about

# Lumeta

domain

# Enterprise ATT&CK v9

## Reconnaissance

- T1595: Active Scanning
  - T1595.001: Scanning IP Blocks
  - T1595.002: Vulnerability Scanning
- T1592: Gather Victim Host Information
  - T1592.001: Hardware
  - T1592.002: Software
  - T1592.003: Firmware
  - T1592.004: Client Configurations
- T1590: Gather Victim Network Information
  - T1590.001: Domain Properties
  - T1590.002: DNS
  - T1590.003: Network Trust Dependencies
  - T1590.004: Network Topology
  - T1590.005: IP Addresses
  - T1590.006: Network Security Appliances
- T1596: Search Open Technical Databases
  - T1596.002: WHOIS
  - T1596.001: DNS/Passive DNS
  - T1596.003: Digital Certificates
  - T1596.004: CDNs
  - T1596.005: Scan Databases
- T1589: Gather Victim Identity Information
- T1591: Gather Victim Org Information
- T1598: Phishing for Information
- T1597: Search Closed Sources
- T1593: Search Open Websites/Domains
- T1594: Search Victim-Owned Websites

## Resource Development

- T1583: Acquire Infrastructure
- T1586: Compromise Accounts
- T1584: Compromise Infrastructure
- T1587: Develop Capabilities
- T1585: Establish Accounts
- T1588: Obtain Capabilities
- T1608: Stage Capabilities

## Initial Access

- T1199: Trusted Relationship
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1200: Hardware Additions
- T1078: Valid Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts
  - T1078.004: Cloud Accounts
- T1189: Drive-by Compromise
- T1566: Phishing
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise

## Execution

- T1047: Windows Management Instrumentation
- T1059: Command and Scripting Interpreter
- T1609: Container Administration Command
- T1610: Deploy Container
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
- T1106: Native API
- T1053: Scheduled Task/Job
- T1129: Shared Modules
- T1072: Software Deployment Tools
- T1569: System Services
- T1204: User Execution

## Persistence

- T1133: External Remote Services
- T1205: Traffic Signaling
- T1078: Valid Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts
  - T1078.004: Cloud Accounts
- T1098: Account Manipulation
- T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1176: Browser Extensions
- T1554: Compromise Client Software Binary
- T1136: Create Account
- T1543: Create or Modify System Process
- T1546: Event Triggered Execution
- T1574: Hijack Execution Flow
- T1525: Implant Internal Image
- T1556: Modify Authentication Process
- T1137: Office Application Startup
- T1542: Pre-OS Boot
- T1053: Scheduled Task/Job
- T1505: Server Software Component

## Privilege Escalation

- T1078: Valid Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts
  - T1078.004: Cloud Accounts
- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1543: Create or Modify System Process
- T1484: Domain Policy Modification
- T1611: Escape to Host
- T1546: Event Triggered Execution
- T1068: Exploitation for Privilege Escalation
- T1574: Hijack Execution Flow
- T1055: Process Injection
- T1053: Scheduled Task/Job

## Defense Evasion

- T1564: Hide Artifacts
  - T1564.001: Hidden Files and Directories
  - T1564.002: Hidden Users
  - T1564.003: Hidden Window
  - T1564.004: NTFS File Attributes
  - T1564.005: Hidden File System
  - T1564.006: Run Virtual Instance
  - T1564.007: VBA Stomping
- T1578: Modify Cloud Compute Infrastructure
  - T1578.001: Create Snapshot
  - T1578.002: Create Cloud Instance
  - T1578.003: Delete Cloud Instance
  - T1578.004: Revert Cloud Instance
- T1599: Network Boundary Bridging
  - T1535: Unused/Unsupported Cloud Regions
- T1562: Impair Defenses
  - T1562.001: Disable or Modify Tools
  - T1562.002: Disable Windows Event Logging
  - T1562.003: Impair Command History Logging
  - T1562.004: Disable or Modify System Firewall
  - T1562.006: Indicator Blocking
  - T1562.007: Disable or Modify Cloud Firewall
  - T1562.008: Disable Cloud Logs
- T1553: Subvert Trust Controls
  - T1553.001: Gatekeeper Bypass
  - T1553.002: Code Signing
  - T1553.003: SIP and Trust Provider Hijacking
  - T1553.004: Install Root Certificate
  - T1553.005: Mark-of-the-Web Bypass
  - T1553.006: Code Signing Policy Modification
- T1205: Traffic Signaling
- T1078: Valid Accounts
- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
- T1197: BITS Jobs
- T1612: Build Image on Host
- T1140: Deobfuscate/Decode Files or Information
- T1610: Deploy Container
- T1006: Direct Volume Access
- T1484: Domain Policy Modification
- T1480: Execution Guardrails
- T1211: Exploitation for Defense Evasion
- T1222: File and Directory Permissions Modification
- T1574: Hijack Execution Flow
- T1070: Indicator Removal on Host
- T1202: Indirect Command Execution
- T1036: Masquerading
- T1556: Modify Authentication Process
- T1112: Modify Registry
- T1601: Modify System Image
- T1027: Obfuscated Files or Information
- 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

## Credential Access

- T1110: Brute Force
- T1555: Credentials from Password Stores
- T1212: Exploitation for Credential Access
- T1187: Forced Authentication
- T1606: Forge Web Credentials
- T1056: Input Capture
- T1557: Man-in-the-Middle
- T1556: Modify Authentication Process
- T1040: Network Sniffing
- T1003: OS Credential Dumping
- T1528: Steal Application Access Token
- T1558: Steal or Forge Kerberos Tickets
- T1539: Steal Web Session Cookie
- T1111: Two-Factor Authentication Interception
- T1552: Unsecured Credentials

## Discovery

- T1018: Remote System Discovery
- T1016: System Network Configuration Discovery
  - T1016.001: Internet Connection Discovery
- T1049: System Network Connections Discovery
- T1007: System Service Discovery
- T1087: Account Discovery
  - T1087.001: Local Account
  - T1087.002: Domain Account
  - T1087.003: Email Account
  - T1087.004: Cloud Account
- T1580: Cloud Infrastructure Discovery
- T1526: Cloud Service Discovery
- T1046: Network Service Scanning
- T1069: Permission Groups Discovery
  - T1069.002: Domain Groups
  - T1069.003: Cloud Groups
  - T1069.001: Local Groups
- T1518: Software Discovery
  - T1518.001: Security Software Discovery
- T1082: System Information Discovery
- T1614: System Location Discovery
- T1010: Application Window Discovery
- T1217: Browser Bookmark Discovery
- T1538: Cloud Service Dashboard
- T1613: Container and Resource Discovery
- T1482: Domain Trust Discovery
- T1083: File and Directory Discovery
- T1135: Network Share Discovery
- T1040: Network Sniffing
- T1201: Password Policy Discovery
- T1120: Peripheral Device Discovery
- T1057: Process Discovery
- T1012: Query Registry
- T1033: System Owner/User Discovery
- T1124: System Time Discovery
- T1497: Virtualization/Sandbox Evasion

## Lateral Movement

- T1210: Exploitation of Remote Services
- T1021: Remote Services
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares
  - T1021.003: Distributed Component Object Model
  - T1021.004: SSH
  - T1021.005: VNC
  - T1021.006: Windows Remote Management
- T1534: Internal Spearphishing
- T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking
- T1091: Replication Through Removable Media
- T1072: Software Deployment Tools
- T1080: Taint Shared Content
- T1550: Use Alternate Authentication Material

## Collection

- T1530: Data from Cloud Storage Object
- T1560: Archive Collected Data
- T1123: Audio Capture
- T1119: Automated Collection
- T1115: Clipboard Data
- T1602: Data from Configuration Repository
- T1213: Data from Information Repositories
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1074: Data Staged
- T1114: Email Collection
- T1056: Input Capture
- T1185: Man in the Browser
- T1557: Man-in-the-Middle
- T1113: Screen Capture
- T1125: Video Capture

## Command and Control

- T1571: Non-Standard Port
- T1071: Application Layer Protocol
  - T1071.001: Web Protocols
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.004: DNS
- T1105: Ingress Tool Transfer
- T1095: Non-Application Layer Protocol
- T1219: Remote Access Software
- T1205: Traffic Signaling
- T1092: Communication Through Removable Media
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1568: Dynamic Resolution
- T1573: Encrypted Channel
- T1008: Fallback Channels
- T1104: Multi-Stage Channels
- T1572: Protocol Tunneling
- T1090: Proxy
- T1102: Web Service

## Exfiltration

- T1048: Exfiltration Over Alternative Protocol
- T1011: Exfiltration Over Other Network Medium
- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1041: Exfiltration Over C2 Channel
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
- T1029: Scheduled Transfer
- T1537: Transfer Data to Cloud Account

## Impact

- T1531: Account Access Removal
- T1489: Service Stop
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1565: Data Manipulation
- T1491: Defacement
- T1561: Disk Wipe
- T1499: Endpoint Denial of Service
- T1495: Firmware Corruption
- T1490: Inhibit System Recovery
- T1498: Network Denial of Service
- T1496: Resource Hijacking
- T1529: System Shutdown/Reboot