

# Trojan Horses and

A Trojan horse program - "Trojan" for short - is a piece of computer software that provides intentionally hidden or covert functionality.

This definition includes a wide range of malicious software, such as keystroke loggers<sup>1</sup> and logic bombs<sup>2</sup>. However, the commonest types of Trojans are those that, once executed, enable attackers to bypass existing security measures to access a computer. Among these, the most effective incorporate a "rootkit" program designed to conceal their presence.

Trojans are usually network applications that typically comprise a server installed on the victim's computer and a client on the attacker's computer. The server listens for commands sent from the client and responds by returning data to the client. It is also possible for Trojans to be "peer-to-peer" applications, such as file sharing software or Internet Relay Chat (IRC). Although these types of applications may be installed by attackers on compromised machines, they are not Trojans in themselves.

Trojans, which are continually evolving, can undermine the central pillars of information security; **confidentiality**, **integrity**, and **availability**. For "stealthiness" reasons, they have an increasing tendency to make their network traffic appear as existing services in order to obscure their presence. For example, Setiri, a recent proof-of-concept Trojan, bypasses network intrusion detection devices and firewalls by using commands embedded in web traffic to communicate.

Rootkits designed to hide Trojans fall into three types: file system rootkits, library rootkits and kernel rootkits.

Traditional rootkits simply modify common user programs so that the Trojan is invisible to the system administrator when file and process listings are

made. A variation on the traditional rootkit replaces some system library functions with Trojan versions, thereby avoiding detection by a system administrator who was using checksum and file integrity checking software to identify changes to key programs. However, changes to library files are also likely to be detected by integrity checking software, although the system administrator may ignore the warning because new programs might at any rate require updated libraries.

The most sophisticated type of Trojan modifies some objects or processes that run with system privilege. Some techniques used by hackers are to:

- modify the system kernel executable file and its integrity checking;
- install a device driver, loadable kernel module or other program running at system level, and use it to modify the code executed by another system process;
- patch system memory or running processes.

Each of these techniques requires administrator access to load a system level executable or to patch a system file, while writing an effective rootkit of this kind also requires a good knowledge of system programming. There are, however, kernel rootkits available for both Windows (for example, NT Rootkit) and UNIX systems (for example, Adore/ava) and a number of do-it-yourself guides. It's important to appreciate that because kernel rootkits undermine the trusted computing base, they represent the most serious way in which a computer can be compromised.



"Trojans, trust not the horse. Whatever it be, I fear the Greeks, even when bringing gifts."

Virgil (70-19BC) - Aeneid, Book II

<sup>1</sup> Keystroke loggers - software that covertly monitors what is typed at the keyboard (including passwords).

<sup>2</sup> Logic bombs - software that can be triggered to damage data on your computer system.

# Kernel Rootkits

...an anti-virus or Trojan detection program might detect malicious software on your system, but it might not, especially if the system kernel has been compromised.

Common examples of Trojans - which should be detected by your organisation's firewall - are Subseven, *Back Orifice 2000 (BO2K)*, Netbus and distributed denial of service tools such as *Trinoo* and *Stacheldraht*. They provide a rich set of functionality, including:

- logging the victim's keystrokes (including passwords);
- representing the victim's screen on the attacker's computer;
- monitoring network traffic on the victim's network;
- hijacking TCP sessions involving the victim's computer;
- recording conversations via the victim computer's microphone or controlling a webcam;
- sending files from the victim's computer to the attacker;
- using the computer as a platform for attacks on other computers (denial of service, for example);
- using the compromised host for email, chat and file storage;
- modifying data on the victim's computer.

With a kernel rootkit installed a computer becomes totally untrustworthy and might not implement any of the security measures that the standard operating system implements.

A key message to conclude this brief overview of Trojans and rootkits is that **prevention is far better than cure**.

Fortunately there are a number of steps that you can use to reduce the chances of system compromise by a Trojan:

- follow good network security practice<sup>3</sup>;
- because e-mail is a common way for a Trojan to be sent to a victim's computer, block all *executable* mail attachments at the network

perimeter, or at the very least ensure that they are digitally signed by a trusted party;

- ensure that the security permissions of all users reflect least privilege (for example, restricting installation privileges to a sensible number of system administrators);
- follow the vendor's best practice security advice for operating system and application configuration;
- use an appropriate virus/Trojan scanner on a regular basis.

Least privilege can be hard to enforce, but system administrators should ensure that users have appropriate read, write and execute permissions on system objects, including keys in the Microsoft Windows registry.

If you suspect that your system has been compromised, an anti-virus or Trojan detection program might detect

malicious software on your system, but it might not, especially if the system kernel has been compromised. In general you will need to employ specialist analysis tools, perhaps through a specialist security consultant.

**N.I.S.C.C.** (<http://www.niscc.gov.uk>)

**Editor:** the major anti-virus software suppliers provide good descriptions of many Trojans (and viruses and worms) on their web sites. For example:

Sophos... <http://www.sophos.com/virusinfo/analyses/>

Symantec... <http://securityresponse.symantec.com/avcenter/vinfodb.html/>

Network Associates... [http://www.mcafee.com/antivirus/virus\\_glossary.asp](http://www.mcafee.com/antivirus/virus_glossary.asp)

MessageLabs (managed service)... <http://www.message-labs.com/viruseye/threats/default.asp>

<sup>3</sup> See NISCC Technical Note 01/02... <http://www.uniras.gov.uk> (see **Alerts & Briefings** for 2002)