

- Filename: eccouncil-ceh31250-v12-7-4-1-viruses-and-worms.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Viruses and Worms

=====

Viruses and Worms

Objectives:

- Define Viruses and and Worms and explain their characteristics
- List the phases of the Virus Lifecycle
- List and define the common virus types
- List and explain how viruses and worms are able to infect computer systems

-
- What is the difference between viruses and worms?
 - Virus
 - Malicious software that attaches itself to host file or program
 - Self-replicating
 - It infects other programs or files
 - Requires human interaction to activate
 - Worm
 - Spreads independently through software vulnerabilities
 - Doesn't require human interaction
 - <https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history>
 - What are typical goals?
 - Destruction/damage of systems
 - Cyber theft
 - Chaos!
 - Hacktivism
 - What are symptoms of infection?
 - Poor system performance
 - Lack of disk space
 - Memory/CPU/Network utilization is high
 - System crashes
 - Missing data
 - What are the stages of the Virus Lifecycle?
 - Design
 - Virus dev designs and develops new virus
 - Programming skills
 - Construction kits
 - Replication
 - Virus is released and spreads
 - Launch
 - User downloads and executes virus
 - Detection
 - Virus is discovered and analyzed
 - Virus attributes and specifics are cataloged
 - Incorporation

- AV orgs add new virus defenses to their software
 - Execution of the damage routine
 - Removing viruses with AV
- What are some common virus types?
 - Boot sector
 - Elk Cloner
 - Stoned
 - Michelangelo
 - File
 - Macro
 - Melissa
 - Polymorphic
 - Encryption Key
 - WannaCry
 - CryptoLocker
 - Metamorphic
 - No Encryption Key
 -
 - Logic Bombs
 - Ransomware