**Module 1 Threats, Attacks & Vulnerabilities**

* 1. **IOC and Types of Malware**

**Malware Attacks**

* Delivery – How did it get to the target?
* Propagation – How did it spread?
* Payload – What does it do once it’s there?
* IOC (Indications of Compromise) – An artefact observed on network/OS that indicates intrusion

**Types of Malware**

* Viruses
* Crypto-malware
* Ransomware
* Worm
* Trojan
* Rootkit
* Keylogger
* Adware
* Spyware
* Bots
* RAT
* Logic Bomb
* Backdoor

**Viruses**

* Program intended to damage a computer system
* Types of viruses:
  1. Armoured virus
     1. Virus that is protected in a way that makes disassembling it difficult
     2. Antivirus have trouble getting to & understanding its code
  2. Companion virus
     1. Virus that creates new program that runs in place of itself
  3. Macro virus
     1. Software exploitation virus that works by using macro feature included in apps Eg. Microsoft Office
  4. Multipartite virus
     1. Virus that attacks system in more than 1 way
  5. Phage virus
     1. Virus that modifies & alters other programs & databases
  6. Polymorphic virus
     1. Virus that changes form/mutates to avoid detection
  7. Retro virus
     1. Virus that attacks/bypasses antivirus installed on the computer
  8. Stealth virus
     1. Virus that attempts to avoid detection by antivirus & OS by remaining in memory

**Crypto-malware & Ransomware**

* Malware that uses cryptography as part of attack
* Prevents users from accessing system/personal files through encryption & demands ransom payment to regain access
* Ransomware authors order that payment be sent via cryptocurrency/online payments/credit card
* Eg. CryptoLocker, WannaCry, Locky, zCrypt, NotPetya

**Rootkit**

* Clandestine computer program designed to provide continued privilege access to computer while hiding its presence
* Software program that has the ability to obtain admin/root-level access & hide from OS
* Eg. NTRootkit, Zeus, Stuxnet, Knark, Adore

**Trojan/Trojan Horse**

* Harmful software that looks legit/included with legit apps
* And app that masquerades as 1 thing to get past scrutiny & does something malicious
  1. 1 major difference between Trojan & Viruses is that Trojan tend not to replicate themselves
* Eg. BackOrifice, Stuxnet, Zeus

**Worms**

* Use network to replicate copies of itself to systems/devices automatically w/o user intervention
* To spread, worms either exploit vulnerability on target system/use social engineering to trick users into executing
* Worm takes advantage of file-transport/information-transport features on system, allowing it to travel unaided
* Eg. ILoveYou, MyDoom, StormWorm, Anna Kournikova, Slammer

**Logic/Time Bomb**

* Any code that is hidden within app & causes something unexpected to happen based on some criteria being met
* For example,

1. Programmer can create a program that always makes sure her name appears on payroll roster; if not key files begin to be erased
2. Backdoor created during certain times

**Keylogger/Keystroke Loggers**

* Software programs/hardware devices that track activities from input devices

1. Keys pressed on keyboard
2. Mouse clicks
3. Screen recorders/scrapers

* Keyloggers are form of spyware where users are unaware their actions are tracked
* Keylogger software typically stores keystrokes in small file, which is either accessed later/automatically emailed to person monitoring your actions

**Bots/Botnets**

* Bot – automated software program (network robot) that collects information on web. In its malicious form, a bot is a compromised computer being controlled remotely
* Bots are AKA “Zombie Computers” due to their ability to operate under remote direction w/o owners’ knowledge
* Botnet – network of compromised computers under control of malicious actor
* Attackers that control botnets referred to as “Bot Herders”/”Bot Masters”

**Backdoor**

* Undocumented way of accessing a system, bypassing the normal authentication mechanisms
* An opening left in a program app (usually by developer) that allows additional access to systems/data. These should be closed when system moved to production

**RATs (Remote Access Trojans/Remote Admin Tools)**

* Software that remotely gives person full control over a device
* Programs that provide capability to allow covert surveillance/ability to gain unauthorised access to victim pc
* Provide capability for attacker to gain unauthorised remote access to victim machine via specially configured communication protocols/backdoors created upon infection

1. Often mimic behaviours of keylogger apps by allowing automated collection of input data

* Eg. SubSeven, Back Orifice, ProRat, Turkojan, Poison-Ivy

**Spyware/Adware**

* Apps that covertly monitors online behaviour w/o user’s knowledge/permission
* Collected data relayed to 3rd parties, often for advertising
* Otherwise, does not harm infected computer/user/data
* There’s line between illegal spyware & legit data collection

**APT (Advanced Persistent Threat)**

* Set of stealthy & continuous hacking processes, orchestrated by person(s) targeting a specific entity
* Usually targets private orgs, states, or both for business/political motives
* APT processes require high degree of covertness over long period of time

1. “advanced” process signifies sophisticated techniques using malware to exploit vulnerabilities in systems
2. “Persistent” process suggests an external command & control system is continuously monitoring & extracting data from specific target
3. “Threat” process indicates human involvement in orchestrating attack