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
T1589: Gather Victim Identity Information
T1589.001: Credentials
T1589.002: Email Addresses
T1589.003: Employee Names
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
T1591: Gather Victim Org Information
T1591.001: Determine Physical Locations
T1591.002: Business Relationships
T1591.003: Identify Business Tempo
T1591.004: Identify Roles
T1598: Phishing for Information
T1598.001: Spearphishing Service
T1598.002: Spearphishing Attachment
T1598.003: Spearphishing Link
T1597: Search Closed Sources
T1597.001: Threat Intel Vendors
T1597.002: Purchase Technical Data
T1593: Search Open Websites/Domains
T1593.001: Social Media
T1593.002: Search Engines
T1596: Search Open Technical Databases
T1596.001: DNS/Passive DNS
T1596.002: WHOIS
T1596.003: Digital Certificates
T1596.004: CDNs
T1596.005: Scan Databases
T1594: Search Victim-Owned Websites

Resource Development
T1583: Acquire Infrastructure
T1583.001: Domains
T1583.002: DNS Server
T1583.003: Virtual Private Server
T1583.004: Server
T1583.005: Botnet
T1583.006: Web Services
T1586: Compromise Accounts
T1586.001: Social Media Accounts
T1586.002: Email Accounts
T1584: Compromise Infrastructure
T1584.001: Domains
T1584.002: DNS Server
T1584.003: Virtual Private Server
T1584.004: Server
T1584.005: Botnet
T1584.006: Web Services
T1587: Develop Capabilities
T1587.001: Malware
T1587.002: Code Signing Certificates
T1587.003: Digital Certificates
T1587.004: Exploits
T1585: Establish Accounts
T1585.001: Social Media Accounts
T1585.002: Email Accounts
T1588: Obtain Capabilities
T1588.001: Malware
T1588.002: Tool
T1588.003: Code Signing Certificates
T1588.004: Digital Certificates
T1588.005: Exploits
T1588.006: Vulnerabilities

Initial Access
T0810: Data Historian Compromise
T1189 / T0817: Drive-by Compromise
T0819: Engineering Workstation Compromise
T1190 / T0819: Exploit Public-Facing Applicati
T1133 / T0822: External Remote Services
T1200: Hardware Additions
T0883: Internet Accessible Device
T1566: Phishing
T1566.001 / T0865: Spearphishing Attachmen
T1566.002: Spearphishing Link
T1566.003: Spearphishing via Service
T1091 / T0847: Replication Through Removab
T1195 / T0862: Supply Chain Compromise
T1195.001: Compromise Software Dependenci
T1195.002: Compromise Software Supply Cha
T1195.003: Compromise Hardware Supply Cha
T1199: Trusted Relationship
T0878: Valid Accounts
T1078: Valid Accounts
T1078.001: Default Accounts
T1078.002: Domain Accounts
T1078.003: Local Accounts
T1078.004: Cloud Accounts
T0860: Wireless Compromise

Execution
T0875: Change Program State
T1059: Command and Scripting Interpreter
T1059.001: PowerShell
T1059.002: AppleScript
T1059.003: Windows Command Shell
T1059.004: Unix Shell
T1059.005: Visual Basic
T1059.006: Python
T1059.007: JavaScript/JScript
T1059.008: Network Device CLI
T0807: Command-Line Interface
T0871: Execution through API
T1203: Exploitation for Client Execution
T0823: Graphical User Interface
T1559: Inter-Process Communication
T1559.001: Component Object Model
T1559.002: Dynamic Data Exchange
T0830: Man in the Middle
T1106: Native API
T0844: Program Organization Units
T0873: Project File Infection
T1053: Scheduled Task/Job
T1053.001: At (Linux)
T1053.002: At (Windows)
T1053.003: Cron
T1053.004: Launchd
T1053.005: Scheduled Task
T1053.006: Systemd Timers
T1569: System Services
T1569.001: Launchctl
T1569.002: Service Execution
T1204 / T0863: User Execution
T1204.001: Malicious Link
T1204.002: Malicious File
T1047: Windows Management Instrumentatio

Persistence
T1098: Account Manipulation
T1098.001: Additional Cloud Credentials
T1098.002: Exchange Email Delegate Permiss
T1098.003: Add Office 365 Global Administrat
T1098.004: SSH Authorized Keys
T1197: BITS Jobs
T1547: Boot or Logon Autostart Execution
T1547.001: Registry Run Keys / Startup Folder
T1547.002: Authentication Package
T1547.003: Time Providers
T1547.004: Winlogon Helper DLL
T1547.005: Security Support Provider
T1547.006: Kernel Modules and Extensions
T1547.007: Re-opened Applications
T1547.008: LSASS Driver
T1547.009: Shortcut Modification
T1547.010: Port Monitors
T1547.011: Plist Modification
T1547.012: Print Processors
T1037: Boot or Logon Initialization Scripts
T1037.001: Logon Script (Windows)
T1037.002: Logon Script (Mac)
T1037.003: Network Logon Script
T1037.004: Rc.common
T1037.005: Startup Items
T1176: Browser Extensions
T1554: Compromise Client Software Binary
T1136: Create Account
T1136.001: Local Account
T1136.002: Domain Account
T1136.003: Cloud Account
T1543: Create or Modify System Process
T1543.001: Launch Agent
T1543.002: Systemd Service
T1543.003: Windows Service
T1543.004: Launch Daemon
T1546: Event Triggered Execution
T1546.001: Change Default File Association
T1546.002: Screensaver
T1546.003: Windows Management Instrumen
T1546.004: .bash_profile and .bashrc
T1546.005: Trap
T1546.006: LC_LOAD_DYLIB Addition
T1546.007: Netsh Helper DLL
T1546.008: Accessibility Features
T1546.009: AppCert DLLs
T1546.010: AppInit DLLs
T1546.011: Application Shimming
T1546.012: Image File Execution Options Injec
T1546.013: PowerShell Profile
T1546.014: Emond
T1546.015: Component Object Model Hijackin
T1068: Exploitation for Privilege Escalation
T1484: Group Policy Modification
T1574: Hijack Execution Flow
T1574.001: DLL Search Order Hijacking
T1574.002: DLL Side-Loading
T1574.004: Dylib Hijacking
T1574.005: Executable Installer File Permissio
T1574.006: LD_PRELOAD
T1574.007: Path Interception by PATH Environ
T1574.008: Path Interception by Search Order
T1574.009: Path Interception by Unquoted Pa
T1574.010: Services File Permissions Weakness
T1574.011: Services Registry Permissions Weak
T1574.012: COR_PROFILER
T0874: Hooking
T1125: Implant Container Image
T0839: Module Firmware
T1137: Office Application Startup
T1137.001: Office Template Macros
T1137.002: Office Test
T1137.003: Outlook Forms
T1137.004: Outlook Home Page
T1137.005: Outlook Rules
T1137.006: Add-ins
T1542: Pre-OS Boot
T1542.001 / T0857: System Firmware
T1542.002: Component Firmware
T1542.003: Bootkit
T1542.004: ROMMONkit
T1542.005: TFTP Boot
T0843: Program Download
T0873: Project File Infection
T1053: Scheduled Task/Job
T1053.001: At (Linux)
T1053.002: At (Windows)
T1053.003: Cron
T1053.004: Launchd
T1053.005: Scheduled Task
T1053.006: Systemd Timers
T1205: Traffic Signaling
T1205.001: Port Knocking
T1505: Server Software Component
T1505.001: SQL Stored Procedures
T1505.002: Transport Agent
T1505.003: Web Shell
T1078 / T0859: Valid Accounts
T1078.001: Default Accounts
T1078.002: Domain Accounts
T1078.003: Local Accounts
T1078.004: Cloud Accounts

Privilege Escalation
T1548: Abuse Elevation Control Mechanism
T1548.001: Setuid and Setgid
T1548.002: Bypass User Account Control
T1548.003: Sudo and Sudo Caching
T1548.004: Elevated Execution with Prompt
T1134: Access Token Manipulation
T1134.001: Token Impersonation/Theft
T1134.002: Create Process with Token
T1134.003: Make and Impersonate Token
T1134.004: Parent PID Spoofing
T1134.005: SID-History Injection
T1547: Boot or Logon Autostart Execution
T1547.001: Registry Run Keys / Startup Folder
T1547.002: Authentication Package
T1547.003: Time Providers
T1547.004: Winlogon Helper DLL
T1547.005: Security Support Provider
T1547.006: Kernel Modules and Extensions
T1547.007: Re-opened Applications
T1547.008: LSASS Driver
T1547.009: Shortcut Modification
T1547.010: Port Monitors
T1547.011: Plist Modification
T1547.012: Print Processors
T1037: Boot or Logon Initialization Scripts
T1037.001: Logon Script (Windows)
T1037.002: Logon Script (Mac)
T1037.003: Network Logon Script
T1037.004: Rc.common
T1037.005: Startup Items
T1543: Create or Modify System Process
T1543.001: Launch Agent
T1543.002: Systemd Service
T1543.003: Windows Service
T1543.004: Launch Daemon
T1546: Event Triggered Execution
T1546.001: Change Default File Association
T1546.002: Screensaver
T1546.003: Windows Management Instrumen
T1546.004: .bash_profile and .bashrc
T1546.005: Trap
T1546.006: LC_LOAD_DYLIB Addition
T1546.007: Netsh Helper DLL
T1546.008: Accessibility Features
T1546.009: AppCert DLLs
T1546.010: AppInit DLLs
T1546.011: Application Shimming
T1546.012: Image File Execution Options Injec
T1546.013: PowerShell Profile
T1546.014: Emond
T1546.015: Component Object Model Hijackin
T1068: Exploitation for Privilege Escalation
T1484: Group Policy Modification
T1574: Hijack Execution Flow
T1574.001: DLL Search Order Hijacking
T1574.002: DLL Side-Loading
T1574.004: Dylib Hijacking
T1574.005: Executable Installer File Permissio
T1574.006: LD_PRELOAD
T1574.007: Path Interception by PATH Environ
T1574.008: Path Interception by Search Order
T1574.009: Path Interception by Unquoted Pa
T1574.010: Services File Permissions Weakness
T1574.011: Services Registry Permissions Weak
T1574.012: COR_PROFILER
T1055: Process Injection
T1055.001: Dynamic-link Library Injection
T1055.002: Portable Executable Injection
T1055.003: Thread Execution Hijacking
T1055.004: Asynchronous Procedure Call
T1055.005: Thread Local Storage
T1055.008: Ptrace System Calls
T1055.009: Proc Memory
T1055.011: Extra Window Memory Injection
T1055.012: Process Hollowing
T1055.013: Process Doppelgänging
T1055.014: VDSO Hijacking
T1053: Scheduled Task/Job
T1053.001: At (Linux)
T1053.002: At (Windows)
T1053.003: Cron
T1053.004: Launchd
T1053.005: Scheduled Task
T1053.006: Systemd Timers
T1078: Valid Accounts
T1078.001: Default Accounts
T1078.002: Domain Accounts
T1078.003: Local Accounts
T1078.004: Cloud Accounts

Defense Evasion
T1548: Abuse Elevation Control Mechanism
T1548.001: Setuid and Setgid
T1548.003: Sudo and Sudo Caching
T1548.004: Elevated Execution with Prompt
T1548.002: Bypass User Account Control
T1134: Access Token Manipulation
T1134.001: Token Impersonation/Theft
T1134.002: Create Process with Token
T1134.003: Make and Impersonate Token
T1134.004: Parent PID Spoofing
T1134.005: SID-History Injection
T1197: BITS Jobs
T1140: Deobfuscate/Decode Files or Informat
T1006: Direct Volume Access
T1480: Execution Guardrails
T1480.001: Environmental Keying
T1211 / T0820: Exploitation for Defense Evasio
T1222: File and Directory Permissions Modific
T1222.001: Windows File and Directory Permi
T1222.002: Linux and Mac File and Directory P
T1484: Group Policy Modification
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
T1574: Hijack Execution Flow
T1574.001: DLL Search Order Hijacking
T1574.002: DLL Side-Loading
T1574.004: Dylib Hijacking
T1574.005: Executable Installer File Permissio
T1574.006: LD_PRELOAD
T1574.007: Path Interception by PATH Environ
T1574.008: Path Interception by Search Order
T1574.009: Path Interception by Unquoted Pa
T1574.010: Services File Permissions Weakness
T1574.011: Services Registry Permissions Weak
T1574.012: COR_PROFILER
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
T1070 / T0872: Indicator Removal on Host
T1070.001: Clear Windows Event Logs
T1070.002: Clear Linux or Mac System Logs
T1070.003: Clear Command History
T1070.004: File Deletion
T1070.005: Network Share Connection Removal
T1070.006: Timestomp
T1202: Indirect Command Execution
T1036 / T0849: Masquerading
T1036.001: Invalid Code Signature
T1036.002: Right-to-Left Override
T1036.003: Rename System Utilities
T1036.004: Masquerade Task or Service
T1036.005: Match Legitimate Name or Location
T1036.006: Space after Filename
T1556: Modify Authentication Process
T1556.001: Domain Controller Authentication
T1556.002: Password Filter DLL
T1556.003: Pluggable Authentication Modules
T1556.004: Network Device Authentication
T1578: Modify Cloud Compute Infrastructure
T1578.001: Create Snapshot
T1578.002: Create Cloud Instance
T1578.003: Delete Cloud Instance
T1578.004: Revert Cloud Instance
T1112: Modify Registry
T1601: Modify System Image
T1601.001: Patch System Image
T1601.002: Downgrade System Image
T1599: Network Boundary Bridging
T1599.001: Network Address Translation Traversal
T1027: Obfuscated Files or Information
T1027.001: Binary Padding
T1027.002: Software Packing
T1027.003: Steganography
T1027.004: Compile After Delivery
T1027.005: Indicator Removal from Tools
T1542: Pre-OS Boot
T1542.001: System Firmware
T1542.002: Component Firmware
T1542.003: Bootkit
T1542.004: ROMMONkit
T1542.005: TFTP Boot
T1055: Process Injection
T1055.001: Dynamic-link Library Injection
T1055.002: Portable Executable Injection
T1055.003: Thread Execution Hijacking
T1055.004: Asynchronous Procedure Call
T1055.005: Thread Local Storage
T1055.008: Ptrace System Calls
T1055.009: Proc Memory
T1055.011: Extra Window Memory Injection
T1055.012: Process Hollowing
T1055.013: Process Doppelgänging
T1055.014: VDSO Hijacking
T1207: Rogue Domain Controller
T0848: Rogue Master Device
T1014 / T0851: Rootkit
T1218: Signed Binary Proxy Execution
T1218.001: Compiled HTML File
T1218.002: Control Panel
T1218.003: CMSTP
T1218.004: InstallUtil
T1218.005: Mshta
T1218.007: Msiexec
T1218.008: Odbcconf
T1218.009: Regsvcs/Regasm
T1218.010: Regsvr32
T1218.011: Rundll32
T1218.012: Verclsid
T1216: Signed Script Proxy Execution
T1216.001: PubPrn
T0856: Spoof Reporting Message
T1553: Subvert Trust Controls
T1553.001: Gatekeeper Bypass
T1553.002: Code Signing
T1553.003: SIP and Trust Provider Hijacking
T1553.004: Install Root Certificate
T1221: Template Injection
T1205: Traffic Signaling
T1205.001: Port Knocking
T1127: Trusted Developer Utilities Proxy Execution
T1127.001: MSBuild
T1535: Unused/Unsupported Cloud Regions
T1550: Use Alternate Authentication Material
T1550.001: Application Access Token
T1550.002: Pass the Hash
T1550.003: Pass the Ticket
T1550.004: Web Session Cookie
T0858: Utilize/Change Operating Mode
T1078: Valid Accounts
T1078.001: Default Accounts
T1078.002: Domain Accounts
T1078.003: Local Accounts
T1078.004: Cloud Accounts
T1497: Virtualization/Sandbox Evasion
T1497.001: System Checks
T1497.002: User Activity Based Checks
T1497.003: Time Based Evasion
T1600: Weaken Encryption
T1600.001: Reduce Key Space
T1600.002: Disable Crypto Hardware
T1220: XSL Script Processing

Credential Access
T1110: Brute Force
T1110.001: Password Guessing
T1110.002: Password Cracking
T1110.003: Password Spraying
T1110.004: Credential Stuffing
T1555: Credentials from Password Stores
T1555.001: Keychain
T1555.002: Securityd Memory
T1555.003: Credentials from Web Browsers
T1212: Exploitation for Credential Access
T1187: Forced Authentication
T1056: Input Capture
T1056.001: Keylogging
T1056.002: GUI Input Capture
T1056.003: Web Portal Capture
T1056.004: Credential API Hooking
T1557: Man-in-the-Middle
T1557.001: LLMNR/NBT-NS Poisoning and SMB
T1557.002: ARP Cache Poisoning
T1556: Modify Authentication Process
T1556.001: Domain Controller Authentication
T1556.002: Password Filter DLL
T1556.003: Pluggable Authentication Modules
T1556.004: Network Device Authentication
T1040: Network Sniffing
T1003: OS Credential Dumping
T1003.001: LSASS Memory
T1003.002: Security Account Manager
T1003.003: NTDS
T1003.004: LSA Secrets
T1003.005: Cached Domain Credentials
T1003.006: DCSync
T1003.007: Proc Filesystem
T1003.008: /etc/passwd and /etc/shadow
T1528: Steal Application Access Token
T1558: Steal or Forge Kerberos Tickets
T1558.001: Golden Ticket
T1558.002: Silver Ticket
T1558.003: Kerberoasting
T1558.004: AS-REP Roasting
T1539: Steal Web Session Cookie
T1111: Two-Factor Authentication Interception
T1552: Unsecured Credentials
T1552.001: Credentials In Files
T1552.002: Credentials in Registry
T1552.003: Bash History
T1552.004: Private Keys
T1552.005: Cloud Instance Metadata API
T1552.006: Group Policy Preferences

Discovery
T1087: Account Discovery
T1087.001: Local Account
T1087.002: Domain Account
T1087.003: Email Account
T1087.004: Cloud Account
T1010: Application Window Discovery
T1217: Browser Bookmark Discovery
T1580: Cloud Infrastructure Discovery
T1538: Cloud Service Dashboard
T1526: Cloud Service Discovery
T0808: Control Device Identification
T1482: Domain Trust Discovery
T1083: File and Directory Discovery
T0824: I/O Module Discovery
T0840: Network Connection Enumeration
T1046 / T0841: Network Service Scanning
T1135: Network Share Discovery
T1040 / T0842: Network Sniffing
T1201: Password Policy Discovery
T1120: Peripheral Device Discovery
T1069: Permission Groups Discovery
T1069.001: Local Groups
T1069.002: Domain Groups
T1069.003: Cloud Groups
T1057: Process Discovery
T1012: Query Registry
T1018 / T0846: Remote System Discovery
T1091: Replication Through Removable Medi
T1072: Software Deployment Tools
T1080: Taint Shared Content
T1550: Use Alternate Authentication Material
T1550.001: Application Access Token
T1550.002: Pass the Hash
T1550.003: Pass the Ticket
T1550.004: Web Session Cookie
T0859: Valid Accounts

Lateral Movement
T0812: Default Credentials
T1210 / T0866: Exploitation of Remote Servic
T0822: External Remote Services
T1534: Internal Spearphishing
T1570: Lateral Tool Transfer
T0844: Program Organization Units
T0867: Remote File Copy
T1563: Remote Service Session Hijacking
T1563.001: SSH Hijacking
T1563.002: RDP Hijacking
T1021: Remote Services
T1021.001: Remote Desktop Protocol
T1021.002: SMB/Windows Admin Shares
T1021.003: Distributed Component Object Mo
T1021.004: SSH
T1021.005: VNC
T1021.006: Windows Remote Management
T1091: Replication Through Removable Medi
T1072: Software Deployment Tools
T1080: Taint Shared Content
T1550: Use Alternate Authentication Material
T1550.001: Application Access Token
T1550.002: Pass the Hash
T1550.003: Pass the Ticket
T1550.004: Web Session Cookie
T0859: Valid Accounts

Collection
T1560: Archive Collected Data
T1560.001: Archive via Utility
T1560.002: Archive via Library
T1560.003: Archive via Custom Method
T1123: Audio Capture
T1119 / T0802: Automated Collection
T1115: Clipboard Data
T1530: Data from Cloud Storage Object
T1602: Data from Configuration Repository
T1602.001: SNMP (MIB Dump)
T1602.002: Network Device Configuration Dum
T1213 / T0811: Data from Information Reposit
T1213.001: Confluence
T1213.002: Sharepoint
T1005: Data from Local System
T1039: Data from Network Shared Drive
T1025: Data from Removable Media
T1074: Data Staged
T1074.001: Local Data Staging
T1074.002: Remote Data Staging
T0868: Detect Operating Mode
T0870: Detect Program State
T1114: Email Collection
T1114.001: Local Email Collection
T1114.002: Remote Email Collection
T1114.003: Email Forwarding Rule
T0877: I/O Image
T1056: Input Capture
T1056.001: Keylogging
T1056.002: GUI Input Capture
T1056.003: Web Portal Capture
T1056.004: Credential API Hooking
T0825: Location Identification
T1185: Man in the Browser
T1557: Man-in-the-Middle
T1557.001: LLMNR/NBT-NS Poisoning and SMB
T1557.002: ARP Cache Poisoning
T0801: Monitor Process State
T0861: Point & Tag Identification
T0845: Program Upload
T0850: Role Identification
T1113 / T0852: Screen Capture
T1125: Video Capture

Command and Control
T1071: Application Layer Protocol
T1071.001: Web Protocols
T1071.002: File Transfer Protocols
T1071.003: IM
T1071.004: DNS
T0885: Commonly Used Port
T1092: Communication Through Removable M
T0884: Connection Proxy
T1132: Data Encoding
T1132.001: Standard Encoding
T1132.002: Non-Standard Encoding
T1001: Data Obfuscation
T1001.001: Junk Data
T1001.002: Steganography
T1001.003: Protocol Impersonation
T1568: Dynamic Resolution
T1568.001: Fast Flux DNS
T1568.002: Domain Generation Algorithms
T1568.003: DNS Calculation
T1573: Encrypted Channel
T1573.001: Symmetric Cryptography
T1573.002: Asymmetric Cryptography
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
T1090.001: Internal Proxy
T1090.002: External Proxy
T1090.003: Multi-hop Proxy
T1090.004: Domain Fronting
T1219: Remote Access Software
T0869: Standard Application Layer Protocol
T1205: Traffic Signaling
T1205.001: Port Knocking
T1102: Web Service
T1102.001: Dead Drop Resolver
T1102.002: Bidirectional Communication
T1102.003: One-Way Communication

Exfiltration
T1020: Automated Exfiltration
T1020.001: Traffic Duplication
T1030: Data Transfer Size Limits
T1048: Exfiltration Over Alternative Protocol
T1048.001: Exfiltration Over Symmetric Encryp
T1048.002: Exfiltration Over Asymmetric Encry
T1048.003: Exfiltration Over Unencrypted/Obf
T1041: Exfiltration Over C2 Channel
T1011: Exfiltration Over Other Network Mediu
T1011.001: Exfiltration Over Bluetooth
T1052: Exfiltration Over Physical Medium
T1052.001: Exfiltration over USB
T1567: Exfiltration Over Web Service
T1567.001: Exfiltration to Code Repository
T1567.002: Exfiltration to Cloud Storage
T1537: Transfer Data to Cloud Account

Impact
T1531: Account Access Removal
T1485: Data Destruction
T1486: Data Encrypted for Impact
T1565: Data Manipulation
T1565.001: Stored Data Manipulation
T1565.002: Transmitted Data Manipulation
T1565.003: Runtime Data Manipulation
T1491: Defacement
T1491.001: Internal Defacement
T1491.002: External Defacement
T0838: Modify Alarm Settings
T0833: Modify Control Logic
T0843: Program Download
T0851: Rootkit
T0857: System Firmware
T0858: Utilize/Change Operating Mode

Inhibit Response Function
T0800: Activate Firmware Update Mode
T0878: Alarm Suppression
T0803: Block Command Message
T0803: Modify Control Logic
T0805: Block Serial COM
T0809: Data Destruction
T0814: Denial of Service
T0816: Device Restart/Shutdown
T0835: Manipulate I/O Image
T0836: Modify Parameter
T0839: Module Firmware
T0843: Program Download
T0800: Activate Firmware Update Mode
T0855: Unauthorized Command Message

Impair Process Control
T0806: Brute Force I/O
T0836: Modify Parameter
T0827: Loss of Control
T0828: Loss of Productivity and Revenue
T0880: Loss of Safety
T0829: Loss of View
T0831: Manipulation of Control
T0832: Manipulation of View
T0882: Theft of Operational Information

Impact - ICS
T0879: Damage to Property
T0813: Denial of Control
T0815: Denial of View
T0826: Loss of Availability
T0827: Loss of Control
T0828: Loss of Productivity and Revenue
T0880: Loss of Safety
T0829: Loss of View
T0831: Manipulation of Control
T0832: Manipulation of View
T0882: Theft of Operational Information