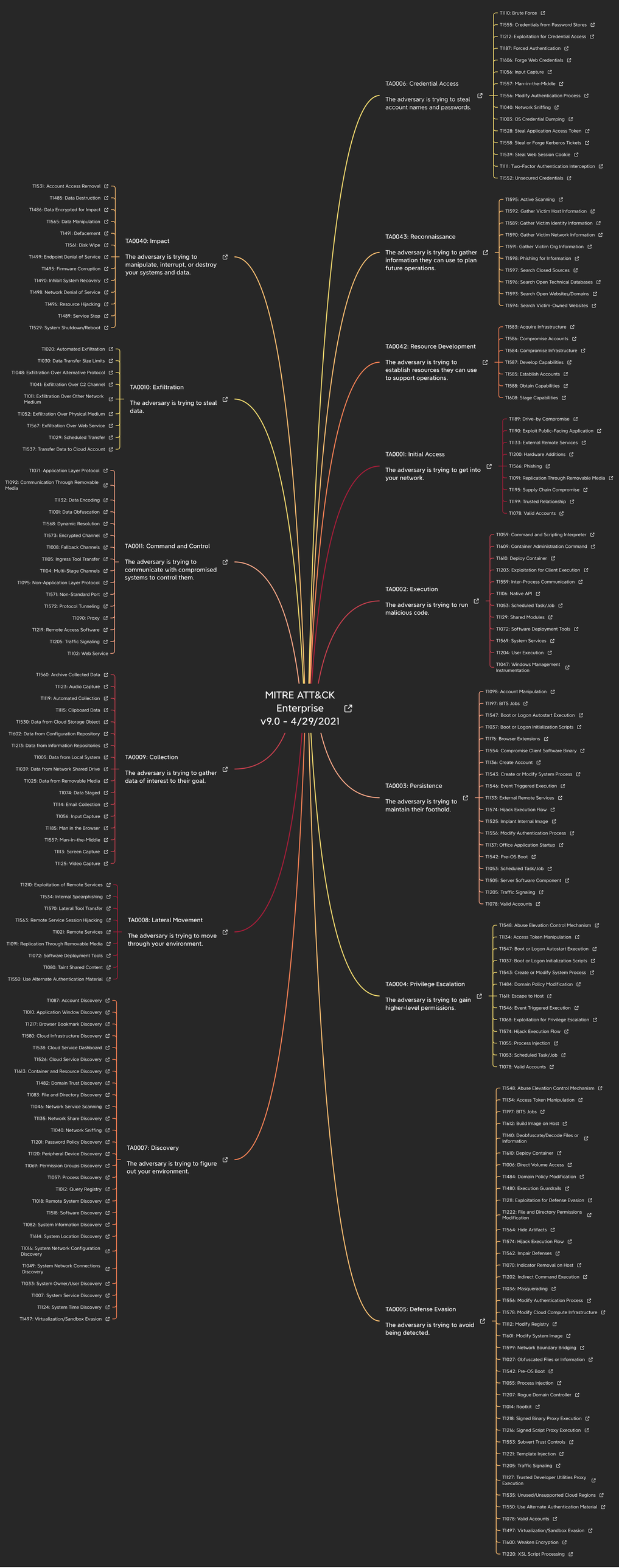
MITRE ATT&CK
Enterprise
v9.0 - 4/29/2021
TA0006: Credential Access
The adversary is trying to steal account names and passwords.
T1110: Brute Force
T1555: Credentials from Password Stores
T1212: Exploitation for Credential Access
T1187: Forced Authentication
T1606: Forge Web Credentials
T1056: Input 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
TA0043: Reconnaissance
The adversary is trying to gather information they can use to plan future operations.
T1595: Active Scanning
T1592: Gather Victim Host Information
T1589: Gather Victim Identity Information
T1590: Gather Victim Network Information
T1591: Gather Victim Org Information
T1598: Phishing for Information
T1597: Search Closed Sources
T1596: Search Open Technical Databases
T1593: Search Open Websites/Domains
T1594: Search Victim-Owned Websites
TA0042: Resource Development
The adversary is trying to establish resources they can use to support operations.
T1583: Acquire Infrastructure
T1586: Compromise Accounts
T1584: Compromise Infrastructure
T1587: Develop Capabilities
T1585: Establish Accounts
T1588: Obtain Capabilities
T1608: Stage Capabilities
TA0001: Initial Access
The adversary is trying to get into your network.
T1189: Drive-by Compromise
T1190: Exploit Public-Facing Application
T1133: External Remote Services
T1200: Hardware Additions
T1566: Phishing
T1091: Replication Through Removable Media
T1195: Supply Chain Compromise
T1199: Trusted Relationship
T1078: Valid Accounts
TA0002: Execution
The adversary is trying to run malicious code.
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
T1047: Windows Management Instrumentation
TA0003: Persistence
The adversary is trying to maintain their foothold.
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
T1133: External Remote Services
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
T1205: Traffic Signaling
T1078: Valid Accounts
TA0004: Privilege Escalation
The adversary is trying to gain higher-level permissions.
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
T1078: Valid Accounts
TA0005: Defense Evasion
The adversary is trying to avoid being detected.
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
T1564: Hide Artifacts
T1574: Hijack Execution Flow
T1562: Impair Defenses
T1070: Indicator Removal on Host
T1202: Indirect Command Execution
T1036: Masquerading
T1556: Modify Authentication Process
T1578: Modify Cloud Compute Infrastructure
T1112: Modify Registry
T1601: Modify System Image
T1599: Network Boundary Bridging
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
T1553: Subvert Trust Controls
T1221: Template Injection
T1205: Traffic Signaling
T1127: Trusted Developer Utilities Proxy Execution
T1535: Unused/Unsupported Cloud Regions
T1550: Use Alternate Authentication Material
T1078: Valid Accounts
T1497: Virtualization/Sandbox Evasion
T1600: Weaken Encryption
T1220: XSL Script Processing
TA0040: Impact
The adversary is trying to manipulate, interrupt, or destroy your systems and data.
T1531: Account Access Removal
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
T1489: Service Stop
T1529: System Shutdown/Reboot
TA0010: Exfiltration
The adversary is trying to steal data.
T1020: Automated Exfiltration
T1030: Data Transfer Size Limits
T1048: Exfiltration Over Alternative Protocol
T1041: Exfiltration Over C2 Channel
T1011: Exfiltration Over Other Network Medium
T1052: Exfiltration Over Physical Medium
T1567: Exfiltration Over Web Service
T1029: Scheduled Transfer
T1537: Transfer Data to Cloud Account
TA0011: Command and Control
The adversary is trying to communicate with compromised systems to control them.
T1071: Application Layer Protocol
T1092: Communication Through Removable Media
T1132: Data Encoding
T1001: Data Obfuscation
T1568: Dynamic Resolution
T1573: Encrypted Channel
T1008: Fallback Channels
T1105: Ingress Tool Transfer
T1104: Multi-Stage Channels
T1095: Non-Application Layer Protocol
T1571: Non-Standard Port
T1572: Protocol Tunneling
T1090: Proxy
T1219: Remote Access Software
T1205: Traffic Signaling
T1102: Web Service
TA0009: Collection
The adversary is trying to gather data of interest to their goal.
T1560: Archive Collected Data
T1123: Audio Capture
T1119: Automated Collection
T1115: Clipboard Data
T1530: Data from Cloud Storage Object
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
TA0008: Lateral Movement
The adversary is trying to move through your environment.
T1210: Exploitation of Remote Services
T1534: Internal Spearphishing
T1570: Lateral Tool Transfer
T1563: Remote Service Session Hijacking
T1021: Remote Services
T1091: Replication Through Removable Media
T1072: Software Deployment Tools
T1080: Taint Shared Content
T1550: Use Alternate Authentication Material
TA0007: Discovery
The adversary is trying to figure out your environment.
T1087: Account Discovery
T1010: Application Window Discovery
T1217: Browser Bookmark Discovery
T1580: Cloud Infrastructure Discovery
T1538: Cloud Service Dashboard
T1526: Cloud Service Discovery
T1613: Container and Resource Discovery
T1482: Domain Trust Discovery
T1083: File and Directory Discovery
T1046: Network Service Scanning
T1135: Network Share Discovery
T1040: Network Sniffing
T1201: Password Policy Discovery
T1120: Peripheral Device Discovery
T1069: Permission Groups Discovery
T1057: Process Discovery
T1012: Query Registry
T1018: Remote System Discovery
T1518: Software Discovery
T1082: System Information Discovery
T1614: System Location Discovery
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery
T1033: System Owner/User Discovery
T1007: System Service Discovery
T1124: System Time Discovery
T1497: Virtualization/Sandbox Evasion