DEFINITION

Trojan horse

Casey Clark, TechTarget

Michael Cobb

What is a Trojan horse?

In computing, a Trojan horse is a program downloaded and installed on a computer that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.

Typically, the Trojan horse is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware hidden inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

How a Trojan horse works

Before a Trojan horse can infect a machine, the user must download the server side of the malicious application. The Trojan horse cannot manifest by itself. The executable file (.exe file) must be implemented and the program must be installed in order for the attack to be unleashed on the system. Social engineering tactics are often used to convince end users to download the malicious application. The download trap may be found in banner ads, website links or pop-up advertisements.

However, the most popular tactic for spreading Trojan horses is through seemingly unthreatening emails and email attachments. Trojan horse developers frequently use spamming techniques to send their emails to hundreds or thousands of people. As soon as the email has been opened and the attachment has been downloaded, the Trojan server will be installed and will run automatically each time the computer turns on.

It is also possible for an infected computer to continue spreading the Trojan horse to other computers, creating a botnet. This is accomplished by turning an innocent computer into a zombie computer, meaning the person using the infected computer has no idea it is being controlled by somebody else. Hackers use these zombie computers to continue dispersing additional malware to create a whole network of zombie computers.

Laptop and desktop computer users are not the only ones who are at risk of a Trojan horse infection. Trojans can also attack mobile devices, such as smartphones and tablets with mobile malware. This form of infection could result in an attacker redirecting traffic on these Wi-Fi connected devices and using them to commit cybercrimes.

Here is one example of how a Trojan horse might be used to infect a personal computer:

The victim receives an official-looking email with an attachment. The attachment contains malicious code that is executed as soon as the victim clicks on the attachment. Because nothing bad happens and the computer continues to work as expected, the victim does not suspect that the attachment is actually a Trojan horse, and his computing device is now infected.

The malicious code resides undetected until a specific date or until the victim carries out a specific action, such as visiting a banking website. At that time, the trigger activates the malicious code and carries out its intended action. Depending upon how the Trojan has been created, it may delete itself after it has carried out its intended function, it may return to a dormant state or it may continue to be active.

Uses of a Trojan horse

When a Trojan horse becomes active, it puts sensitive user data at risk and can negatively impact performance. Once a Trojan has been transferred, it can:

- give the attacker backdoor control over the computing device;
- record keyboard strokes to steal the user's account data and browsing history;
- download and install a virus or worm to exploit a vulnerability in another program;
- install ransomware to encrypt the user's data and extort money for the decryption key;
- activate the computing device's camera and recording capabilities;
- turn the computer into a zombie computer that can be used to carry out click fraud schemes or illegal actions;
- legally capture information relevant to a criminal investigation for law enforcement.

Examples of Trojan horses

Over the years, Trojan horses have been discovered by antimalware vendors, security researchers and private individuals. Some of the most famous discoveries include:

- Bitfrost, a remote access Trojan (RAT) that infected Windows clients by changing, creating and altering components.
- Tiny Banker, which allowed attackers to steal sensitive financial information. Researchers in the Center for Strategic and International Studies Security Group identified "Tinba" in 2012 after two dozen major U.S. banks were infected.
- FakeAV Trojan, which embedded itself in the Windows system tray and continuously delivered an official-looking pop-up window, alerting the user to a problem with the computer. When users followed directions to fix the problem, they actually downloaded more malware.
- Magic Lantern, a government Trojan that uses keystroke logging, created by the FBI around the turn of the century to assist with criminal surveillance.
- Zeus, a financial services crimeware toolkit that allows a hacker to build their own Trojan horse. First detected in 2007, the Trojans built with Zeus still remain the most dangerous banking Trojans in the world, using form grabbing, keylogging and polymorphic variants of the Trojan that use drive-by downloads to capture victim credentials.

Other common types of Trojan horses include:

- Downloader Trojan, which is a Trojan that targets a computer already affected by downloading and installing new versions of malicious programs.
- Backdoor Trojan, which creates a backdoor on the computer, enabling an attacker's access and control of the computer. Backdoor Trojans can allow data to be downloaded by third parties or stolen as well as additional malware to be uploaded.

- Distributed Denial of Service (DDoS) attack Trojan, which performs a DDoS attack on the computer and attempts to take down a network by flooding it with traffic that comes from the target infected computer and others.
- Game-thief Trojan, which targets online gamers and attempts to steal their account information.
- Mailfinder Trojan, which attempts to steal email addresses stored on a targeted device.
- SMS Trojan, which is a Trojan that infects mobile devices and has the ability to send or intercept text messages.
- Trojan banker, which attempts to steal financial accounts. This Trojan is designed to take the account information for all online activities, including credit card, banking and bill pay data.

Some additional Trojan types include Trojan-ArcBomb, Trojan-Clicker, Trojan-Proxy and Trojan-Notifier.

Is a Trojan horse a virus or malware?

A Trojan horse may also be referred to as a Trojan horse virus, but is technically incorrect. Unlike a computer virus, a Trojan horse is not able to replicate itself, nor can it propagate without an end user's assistance. Attackers must use social engineering tactics to trick the end user into executing the Trojan.

Since there are so many kinds of Trojan horses, the term can be used as a general umbrella for malware delivery. Depending on the attacker's intent and application structure, the Trojan can work in a multitude of ways -- sometimes behaving as standalone malware, other times serving as a tool for other activities like delivering payloads, opening the system up to attacks or communicating with the attacker.

How to identify a Trojan horse

Since Trojan horses frequently appear disguised as legitimate system files, they are often very hard to find and destroy with conventional virus and malware scanners. Specialized software tools are often necessary for the identification and removal of discrete Trojan horses.

However, it's possible to identify the presence a Trojan horse through unusual behaviors displayed by a computer. The quirks could include:

- A change in the computer's screen, including changing color andresolution or an unnecessary flip upside down.
- Excessive amounts of pop-up ads appear, offering solutions to various errors which might prompt the end user to click on the ad.
- The computer mouse may start moving by itself or freezing up completely and the functions of the mouse buttons may reverse.
- The browser's homepage may change or the browser will consistently redirect the user to a different website than the one they are requesting. This redirected website will often contain an offer that users can click on or download which will, in turn, install more malware.
- The computer's antivirus and antimalware programs will be disabled and the necessary steps to remove malware will be inaccessible.
- Mysterious messages and abnormal graphic displays may start appearing.
- Unrecognized programs will be running in the task manager.
- The taskbar will either change in appearance or completely disappear.
- The computer's desktop wallpaper may change as well as the format of desktop icons and applications.
- The user's personal email service may start sending spam messages to all or some of the addresses in the contact list that frequently contain malware and a persuasive tactic to get recipients to open and download the attack, thus spreading the Trojan horse to other computers.

It is necessary to note that safe, legitimate software applications can also cause some of the uncommon behaviors listed above. Furthermore, adware and potentially unwanted programs (PUPs) are sometimes confused with Trojan horses due to their similar delivery methods. For example, adware can sneak onto a computer while hiding inside a bundle of software. However, unlike Trojan horses, adware and PUPs do not

How to protect against a Trojan horse

The easiest way to protect a system from a Trojan horse is by never opening or downloading emails or attachments from unknown sources. Deleting these messages before opening will prevent the Trojan horse threat.

However, computer security begins with and depends on the installation and implementation of an internet security suite. Because the user is often unaware that a Trojan horse has been installed, antimalware software must be used to recognize malicious code, isolate it and remove it. To avoid being infected by a Trojan horse, users should keep their antivirus and antimalware software up to date and practice running periodic diagnostic scans.

Other tips for protecting a system include:

- Updating the operating system (OS) software as soon as the software company releases an update.
- Protecting personal accounts with complicated and unique passwords that contain numbers, letters and symbols.
- Using discretion with all email attachments, even those from recognized senders, since a Trojan horse could have infected their computer and is using it to spread malware.
- Backing up files on a regular basis so they can be easily recovered if a Trojan horse attack occurs.
- Protecting all personal information with firewalls.
- Avoiding suspicious and unsafe websites; Internet security software can sometimes be used to indicate which sites are safe and which should be avoided.
- Only installing or downloading programs from verified, trustworthy publishers.
- Refusing pop-up ads that attempt to entice users to click through for tempting offers and promotions.
- Never opening an email if the topic, content or sender is unknown or if there is any suspicion or question about the email in general.

How to remove a Trojan horse

If a Trojan horse is identified on a computer, the system should immediately be disconnected from the Internet and the questionable files should be removed using an antivirus or antimalware program or by reinstalling the operating system.

The hardest part of the removal process is recognizing which files are infected. Once the Trojan has been identified, the rest of the process becomes simpler. Users can sometimes find the infected files using the dynamic link library (DLL) error which is frequently presented by the computer to signify the presence of a Trojan horse. This error can be copied and searched online to find information about the affected .exe file.

Once the files are identified, the System Restore function must be disabled. If this function is not disabled, then all the malicious files that are deleted will be restored and will infect the computer once again.

Next, users must restart their computer. While restarting, users should press the F8 key and select safe mode. Once the computer has successfully started up, users should access Add or Remove programs in the control panel. From here, the infected programs can be removed and deleted. In order to ensure all extensions associated with the Trojan application are removed, all of the program files should be deleted from the system.

Once this is complete, the system should be restarted once again, but this time in the normal start-up mode. This should complete the Trojan horse removal process.

History of the Trojan horse

The term *Trojan horse* stems from Greek mythology. According to legend, the Greeks built a large wooden horse that the people of Troy pulled into the city. During the night, soldiers who had been hiding inside the horse emerged, opened the city's gates to let their fellow soldiers in and overran the city.

In computing, the term was first named in a 1974 U.S. Air Force report that discussed vulnerability in computer systems. It was later made popular by Ken Thompson when he received the Turing Award in 1983 -- an award given by the Association for Computing Machinery (ACM) to an individual of technical importance in the computer field.

During the 1980s, an increase in bulletin board systems (BBS) contributed to the accelerated spread of Trojan horse attacks. A BBS was a computer system that ran software that permitted users to penetrate the system using a phone line. Once a user was logged into the BBS, they could proceed with actions like uploading, downloading and sharing potentially malicious data.

The first Trojan horse virus was called the pest trap or Spy Sheriff. This early Trojan horse was able to reach and infect about one million computers around the world. It appears as a mass amount of pop-up ads that mostly looked like warnings, alerting users to the necessity of an obscure software application. Once the Spy Sheriff Trojan horse is successfully installed on a computer, it becomes extremely difficult to remove. Antivirus and antimalware software are usually unable to detect Spy Sheriff and cannot remove it with a system restore. Furthermore, if a user tries to erase the Spy Sheriff software, the Trojan horse reinstalls itself using hidden infected files on the computer.

In October 2002, a man was arrested after 172 images of child pornography were found on his computer's hard drive. It took almost a year for the court to finally acquit him of charges and accept his defense declaring that the files had been downloaded without his knowledge by a Trojan horse. This is one of the first cases in which the Trojan horse defense was successful.

Editor's note: *This article was republished in December 2022 to improve the reader experience.*

This was last updated in December 2022

Continue Reading About Trojan horse

- 10 common types of malware attacks and how to prevent them
- 7 common file sharing security risks

- 10 biggest data breaches in history, and how to prevent them
- 13 common types of cyber attacks and how to prevent them

Related Terms

antivirus software (antivirus program)

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other ... See complete definition

information security (infosec)

Information security (infosec) is a set of policies, procedures and principles for safeguarding digital data and other kinds of ... See complete definition

quantum supremacy

Quantum supremacy is the experimental demonstration of a quantum computer's dominance and advantage over classical computers by ... See complete definition

Dig Deeper on Data security and privacy

mobile malware

By: Casey Meserve

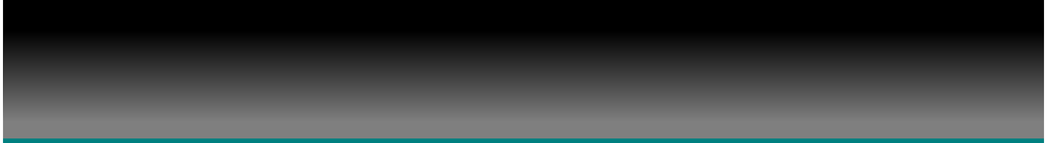
Dridex malware

By: Alexander Gillis

RAT (remote access Trojan)

By: Kinza Yasar

blended threat



By: Kinza Yasar

NETWORKING CIO ENTERPRISE DESKTOP CLOUD COMPUTING COMPUTER WEEKLY

Networking

Top 9 SD-WAN benefits for businesses

Make the case for an SD-WAN implementation, and explore the benefits and main use cases for SD-WAN in enterprises, beyond ...

White box networking use cases and how to get started

Rising cloud costs have prompted organizations to consider white box switches to lower costs and simplify network management. ...