TASK :- Threat Intelligence

Name: - Saloni Singh

Intern ID: - YOUR-ID

Tactic Chosen: Command and Control (TA0011)

MITRE Link: https://attack.mitre.org/tactics/TA0011/

Description of the Tactic:-

Command and Control (C2) refers to how adversaries communicate with compromised systems to issue commands, move laterally, or exfiltrate data. Techniques under this tactic involve maintaining access, controlling malware, and hiding malicious traffic through encryption or protocol manipulation.

Objective of This PoC:

To demonstrate how attackers use three Command and Control techniques to maintain communication with compromised systems using:
• Application Layer Protocol: Web Protocols (T1071.001)
• Encrypted Channel: HTTPS (T1573.001)
• Remote Access Software (T1219)

■ ***Techniques Selected (with MITRE IDs):***

T1071.001 – Application Layer Protocol: Web Protocols
https://attack.mitre.org/techniques/T1071/001/

T1573.001 – Encrypted Channel: HTTPS
https://attack.mitre.org/techniques/T1573/001/

T1219 – Remote Access Software
https://attack.mitre.org/techniques/T1219/

Technique 1: T1071.001 – Application Layer Protocol: Web Protocols

Description: Attackers use web-based protocols like HTTP/S for C2 communication because it blends with regular internet traffic, making it difficult to detect.

Purpose: Allows attackers to send/receive commands over common ports (80/443) without triggering firewalls.

Real-world Use: APT33 used HTTP POST requests to communicate with infected systems disguised as web traffic.

PoC Scenario:
1. Victim system is infected with malware.
2. Malware contacts http://attacker.com/command for further instructions.
3. Sends data as a POST request every 60 seconds.

Detection:
• Monitor unusual POST traffic to unknown domains.
• Check for beaconing patterns in logs.

Mitigation:
• Use network segmentation.
• Deploy DPI (Deep Packet Inspection).
• Alert on repeated outbound traffic with fixed intervals.

Technique 2: T1573.001 – Encrypted Channel: HTTPS

Description: Attackers use encrypted HTTPS channels to hide their C2 traffic from security monitoring tools.

Purpose: To avoid detection and prevent content inspection.

Real-world Use: FIN6 used HTTPS-based RATs to exfiltrate credit card data over encrypted connections.

PoC Scenario:
1. Attacker configures malware to use HTTPS to access attacker-controlled server.
2. Malware sends encrypted data via port 443.

Detection:
• Use SSL inspection tools (where legal).
• Monitor SSL certificate anomalies.
• Alert on rare SNI values.

Mitigation:
• Implement proxy-based decryption.
• Use certificate pinning validation.
• Restrict outbound traffic to trusted domains.

Technique 3: T1219 – Remote Access Software

Description: Attackers use legitimate tools like AnyDesk, TeamViewer, or custom RATs to maintain persistent access.

Purpose: To interact with the victim system remotely, bypassing traditional malware detection.

Real-world Use: TA505 used legitimate remote software to blend with admin activity during financial theft campaigns.

PoC Scenario:
1. Attacker installs AnyDesk on the victim's system.
2. Uses stolen credentials to log in remotely.

Detection:
• Monitor installation of remote software.
• Alert on traffic to known remote-access domains.

Mitigation:
• Whitelist approved remote tools only.
• Block unauthorized tools by hash or signature.
• Enforce MFA for remote access sessions.

Conclusion: Why This PoC Is Valuable

• Demonstrates realistic C2 paths attackers use post-exploitation.
• Shows how legitimate protocols and tools are abused.
• Helps blue teams detect hidden communication channels.
• Aligns with MITRE ATT&CK; framework and real-world APT activity.

Sources:

• https://attack.mitre.org/techniques/T1071/001/
• https://attack.mitre.org/techniques/T1573/001/
• https://attack.mitre.org/techniques/T1219/