What You Click May Not Always Be What You Get!

Robert B. Fried, BS, MS

Abstract

Homer's Iliad makes mention of the legendary Trojan War. During the time of this war, the citizens of Troy were deceived into accepting a wooden horse from a Greek spy. The people of Troy were told that by accepting this gift, they would become invincible. However, contained within the wooden horse was a group of Greek soldiers. These soldiers waited until nightfall and at that point, demolished the city and victimized the citizens of Troy.

Today, there exists a new breed of Trojan horse. This new kind of Trojan is wreaking havoc on the netizens of cyberspace. The Trojan horse programs on the Internet today often have hidden agendas. On the outside, these programs may look appealing, but their true intentions are disguised to the average individual.

This paper will discuss the emergence of Trojan horse programs onto the Internet. A distinction between a computer virus and a Trojan horse will be made. This paper will also examine the nature of such programs. Methods of infection and prevention will be analyzed in detail. Furthermore, specific examples of known computer attacks where Trojan horses were utilized will be discussed. Finally, several conclusions will be drawn with respect to Trojan horses and the role they play / will play, with respect to the online world.

For Starters: A Clarification

When one begins to think about Trojan horses, one may automatically classify such an attack as a computer virus. This tends to be a common misunderstanding amongst computer users. Computer viruses fall under a completely different category of computer attacks. In order to truly understand Trojan horses and how they differ from that of computer viruses, it is important that each term be defined/characterized. Dr. Frederick B. Cohen is most noted for his work and research on computer viruses. His definition of a computer virus is widely accepted by experts within the computer world. Cohen defines a computer virus as a “program that can ‘infect’ other programs by modifying them to include a, possibly evolved, version of itself [2]. Like viruses found in the human body, without proper antibiotics; or in the case of a computer system, without the proper maintenance or other preventative measures, viruses can spread until many, if not all files in a system are infected. Ultimately, such an infection can render a system unusable.

A Trojan horse is a unique form of computer attack. According to Dr. Cohen, an attack can be deemed a Trojan horse when "unintended components or operations are placed in hardware, firmware, software, or wetware causing unintended and/or inappropriate behavior" [3]. Trojan Horses therefore, are the type of computer attack, which is often viewed as being more sophisticated and complex when compared to a typical computer virus. This complexity can be seen in that in several instances. For example, programmers have designed Trojan horses that are known to have computer viruses or residing within them [4].

Marquis Grove, an individual affiliated with a hacking news site, provides a rather unique distinction between computer viruses and Trojan horse programs. "Unlike viruses, Trojans don't e-mail hundreds of copies of themselves out, nor do they necessarily interfere with a computer's performance". Grove adds that "antiviral programs don't always catch them; therefore, many infected users have no idea their computers harbor a Trojan" [5].

What Lies Beneath?

Have you ever downloaded a program from an Internet website? How do you know if what you downloaded was from a legitimate source? Can you validate that the programs you download via the Internet are programmed to do only things you intend them to do? The majority of Internet users are not computer savvy and truly don’t know. As a result, Trojan horses have successfully invaded and infected many computer systems.

Originally, programmers who wanted to cause certain modifications on their victim’s computer system designed Trojan horses. Programming of this sort was, and still is viewed today as a form of self-expression [1]. A majority of the one thousand or so Trojan horses in existence do "little more than to cause the system to lock up, behave abnormally in a specific way or perhaps cause the loss of data on the user's machine" [1].

In recent years Trojan horse programs have become more malicious and sophisticated. The programmers have utilized new tactics and methods to both deceive others and to unleash payloads. "Their primary objective is to allow a remote user a means of gaining access to a victim's machine without their knowledge. Once that has been achieved, the intruder can do anything with the machine that the user can do" [1]. Imagine having complete unrestricted access and control over someone else's personal computer. Such access could allow the intruder to cause serious damage to their victim's computer. In a recent article regarding the matter, it was said "there may be a ghost in your machine -- a hidden program known as a Trojan horse -- that allows a malicious hacker to spy on you, ruin your data and computer and, in extreme cases, wreck your business or your life" [4]. Although, this statement may sound a bit over exaggerated, many people fear that their computer may become infected with such a critter. The concern is strong enough, that one individual, David Kroll of Finjan software, a computer security firm, recently referred to Trojans as the "silent killer" [5].

How These Critters Are Utilized

As stated previously, programming is a form of self-expression. However, why does one have to exploit others in the process of expressing themselves? What pleasure do these individuals obtain from damaging the data of others? There are many reasons why computer programmers create Trojans.

Trojans can be utilized in many different respects. Besides serving as a form of freedom of expression, Trojans can also help enlighten a programmer's sense of curiosity. It’s amazing to think about what a person with proper skill sets could actually do. What would a person be likely to do if they were granted full-unrestricted access to another's computer? "An intruder's usual objective is to browse the user's hard drive in order to determine if there is anything of value store on it. That could be almost anything such as valuable research papers, credit card details or passwords to restricted web sites for example" [1]. Once an intruder gains access, the list of possibilities can be endless. What is unfortunate is that a vulnerable computer user can be victimized by such an at any given moment without even knowing it {1].

Browsing through mounts of available information is one thing, exploiting it is another. Malicious Trojans can be utilized to help intruders commit all sorts of criminal acts. If the intruder comes across their victim's credit card information, he/she can go on a daylong shopping spree. With stock portfolio/bank account information, an intruder can easily determine their victim's financial worth. With access to their victim's e-mail address books, the intruder can determine their victim's personal and/or business contacts. Imagine what could happen if an intruder gained access to a major competitor's financial records; the results could be absolutely devastating! Trojan horses can even allow an intruder to view their victims who have a web cam. What can be done is simply astonishing.

Most recently, many Trojan horses have been utilized to launch Denial of Service (DoS) attacks. Essentially, "malicious hackers can use a collection of Trojan infected machines to bolster the effects of DoS attacks. Hackers can also hide their location by funneling their attacks though others' computers" [5]. DoS attacks have caused much concern because not only are they hard to track back to their source, they also are hard to predict and prevent.

How The Seed is Planted

Trojan horses can be planted into a computer system in many ways. Probably the most popular and easiest way to do so is through electronic mail. The beauty of e-mail is that a programmer can literally create a Trojan and in a matter of minutes attach it to a message and send it to thousands of names he/she has compiled in his/her address book. Many recipients of the e-mail will probably delete the message because they may not recognize the sender. Yet, there are always those individuals who click before they think and will actually open the e-mail, download the attachment and become a victim.

Another way to place a Trojan on another's computer is through software. Many programmers place Trojans within programs that may look appealing to vulnerable computer users. Trojans can exist in programs downloaded from the Internet. However, many Trojan horses have also been found on software titles issues from reputable software vendors.

Have you ever surfed the Internet and downloaded a free game, screensaver, picture, mp3, video or audio file? In this day and age it is likely that a majority of you have. You may be surprised to learn that a majority of the Trojan horses in existence today are transmitted when such programs and files are executed [6]. "You probably downloaded the Trojan from a WWW or FTP archive, ICQ file exchange, or through IRC's DCC file transfer" [6].

To become infected, the computer user has to simply initiate the executable file associated with a Trojan horse program. In a majority of the cases the computer user must initiate the executable file. However, some programs have an auto-initiate feature once the executable file has been downloaded. Trojan horses may have a variety of extensions associated with its executable file. For example "in Windows, executable programs have file extensions like 'exe', 'vbs', 'com', 'bat', 'pif', 'scr' 'lnk' or 'js'" [6]. Many Trojans have multiple extensions, however, if a Microsoft Windows user does not unhide his/her file extensions they may be fooled into thinking that the file they just downloaded is safe to click on and execute [6].

Incidents Involving Trojan Horses

The cracker group ‘Cult of the Dead Cow’ first released a well-known Trojan horse by the name of Back Orifice on August 03, 1998. The program is designed to do something other than what it says. Those in the industry refer to this critter, which has affected nearly 100,000 people, as a 'remote administration tool'. Essentially, Back Orifice grants a remote user access privileges to an infected system operated by the victim. With such privileges, the remote user can make almost any change he/she desires when the victim's system is signed online. Like most Trojan programs of this sort, the victim does not have a clue as to what is taking place. Furthermore, Back Orifice tries to cover its tracks by deleting the original copy of itself from the victim's computer and using an insignificant amount of system memory/resources [7].

Another Trojan program, Sub Seven DEFCON8 2.1, has also gained notability. Sub Seven is commonly found as an attachment to messages in newsgroups on the Internet. This particular program allows for an intruder to take control of their victim's computer. With this tool, an intruder can gain access to files on their victim's computer. The intruder can even utilize Sub Seven to coordinate DoS attacks. It is therefore, a very powerful tool if the intruder knows how to properly utilize it to accomplish his goals. Like other Trojans, Sub Seven operates and functions without the victim knowing [8].

Mechanisms of Prevention/Detection

Due to their complexity and sophistication, a computer user may not be aware that a Trojan horse has infected their system. Gerry Freeze, a security advisor/analyst once stated, "Trojans often hide multiple copies of themselves in multiple locations, and can be very hard to find and remove completely. Removing a Trojan from an infected system is a difficult if not almost impossible -- task" [5]. According to Dr. Cohen, "detecting Trojan horses is almost certainly an undecidable problem but inadequate mathematical analysis has been done in this subject to provide further clarification" [3]. If they appear to be invisible, hard to detect and difficult to remove, how can one defend his/her system from such an attack?

There are several approaches that people in the computer security industry have in regards to preventing/dealing with infection by Trojans. Ken Dunham, with AtomicTangerine, recommends the utilization of "multiple tools, an antiviral program, an anti-Trojan program, and a firewall to reduce the risk of infection" [5].

Although prevention techniques can be practiced, Trojans can still slip through the cracks. Many people do not keep their antiviral programs updated regularly. It is also quite possible that a new Trojan horse can be too complex to be picked up by a scanner looking for Trojans. There are many possibilities that come into play with regards to how computers become infected with Trojans.

The question then becomes, what happens if a computer is in fact infected with a Trojan? Well, there are several routes to take. Many programs exist on the markets that claim to disinfect/protect systems. Such programs include: BackWork 2.12, BoDetect 3.5, Jammer 1.95, Kaspersky Anti-Virus, LockDown 2000 5.0.0.4, NetAlert 2000, NoBackDoors 1.4, Panda Anti-Virus Platinum, Protect 3.0.1, Trojan Defense Suite 3.2.0 and The Cleaner 3.2 [9]. However, Gerry Freeze, feels that in dealing with Trojans be it prevention or removal, "many times the best or only answer is to go back to a known clean backup or the original installation media and completely delete and reinstall clean copies of all the software" [5].

Summary, Conclusions, and Further Work

Trojan Horses are a popular form of computer attack. With time, these critters are becoming more complex and sophisticated. As the Internet becomes more populated with 'netizens' this form of attack has the potential to affect millions of individuals.

We all hear about the dangers of Trojan horse infections, but what do we really know? How do we know that a Trojan horse is present on our own computer system? Sure there may be some programs which help to comfort us and appear to have the perfect solution. In reality, there is no real solution. Trojan horses are good at disguising themselves and preventing detection. If we can't locate them how can we prevent them? Dr. Cohen has the best advice, which he claims has been proven mathematically: " There are three things you can ever do to absolutely and perfectly prevent a computer virus (or with regard to this paper, a Trojan horse) from spreading throughout a computer system or network; limit sharing, limit transitivity, or limit programming" [10]. In the real world, we have become so reliant on computers that this advice would be impossible to follow.

References

[1]. Agnitum: Tauscan: What is a Trojan Horse and What Threat Does it Pose?

http://www.agnitum.com/products/tauscan/ttour1.phtml

[2]. Cohen, Frederick B. A Short Course on Computer Viruses</U>.
ASP Press 1990: Page 11.

[3]. Fred Cohen &amp; Associates: The All.Net Security Database: Attack #16

http://www.agnitum.com/products/tauscan/ttour1.phtml

[4]. Lo, Joseph. "Trojan Horse or Virus?". May 6, 2000.

http://www.irchelp.org/irchelp/security/trojanterms.html

[5]. Delio, Michelle. "Viruses? Feh! Fear the Trojan". May 24, 2001.

http://www.wired.com/news/infostructure/0,1377,43981,00.html

[6]. Lo, Joseph. "Trojan Horse Attacks". June 4, 2000.
http://www.irchelp.org/irchelp/security/trojan.html

[7]. "The Back Orifice 'Backdoor' Program: Your Security is at Risk.

http://www.nwinternet.com/~pchelp/bo/bo.html

[8]. SubSeven DEFCON8 2.1 Backdoor.

http://support.cai.com/techbases/ilnt/in0001.html

[9]. Security: Anti Trojan Horse.

http://www.polderware.com/apps/sec-atrh.shtml

[10]. Cohen, Frederick B. <U>A Short Course on Computer Viruses.
ASP Press 1990: Page 61.

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).