# CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

filename:comptia-secplussy0501-1-1-determining_types_of_malware
Title: Determining Types of Malware
Subtitle: CompTIA Security+ (SY0-501)

## 1.1 Determining Types of Malware

- Given a scenario, analyze indicators of compromise and determine the type of malware
  - Viruses
    - Boot sector virus
    - Polymorphic virus
    - Macro virus
    - Resident virus
      - loads itself into RAM and infects any file or program
      - can load itself into memory with the OS
      - can block the actions of the antivirus
    - File Infectors
    - Stealth virus
      - intercepts calls from the OS
    - Logic Bombs
    - Multipartite Virus
  - Crypto-malware
    - CryptoLocker
    - CryptoDefense
    - CryptoWall
  - Ransomware(type of scareware)
    - https://www.us-cert.gov/ncas/alerts/TA14-295A
    - Ransomware is a type of malware that infects a computer and restricts a user's access to the infected computer or files typically until a ransom is paided.
    - FBI Warning locks the user out of their desktop while not requiring a payment
    - FAKEAV shows fake antimalware scanning results to coax the user into purchasing the bogus software.
  - Worm
    - Polymorphic-worm have the ability to change their form
    - They can encrypt themselves to avoid detection
  - Trojan
    - One difference between trojans and other malware types is that trojans do not try to replicate/propagate themselves]
    - What types of attacks the trojan paves the way for depends on the motivation of the attacker.
    - Botnets, viruses, ransomware, identity theft, data theft, money theft, spying
  - Rootkit
    - Zues = 2007
    - Stuxnet = IDS/SCADA
    - Flame
    - Can monitor & record
      - Audio & Video
      - Capture Screenshots
      - Keyboard activity(keylogger)
      - Network activity
    - Remote control
    - User-mode = simpler, easiest to remove
    - Kernal-mode = OS privilege
    - Firmware-based = Loads itself into memory at the same time or before the OS and drivers
    - Symptoms
      - Bluescreens
      - Keyboard lockups
      - Permission changes
      - Network communication problems(intermittent)
      - Heavy workload
  - Keylogger
    - Survellience Sofware/Hardware
    - Malicious/Non-Malicious
    - Security Auditing
    - Demo capabilities
  - Adware

---

Ransomware stats from the US Computer Emergency Readiness Team

2012 Symantec
Single C2/C&C server, compromised 5,700 Computers

Average ransom = $200
2.9% of all users paid
$33,600 per day
$394,000 per month

---

Use BurnIn on Desktop 1 with all tests and cycles max
Use CMD x 2 running ping -l 65500 local IP