

Title:

Trojan Horse

Word Count:

600

Summary:

The original trojan horse was built by Odysseus, the King of Ithica, during the legendary Trojan Wars. The Greeks were losing the siege of the city of Troy. Odysseus had a large wooden horse built and left as a "gift" outside the walls of the city of Troy. He then ordered the Greek army to sail away.

Keywords:

Trojan Horse

Article Body:

The original trojan horse was built by Odysseus, the King of Ithica, during the legendary Trojan Wars. The Greeks were losing the siege of the city of Troy. Odysseus had a large wooden horse built and left as a "gift" outside the walls of the city of Troy. He then ordered the Greek army to sail away.

The Trojans believed the horse to be a peace offering from Odysseus. Instead, the horse was filled with Greek warriors, including Odysseus and Menelaus. As the Trojans slept, the Greek army sailed back to Troy and the soldiers hiding in the wooden horse snuck out and opened the gates of the city for them.

The Computer Trojan Horse

A computer trojan horse is a program which appears to be something good, but actually conceals something bad.

One way to spread a trojan horse is to hide it inside a distribution of normal software. In 2002, the sendmail and OpenSSH packages were both used to hide trojan horses. This was done by an attacker who broke into the distribution sites for these software packages and replaced the original distributions with his own packages.

A more common method of spreading a trojan horse is to send it via e-mail. The attacker will send the victim an e-mail with an attachment called something like "prettygirls.exe." When the victim opens the attachment to see the pretty girls, the trojan horse will infect his system.

A similar technique for spreading trojan horses is to send files to unsuspecting users over chat systems like IRC, AIM, ICQ, MSN, or Yahoo Messenger.

The Trojan Horses Virus

Unlike viruses, trojan horses do not normally spread themselves. Trojan horses must be spread by other mechanisms.

A trojan horse virus is a virus which spreads by fooling an unsuspecting user into executing it.

An example of a trojan horse virus would be a virus which required a user to open an e-mail attachment in Microsoft Outlook to activate. Once activated, the trojan horse virus would send copies of itself to people in the Microsoft Outlook address book.

The trojan horse virus infects like a trojan horse, but spreads like a virus.

#### Effects of a Trojan Horse

The victim running the trojan horse will usually give the attacker some degree of control over the victim's machine. This control may allow the attacker to remotely access the victim's machine, or to run commands with all of the victim's privileges.

The trojan horse could make the victim's machine part of a Distributed Denial of Service (DDoS) network, where the victims machine is used to attack other victims.

Alternatively, the trojan horse could just send data to the attacker. Data commonly targeted by trojan horses includes usernames and passwords, but a sophisticated trojan horse could also be programmed to look for items such as credit card numbers.

#### Protecting Against a Trojan Horse

Anti-virus programs detect known trojan horses. However, trojan horse programs are easier to create than viruses and many are created in small volumes. These trojan horse programs will not be detected by anti-virus software.

The best defense against a trojan horse is to never run a program that is sent to you. E-mail and chat systems are not safe methods of software distribution.

#### Spyware and adware

Many people consider spyware and adware to be forms of a trojan horse.

Spyware programs perform a useful function, and also install a program that monitors usage of the victim's computer for the purpose of marketing to the user.

Adware programs are similiar to spyware programs, except the additional software they install shows advertising messages directly to the user.