

## Objectives

Analyze potential Indicators to determine the type of attack

## Malware Classification

- Classification by Vector or Infection method
  - Virus and Worms
    - Spread within code without authorisation
  - Trojans
    - Malicious program concealed within a benign one (in the)
  - Potentially unwanted programs / applications (PUP's/ PAP's)
    - Pre-installed "bbleware" or installed alongside another app
    - Not completely concealed, but installation may be covert (Gray ware)
  - Classification by payload (Spyware, rootkit, remote access trojan)

# Computer Virus's (Designed to replicate)

- Rely on some sort of host file or media
- Only executed when a user performs an action (download, open doc)
  - Non-resident
    - Not on RAM, In files, Infects others each time it's run.
    - only working when the infected host process is running
- Memory-resident
  - Stores itself in ROM (non-volatile)
  - Can infect the PC even when the infected process/program isn't running any more
- Boot
  - Virus code written to the disk sector.
  - Starts when PC is turned on.
- Script / Macro
  - Uses programming features in local scripting engines for the OS/browser.  
(JavaScript, PDF, PowerShell)
- Multipartite
- Polymorphic
- Vector for delivery

# Computer Worms and Fileless Malware

## Worm

- memory-resident
- Can run without user intervention

## Early Computer Worms + Fileless Malware Goals/effects

- Propagate in memory / Over networks
- Consume bandwidth and crash process's

## Fileless Malware (A collection of techniques)

- Exploits remote execution and memory residence to deliver pay loads
  - ↓
  - In host
  - or Dynamic link library
- May run from an initial Script or Trojan
- Persistence Via Registry →
  - Contains info about everything important, Hardware/Apps
  - Malware may need to create an entry in the registry

- Use of shellcode to create backdoors and download additional tools.
- "Living off the land" exploit
  - ↳ Malware code uses legitimate System Scripting tools such as Powershell. Instead of living in an executable to avoid detection.

Advanced Persistant threat / Advanced Volatile threat  
 (APT) (AVT)

- Fileless / Living off the land malware
- Low Observable characteristics (LOC)
    - ↳ Hard to detect

## Spy Ware, Adware, and Key loggers

- Tracking Cookie (Analytics)
- Adware (PUP/Greyware)
  - Changes browser settings
    - e.g. enable cookies
    - Add bookmarks
    - redirection
- Spy Ware (malware)
  - log all local activities

- Use of recording devices / Screenshots
- Redirection

- Keylogger
  - Software and hardware

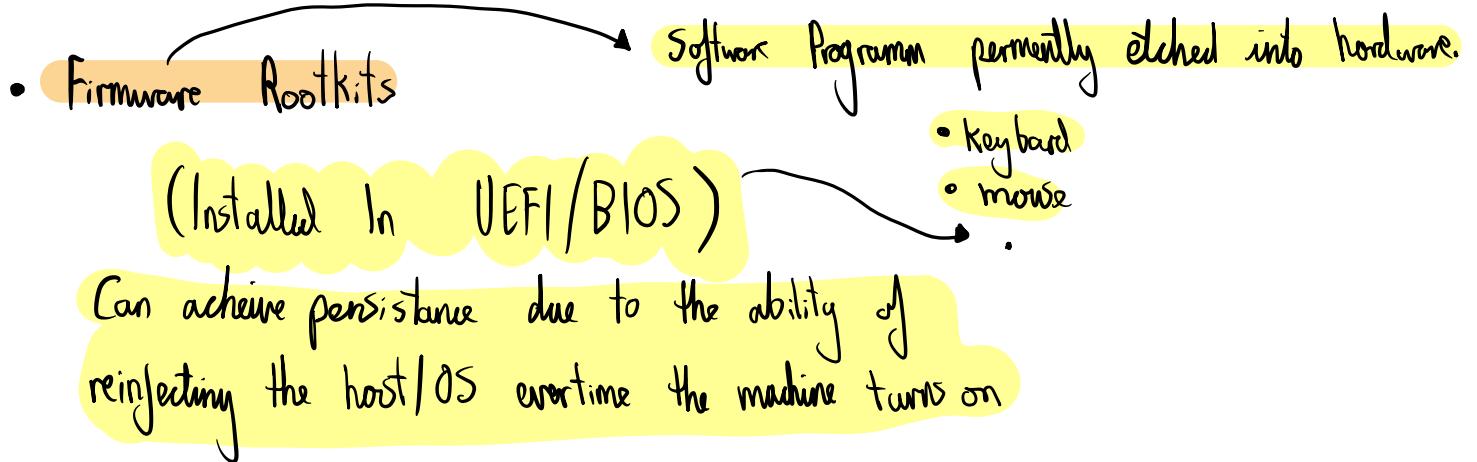
## Back Doors + remote access trojan

- Back Door malware
- Remote access trojan
- Command and control
- Back door from misconfigured or unauthorized software

## Root kits + Abilities

- Local Admin Vs System / root privileges
  - Some exploits will allow the execution of system level process
  - Some will allow root access by using an exploit after being installed
- Rootkit can Replace key System files and utilities

- Purge/Delete log files



## Ransomware, Crypto-Malware and Logic bombs

### • Ransomware

- Nuisance (lock user out by replacing shell)

### • Crypto-Malware

- High Impact ransomware (encrypt data files of drives)

### • Crypto-mining / Cryptojacking

- High jacks resources to mine crypto.

### • Logic bombs

- (a script or attack that will happen once a specific event happens or a date is reached)

Malware Indicators → can require deep analysis to be found.

- Browser changes / Overt ransomware notification

- Anti-Virus Notifications

- End point protection platform (EPPP) / next gen A-V
  - Detects malware based on signature.
- Behavioural based analysis. (AI)

- Sandbox execution

- Cuckoo

- Resource Consumption

- Task manager / Top

- File System changes

- Registry
- Temp files