TASK :- Threat Intelligence

Name: Sahil Dabekar

Intern ID: 339

➢ Tactic Chosen: Defense Evasion (TA0005)

MITRE Link: https://attack.mitre.org/tactics/TA0005/

➢ Description of the Tactic:-

Defense Evasion includes techniques adversaries use to avoid detection throughout their attack lifecycle. This includes disabling security tools, hiding malicious code, obfuscating commands, and impersonating legitimate processes. The goal is to bypass antivirus, EDR, firewalls, and other detection mechanisms.

➢ Objective of This PoC:

To demonstrate how attackers use three defense evasion techniques to avoid detection using:
• Obfuscated Files or Information (T1027)
• Impair Defenses: Disable or Modify Tools (T1562.001)
• Masquerading (T1036)

■ Techniques Selected (with MITRE IDs):

T1027 – Obfuscated Files or Information
https://attack.mitre.org/techniques/T1027/

T1562.001 – Impair Defenses: Disable or Modify Tools
https://attack.mitre.org/techniques/T1562/001/

T1036 – Masquerading
https://attack.mitre.org/techniques/T1036/

Technique 1: T1027 – Obfuscated Files or Information

Description: Adversaries obfuscate scripts, executables, or data to hide their intent and avoid detection.

Purpose: Obfuscation can prevent static analysis and signature-based detection tools from recognizing malicious content.

Real-world Use: Emotet malware used heavily obfuscated PowerShell payloads to evade antivirus detection.

PoC Scenario:
1. Attacker encodes a PowerShell payload using Base64.
2. Payload is embedded in a scheduled task.

Detection:

• Alert on Base64 or encoded strings in PowerShell scripts.
• Monitor usage of 'FromBase64String' function.

Mitigation:
• Enable Script Block Logging.
• Restrict use of encoded commands in PowerShell.

Technique 2: T1562.001 – Impair Defenses: Disable or Modify Tools

Description: Attackers may disable antivirus, logging, or firewalls to operate undetected.

Purpose: To remove barriers to malware execution and persistence.

Real-world Use: TrickBot malware disables Windows Defender via registry modifications.

PoC Scenario:
1. Attacker runs a command to disable Windows Defender real-time monitoring.

Detection:
• Monitor registry changes related to AV settings.
• Alert on use of 'Set-MpPreference' in PowerShell.

Mitigation:
• Apply Group Policies to prevent AV modifications.
• Use EDR tools to monitor and block such changes.

Technique 3: T1036 – Masquerading

Description: Adversaries rename files or use misleading metadata to disguise malicious content as legitimate.

Purpose: To trick users and security tools into trusting or ignoring the file.

Real-world Use: APT32 used renamed payloads to mimic legitimate system binaries (e.g., svchost.exe).

PoC Scenario:
1. Malware is named 'explorer.exe' and placed in a user folder.
2. It mimics system behavior to avoid suspicion.

Detection:
• Monitor for duplicate or unusual file names in user directories.
• Alert on execution from uncommon file paths.

Mitigation:
• Enforce file integrity monitoring.
• Whitelist valid binary paths and names.

Conclusion: Why This PoC Is Valuable

• Highlights how attackers evade detection and persist silently.
• Raises awareness of techniques that bypass traditional AV tools.
• Maps to real-world malware behaviors aligned with MITRE ATT&CK.;
• Helps defenders tune detection and mitigation strategies.

➢ Sources:

• https://attack.mitre.org/techniques/T1027/
• https://attack.mitre.org/techniques/T1562/001/
• https://attack.mitre.org/techniques/T1036/