Module - 6
Malware Threats

Propagation Malware

1. **Virus** :
   Require Human Assisted Means we have to actually execute the file in order to get infected with virus.
2. **Worms**:
   Automatic, No human Interaction is required

Concealment Malware : These are ones that hide themselves

1. **Rootkits**
   it designed to hide itself by modifying the OS so it is not visible to the end user
2. **Trojan** :
   Simply a code that's has been hiden inside a file

Malware is deployed by the insider threat.

Backdoor :
   it is also known as "trapdoor"
   It allows the used to implement hidden feature
   program executes as expected unless some one activate the backdoor

Logic Bomb :
   Activates based on "logical Condition"
   Many times it based on time and date

How to get in :
   1. Untrusted Source
   2. During Installation
   3. Propagation
   4. Not updating "anti-malware"

Sign of Malware :
   1. Looks at your processes
   2. No Icons ??
   3. No Description
   4. Live in Windows / User profile directory
   5. Weird URL's in their strings
   6. Open TCP/IP endpoints

Any thing over 2000 in PID is launched after the operating systems fires up

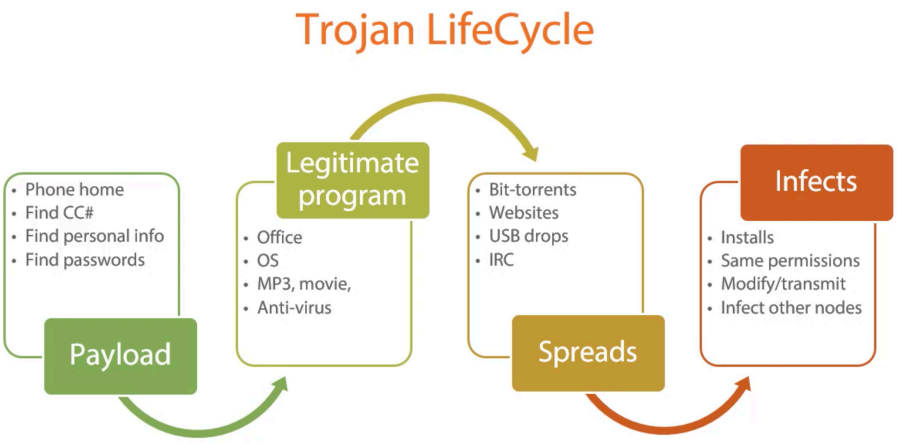
The Numbers Behind Malware :
   - Only 4% of alerts are investigated
   - 1.25 million a year is wasted
   - 317 million is created in 2014
   - Mobile is a HUGE target

Admin Reports :
   - 75% of malware is installed by end-users
   - 71% have protection in place
   - 39% audit less than once in a year

End-User's biggest fear ??
   - 60% loss of data
   - 51% online fraud
   - 43% don't install security updates

 # Trojans :

Trojan horse : A program in which malicious or harmful code (called a "payload") is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage.
Trojan typically contains spyware, keyloggers, rootkits, or other executables.
Trojan can relay or steal data.
Trojans are typically spread through Social Engineering.



Goals of Trojan :

1. Disable Firewalls
2. Replace or delete OS files
3. Open a backdoor
4. Disable Anti-Virus
5. Turns the target into a proxy
6. Add to a Botnet
7. Generating Bogus traffic for DOS
8. Download & install spyware, adware, and malware.
9. Grab screenshots
10. Record Video from camera
11. Steal passwords, codes, financial, and personal Data
12. Use target for spamming

How Trojans communicate and hide ??

Overt Channel : legitimate communication channels used by programs
Covert Channel : used to transfer data in unintended way.

Clue that you have trojans :

1. Anti-Virus is Disabled
2. Ctrl+Alt+Del stops working
3. Random Restart or Shutdown
4. Screen saver change
5. TaskBar Disappear
6. Screen flips / inverts
7. Backgroung Changes
8. Start button disappears
9. Web Browser goes anywhere
10. DVD Ejects randomly
11. Documents start printing
12. Mouse Key reverse
13. Heavy hard drive activity
14. Heavy Network Traffic
15. ISP complaints
16. Unknown purchase on credit cards

Infection via :

1. Click on file
2. Email Attachments
3. Socially Engineered

Different Ways to Enter :

- Physical access (Pendrive)
- Emails
- Freeware
- Shrink-Wrapped
- Fake Application
- Torrents
- Virus

 # Evading Antivirus :

- Change Checksum
- Write your own trojans
- Use a Hex Editor
- Break the Trojans into multiple files
- Modify the syntax
- Avoid ID's Trojans

 # Types of Trojans :

Superdale's Top 10 Trojans :

1. Notification Trojans :

It notify the attacker that the target is affected

1. IRC Trojan : uses IRC channel to communicate to the attacker
2. PHP Trojan : it Sends its data using php server
3. Net Send : sending information or commands to the target machine via netsend
4. ICQ
5. Emails

2. Botnet Trojans :

it help in combining multiple pwned system together, one command to controll all the machine
this type of trojan mostly target Educational / government / military
DOS / SMTP / Click Fraud

3. Proxy Server Trojans :

first it get loaded on the target
it then start prox-ing out for us -> turn the victim machine into a proxy server like chained proxy

4. FTP Server Trojans :

this trojan first install the ftp server and then send a remote connection back to the attacker and after that attack has been provided with full access via ftp protocol.

5. VNC Trojan :

use VNC server
VNC is an utility

6. HTTP / HTTPS Trojans :

- Create a tunnel
- port 80 / 443
- Traffic is converted Base64

7. Command Shell Trojans :

trojan that install a server on the target machine which then in turn opens up a port for the attacker to coonect to.

1. Netcat :

- Telnet into a shell
- Full DNS Checking
- Use ANY local port
- Slowmo : we decrease the speed in which we send and receive information back and forth similar to paranoid mode in nmap so that I will not become very noisy or loud on the network

8. Document Trojans :

we embeded the trojan inside a document and send it through email.

9. Email Trojan :

these Trojans get triggered as we open the mail and it send the command via email back and forth, we can execute, show, open the files.

10. RATs : Remote Access Trojans

ex. Back Orifice / Netbus
Loads small application (server side)

11. Backdoor Trojans :

in this trojan a attacker uses a backdoor program to access the target system
installation of this backdoor is typically done without user's interaction

PoisonIvy RAT

12. Ransomeware
13. Mobile Trojan : Hummer
14. IoT

 # Viruses and Worms :

Differences :

Virus :
Type of malware that attaches itself to a file / program
Sometimes replaces system files
Can't be spread ***WITHOUT*** human interaction. ***
Transmitted via download, drivers and/or emails

Worms :
It Copies itself and replicates
Doesn't require human
Enters via vulnerability
Uses standard file transport features
ex. SQL Slammer : It is a DOS type worm that it slow down the internet as a whole. In this router is flooded with the traffic from the infected servers.

 # Types of Virus and Worms :

1. File Virus : this virus targets files such as executables or COMs
   1. Prepending File Virus : Which write themselves to the beginning of the hosts file code
   2. Appending File Virus : Which write themselves to the end of the file
   3. Overwriting : Overwrites the host code with its own code
   4. Inserting : in which the virus code inject itself inside the gaps inside the host files

2. Cluster Virus : It is a type of virus that actually doesn't change the targeted file or put any info. Inside the file instead it just goes through and modifies the directory information so that the entry points to the virus code instead of the actual program itself.

3. Boot Sector Virus :
MBR (Master Boot Record) : it tracks everything on the harddrive if we destroy the boot sector all the data will erase.
the DOS boot Sector (DBR) : this record is executed whenever the operating system is turned on or boots up
so the what does the boot sector virus does is that : it moves the MBR to a differnt location altogether and replaced it or the original location with our own virus code. So when the OS boots up first the virus is executed then it point to the MBR and the system boots up correctly with virus exected.

4. Macro Virus : using VBA script in Microsoft Word, Excel

5. Polymorphic Virus : These virus typically modifies there code on their own to avoid detetction

6. Metamorphic Virus : these rewrite themselves completely each time that they infect a new file.
Reprogram themselves by taking their own code translating into a temporary representation and get back to the normal code again.
1. Skynet
2. Simile
3. Zmist

7. Cavity Based Virus : they are known as space fillers. They take a document then the virus overwrite the host file with consistent NULL statement and it do this without increasing the length of the file.

8. Encryption Viruses : virus is encrypted with different key so the anti-virus not able to detect it

9. Camouflage virus : It make the copy of the file and put the extension as .com when the file is executed the .com file run first which is infected.

10. Shell virus : Virus code forms a shell around the actual program code making itself the original program and the host code as a sub routine.

11. File Extension Virus : basically it changes the file extension , virus.jpg.exe

12. Tunneling Virus or Stealth Virus : These Virus hide themselves from antivirus programs by hiding the original size of the file or possibly temporarily placing a copy of itself in some other drive in the system.

Life Cycle :

Creation -> Replication -> Discovery -> Resolution -> Purging —
|_____|

 # Phases :

1. **Infection Phase :** Replicates and Attaches
   Need an “Event”
   Setup Files
   Startup
   TSR : Terminate State Ready : Hides the virus in memory it waits inside RAM
2. **Attack Phase :**
   Corruption Begins
   Delete Files
   Altering the file content
   Execute Tasks
   Camouflage

 # Signs that you got infected from virus :

1. Drive issues
2. Video Issues
3. Memory Issues
4. Apps are slow
5. Freezing of system

 # Deployement :
- Downloading a file
- Pirated Software
- Email Attachments
- Not updating their AV/Softwares/apps
- Watch your plugins
- Compromised Legit sites
- Drive by Download
- spear phishing sites
- Click-Jacking
- Search Engine Optimization (SEO)

Investigation of Malware :
1. Sheep Dip
   1. Clean System
   2. SuperDale: Virtualized
   3. Monitoring EVERYTHING

   Setup :
   1. Install your virtualization
   2. Quarantine the network
   3. Disable Shared Folder
   4. Copy malware over

Types of Analysis :

1. Static Analysis : Basically going through and investigating the executable file without running it or installing it
   FingerPrint Analysis : Process of computing the hash value of the binary file to check integrity
   - Comparing hash
   - File Dependencies

2. Dynamic Analysis : We analyse the behaviour of the malware as it running on a monitored environment.

Baseline of System : Taking snapshot of vitualized machine

Host Integrity Monitor : : looking at the changed taking place across the system

- Ports
- Process
- Registry
- Service
- Startup

Event Logs :

- System
- Security
- Application
- Services

Collect String values inside binaries

- BinText : Extract Out text from any files, including the ability to define string value that may be in binary.
- UPX : Collect Compression Methods : Portable executable packer; this can decompress the file without installing it

Port related tools :

- Wireshark
- Sysinternal : Process Explorer and Process Monitor

Debugging :

- Looking for installation instruction
- Looking for installation Location

Sysinternal (Autorun)

- IDA Pro

Online Malware Testing :

- VirusTotal
- Malware Protection Center
- Avast Online scanner

Tools :

1. TcpView : similar to netstat ; Display all the connection made to the outside world and itself
2. Autoruns : Shows everything that going on with your machine
3. DriverView : List the information about your drivers that is loaded on your machine
4. SFC : System File Checker : It will scan your system for any corruption and will restore that corrupted files
   SFC /scannow

 # Countermeasure :

Virus Discovery Methods :

1. Scanning
2. Integrity checking
3. Interceptors

The “Master list” of Countermeasure :

1. Anti-Virus
2. Create a Policy
3. Watch Downloading
4. Update Software
5. Attachment issues
6. Source of the file
7. Keep in informed
8. Scan System Daily
9. Check Media
10. Popup’s
11. Chat Files
12. Firewall and UAC
13.