Objectives

Analyze potential Indicators to determine the type of attack

Malware Classification

- Classification by Vector or Injection method
- Virus and Worms
  - Spread within code without authorization
- Trojans
  - Malicious program concealed within a begnin one (in the
- Potentially unwanted programs / applications (PUP's / PAP's)
  - Pre-Installed "bloatware" 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 preforms an action (download, open doc)
  - Non-resident
    - Not on RAM, In files, Injects others each time its run.
    - only working when the injected host process is running
  - Memory-resident
    - Stores its self in ROM(non-voltile)
    - Can Inject the PC even when the injected 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 deliverey

Computer Worms and Fileless Malware

Worm

- memory-resident
- Can run without user intervention

Early Computer Worms + Fileless Malware Goals/effects

- Propgate in memory / Over networkes
- Consume bandwidth and crash process's

File less Malewrare (A collection of techniques)

- Eploits remote execution and memory residence to deliver pay loads
  - In host
  - or Dynamic link library
- May run from an initial Script or Trojan
- Persistance Via Registry → contains Info about everything important, Hardware/Apps
  - Malewrare may need to create an entry in the registry

- Use of shell code to create backdoors and download additional tools.

- "Living of 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 (APT) / Advanced Volatile threat (AVT)

  Fileless / Live of the land malware

- Low Observable characteristics (LOC)
  - ↳ Hard to detect

Spy Ware, Adware, and Keyloggers

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

- Use of recording devices / screenshots
- Redirection

- Keylogger
  - Software and hardware

Back Doors + remote access trojan

- Back Door malware
- Remot access trojan
- Command and control
- Back door from misconfigured or unauthorised software

Root kits + Abilties

- Local Admin Vs System / root privelages
  - 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 utilties

- Purge / Delete log files

- Firmware Rootkits → Software Programs permanently etched into hardware.

(Installed In UEFI/BIOS) → • keyboard • mouse

Can achieve persistance due to the ability of reinjecting the host/OS everytime the machine turns on

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 / Crypojacking
  - High jack resources to mine cypto.

- 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 ransome ware notifications
- Anti-Virus Notifications
  - End point protection platform (EPPP) / next gen A-V
    - Detects malware based on Signature.
  - Behavioural based analysis. (AI)
- Sandbox execution
  - Cukoo
- Resource Consumption
  - Task manager / Top
- File system changes
  - Registry
  - Temp files