Trojan
Basic Concepts

Prof. Zaheed Shaikh

Overview

- What is Trojan Horse?
- Types of Trojan Horses?
- How can you be infected?
- What do attackers want?

Definition

- **a Trojan horse is a malicious program that is disguised as legitimate software.**

- **Like the gift horse left outside the gates of Troy by the Greeks, Trojan Horses appear to be useful or interesting to an unsuspecting user, but are actually harmful**

Virus or Worm?

- **Trojan horse programs cannot replicate themselves, in contrast to some other types of malware, like viruses or worms.**
- **A Trojan horse can be deliberately attached to otherwise useful software by a cracker, or it can be spread by tricking users into believing that it is a useful program.**

Types of Trojans

- Erasing or overwriting data on a computer
- Corrupting files in a subtle way
- Spreading other malware, such as viruses. In this case the Trojan horse is called a 'dropper'.
- Setting up networks of zombie computers in order to launch DDoS attacks or send Spam.
- Logging keystrokes to steal information such as passwords and credit card numbers (known as a key logger)
- Phish for bank or other account details, which can be used for criminal activities.
- Installing a backdoor on a computer system.

How can you be infected

- **Websites: You can be infected by visiting a rogue website. Internet Explorer is most often targeted by makers of Trojans and other pests. Even using a secure web browser, such as Mozilla's Firefox, if Java is enabled, your computer has the potential of receiving a Trojan horse.**

- **Instant message: Many get infected through files sent through various messengers. This is due to an extreme lack of security in some instant messengers, such of AOL's instant messenger.**

- **E-mail: Attachments on e-mail messages may contain Trojans. Trojan horses via SMTP.**

Sample Delivery

- Attacker will attach the Trojan to an e-mail with an enticing header
- The Trojan horse is typically a Windows executable program file, and must have an executable file extension such as .exe, .com, .scr, .bat, or .pif. Since Windows is configured by default to hide extensions from a user, the Trojan horse's extension might be "masked" by giving it a name such as 'Readme.txt.exe'. With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file.

Where They Live

- **Autostart Folder**
  The Autostart folder is located in C:\Windows\Start Menu\Programs\startup and as its name suggests, automatically starts everything placed there.
- **Win.ini**
  Windows system file using load=Trojan.exe and run=Trojan.exe to execute the Trojan
- **System.ini**
  Using Shell=Explorer.exe trojan.exe results in execution of every file after Explorer.exe
- **Wininit.ini**
  Setup-Programs use it mostly; once run, it's being auto-deleted, which is very handy for trojans to restart

Where They Live(con't)

- **Winstart.bat**
  Acting as a normal bat file trojan is added as @trojan.exe to hide its execution from the user
- **Autoexec.bat**
  It's a DOS auto-starting file and it's used as auto-starting method like this -> c:\Trojan.exe
- **Config.sys**
  Could also be used as an auto-starting method for trojans
- **Explorer Startup**
  Is an auto-starting method for Windows95, 98, ME, XP and if c:\explorer.exe exists, it will be started instead of the usual c:\Windows\Explorer.exe, which is the common path to the file.

What the attacker wants?

- Credit Card Information (often used for domain registration, shopping with your credit card)
- Any accounting data (E-mail passwords, Dial-Up passwords, WebServices passwords, etc.)
- Email Addresses (Might be used for spamming, as explained above)
- Work Projects (Steal your presentations and work related papers)
- Children's names/pictures, Ages (pedophile attacker?!)
- School work (steal your papers and publish them with his/her name on it)

Are you infected?

- Its normal to visit a web site and several more pop-ups to appear with the one you've visited. But when you do completely nothing and suddenly your browser directs you to some page unknown to you, take that serious.
- A strange and unknown Windows Message Box appears on your screen, asking you some personal questions.
- Your Windows settings change by themselves like a new screensaver text, date/time, sound volume changes by itself, your mouse moves by itself, CD-ROM drawer opens and closes.

Well Know Trojans

- **The Secup Trojan displays fake security related messages. When the user clicks on such a message the Trojan opens malicious web site that quietly installs potentially harmful software. Secup also serves undesirable commercial advertisements.**
- **Dmsys is a dangerous Trojan that specializes in infecting various instant messengers and stealing user confidential information. By using its keystroke logging technique, Dmsys easily steals user passwords and captures private conversations. This information is written into a log file, which is then sent to the hacker.**

VNC (Virtual Network Computing)

- **Remote desktop program freely distributed**
- **Server executable attached to e-mail and unknowingly installed on your system**
- **Attacker can use client to uses your system as if he was sitting at the terminal**

Resources

- **Trojan Removal** http://www.2-spyware.com/trojans-removal **updated November 2005**
- **Trojan Horse Computing** http://en.wikipedia.org/wiki/Trojan_horse_(computing**)**
- **Anti-Trojan** http://www.anti-trojan.com/
- **The Complete Windows Trojan Papers** http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Trojans_Paper.html
- **Beware Sony's Trojan Horse** http://www.nctimes.com/articles/2005/11/06/news/columnists/silicon_beach/20_12_0511_5_05.txt **5 November 2005**

How to Make a Trojan

- https://www.gohacking.com/make-trojan-horse/

Algorithm

- Search for the root drive.
- Navigate to the following location on the root drive.
- %systemroot%\Windows\System32
- Create the file named “spceshot.dll“.
- Start dumping the junk data onto the above file and keep increasing its size until the drive is full.
- Once the drive is full, stop the process.