filename:comptia-secplussy0601-1-2-malware
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Malware
Learner Objectives:

Given a scenario, analyze potential indicators to determine the type of attack.

Description:In this episode, the viewer will dive into the world of malware as we compare and contrast the most common malware types such as worms, trojans, rootkits, ransomware bots and more.

---

* Malware \(What is it?\)
    + Virus
    + Virus Types
        - Macro
        - Boot-sector
        - Attachment
        - File Infector
        - Polymorphic
        - Network
    + Worms
    + Fileless
    + RootKit
    + Keyloggers
    + Backdoors
        - Demo creating a user in Active Directory
    + Keyloggers
        - Can be installed by most of these malware types
        - Could be a byproduct of malware attack
    + Ransomware
        - Victims have to pay for attackers to gain money
        - [Cryptomalware] - Does not require a response from the victim or payment for attackers to make money
    + Bots
    + Botnets
    + Command and control
        - [Bots]
    + Trojan

+ Potentially unwanted programs (PUPs)

[Fileless virus]:https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
[Bots]:https://us.norton.com/internetsecurity-malware-what-are-bots.html#:~:text=Malicious%20bots%20are%20defined%20as,compromised%20computers%20and%20similar%20devices.
[Cryptomalware]:https://www.lastline.com/blog/crypto-malware-a-look-at-the-latest-malware-threat/#:~:text=Ransomware%20requires%20that%20someone%20pay,and%20may%20never%20be%20noticed.