- Filename: eccouncil-ceh31250-v11-7-7-1-malware-countermeasures.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Malware Countermeasures
  ==========

# Malware Countermeasures

# Objectives:

- List common tools and techniques used in defense of malware

---

- What are some countermeasures we can employ to help us defend against malware?
    - **Updates/Patches**
        - Defined
            - Policy
                - Schedule
                - Procedure
                    - In-band
                    - Out-of-band
    - **Run AV,Anti-Malware,EDR solution**
        - Update signatures and engine REGULARLY!
        - Run scans REGULARLY!
        - Enable Real-Time Protections
    - **End-User Security Awareness Training**
        - Don't click links in email
        - Don't download/run email attachments
            - Run AV scan at least
        - Enable 2FA/MFA
        - For Admins
            - Threat feeds
            - Threat modeling
            - Vulnerability assessments / Pentesting
    - **Backups**
        - Defined
            - Policy
                - Schedule
                - Procedure
                    - In-band
                    - Out-of-band
    - **Logging and Monitoring**
        - Network traffic
        - IPS
        - File Integrity
        - System Access/Authentication

        - Use a syslog/SIEM solution
            - Splunk
    - **BLOCKING**
        - Apps from untrusted sources
        - Blacklisting/Whitelisting
        - Firewalls, IDS
        - Disable PowerShell, WMI, Macros, JavaScript, etc
    - **Others**
        - Principal of Least Privilege
        - Defense-in-Depth
        - Disable unnecessary protocols and services
        - Use a system hardening guide, security framework