in an antivirus program.

One of the most longstanding viruses was the Melissa virus, which spread through Microsoft Word Macros. Melissa infected many users by attaching to the Word doc and then when the file was copied or emailed, the virus spread along with the file.

Virus Hoaxes are emails sent to users usually with a warning about a virus attack. The Virus Hoax emails usually make outlandish claims about the damage that will be caused by a virus and then offer to download a remediation patch from well-known companies such as

Microsoft or Norton. Other Hoaxes recommend users delete certain critical systems files in order to remove the virus. Of course, should a user follow these recommendations they will most certainly have negative consequences.

Common Virus Hoaxes

Name	Executable	Description
Antichrist	(none)	This is a hoax that warned about a supposed virus discovered by Microsoft and McAfee named "Antichrist", telling the user that it is installed via an email with the subject line: "SURPRISE?!!!!!!!!!!" after which it destroys the zeroth sector of the hard disk, rendering it unusable.
Budweiser Frogs	BUDSAVER.EXE	Supposedly would erase the user's hard drive and steal the user's screen name and password.
Goodtimes virus	(none)	Warnings about a computer virus named "Good Times" began being passed around among Internet users in 1994. The Goodtimes virus was supposedly transmitted via an email bearing the subject header "Good Times" or "Goodtimes," hence the virus's name, and the warning recommended deleting any such email unread. The virus described in the warnings did not exist, but the warnings themselves, were, in effect, virus-like.

Virus Detection Methods

The following techniques are used to detect viruses:

- Scanning
- Integrity checking with checksums
- Interception based on a virus signature

The process of virus detection and removal is as follows:

1. Detect the attack as a virus. Not all anomalous behavior can be attributed to a virus.
2. Trace processes using utilities such as handle.exe, listdlls.exe, fport.exe, netstat.exe, and pslist.exe, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced, or deleted files. New files, changed file attributes, or shared library files should be checked.
4. Acquire the infection vector and isolate it. Then, update your antivirus definitions and rescan all systems.