TROJAN HORSES: THEY DECEIVE, THEY INVADE, THEY DESTROY

Hector J. Garcia, Jr., Texas A&M University-Kingsville
Dr. Ralph Reilly, University of Hartford
Dr. Jack D. Shorter, Texas A&M University-Kingsville, j-shorter@tamuk.edu

ABSTRACT

You could have a Trojan horse on your computer as you read this. "Trojan Horses" are programs that inhabit your PC, erasing data or providing hackers with personal information. Trojan Horses are the deceiving and harmless looking programs that can sit on your system undetected, unnoticed, hidden within other programs, waiting for you to execute them. They are the ones that come attached to a clever, misleading email, waiting for you to download them. Trojan Horses deceive, they invade, and they destroy.

Keywords: Trojan Horse, Trojan, Virus, Worm, Anti-Trojan Horse Software, Crackers

INTRODUCTION

You could have a Trojan horse on your computer as you read this. And no, I'm not suggesting that a lot of little Greek men are going to jump out of your PC at any minute. I am talking about a specific computer program that can run undetected in your system, invade your privacy, destroy your files and cause your system harm. Almost everyone uses, works, or will have to work on a computer sometime in their future. So, after reading this paper you will have a basic knowledge about Trojan horses, how they work and spread, and how to protect your personal computer and any others you might visit.

Definition of a Trojan Horse

"Trojan Horses" are programs that inhabit your PC, erasing data or providing hackers with personal information. [4] If Trojan horses are so bad, it is hard to believe that anyone would be unaware of one running on their computer. Trojan horse Viruses, much like the Trojan Horse of Greece, can seem harmless, when in fact, the Greek Trojan Horse was filled with Greek warriors waiting to enter and conquer the city of Troy. The Trojan Horse does not contain Greek warriors, but instead a malicious code that carries out different functions. [6] The Trojan Horse Virus waits for an opening into a computer system and then takes over. Some Trojans also provide a "backdoor" or open port for hackers to gain control of your computer at any time. [9] Other Trojans steal passwords from ISP accounts such as America Online, and send them back to their author via email. Trojans can also be hidden inside other files, such as mp3's, mpg's (movie files), avi's (audio video interleave files), and email attachments. [9] The computer user who has just downloaded one of the above file types may have no idea that a Trojan horse is hidden in one of these files. However, Trojans are harmless until they are executed.

Differences Between Trojan Horses and Other Viruses

So what is the difference between Trojan horses and other types of viruses? Well, as mentioned in the above paragraph, Trojans are harmless until they are executed, unlike some viruses, which can start harming your system upon download or entrance into your system. [15] Trojans have a simpler code than viruses or worms; therefore they can be hidden inside other files, thus making their detection even harder. Viruses and worms cannot be hidden inside other files making them easily detectable by virus scanners, unlike Trojan Horses that often go undetected. Another difference is that Trojan Horses will send the programmer feedback, where a virus is simply a mischievous information destroying program. [5]

Who Creates These Trojan Horse Viruses?

"Hackers" are individuals who attempt to gain unauthorized access to a computer system and usually write these programs. They have many means at their disposal for breaking into your system. But you don't have to be a hacker to create a Trojan horse. As mentioned before, Trojan code is simpler than virus or worm code, this makes them easier to create and harder to detect. People with little or no computer programming knowledge can write one of these malicious programs. Most Trojans are written in Visual Basic programming language or C ++. Some hacker web sites even contain ready made Trojans that can be modified by anyone. [6]

Types of Trojans and How Much Damage They Can Cause

A Trojan horse installs itself on your computer, where it can wreak havoc later by modifying or deleting data or spying on you. [8] There are different types of Trojans. There are password stealers, remote access Trojans, and other Trojans that can contain smaller viruses. Specifically, when you execute a program that contains a Password stealing Trojan horse on your computer it can steal your passwords for a specific password-protected item such as log in accounts, system user accounts, and data bases. [2] Then it will send them to the original programmer's e-mail address. Once a hacker has these he can gain access to items that were previously password protected. One such Trojan was the infamous "Hey You" Trojan, which hit America Online about 2 years ago. This Password Stealing Trojan was passed on via AOL's email system in which AOL users received an email from other AOL users with an attachment (mine.exe or mine.zip), the subject line "Hey You", and text in the email that claimed the attachment was a file containing pictures. It's very common for AOL users to trade pictures via AOL's Email account. [16] This is why many users got tricked into downloading the attachment that contained the Trojan horse, causing many computers running the AOL software to become infected. This Trojan was also called the "Buddy List Trojan" because when an AOL user logged on to the AOL service, the Trojan horse would also try to email itself to all of the contacts listed in that member's Buddy List. [17] An example of how the Trojan Horse operates is one person with an infected computer trades pictures with friends, the Trojan then sends a fake email to everyone on their buddy list. Other computers become infected with the Trojan horse when they download and execute the fake, infected attachment. Their passwords are also sent back to the author who created the Hey You Trojan.
Some Trojans even provide a "backdoor" to your computer and its files from outside your network. These are called Remote Access Trojans. You are open to harm as long as the Trojan is

installed and runs every time you start up your computer. A hacker or programmer uses a remote access Trojan for the sole purpose of gaining access to all your information without your knowledge. That is why they try to make Trojans as discreet as possible. If you log onto any kind of account, like email, a Trojan horse can see your passwords. If you do online banking, someone can find your information. Certain E-commerce sites have the option to pay online with a credit card. If you have a standing account, you may have saved your credit card information somewhere on your computer. Web-site security is tightening, but if you have a Trojan horse, all that Internet security is in vain and your privacy has been invaded. [1]

Some Trojans are more complex than others. They send information to the programmer, but also carry small viruses that can cause a great deal of damage to your computer. For example, a certain type of Trojan horse virus releases five small viruses that delete files every time you restart your computer. In due time, your computer will die and the hard-drive will need to be reformatted. [4] Another complex Trojan horse replicates itself many more times, which means you now have multiple Trojan horse viruses on your computer. The internally replicating Trojan is insurance so that if you do find and delete the original, the program writer will still have access to your account through the replicates.

How a Trojan Horse Can Get On Your Computer.

The password stealing Trojan horse is the most common form and targets anyone who has a computer that uses the Internet. As mentioned before, people using America Online are attacked often by password stealing Trojan horses. Usually someone who has a Trojan horse on their computer is tricked into downloading and opening it. For example, someone on AOL might get e-mail with a downloadable attachment. The programmer trying to use the Trojan will most likely pose as an AOL employee. They may write text in the e-mail that claims the user can get free Internet access if the attachment is downloaded and the computer is registered with their online service. This catches the reader's attention and he/she opens the e-mail and begins to download the program. When they download the attachment it is usually a small file, around 30 to 200 kilobytes. Files this small take less than a minute to download and install with most internet connections. Once the file is executed, the user may get a message that says "File Not Found" or other such error prompt. They have just downloaded the Trojan horse into their computers memory. [3] The next time the user reboots their computer; the Trojan will begin running and steal the user's passwords, sending them to a preset e-mail address that is accessed by the Trojan programmer. The hacker now has access to your account and files with the help of their Trojan horse password stealer.

Another way to become infected is by downloading shared music, movies, and software through file sharing programs such as Kazaa Media Desktop. Many of these peer-to-peer file-sharing programs are being used with no anti-virus filters. A large part of the Internet using community utilizes these file sharing programs so that they will not be charged for the original. Note that these programs are unsafe and should be used to download files with caution. You can pick up the Trojan horse if that file is saved in the infected computers "shared" files, or if a file you downloaded has a Trojan hidden within it. [2] It is a good idea to download from web sites that are trustworthy. If you download a program from a hacker site, more than likely it's going to have something extra. Be cautious when downloading.

How Can You Avoid Getting a Trojan Horse Virus on Your Computer?

Because of the discreet nature of the Trojan horse virus, you may not know if you have one on your computer. Any files downloaded from the Internet or from outside computers should be scanned with anti-virus software, even if a close friend sent the program. Some of the larger email providers, like MSN's Hotmail accounts, have virus scanners check all incoming email attachments. Even if you use these accounts you should invest in anti-virus software for yourself or business. Your personal computer's anti-virus software should be updated regularly, as well, because new mutations of viruses and Trojan horses are being created constantly.

There are anti-Trojan horse programs that have been made specifically for the purpose of detecting, removing, and repairing damage caused by Trojan horse viruses. [10] In addition to anti-Trojan horse programs, there are some firewalls that can prevent a Trojan horse from sending information to its original programmer. This does protect your computer from receiving a Trojan horse, and if it is a virus-releasing Trojan horse, or an internally replicating one, you may still have a problem. Some types of anti-virus software can detect Trojan horses, but virus scanners are not fully adequate because it can be difficult to catch the simple text of a Trojan horse. Because anti-virus software alone may not be able to fully protect your computer from a Trojan horse, they should be used in conjunction with anti-Trojan horse software. [11]

Anti-Trojan Horse Software

There are many Trojan-scanning programs in the market right now available for purchase. There are also many trial versions of Trojan scanners that can be downloaded from the Internet that can help aid you in the detection and removal of a Trojan horse, as well as, for security purposes. We have dealt with a few Trojans ourselves and in the process we have sampled many different anti-Trojan scanners.

The first one is **Trojan Remover**, by Simply Super Software. This program scans for Trojans, worms and viruses. This is a very easy to use Trojan scanner with an exceptional graphical user interface. Another advantage of Trojan Remover is that it can perform a scan every time you start up your computer. This helps detect Trojans that load during boot up, never giving Trojans a chance to load. You can also run scans from within Windows Explorer, performing them on files, directories, or an entire drive. You can get the details on the Trojans that may be on your system, by using the integrated database, which contains information on over 5000 Trojan Horses. Unlike virus scanners that cannot remove Trojans that may be running on your system, Trojan Remover finds Trojan horses, then removes the offender and repairs the modified system files and registry for you. Trojan Remover works on WINDOWS 9x, ME, NT, & XP Operating Systems, and is only a 2 megabyte download for the full installation. You can also update your Trojan Remover as soon as the creators update it to modified versions. [10]

The only slight disadvantage of Trojan remover was that it is a trial version; only lasting 30 days and then it must be registered for $25. It's not that bad of a disadvantage considering it can save your computer's hard drive. [10]

Tiny Trojan Trap, by Tiny Software is another great Trojan Scanning program, which also happens to scan for viruses too. It scans for known and unknown applications and controls their access to system resources, such as memory, the registry, and space on the hard drive. It protects workstations and networks from attacks by any kind of active content (ActiveX, Java, VBS, and other executable code) received from the Internet or by any other means. [11] Tiny Trojan Trap somewhat acts like a firewall, which can be an advantage and also a disadvantage. If they don't know anything about firewalls, then Tiny Trojan Trap may be confusing. One definite advantage is that it protects your computer from software with bugs in it (preventing crashes) and detecting programs which may have a Trojan attached. Tiny Trojan Trap also sets up a firewall like action when using a web browser that will catch unknown applications or scripts being accessed through the browser. Tiny Trojan Trap works on WINDOWS 9x, ME, 2000, and XP Operating Systems. It is a 9.75-megabyte download. [11]

Pest Patrol 4.2, wins the all-around award for Trojan Scanners. This scanner not only detects Trojans, worms and viruses, but also spyware, adware, spy cookies, hacker tools and other pests. It includes a memory scanner, and updates come out regularly. You can download the updates from the web site, so you'll always have the best available protection for your computer. Pest Patrol also cleans up after the "BUGBEAR" Worm that installs a backdoor and a key logger. Anti-Virus software cannot fix this problem, but Pest Patrol can. Pest Patrol works on WINDOWS 98, ME, NT, 2000, and XP Operating Systems. The download for Pest Patrol 4.2 is 5.3-mega-bytes. [12]

As splendid as Pest Patrol might sound, it has a few disadvantages. One disadvantage is the graphical user interface. It may be a little confusing for non-experienced computer users. Pest Patrol will not catch Trojans, or any of the other pests it detects, the only way you can detect them with pest patrol is if you manually run the program and perform a scan. The memory scanner does not work too well against spyware, adware and hacker tools. Overall, it's a good program that is a definite winner because it not only finds Trojans, but other mischievous spyware and adware. [12]

The Cleaner 3.2, by MooSoft is an easy to use Trojan scanner. The interface is very easy to get along with, and it also scans archived files such as .zip, .ace, .rar, .cab and .arj files that may hide Trojans. It works on Windows 9x, 2000, and NT. The file size download is 1.8 mega-bytes, a definite advantage. [13]

The disadvantages are that Cleaner 3.2 is pretty basic because it only scans for Trojans horses and worms. It is recommended that you use it alongside other anti-virus and firewall software, but then again, all Trojan scanners should be used with anti-virus software also. But, the main disadvantage was the price for the fully functional working copy of this Trojan scanner, $30. That's too much for a program that doesn't detect viruses. If you need a quick, easy to use, one time scan of your system, this would be the scanner to download. [13]
Anti-Trojan v5.5.405 is a very good program. This scanner checks archived files, email attachments, and also scans your registry for Trojans. Anti-Trojan also determines if there are open ports on your computer. If it detects a Trojan horse, it can remove it for you and clean up any damage it may have caused. This Trojan scanner has a big database of about 8000 different Trojans. It has an easy to use graphical user interface, with tabs, making it easy for novice

computer users to follow. Anti-Trojan v5.5.405 works on WINDOWS 9x, ME, 2000, NT, and XP Operating Systems. The download file size is 4.6 mega-bytes. This is a great scanner. The large database gives it an edge in that aspect over the other scanners. [14]

The disadvantages are mainly the trial version and price to register. It would be nice to have a program like Anti-Trojan v5.5.405 or Trojan Remover and not have to pay for it. Unfortunately, it costs $22 to register Anti-Trojan v5.5.405. That is not too much to pay considering all that it can do. [14]

Knowing is Half the Battle

The use of any Trojan Scanning software is a good way of protecting your computer. It gives you extra security for your system. However, the easiest and cheapest way to protect against Trojan horses is to know your computer and be knowledgeable about Trojans. It's important to know your system. Take note of any changes to it and watch for suspicious activities. You should never change any important system files on your own, nor should you try to manually delete a Trojan horse. Let the aid of an anti-Trojan scanning program detect and remove a Trojan horse, as well as clean up any files the Trojan may have corrupted. Use caution when browsing the Internet and be careful of any suspicious scripts from mistrustful web sites. Try not to visit web sites that pertain to hacking, cracking and other forms of mischievous activities. These sites can instantly add scripts and files to your computer, misleading you in the future into clicking on them. It's also important to stay alert when checking email. [7] Watch out for unsolicited email attachments. Limit the downloading of programs from non-business web sites. And remember that purchased programs are always the safest to use. It may not be cheaper, but in the long run, a free, harmless looking program can be harmful and not only hurt your computer, but also your wallet..

CONCLUSION

In the computer world, there are viruses, there are worms, and there are Trojan horses. Trojan horses are the deceiving and harmless looking programs that can sit on your system undetected, unnoticed, hidden within other programs, waiting for you to execute them. They are the ones that come attached to a clever, misleading email, waiting for you to download them. Trojan Horses deceive, they invade, and they destroy. Because most of us already use, work, or will work on a computer someday, it's important to know about Trojan Horses. Trojan Horses are not always detected by your Anti-Virus software, so, as you read on, there could be a Trojan on your computer, waiting for you to open it so that it can perform its malicious acts. There are Trojan Scanning Programs out there that can help you fight back against Trojan horses and protect your system and its files. It may cost you a little now, but it sure is a lot better to pay a little now, than to have to pay more later for the damage a Trojan horse may cause your computer system.

REFERENCES

1. Internet Fixes, February 27, 2003, PC World Magazine, http://www.pcworld.com/howto/article/0,aid,109364,00.asp

2. Security Threats to beware of in 2003, January 3, 2003, PC World Magazine, http://www.pcworld.com/news/article/0,aid,108376,00.asp
3. E-Mail Threats Increase Sharply, December 12, 2002, PC World Magazine, http://www.pcworld.com/news/article/0,aid,107930,00.asp
4. Protect Your Hard Drive from Attack, March 2, 2003**,** PC World Magazine, http://www.pcworld.com/downloads/collection/0,collid,704,00.asp
5. Yes, You Are Being Watched, December 27, 2002**,** PC World Magazine, http://www.pcworld.com/news/article/0,aid,108121,pg,3,00.asp
6. News-Sobig Worm Stomps on PC's, January 13, 2003 , ZD NET Magazine, http://zdnet.com.com/2100-1105-980338.html
7. News-Linux Utility Site Hacked, November 14, 2002**,** ZD Net Magazine, http://zdnet.com.com/2100-1105-965800.html
8. Anti-Trojan v5.5.405, January 4, 2003, PC World Magazine http://www.pcworld.com/downloads/file_description/0,fid,22519,00.asp
9. Sobig Worm Gets Even Bigger, January 14, 2003, PC World Magazine http://www.pcworld.com/news/article/0,aid,108793,00.asp
10. Simply Super Software (Makers of Trojan Remover), (2003) http://www.simplysup.com
11. Tiny Software (Makers of Tiny Trojan Trap), (2003) http://www.tinysoftware.com
12. Pest Patrol Homepage, (2003) http://www.pestpatrol.com/
13. MooSoft (Makers of The Cleaner 3.2), (2003) http://www.moosoft.com/
14. Anti-Trojan v5.5.405 (Anti-Trojan v5.5.405 homepage), (2003) http://www.anti-trojan.net/en
15. Trojan Horse, (2003) http://whatis.techtarget.com/definition/0,289893,sid9_gci213221,00
16. Hey you Trojan, (2003) http://www.claws-and-paws.com/virus/articles/heyyou
17. Buddy List Trojan, (2003) http://www.glocksoft.com/trojan_list/AOL_Buddy