ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

MITRE ATT&CK
Perché un nuovo framework e come utilizzarlo

Antonio Forzieri
EMEA Cyber Security Specialization and Advisory

Roma 10/07/2020

Agenda

1. whoami
2. A look into Cyber Security Frameworks
3. MITRE ATT&CK introduction
4. Let’s have a look at ATT&CK
5. Most common use cases
6. The Good the Bad and the Ugly
7. APT10 Example
8. Q&A

whoami

- Happy husband and dad
  - My little daughter will be ***1 year old tomorrow***
- Degree as a Telecommunication Engineer at Politecnico di Milano
- **Today**: EMEA Cyber Security Spcialization and Advisory at Splunk (3 months):
  - Responsible for Cyber Security across EMEA
- **Past**: Global Cyber Security Practice Lead at Symantec (13 long years):
  - Built Centralized/Decentralized SOCs for customers
  - Worked on building Threat Intel Programs
  - Supported customers during various breaches
- Lecturer at **Politecnico di Milano** since 13 years
- Love **hacking** and **coding**
- EMT since 25 years (yes COVID was/is a mess).
- Wine taster/snowboarder/biker/love sailing

A Look into Cyber Security Frameworks

splunk> turn data into doing™

A nice story about frameworks

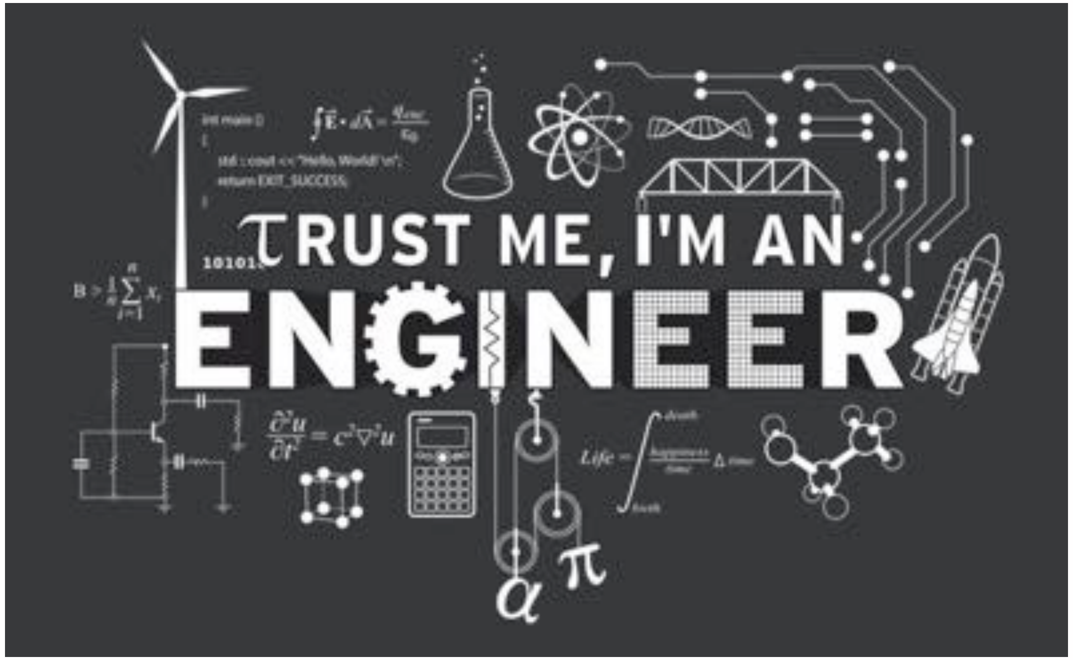
Si narra di un signore ricchissimo che decide di interpellare un ***matematico*** un ***fisico*** e un ***ingegnere*** chiedendogli di fare un modello applicato alle gare ippiche che permetta di indovinare scientificamente il cavallo vincente.

Da ai tre un mese di tempo…

A nice story about frameworks

Alla fine del mese:

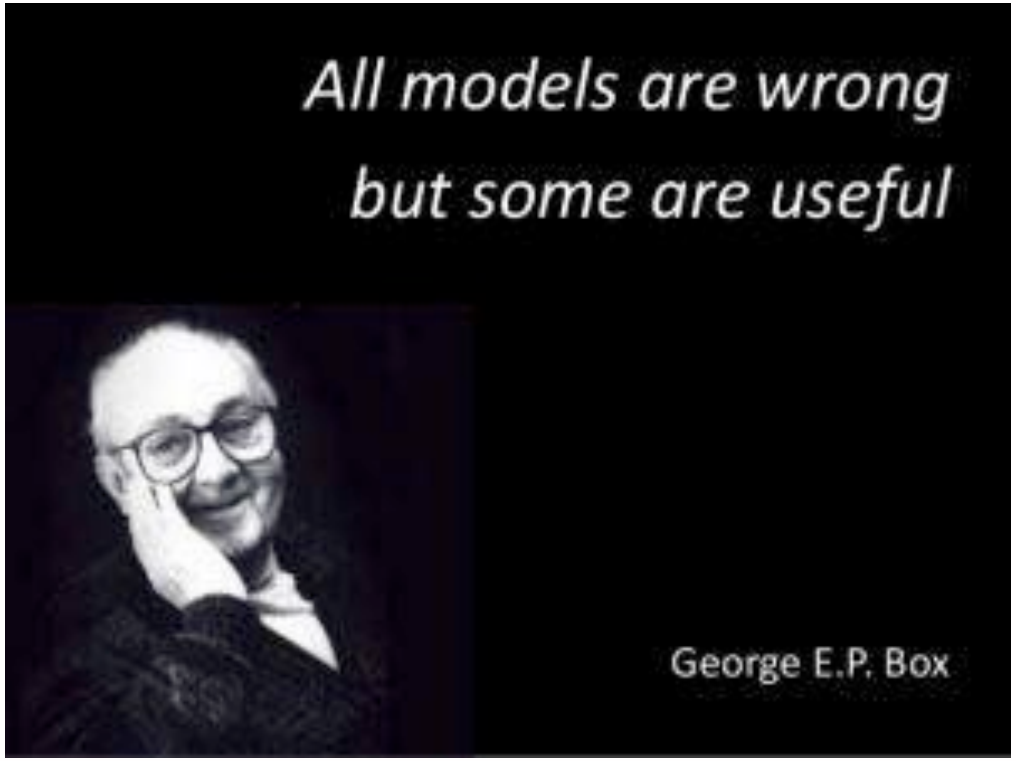
- il ***matematico*** risponde dicendo il problema è mal posto e che non è possibile raggiungere una soluzione
- il ***fisico*** fa altrettanto dicendo che ci sono troppe variabili dunque troppe incognite
- ***l'ingegnere*** invece arriva bello bello con la sua relazione di 20 pagine e il suo modello per predire il vincitore



A nice story about frameworks

alla fine della relazione vi è però una nota:

Per comodità di calcolo i cavalli sono supposti sferici



All models are wrong but some are useful

George E.P. Box

Common Cyber Security Attack & Response Frameworks

For SOC Managers, IT Security Architecture, SOC Analysts

- **OODA Loop**
- **Diamond Model**
- **Lockeed Martin Cyber Kill Chain**
- **MITRE ATT&CK**

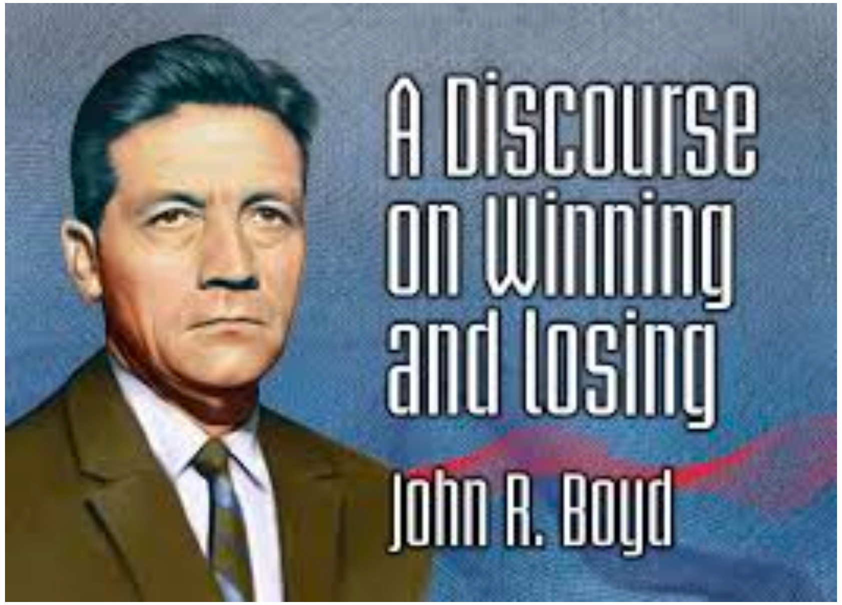
Which one is "best?"

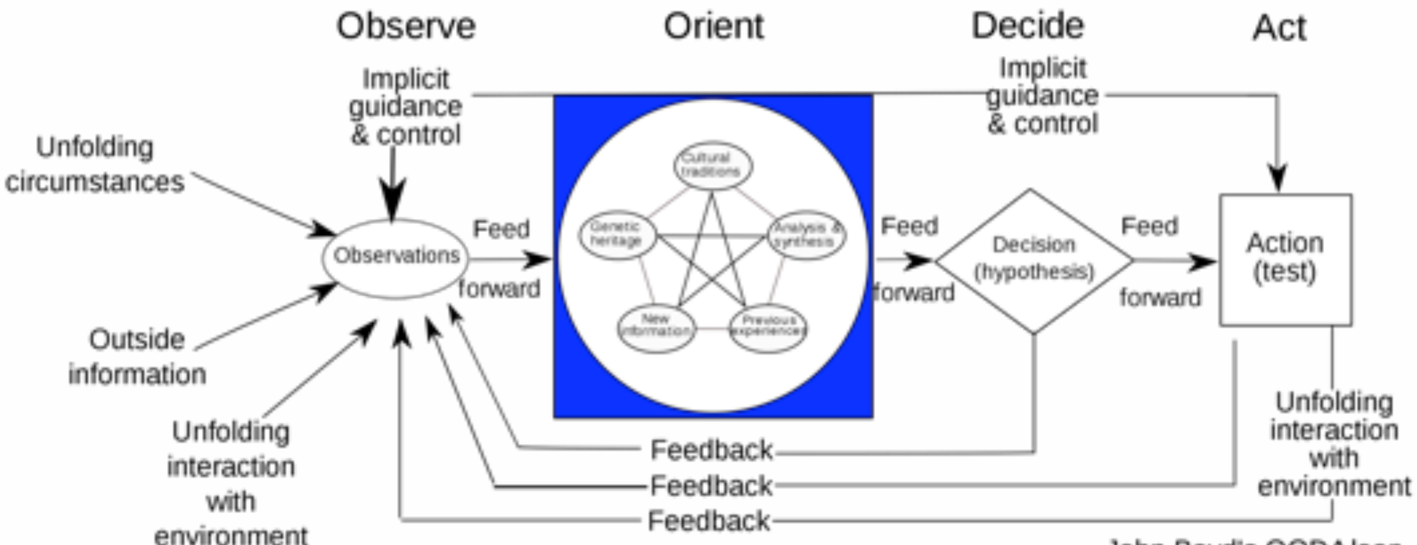
It depends on your requirements!

OODA Loop

From Dogfight to Cyber Security

- Fairly high level and flexible.
- **Observe**: Track security bulletins, advisories
- **Orient**: Assess applicability, operational issues, risk
- **Decide**: Prioritize remediation strategy
- **Act**: Rollout, Monitor, Manage "breakage"





John Boyd's OODA loop

1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

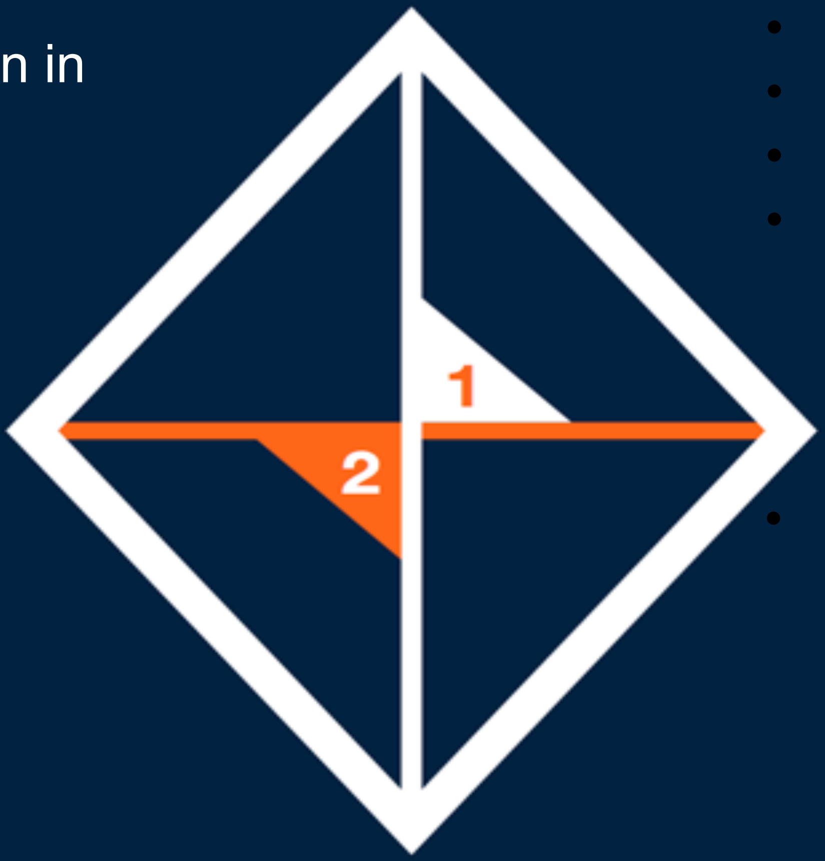
- Nation-state sponsored adversary
- Located (+8.5 timezone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office

CAPABILITIES

- PowerShell Empire
- Spearphishing

INFRASTRUCTURE

- European VPS servers



2 TECHNICAL AXIS

- Documents with .hwp suffix
- PS exec lateral movement
- YMLP
- Self signed SSL/TLS certificates
- +8.5 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara useragent string

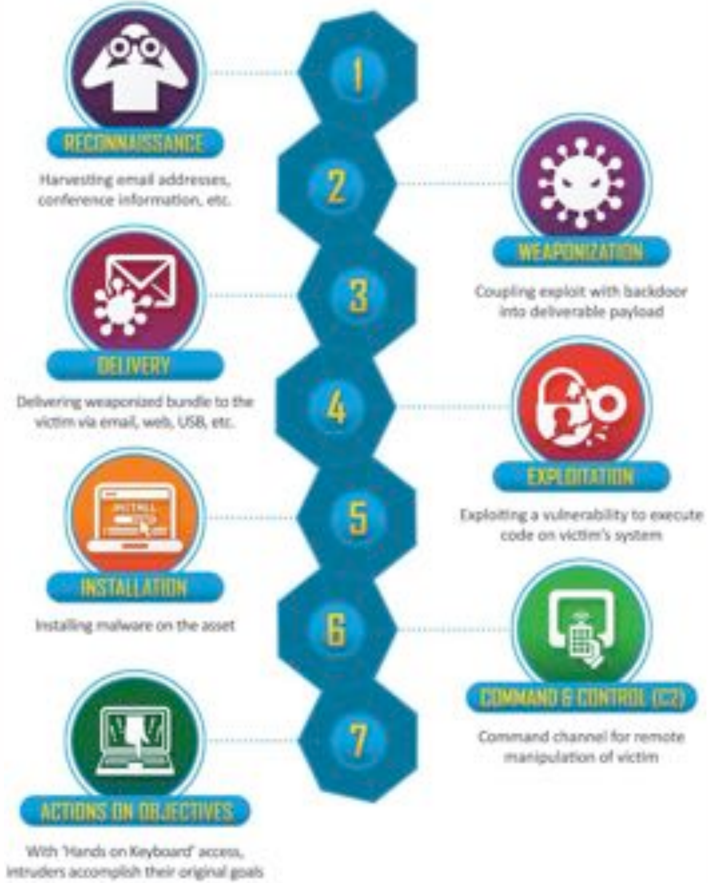
VICTIMS

- Western innovative Brewers and Home Brewing companies

A special thanks to THREATCONNECT

Lockheed Martin Cyber Kill Chain

- **When is it useful?**
  - To "bin" the phases of an adversary's intrusion
  - To examine what you might be missing
- **Limitations**
  - High-level
  - Flexible – need to decide among your team how you "bin" information
- **Also examine Courses of Action:**
  - Detect, Deny, Disrupt, Degrade, Deceive, Destroy


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

ONE SIZE DOES NOT FIT ALL
30°C
Von links bügeln/
repasser

So cyber looked for something different

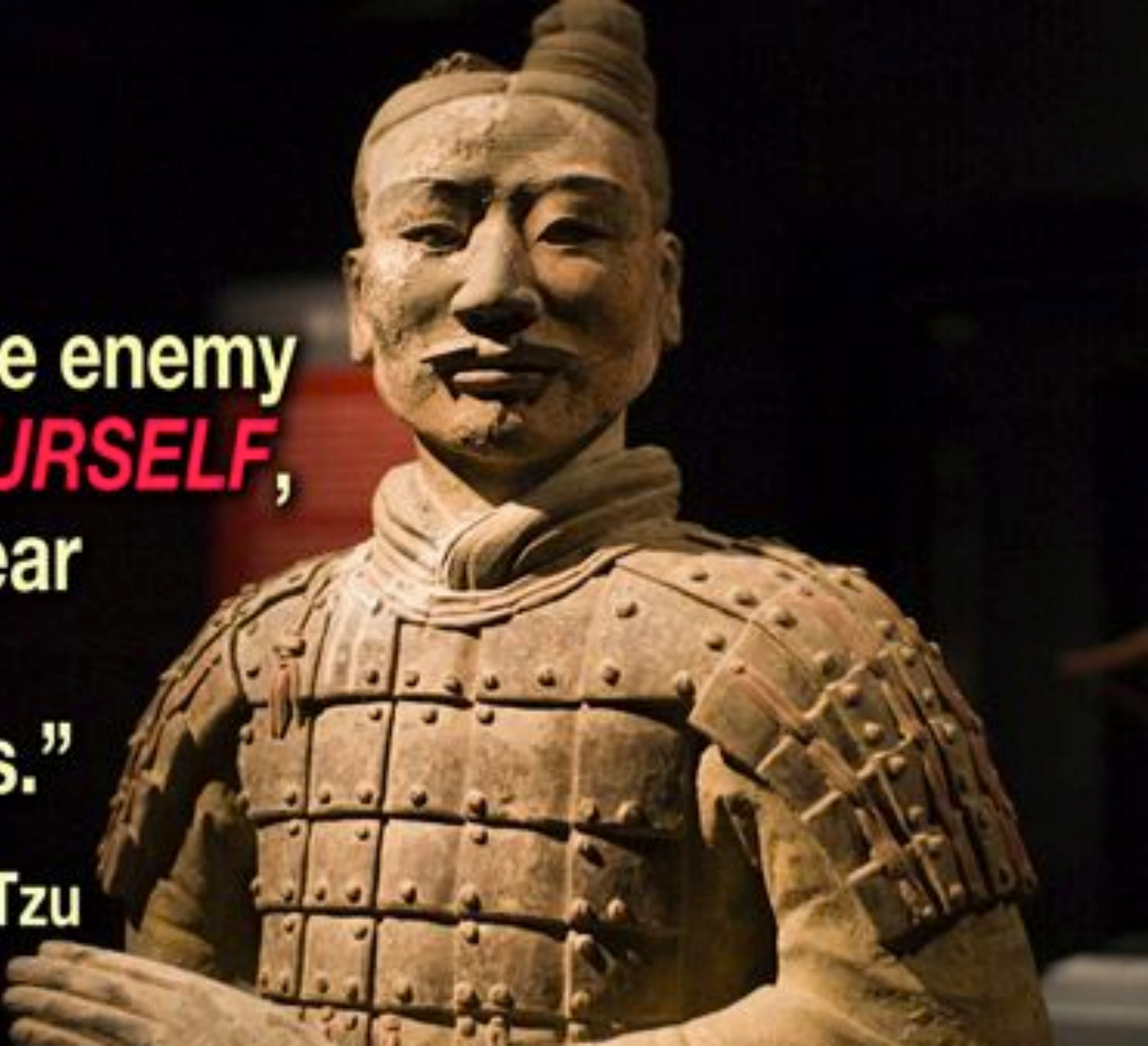
MITRE | ATT&CK™

MITRE ATT&CK explained

splunk> turn data into doing™

“If you know the enemy
and ***KNOW YOURSELF***,
you need not fear
the result of a
hundred battles.”

~ Sun Tzu



MITRE ATT&CK

Few things you need to know

- **ATT&CK**: Adversarial Tactics, Techniques, and Common Knowledge.

- **Tactics**: represent the “why” of an ATT&CK technique or sub-technique. It is the adversary’s tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access. (ROWs in ATT&CK matrix)

- **Techniques**: represent “how” an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. (COLUMNs in ATT&CK matrix)

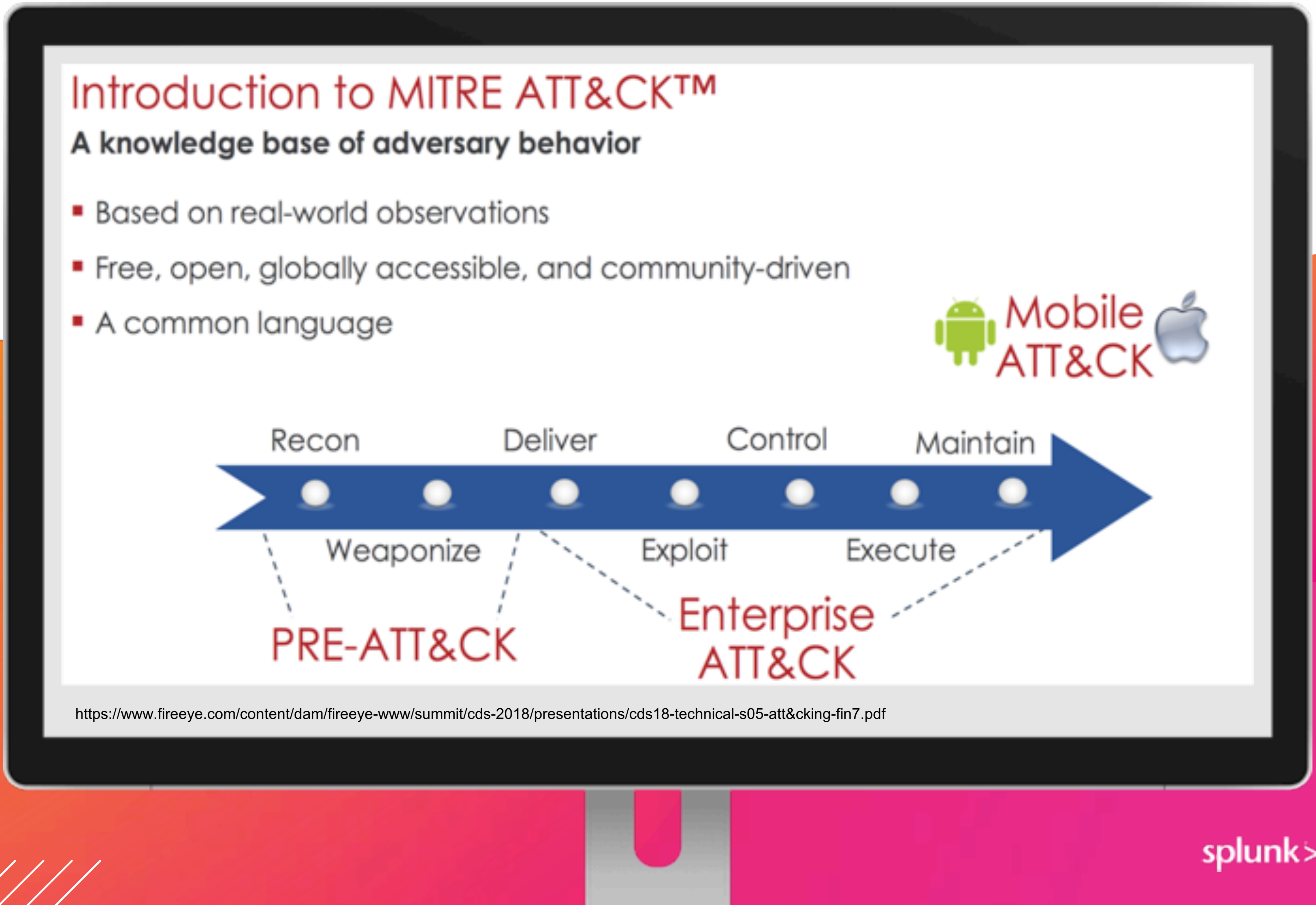
- **Sub-techniques**: are a more specific description of the adversarial behaviour used to achieve a goal. They describe behaviour at a lower level than a technique. *For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.*

MITRE ATT&CK

Few things you need to know

- **Procedures**: are the specific implementation the adversary uses for techniques or sub-techniques. *For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim*. Procedures are categorized in ATT&CK as the observed in the wild use of techniques in the "Procedure Examples" section of technique pages.

- **Sub-techniques vs Procedures**: they describe different things in ATT&CK. Sub-techniques are used to categorize behaviour and procedures are used to describe in-the-wild use of techniques. Furthermore, since procedures are specific implementations of techniques and sub-techniques, they may include several additional behaviours in how they are performed. *For example, an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim is a procedure implementation containing several (sub)techniques covering the PowerShell, Process Injection, and Credential Dumping against LSASS behaviors*.



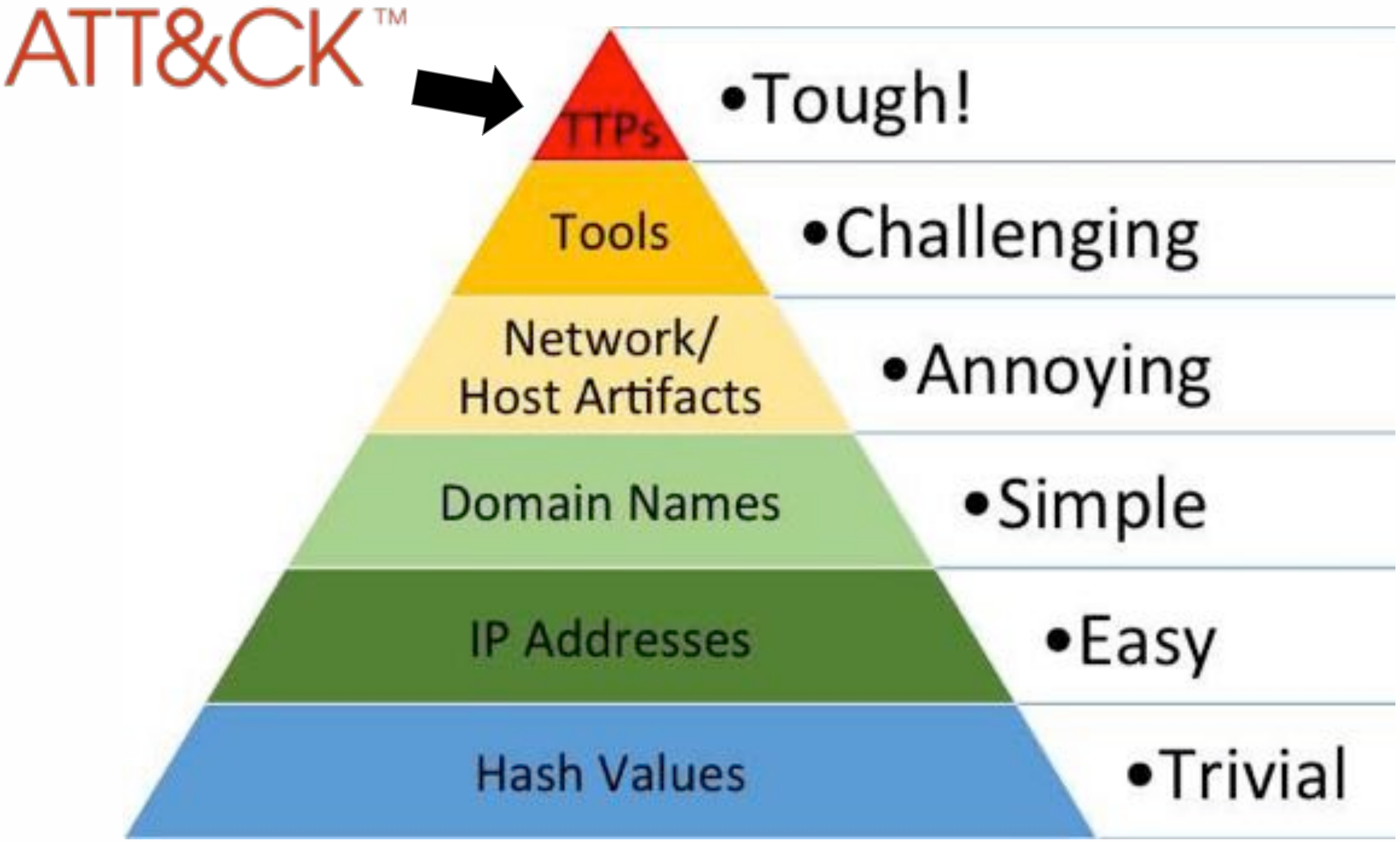
Introduction to MITRE ATT&CK™

A knowledge base of adversary behavior

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

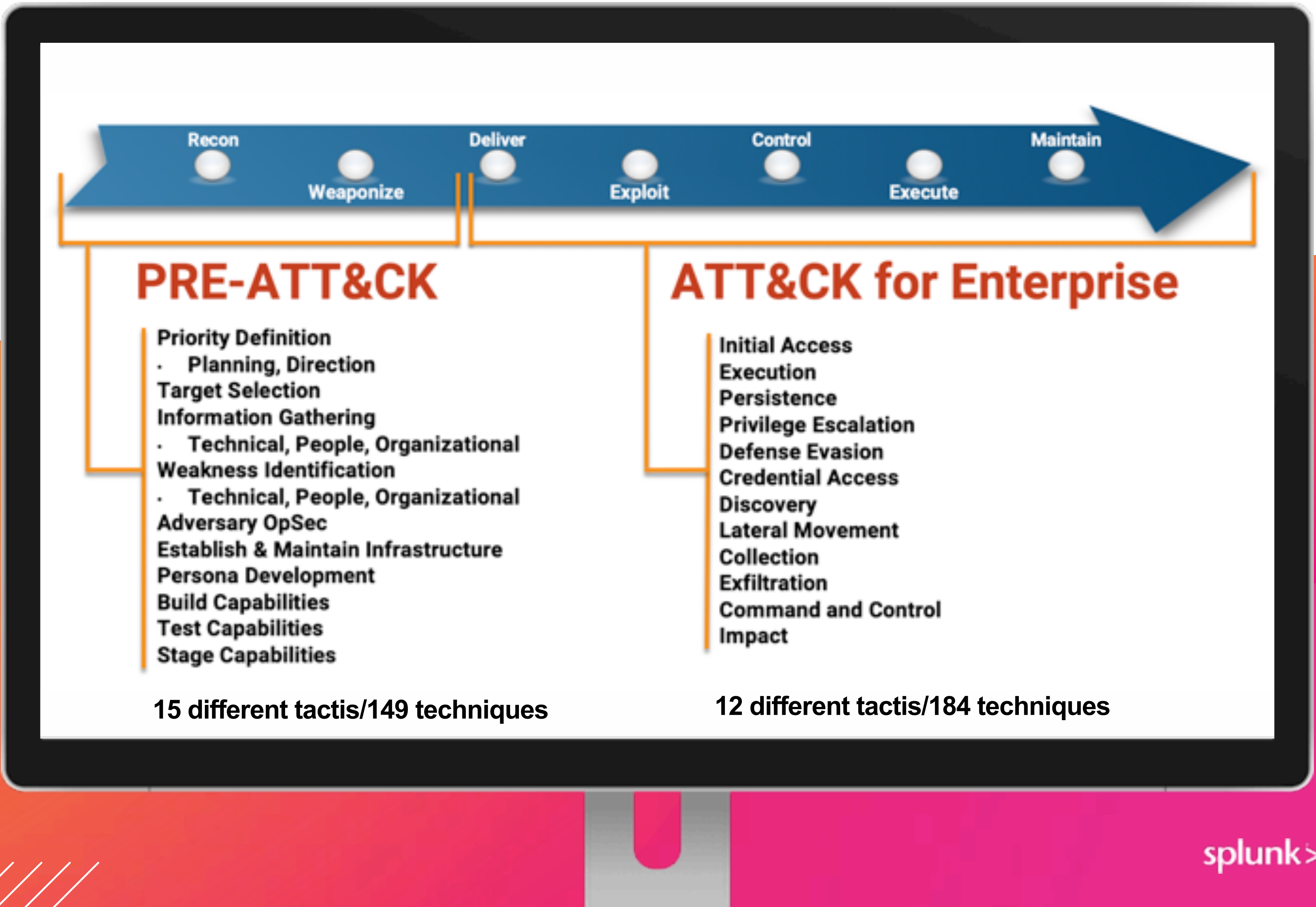
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

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



PRE-ATT&CK

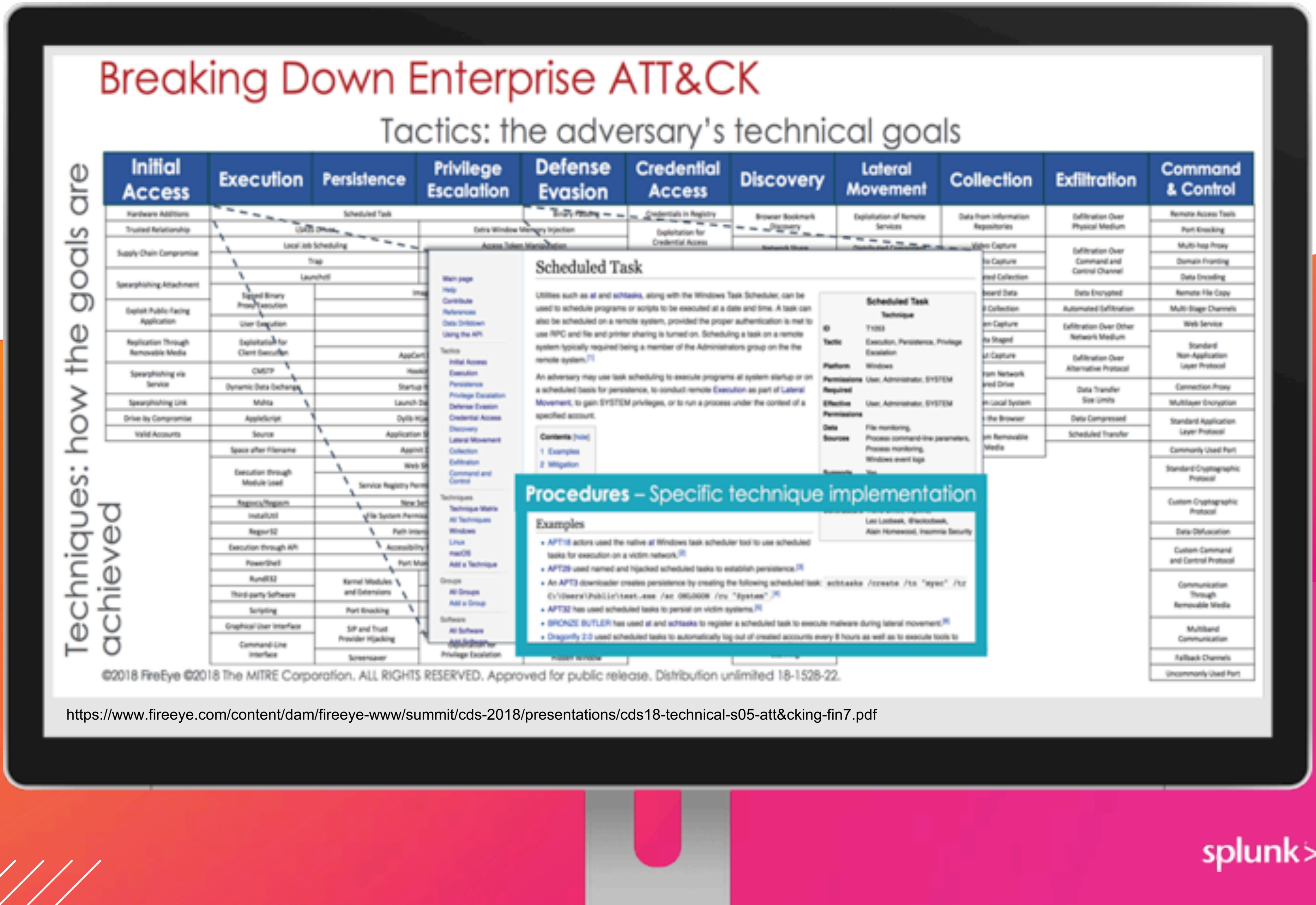
- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

15 different tactis/149 techniques

ATT&CK for Enterprise

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

12 different tactis/184 techniques



Breaking Down Enterprise ATT&CK

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access
- Hardware Additions
- Trusted Relationship
- Supply Chain Compromise
- Spearphishing Attachment
- Exploit Public-Facing Application
- Replication Through Removable Media
- Spearphishing via Service
- Spearphishing Link
- Drive-by Compromise
- Valid Accounts

Execution
- Scheduled Task
- LSASS Driver
- Local Job Scheduling
- Trap
- Launchctl
- Signed Binary Proxy Execution
- User Execution
- Exploitation for Client Execution
- CMSTP
- Dynamic Data Exchange
- Mshta
- AppleScript
- Source
- Space after Filename
- Execution through Module Load
- Regsvcs/Regasm
- InstallUtil
- Regsvr32
- Execution through API
- PowerShell
- Rundll32
- Third-party Software
- Scripting
- Graphical User Interface
- Command-Line Interface

Persistence
- Imag
- AppCert
- Hooki
- Startup
- Launch Da
- Dylib Hij
- Application S
- AppInit
- Web Sh
- Service Registry Perm
- New Ser
- File System Permi
- Path Interc
- Accessibility
- Port Mon
- Kernel Modules and Extensions
- Port Knocking
- SIP and Trust Provider Hijacking
- Screensaver

Privilege Escalation
- Extra Window Memory Injection
- Access Token Manipulation
- Privilege Escalation

Defense Evasion
- Binary Padding
- Hidden Window

Credential Access
- Credentials in Registry
- Exploitation for Credential Access

Discovery
- Browser Bookmark Discovery
- Network Share

Lateral Movement
- Exploitation of Remote Services
- Distributed Component

Collection
- Data from Information Repositories
- Video Capture
- io Capture
- ated Collection
- board Data
- l Collection
- en Capture
- ta Staged
- ut Capture
- rom Network ared Drive
- m Local System
- the Browser
- om Removable Media

Exfiltration
- Exfiltration Over Physical Medium
- Exfiltration Over Command and Control Channel
- Data Encrypted
- Automated Exfiltration
- Exfiltration Over Other Network Medium
- Exfiltration Over Alternative Protocol
- Data Transfer Size Limits
- Data Compressed
- Scheduled Transfer

Command & Control
- Remote Access Tools
- Port Knocking
- Multi-hop Proxy
- Domain Fronting
- Data Encoding
- Remote File Copy
- Multi-Stage Channels
- Web Service
- Standard Non-Application Layer Protocol
- Connection Proxy
- Multilayer Encryption
- Standard Application Layer Protocol
- Commonly Used Port
- Standard Cryptographic Protocol
- Custom Cryptographic Protocol
- Data Obfuscation
- Custom Command and Control Protocol
- Communication Through Removable Media
- Multiband Communication
- Fallback Channels
- Uncommonly Used Port

Main page
Help
Contribute
References
Data Dictionary
Using the API

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

Techniques
Technique Matrix
All Techniques
Windows
Linux
macOS
Add a Technique

Groups
All Groups
Add a Group

Software
All Software
Add Software

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.[1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

Contents [hide]
1 Examples
2 Mitigation

Scheduled Task	
Technique	
ID	T1053
Tactic	Execution, Persistence, Privilege Escalation
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Effective Permissions	User, Administrator, SYSTEM
Data Sources	File monitoring, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote	Yes
Contributors	[illegible] Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security

Procedures – Specific technique implementation

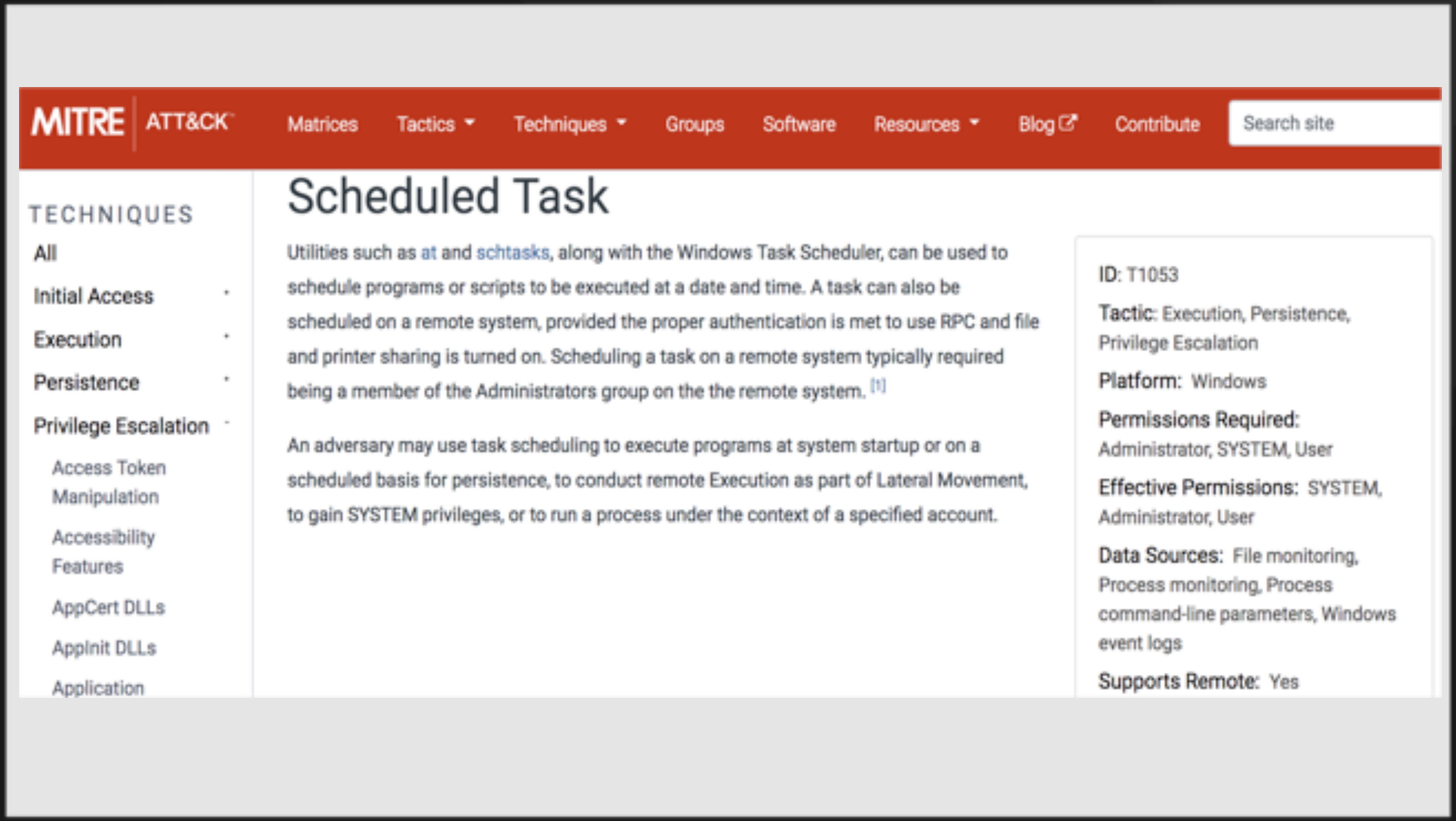
Examples

- APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.[2]
- APT29 used named and hijacked scheduled tasks to establish persistence.[3]
- An APT3 downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[4]
- APT32 has used scheduled tasks to persist on victim systems.[5]
- BRONZE BUTLER has used at and schtasks to register a scheduled task to execute malware during lateral movement.[6]
- Dragonfly 2.0 used scheduled tasks to automatically log out of created accounts every 8 hours as well as to execute tools to

©2018 FireEye ©2018 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 18-1528-22.

https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

splunk> turn data into doing



Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. [1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

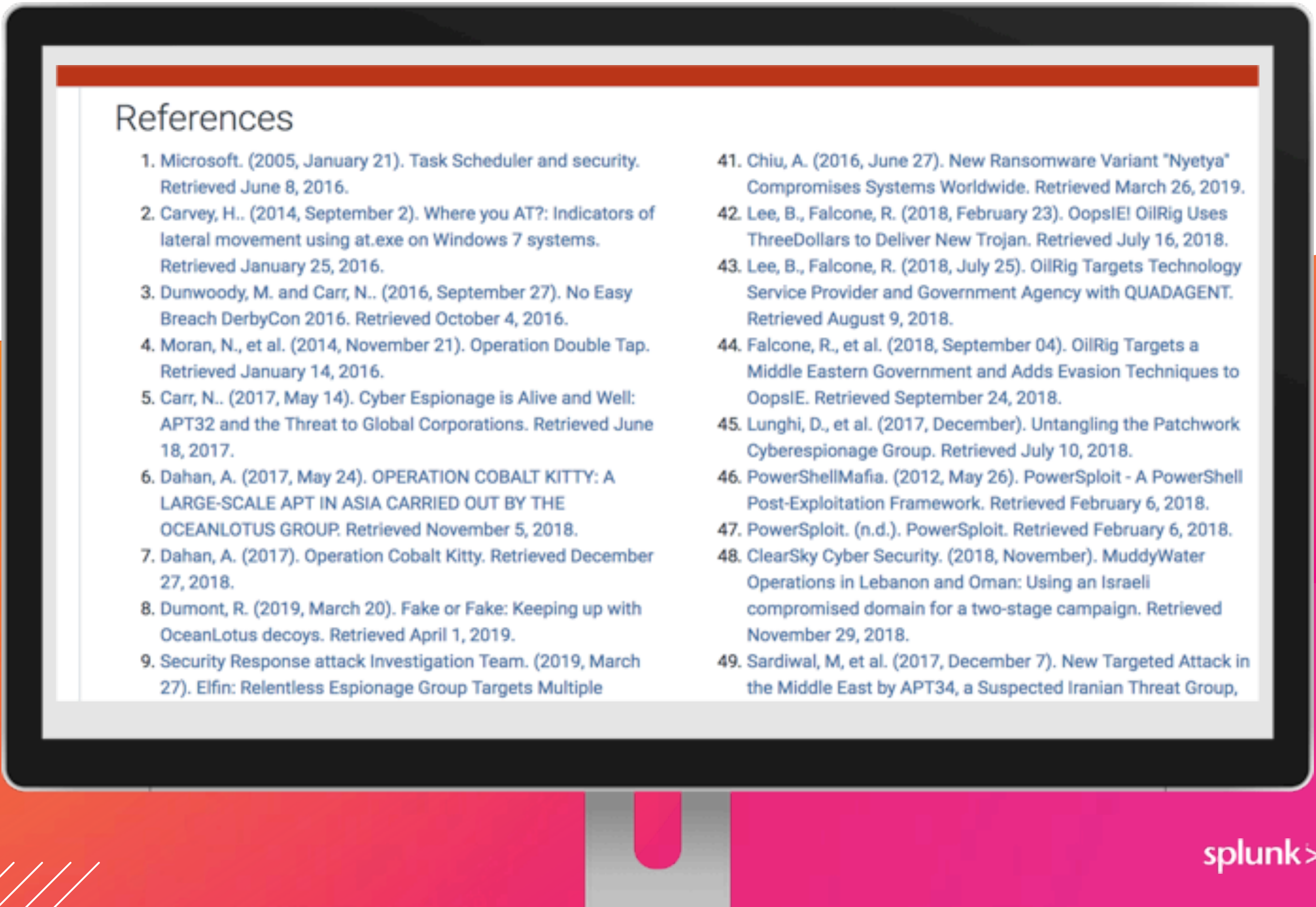
Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: SYSTEM, Administrator, User

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

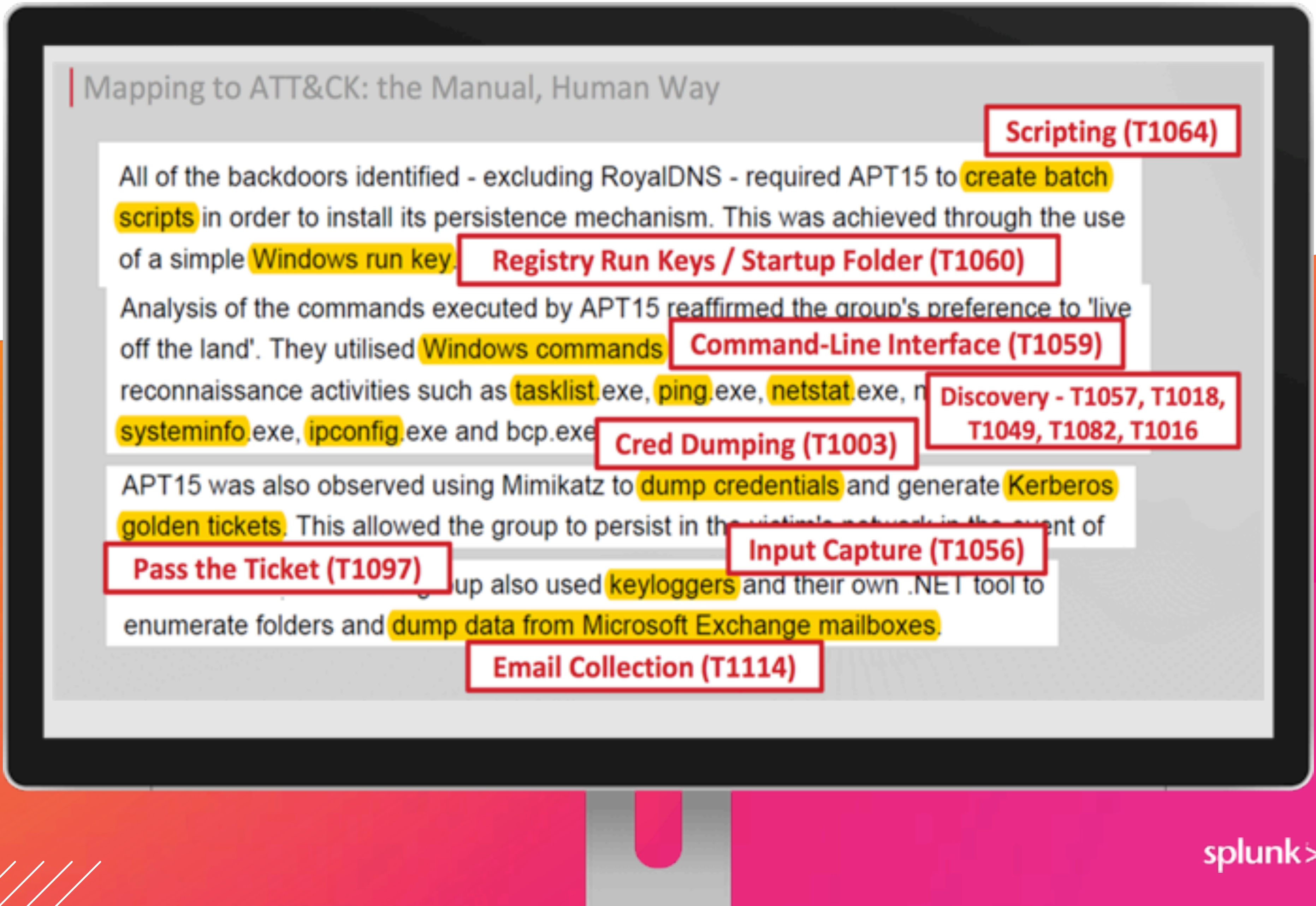
Supports Remote: Yes



References

1. Microsoft. (2005, January 21). Task Scheduler and security. Retrieved June 8, 2016.
2. Carvey, H.. (2014, September 2). Where you AT?: Indicators of lateral movement using at.exe on Windows 7 systems. Retrieved January 25, 2016.
3. Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.
4. Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved January 14, 2016.
5. Carr, N.. (2017, May 14). Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Retrieved June 18, 2017.
6. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
7. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
8. Dumont, R. (2019, March 20). Fake or Fake: Keeping up with OceanLotus decoys. Retrieved April 1, 2019.
9. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple

41. Chiu, A. (2016, June 27). New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Retrieved March 26, 2019.
42. Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
43. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
44. Falcone, R., et al. (2018, September 04). OilRig Targets a Middle Eastern Government and Adds Evasion Techniques to OopsIE. Retrieved September 24, 2018.
45. Lunghi, D., et al. (2017, December). Untangling the Patchwork Cyberespionage Group. Retrieved July 10, 2018.
46. PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.
47. PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.
48. ClearSky Cyber Security. (2018, November). MuddyWater Operations in Lebanon and Oman: Using an Israeli compromised domain for a two-stage campaign. Retrieved November 29, 2018.
49. Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group,



Mapping to ATT&CK: the Manual, Human Way

Scripting (T1064)

All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Registry Run Keys / Startup Folder (T1060)

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

Command-Line Interface (T1059)

reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, n

systeminfo.exe, ipconfig.exe and bcp.exe

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

Input Capture (T1056)

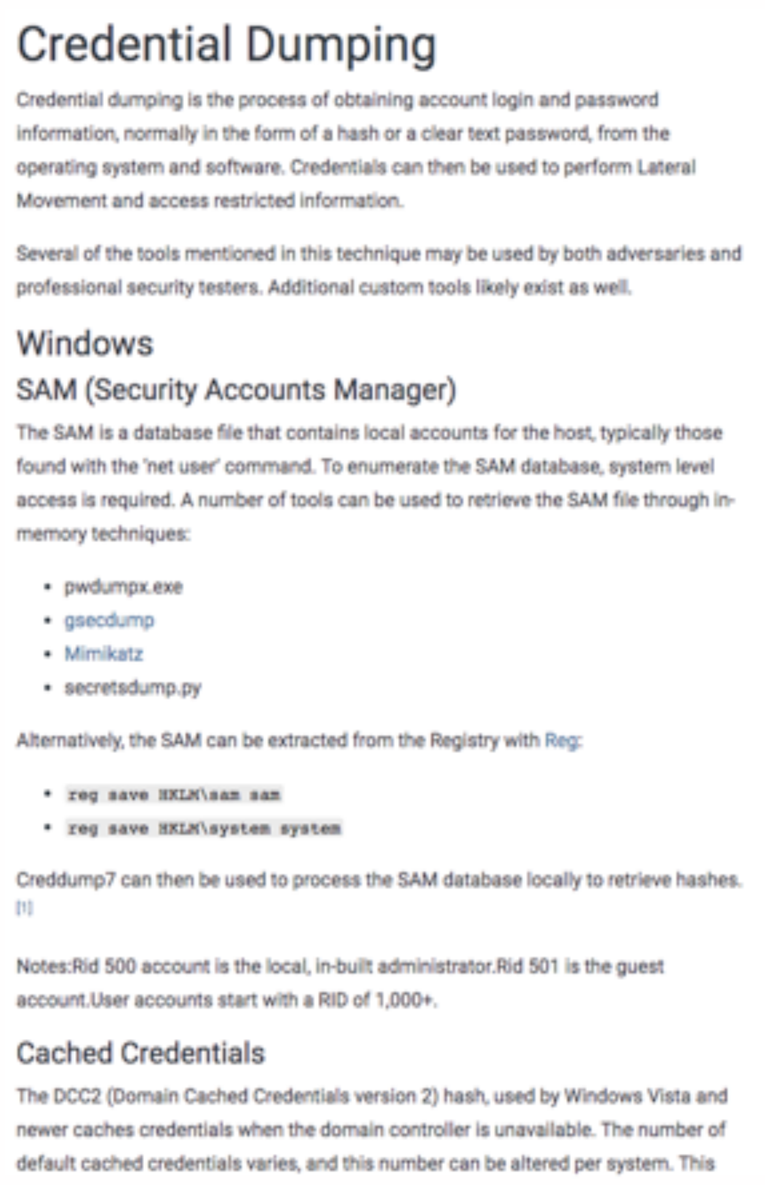
Pass the Ticket (T1097)

up also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

Email Collection (T1114)

Example: Credential Dumping

8 different ways of dumping credentials all lumped together into the label Credential Dumping.



Credential Dumping

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Windows

SAM (Security Accounts Manager)

The SAM is a database file that contains local accounts for the host, typically those found with the 'net user' command. To enumerate the SAM database, system level access is required. A number of tools can be used to retrieve the SAM file through in-memory techniques:

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg:

- `reg save HKLM\sam sam`
- `reg save HKLM\system system`

Creddump7 can then be used to process the SAM database locally to retrieve hashes.[1]

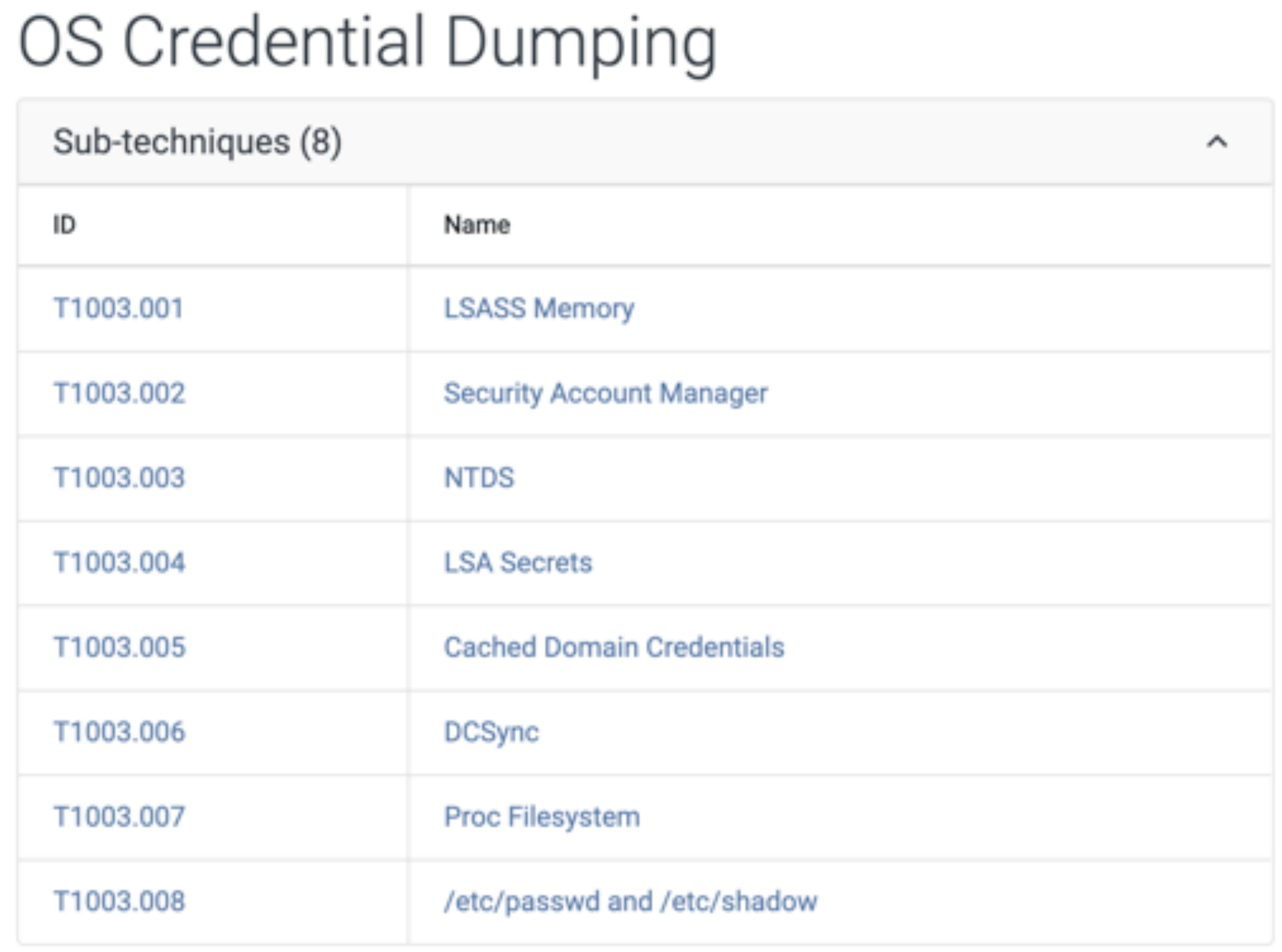
Notes:Rid 500 account is the local, in-built administrator.Rid 501 is the guest account.User accounts start with a RID of 1,000+.

Cached Credentials

The DCC2 (Domain Cached Credentials version 2) hash, used by Windows Vista and newer caches credentials when the domain controller is unavailable. The number of default cached credentials varies, and this number can be altered per system. This

Example: Credential Dumping with Sub-Techniques

Technique renamed with the addition of 8 Sub-Techniques.

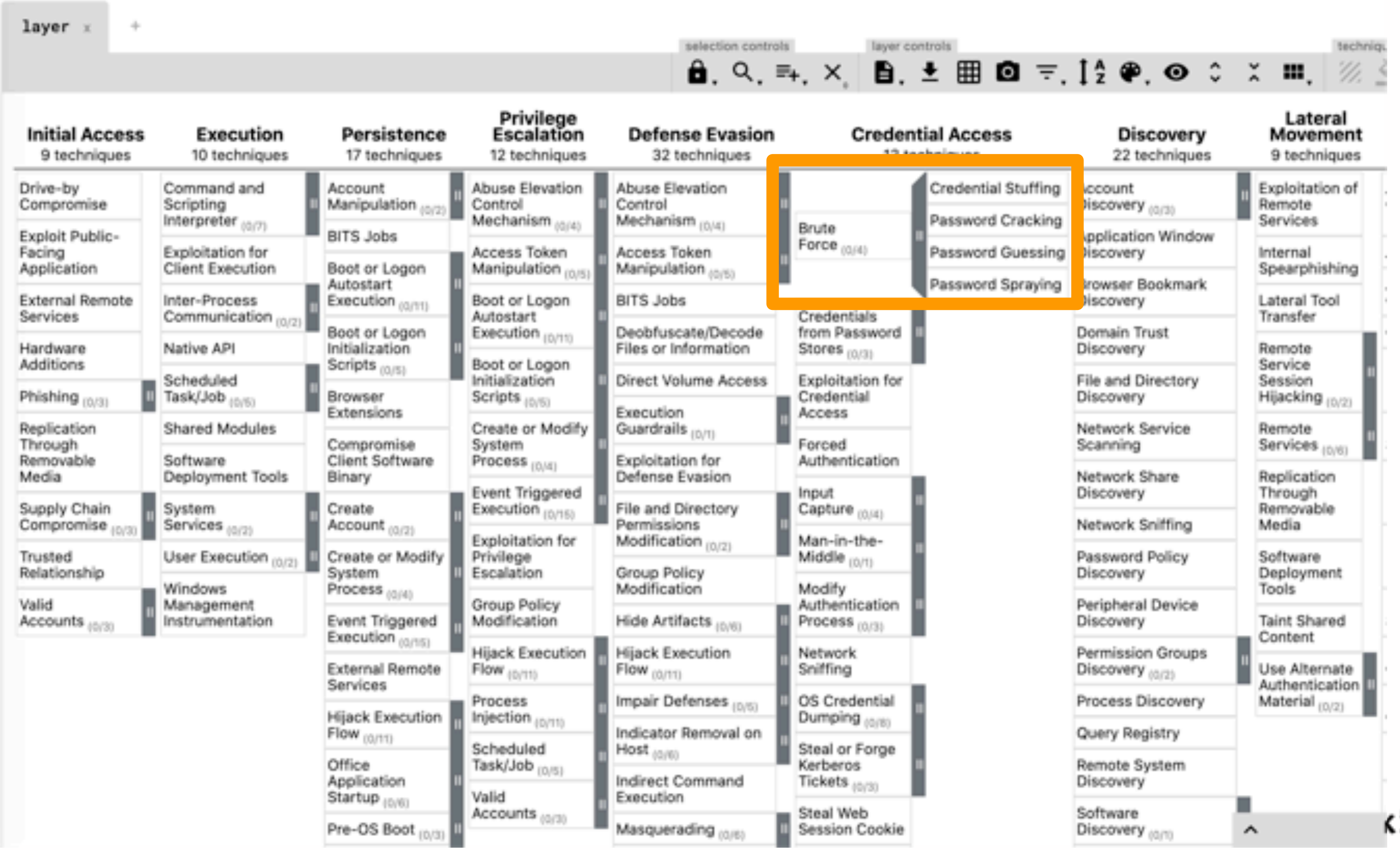


OS Credential Dumping

Sub-techniques (8)

ID	Name
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS
T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc Filesystem
T1003.008	/etc/passwd and /etc/shadow

ATT&CK Navigator with Sub-Techniques



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution
10 techniques

- Command and Scripting Interpreter (0/7)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence
17 techniques

- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (0/11)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Office Application Startup (0/6)
- Pre-OS Boot (0/3)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/11)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/3)

Defense Evasion
32 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/6)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/5)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)

Credential Access
12 techniques

- Brute Force (0/4)
  - Credential Stuffing
  - Password Cracking
  - Password Guessing
  - Password Spraying
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/1)
- Modify Authentication Process (0/3)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal or Forge Kerberos Tickets (0/3)
- Steal Web Session Cookie

Discovery
22 techniques

- ccount Discovery (0/3)
- pplication Window Discovery
- rowser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/2)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/2)

Let’s have a look at the ATT&CK framework.

What are the most common use cases

splunk> turn data into doing™

ATT&CK Use Cases

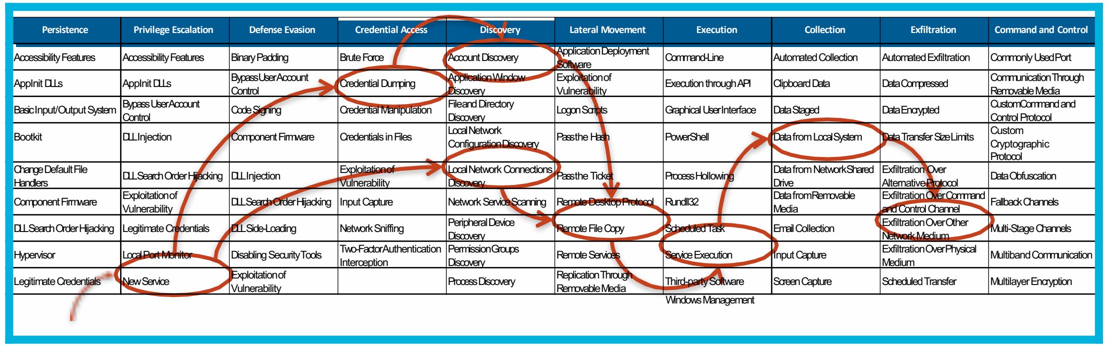
Detection

```
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

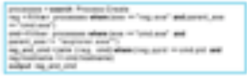
Assessment and Engineering

Adversary Emulation



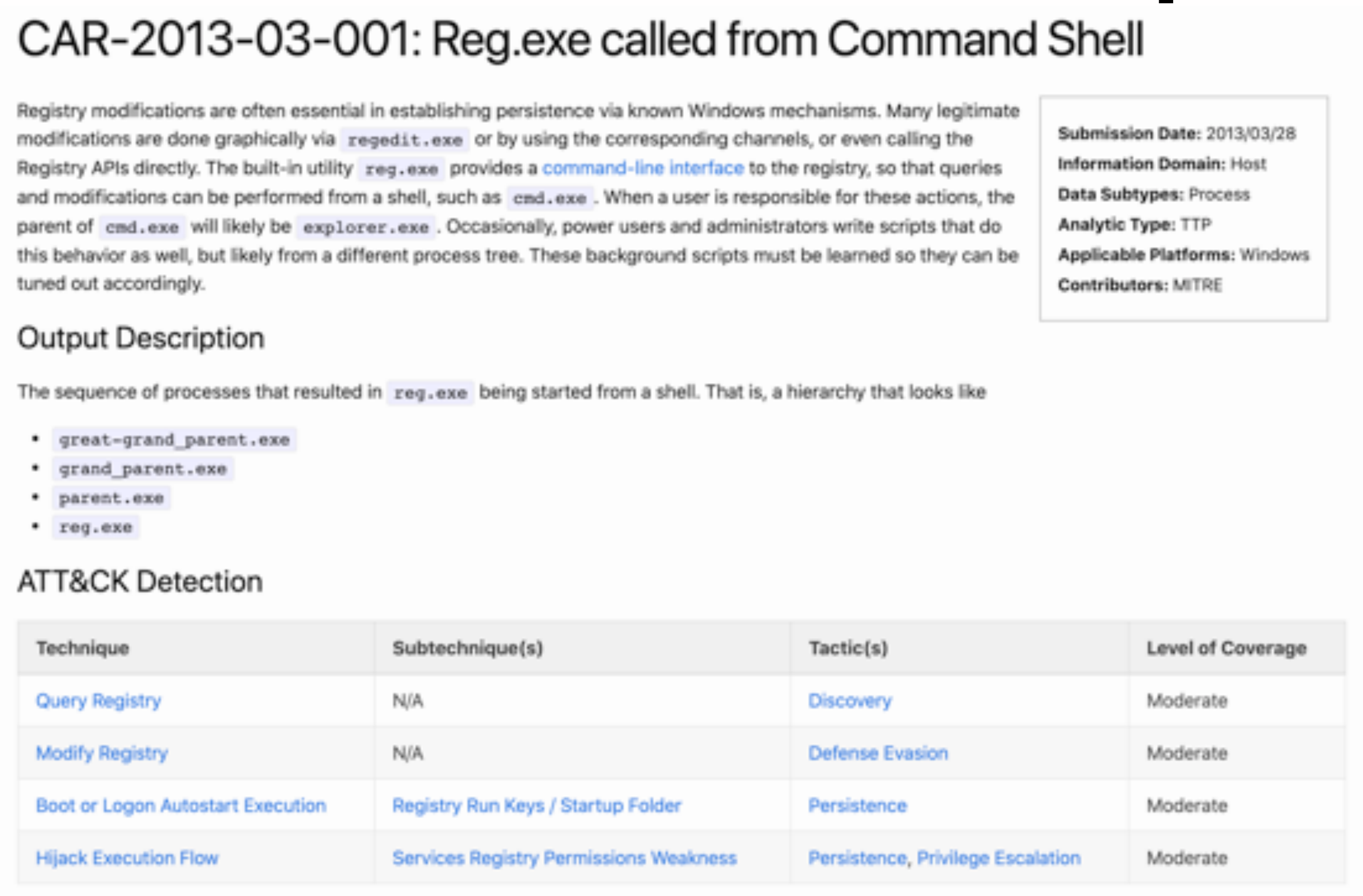
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	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			

Detection – reuse what you can!



- Look at shared analytics/content and choose what to implement
- Adapt them for your own data sources and environment
- This is where you can start from:
  - Splunk Security Essentials: https://www.splunksecurityessentials.com/
  - Splunk ES Content Updates: https://splunkbase.splunk.com/app/3449/
  - MITRE 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/hunters-forge/ThreatHunter-Playbook
  - Sigma: https://github.com/Neo23x0/sigma
  - Atomic Threat Coverage: https://github.com/krakow2600/atomic-threat-coverage

Detection – MITRE Example Analytic



CAR-2013-03-001: Reg.exe called from Command Shell

Registry modifications are often essential in establishing persistence via known Windows mechanisms. Many legitimate modifications are done graphically via `regedit.exe` or by using the corresponding channels, or even calling the Registry APIs directly. The built-in utility `reg.exe` provides a command-line interface to the registry, so that queries and modifications can be performed from a shell, such as `cmd.exe`. When a user is responsible for these actions, the parent of `cmd.exe` will likely be `explorer.exe`. Occasionally, power users and administrators write scripts that do this behavior as well, but likely from a different process tree. These background scripts must be learned so they can be tuned out accordingly.

Submission Date: 2013/03/28
Information Domain: Host
Data Subtypes: Process
Analytic Type: TTP
Applicable Platforms: Windows
Contributors: MITRE

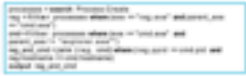
Output Description

The sequence of processes that resulted in `reg.exe` being started from a shell. That is, a hierarchy that looks like

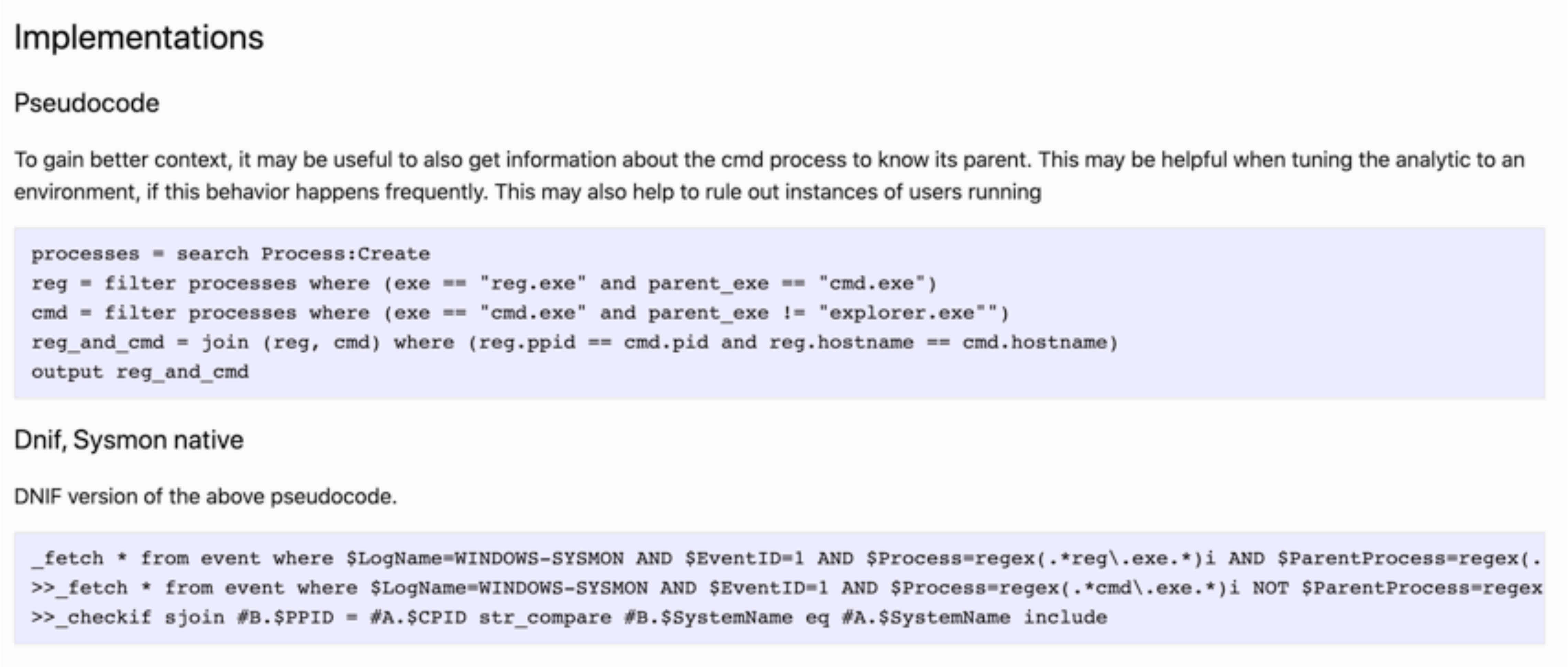
- `great-grand_parent.exe`
- `grand_parent.exe`
- `parent.exe`
- `reg.exe`

ATT&CK Detection

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
Query Registry	N/A	Discovery	Moderate
Modify Registry	N/A	Defense Evasion	Moderate
Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder	Persistence	Moderate
Hijack Execution Flow	Services Registry Permissions Weakness	Persistence, Privilege Escalation	Moderate



Detection – MITRE Example Analytic



Implementations

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

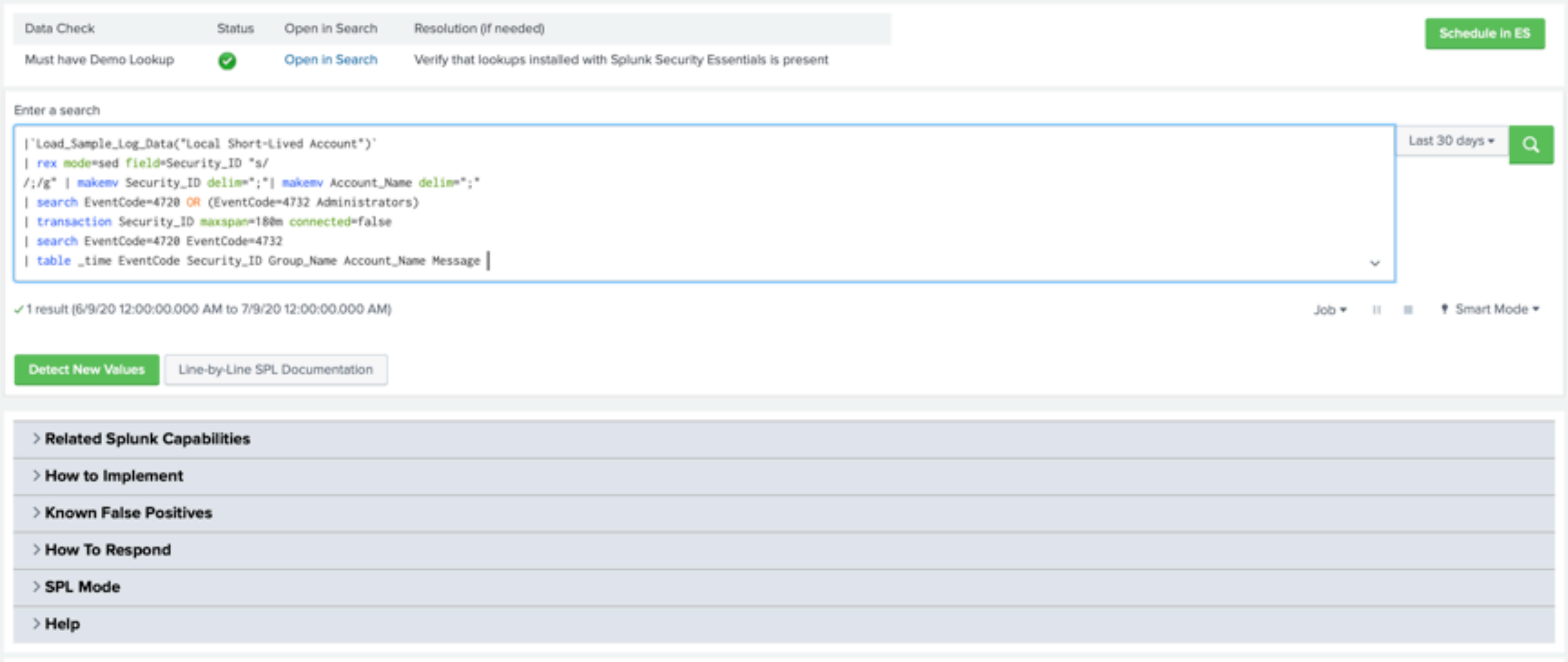
```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe == "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and reg.hostname == cmd.hostname)
output reg_and_cmd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

Dnif, Sysmon native

DNIF version of the above pseudocode.

```
_fetch * from event where $LogName=WINDOWS-SYSMON AND $EventID=1 AND $Process=regex(.*reg\.exe.*)i AND $ParentProcess=regex(.
>>_fetch * from event where $LogName=WINDOWS-SYSMON AND $EventID=1 AND $Process=regex(.*cmd\.exe.*)i NOT $ParentProcess=regex
>>_checkif sjoin #B.$PPID = #A.$CPID str_compare #B.$SystemName eq #A.$SystemName include
```

Detection – Splunk Example Analytic



Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	✓	Open in Search	Verify that lookups installed with Splunk Security Essentials is present

Enter a search

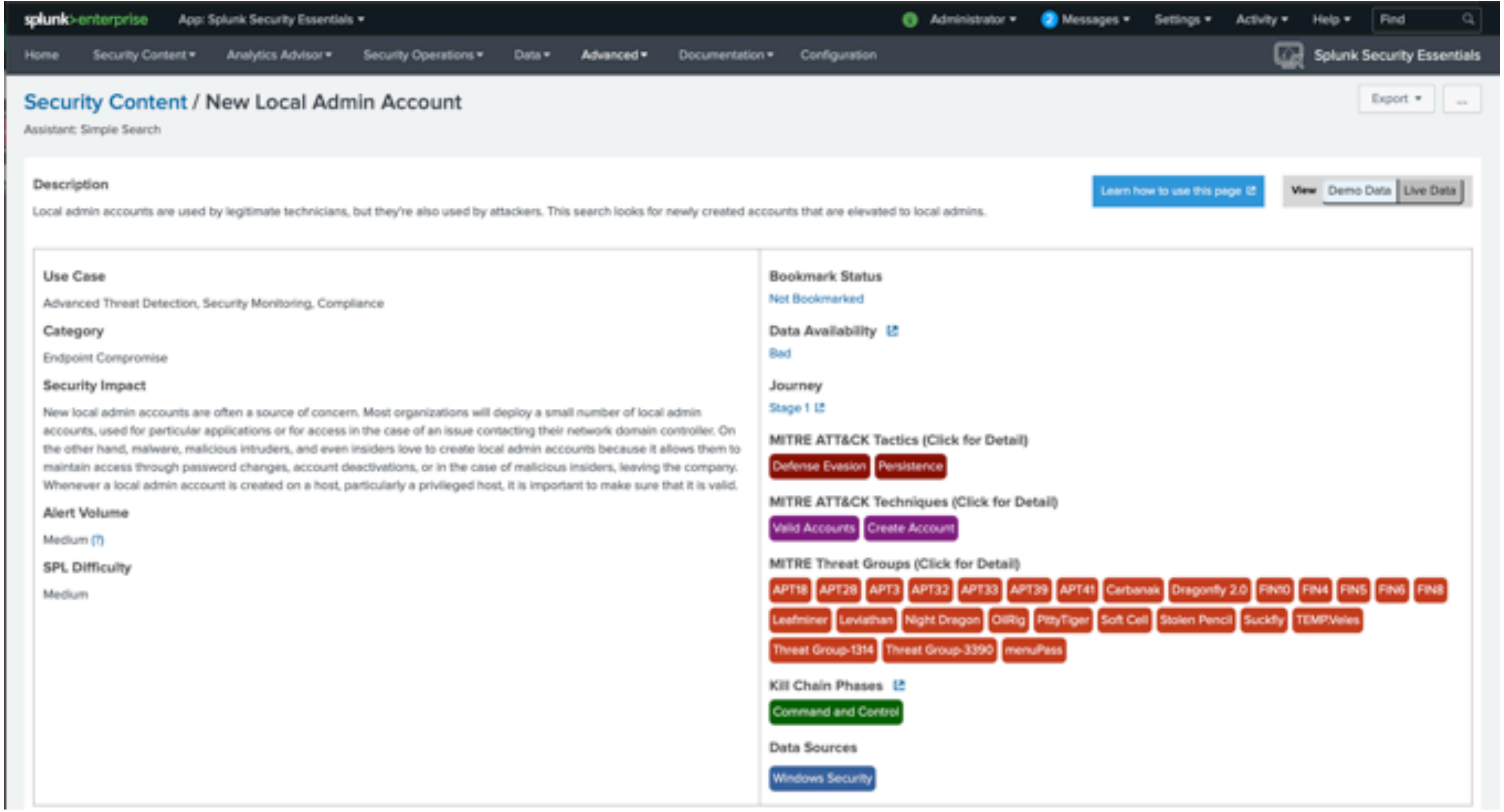
```
|`Load_Sample_Log_Data("Local Short-Lived Account")`
| rex mode=sed field=Security_ID "s/
/;/g" | makemv Security_ID delim=";"| makemv Account_Name delim=";"
| search EventCode=4720 OR (EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m connected=false
| search EventCode=4720 EventCode=4732
| table _time EventCode Security_ID Group_Name Account_Name Message
```

Last 30 days

✓ 1 result (6/9/20 12:00:00.000 AM to 7/9/20 12:00:00.000 AM)

Smart Mode

Detection – Splunk Example Analytic



Security Content / New Local Admin Account

Assistant: Simple Search

Description

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

Use Case

Advanced Threat Detection, Security Monitoring, Compliance

Category

Endpoint Compromise

Security Impact

New local admin accounts are often a source of concern. Most organizations will deploy a small number of local admin accounts, used for particular applications or for access in the case of an issue contacting their network domain controller. On the other hand, malware, malicious intruders, and even insiders love to create local admin accounts because it allows them to maintain access through password changes, account deactivations, or in the case of malicious insiders, leaving the company. Whenever a local admin account is created on a host, particularly a privileged host, it is important to make sure that it is valid.

Alert Volume

Medium (?)

SPL Difficulty

Medium

Bookmark Status

Not Bookmarked

Data Availability

Bad

Journey

Stage 1

MITRE ATT&CK Tactics (Click for Detail)

Defense Evasion Persistence

MITRE ATT&CK Techniques (Click for Detail)

Valid Accounts Create Account

MITRE Threat Groups (Click for Detail)

APT18 APT28 APT3 APT32 APT33 APT39 APT41 Carbanak Dragonfly 2.0 FIN10 FIN4 FIN5 FIN6 FIN8 Leafminer Leviathan Night Dragon OilRig PittyTiger Soft Cell Stolen Pencil Suckfly TEMP.Veles Threat Group-1314 Threat Group-3390 menuPass

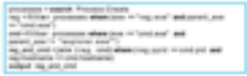
Kill Chain Phases

Command and Control

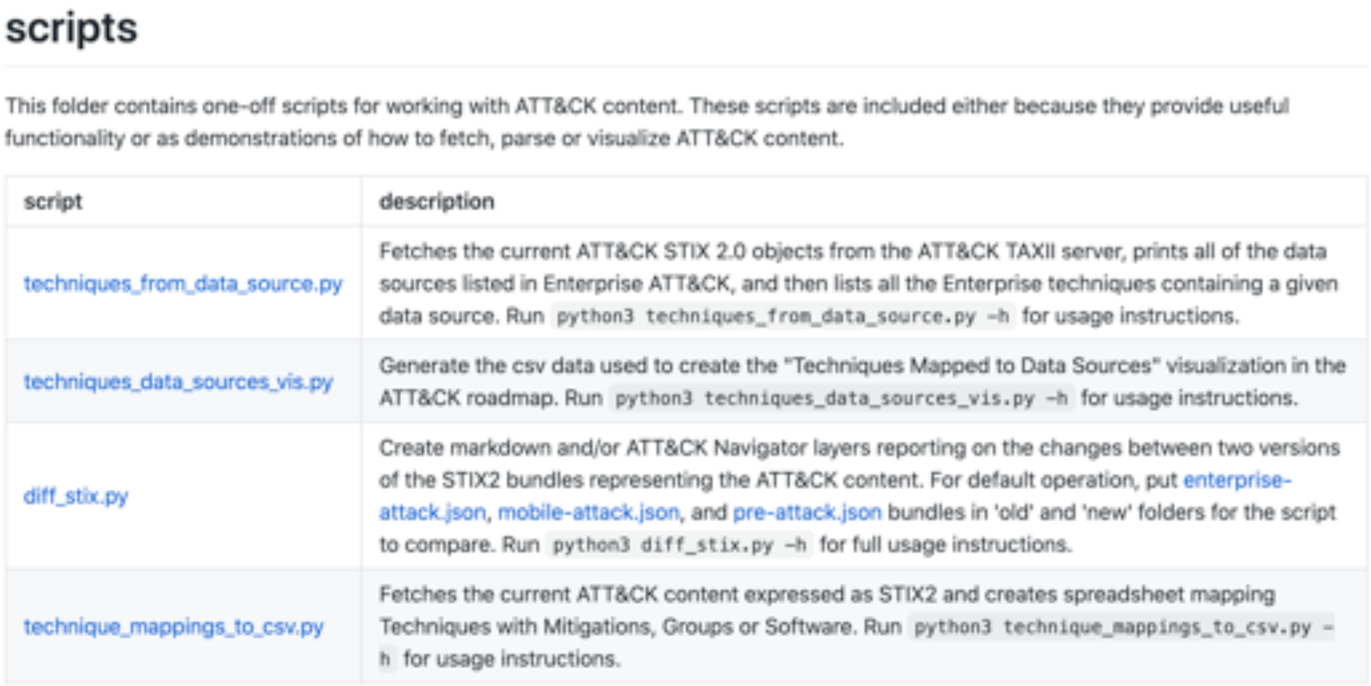
Data Sources

Windows Security

Detection – what can I detect?



- Given the datasources you have what can you detect with your SIEM?
- Which additional data can provide you better coverage?
- Are you considering:
  - Sysmon
  - OSQuery
  - Zeek
  - Command-line parameters
  - Windows Registry
  - ?!?



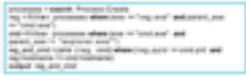
scripts

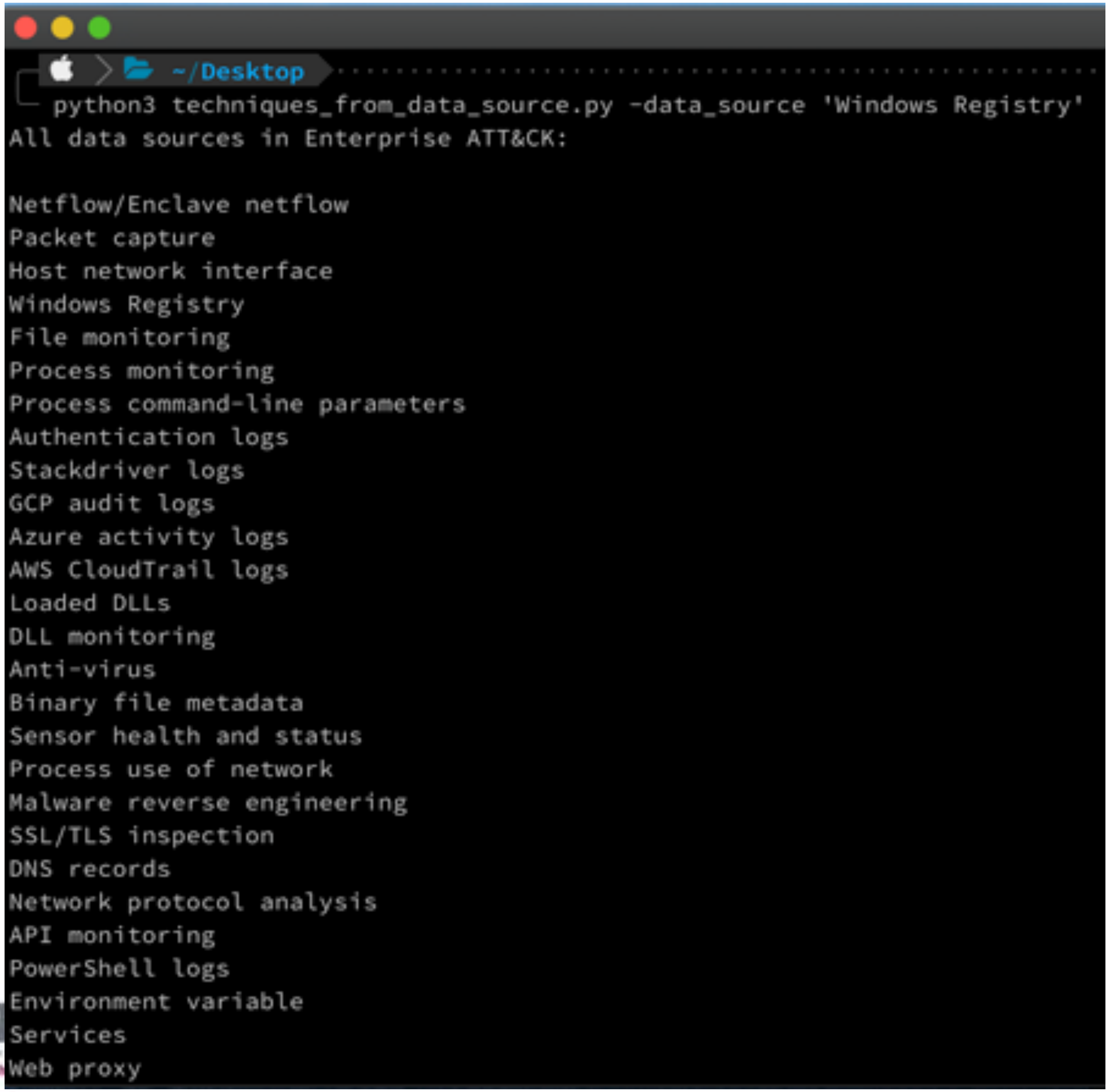
This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

script	description
techniques_from_data_source.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.
techniques_data_sources_vis.py	Generate the csv data used to create the "Techniques Mapped to Data Sources" visualization in the ATT&CK roadmap. Run `python3 techniques_data_sources_vis.py -h` for usage instructions.
diff_stix.py	Create markdown and/or ATT&CK Navigator layers reporting on the changes between two versions of the STIX2 bundles representing the ATT&CK content. For default operation, put enterprise-attack.json, mobile-attack.json, and pre-attack.json bundles in 'old' and 'new' folders for the script to compare. Run `python3 diff_stix.py -h` for full usage instructions.
technique_mappings_to_csv.py	Fetches the current ATT&CK content expressed as STIX2 and creates spreadsheet mapping Techniques with Mitigations, Groups or Software. Run `python3 technique_mappings_to_csv.py -h` for usage instructions.

- We can use MITRE script to pull data sources from ATT&CK:
  - https://github.com/mitre-attack/attack-scripts/tree/master/scripts

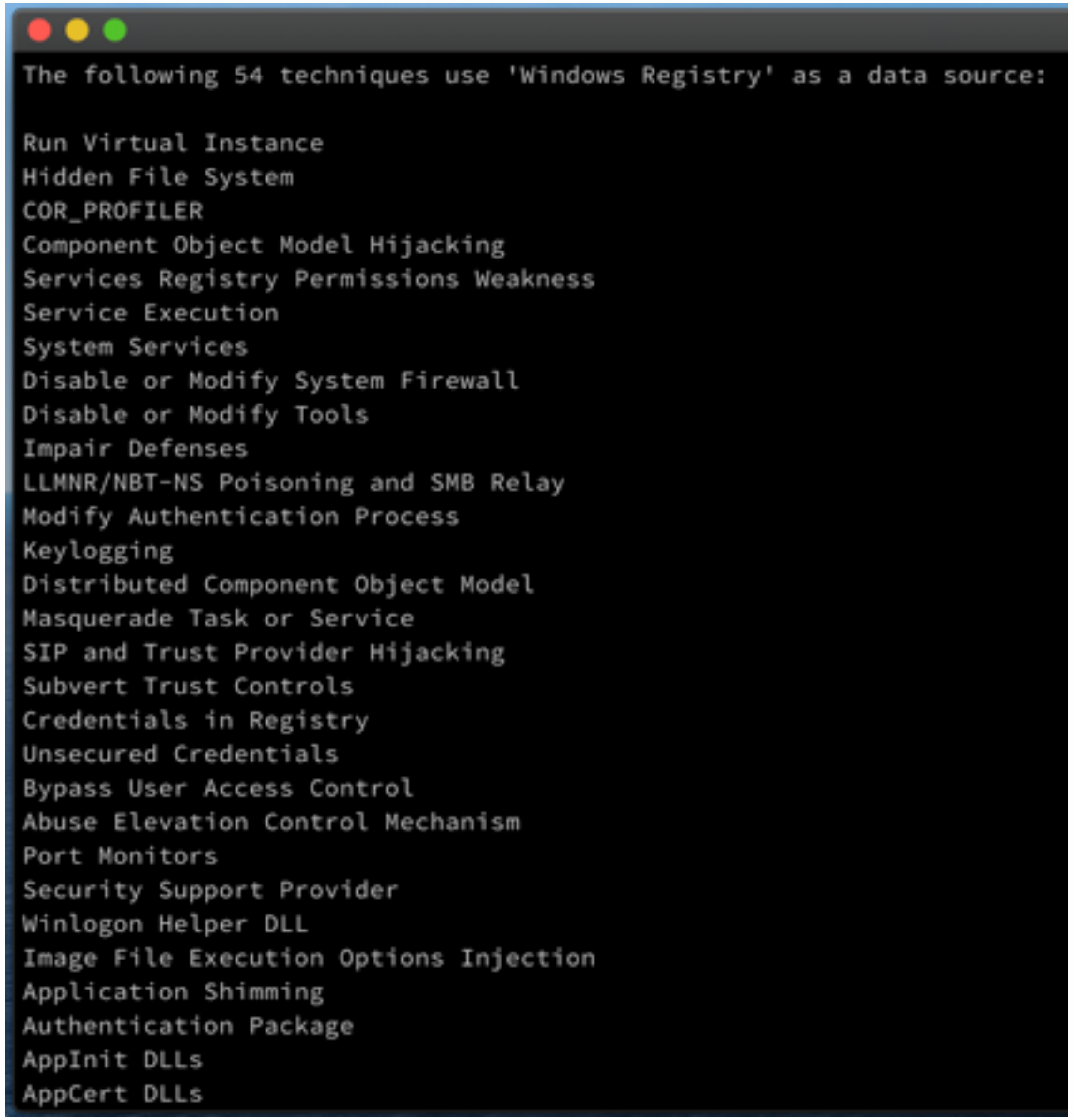
Detection – what can I detect?





```
 ~/Desktop
python3 techniques_from_data_source.py -data_source 'Windows Registry'
All data sources in Enterprise ATT&CK:

Netflow/Enclave netflow
Packet capture
Host network interface
Windows Registry
File monitoring
Process monitoring
Process command-line parameters
Authentication logs
Stackdriver logs
GCP audit logs
Azure activity logs
AWS CloudTrail logs
Loaded DLLs
DLL monitoring
Anti-virus
Binary file metadata
Sensor health and status
Process use of network
Malware reverse engineering
SSL/TLS inspection
DNS records
Network protocol analysis
API monitoring
PowerShell logs
Environment variable
Services
Web proxy
```

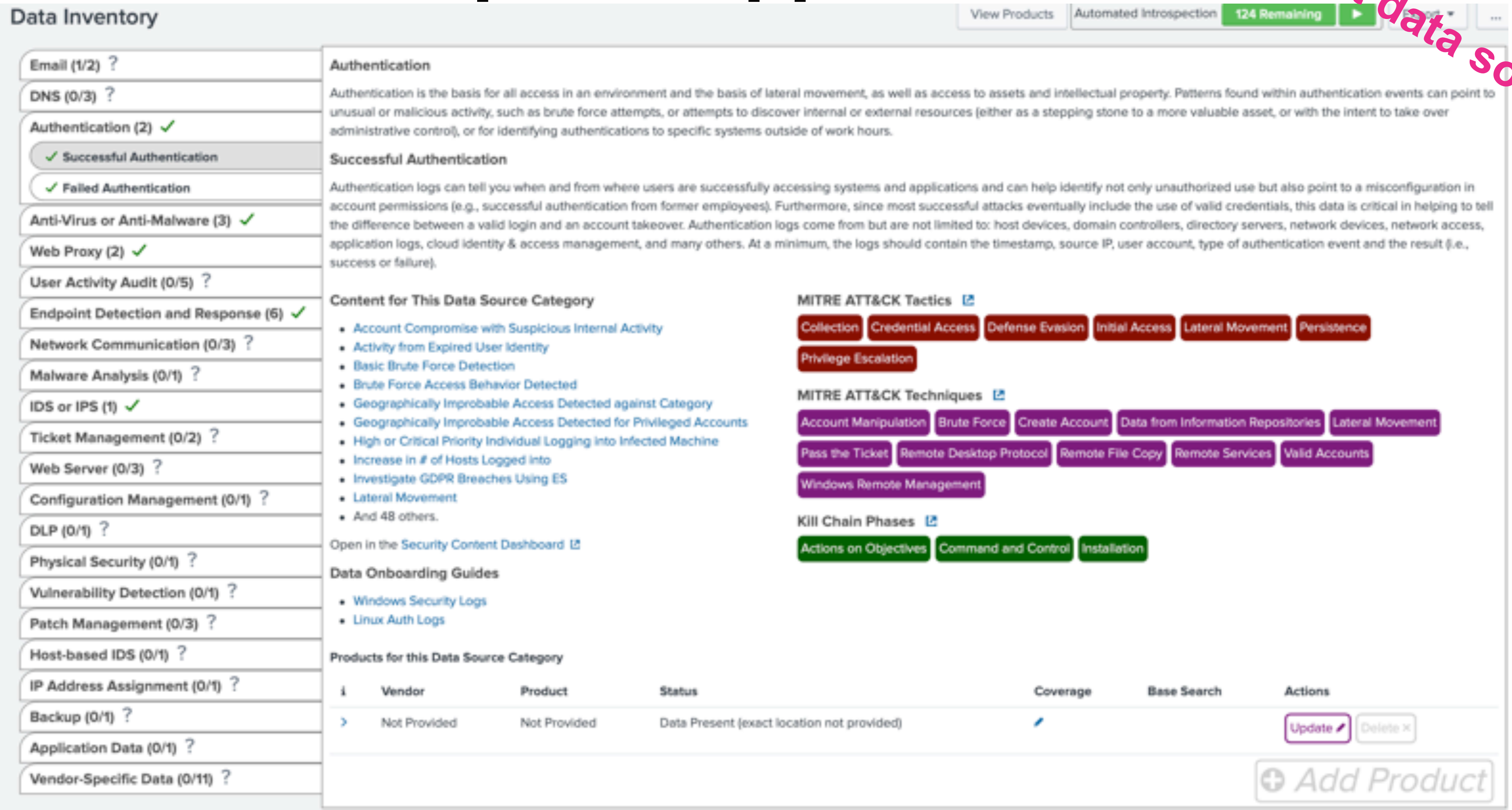


```
The following 54 techniques use 'Windows Registry' as a data source:

Run Virtual Instance
Hidden File System
COR_PROFILER
Component Object Model Hijacking
Services Registry Permissions Weakness
Service Execution
System Services
Disable or Modify System Firewall
Disable or Modify Tools
Impair Defenses
LLMNR/NBT-NS Poisoning and SMB Relay
Modify Authentication Process
Keylogging
Distributed Component Object Model
Masquerade Task or Service
SIP and Trust Provider Hijacking
Subvert Trust Controls
Credentials in Registry
Unsecured Credentials
Bypass User Access Control
Abuse Elevation Control Mechanism
Port Monitors
Security Support Provider
Winlogon Helper DLL
Image File Execution Options Injection
Application Shimming
Authentication Package
AppInit DLLs
AppCert DLLs
```

Detection – Splunk Approach

Select data sources



Data Inventory

View Products | Automated Introspection | 124 Remaining ▶ | Export ▾ | ...

- Email (1/2) ?
- DNS (0/3) ?
- Authentication (2) ✓
  - ✓ Successful Authentication
  - ✓ Failed Authentication
- Anti-Virus or Anti-Malware (3) ✓
- Web Proxy (2) ✓
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (6) ✓
- Network Communication (0/3) ?
- Malware Analysis (0/1) ?
- IDS or IPS (1) ✓
- Ticket Management (0/2) ?
- Web Server (0/3) ?
- Configuration Management (0/1) ?
- DLP (0/1) ?
- Physical Security (0/1) ?
- Vulnerability Detection (0/1) ?
- Patch Management (0/3) ?
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (0/1) ?
- Application Data (0/1) ?
- Vendor-Specific Data (0/11) ?

Authentication

Authentication is the basis for all access in an environment and the basis of lateral movement, as well as access to assets and intellectual property. Patterns found within authentication events can point to unusual or malicious activity, such as brute force attempts, or attempts to discover internal or external resources (either as a stepping stone to a more valuable asset, or with the intent to take over administrative control), or for identifying authentications to specific systems outside of work hours.

Successful Authentication

Authentication logs can tell you when and from where users are successfully accessing systems and applications and can help identify not only unauthorized use but also point to a misconfiguration in account permissions (e.g., successful authentication from former employees). Furthermore, since most successful attacks eventually include the use of valid credentials, this data is critical in helping to tell the difference between a valid login and an account takeover. Authentication logs come from but are not limited to: host devices, domain controllers, directory servers, network devices, network access, application logs, cloud identity & access management, and many others. At a minimum, the logs should contain the timestamp, source IP, user account, type of authentication event and the result (i.e., success or failure).

Content for This Data Source Category

- Account Compromise with Suspicious Internal Activity
- Activity from Expired User Identity
- Basic Brute Force Detection
- Brute Force Access Behavior Detected
- Geographically Improbable Access Detected against Category
- Geographically Improbable Access Detected for Privileged Accounts
- High or Critical Priority Individual Logging into Infected Machine
- Increase in # of Hosts Logged into
- Investigate GDPR Breaches Using ES
- Lateral Movement
- And 48 others.

Open in the Security Content Dashboard

Data Onboarding Guides

- Windows Security Logs
- Linux Auth Logs

MITRE ATT&CK Tactics

Collection | Credential Access | Defense Evasion | Initial Access | Lateral Movement | Persistence | Privilege Escalation

MITRE ATT&CK Techniques

Account Manipulation | Brute Force | Create Account | Data from Information Repositories | Lateral Movement | Pass the Ticket | Remote Desktop Protocol | Remote File Copy | Remote Services | Valid Accounts | Windows Remote Management

Kill Chain Phases

Actions on Objectives | Command and Control | Installation

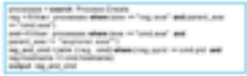
Products for this Data Source Category

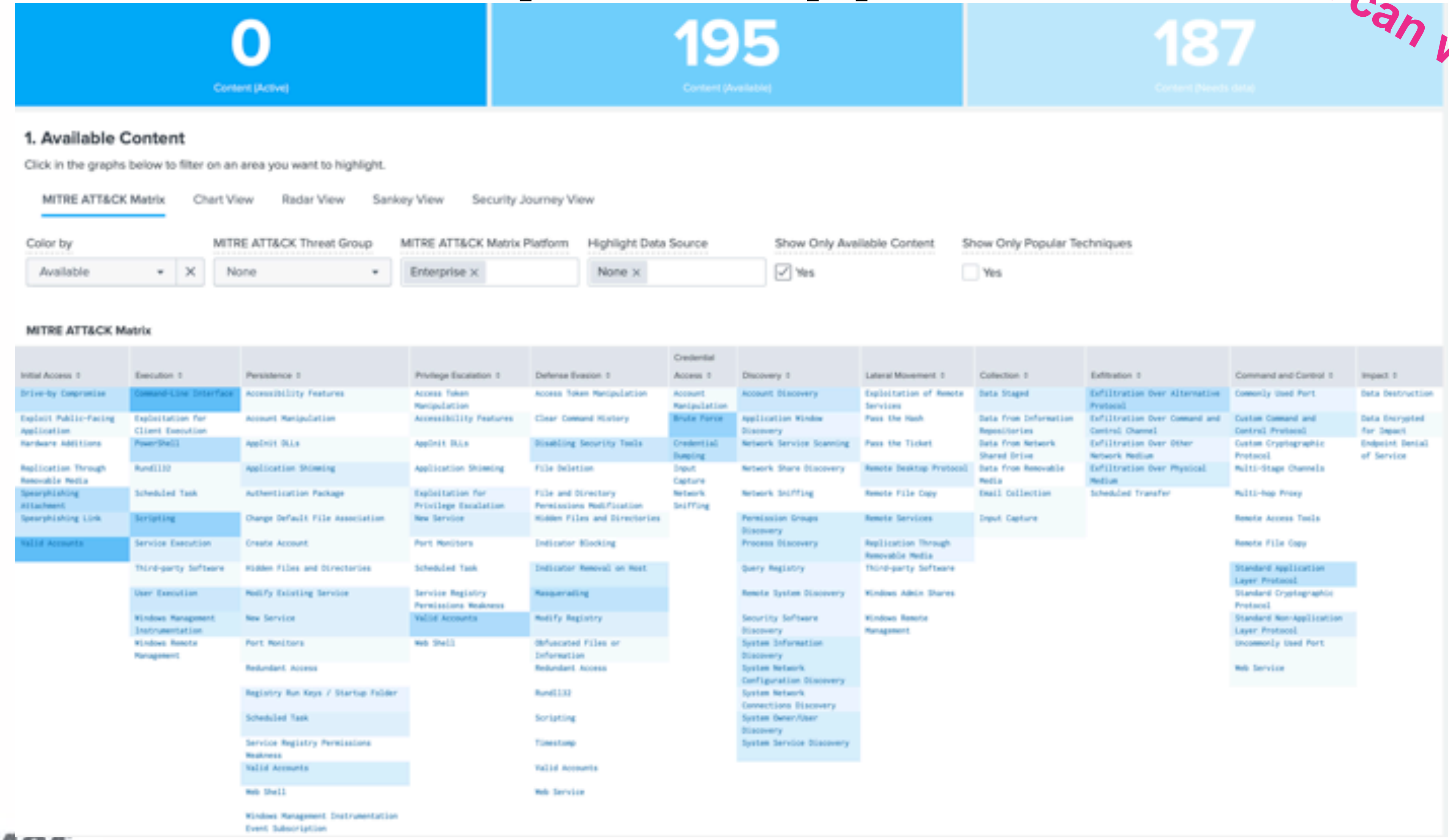
i	Vendor	Product	Status	Coverage	Base Search	Actions
›	Not Provided	Not Provided	Data Present (exact location not provided)	✎		Update ✎ Delete ×

⊕ Add Product

Detection – Splunk Approach

What can we detect?





0
Content (Active)

195
Content (Available)

187
Content (Needs data)

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

MITRE ATT&CK Matrix | Chart View | Radar View | Sankey View | Security Journey View

Color by: Available ▾ ✕

MITRE ATT&CK Threat Group: None ▾

MITRE ATT&CK Matrix Platform: Enterprise ×

Highlight Data Source: None ×

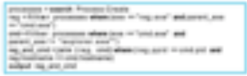
Show Only Available Content: ☑ Yes

Show Only Popular Techniques: ☐ Yes

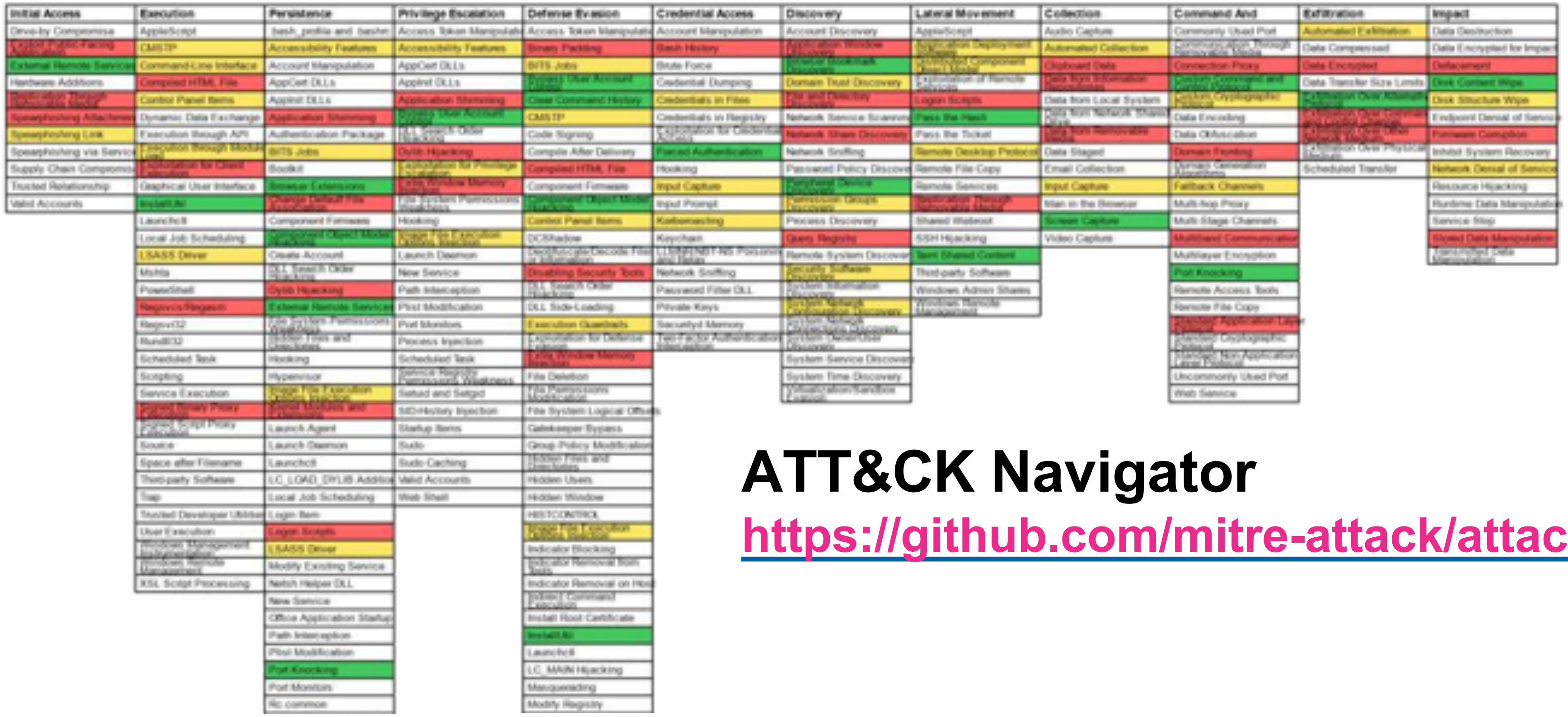
MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Exploitation of Remote Services	Data Staged	Exfiltration Over Alternative Protocol	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation	Accessibility Features	Clear Command History	Brute Force	Application Window Discovery	Pass the Hash	Data from Information Repositories	Exfiltration Over Command and Control Channel	Custom Command and Control Protocol	Data Encrypted for Impact
Hardware Additions	PowerShell	AppInit DLLs	AppInit DLLs	Disabling Security Tools	Credential Dumping	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Custom Cryptographic Protocol	Endpoint Denial of Service
Replication Through Removable Media	Rundll32	Application Shimming	Application Shimming	File Deletion	Input Capture	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Multi-Stage Channels	
Spearphishing Attachment	Scheduled Task	Authentication Package	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Remote File Copy	Email Collection	Scheduled Transfer	Multi-hop Proxy	
Spearphishing Link	Scripting	Change Default File Association	New Service	Hidden Files and Directories		Permission Groups Discovery	Remote Services	Input Capture		Remote Access Tools	
Valid Accounts	Service Execution	Create Account	Port Monitors	Indicator Blocking		Process Discovery	Replication Through Removable Media			Remote File Copy	
	Third-party Software	Hidden Files and Directories	Scheduled Task	Indicator Removal on Host		Query Registry	Third-party Software			Standard Application Layer Protocol	
	User Execution	Modify Existing Service	Service Registry Permissions Weakness	Masquerading		Remote System Discovery	Windows Admin Shares			Standard Cryptographic Protocol	
	Windows Management Instrumentation	New Service	Valid Accounts	Modify Registry		Security Software Discovery	Windows Remote Management			Standard Non-Application Layer Protocol	
	Windows Remote Management	Port Monitors	Web Shell	Obfuscated Files or Information		System Information Discovery				Uncommonly Used Port	
		Redundant Access		Redundant Access		System Network Configuration Discovery				Web Service	
		Registry Run Keys / Startup Folder		Rundll32		System Network Connections Discovery					
		Scheduled Task		Scripting		System Owner/User Discovery					
		Service Registry Permissions Weakness		Timestomp		System Service Discovery					
		Valid Accounts		Valid Accounts							
		Web Shell		Web Service							
		Windows Management Instrumentation Event Subscription									

Detection – Self Assess!



- Assess your detections against ATT&CK
  - Score: (e.g.: 1-5 based on quality or number of detections or quality)
  - 100% is a paramount, don’t aim for it.



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							

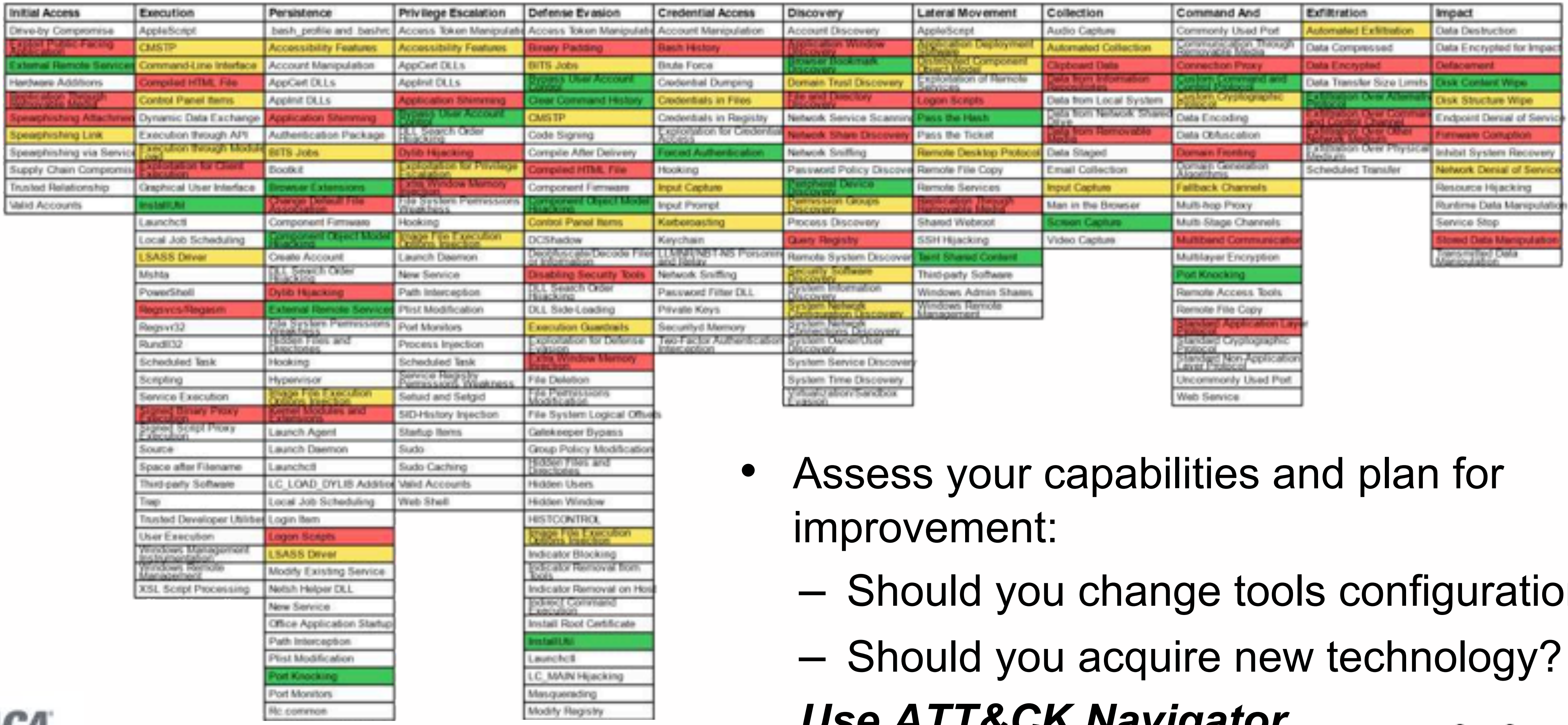
ATT&CK Navigator

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

Assess and Engineeering

- Prioritize Sources that will provide coverage for multiple tactics and threats actors
  - Windows Event Logs
    - Malware Archaeology Cheat Sheets (including ATT&CK): https://www.malwarearchaeology.com/cheat-sheets/
  - Sysmon:
    - SwiftonSecurity sysmon-config: https://github.com/SwiftOnSecurity/sysmon-config
- Any other Endpoint Detection and Response: Crowdstrike, Carbon Black etc.
- Can you mitigate anything?
  - Consider additional tools for mitigation
  - Consider policies for mitigation
- Can you automate something?

Assess and Engineeering



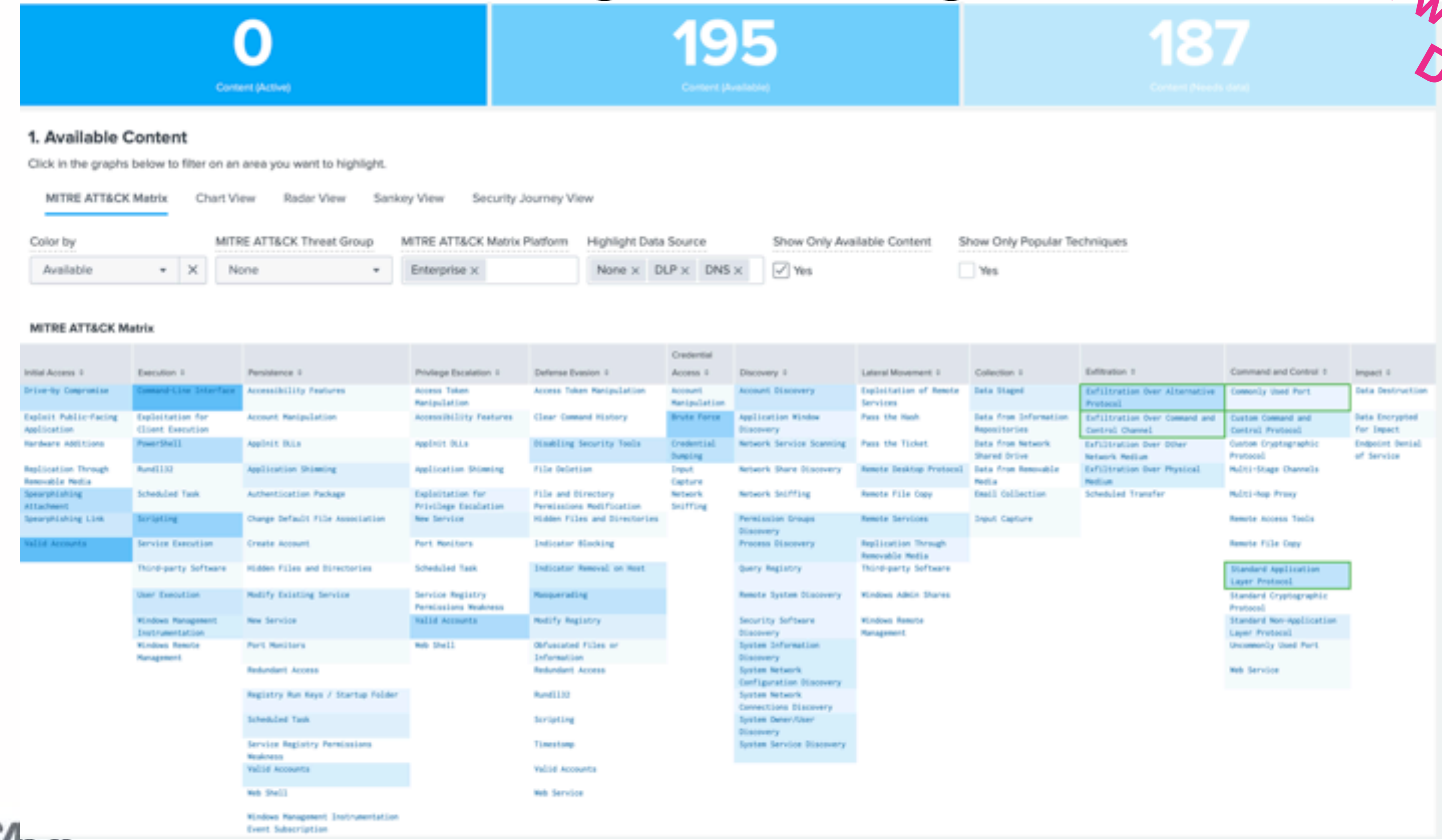
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulati	Account Manipulation	Account Discovery	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 Alternative 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 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 Servic	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 Poisoning 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 Utilitie	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							

- Assess your capabilities and plan for improvement:
  - Should you change tools configuration?
  - Should you acquire new technology?

Use ATT&CK Navigator

Assess and Engineeering

What if we add DLP and DNS?



0
Content (Active)

195
Content (Available)

187
Content (Needs data)

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

MITRE ATT&CK Matrix | Chart View | Radar View | Sankey View | Security Journey View

Color by: Available
MITRE ATT&CK Threat Group: None
MITRE ATT&CK Matrix Platform: Enterprise
Highlight Data Source: None, DLP, DNS
Show Only Available Content: ☑ Yes
Show Only Popular Techniques: □ Yes

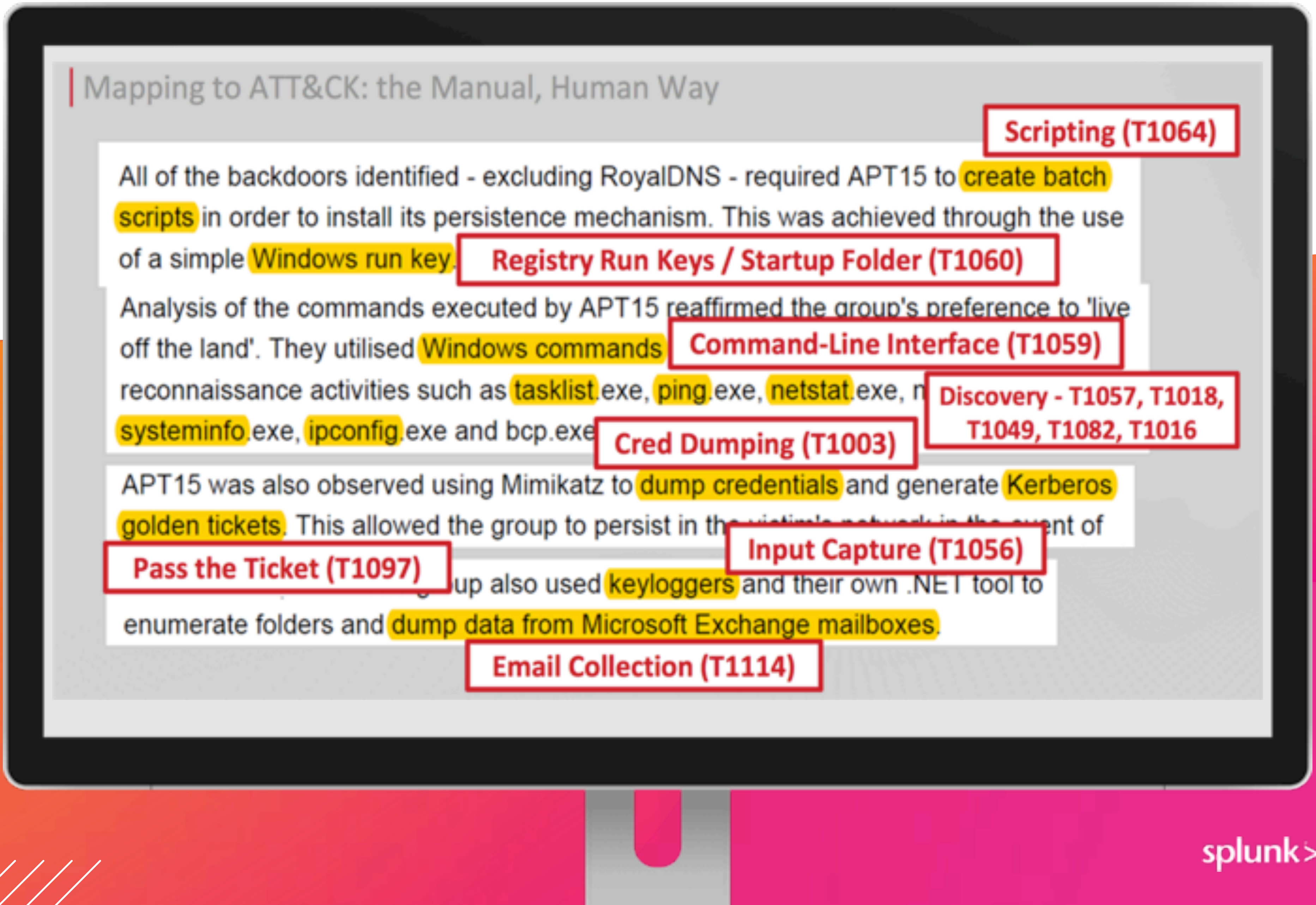
MITRE ATT&CK Matrix

Initial Access ↕	Execution ↕	Persistence ↕	Privilege Escalation ↕	Defense Evasion ↕	Credential Access ↕	Discovery ↕	Lateral Movement ↕	Collection ↕	Exfiltration ↕	Command and Control ↕	Impact ↕
Drive-by Compromise	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Exploitation of Remote Services	Data Staged	Exfiltration Over Alternative Protocol	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation	Accessibility Features	Clear Command History	Brute Force	Application Window Discovery	Pass the Hash	Data from Information Repositories	Exfiltration Over Command and Control Channel	Custom Command and Control Protocol	Data Encrypted for Impact
Hardware Additions	PowerShell	AppInit DLLs	AppInit DLLs	Disabling Security Tools	Credential Dumping	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Custom Cryptographic Protocol	Endpoint Denial of Service
Replication Through Removable Media	Rundll32	Application Shimming	Application Shimming	File Deletion	Input Capture	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Multi-Stage Channels	
Spearphishing Attachment	Scheduled Task	Authentication Package	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Remote File Copy	Email Collection	Scheduled Transfer	Multi-hop Proxy	
Spearphishing Link	Scripting	Change Default File Association	New Service	Hidden Files and Directories		Permission Groups Discovery	Remote Services	Input Capture		Remote Access Tools	
Valid Accounts	Service Execution	Create Account	Port Monitors	Indicator Blocking		Process Discovery	Replication Through Removable Media			Remote File Copy	
	Third-party Software	Hidden Files and Directories	Scheduled Task	Indicator Removal on Host		Query Registry	Third-party Software			Standard Application Layer Protocol	
	User Execution	Modify Existing Service	Service Registry Permissions Weakness	Masquerading		Remote System Discovery	Windows Admin Shares			Standard Cryptographic Protocol	
	Windows Management Instrumentation	New Service	Valid Accounts	Modify Registry		Security Software Discovery	Windows Remote Management			Standard Non-Application Layer Protocol	
	Windows Remote Management	Port Monitors	Web Shell	Obfuscated Files or Information		System Information Discovery				Uncommonly Used Port	
		Redundant Access		Redundant Access		System Network Configuration Discovery				Web Service	
		Registry Run Keys / Startup Folder		Rundll32		System Network Connections Discovery					
		Scheduled Task		Scripting		System Owner/User Discovery					
		Service Registry Permissions Weakness		Timestomp		System Service Discovery					
		Valid Accounts		Valid Accounts							
		Web Shell		Web Service							
		Windows Management Instrumentation Event Subscription									

Threat Intelligence

- We can use ATT&CK framework
  - To communicate in a **common language**
    - Across teams (e.g. Blue Team/Read Team)
    - Across Organizations
  - To compare attackers behaviour:
    - We can compare different groups
    - We can compare the same group over time
    - We can compare a group against the blue team capabilities
  - We can make recommendation to defenders:

ISACA
Rome Chapter



Mapping to ATT&CK: the Manual, Human Way

Scripting (T1064)

All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Registry Run Keys / Startup Folder (T1060)

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

Command-Line Interface (T1059)

reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, n

Discovery - T1057, T1018, T1049, T1082, T1016

systeminfo.exe, ipconfig.exe and bcp.exe

Cred Dumping (T1003)

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in th ent of

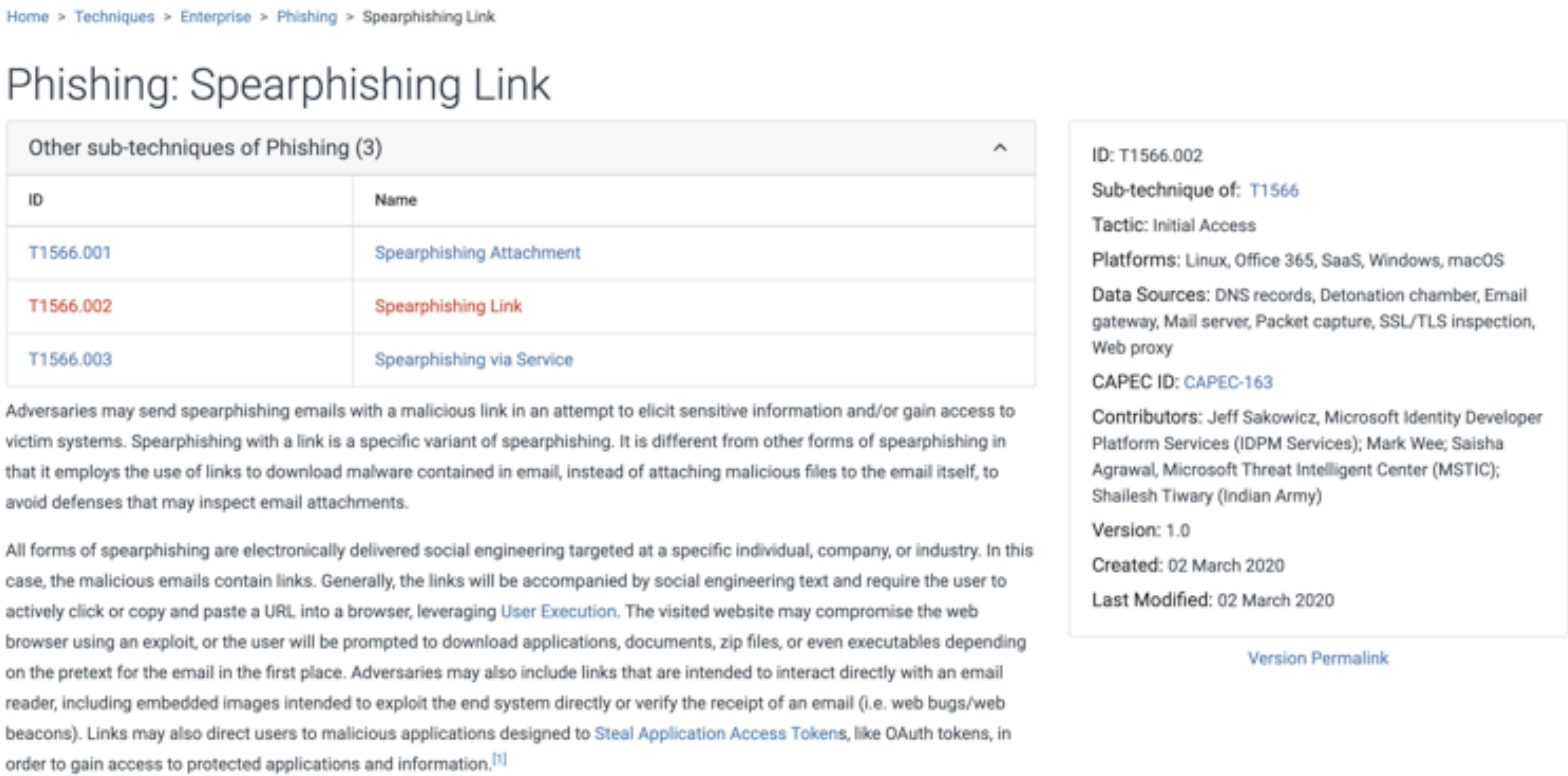
Input Capture (T1056)

Pass the Ticket (T1097)

up also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

Email Collection (T1114)

Threat Intelligence



Home > Techniques > Enterprise > Phishing > Spearphishing Link

Phishing: Spearphishing Link

Other sub-techniques of Phishing (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Adversaries may send spearphishing emails with a malicious link in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to Steal Application Access Tokens, like OAuth tokens, in order to gain access to protected applications and information.[1]

ID: T1566.002

Sub-technique of: T1566

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

Data Sources: DNS records, Detonation chamber, Email gateway, Mail server, Packet capture, SSL/TLS inspection, Web proxy

CAPEC ID: CAPEC-163

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Mark Wee; Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC); Shailesh Tiwary (Indian Army)

Version: 1.0

Created: 02 March 2020

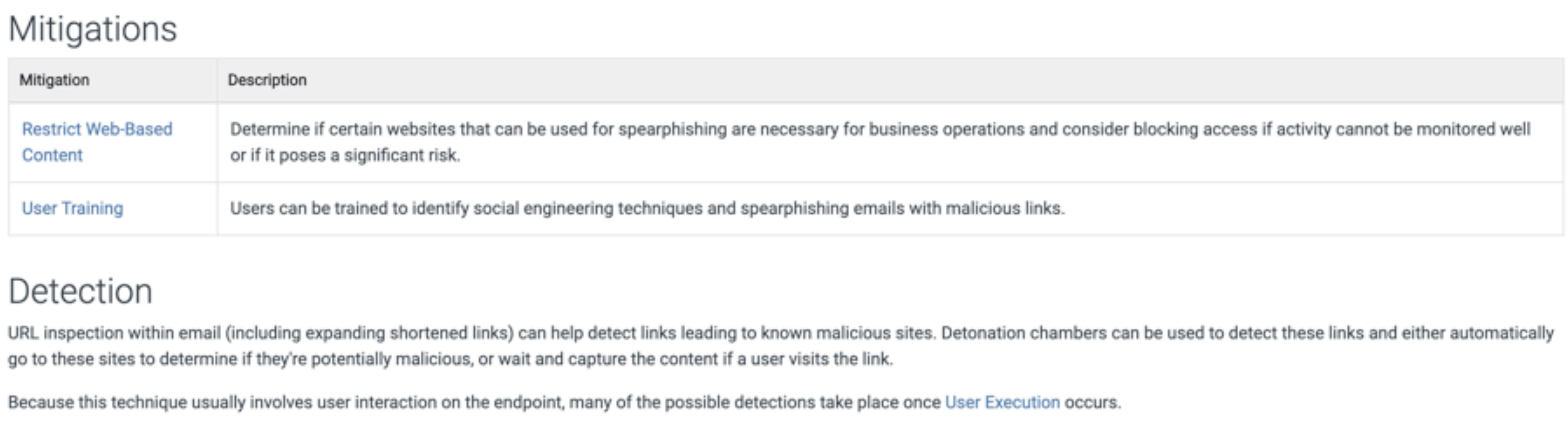
Last Modified: 02 March 2020

Version Permalink

Rome Chapter

turn data into doing

Threat Intelligence



Mitigations

Mitigation	Description
Restrict Web-Based Content	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails with malicious links.

Detection

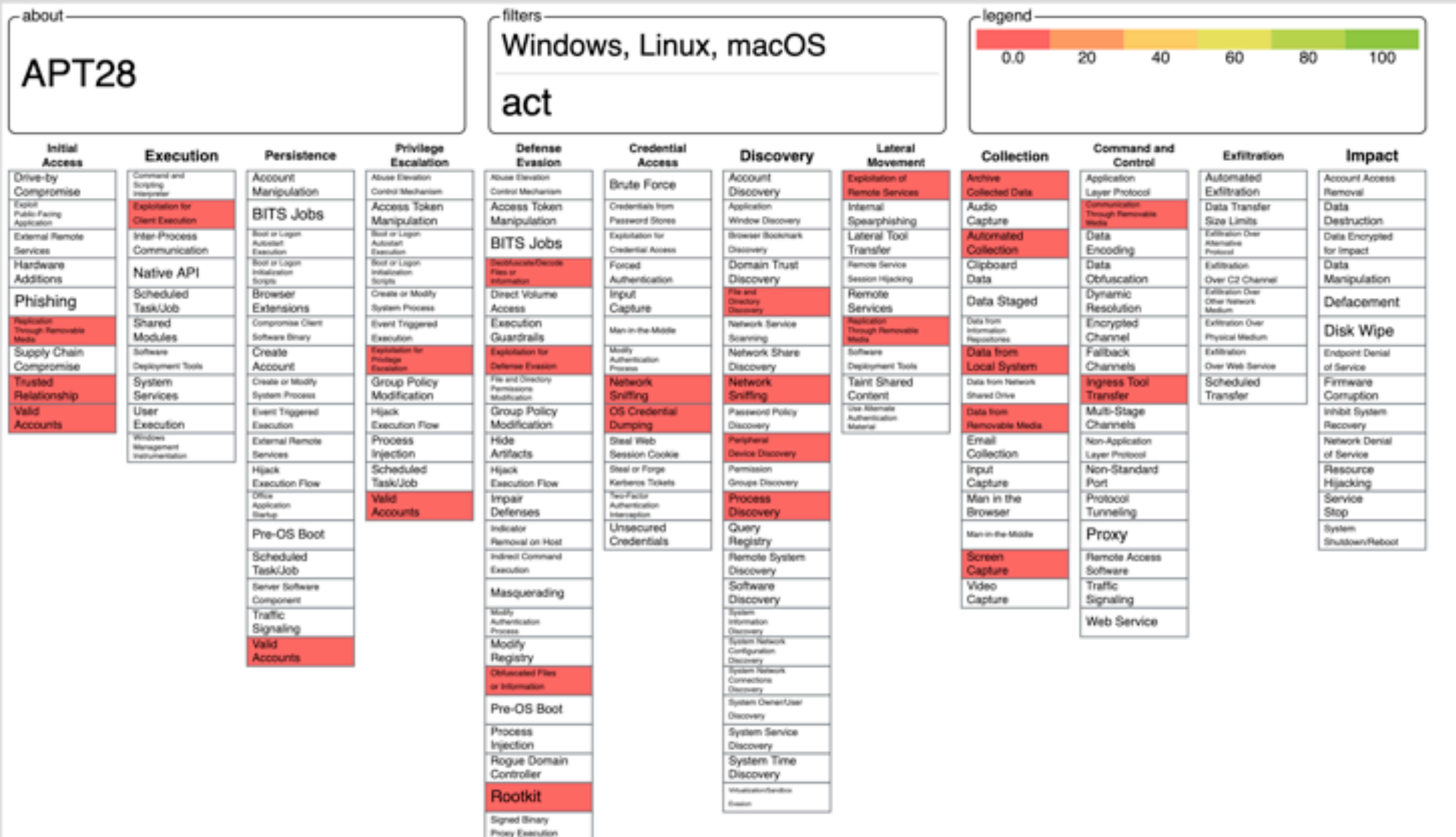
URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

Because this technique usually involves user interaction on the endpoint, many of the possible detections take place once User Execution occurs.

Let’s have a look at some techniques.

splunk> turn data into doing

ATT&CK Navigator – APT28



about

APT28

filters

Windows, Linux, macOS

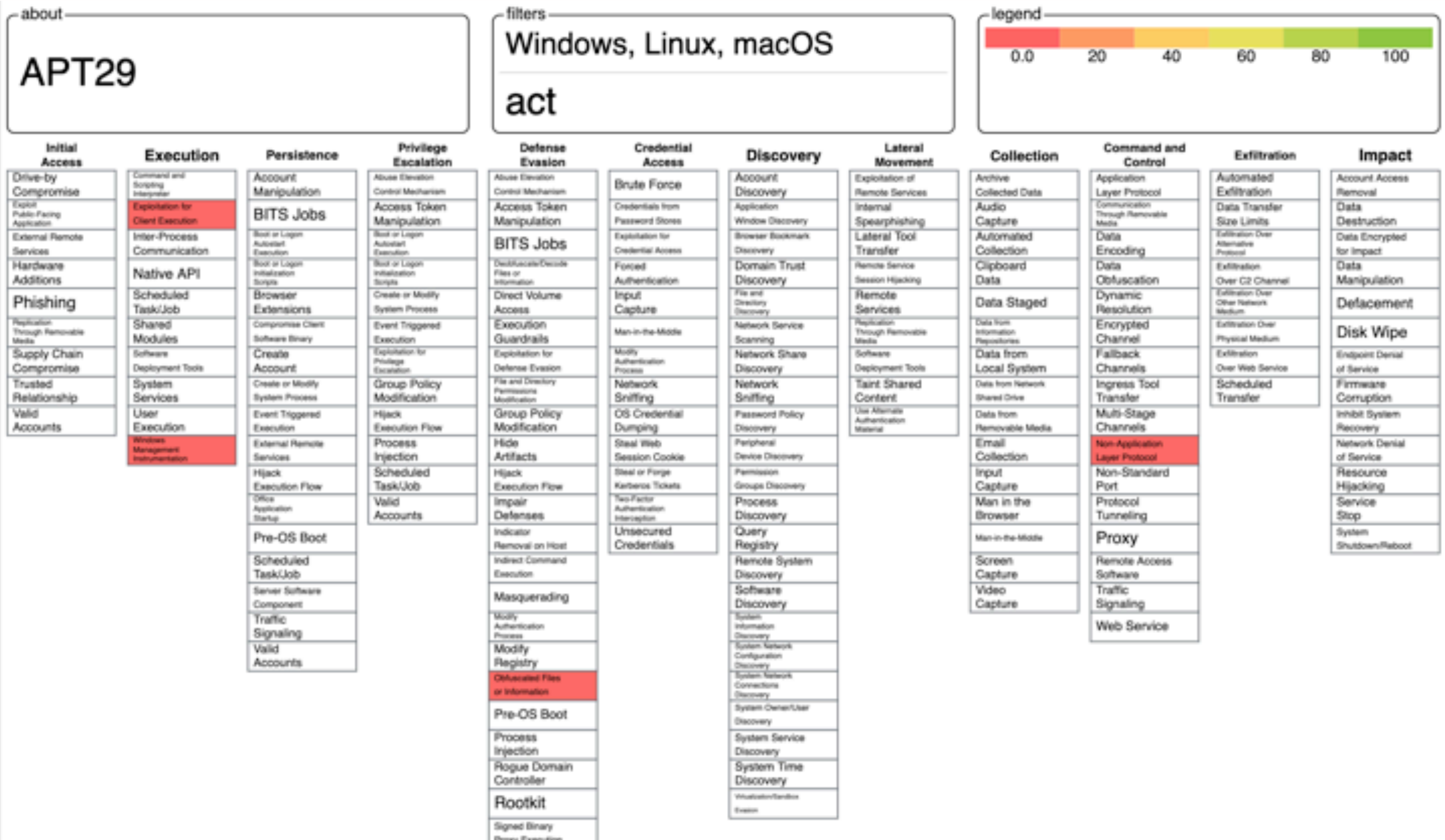
act

legend

0.0 20 40 60 80 100

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	🟥 Exploitation of Remote Services	🟥 Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	🟥 Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	🟥 Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	🟥 Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	🟥 Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	🟥 File and Directory Discovery	Remote Services	Data Staged	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
🟥 Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Network Service Scanning	🟥 Replication Through Removable Media	Data from Information Repositories	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	🟥 Exploitation for Privilege Escalation	🟥 Exploitation for Defense Evasion	Modify Authentication Process	Network Share Discovery	Software Deployment Tools	🟥 Data from Local System	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
🟥 Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	🟥 Network Sniffing	🟥 Network Sniffing	Taint Shared Content	Data from Network Shared Drive	🟥 Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
🟥 Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	🟥 OS Credential Dumping	Password Policy Discovery	Use Alternate Authentication Material	🟥 Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Web Session Cookie	🟥 Peripheral Device Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Office Application Startup	🟥 Valid Accounts	Impair Defenses	Two-Factor Authentication Interception	🟥 Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Query Registry		Man-in-the-Middle	Proxy		System Shutdown/Reboot
		Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		🟥 Screen Capture	Remote Access Software		
		Server Software Component		Masquerading		Software Discovery		Video Capture	Traffic Signaling		
		Traffic Signaling		Modify Authentication Process		System Information Discovery			Web Service		
		🟥 Valid Accounts		Modify Registry		System Network Configuration Discovery					
				🟥 Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					
				🟥 Rootkit		Virtualization/Sandbox Evasion					
				Signed Binary Proxy Execution							

ATT&CK Navigator – APT29



about

APT29

filters

Windows, Linux, macOS

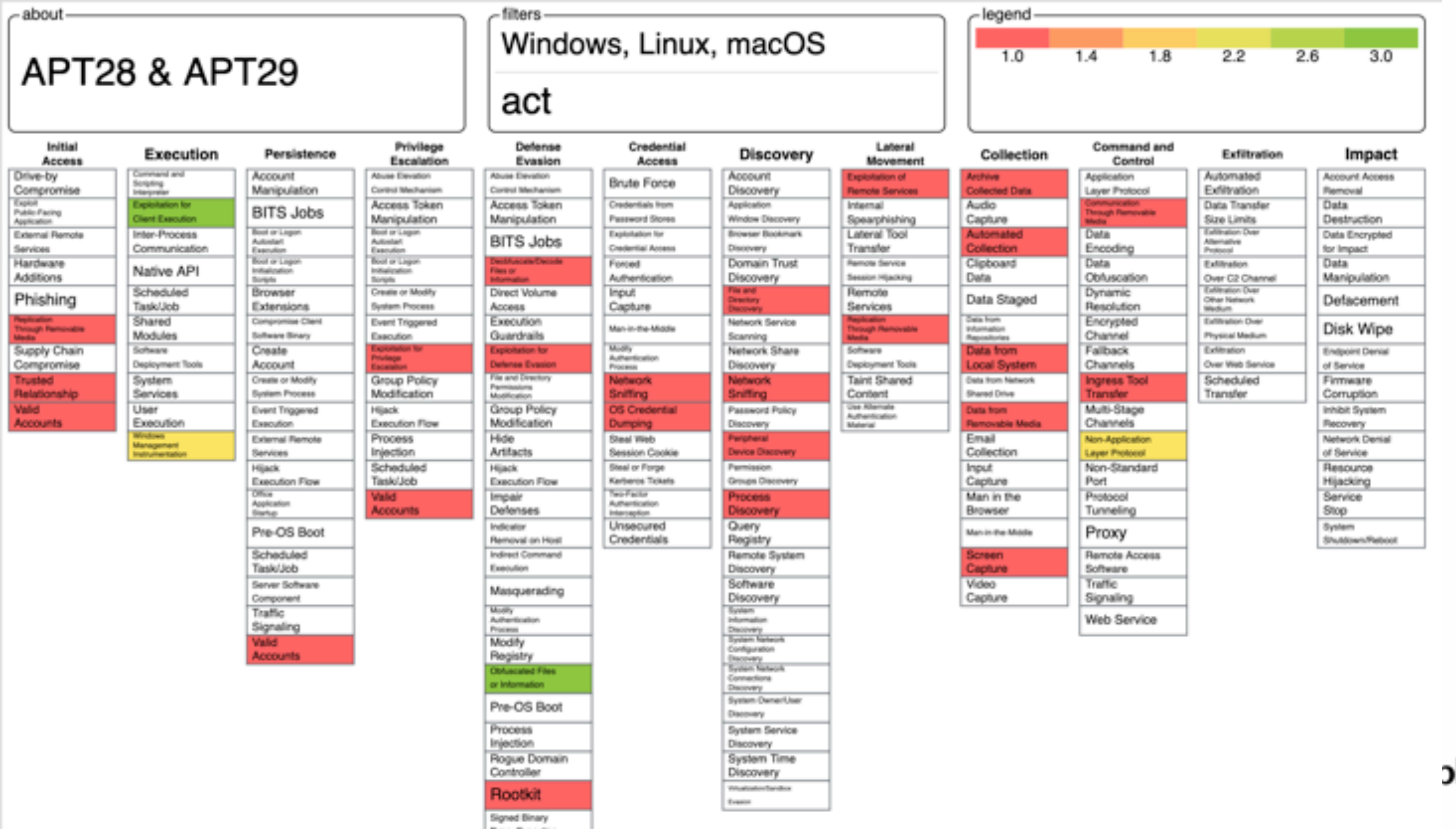
act

legend

0.0 20 40 60 80 100

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	File and Directory Discovery	Remote Services	Data Staged	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Network Service Scanning	Replication Through Removable Media	Data from Information Repositories	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	Network Share Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Password Policy Discovery	Use Alternate Authentication Material	Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Office Application Startup	Valid Accounts	Impair Defenses	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Query Registry		Man-in-the-Middle	Proxy		System Shutdown/Reboot
		Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component		Masquerading		Software Discovery		Video Capture	Traffic Signaling		
		Traffic Signaling		Modify Authentication Process		System Information Discovery			Web Service		
		Valid Accounts		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					
				Rootkit		Virtualization/Sandbox Evasion					
				Signed Binary Proxy Execution							

ATT&CK Navigator – Comparison



about: APT28 & APT29

filters: Windows, Linux, macOS

act

legend: 1.0 | 1.4 | 1.8 | 2.2 | 2.6 | 3.0

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	File and Directory Discovery	Remote Services	Data Staged	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Network Service Scanning	Replication Through Removable Media	Data from Information Repositories	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	Network Share Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Password Policy Discovery	Use Alternate Authentication Material	Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Office Application Startup	Valid Accounts	Impair Defenses	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Query Registry		Man-in-the-Middle	Proxy		System Shutdown/Reboot
		Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component		Masquerading		Software Discovery		Video Capture	Traffic Signaling		
		Traffic Signaling		Modify Authentication Process		System Information Discovery			Web Service		
		Valid Accounts		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					
				Rootkit		Virtualization/Sandbox Evasion					
				Signed Binary							

Let’s have a look at the ATT&CK navigator.

Adversary Emulation - Challenges

Build

Building a lab infrastructure

Simulate

Simulate attacks

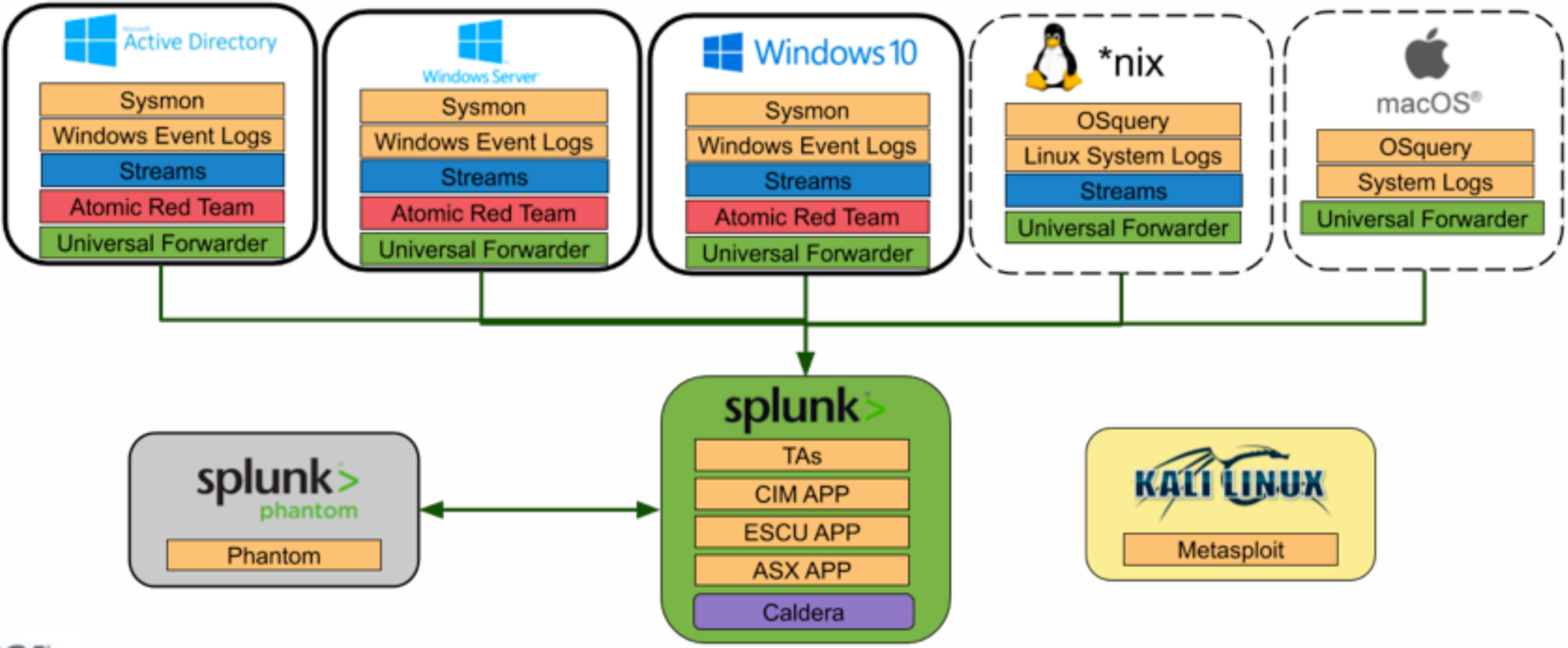
Test Detections

Write and test detection queries

Adversary Emulation -Attack Range

- Multiple tools can be used to test the detections we are building.
- Here few examples (most commonly used):
  - CALDERA: https://github.com/mitre/caldera
  - Red Team Automation: https://github.com/endgameinc/RTA
  - Metta: https://github.com/uber-common/metta
  - Red Canary’s Atomic Red Team: https://atomicredteam.io/
  - SPLUNK ATT&CK RANGE: https://github.com/splunk/attack_range

Adversary Emulation - Attack Range



Active Directory
- Sysmon
- Windows Event Logs
- Streams
- Atomic Red Team
- Universal Forwarder

Windows Server
- Sysmon
- Windows Event Logs
- Streams
- Atomic Red Team
- Universal Forwarder

Windows 10
- Sysmon
- Windows Event Logs
- Streams
- Atomic Red Team
- Universal Forwarder

*nix
- OSquery
- Linux System Logs
- Streams
- Universal Forwarder

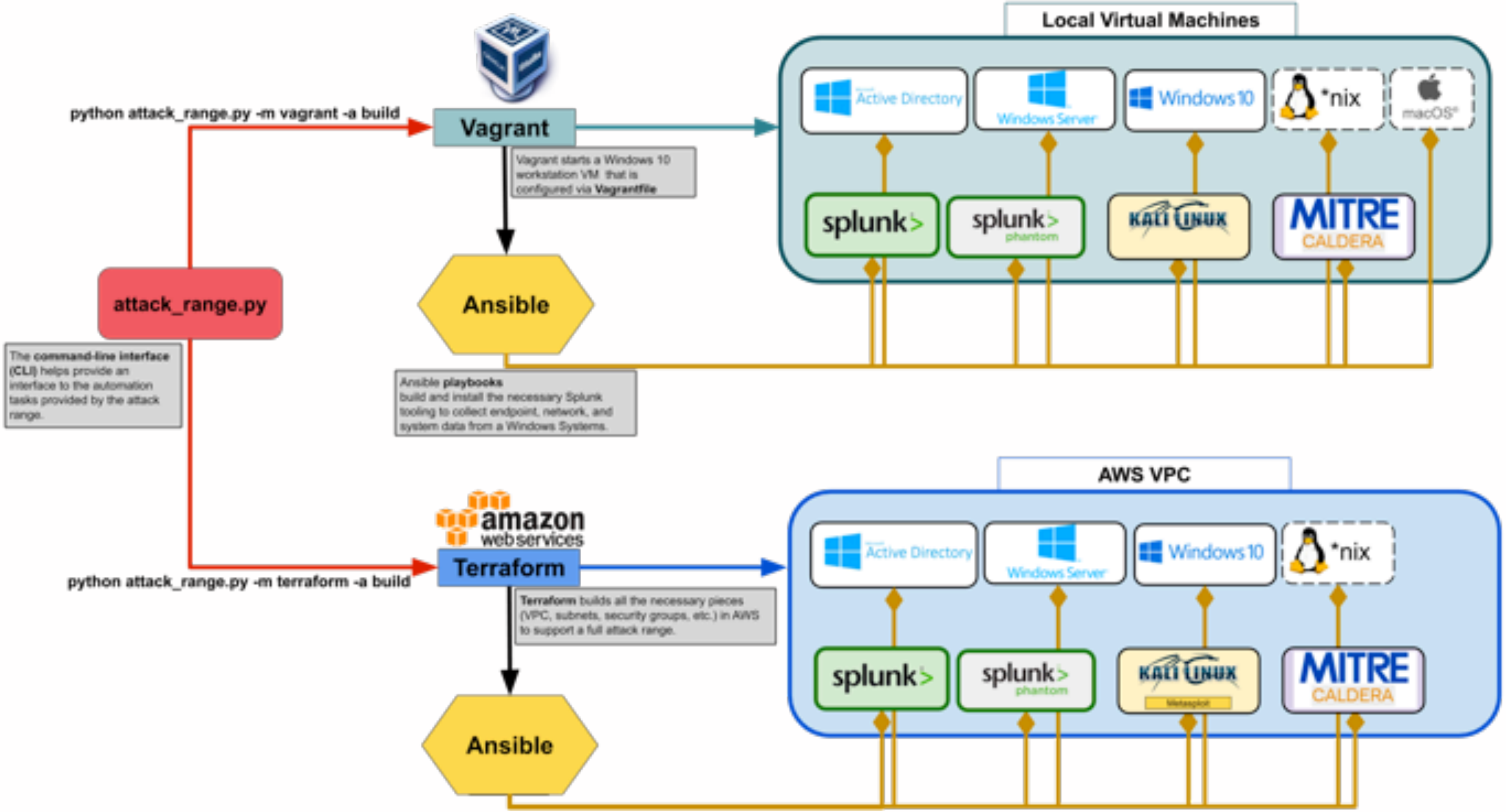
macOS®
- OSquery
- System Logs
- Universal Forwarder

splunk>
- TAs
- CIM APP
- ESCU APP
- ASX APP
- Caldera

splunk> phantom
- Phantom

KALI LINUX
- Metasploit

Attack Range Architecture



python attack_range.py -m vagrant -a build

Vagrant starts a Windows 10 workstation VM that is configured via **Vagrantfile**

The **command-line interface (CLI)** helps provide an interface to the automation tasks provided by the attack range.

Ansible **playbooks** build and install the necessary Splunk tooling to collect endpoint, network, and system data from a Windows Systems.

python attack_range.py -m terraform -a build

Terraform builds all the necessary pieces (VPC, subnets, security groups, etc.) in AWS to support a full attack range.

ISACA
Rome Chapter

splunk> turn data into doing

Attack Range Commands

Build

Automated building process with commands: **Build, destroy, stop, resume**

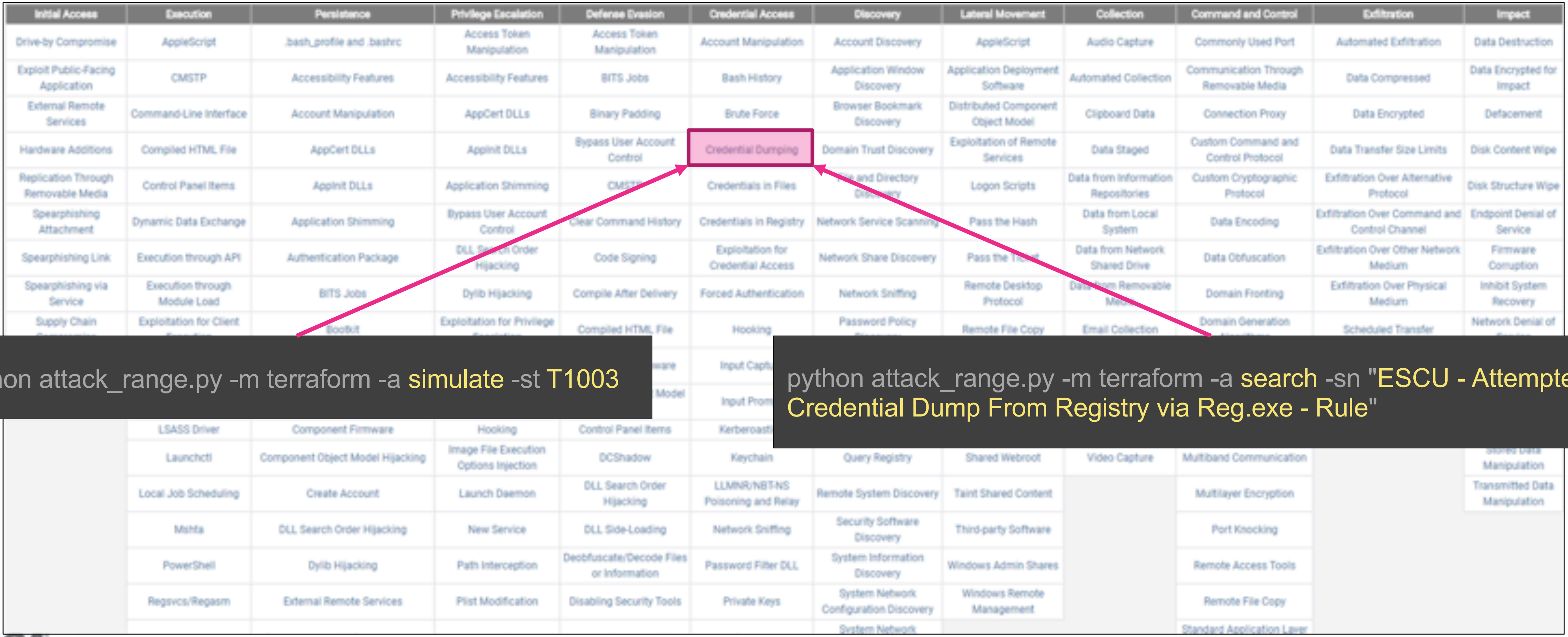
Simulate

Simulate attacks with Atomic Red Team with command: **simulate**

Test Detections

Run Splunk queries with the command: **search**

Adversary Emulation - ATT&CK

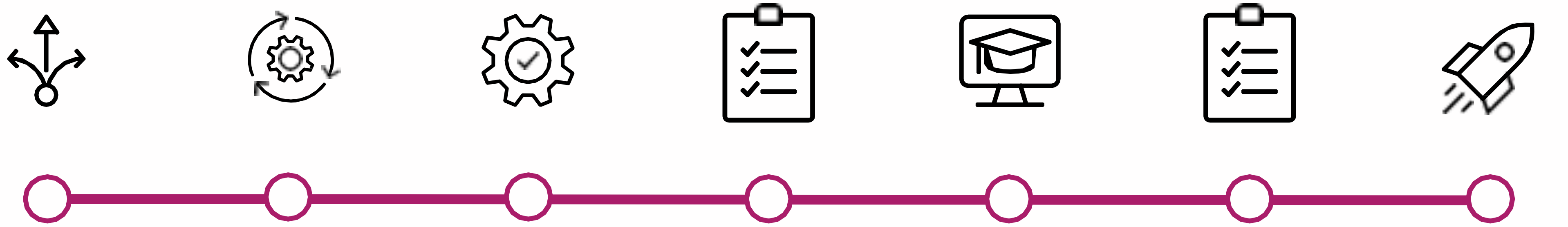


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	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	Binary Padding	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 Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	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 Network Shared Drive	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 from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain	Exploitation for Client	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy	Remote File Copy	Email Collection	Domain Generation	Scheduled Transfer	Network Denial of
				ware	Input Captu						
				Model	Input Prom						
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasti						
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
						System Network			Standard Application Layer		

```
python attack_range.py -m terraform -a simulate -st T1003
```

```
python attack_range.py -m terraform -a search -sn "ESCU - Attempted Credential Dump From Registry via Reg.exe - Rule"
```

Adversary Emulation - CI/CD



Commit detection

Convert detection

Package detection

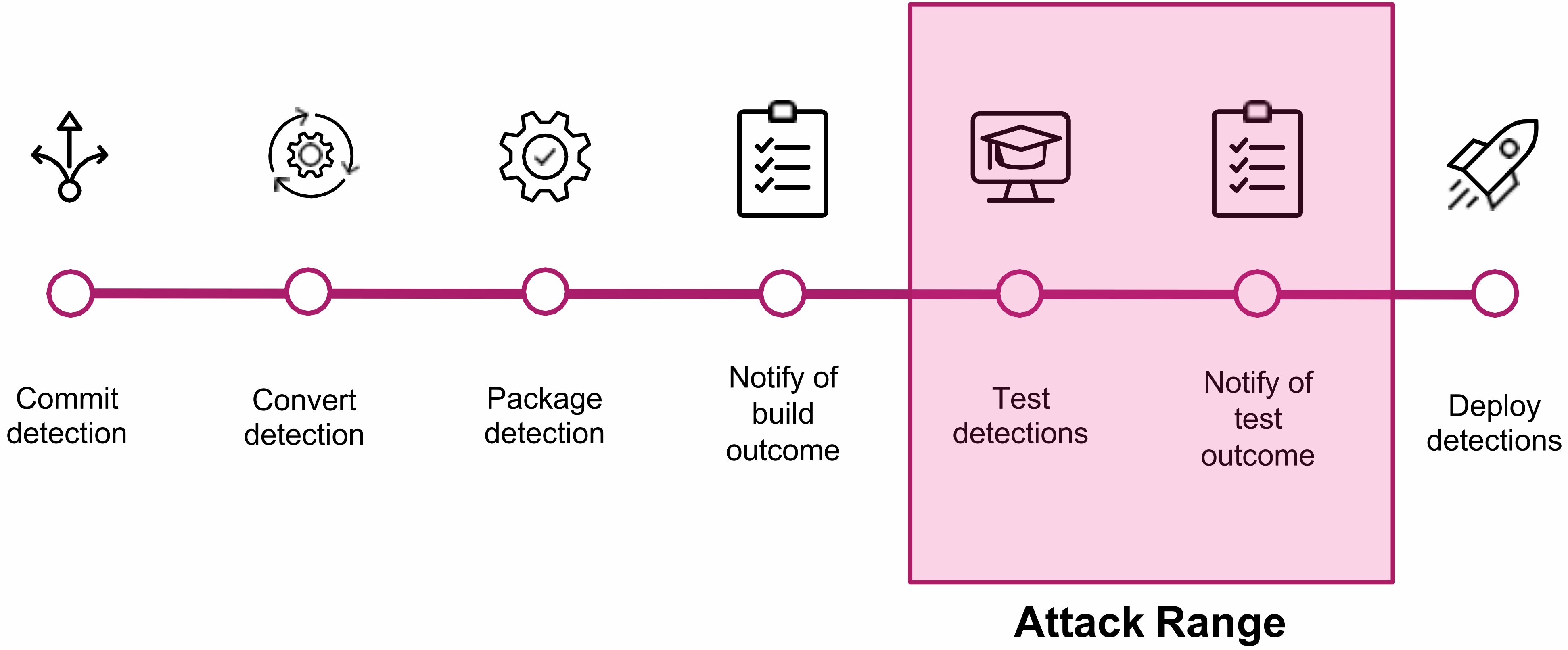
Notify of build outcome

Test detections

Notify of test outcome

Deploy detections

Adversary Emulation - CI/CD



Commit detection

Convert detection

Package detection

Notify of build outcome

Test detections

Notify of test outcome

Deploy detections

Attack Range

Resources

Attack Range: https://github.com/splunk/attack_range

Attack Range Video: https://www.youtube.com/watch?v=xIbln7OQ-Ak

Attack Range White Paper: https://www.splunk.com/en_us/form/using-splunk-attack-range-to-simulate-and-collect-attack-data.html

Mitre ATT&CK Matrix: https://attack.mitre.org/

Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

Good, Bad & Ugly for ATT&CK

Example of APT10 Group

splunk> turn data into doing™

The Good, Bad & Ugly for ATT&CK

Collection of "techniques, tactics, and procedures" manually curated from APT reports.

- Identify where you have gaps in knowledge
- Compare adversaries to each other
- Compare adversary behavior to defenses

When is MITRE ATT&CK useful?

- Tracking adversaries at a detailed level
- Sharing TTPs with defenders in a common taxonomy
- Measuring your defenses against your adversaries capabilities

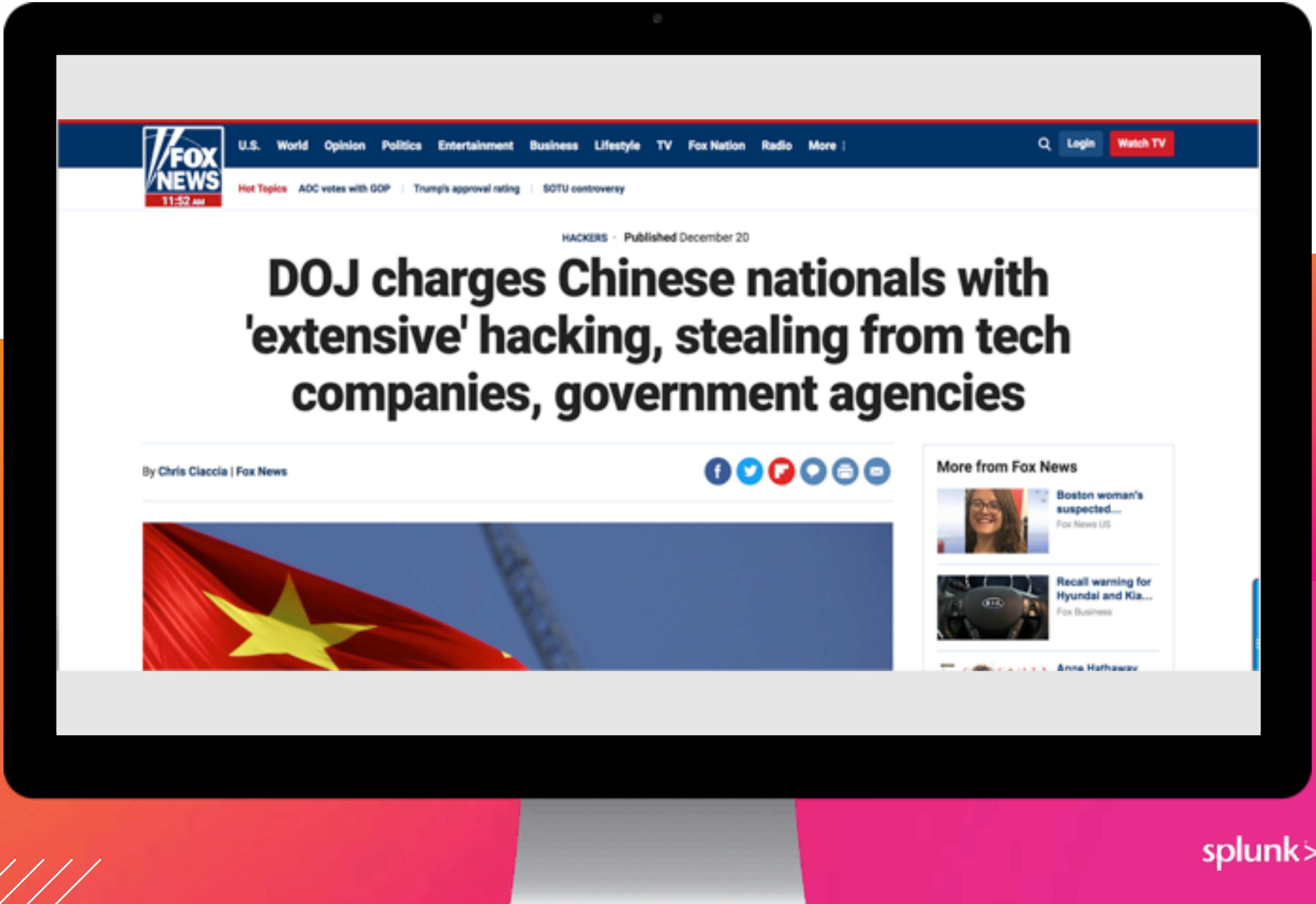
What are the limitations?

- It has inherent biases of being based on APT reporting
- It is tactical NOT strategic
- Mapping Techniques/Tactics can be… hard
- It doesn't cover everything

Example from APT10 Group

splunk> turn data into doing™

ATT&CK™



HACKERS · Published December 20

DOJ charges Chinese nationals with 'extensive' hacking, stealing from tech companies, government agencies

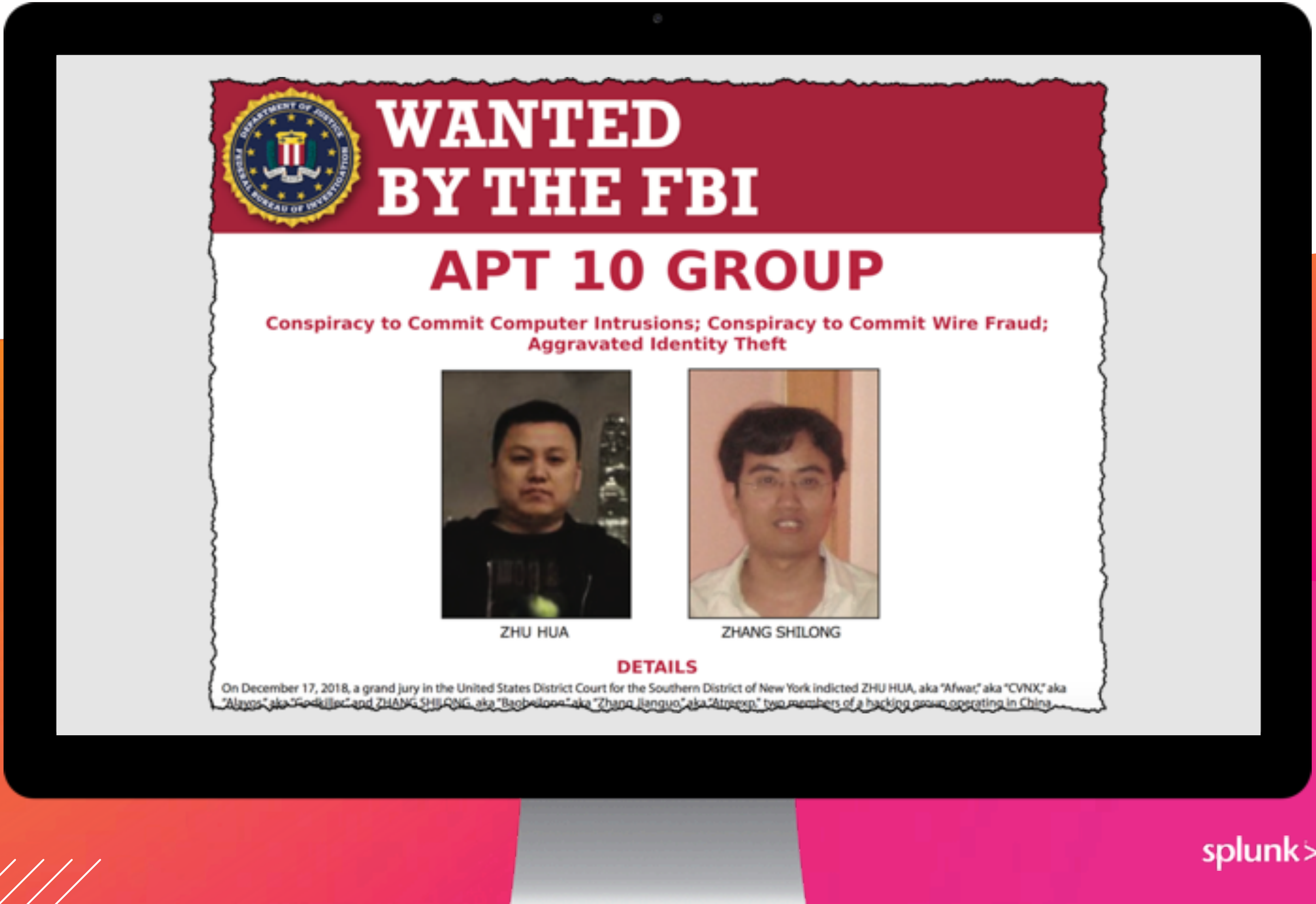
By Chris Ciaccia | Fox News

More from Fox News

Boston woman's suspected...
Fox News US

Recall warning for Hyundai and Kia...
Fox Business

Anne Hathaway



WANTED BY THE FBI

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

ZHU HUA

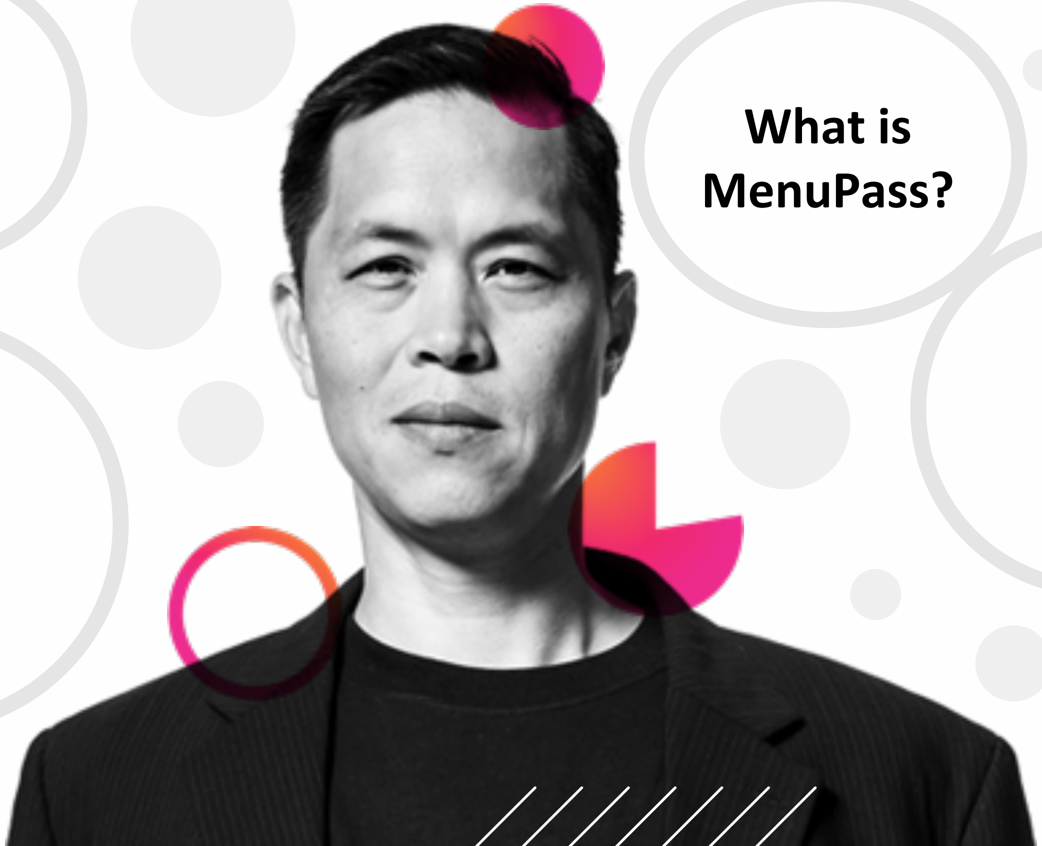
ZHANG SHILONG

DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Afwar," aka "CVNX," aka "Alayos," aka "Godkiller," and ZHANG SHILONG, aka "Baobeilong," aka "Zhang Jianguo," aka "Atreexp," two members of a hacking group operating in China

Who is APT 10?

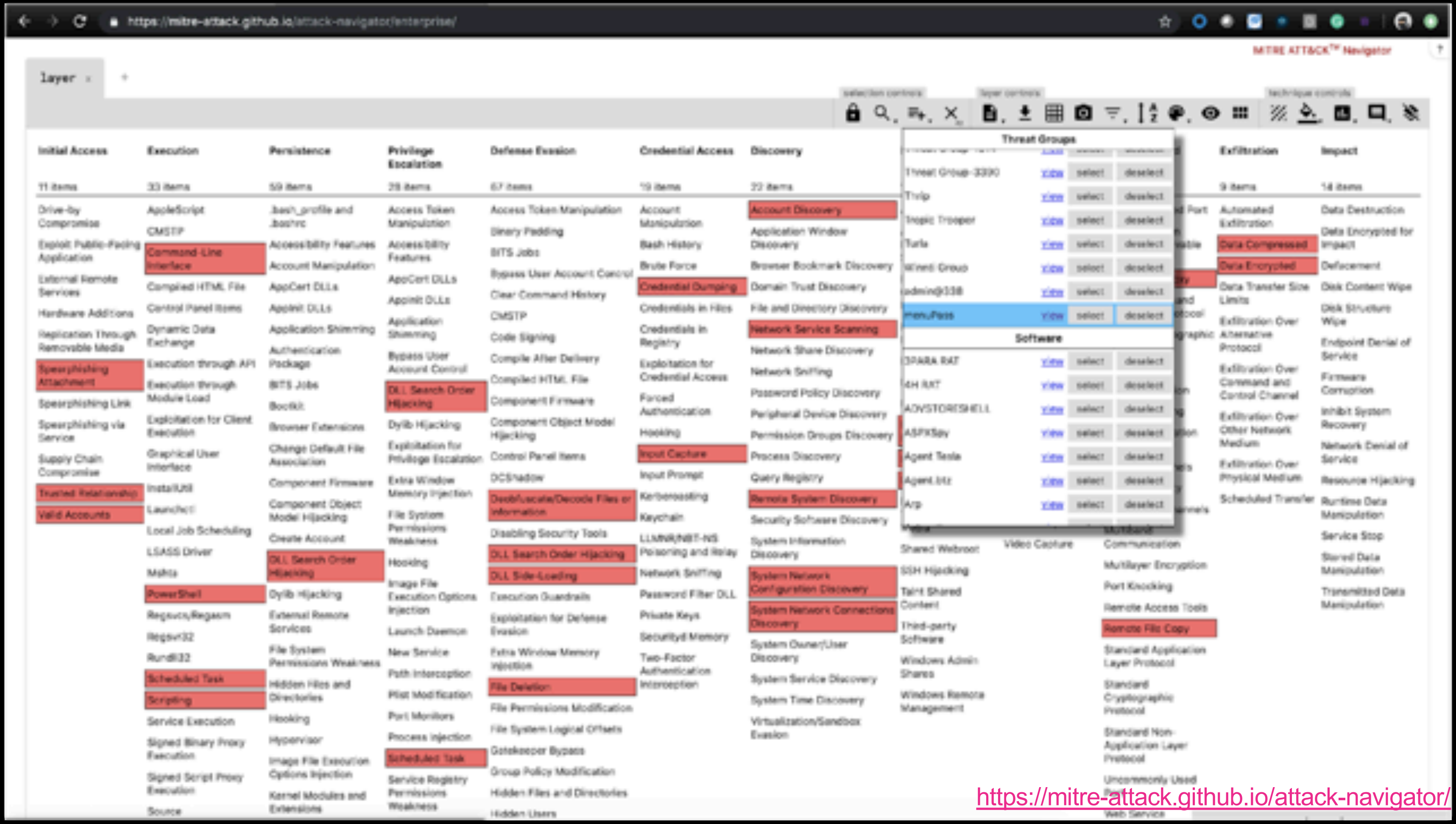
Am I a target?



What is MenuPass?

How do I defend my org?

One screen. All the answers



https://mitre-attack.github.io/attack-navigator/enterprise/

MITRE ATT&CK™ Navigator

layer

selection controls · layer controls · technique controls

Initial Access (11 items)
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution (33 items)
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source

Persistence (59 items)
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions

Privilege Escalation (28 items)
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Plist Modification
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness

Defense Evasion (67 items)
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users

Credential Access (19 items)
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery (22 items)
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

- Video Capture

- Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration (9 items)
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact (14 items)
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

Threat Groups

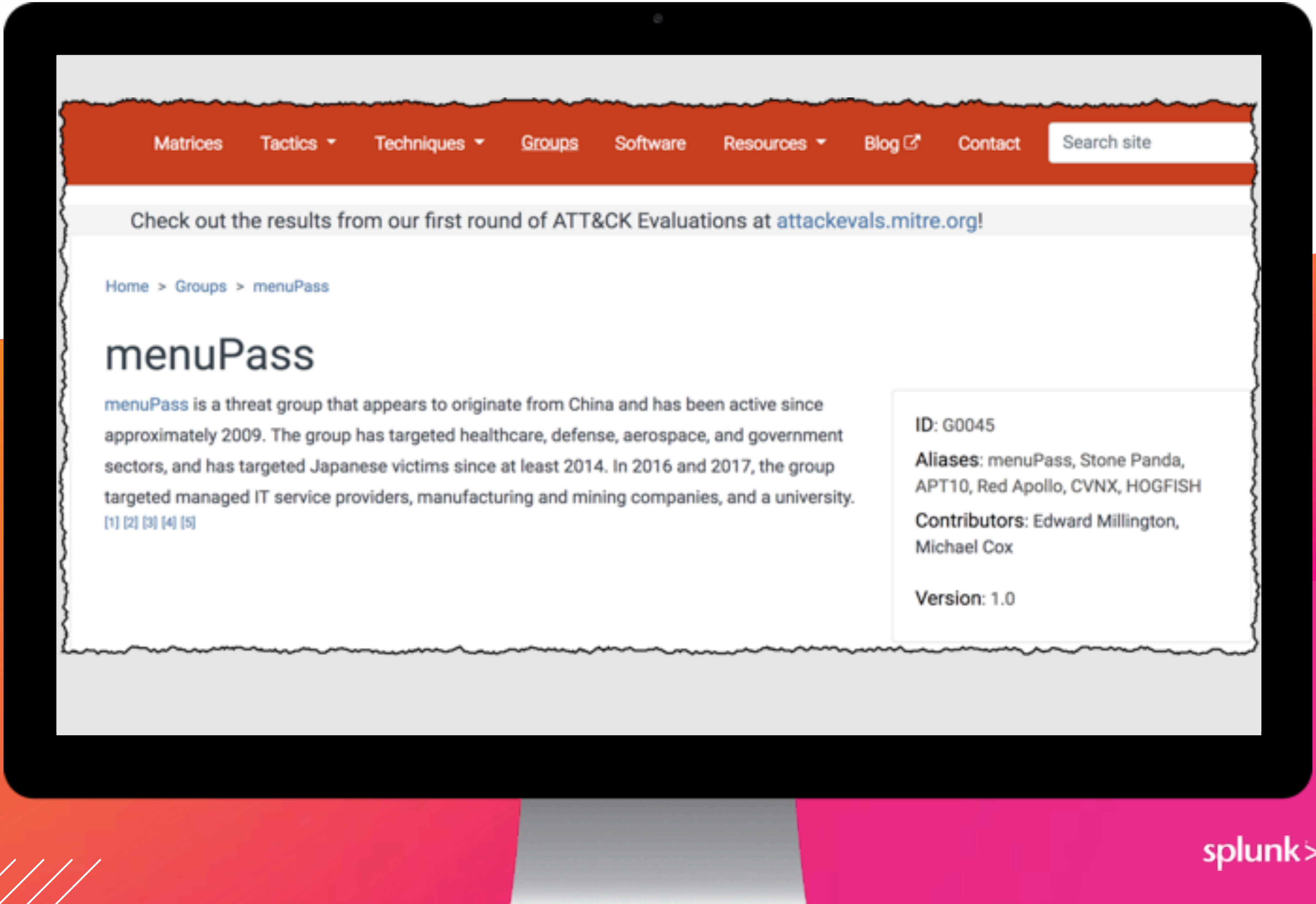
Threat Group-3390	view	select	deselect
Thrip	view	select	deselect
Tropic Trooper	view	select	deselect
Turla	view	select	deselect
Winnti Group	view	select	deselect
admin@338	view	select	deselect
menuPass	view	select	deselect

Software

3PARA RAT	view	select	deselect
4H RAT	view	select	deselect
ADVSTORESHELL	view	select	deselect
ASPXSpy	view	select	deselect
Agent Tesla	view	select	deselect
Agent.btz	view	select	deselect
Arp	view	select	deselect

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

Who and am I a target?



Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

Home > Groups > menuPass

menuPass

menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university. [1] [2] [3] [4] [5]

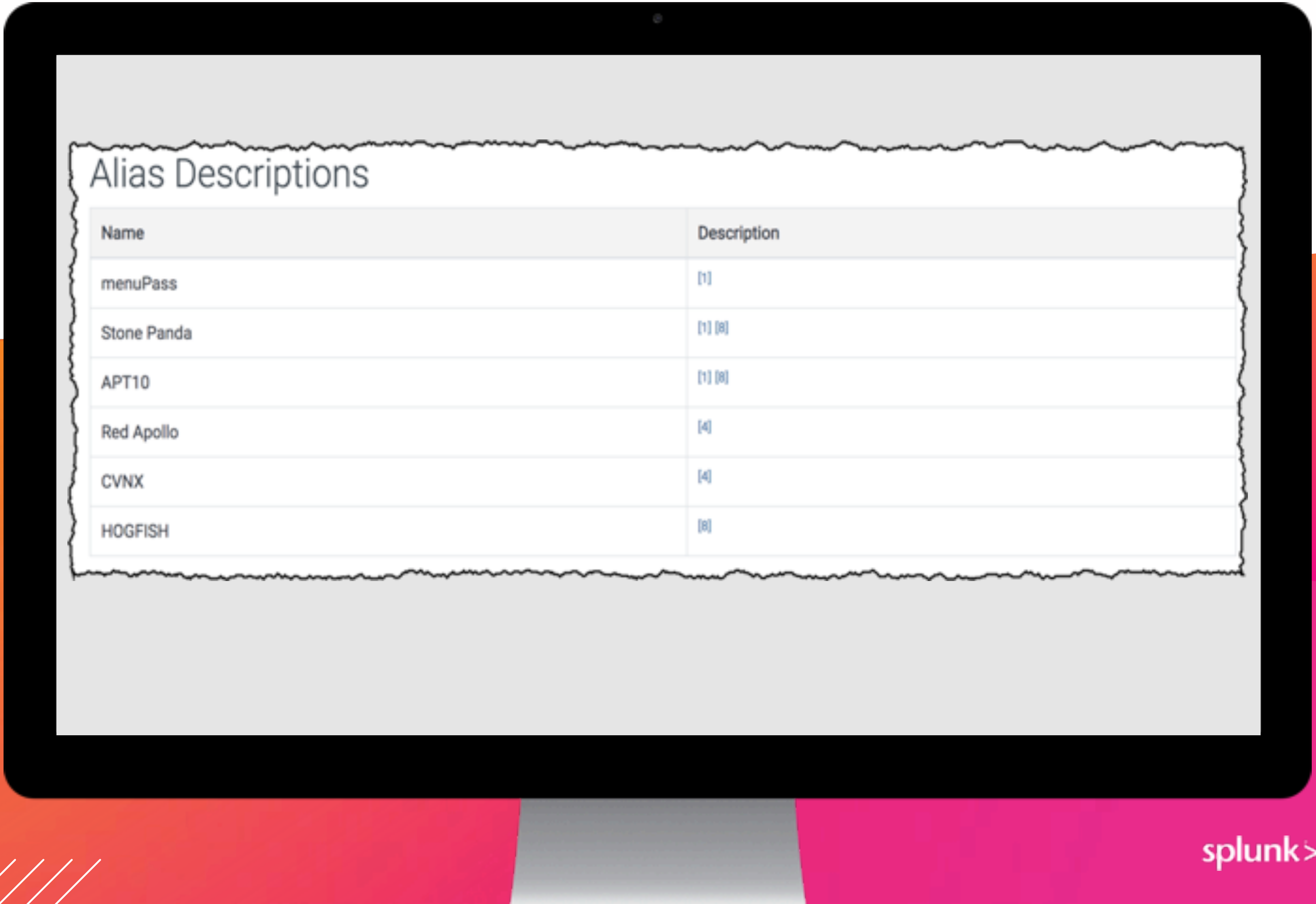
ID: G0045

Aliases: menuPass, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

Contributors: Edward Millington, Michael Cox

Version: 1.0

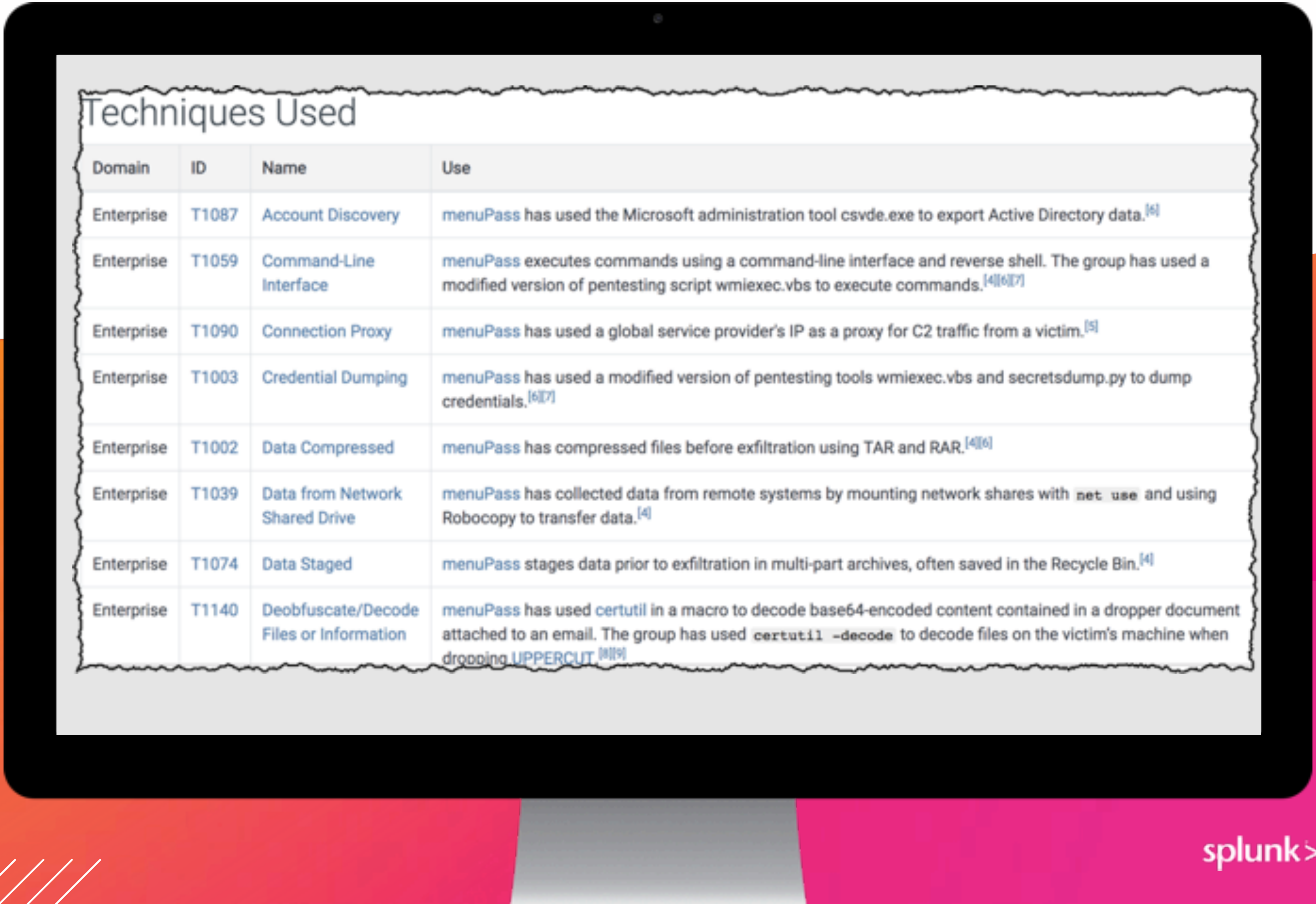
What’s menuPass?



Alias Descriptions

Name	Description
menuPass	[1]
Stone Panda	[1] [8]
APT10	[1] [8]
Red Apollo	[4]
CVNX	[4]
HOGFISH	[8]

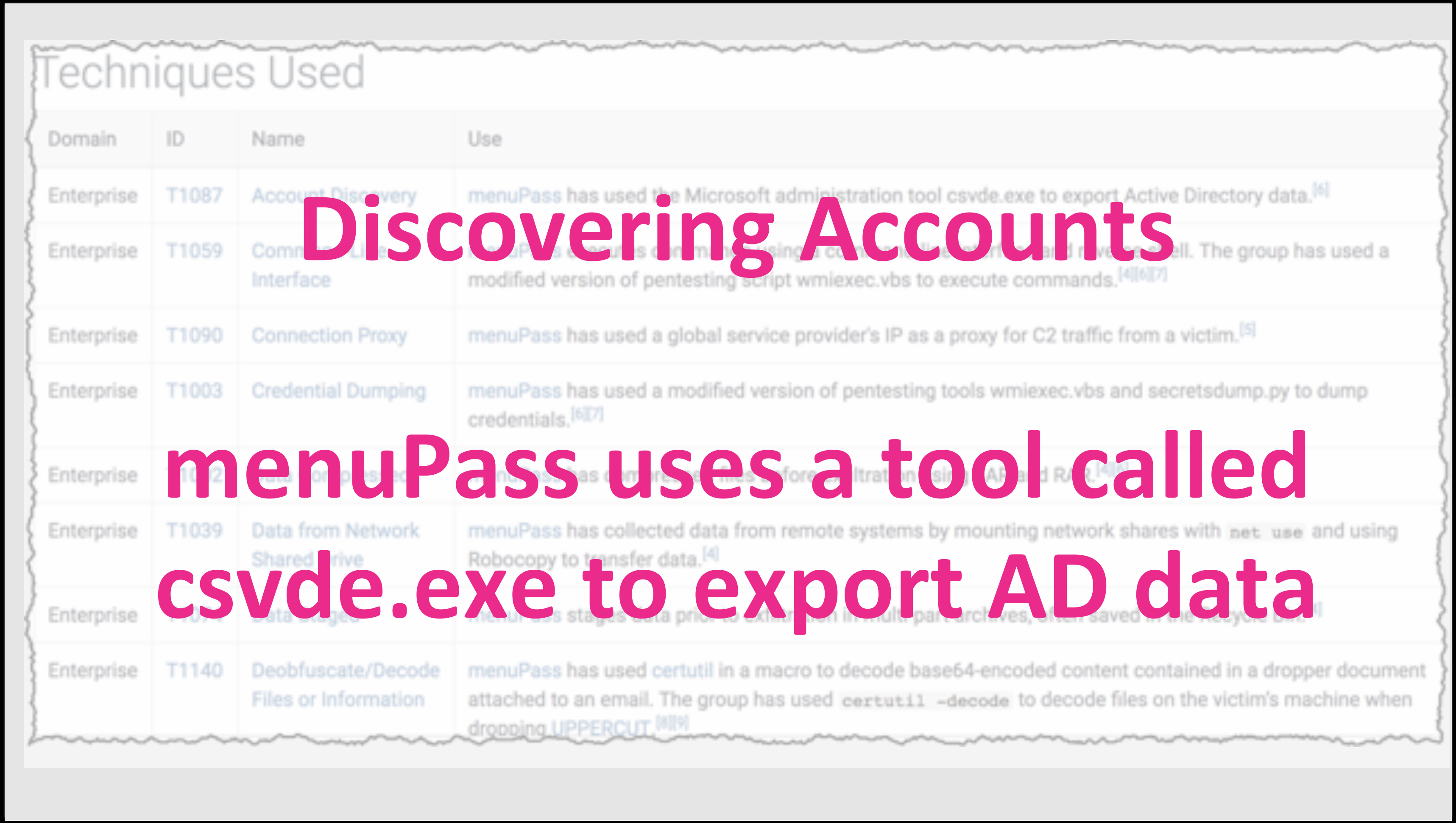
How do I defend my org?



Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[6]
Enterprise	T1059	Command-Line Interface	menuPass executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[4][6][7]
Enterprise	T1090	Connection Proxy	menuPass has used a global service provider's IP as a proxy for C2 traffic from a victim.[5]
Enterprise	T1003	Credential Dumping	menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[6][7]
Enterprise	T1002	Data Compressed	menuPass has compressed files before exfiltration using TAR and RAR.[4][6]
Enterprise	T1039	Data from Network Shared Drive	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[4]
Enterprise	T1074	Data Staged	menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[8][9]

How do I defend my org?



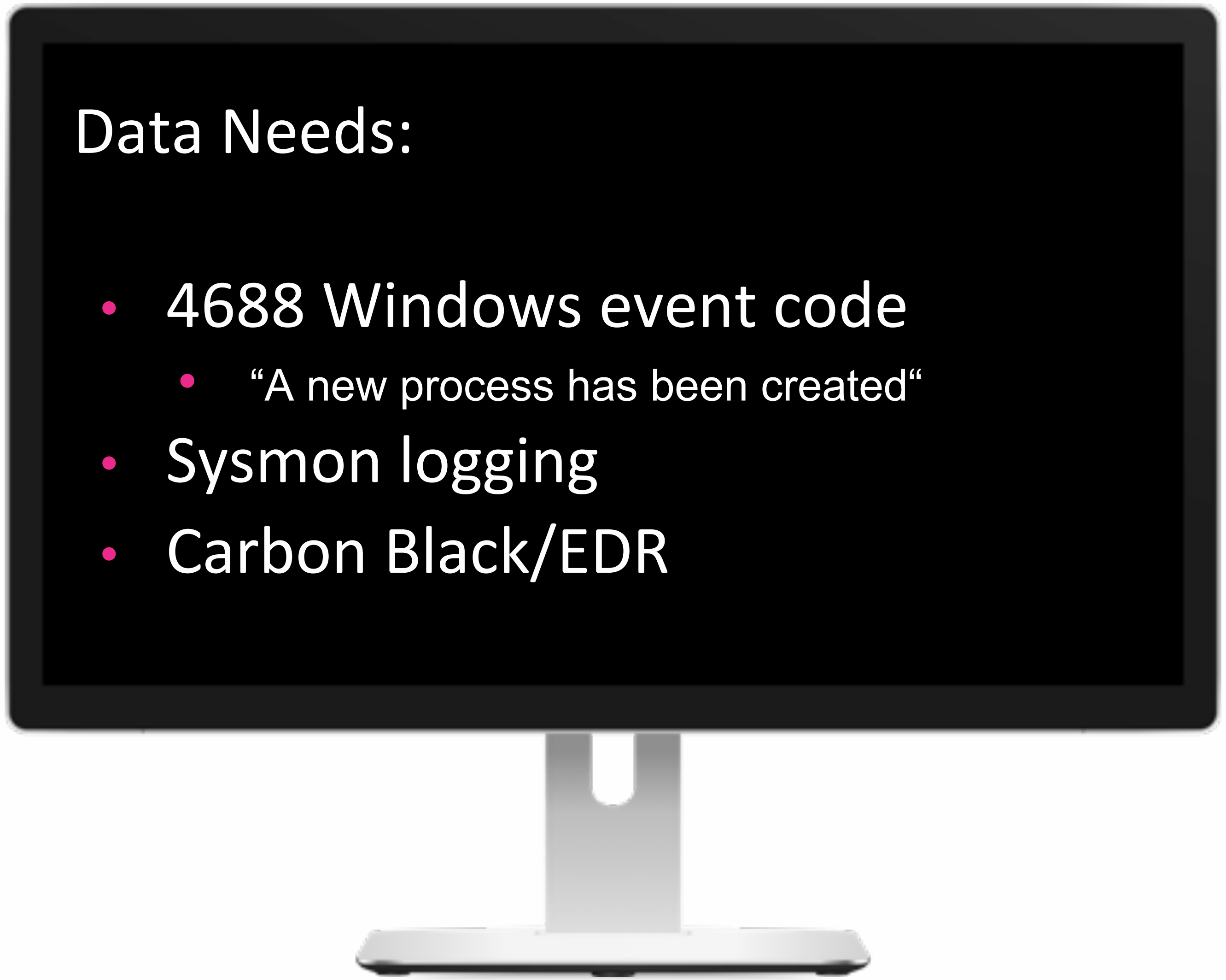
Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[6]
Enterprise	T1059	Command-Line Interface	menuPass executes commands using [illegible] and [illegible] shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[4][6][7]
Enterprise	T1090	Connection Proxy	menuPass has used a global service provider's IP as a proxy for C2 traffic from a victim.[5]
Enterprise	T1003	Credential Dumping	menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[6][7]
Enterprise	T1002	Data Compressed	menuPass has compressed files before exfiltration using [illegible] and RAR.[4][5]
Enterprise	T1039	Data from Network Shared Drive	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[4]
Enterprise	T1074	Data Staged	menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[8][9]

Discovering Accounts

menuPass uses a tool called csvde.exe to export AD data

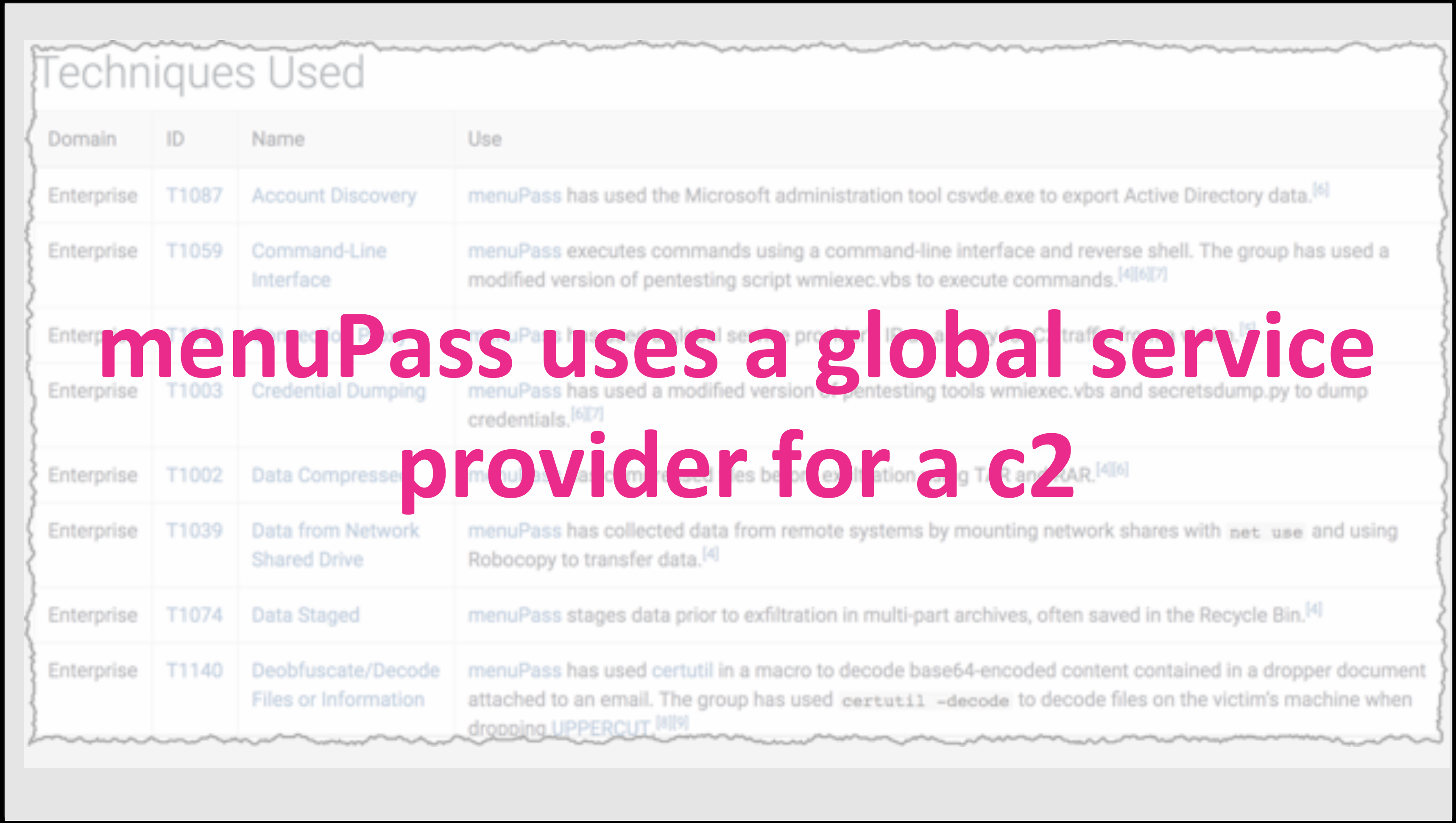
csvde.exe will be executed on an endpoint



Data Needs:

- 4688 Windows event code
  - “A new process has been created“
- Sysmon logging
- Carbon Black/EDR

How do I defend my org?



Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[6]
Enterprise	T1059	Command-Line Interface	menuPass executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[4][6][7]
Enterprise	T1090	Connection Proxy	menuPass has used a global service provider's IP as a proxy for C2 traffic from a victim.[5]
Enterprise	T1003	Credential Dumping	menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[6][7]
Enterprise	T1002	Data Compressed	menuPass has compressed files before exfiltration using TAR and RAR.[4][6]
Enterprise	T1039	Data from Network Shared Drive	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[4]
Enterprise	T1074	Data Staged	menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[8][9]

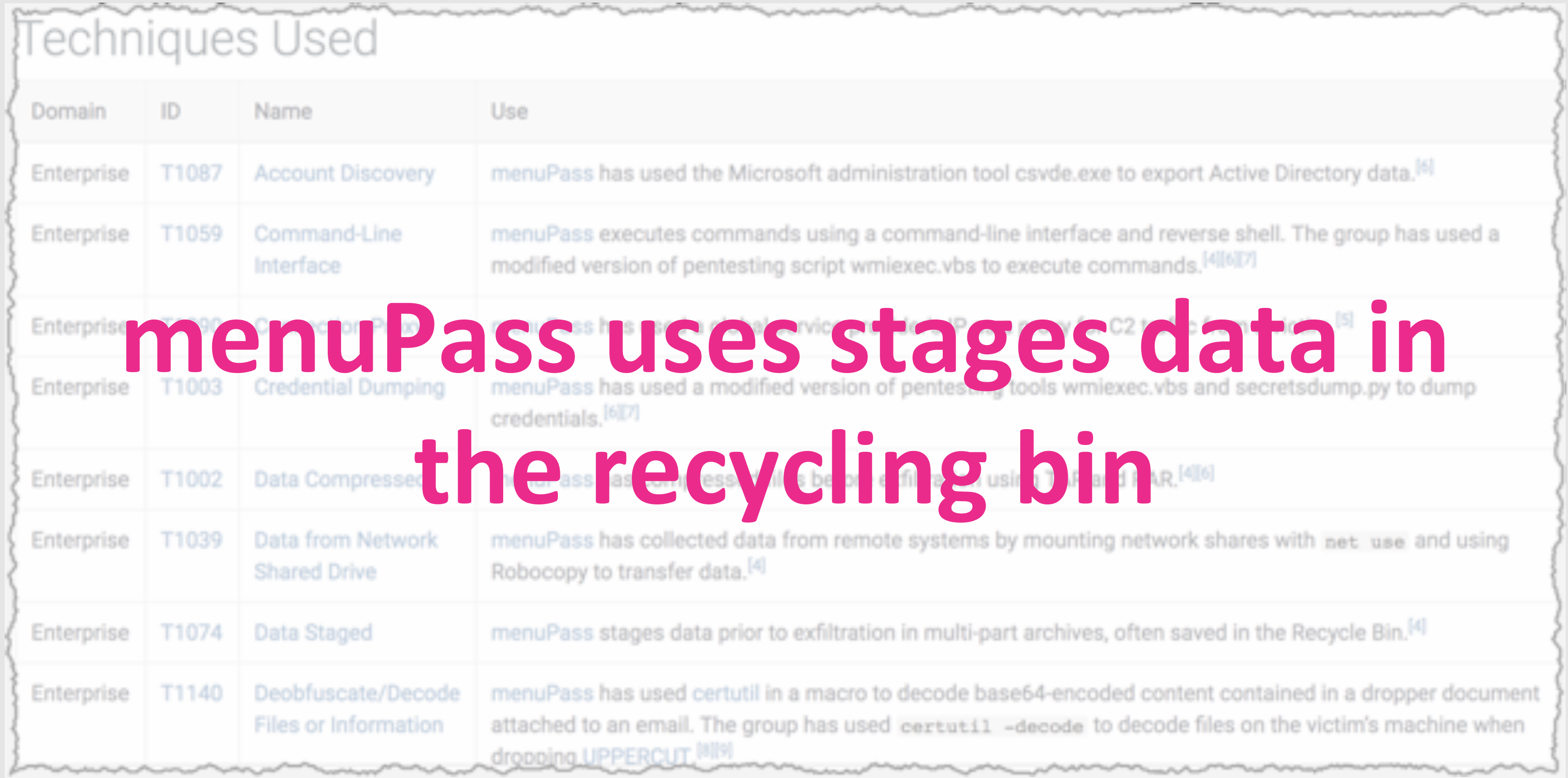
menuPass uses a global service provider for a c2

C2 is in network traffic

Data Needs:

- Stream/Zeek/Wiredata
- DNS
- Firewall traffic
- Netflow traffic

How do I defend my org?



Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[6]
Enterprise	T1059	Command-Line Interface	menuPass executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[4][6][7]
Enterprise	T1090	Connection Proxy	menuPass has used a global service provider's IP as a proxy for C2 traffic from a victim.[5]
Enterprise	T1003	Credential Dumping	menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[6][7]
Enterprise	T1002	Data Compressed	menuPass has compressed files before exfiltration using TAR and RAR.[4][6]
Enterprise	T1039	Data from Network Shared Drive	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[4]
Enterprise	T1074	Data Staged	menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[8][9]

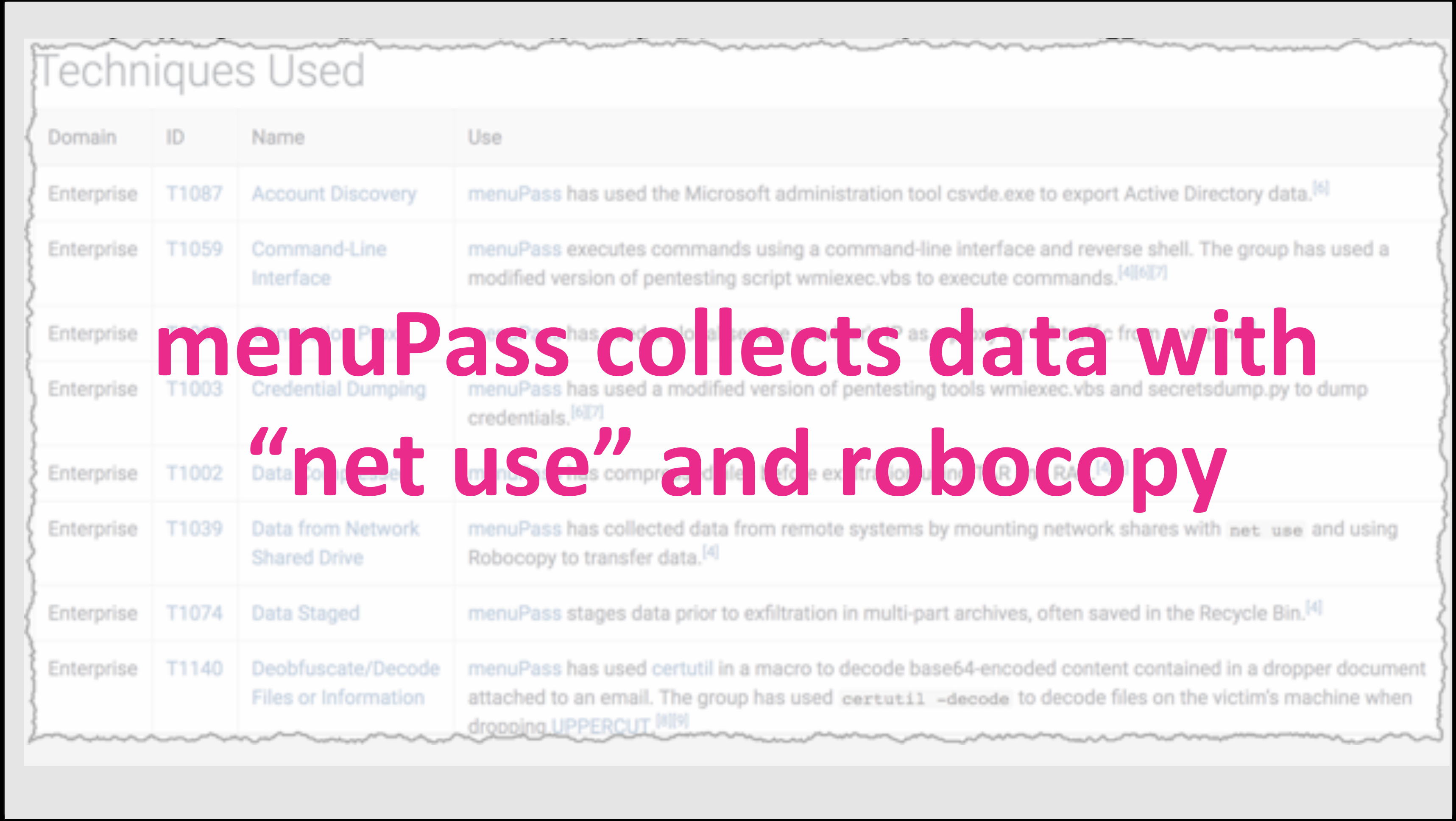
menuPass uses stages data in the recycling bin

Files written to disk on an endpoint

Data Needs:

- Sysmon logging
- Carbon Black/EDR

How do I defend my org?



Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[6]
Enterprise	T1059	Command-Line Interface	menuPass executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands.[4][6][7]
Enterprise	[illegible]	Connection Proxy	[illegible] has [illegible] as [illegible] from [illegible]
Enterprise	T1003	Credential Dumping	menuPass has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.[6][7]
Enterprise	T1002	Data Compressed	menuPass has compressed files before exfiltration using TAR and RAR.[4]
Enterprise	T1039	Data from Network Shared Drive	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[4]
Enterprise	T1074	Data Staged	menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	menuPass has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has used `certutil -decode` to decode files on the victim's machine when dropping UPPERCUT.[8][9]

menuPass collects data with "net use" and robocopy

“net use” will be executed on an endpoint

Data Needs:

- 4688 Windows event code
- Sysmon logging
- Carbon Black/EDR

When does ATT&CK go off the rails

Do Not Think You Have To Alert On Each

Do Not Assume All Techniques Are Equal

Do Not Forget About The Security Basics

Do Not Think It Covers Protection Of What Is Most Important For Your Organization

splunk> turn data into doing

Contatti

@ilf0rz

aforzieri@splunk.com

https://www.linkedin.com/in/antonio-forzieri-1812375/

Grazie...