**Defence Strategy Against APT- 34 Using MITRE ATT&CK Framework**

**Team -C**

**28805- Deep Raghuwanshi**

**28806- Kundan Keshav Gawade**

**28807- Prajwal Thangan**

**28809- Devashish Lokhande**

**29080- V.S Goptherya**

**29084- Thulasi Ram**

**Content**

* **What is MITRE ATT&CK Framework**
* **Why it is used**
* **What is APT- 34**
* **T- Tactics**
* **T- Technique**
* **P- Procedure**
* **Recommeded Security Tools**
* **Conclusion**

**What is MITRE ATT&CK**

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge

**Why it is Used**

* MITRE ATT&CK is a valuable framework for cybersecurity professionals because it provides a standardized and comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs).
* This framework helps organizations understand how attackers behave, develop more effective defenses, and improve their incident response capabilities.
* It also facilitates communication and collaboration among security teams by providing a shared language for discussing cyber threats**.**

**What is APT-34**

* APT-34 or Oilrig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014.
* The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications.
* It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets.
* The group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.

**Tactics, Technique and Procedure (TTPs)**

**1. Reconnaissance (TA0043)**

APT34 conducts extensive reconnaissance to identify targets.

**Techniques Used:**

* **T1595** (Active Scanning)
* **T1592** (Gather Victim Host Information)
* **T1589** (Gather Victim Identity Information)

**Prevention & Detection:**

* **Monitor for scanning activities** (e.g., excessive port scans, DNS queries).
* **Restrict public-facing employee information** (LinkedIn, corporate directories).
* **Deploy honeypots** to detect reconnaissance attempts.

**2. Initial Access (TA0001)**

APT34 commonly uses phishing and exploit vulnerabilities.

**Techniques Used:**

* **T1566** (Phishing – Spear phishing Link/Attachment)
* **T1195** (Supply Chain Compromise)
* **T1078** (Valid Accounts – Stolen credentials)

**Prevention & Detection:**

* **Email Filtering (DMARC, DKIM, SPF)** to block phishing.
* **User Awareness Training** (simulated phishing tests).
* **Multi-Factor Authentication (MFA)** to prevent credential misuse.
* **Patch Management** (prioritize CVEs exploited by APT34).

**3. Execution (TA0002)**

APT34 leverages scripts and living-off-the-land binaries (LOL Bins).

**Techniques Used:**

* **T1059** (Command-Line Interface – PowerShell, WMI, BASH)
* **T1204** (User Execution – Malicious documents)

**Prevention & Detection:**

* **Restrict script execution** (AppLocker, PowerShell Constrained Language Mode).
* **Monitor command-line activity** (Sysmon, EDR solutions).
* **Disable Office macros** or use **macro allowlisting**.

**4. Persistence (TA0003)**

APT34 establishes long-term access.

**Techniques Used:**

* **T1547** (Boot or Logon Auto start Execution – Registry Run Keys)
* **T1053** (Scheduled Task/Job)
* **T1136** (Create Account – Adding backdoor users)

**Prevention & Detection:**

* **Monitor registry changes** (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run).
* **Audit scheduled tasks** (compare against baseline).
* **Enforce least privilege** (prevent unauthorized account creation).

**5. Privilege Escalation (TA0004)**

APT34 exploits misconfigurations to gain higher privileges.

**Techniques Used:**

* **T1548** (Abuse Elevation Control Mechanism – Bypass UAC)
* **T1068** (Exploitation for Privilege Escalation)

**Prevention & Detection:**

* **Patch known privilege escalation vulnerabilities**.
* **Enable User Account Control (UAC)** at highest level.
* **Monitor for unusual process elevation** (e.g., cmd.exe spawning powershell.exe as admin).

**6. Defense Evasion (TA0005)**

APT34 uses obfuscation and disabling security tools.

**Techniques Used:**

* **T1027** (Obfuscated Files or Information – Encrypted C2 traffic)
* **T1562** (Impair Defenses – Disable logging, kill AV processes)

**Prevention & Detection:**

* **Deploy EDR/XDR solutions** with behavioral detection.
* **Monitor for unexpected process termination** (e.g., taskkill /f /im MsMpEng.exe).
* **Enable tamper protection** in security tools.

**7. Credential Access (TA0006)**

APT34 steals credentials for lateral movement.

**Techniques Used:**

* **T1003** (OS Credential Dumping – Mimikatz, LSASS dumping)
* **T1110** (Brute Force – Password spraying)

**Prevention & Detection:**

* **Enable Credential Guard** (Windows) to protect LSASS.
* **Monitor for abnormal authentication attempts** (SIEM alerts on multiple failed logins).
* **Use strong, unique passwords** + MFA.

**8. Lateral Movement (TA0008)**

APT34 moves across networks using valid accounts and exploits.

**Techniques Used:**

* **T1021** (Remote Services – RDP, SMB, WinRM)
* **T1072** (Lateral Tool Transfer – PsExec, WMI)

**Prevention & Detection:**

* **Segment networks** to restrict unnecessary lateral movement.
* **Monitor for anomalous RDP/SMB connections** (e.g., unusual login times).
* **Restrict admin access** to critical systems.

**9. Exfiltration (TA0010)**

APT34 exfiltrates data via FTP, HTTP, or cloud storage.

**Techniques Used:**

* **T1041** (Exfiltration Over C2 Channel)
* **T1567** (Exfiltration Over Web Service – Dropbox, Mega)

**Prevention & Detection:**

* **Monitor large data transfers** (DLP solutions).
* **Block unauthorized cloud storage access**.
* **Encrypt sensitive data** at rest and in transit.

**10. Command & Control (TA0011)**

APT34 uses encrypted C2 channels.

**Techniques Used:**

* **T1071** (Application Layer Protocol – HTTP/S, DNS tunneling)
* **T1132** (Data Encoding – Base64, XOR)

**Prevention & Detection:**

* **Block known malicious domains/IPs** (Threat Intelligence feeds).
* **Inspect encrypted traffic** (SSL decryption where possible).
* **Monitor for unusual DNS queries** (long subdomains, high frequency).

**Recommended Security Tools**

| **Category** | **Tools** |
| --- | --- |
| **EDR/XDR** | CrowdStrike, Microsoft Defender for Endpoint, SentinelOne |
| **SIEM** | Splunk, Microsoft Sentinel, IBM QRadar |
| **Network Security** | Firewalls (Palo Alto, Fortinet), IDS/IPS (Snort, Suricata) |
| **Email Security** | Proofpoint, Mimecast |
| **DLP** | Symantec DLP, Microsoft Purview |
| **Threat Intel** | VirusTotal, AlienVault OTX, MITRE ATT&CK Navigator |

**Conclusion**

To defend against APT34:

1. **Patch vulnerabilities** and enforce **least privilege**.
2. **Monitor for TTPs** using MITRE ATT&CK-based detection rules.
3. **Train employees** to recognize phishing.
4. **Segment networks** and **restrict lateral movement**.
5. **Deploy layered defenses** (EDR, SIEM, DLP).

By aligning defenses with **MITRE ATT&CK**, organizations can systematically disrupt APT34’s attack chain.