Global Information Assurance Certification Paper

Lysa Messineo
APStrojan.qa Trojan Horse
February 19, 2001

APStrojan.qa Trojan Horse

Today it seems that computer attacks are becoming more and more common and many entities, mainly corporations, are becoming more attuned to it. For example, every couple of days when I reboot my PC at work, updated anti-virus downloads are there available for me to download, and prompting me to do so. Our CIS department tries to ensure that there is a very low chance that any kind of attack will affect us. While this is an excellent security practice for a company to maintain, it is not going to catch every single attack, even if all employees download the updates regularly. Hackers are constantly trying to break into systems. They are always looking for new ways to gain valuable information or to disrupt service in some way. There are many different kinds of attacks that allow them to do this. One of the most popular is the Trojan horse, which recently infected America Online's (AOL) Internet service. This Trojan horse, called APStrojan.qa, "…attempts to steal members' names and passwords and then send them via e-mail to the virus' author".[1] This particular variant of the Trojan horse will be discussed in depth after the Trojan horse is defined below.

Trojan Horses Defined

A Trojan horse is a program that appears to be useful but actually contains "…hidden functions that can exploit the privileges of the user, with a resulting security threat. A Trojan horse does things that the program user did not intend".[2] There are many ways that a Trojan horse can be installed. One way is by tricking the user. For example, a Trojan horse could be in an email attachment that appears to be some kind of downloadable game. The user could be enticed by the game, leading him/her to download it. It could also be a message that appears to be from a notable organization urging system administrators to download a certain kind of patch.[3] In another example, an intruder could call a system administrator and act like a legitimate user who needs some kind of help. The intruder could then trick the system administrator into running a program that he/she designed. This is a form of "social engineering", which involves "…fooling people into revealing information that they shouldn't. It plays upon people's general willingness to trust what they see and hear as being truthful."[4] Successful social engineers know that most people believe that others are truthful and have good intentions. This is why they are successful at gathering the information they want.

Another way that a Trojan horse can be installed is if an intruder compromises a software

[1] http://news.cnet.com/news/0-1005-200-4681471.html
[2] http://www.cert.org/advisories/CA-1999-02.html, 1
[3] http://www.cert.org/advisories/CA-1999-02.html, 4
[4] Fried, Stephen.

distribution site. Once the intruder has control of the site, he/she can replace legitimate software with Trojan horse versions, which is what legitimate users will download. Users can also be tricked into connecting to sites other than what they intended since DNS does not provided strong authentication.[5] If an intruder exploits this, it could cause the user to download a Trojan horse or to expose confidential information.

After an intruder has compromised a system, he/she could install Trojan horse versions of system utilities. "Often, collections of Trojan horses are distributed in toolkits that an intruder can use to compromise a system and conceal their activity after the compromise, e.g., a toolkit might include a Trojan horse version of *ls* which does not list files owned by the intruder."[6] It is very difficult to re-establish trust in a system once it has been compromised by an intruder, unless the system is rebuilt.

Trojan horses can also come in the form of a compiler, which allow it to be inserted into a program. A final example of how a Trojan horse can be installed on a system is if an intruder places one on a website that entices users. The Trojan horse could be in the forma of a Java applet, JavaScript, ActiveX control, or other executable.

As the above examples show, it is very easy for a user to download a Trojan horse without realizing it. This is dangerous because "…Trojan horses can do anything that the user executing the program has privileges to do."[7] This includes the following:

- Deleting files
- Transmitting files to the intruder
- Modifying files
- Installing other programs, such as those that allow unauthorized network access
- Attempting to increase the level of access beyond that of the user running the Trojan horse
- Installing viruses
- Installing other Trojan horses[8]

Any time a system on your network is compromised, it could have serious consequences on your entire network. Systems that are most vulnerable are those that transmit authentication material, such as passwords, over a shared network and are not properly encrypted. This is a common vulnerability and if compromised, an intruder can gain username and password information or other sensitive information by installing a network sniffer to record the information as it traverses the network.[9] This is obviously very sensitive information to organizations and must be protected. Therefore, the next aspect of Trojan horses to be discussed is how to prevent users from inadvertently downloading

[5] http://www.cert.org/advisories/CA-1999-02.html, 4
[6] http://www.cert.org/advisories/CA-1999-02.html, 4
[7] http://www.cert.org/advisories/CA-1999-02.html, 3
[8] http://www.cert.org/advisories/CA-1999-02.html, 3
[9] http://www.cert.org/advisories/CA-1999-02.html, 4

them.

Prevention of Trojan horses

System administrators should verify that all software is installed from a legitimate source and has not been modified in transit. If digital signatures are used, make sure that users validate the signature *and* any public keys that are associated with the signature. The signature must be from a trusted source. If digital signatures are not used, it is also suggested to obtain the software on physical media from the manufacturer, such as CDs. This is not totally fail-safe either, but it is safer than simply downloading a software program from the Internet. The importance here is to be aware and be paranoid about installing software from unknown sources. On the other side of this, software developers and distributors should use "…cryptographically strong validation for all software they produce or distribute."[10]

Users must also know that they should not execute anything sent to them via unsolicited e-mail. Also be careful when executing web page content such as Java applets, JavaScript, or ActiveX controls. Note that Internet browsers can be configured to disable the automatic execution of web page content. Another good rule to live by is do not use privileges that are not needed to run a task. For example, do not log in as root or administrator for ordinary tasks that do not require it. If you are logged in as root or administrator and you inadvertently download a Trojan horse, the intruder now has root/administrator privileges and can do whatever he/she wishes on the system. There are tools available that allow you to identify changes in system files. It is recommended that such a tool be installed and configured, such as Tripwire. This kind of tool, although not totally foolproof, allows you to identify the kind of system file changes that an intruder might make in which you may not otherwise take notice.

Firewalls and anti-virus products should be used to help in preventing Trojan horses from affecting your systems. They should be updated regularly with the latest Trojan horse information. It is impossible to detect every Trojan horse, but it can help in preventing the more popular ones. In addition, any open source code to open source products installed should be reviewed first. Any obvious Trojan horses can be detected quickly. The only difficulty with this is that you cannot trust any one entity in the open source world because the code is developed by many different people and there is no control over it. So this may not be possible in every case, but it is something to be aware of.

Cryptographically strong authentication systems should be implemented "…such as *ssh*, for terminal emulation, X.509 public key certificates in web servers, *S/MIME* or *PGP* for e-mail, and kerberos for a variety of services."[11] Additionally, systems that require DNS should be avoided unless your network is designed to support that trust. Examples of these services include telnet, http, ftp, and smtp.

---

[10] http://www.cert.org/advisories/CA-1999-02.html, 5
[11] http://www.cert.org/advisories/CA-1999-02.html, 6

Some final recommendations for prevention of Trojan horses include do not rely on file attributes to determine if a file has a Trojan horse, and use caution when downloading unauthenticated software. Furthermore, educate users on Trojan horses and heighten their awareness on the dangers of them. Educating users really is a huge step in trying to prevent your systems from being infected by a Trojan horse since they will be likely to download software from the Internet freely and open up email attachments that appear to be from trusted sources.

If a Trojan horse does get into your system, there is some anti-virus software available that may be able to clean up your system. However, if an intruder gains access to your system through a Trojan horse, it may not be possible to re-establish trust in the system. In this case, you should disconnect from the network and rebuild the system from trusted software.[12]

APStrojan.qa Trojan horse

The above overview of Trojan horses provides an introduction to a particular Trojan horse that infected many home AOL Internet subscribers. This Trojan horse, called APStrojan.qa, has been around for about one year and it recently emerged again at the end of January 2001. The Trojan horse "…attempts to steal a member's names and passwords and then send them via e-mail to the virus' author. If a user is logged onto AOL 4.0 or 5.0, the virus also tries to e-mail itself to active people on the member's 'buddy list.'"[13] This could allow an intruder to access users' email and other personal information. Non-AOL users who receive the virus "…are not at risk of having passwords stolen, but the virus will slow down the performance of any PC it infects."[14] Note also that the Trojan is only able to e-mail itself to others with the use of versions 4.0 and 5.0. Version 6.0 contains improvements that prevent the virus from replicating itself, but it still can steal passwords from users who have that version. Additionally, users of Version 6.0 who are infected with the Trojan will receive a pop-up message that suggests the user switch back to Version 4.0.[15]

The Trojan horse arrives in an AOL e-mail with a subject line of "hey you" and the following message:

> "hey I finally got my pics scanned…theres like 5 or 6 of them…so just download it and unzip it…and for you people who don't know how to then scroll down…tell me what you think of my pics ok? If you don't know how to unzip then follow these steps When you sign off, AOL will automatically unzip the file, unless you have turned this feature off in your download preferences. If you want to do it manually then On the My Files menu on the AOL toolbar, click Download Manager. In the Download Manager window, click Show Files Downloaded.

[12] http://www.cert.org/advisories/CA-1999-02.html, 6
[13] http://news.cnet.com/news/0-1005-200-4681471.html, 1
[14] http://www.cnn.com/2001/TECH/computing/02/01/aol.virus.idg/index.html, 2
[15] http://www.cnn.com/2001/TECH/computing/02/01/aol.virus.idg/index.html, 2

Select my file and click Decompress"[16]

There is an attachment on the email called MINE.ZIP that contains the supposed "pics." To activate the Trojan horse, the user must unzip the attachment, MINE.ZIP, which unzips into two files, MINE.EXE and README.TXT. The README.TXT file is not significant but it can identify the Trojan's presence with the message it contains, "Did you like it? Write back ok?= " The damaging file is MINE.EXE, which is "…a Visual Basic 5 (VB5) application which hooks into over 20 Windows DLL file. This is a complicated virus that uses a legacy configuration file which is often overlooked in Windows 98 and 95, WIN.INI."[17] The virus makes the WIN.INI file read only which ensures that it will always be loaded in a RUN line in WIN.INI. It also ensures that any program that uses the WIN.INI file is not able to make any changes to it. APStrojan.qa also "…creates three identical hidden files in the root, WINDOWS, and WINDOWSSYSTEM directories: msdos98.exe; uninstallms.exe; and both mine.exe and ReadMe.Txt."[18] Additionally, the Windows Registry is modified so that if WIN.INI is deleted the Trojan horse will still operate. This is the key added to the Windows Registry to enable this function:

HKEY_LOCAL_MACHINESoftwareMicrosoftWindows CurrentVersionRunWindows="c:msdos98.exe"[19]

If your system is infected by this Trojan horse, the best way to clean up your system is with the latest update of your anti-virus software. However, it is possible to fix your system yourself. Following are instructions on how to do this:

- Boot your system into "safe mode" by using the Run command on the Start menu and executing MSCONFIG.EXE. Select the General tab, then the advanced button, and then select Enable Startup Menu. Reboot the system and choose safe mode from the menu when it appears.
- Once the system has rebooted into safe mode, you will have to search for all signs of the Trojan horse and remove them. Start at the registry by executing REGEDIT.EXE from the Run command on the Start menu. When the registry appears, do a search for msdos98.exe. Delete this entry (as noted above) in its entirety. Once this is done, close the registry editor.
- Go back to the Run command on the Start menu and execute SYSEDIT.EXE. Search for the WIN.INI file and look under the Windows section for the line RUN=uninstall.exe. Scroll the entire window for this line because the Trojan horse may try to hide it by moving it somewhere that is not directly visible. Delete the line when found.
- Finally, open Windows Explorer and search for all files mentioned above. If found, delete them. Also include a search for MINE.* so you get all forms, or variations, of the Trojan. Searching for the README.TXE file will be more

[16] http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html, 1
[17] http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html, 1
[18] http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html, 2
[19] http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html, 2

difficult since all programs installed have a file of this name. Therefore, the easiest way to find the README.TXT associated with the Trojan is to use the search dialog to find the text strings "Did you like it? Write back ok?" and some text from the Trojan's e-mail message.

- The last step is to delete the AOL e-mail message and then reboot the system. To disable the Startup Menu, execute MSCONFIG.EXE from the Run menu again, select the General tab, then the advanced button, and then deselect Enable Startup Menu.[20]

From the above description of the APStrojan.qa, you can see how it can be nearly impossible to detect a Trojan horse. It is very powerful as it fools users easily and allows intruders access to systems and valuable information. AOL is a good target for intruders since there is an immense amount of users, which means an immense amount of information that intruders can gain about people. Therefore, users should be aware of Trojan horses and their effects.

This Trojan horse, APStrojan.qa, was rated medium-risk for AOL users. Additionally, it was unclear how many users were affected, although the activity increased 100% during the month of January 2001.[21] This kind of increased activity shows the strength of Trojans and reinforces the need for user awareness and prevention.

[20] http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html, 2
[21] http://www.cnn.com/2001/TECH/computing/02/01/aol.virus.idg/index.html, 1

Bibliography

Barnes, Cecily. "Trojan horse targets AOL subscribers." 1 February 2001. URL: http://news.cnet.com/news/0-1005-200-4681471.html (16 February 2001).

CERT Coordination Center. "CERT Advisory CA-1999-02 Trojan Horses." 8 March 1999. URL: http://www.cert.org/advisories/CA-1999-02.html (16 February 2001).

Fried, Stephen. *Information Security: The Big Picture, K-1*. The SANS Institute, 2000.

Harvey, David A. "The APSTrojan horse rides again." 25 February 2000. URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2449644-77,00.html (16 February 2001).

Niccolai, James. "Virus may steal AOL users' passwords." 1 February 2001. URL: http://www.cnn.com/2001/TECH/computing/02/01/aol.virus.idg/index.html (16 February 2001).