Accurately ATT&CKing Your Maturity Level

Using MITRE ATT&CK to identify the appropriate offensive assessments

Isaiah Sarju

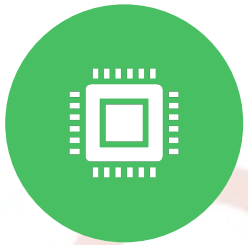
About Me

- Red Teamer
- Teacher
- Anti: nihilism, security theater, wasted time
- Pro: risk-based security
- Love chocolate chip cookies

What is MITRE ATT&CK?

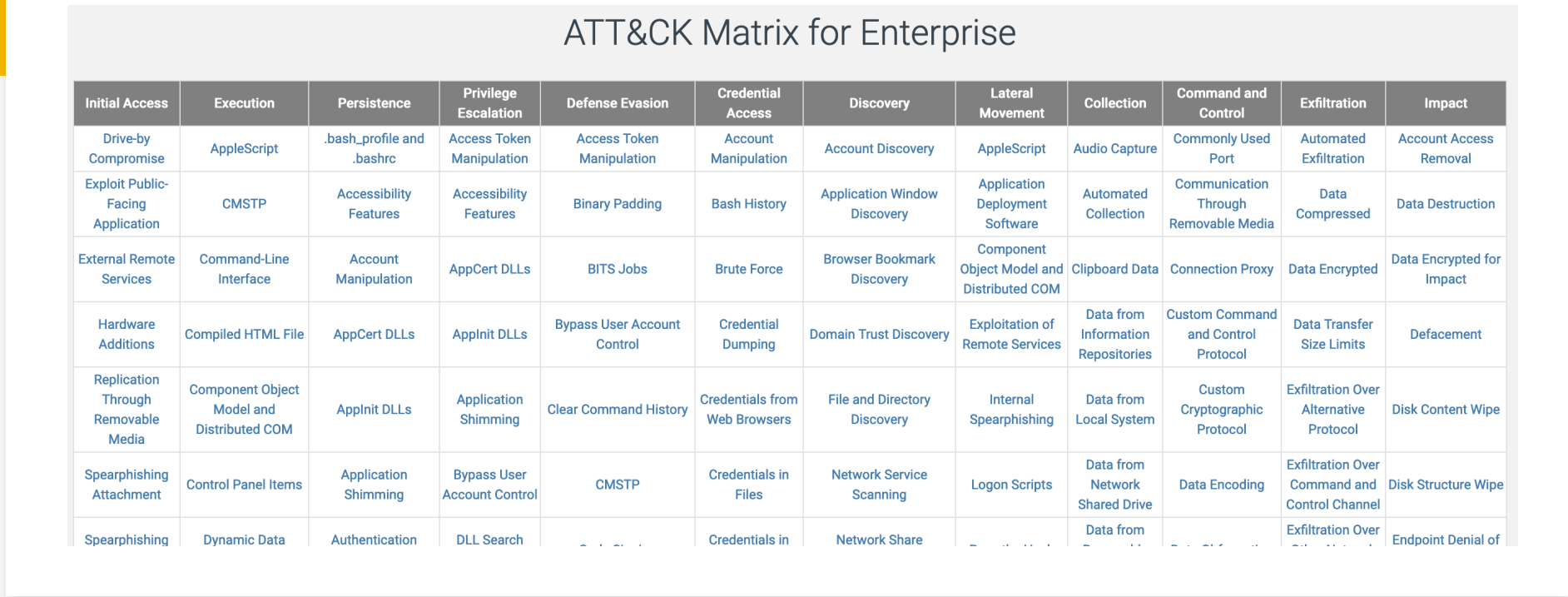
FRAMEWORK TO CATEGORIZE POST-COMPROMISE ADVERSARIAL TACTICS, TECHNIQUES, & COMMON KNOWLEDGE

PROVIDES COMMON LANGUAGE FOR TALKING ABOUT OFFENSIVE TTPS (E.G. THREAT INTEL)



ALLOWS DEFENDERS TO MAP AGAINST AND PRIORITIZE DEFENSES BASED ON KNOWN ADVERSARIES

EXPANDED TO PRE-ATT&CK, SUB-TECHNIQUES, INDUSTRY SPECIFIC (E.G. MOBILE, ICS)



MITRE ATT&CK Framework

- Tactics are columns
- Techniques are items
- Procedures are referenced within techniques

ATT&CK vs Kill Chain

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command and Control
Actions on Objective

APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. [1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same. [2] [3] [4]

ID: G0073

Associated Groups: Codoso, C0d0so0, Codoso Team, Sunshop Group

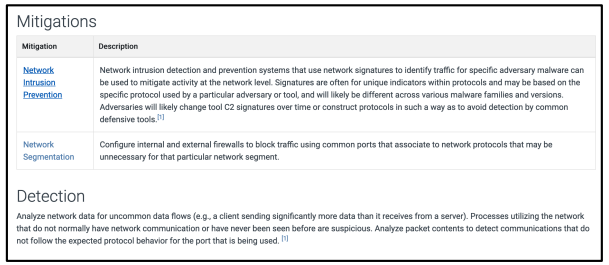
Contributors: FS-ISAC, Darren Spruell

Version: 1.2

Created: 17 October 2018

Last Modified: 11 October 2019

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System		Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Fallback Channels		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multiband Communication		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Multilayer Encryption		System Shutdown/Reboot
	Mshta	Dylib Hijacking		Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Port Knocking		Transmitted Data Manipulation
	PowerShell	Emond		DLL Search Order Hijacking	Password Filter DLL	System Information Discovery			Remote Access Tools		
	Regsvcs/Regasm			DLL Side-Loading							
				Execution Guardrails							
				Exploitation for Defense Evasion							

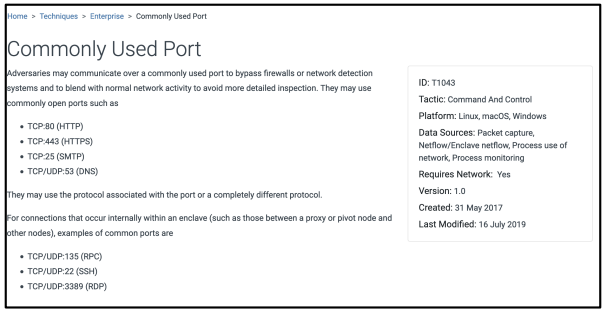


Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[1]
Network Segmentation	Configure internal and external firewalls to block traffic using common ports that associate to network protocols that may be unnecessary for that particular network segment.

Detection

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. [1]



Home > Techniques > Enterprise > Commonly Used Port

Commonly Used Port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as

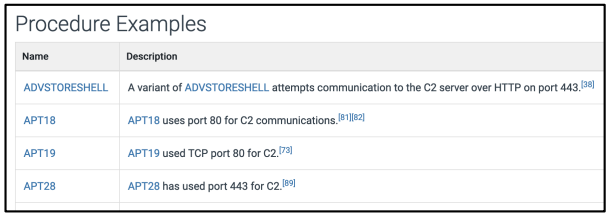
- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are

- TCP/UDP:135 (RPC)
- TCP/UDP:22 (SSH)
- TCP/UDP:3389 (RDP)

ID: T1043
Tactic: Command And Control
Platform: Linux, macOS, Windows
Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring
Requires Network: Yes
Version: 1.0
Created: 31 May 2017
Last Modified: 16 July 2019



Procedure Examples

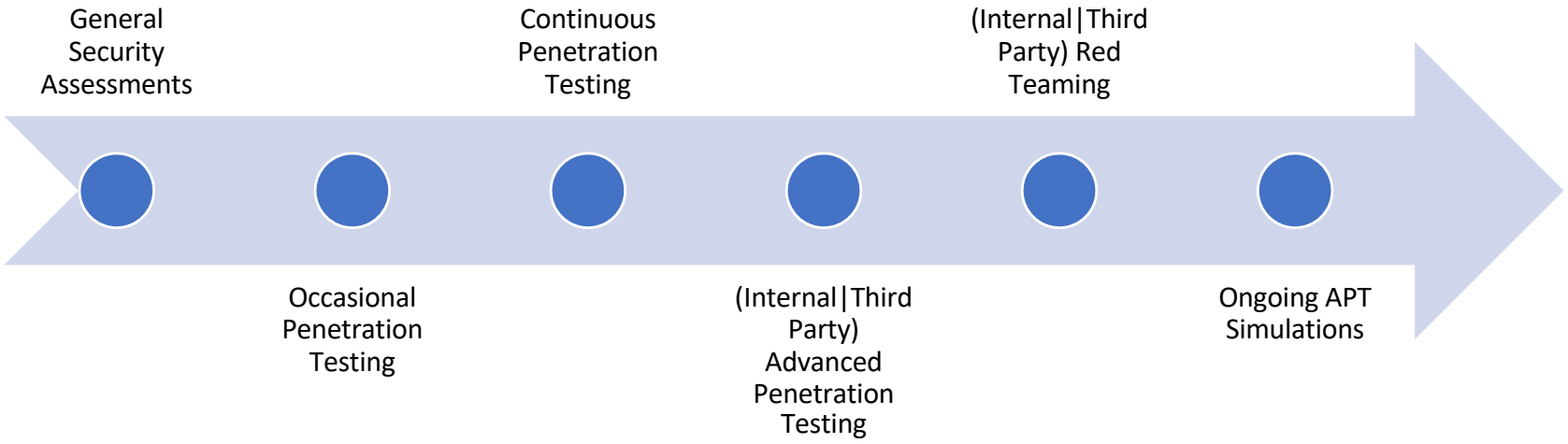
Name	Description
ADVSTORESHELL	A variant of ADVSTORESHELL attempts communication to the C2 server over HTTP on port 443.[38]
APT18	APT18 uses port 80 for C2 communications.[81][82]
APT19	APT19 used TCP port 80 for C2.[73]
APT28	APT28 has used port 443 for C2.[89]

Technique: Commonly Used Ports

Why should you have offensive testing?

- Every organization can use it *on some level*
- May need more than a pentest (or less)
- Challenge SOC/blue team
- Fine tune processes, decrease response time
- There are APTs in your threat model
- Justify security decisions with evidence

Levels of Offensive Testing



Problems with Offensive Testing

- Often compliance driven
- Too many options not enough direction
- Personal anecdotes:
  - Same pentests year after year
  - Pentests that don't map to known adversaries
  - Pentests that don't increase defender capabilities

Solution: Use ATT&CK to guide offensive testing

Use ATT&CK to Determine Offensive Assessments

*LEVEL 0

LEVEL 1 - JUST GETTING STARTED

LEVEL 2 - STARTING TO MATURE, MAYBE HAVE AN INTERNAL RED TEAM

LEVEL 3 - ADVANCED TEAMS, APT SIMULATIONS

- Recently suffered a breach
- Beginning security program
- Have some buy-in from leadership
- APTs that target Pharmaceutical
  - G0010: Turla
  - G0073: APT 19

PHARMAPHLOWERS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise ★	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment ★	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services		DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness		Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard		
	Rundll32			Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User					
	Scheduled Task			Extra Window Memory Injection							
				File and Directory Permissions Modification							

Level 0

Offensive	Defensive	Level Up When…
General Security Assessments	Familiarity with ATT&CK	Understand how to map assessments to ATT&CK
Occasional Penetration Testing	Understand threats in threat model (identify them)	Understand techniques of adversaries in threat model
	Logging/monitoring	Understand where data lives to create necessary analytics

PharmaPhlowers @ Level 0

Offensive	Defensive
Internal Scanning	Patch management program
Occasional “Security Assessment”	Begin researching ATT&CK
One-off Penetration Tests	Begin mapping assessments to ATT&CK
	Know of techniques used by threats

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness		Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories		Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
	Scheduled Task			Extra Window Memory Injection	Two-Factor						
	Scripting			File and Directory Permissions Modification							
				File Deletion							

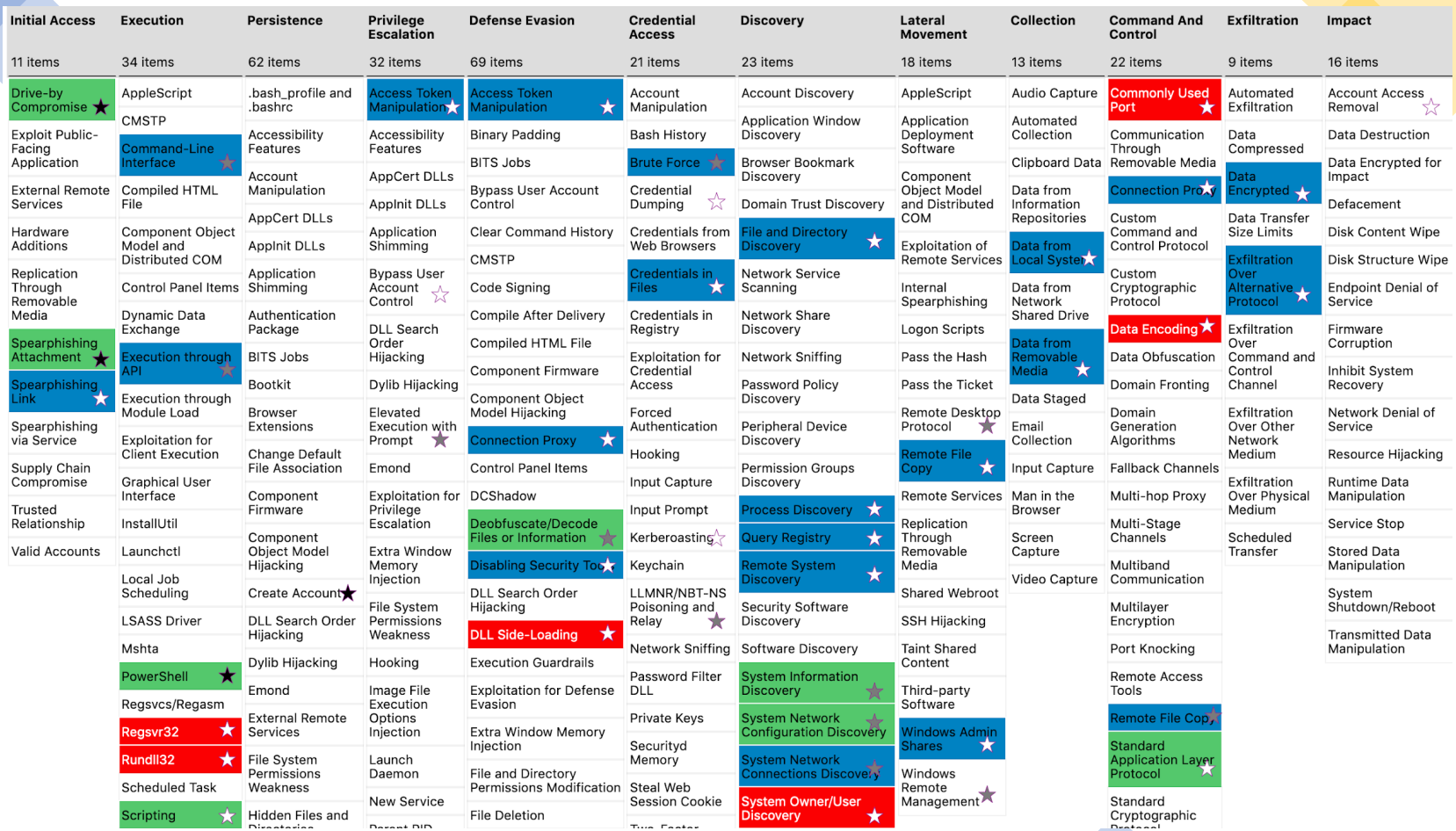
Level 1

Offensive	Defensive	Level Up When…
Continuous Penetration Testing	Map pentests to ATT&CK	Map pentests to ATT&CK with ease
[Previous Offensive Work]	Ability to create analytics from logging/monitoring	Analytics are alerting and teams are responding

MITRE Recommends: Atomic Red Team

PharmaPhlowers @ Level 1

Offensive	Defensive
Quarterly penetration tests	Understand ATT&CK
Atomic Red Team	Create analytics to detect known techniques


Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Persistence
62 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Defense Evasion
69 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
Lateral Movement
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command And Control
22 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
16 items
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

Level 2

Offensive	Defensive	Level Up When…
Internal Penetration Testing Capabilities	Detecting techniques of known adversaries	Able to detect related techniques (Co-occurrence technique identification)
Red Teaming	Ability to create analytics around procedures	Identify attack procedures not just techniques
[Previous Offensive Work]	Multiple identified techniques are responded to and resolved	Detecting attacks that start deeper into kill chain

MITRE Recommends:

- Planning engagements based on CTI and adversary tools
- Mapping RT techniques used to ATT&CK

PharmaPhlowers @ Level 2

Offensive	Defensive
Internal Penetration Testing Team	Cyber Threat Intelligence Feeds
Third Party Pentesters can emulate techniques of known adversaries	Detect procedures vs disparate techniques
	Identify threats based on analytics
	Responding to and resolving (un)announced offensive assessments

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Port Monitors	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
	Scheduled Task	Hooking	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery					
	Scripting	Hypervisor	Scheduled Task	File and Directory Permissions Modification		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Launch Agent	Setuid and Setgid	File Permissions Modification							
	Signed Script Proxy Execution	Launch Daemon	SID-History Injection	File System Logical Offsets							
	Source	Launchctl	Startup Items	Gatekeeper Bypass							
	Space after Filename	Launchctl	Sudo	Group Policy Modification							
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Hidden Files and Directories							
	Trap	Local Job Scheduling	Valid Accounts	Hidden Users							
	Trusted Developer Utilities	Login Item	Web Shell	Hidden Window							
	User Execution	Logon Scripts		HISTCONTROL							
	Windows Management Instrumentation	LSASS Driver		Image File Execution Options Injection							
	Windows Remote Management	Modify Existing Service		Indicator Blocking							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal from Tools							
		New Service		Indicator Removal on Host							
		Office Application Startup		Indirect Command Execution							
		Path Interception		Install Root Certificate							
		Plist Modification		InstallUtil							
		Port Knocking		Launchctl							
		Port Monitors		LC_MAIN Hijacking							
		Rc.common		Masquerading							
		Redundant Access		Modify Existing Service							
		Registry Run Keys / Startup Folder		Modify Registry							
		Re-opened Applications		Mshta							
		Screensaver		Network Share Connection Removal							
		Security Support Provider		NTFS File Attributes							
		Service Registry Permissions Weakness		Obfuscated Files or Information							
		Setuid and Setgid		Parent PID Spoofing							
		Shortcut Modification		Path Interception							
		SIP and Trust Provider Hijacking		Plist Modification							
		Startup Items		Port Knocking							
		System Firmware		Process Doppelgänging							
		Systemd Service		Process Hollowing							
		Time Providers		Process Injection							
		Trap		Redundant Access							
		Valid Accounts		Regsvcs/Regasm							
		Web Shell		Regsvr32							
		Windows Management Instrumentation Event Subscription		Rootkit							
		Winlogon Helper DLL		Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

Level 3

Offensive	Defensive
APT Style Engagements	Detecting and responding to adversary emulation
Red Teaming informed by CTI	Stopping attacks that deviate from known ATT&CK TTPs
[Previous Offensive Work]	
Red Team has custom tooling capabilities	
Varied procedures during assessments	
End-to-end adversary emulation	

MITRE Recommends

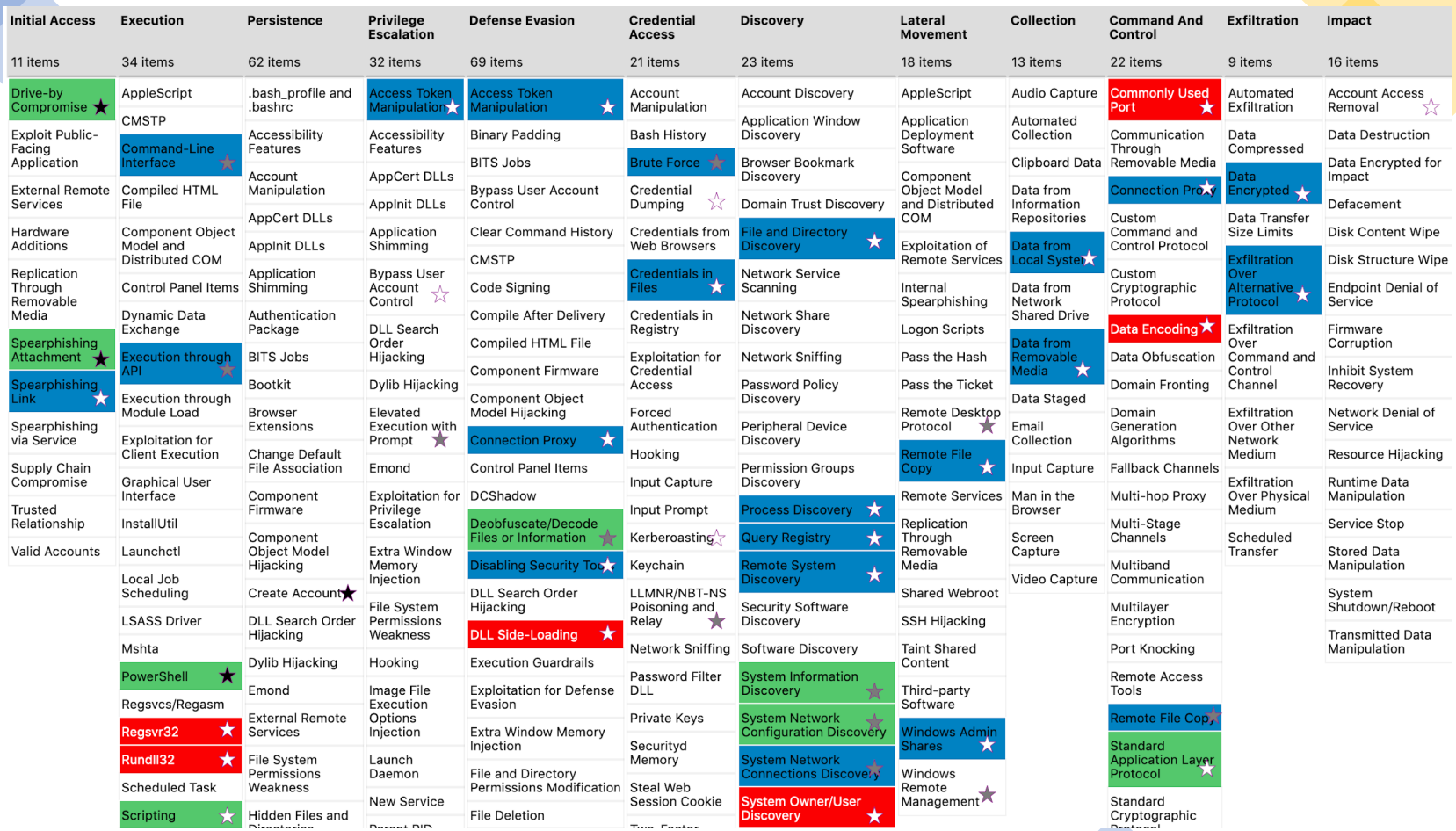
- Planning engagements based on CTI and adversary tools
- Performing threat-based adversary simulations

PharmaPhlowers @ Level 3

Offensive	Defensive
Advanced simulations	Working to detect Pre-Attack
Multiple testing's scenarios	Stopping attacks that deviate from known ATT&CK TTPs
Testing adapted from emerging CTI	
Multiphase, antagonistic assessments	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise ★	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment ★	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services		DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness		Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard		
	Rundll32			Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User					
	Scheduled Task			Extra Window Memory Injection							
				File and Directory Permissions Modification							

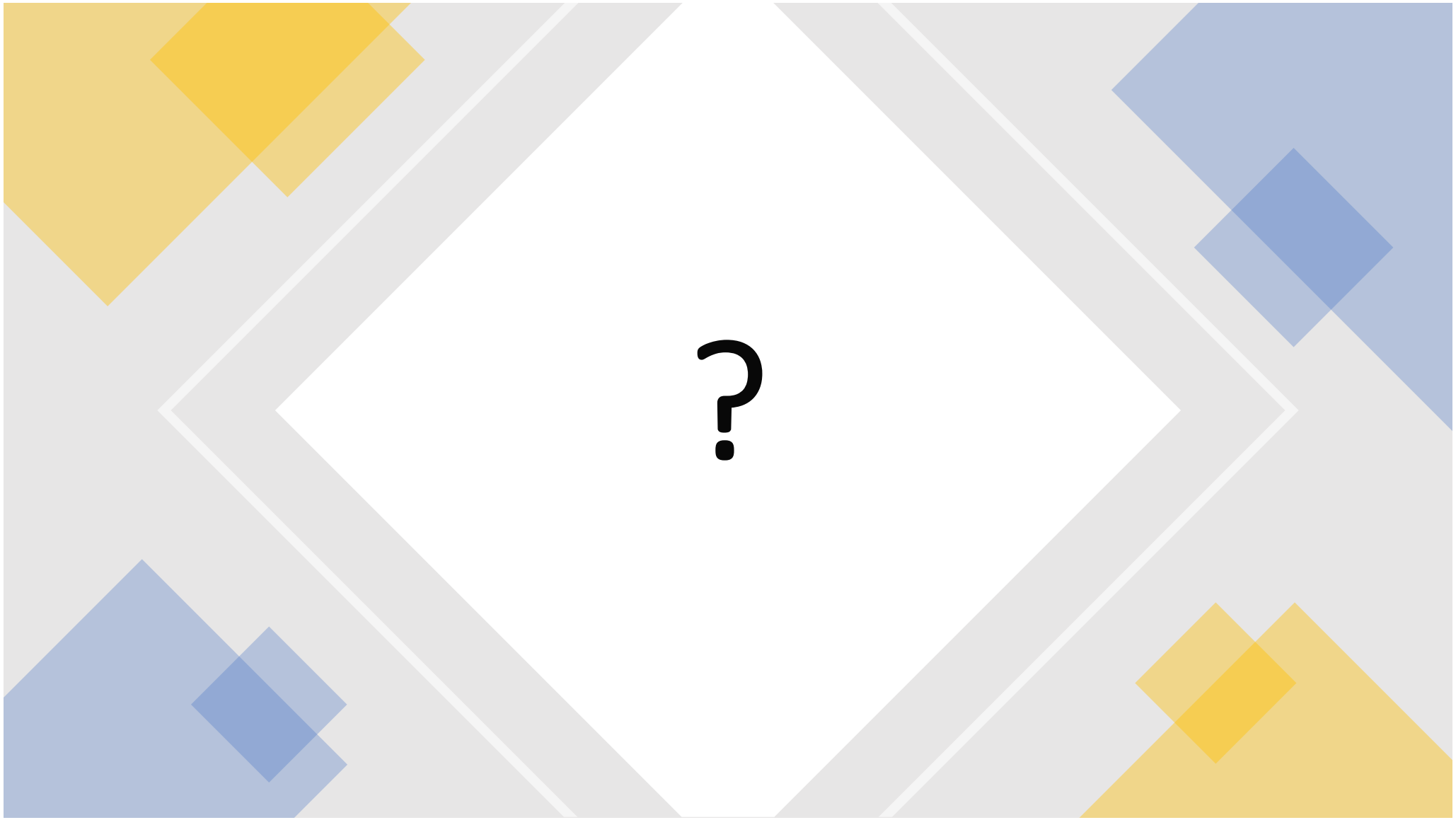
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness		Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories		Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
	Scheduled Task			Extra Window Memory Injection	Two-Factor						
	Scripting			File and Directory Permissions Modification							
				File Deletion							


Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Persistence
62 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Defense Evasion
69 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
Lateral Movement
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command And Control
22 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
16 items
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Port Monitors	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
	Scheduled Task	Hooking	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery					
	Scripting	Hypervisor	Scheduled Task	File and Directory Permissions Modification		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Launch Agent	Setuid and Setgid	File Permissions Modification							
	Signed Script Proxy Execution	Launch Daemon	SID-History Injection	File System Logical Offsets							
	Source	Launchctl	Startup Items	Gatekeeper Bypass							
	Space after Filename	Launchctl	Sudo	Group Policy Modification							
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Hidden Files and Directories							
	Trap	Local Job Scheduling	Valid Accounts	Hidden Users							
	Trusted Developer Utilities	Login Item	Web Shell	Hidden Window							
	User Execution	Logon Scripts		HISTCONTROL							
	Windows Management Instrumentation	LSASS Driver		Image File Execution Options Injection							
	Windows Remote Management	Modify Existing Service		Indicator Blocking							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal from Tools							
		New Service		Indicator Removal on Host							
		Office Application Startup		Indirect Command Execution							
		Path Interception		Install Root Certificate							
		Plist Modification		InstallUtil							
		Port Knocking		Launchctl							
		Port Monitors		LC_MAIN Hijacking							
		Rc.common		Masquerading							
		Redundant Access		Modify Existing Service							
		Registry Run Keys / Startup Folder		Modify Registry							
		Re-opened Applications		Mshta							
		Screensaver		Network Share Connection Removal							
		Security Support Provider		NTFS File Attributes							
		Service Registry Permissions Weakness		Obfuscated Files or Information							
		Setuid and Setgid		Parent PID Spoofing							
		Shortcut Modification		Path Interception							
		SIP and Trust Provider Hijacking		Plist Modification							
		Startup Items		Port Knocking							
		System Firmware		Process Doppelgänging							
		Systemd Service		Process Hollowing							
		Time Providers		Process Injection							
		Trap		Redundant Access							
		Valid Accounts		Regsvcs/Regasm							
		Web Shell		Regsvr32							
		Windows Management Instrumentation Event Subscription		Rootkit							
		Winlogon Helper DLL		Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

MITRE ATT&CK

- Familiarize yourself
- Examine how the work you're already doing fits into ATT&CK
- Understand threats in threat model



Infoz

https://github.com/isaiahsarju/presentations

@isaiahsarju all over the interwebz

Sources and Thanks

- https://attack.mitre.org/
- @marcusjcarey
- Folks @BurbsecEast
- @_joannatess
- https://medium.com/mitre-attack/how-to-be-a-savvy-attack-consumer-63e45b8e94c9
- https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4
- https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3
- https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
- https://medium.com/mitre-attack/finding-related-att-ck-techniques-f1a4e8dfe2b6