RED TEAM FRAMEWORKS & METHODOLOGIES

CYBERSECURITY TRAINING SIMPLIFIED

HACKERSPLOIT.ORG // HACKERSPLOIT.ACADEMY

$HACKERSPLOIT_

RED TEAM ENGAGEMENTS

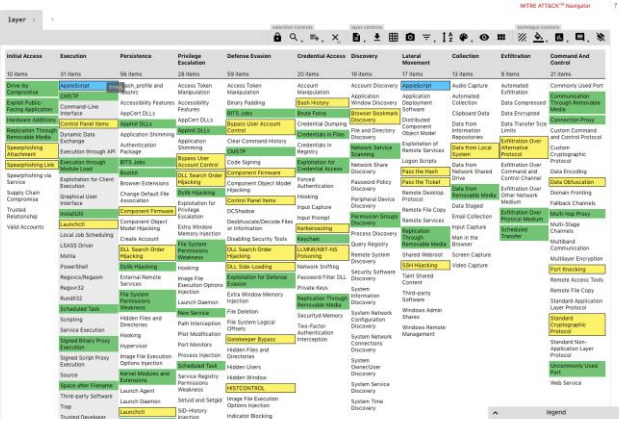
- A successful Red Team engagement begins with clearly defining the goals/objectives of the engagement with the client.
- The Red Team is then tasked with planning and orchestrating the engagement based on the pre-defined goals/objectives.
- It is important to note that Red Team engagement does not focus on the search for vulnerabilities, instead, they target security operations as a whole.
- The results of a Red Team engagement should highlight the Blue Teams ability to detect and defend against attacks and where improvements can be made.

RED TEAM ENGAGEMENTS

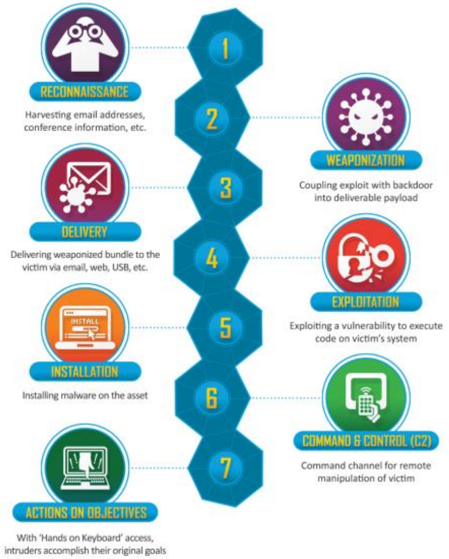
- Red Team engagements should also simulate/emulate new TTPs for the Blue Team to learn how to detect and defend against.
- A successful Red Team engagement requires a structured methodological approach, especially when simulating/emulating and adversary.
- It is therefore recommended to use an appropriate Red Team methodology/framework as a basis on which to plan, structure and orchestrate your campaign.
- Frequently utilized Red Team frameworks/methodologies include:
  - Cyber Kill Chain
  - MITRE ATT&CK Framework

RED TEAM FRAMEWORKS & METHODOLOGIES

- Cyber Kill Chain (Lockheed Martin): https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- MITRE ATT&CK – https://attack.mitre.org/
- Unified Cyber Kill Chain – https://www.unifiedkillchain.com/



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window						
	Source	Launch Daemon		HISTCONTROL						
	Space after Filename	Launchctl		Image File Execution Options Injection						
	Third-party Software			Indicator Blocking						
	Trap									
	Trusted Developer									



RECONNAISSANCE
Harvesting email addresses, conference information, etc.

WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

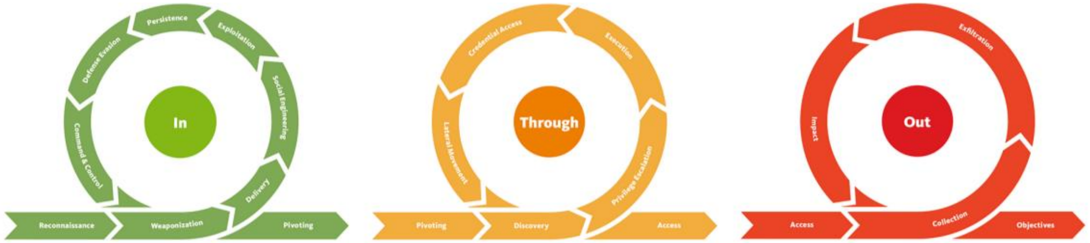
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

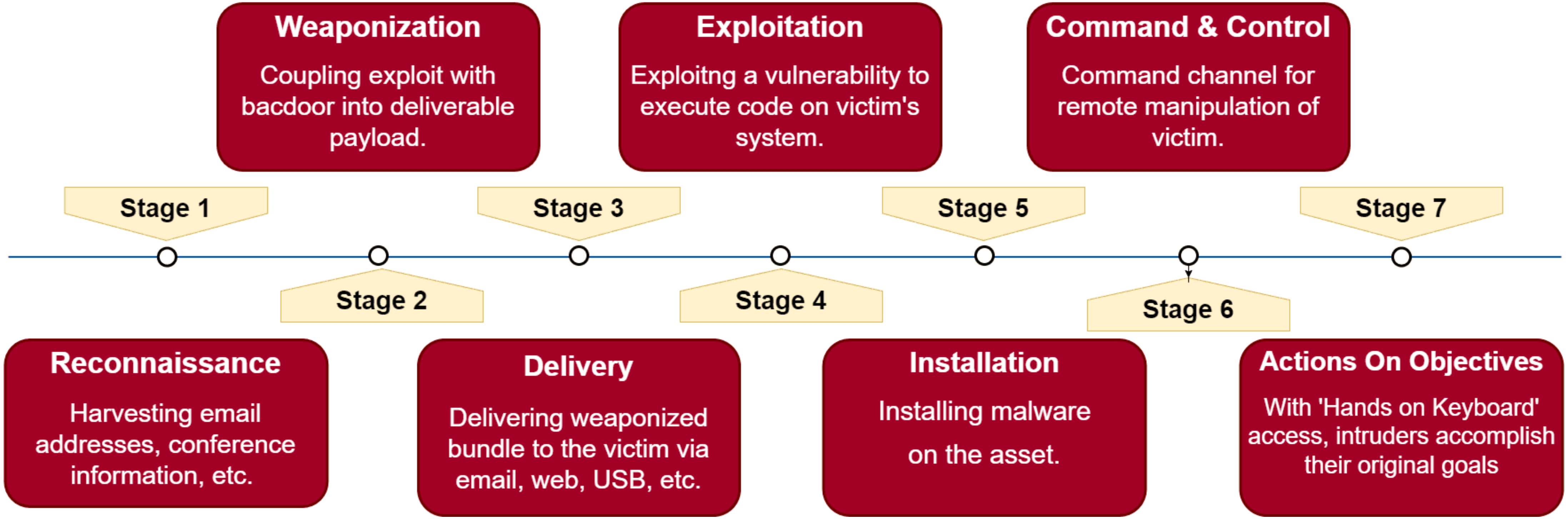
INSTALLATION
Installing malware on the asset

COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals



CYBER KILL CHAIN



Stage 1

Reconnaissance

Harvesting email addresses, conference information, etc.

Stage 2

Weaponization

Coupling exploit with bacdoor into deliverable payload.

Stage 3

Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

Stage 4

Exploitation

Exploitng a vulnerability to execute code on victim's system.

Stage 5

Installation

Installing malware on the asset.

Stage 6

Command & Control

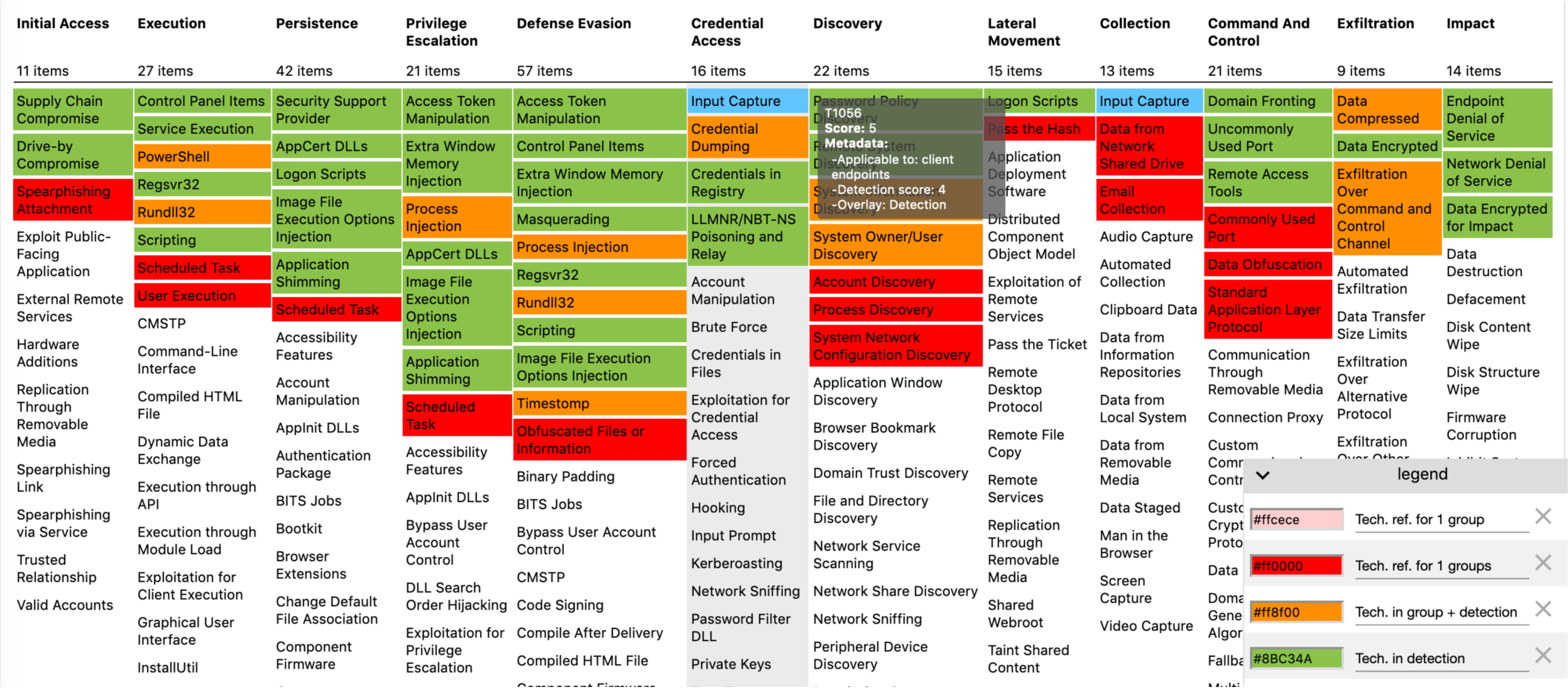
Command channel for remote manipulation of victim.

Stage 7

Actions On Objectives

With 'Hands on Keyboard' access, intruders accomplish their original goals

MITRE ATT&CK Framework



Initial Access

11 items

- 🟩 Supply Chain Compromise
- 🟩 Drive-by Compromise
- 🟥 Spearphishing Attachment
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Link
- Spearphishing via Service
- Trusted Relationship
- Valid Accounts

Execution

27 items

- 🟩 Control Panel Items
- 🟩 Service Execution
- 🟧 PowerShell
- 🟩 Regsvr32
- 🟧 Rundll32
- 🟩 Scripting
- 🟥 Scheduled Task
- 🟥 User Execution
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil

Persistence

42 items

- 🟩 Security Support Provider
- 🟩 AppCert DLLs
- 🟩 Logon Scripts
- 🟩 Image File Execution Options Injection
- 🟩 Application Shimming
- 🟥 Scheduled Task
- Accessibility Features
- Account Manipulation
- AppInit DLLs
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware

Privilege Escalation

21 items

- 🟩 Access Token Manipulation
- 🟩 Extra Window Memory Injection
- 🟧 Process Injection
- 🟩 AppCert DLLs
- 🟩 Image File Execution Options Injection
- 🟩 Application Shimming
- 🟥 Scheduled Task
- Accessibility Features
- AppInit DLLs
- Bypass User Account Control
- DLL Search Order Hijacking
- Exploitation for Privilege Escalation

Defense Evasion

57 items

- 🟩 Access Token Manipulation
- 🟩 Control Panel Items
- 🟩 Extra Window Memory Injection
- 🟩 Masquerading
- 🟧 Process Injection
- 🟩 Regsvr32
- 🟧 Rundll32
- 🟩 Scripting
- 🟩 Image File Execution Options Injection
- 🟧 Timestomp
- 🟥 Obfuscated Files or Information
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware

Credential Access

16 items

- 🟦 Input Capture
- 🟧 Credential Dumping
- 🟩 Credentials in Registry
- 🟩 LLMNR/NBT-NS Poisoning and Relay
- Account Manipulation
- Brute Force
- Credentials in Files
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Prompt
- Kerberoasting
- Network Sniffing
- Password Filter DLL
- Private Keys

Discovery

22 items

- 🟩 Password Policy Discovery
- 🟩 Remote System Discovery
- 🟩 Sys[illegible] Discovery
- 🟧 System Owner/User Discovery
- 🟥 Account Discovery
- 🟥 Process Discovery
- 🟥 System Network Configuration Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Peripheral Device Discovery

T1056
Score: 5
Metadata:
-Applicable to: client endpoints
-Detection score: 4
-Overlay: Detection

Lateral Movement

15 items

- 🟩 Logon Scripts
- 🟥 Pass the Hash
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- Taint Shared Content

Collection

13 items

- 🟦 Input Capture
- 🟥 Data from Network Shared Drive
- 🟥 Email Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Removable Media
- Data Staged
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control

21 items

- 🟩 Domain Fronting
- 🟩 Uncommonly Used Port
- 🟩 Remote Access Tools
- 🟥 Commonly Used Port
- 🟥 Data Obfuscation
- 🟥 Standard Application Layer Protocol
- Communication Through Removable Media
- Connection Proxy
- Custom Comm Contr
- Custo Crypt Proto
- Data
- Doma Gene Algor
- Fallba

Exfiltration

9 items

- 🟧 Data Compressed
- 🟩 Data Encrypted
- 🟧 Exfiltration Over Command and Control Channel
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Other

Impact

14 items

- 🟩 Endpoint Denial of Service
- 🟩 Network Denial of Service
- 🟩 Data Encrypted for Impact
- Data Destruction
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Firmware Corruption

legend

#ffcece	Tech. ref. for 1 group ✕
🟥 #ff0000	Tech. ref. for 1 groups ✕
🟧 #ff8f00	Tech. in group + detection ✕
🟩 #8BC34A	Tech. in detection ✕

ATT&CK vs CYBER KILL CHAIN

MITRE ATT&CK	Cyber Kill Chain
Recon	Recon
Resource Development	Weaponization
Initial Access	Delivery
Execution	Exploitation
Persistence	Installation
PrivEsc	C2
Defense Evasion	Actions On Objectives
Credential Access	
Discovery	
Lateral Movement	
Collection	
Command and Control	
Exfiltration	
Impact	

Thank You