

# A Trojan

(Malicious program not a Virus)

Amit P. Jadhav  
S.E. COMP (A)

**A Trojan**, sometimes referred to as a Trojan horse, is non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system. The term is derived from the Trojan horse story in Greek mythology. Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse.

Operations that could be performed by a hacker on a target computer system include:

- \* Use of the machine as part of a botnet (i.e. to perform spamming or to perform Distributed Denial-of-service (DDoS) attacks)
- \* Data theft (e.g. passwords, credit card information, etc.)
- \* Installation of software (including other malware)
- \* Downloading or uploading of files
- \* Modification or deletion of files
- \* Keystroke logging
- \* Viewing the user's screen
- \* Wasting computer storage space

Trojan horses require interaction with a hacker to fulfill their purpose, though the hacker need not be the individual responsible for distributing the Trojan horse. In fact, it is possible for hackers to scan computers on a

network using a port scanner in the hope of finding one with a Trojan horse installed, that the hacker can then use to control the target computer.

A trojan differs from a virus in that only a file specifically designed to carry it can do so.

## Installation and distribution

Trojan horses can be installed through the following methods:

- \* *Software downloads* (e.g., a Trojan horse included as part of a software application downloaded from a file sharing network)
- \* *Websites containing executable content* (e.g., a Trojan horse in the form of an ActiveX control)
- \* *Email attachments*
- \* *Application exploits* (e.g., flaws in a web browser, media player, messaging client, or other software that can be exploited to allow installation of a Trojan horse)

Also, there have been reports of compilers that are themselves Trojan horses.[citation needed] While compiling code to executable form, they include code that causes the output executable to become a Trojan horse.

**Removal**

Antivirus software is designed to detect and delete Trojan horses, as well as preventing them from ever being installed. Although it is possible to remove a Trojan horse manually, it requires a full understanding of how that particular Trojan horse operates. In addition, if a Trojan horse has possibly been used by a hacker to access a computer system, it will be difficult to know what damage has been done and what other problems have been

introduced. In situations where the security of the computer system is critical, it is advisable to simply erase all data from the hard disk and reinstall the operating system and required software.

SearchLight