TROJAN & BACKDOORS

Contents

- What is Trojan horse?
- Purposes and use of trojan.
- HOW OUR COMPUTERS ARE AFFECTED...!!
- Beneficial uses of Trojan.
- Examples of Trojan.
- Backdoors.
- Introduction.
- How they work??
- List of Known Backdoors.

WHAT IS TROJAN HORSE??

- A Trojan horse, or Trojan, in computing is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it.
- The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops sneak invading the city of Troy.
- A trojan horse is a program that appears to be something safe, but in is performing tasks such as giving access to your computer or sending personal information to other computers.
- Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

PURPOSES AND USES OF TROJAN

Destructive

- Crashing the computer or device.
- Modification or deletion of files.
- Data corruption.
- Formatting disks, destroying all contents.
- Spread malware across the network.
- Spy on user activities and access sensitive informatio

Use of resources or identity

- Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-service attacks).
- Using computer resources for mining cryptocurrencies
- Using the infected computer as proxy for illegal activities and/or attacks on other computers.
- Infecting other connected devices on the network.

Money theft, ransom

- Electronic money theft.
- Installing ransomware such as CryptoLocker.

HOW OUR COMPUTERS ARE AFFECTED...!!

- A site offers a free download to a program or game that normally costs money. Downloading the pirated version of a program or game allows you to illegally use or play, however, during the install it also installs a trojan horse onto the computer.
- You receive an e-mail that appears to be from a friend asking you to view this fantastic new program or look at a file. Opening the file infects your computer with a trojan horse virus.
- A popular screen saver website has become infected or uploaded infected screen savers. Downloading the screen saver to your computer also installs a trojan horse onto the computer.

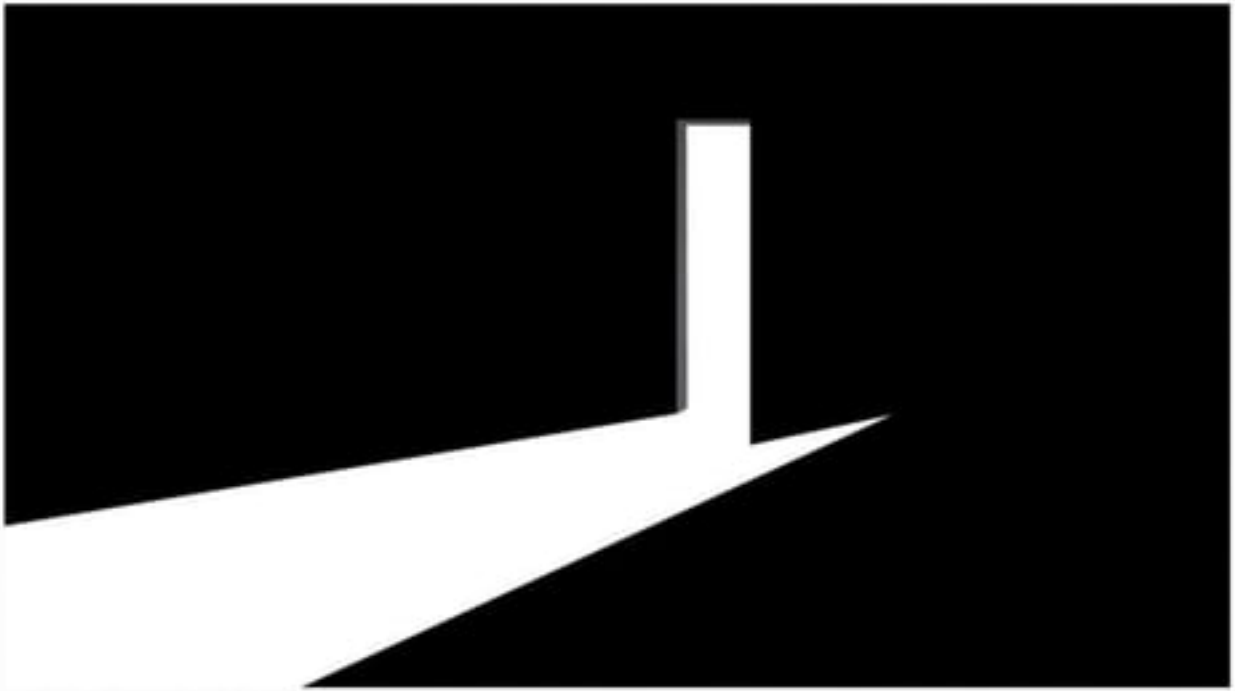
BENEFICIAL USE OF TROJAN

- In German-speaking countries, spyware used or made by the government is sometimes called govware.
- Govware is typically a trojan horse software used to intercept communications from the target computer.
- Some countries like Switzerland and Germany have a legal framework governing the use of such software.
- Examples of govware trojans include the Swiss MiniPanzer and MegaPanzer and the German "state trojan" nicknamed R2D2.

EXAMPLES OF TROJAN

- Netbus Advance System Care
- Subseven or Sub7
- Back Orifice
- Beast
- Zeus
- Flashback Trojan (Trojan BackDoor.Flashback)
- ZeroAccess
- Koobface
- Vundo

BACKDOORS



INTRODUCTION

- A backdoor in a computer system is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- The backdoor may take the form of a hidden part of a program,a separate program (e.g., Back Orifice) may subvert the system through a rootkit.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves, as part of an exploit .

HOW THEY WORK???

Direct connection

- Backdoors are usually based on a client-server network communication,where the server is the attacked machine,
  and the client is the attacker.It is a kind of standard.
- This is called direct connection,when the client directly connects to the server.
- The server application is installed on the computer you want to control and is hidden from the victim.
- When the server application is runned,it will start listening for incoming connections from the client.

Contd.

- Attackers use the client application is different from the server,as it has a GUI (graphic user interface) that allows the attacker to connect to the server remotely,by specifying the IP address of the server computer and the port number (1-65535) on which the server application is listening.
- If the connection is successfull,the client can now retreave information about the server and send commands to it.
- The server recognizes the commands,and executes a part of code for each commands.

LIST OF KNOWN BACKDOORS

- Back Orifice was created in 1998 by hackers from Cult of the Dead Cow group as a remote administration tool. It allowed Windows computers to be remotely controlled over a network and exploited the name similarity with Microsoft BackOffice.
- The Dual_EC_DRBG cryptographically secure pseudorandom number generator was revealed in 2013 to possibly have a kleptographic backdoor deliberately inserted by NSA, who also had the private key to the backdoor.

REFERENCES

- http://feky.bizhat.com/tuts/backdoor.htm
- https://en.wikipedia.org/wiki/Backdoor_(computing)#List_of_known_backdoors
- http://www.computerhope.com/jargon/t/trojhors.htm
- https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Thank you

☺☺☺