What is Trojan? How to avoid Trojan horse virus

A Trojan or Trojan horse is a type of malicious code or software that can take control of a user's computer remotely.

Trojans are one of the most common threats on the internet, affecting individuals and businesses. Trojans can not only steal personal information but also put you at risk of identity theft and other serious damage. In this article, let's learn with ***TipsMake*** what Trojan viruses are, how they work, and how you can protect yourself from them so you can operate safely online.

What is Trojan?

1. Definition

A Trojan horse, also known as a **Trojan** virus , is a type of malicious code or software that appears legitimate but actually takes control of a user's computer. The purpose of creating a Trojan is to cause damage, sabotage, steal information, or in general, perform harmful actions on a person's data or network.

A Trojan often acts like a real application or file in order to trick users. This malicious virus will intentionally trick users into downloading and using malware on their devices. Once installed, a Trojan can perform pre-programmed actions.

Trojans are sometimes also called Trojan viruses or Trojan horse viruses, however, this is incorrect. Viruses can run and replicate themselves, whereas Trojans cannot. The user is the one who runs these Trojans. However, Trojan malware and Trojan viruses are often used interchangeably.

However, no matter what you call this software, it is important to know how this virus works so that you can deal with it and protect your system.

2. How does Trojan work?

- A Trojan horse is a computer program that disguises itself as a useful program and has desired functions, or at least appears to have these functions. It secretly performs other unwanted operations. The desired functions are just a facade to hide these operations.

- In fact, many Trojan horses contain spyware that allows the client computer to be controlled remotely over the network.

- The fundamental difference with a computer virus is that a Trojan Horse is technically just a regular software and is not meant to propagate itself. These programs only trick the user into performing other operations that the client would not voluntarily allow to be performed. Nowadays, Trojan horses have added self-distributing functions. This pushes the concept of a Trojan horse closer to the concept of a virus and they become difficult to

distinguish.

3. Example of Trojan horse virus

- A simple example of a Trojan horse is a program called "SEXY.EXE" posted on a Web site with the promise of "sexy pictures"; but, when run, the program deletes all the files on the computer and displays teasing messages.

- A sample Trojan horse is available at www.freewebs.com/em_ce_do/doctor.exe. This program will automatically shut down the computer when run and will copy itself to the "StartUp" folder so that the computer will automatically shut down every time it is started. This Trojan horse will self-destruct after an hour or can be removed by booting into command prompt mode and then deleting the file using the delete command. This program only runs on Windows XP.

4. Tips

- On Microsoft Windows machines, an attacker can attach a Trojan horse with a seemingly innocent name to an email message, enticing the recipient to open the attachment. Trojan horses are typically executable files on Windows and will therefore have extensions such as .exe, .com, .scr, .bat, or .pif. Many Windows applications are configured by default to not display these extensions. Therefore, if a Trojan horse has a name such as "Readme.txt.exe", the file will display by default as "Readme.txt" and this will fool the user into thinking it is just a harmless text file.

- Icons can also be assigned to different types of files and can be attached to e-mails. When users open these icons, hidden Trojan horses will carry out unexpected damage. Currently, Trojan horses not only delete files, secretly adjust the configuration of the infected computer but also use this computer as a base to attack other computers on the network.

- Exploiting some web browser bugs, such as Internet Explorer, to embed Trojans into a website, when users view this page they will be infected. Users should update patches regularly and use a highly secure web browser such as Firefox and Google Chrome.

The harmful effects of Trojans on the system

Following are the common activities that Trojan will do to the infected user's computer system:

- Erase or rewrite data on the computer.

- Damage the functionality of files.

- Infect with other malicious software such as viruses.

- Set up the network so that the machine can be controlled by another machine or use the infected machine to send corrupt emails.

- Sneak through necessary information and send reports elsewhere.

- Steal information such as passwords and credit card numbers.

- Read bank account details and use them for criminal purposes.

- Install unauthorized software.

How Trojan virus works

Trojans work by masquerading as legitimate files, with the aim of tricking victims into clicking, opening, or installing them. When this happens, the Trojan begins installing malware on your device, spying on you, or causing other types of harm.

For example, email Trojans spread through legitimate-looking emails and email attachments, which are spammed to reach as many people's inboxes as possible. When the email is opened and the malicious attachment is downloaded, a Trojan server is installed and automatically runs every time the infected device is turned on.

Devices can also be infected with Trojans through social engineering tactics, which cybercriminals use to coerce users into downloading a malicious app. Malicious files can be hidden in banner or pop-up ads, or links on websites.

A computer infected with Trojan malware can also spread to other computers. A cybercriminal turns a device into a zombie computer, meaning they have remote control over it without the user knowing. The hacker can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.

For example, a user may receive an email from someone they know that contains an attachment that appears legitimate. However, the attachment contains malicious code that executes and installs a Trojan on their device. The user will often be unaware that anything has happened as their computer may continue to function normally with no indication that it has been infected.

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

Trojans can also attack and infect smartphones and tablets using a variety of mobile malware. This can happen through attackers redirecting traffic to a device connected to a Wi-Fi network and then using it to carry out cyber attacks.

Some common types of Trojan viruses

Some of the most common Trojan viruses include:

1. Backdoor Trojan

This type of Trojan allows hackers to access and control a computer remotely, usually for the purpose of uploading, downloading, or executing files at will.

2. Exploit Trojan

These trojans inject a machine with code that is deliberately designed to take advantage of an inherent weakness in a particular piece of software.

3. Rootkit Trojan

These trojans are intended to prevent the detection of malware that has infected the system so that it can prolong the malicious program, causing maximum damage.

4. Banker Trojan

This Trojan targets your financial accounts. It is designed to steal your account information for everything you do online, including banking data, credit cards, and bill payments.

5. DDoS Trojan

They are programmed to perform DDoS attacks, in which a network or machine is disabled by a flood of requests originating from multiple sources.

6. Downloader Trojan

This Trojan targets your already infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

Signs that your computer is infected with Trojan

Here are the signs that your computer is infected with Trojan:

- Slow computer speed: The computer runs slower than usual, especially when opening applications or files.

- Strange windows appear: Strange notifications or windows appear on the screen without the user's permission. These windows often contain advertisements or fake information.

-Automatically downloading programs: If you see new applications or tools appearing that you don't remember installing, this could be a sign of a Trojan.

- Lost or hidden data: Some files and folders may be deleted or hidden for no apparent reason.

- Security notice from antivirus software: If your antivirus program detects threats but cannot fix them, or if it is disabled without you knowing the reason, this is also a sign of a Trojan.

- Computer restarts or shuts down automatically: Unusual behavior such as the computer restarting itself repeatedly or failing to boot normally can also indicate a Trojan infection.

- Unable to access system tools: You may have difficulty when trying to open Task Manager, Control Panel or Registry Editor, this often happens when the computer is infected with malware.

- Unusual hardware behavior: Devices such as CD-ROM drives opening/closing automatically or printers automatically printing text without user commands are also warning signs.

How to prevent Trojan virus

To protect yourself from Trojan malware, here's what you need to do:

1. Secure your computer by installing and running anti-virus software.
2. Update your operating system software as soon as new updates are available to avoid security holes that cybercriminals can exploit in outdated software programs. You should also check for updates to other software you use on your computer.
3. Protect your account with strong, complex passwords, enable 2-way authentication, use a password manager
4. Back up your files regularly so you can restore data in case of an attack.
5. Use a firewall. While most operating systems have built-in firewalls, you should also use a hardware firewall for complete protection.
6. Be cautious with email attachments. To help stay safe, scan email attachments first, and never click on suspicious email attachments. Use spam filters to prevent most phishing emails from reaching your inbox.
7. Never visit insecure websites. Only visit URLs that begin with HTTPS.
8. Do not download or install suspicious software/programs that you do not fully trust.

Popular Trojan antivirus software

Not all antivirus software is capable of detecting Trojan viruses. In fact, many free or low-cost options may actually be malware in disguise! That's why it's important to choose the best solutions that can ensure top-notch security for your devices. Here are some suggestions:

1. Norton

Norton is a globally recognized and trusted security suite with an impressive 100% detection rate. Using Norton, you can easily scan all known Trojan viruses, quarantine infected files, and remove any threats from your system.

2. BitDefender

Known as one of the most reliable antivirus programs, BitDefender excels at identifying malware and recovering from problems quickly. It offers real-time protection and web filtering, with a 100% Trojan virus detection rate.

3. Avira

Avira is also one of the most popular antivirus brands out there, and its Trojan virus detection and removal rates are quite impressive. Avira offers a pretty good free version, but it also has a paid option with additional features.

Questions related to Trojan

Question: What are the common types of Trojans?

Answer: Some common types include:

1. Trojan Backdoor: Allows attackers to access computers remotely.
2. Trojan Rootkit: Hides the existence of other malware.
3. Data-Sending Trojans: Record and send personal information to the attacker.
4. Destructive Trojans: Capable of causing great harm to computer systems by deleting important data or corrupting operating system settings
5. Trojan-banker: Aims to steal financial information such as credit card numbers, CVV numbers, and banking information.

Question: What is the difference between a Trojan and a virus?

Answer: While viruses replicate themselves and spread from one computer to another, Trojans often sneak into the system without replicating themselves.

Question: How to know if your computer is infected with Trojan?

Answer: Some signs include:

1. CD-ROM drive opens/closes automatically.
2. The screen shows strange signs.
3. The system frequently crashes or fails.
4. Automatically download and install applications.
5. Security software is disabled.

Question: What are the symptoms that indicate a computer is infected with a Trojan?

Answer: Symptoms may include: changing wallpaper, automatically printing text, or restarting the computer for no reason.

Question: What is an effective way to prevent Trojans?

Answer: Use anti-virus software, do not download files from unknown sources, and regularly update your operating system and security software.

Question: If I find my computer is infected with a Trojan, what should I do?

Answer: Immediately disconnect from the internet, scan the system with anti-virus software and change passwords for important accounts.

Question: What damage can a Trojan cause to a user?

Answer: Trojans can steal personal information, destroy data, control computers remotely, and infect the system with other types of malware.

Source: TipsMake share