nuvollo

# What Is a Trojan Horse Virus?

**A Trojan Horse Virus** is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

Indications of a Trojan being active on a device include unusual activity such as computer settings being changed unexpectedly.

# History of the Trojan Horse

The original story of the Trojan horse can be found in the Aeneid by Virgil and the Odyssey by Homer. In the story, the enemies of the city of Troy were able to get inside the city gates using a horse they pretended was a gift. The soldiers hid inside the huge wooden horse and once inside, they climbed out and let the other soldiers in.

There are a few elements of the story that make the term "Trojan horse" an appropriate name for these types of cyber attacks:

- The Trojan horse was a unique solution to the target's defenses. In the original story, the attackers had laid siege to the city for 10 years and hadn't succeeded in defeating it. The Trojan horse gave them the access they had been wanting for a decade. A Trojan virus, similarly, can be a good way to get behind an otherwise tight set of defenses.
- The Trojan horse appeared to be a legitimate gift. In a similar vein, a Trojan virus looks like legitimate software.
- The soldiers in the Trojan horse controlled the city's defense system. With a Trojan virus, the malware takes control of your computer, potentially leaving it vulnerable to other "invaders."

## How Do Trojans Work?

Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device's system.

A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on.

Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites.

A computer infected by Trojan malware can also spread it to other computers. A cyber criminal turns the device into a zombie computer, which means they have remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.

For example, a user might receive an email from someone they know, which includes an attachment that also looks legitimate. However, the attachment contains malicious code that

executes and installs the Trojan on their device. The user often will not know anything untoward has occurred, as their computer may continue to work normally with no signs of it having been infected.

The malware will reside undetected until the user takes a certain action, such as visiting a certain website or banking app. This will activate the malicious code, and the Trojan will carry out the hacker's desired action. Depending on the type of Trojan and how it was created, the malware may delete itself, return to being dormant, or remain active on the device.

Trojans can also attack and infect smartphones and tablets using a strand of mobile malware. This could occur through the attacker redirecting traffic to a device connected to a Wi-Fi network and then using it to launch cyberattacks.

## Most Common Types of Trojan Malware

There are many types of Trojan horse viruses that cyber criminals use to carry out different actions and different attack methods. The most common types of Trojan used include:

1. **Backdoor Trojan**: A backdoor Trojan enables an attacker to gain remote access to a computer and take control of it using a backdoor. This enables the malicious actor to do whatever they want on the device, such as deleting files, rebooting the computer, stealing data, or uploading malware. A backdoor Trojan is frequently used to create a botnet through a network of zombie computers.
2. **Banker Trojan**: A banker Trojan is designed to target users' banking accounts and financial information. It attempts to steal account data for credit and debit cards, e-payment systems, and online banking systems.
3. **Distributed denial-of-service (DDoS) Trojan**: These Trojan programs carry out attacks that overload a network with traffic. It will send multiple requests from a computer or a group of computers to overwhelm a target web address and cause a denial of service.
4. **Downloader Trojan**: A downloader Trojan targets a computer that has already been infected by malware, then downloads and installs more malicious programs to it. This could be additional Trojans or other types of malware like adware.
5. **Exploit Trojan**: An exploit malware program contains code or data that takes advantage of specific vulnerabilities within an application or computer system. The cyber criminal will target users through a method like a phishing attack, then use the code in the program to exploit a known vulnerability.
6. **Fake antivirus Trojan**: A fake antivirus Trojan simulates the actions of legitimate antivirus software. The Trojan is designed to detect and remove threats like a regular antivirus program, then extort money from users for removing threats that may be nonexistent.
7. **Game-thief Trojan**: A game-thief Trojan is specifically designed to steal user account information from people playing online games.
8. **Instant messaging (IM) Trojan**: This type of Trojan targets IM services to steal users' logins and passwords. It targets popular messaging platforms such as AOL Instant Messenger, ICQ, MSN Messenger, Skype, and Yahoo Pager.

9. **Infostealer Trojan**: This malware can either be used to install Trojans or prevent the user from detecting the existence of a malicious program. The components of infostealer Trojans can make it difficult for antivirus systems to discover them in scans.
10. **Mailfinder Trojan**: A mailfinder Trojan aims to harvest and steal email addresses that have been stored on a computer.
11. **Ransom Trojan**: Ransom Trojans seek to impair a computer's performance or block data on the device so that the user can no longer access or use it. The attacker will then hold the user or organization ransom until they pay a ransom fee to undo the device damage or unlock the affected data.
12. **Remote access Trojan**: Similar to a backdoor Trojan, this strand of malware gives the attacker full control of a user's computer. The cyber criminal maintains access to the device through a remote network connection, which they use to steal information or spy on a user.
13. **Rootkit Trojan**: A rootkit is a type of malware that conceals itself on a user's computer. Its purpose is to stop malicious programs from being detected, which enables malware to remain active on an infected computer for a longer period.
14. **Short message service (SMS) Trojan**: An SMS Trojan infects mobile devices and is capable of sending and intercepting text messages. This includes sending messages to premium-rate phone numbers, which increases the costs on a user's phone bill.
15. **Spy Trojan**: Spy Trojans are designed to sit on a user's computer and spy on their activity. This includes logging their keyboard actions, taking screenshots, accessing the applications they use, and tracking login data.
16. **SUNBURST**: The SUNBURST trojan virus was released on numerous SolarWinds Orion Platform. Victims were compromised by trojanized versions of a legitimate SolarWinds digitally signed file named: SolarWinds.Orion.Core.BusinessLayer.dll. The trojanized file is a backdoor. Once on a target machine, it remains dormant for a two-week period and will then retrieve commands that allow it to transfer, execute, perform reconnaissance, reboot and halt system services. Communication occurs over http to predetermined URI's.

## How To Recognize a Trojan Virus

A Trojan horse virus can often remain on a device for months without the user knowing their computer has been infected. However, telltale signs of the presence of a Trojan include computer settings suddenly changing, a loss in computer performance, or unusual activity taking place. The best way to recognize a Trojan is to search a device using a Trojan scanner or malware-removal software.

nuvollo

# How To Protect Yourself from Trojan Viruses

A Trojan horse virus can often remain on a device for months without the user knowing their computer has been infected. However, telltale signs of the presence of a Trojan include computer settings suddenly changing, a loss in computer performance, or unusual activity taking place. The best way to recognize a Trojan is to search a device using a Trojan scanner or malware-removal software.

## Examples of Trojan Horse Virus Attacks

Trojan attacks have been responsible for causing major damage by infecting computers and stealing user data. Well-known examples of Trojans include:

1. **Rakhni Trojan:** The Rakhni Trojan delivers ransomware or a cryptojacker tool—which enables an attacker to use a device to mine cryptocurrency—to infect devices.
2. **Tiny Banker:** Tiny Banker enables hackers to steal users' financial details. It was discovered when it infected at least 20 U.S. banks.
3. **Zeus or Zbot:** Zeus is a toolkit that targets financial services and enables hackers to build their own Trojan malware. The source code uses techniques like form grabbing and keystroke logging to steal user credentials and financial details.

(Article from Fortinet website)