



Kaspersky Lab White Paper

Enemies Bearing Gifts

There are many types of Trojans and each is designed to behave differently. Read on to learn more.

The Kaspersky Lab anti-virus engine, integrated into all Kaspersky® anti-virus products, delivers a unique combination of technologies necessary to successfully find and remove 'malware'. Malware [short for **malicious software**], refers to any program that is deliberately created to perform an unauthorized, often harmful, action: this includes viruses, worms and Trojans of various kinds.

In the last few years, there has been an increase in the number of Trojans. Many of today's most successful threats ['successful' from the author's perspective that is] are a composite 'bundle' that includes different kinds of threat. Increasingly this 'bundle' includes a Trojan of one kind or another. Typically Trojans are dropped onto a victim machine by a virus or worm, or downloaded from a remote site. Trojans don't have their own on-board replication capability. For this reason, they're often perceived as being less dangerous than viruses or worms. Yet their effects can be dangerous and very far-reaching. Not only have they increased in numbers in recent years. They have also become more sophisticated and they are being put to an increasing number of malicious uses.

Let's take a closer look at Trojans. What exactly are they, how do they work and what effects can they have on a victim machine?

The term Trojan [short for Trojan Horse] is taken from the wooden horse used by the Greeks to sneak inside the city of Troy and capture it. The first Trojans, which appeared in the late 1980s, masqueraded as innocent programs. Once the unsuspecting user ran the program, the Trojan would deliver its harmful payload. Hence the copybook definition given by most anti-virus vendors: a non-replicating program that appears to be legitimate but is designed to carry out some harmful action on the victim computer.

The fact that Trojans don't spread by themselves is the key feature that distinguishes them from viruses. Viruses are parasitic, adding their code to an existing host [an EXE file, for example]. So they spread from file to file to file: and the longer a user is infected, the further the virus spreads across their machine [and potentially across the network too, if the user is able to access a network]. Trojans, by contrast, have no on-board replication mechanism. So in the early days of PC malware, Trojan authors had to find some way of distributing their code manually: upload it to a BBS [Bulletin Board System] in the guise of a useful application, deliberately planting it in a corporate network, or using the postal service to send it to a pre-defined list of victims.

Twelve Tricks, for example, was a hacked version of a hard disk benchmarking program. When installed, the Trojan wrote itself to the MBR [Master Boot Record] of the disk and performed one of the twelve 'tricks', many of which made it look as though the victim had a hardware problem. Unfortunately, there was also a chance that the Trojan would format the track on the hard disk containing the boot sector, or cause gradual corruption of the FAT [File Allocation Table].

Another example of an early Trojan was the Aids Information Disk. In late 1989, 20,000 floppy disks containing this Trojan were mailed to addresses stolen from PC Business World and the World Health Organization, by a company called 'PC Cyborg'. The disks supposedly contained information about HIV and the author was clearly 'cashing-in' on widespread concern about the virus. When the user ran the installation program, the Trojan wrote itself to the hard disk, created its own hidden files and directories and modified system files.



After the PC had been booted 90 times, the Trojan encrypted the contents of the hard disk, making the data inaccessible. The only accessible file remaining on the disk was a README file: this contained a bill and a PO Box address in Panama for payment. Interestingly, the use of 'program mechanisms', including some that would 'adversely affect other program applications', was announced up-front in a license agreement contained on the floppy disk used to distribute the Trojan. Dr Joseph Popp, the alleged author of the Trojan, was later extradited to the UK. However, he was deemed unfit to stand trial following his behavior in court [an Italian court later found him guilty *in absentia*].

At this time, Trojans were relatively uncommon, compared to viruses, because they didn't contain the self-replication code that would let them spread automatically. They were either distributed manually, like the Aids Information Disk, or they were uploaded to a bulletin board, where they seemed like a perfectly innocent program. From time to time, tailor-made Trojans were left behind on a corporate network by a disgruntled employee. Increasing connectivity and the development of the World Wide Web in the mid-1990s brought about a significant change. Previously, a Trojan author had to find a way to deliver his malicious program manually. Now, with the power of the Internet, he could distribute it automatically, or simply wait for masses of unsuspecting users to download it themselves from a web site or Internet forum.

This period saw the emergence of password stealing Trojans. The first of them, aimed at AOL, appeared in 1996 and within a few years there were hundreds of them. Unlike earlier Trojans, there was no damage to data. Instead, as the name suggests, they were designed to steal confidential login information and send it to the author, or 'master', of the Trojan, giving them access to the victim's account. AOL password stealing Trojans were distributed as innocent programs, offering to offer better AOL access, new AOL services or an application path. Sometimes, they were embedded in DOC or RTF files and executed when the user double-clicked on them.

Things have moved on considerably since the days when most 'copy-book' definitions of Trojans were written. Far from appearing to be something benign, most Trojans don't 'appear' at all. In other words, they install silently and the victim has no idea that the Trojan is there.

One of the biggest factors driving this change has been the 'commercialization' of malicious code. It's clear that the computer underground has realized the potential for making money from their creations in a wired world. And the use of Trojans is central to their strategy.

Often, victim machines are combined into networks, often using IRC channels or web sites where the author has placed additional functionality. The more complex Trojans combine infected machines into a single P2P network. These so-called 'bot' networks offer an effective way of controlling victim machines.

They can be used to harvest confidential information [username, password, PIN, etc.], for computer fraud: this includes 'phishing' scams that trick users into providing their bank details on a fraudulent web site. Or they can be 'conscripted' into a 'zombie army' to launch a DDoS [Distributed-Denial-of-Service] attack on a victim organization. This could be to extort money, for example: a 'demonstration' DDoS attack offers the victim a 'taster' of what will happen if they don't pay up. Alternatively, victim machines can become proxies for the distribution of spam email.

Since the middle of 2004, there has been a shift in tactics from the writers of malicious code. The relative decline in the number of *global* epidemics seems to signal a move away from the use of mass attacks on victims worldwide. Instead, attacks are becoming more targeted. There are several reasons for this. On the one hand, law enforcement agencies worldwide now have far more expertise than ever before in tracking down the perpetrators of computer crime. The last year has seen a great many arrests, often the result of co-operation of several national law enforcement agencies. On the other hand, anti-virus researchers have had many years practice in dealing with large-scale epidemics. Fast response to new threats, in the form of virus definitions, is just the visible tip of the iceberg here. Anti-virus research teams worldwide have developed 'early warning antennae' giving them early visibility into malicious activity on the Internet. And when an attack occurs, the servers used to gather confidential data harvested from victim machines can be tracked and closed down, mitigating the effects of the attack.



It's also worth recalling the point made above that many of today's attacks are designed to steal confidential data to make money illegally. From this, it follows that the harvested data has to be processed and used. Where millions of victim machines are involved, not only does this make detection more likely. It's also a huge logistical operation. For this reason too, it makes more sense for malware authors to focus their attacks.

This may mean targeting machines one thousand at a time in small-scale, low-key 'hit and run' operations. Or it may mean tailoring a piece of code for an attack on a single victim, or a small number of victims. One high profile example of this was flagged by Operation Horse Race, <http://www.viruslist.com/en/news?id=164628501> in May 2005, when several senior Israeli executives were arrested for allegedly planting a Trojan in the computers of competitors.

There are many different types of Trojan, each purpose-built to carry out a specific function on the victim machine. Let's take a closer look at them.

General Trojans

This is an umbrella category covering any non-replicating, malicious program that threatens data integrity or otherwise adversely affects the use of the machine.

Backdoor Trojans

These are the most dangerous, and most widespread, type of Trojan. Backdoor Trojans provide the author or 'master' of the Trojan with remote 'administration' of victim machines. Unlike legitimate remote administration utilities, they install, launch and run invisibly, without the consent or knowledge of the user. Once installed, backdoor Trojans can be instructed to send, receive, execute and delete files, harvest confidential data from the machine, log activity on the machine and more.

Password Stealers (PSW) Trojans

These Trojans are designed to steal passwords from the victim machine [although some steal other types of information: IP address, registration details, email client details, and so on]. This information is then sent to an e-mail address coded into the body of the Trojan. The first PSW Trojans were AOL password stealing Trojans: and they are so numerous that they form a specific subset of PSW Trojans.

Trojan Clickers

Trojan Clickers re-direct victim machines to a specified web site. This is done either to raise the 'hit-count' of a site, for advertising purposes, or to organize a DDoS attack on a specified site, or to direct the victim to a web site containing other malicious code [another Trojan, for example]. The Trojan does this either by sending commands to the browser or by simply replacing system files that contain URLs [the 'hosts' file in Windows].

Trojan Droppers

The purpose of Trojan Droppers, as the name suggests, is to install malicious code on a victim machine. They either install another malicious program or a new version of some previously installed malware. Trojan Droppers often carry several completely unrelated pieces of malware that may be different in behaviour or even written by different coders: in effect, they're a kind of malware archive containing many kinds of different malicious code. They may also include a joke or hoax, to distract the user from the real purpose of the Dropper, the background installation of malicious code, or adware or 'pornware' programs. Droppers are often used to carry known Trojans, since it is significantly easier to write a dropper than a brand new Trojan that anti-virus programs will not be able to detect. Most droppers are written in Visual Basic Script [VBS] or JavaScript [JS]: they are, therefore, easy to write and can be used to perform multiple tasks.

Trojan Downloaders

These Trojans [like Trojan Droppers] are used to install malicious code on a victim machine. However, they can be more useful to malware authors. First, Downloaders are much smaller than Droppers. Second, they can be used to download endless new versions of malicious code, adware or 'pornware' programs. Like Droppers, Downloaders are also typically written in script languages such as VBS and JS. They also often exploit Microsoft Internet Explorer vulnerabilities.



Trojan Proxies

These Trojans function as a proxy server and provide anonymous access to the Internet. Trojan Proxies are commonly used by spammers for large-scale distribution of spam email.

Trojan Spies

Trojan Spies, as the name suggests, track user activity, save the information to the user's hard disk and then forward it to the author or 'master' of the Trojan. The information collected includes keystrokes and screen-shots, used in the theft of banking data to support online fraud.

Trojan Notifiers

The purpose of these Trojans is to inform the author or 'master' that malicious code has been installed on the victim machine and to relay information about the IP address, open ports, e-mail address and so on. Trojan Notifiers are typically included in a Trojan 'pack' that contains other malware.

ArcBombs

These Trojans are designed to sabotage anti-virus programs. They take the form of a specially constructed archive file. The ArcBomb 'explodes' when the archive is opened for scanning by the anti-virus program's de-compressor. The result is that the machine crashes, slows down or is filled with garbage data. This scenario is particularly bad, of course, if the victim machine is a server. The 'explosion' is achieved by creating an archive with an incorrect header, repeated data or a series of identical files. 5GB of repeating data, for example, can be just 480KB when packed in a ZIP file. And it's possible to pack 10^{100} identical files into a 230KB ZIP file.

Trojans are software, so potentially they can do anything that any program can be code to do. This provides a wide field of activity for Trojan authors. However, here's a list of some characteristic ways in which Trojans may impact a host system.

- Arrive in packed form, to minimize its size and [because the packing involved encryption] make it harder to detect.
- Drop files into the %Windows% or %Windows%\System directories.
- Register itself in the system registry, so that it runs each time the victim machine is booted.
- Use stealth techniques to hide files, processes or registry values belonging to the Trojan: this may include installing API [Application Program Interface] hooks into running processes or changing system APIs.
- Store configuration data within the body of its own code that allows a hacker to vary the name of the Trojan services [or other details] before the code is sent to another victim. As a result, the same Trojan may have different characteristics on different victim machines.
- Delete processes or files belonging to other applications. This may be done, for example, to displace an incumbent Trojan, or to cripple an installed security product [an anti-virus or anti-hacker program].
- Modify the hosts file on the victim machine, to block access to security update sites, or to re-direct searches to a site containing malicious code [or modify the Internet Explorer start page, for the same purpose].
- Use other resources on the victim machine, such as email, FTP or HTTP.
- Drop decoy files [often harmless 'joke' programs] to draw attention away from activity carried out by the Trojan.
- Delete files on the victim machine.
- Steal confidential data from the victim machine.
- Install adware or other potentially hostile applications [so-called 'spyware' programs] on the victim machine.
- Open ports on the victim machine, either specified in the body of the Trojan code or specified remotely by a hacker. This may be to receive remote instructions, to pass system information or other confidential data to a hacker, to connect to another victim machine, or to send data to a specified target as part of a DDoS attack.

For specific information on a Trojan that has been detected on your machine, check out the Virus Encyclopedia (<http://www.viruslist.com/en/viruses/encyclopedia>) on <http://www.viruslist.com> or contact Kaspersky Lab Technical Support.



About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers.