about

# Lumeta

domain

# Enterprise ATT&CK v9

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T1595: Active Scanning | T1583: Acquire Infrastructure | T1199: Trusted Relationship | T1047: Windows Management Instrumentation | T1133: External Remote Services | T1078: Valid Accounts | T1564: Hide Artifacts | T1110: Brute Force | T1018: Remote System Discovery | T1210: Exploitation of Remote Services | T1530: Data from Cloud Storage Object | T1571: Non-Standard Port | T1048: Exfiltration Over Alternative Protocol | T1531: Account Access Removal |
| T1592: Gather Victim Host Information | T1586: Compromise Accounts | T1190: Exploit Public-Facing Application | T1059: Command and Scripting Interpreter | T1205: Traffic Signaling | T1548: Abuse Elevation Control Mechanism | T1578: Modify Cloud Compute Infrastructure | T1555: Credentials from Password Stores | T1016: System Network Configuration Discovery | T1021: Remote Services | T1560: Archive Collected Data | T1071: Application Layer Protocol | T1011: Exfiltration Over Other Network Medium | T1489: Service Stop |
| T1590: Gather Victim Network Information | T1584: Compromise Infrastructure | T1133: External Remote Services | T1609: Container Administration Command | T1078: Valid Accounts | T1134: Access Token Manipulation | T1599: Network Boundary Bridging | T1212: Exploitation for Credential Access | T1049: System Network Connections Discovery | T1534: Internal Spearphishing | T1123: Audio Capture | T1105: Ingress Tool Transfer | T1020: Automated Exfiltration | T1485: Data Destruction |
| T1596: Search Open Technical Databases | T1587: Develop Capabilities | T1200: Hardware Additions | T1610: Deploy Container | T1098: Account Manipulation | T1547: Boot or Logon Autostart Execution | T1535: Unused/Unsupported Cloud Regions | T1187: Forced Authentication | T1007: System Service Discovery | T1570: Lateral Tool Transfer | T1119: Automated Collection | T1095: Non-Application Layer Protocol | T1030: Data Transfer Size Limits | T1486: Data Encrypted for Impact |
| T1589: Gather Victim Identity Information | T1585: Establish Accounts | T1078: Valid Accounts | T1203: Exploitation for Client Execution | T1197: BITS Jobs | T1037: Boot or Logon Initialization Scripts | T1562: Impair Defenses | T1606: Forge Web Credentials | T1087: Account Discovery | T1563: Remote Service Session Hijacking | T1115: Clipboard Data | T1219: Remote Access Software | T1041: Exfiltration Over C2 Channel | T1565: Data Manipulation |
| T1591: Gather Victim Org Information | T1588: Obtain Capabilities | T1189: Drive-by Compromise | T1559: Inter-Process Communication | T1547: Boot or Logon Autostart Execution | T1543: Create or Modify System Process | T1553: Subvert Trust Controls | T1056: Input Capture | T1580: Cloud Infrastructure Discovery | T1091: Replication Through Removable Media | T1602: Data from Configuration Repository | T1205: Traffic Signaling | T1052: Exfiltration Over Physical Medium | T1491: Defacement |
| T1598: Phishing for Information | T1608: Stage Capabilities | T1566: Phishing | T1106: Native API | T1037: Boot or Logon Initialization Scripts | T1484: Domain Policy Modification | T1205: Traffic Signaling | T1557: Man-in-the-Middle | T1526: Cloud Service Discovery | T1072: Software Deployment Tools | T1213: Data from Information Repositories | T1092: Communication Through Removable Media | T1567: Exfiltration Over Web Service | T1561: Disk Wipe |
| T1597: Search Closed Sources | | T1091: Replication Through Removable Media | T1053: Scheduled Task/Job | T1176: Browser Extensions | T1611: Escape to Host | T1078: Valid Accounts | T1556: Modify Authentication Process | T1046: Network Service Scanning | T1080: Taint Shared Content | T1005: Data from Local System | T1132: Data Encoding | T1029: Scheduled Transfer | T1499: Endpoint Denial of Service |
| T1593: Search Open Websites/Domains | | T1195: Supply Chain Compromise | T1129: Shared Modules | T1554: Compromise Client Software Binary | T1546: Event Triggered Execution | T1548: Abuse Elevation Control Mechanism | T1040: Network Sniffing | T1069: Permission Groups Discovery | T1550: Use Alternate Authentication Material | T1039: Data from Network Shared Drive | T1001: Data Obfuscation | T1537: Transfer Data to Cloud Account | T1495: Firmware Corruption |
| T1594: Search Victim-Owned Websites | | | T1072: Software Deployment Tools | T1136: Create Account | T1068: Exploitation for Privilege Escalation | T1134: Access Token Manipulation | T1003: OS Credential Dumping | T1518: Software Discovery | | T1025: Data from Removable Media | T1568: Dynamic Resolution | | T1490: Inhibit System Recovery |
| | | | T1569: System Services | T1543: Create or Modify System Process | T1574: Hijack Execution Flow | T1197: BITS Jobs | T1528: Steal Application Access Token | T1082: System Information Discovery | | T1074: Data Staged | T1573: Encrypted Channel | | T1498: Network Denial of Service |
| | | | T1204: User Execution | T1546: Event Triggered Execution | T1055: Process Injection | T1612: Build Image on Host | T1558: Steal or Forge Kerberos Tickets | T1614: System Location Discovery | | T1114: Email Collection | T1008: Fallback Channels | | T1496: Resource Hijacking |
| | | | | T1574: Hijack Execution Flow | T1053: Scheduled Task/Job | T1140: Deobfuscate/Decode Files or Information | T1539: Steal Web Session Cookie | T1010: Application Window Discovery | | T1056: Input Capture | T1104: Multi-Stage Channels | | T1529: System Shutdown/Reboot |
| | | | | T1525: Implant Internal Image | | T1610: Deploy Container | T1111: Two-Factor Authentication Interception | T1217: Browser Bookmark Discovery | | T1185: Man in the Browser | T1572: Protocol Tunneling | | |
| | | | | T1556: Modify Authentication Process | | T1006: Direct Volume Access | T1552: Unsecured Credentials | T1538: Cloud Service Dashboard | | T1557: Man-in-the-Middle | T1090: Proxy | | |
| | | | | T1137: Office Application Startup | | T1484: Domain Policy Modification | | T1613: Container and Resource Discovery | | T1113: Screen Capture | T1102: Web Service | | |
| | | | | T1542: Pre-OS Boot | | T1480: Execution Guardrails | | T1482: Domain Trust Discovery | | T1125: Video Capture | | | |
| | | | | T1053: Scheduled Task/Job | | T1211: Exploitation for Defense Evasion | | T1083: File and Directory Discovery | | | | | |
| | | | | T1505: Server Software Component | | T1222: File and Directory Permissions Modification | | T1135: Network Share Discovery | | | | | |
| | | | | | | T1574: Hijack Execution Flow | | T1040: Network Sniffing | | | | | |
| | | | | | | T1070: Indicator Removal on Host | | T1201: Password Policy Discovery | | | | | |
| | | | | | | T1202: Indirect Command Execution | | T1120: Peripheral Device Discovery | | | | | |
| | | | | | | T1036: Masquerading | | T1057: Process Discovery | | | | | |
| | | | | | | T1556: Modify Authentication Process | | T1012: Query Registry | | | | | |
| | | | | | | T1112: Modify Registry | | T1033: System Owner/User Discovery | | | | | |
| | | | | | | T1601: Modify System Image | | T1124: System Time Discovery | | | | | |
| | | | | | | T1027: Obfuscated Files or Information | | T1497: Virtualization/Sandbox Evasion | | | | | |
| | | | | | | T1542: Pre-OS Boot | | | | | | | |
| | | | | | | T1055: Process Injection | | | | | | | |
| | | | | | | T1207: Rogue Domain Controller | | | | | | | |
| | | | | | | T1014: Rootkit | | | | | | | |
| | | | | | | T1218: Signed Binary Proxy Execution | | | | | | | |
| | | | | | | T1216: Signed Script Proxy Execution | | | | | | | |
| | | | | | | T1221: Template Injection | | | | | | | |
| | | | | | | T1127: Trusted Developer Utilities Proxy Execution | | | | | | | |
| | | | | | | T1550: Use Alternate Authentication Material | | | | | | | |
| | | | | | | T1497: Virtualization/Sandbox Evasion | | | | | | | |
| | | | | | | T1600: Weaken Encryption | | | | | | | |
| | | | | | | T1220: XSL Script Processing | | | | | | | |