9.1.4 Trojan and Backdoor Facts

A hacker's goal is to gain and maintain access to a system. One method for maintaining access is to have a Trojan horse installed on the target system. The Trojan horse can open backdoors into the system it infects, providing the hacker with covert remote access. Backdoor programs are embedded and hidden inside legitimate programs. When the user runs that program, the Trojan horse runs in the background without the user's knowledge, giving the hacker remote access.

This lesson covers the following topics:

- Symptoms of an infection
- Types of Trojan horses
- Trojan horse creation
- Capabilities
- Communication channels
- Detection
- Countermeasures

Symptoms of an Infection

Trojan infection may be indicated by some of the following behaviors:

- Screen settings change by themselves.
- Chat boxes appear.
- Account passwords are changed.
- Legitimate accounts are accessed without authorization.
- Unknown purchase statements appear on credit card bills.
- Ctrl+Alt+Del stops working.

These are just a few of the symptoms. A general rule of thumb is that if a system begins experiencing weird abnormal actions, there's a decent chance it might be infected and should be examined.

Types of Trojan Horses

There are different types of Trojan horses. The resources that the Trojan attacks define the type it is. Some of the more common Trojan types are listed in the following table:

Trojan Type	Description	Example
Remote access Trojan (RAT)	RATs are one of the most prevalent types of Trojan horses. They provide a hacker with remote desktop GUI access to the victim machine and complete control over the system.	FatRat
Backdoor	A backdoor Trojan is very similar to the RAT. This Trojan also provides complete administrative access to the remote system and can bypass security such as a firewall or IDS. The main difference between the backdoor and a RAT is the backdoor does not provide a remote desktop GUI access, only a shell.	PoisonIvy
Botnet	A botnet controls a large number of computers to carry out an attack. Once installed on a system, the Trojan reports back to its command and control (C&C) center. From the C&C center, the hacker can control the machines to carry out attacks.	Kraken
Distributed Denial of Service (DDoS)	Computers infected with a DDoS Trojan become zombies and listen for the command to attack. When the command is given, all infected computers attack the target simultaneously. The attacks system is almost identical to a botnet; the only difference is the function.	ElectrumDoSMiner
Destructive	These Trojans are designed to delete files on the target machine. Once a destructive Trojan infects the system, it will randomly delete files.	W32.DisTrack (Shamoon)
Banker	Banker Trojans are also called e-Banking Trojans. These malware programs monitor the victim's computer and steal information related to financial records such as bank account, credit cards, and bill pay data.	Backswap
IoT	Internet of Things devices are the target of IoT Trojans. Smart thermostats, lighting systems, HVAC systems are examples of IoT devices that are are vulnerable to this type of Trojan horse.	Mirai
Proxy server	The proxy server Trojan is a standalone application that allows the remote hacker to use the victim's machine as a proxy to access the internet.	Proxy (Linux Trojan)

Defacement	The defacement Trojan has the ability to change the code and modify the contents of a database or a website. These Trojans can change the way a website or program looks and functions, making them extremely destructive.	Restorator
Gaming	A gaming Trojan focuses on stealing user account information from online gamers.	GameThief
Mobile	These Trojans target mobile devices. With the increase in mobile device usage, the use of this Trojans type is increasing rapidly.	Hummer
Security software disabler	The security software disabler stops the security programs, such as the firewall and IDS, from working. These Trojans are known as entry Trojans, as they provide access so the hacker can perform the next level of attack.	Certlock
Command shell	The command shell Trojan gives remote control of a command shell on the target. It does not necessarily provide full system access like a backdoor Trojan.	Netcat

Trojan Horse Creation

The most common way to create a Trojan horse is to use a construction kit. These programs allow the hacker to customize their Trojan. Most Trojan horse creation kits will perform all steps in the Trojan creation process. Once the Trojan horse has been created, it can be distributed using a variety of methods, including email, USB drives, and websites. The steps to create a Trojan horse are:

1. Create the server. This is the file that is dropped into the target machine and what the hacker will connect to.
2. Create the dropper. This is the part of the packet that will install the malicious code onto the target's machine.
3. Wrap the dropper and server into a genuine application file. A program called a Wrapper performs this function.

Capabilities

Once the Trojan horse has been installed on the victim’s machine, the hacker can perform all sorts of activities, including:

- Stealing data
- Installing other software
- Creating backdoors
- Recording from the webcam
- Modifying files

Communication Channels

There are two methods of communication for a Trojan horse, overt and covert. Overt communication is obvious, legitimate communication by the system. HTTP and TCP/IP are examples of overt communication. A channel can be exploited to create a covert channel by hiding communication inside of it. Covert communication is any method of conveying information in a hidden or illegitimate manner. Covert channels violate the security policy on the system. An example of covert communication is the Trojan horse communicating with its command and control center.

Detection

Detecting a Trojan horse can be difficult. The best way is to monitor network traffic and look for any suspicious network activity and open ports. The table below shows the most common ports and which Trojan horse programs use them.

Port	Trojans	Port	Trojans	Port	Trojans	Port	Trojans
2	Death	1492	FTP99CMP	8080	Zeus	1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT
20	Senna Spy	1600	Shivka-Burka	5569	Robo-Hack	21544	Girlfriend 1.0, Beta-1.35
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6670-71	DeepThroat	2222	Prosiak
22	Shaft, SSH RAT	1981	Shockrave	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7000	RemoteGrab	26274	Delta

25	Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth	2001	Trojan Cow	7300-08	NetMonitor	30100-02	NetSphere 1.27a
31	Hackers Paradise	2023	Ripper	7789	ICKiller	31337-38	Back Orifice, DeepBO
80	Poison Ivy, Executor	2115	Bugs	8787	BackOfrice 2000	31339	NetSpy DK
421	TCP Wrappers Trojan	2140	Deep Throat, The Invasor	9872-9875	Portal of Doom	31666	BOWhack
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	9989	iNi-Killer	33333	Prosiak
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	10607	Coma 1.0.9	34324	BigGluck, TN
666	Satanz Backdoor	3150	The Invasor	11000	Sennsa Spy	40412	The Spy
1001	Silencer, WebEx	4092	WinCrash	11223	Progenic Trojan	40421-26	Masters Paradise
1011	Doly Trojan	4567	File Nail 1	12223	Hack´99 KeyLogger	47262	Delta
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50505	Sockets de Troie
1170	Psyber Stream Server, Voice	5000	Bubbel	12361-62	Whack-a-mole	50766	Fore
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	53001	Remote Windows Shutdown
1243	Subseven 1.0-1.8	5321	Firehotcker	20001	Millennium	54321	SchoolBus .69-1.11
1245	VooDoo Doll	5400-02	Blade Runner 0.80 Alpha	20034	NetBus 2.0, Beta-NetBus 2.01	61466	Telecommando
1177	njRAT	1604	DarkComet RAT, Pandora RAT, HellSpy RAT	1863	XtremeRAT	65000	Devil
485	WannaCry, Petya	6666	KillerRat, HoudiniRAT	5000	SpyGate RAT, PunisherRAT		

Countermeasures

The best countermeasure to Trojan horse malware programs is to avoid getting them in the first place. Some basic guidelines to prevent infection are:

- Avoid opening email attachments
- Block unnecessary ports on firewall
- Do not install unknown programs
- Monitor network traffic
- Install and maintain malware software

If a system is infected, run in-depth scans with updated antivirus and anti-Trojan software. Additional steps may be needed, depending on the infection.