MITRE ATT&CK; Technique Quick Reference

INITIAL ACCESS

T1566 – Phishing – Methods: Email links, attachments, spear-phishing; Evidence: Mail gateways, user inbox logs.

T1190 – Exploit Public-Facing Application – Methods: CVE exploit chains; Evidence: Web server logs, WAF alerts.

T1195 – Supply Chain Compromise – Methods: Vendor trojaned software; Evidence: Installer hashes, external host references.

EXECUTION

T1059 – Command and Scripting Interpreter – Methods: PowerShell, Bash; Evidence: Event ID 4688, script logs.

T1204 – User Execution – Methods: Macros, double-click; Evidence: Office startup logs, ShellExecute calls.

T1569 – System Services – Methods: Service installation, DLL hijacking; Evidence: SCM events, service registry keys.

PERSISTENCE

T1053 – Scheduled Task/Job – Methods: cron jobs, Task Scheduler; Evidence: Task XML, Event ID 106.

T1547 – Boot or Logon Autostart Execution – Methods: Run keys, startup folder; Evidence: Registry Run entries.

T1505 – Server Software Component – Methods: Web shells; Evidence: Unexpected web files, HTTP POSTs.

PRIVILEGE ESCALATION

T1068 – Exploitation for Privilege Escalation – Methods: Kernel exploits; Evidence: Crash dumps, unsigned driver loads.

T1134 – Access Token Manipulation – Methods: Token impersonation; Evidence: DuplicateTokenEx calls.

DEFENSE EVASION

T1027 – Obfuscated Files or Information – Methods: Base64, XOR; Evidence: High file entropy, suspicious CLI flags.

T1055 – Process Injection – Methods: DLL injection, reflective loads; Evidence: Remote thread creation.

T1014 – Rootkit – Methods: Kernel module hooks; Evidence: Hidden processes, abnormal kernel modules.

CREDENTIAL ACCESS

T1003 – Credential Dumping – Methods: LSASS memory dump; Evidence: ProcDump logs, Mimikatz traces.

T1558 – Kerberoasting – Methods: AS-REP roasting; Evidence: TGS request anomalies.

T1110 – Brute Force – Methods: SSH/RDP guesses; Evidence: Login failures, account lockouts.

DISCOVERY

T1082 – System Information Discovery – Methods: hostname, os APIs; Evidence: WMI queries.

T1046 – Network Service Scanning – Methods: Nmap, masscan; Evidence: SYN floods.

T1087 – Account Discovery – Methods: net user, AD queries; Evidence: LDAP query logs.

LATERAL MOVEMENT

T1021 – Remote Services – Methods: RDP/SSH; Evidence: Event ID 4624 type 10, SSH logs.

T1550 – Alternate Authentication Material – Methods: Pass-the-Hash; Evidence: NTLM anomalies.

T1075 – Pass the Ticket – Methods: Kerberos ticket injection; Evidence: KERB_SUBMIT_TICKET calls.

COLLECTION

T1056 – Input Capture – Methods: Keyloggers; Evidence: Unusual API hooks.

T1005 – Data from Local System – Methods: File read ops; Evidence: File access logs.

T1113 – Screen Capture – Methods: GDI calls; Evidence: Screenshot files.

EXFILTRATION

T1020 – Automated Exfiltration – Methods: Scheduled scripts; Evidence: Large outbound transfers.

T1567 – Exfiltration Over Web Service – Methods: HTTP POST to cloud; Evidence: Proxy logs.

IMPACT

T1486 – Data Encrypted for Impact – Methods: Ransomware; Evidence: VSS deletion, file rename patterns.

T1485 – Data Destruction – Methods: Disk wipers; Evidence: Bulk deletes.

T1490 – Inhibit System Recovery – Methods: vssadmin delete shadows; Evidence: VSS disable logs.

External References:

ATT&CK; Design & Philosophy: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
Getting Started with ATT&CK;:
https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf
ATT&CK; Navigator: https://github.com/mitre-attack/attack-navigator