T-SOL GLOBAL

Date: August 30, 2024
DRN: SOC0001
Prepared By: Siddique Reza Khan

Use Case Scenario: Defending Against APT28 Using the MITRE ATT&CK Framework

Overview:

E-corp, a manufacturer of rare earth metals for government and non-government clients, has received classified intelligence indicating a potential cyber attack from APT28, a known advanced persistent threat (APT) group. As a SOC analyst, Sunny needs to identify the tactics, techniques, and procedures (TTPs) of APT28 using the MITRE ATT&CK Framework to proactively protect E-corp's network from potential intrusions.

This document will guide you through the process of using the MITRE ATT&CK Framework to understand and counteract the threats posed by APT28, providing a structured approach to threat hunting, detection, and response.

Step-by-Step Guide: Using the MITRE ATT&CK Framework

1. Understanding the Adversary: APT28

APT28, also known as Fancy Bear, is a sophisticated threat group that primarily targets government, military, security, and energy sectors. To defend against this group, it is crucial to understand their typical TTPs as outlined in the MITRE ATT&CK Framework.

2. Reconnaissance and Initial Access

APT28 often begins its attack by gathering information about potential targets and then gaining initial access. Two key techniques used by APT28 in these stages are:

- **Technique: Spearphishing Link**
    - **Description:** APT28 often employs spearphishing emails containing malicious links that, when clicked by a user, can lead to the download of malware or redirect the user to a compromised website.
    - **Action:** Ensure that email filtering systems are updated and that users are trained to recognize suspicious emails and links.

3. Resource Development

Once initial reconnaissance is complete, APT28 may develop further resources to facilitate the attack. For example:

- **Compromising Email Accounts**
    - **Description:** Compromised email accounts can be used to send phishing emails or for internal reconnaissance.
    - **Action:** Monitor for unusual login patterns or behaviors from corporate email accounts and implement multi-factor authentication (MFA).

4. Execution Phase

If APT28 successfully gains initial access, they typically proceed to execute malicious code. Two techniques to watch for are:

- **Technique 1: Malicious File**
- **Technique 2: Malicious Link**
    - **Description:** The execution of malicious files or links by unsuspecting users can lead to malware deployment.
    - **Action:** Deploy endpoint detection and response (EDR) tools to identify and block the execution of unrecognized or malicious files and links.

5. Scripting Interpreters and Execution Detection

To detect potential script-based attacks, Sunny should look for signs of scripting interpreters being used maliciously, such as:

- **Scripting Interpreters: PowerShell and Windows Command Shell**
    - **Description:** APT28 often uses PowerShell and the Windows Command Shell to execute commands and scripts that can manipulate the system environment or deploy additional payloads.
    - **Action:** Monitor script execution logs and use security information and event management (SIEM) systems to alert on the execution of suspicious scripts.

6. Persistence via Registry Modifications

APT28 may attempt to maintain persistence on compromised systems by altering registry keys:

- **Targeted Registry Keys: Registry Run Keys**
    - **Description:** Changes to registry run keys can ensure that malicious scripts or executables run each time the system starts.
    - **Action:** Regularly audit registry keys for unauthorized changes and use tools to revert any unauthorized modifications.

7. Defense Evasion and System Binary Execution

APT28 may use system binaries to evade detection:

- **System Binary: Rundll32**
    - **Description:** This binary can be used to run DLL files and scripts, often bypassing traditional security controls.
    - **Action:** Monitor the use of rundll32.exe and alert on its execution from unexpected directories or with unusual parameters.

8. Discovery and Lateral Movement

APT28 uses tools like tcpdump to sniff network traffic and exploits remote services for lateral movement:

- **Technique: Network Sniffing**
    - **Description:** Capturing network packets to gather sensitive information.
    - **Action:** Detect unauthorized network sniffing tools and ensure they are promptly removed.
- **Remote Services: SMB/Windows Admin Shares**
    - **Description:** Used to move laterally within a network by exploiting remote services.
    - **Action:** Monitor SMB traffic for unusual access patterns and enforce strong access controls.

9. Data Exfiltration Prevention

Preventing data exfiltration is critical to protect intellectual property:

- **Information Repository Target: SharePoint**
    - **Description:** APT28 may target SharePoint servers to access and steal intellectual property.
    - **Action:** Apply strict access controls and monitor for abnormal access or data download patterns.

10. Blocking Command and Control (C2) Communication

To prevent APT28 from exfiltrating data, Sunny should focus on blocking potential C2 channels:

- **Proxy Techniques: External Proxy and Multi-hop Proxy**
    - **Description:** These techniques involve routing malicious traffic through multiple intermediaries to avoid detection.
    - **Action:** Implement network-based anomaly detection to identify unusual outbound traffic patterns and block known malicious IPs and domains.

Conclusion: Building a Resilient Defense

By utilizing the MITRE ATT&CK Framework, Sunny can systematically identify and mitigate the TTPs used by APT28. This proactive approach not only helps in detecting ongoing attacks but also strengthens E-corp's overall security posture, ensuring that intellectual property and sensitive data remain protected against sophisticated adversaries.

Publication Note: This use case scenario can serve as a comprehensive guide for SOC teams to understand and apply the MITRE ATT&CK Framework in real-world scenarios, enhancing threat detection and response capabilities.

Reference

1. Eviction, https://tryhackme.com/r/room/eviction
2. Lab Links, https://static-labs.tryhackme.cloud/sites/eviction/
3. APT28, https://attack.mitre.org/groups/G0007/