Enterprise matrix

# MITRE ATT&CK

## DERANT ANGLE

### What is MITRE Framework?

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

### Why is it relevant?

Defending against cyber-crime is a difficult task. Especially with attackers having endless tools at their disposal, knowing what indicators to look out for and where to start can seem impossible.

MITRE Attack framework, ensure defenders get an overview of what they should defend against and exemplify the actions an attacker might take to compromise their target. Security teams and organizations can utilize this framework to evaluate the effectiveness of their current security setup and processes.

If you want to learn more about the techniques, you can visit
https://attack.mitre.org/techniques/enterprise/

### Derant Angle

To make it easier for you to understand where our platform detects these techniques, we have built a matrix for you.

| ATT&CK Tactic | Techniques | Sub-Techniques |
|---|---|---|
| Reconnaissance | Active Scanning<br>Gather Victim Host Information<br>Gather Victim Network Information<br>Phishing for Information | Spearhishing link |
| Resource Development | Compromise Infrastructure | Botnet |
| Initial Access | Drive-by Compromise<br>Exploit Public-Facing Application<br>External Remote Services<br>Hardware Additions<br>Phishing<br>Supply Chain Compromise<br>Trusted Relationship<br>Valid Accounts | Spearphishing Link<br>Spearphishing via Service<br>Compromise Software Supply chain |
| Execution | | |
| Persistence | BITS Jobs<br>Browser Extensions<br>External Remote Services<br>Server Software Component<br>Traffic Signalling<br>Valid Accounts | Webshell |
| Privilege Escalation | Valid Accounts | |

| | | |
|---|---|---|
| Defense Evasion | BITS Jobs<br>Network Boundary Bridging<br>Rogue Domain Controller<br>Rootkit<br>Traffic Signalling<br>Use Alternate Authentication Material<br>Valid Accounts | Web session cookie |
| Credential Access | Adversary-in-the-Middle<br>Brute Force<br>Network Sniffing<br>OS Credential Dumping<br>Steal or Forge Kerberos Tickets | Cached Domain Credentials<br>DCSync |
| Discovery | Domain Trust Discovery Group Policy Discovery<br>Network Service Scanning<br>Network Share Discovery<br>Network Sniffing<br>Password Policy Discovery<br>Remote System Discovery | |
| Lateral Movement | Exploitation of Remote Services<br>Internal Spear phishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking<br>Remote Services<br>Taint Shared Content<br>Use Alternate Authentication Material | Web Session cookie |
| Collection | Adversary-in-the-Middle<br>Automated Collection<br>Data from Configuration Repository<br>Data from Network Shared Drive<br>Data Staged<br>Email Collection | Remote Email collection |
| Command and Control | Application Layer Protocol<br>Data Encoding<br>Data Obfuscation<br>Dynamic Resolution<br>Encrypted Channel<br>Fallback Channels<br>Ingress Tool Transfer<br>Multi-Stage Channels<br>Non-Application Layer Protocol<br>Non-Standard Port<br>Protocol Tunneling<br>Proxy<br>Remote Access Software<br>Traffic Signalling<br>Web Service | |
| Exfiltration | Automated Exfiltration<br>Data Transfer Size Limits<br>Exfiltration Over Alternative Protocol<br>Exfiltration Over C2 Channel<br>Exfiltration Over Other Network Medium<br>Exfiltration Over Web Service<br>Scheduled Transfer | |
| Impact | Defacement<br>Endpoint Denial of Service<br>Network Denial of Service<br>Resource Hijacking | External Defacement |

www.derant.com