about

HiJackLoader

domain

Enterprise ATT&CK v14

platforms

Windows, PRE,
Containers, Office 365, SaaS, Google
Workspace, IaaS, Azure AD, Network

Reconnaissance

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Initial Access

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
  - Malicious File
  - Malicious Image
  - Malicious Link
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- Valid Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Account Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
  - Binary Padding
  - Command Obfuscation
  - Compile After Delivery
  - Dynamic API Resolution
  - Embedded Payloads
  - Fileless Storage
  - HTML Smuggling
  - Indicator Removal from Tools
  - LNK Icon Smuggling
  - Software Packing
  - Steganography
  - Stripped Payloads
- Pre-OS Boot
- Process Injection
  - Asynchronous Procedure Call
  - Dynamic-link Library Injection
  - Extra Window Memory Injection
  - ListPlanting
  - Portable Executable Injection
  - Process Doppelgänging
  - Process Hollowing
  - Thread Execution Hijacking
  - Thread Local Storage
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access

- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery

- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
  - Internet Connection Discovery
  - Wi-Fi Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection

- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot