Sub-techniques, priorities, more open source & MITRE ATT&CK® at mobile phone

~by Andrii Bezverkhyi, SOC Prime

twitter @andriinb

_whoami

NotPetya attribution using ATT&CK in 5 days, July 2, 2017

Sigma + ATT&CK capability Jan 2018 and acceptance May, 2018

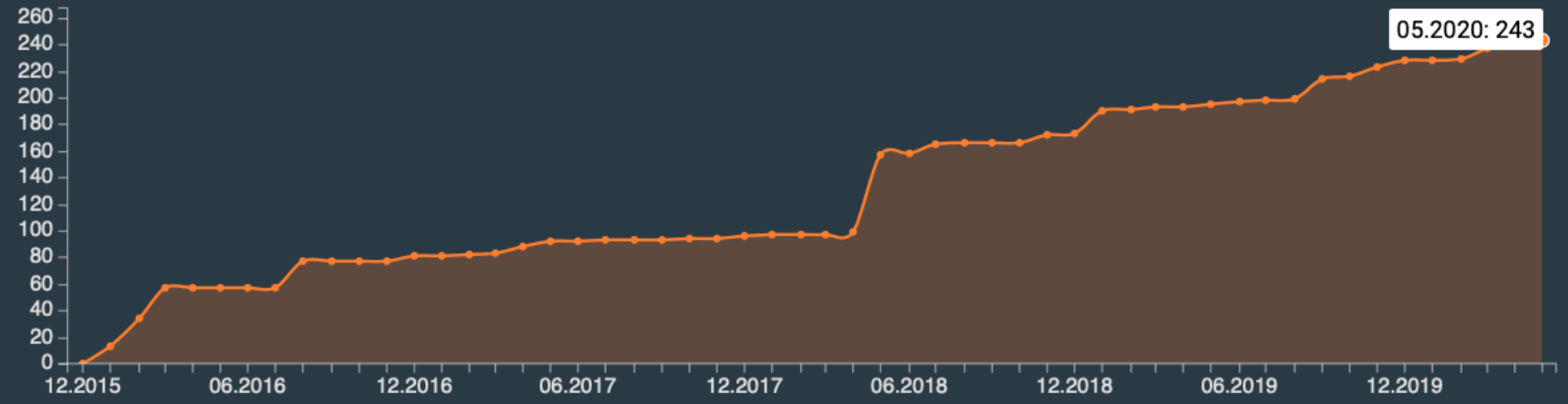
Architect of uncoder.io

THANK YOU
EU ATT&CK & Sigma communities & SOC Prime team,
for making this possible.

SOC PRIME

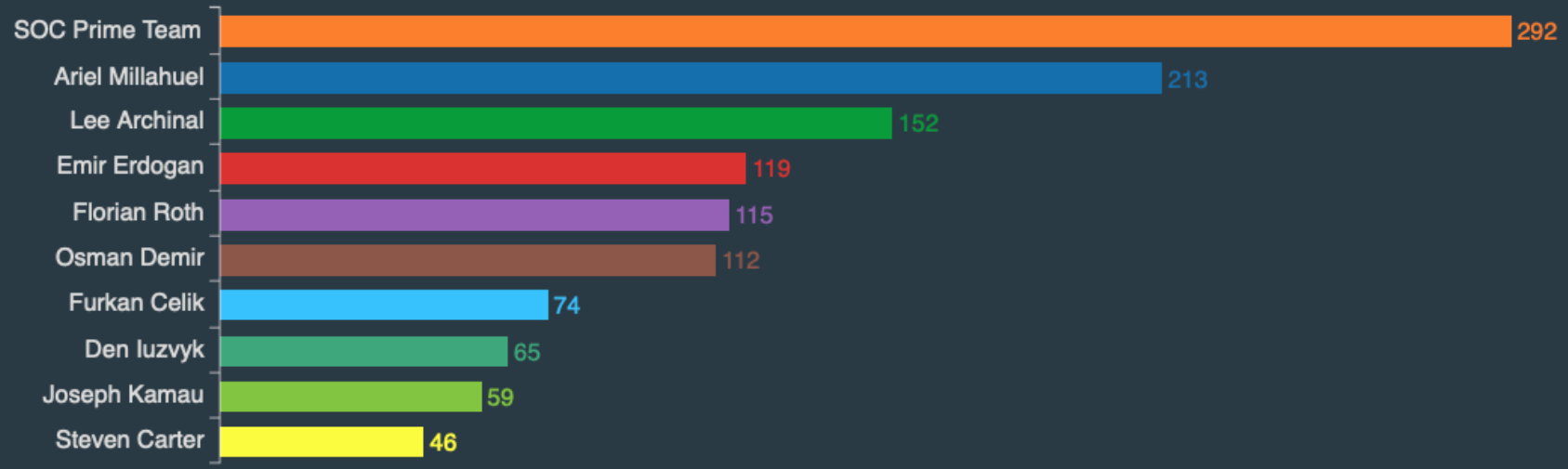
TECHNIQUES, TOOLS & ACTORS

Technique | Release



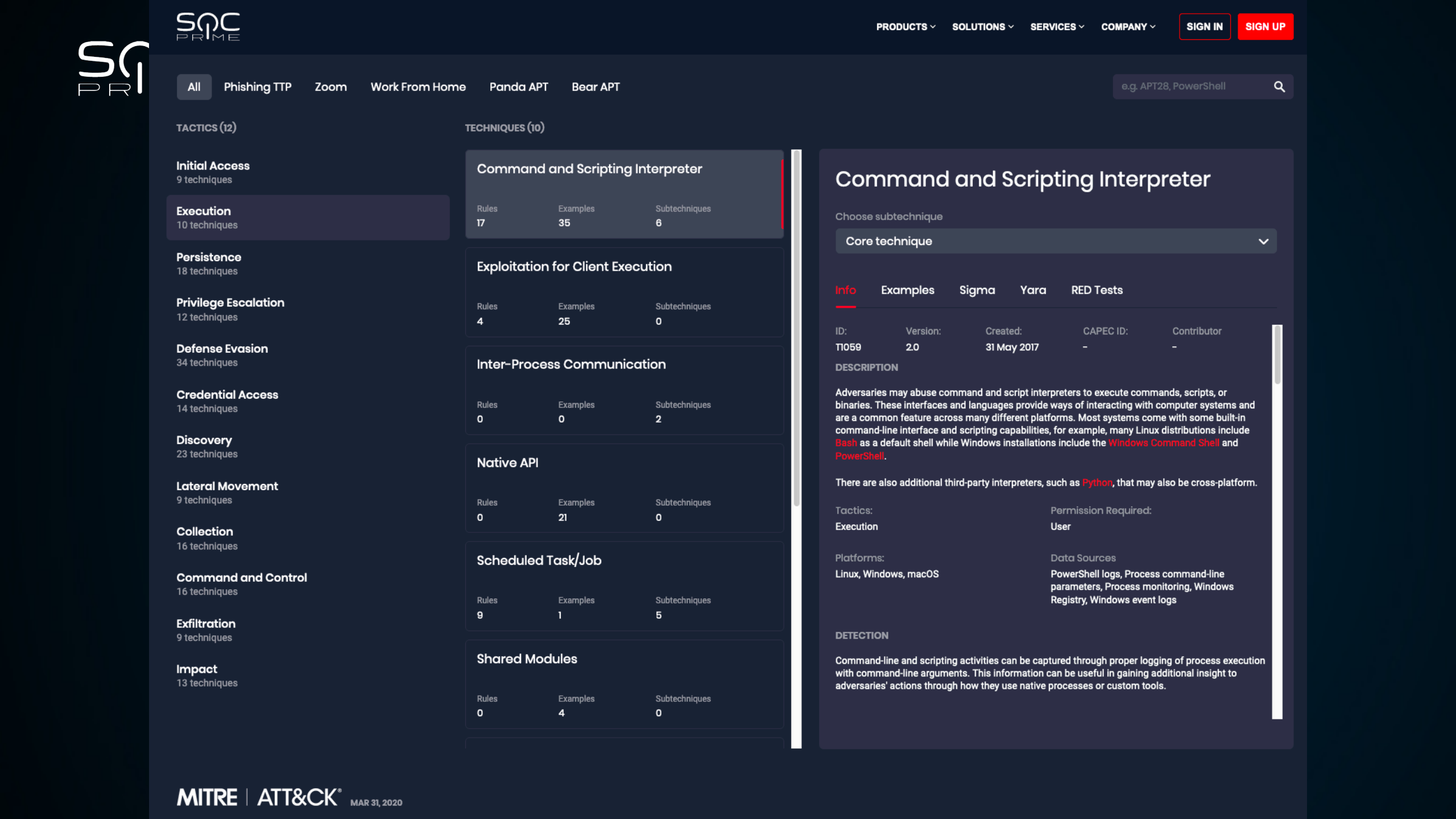
TOP AUTHORS

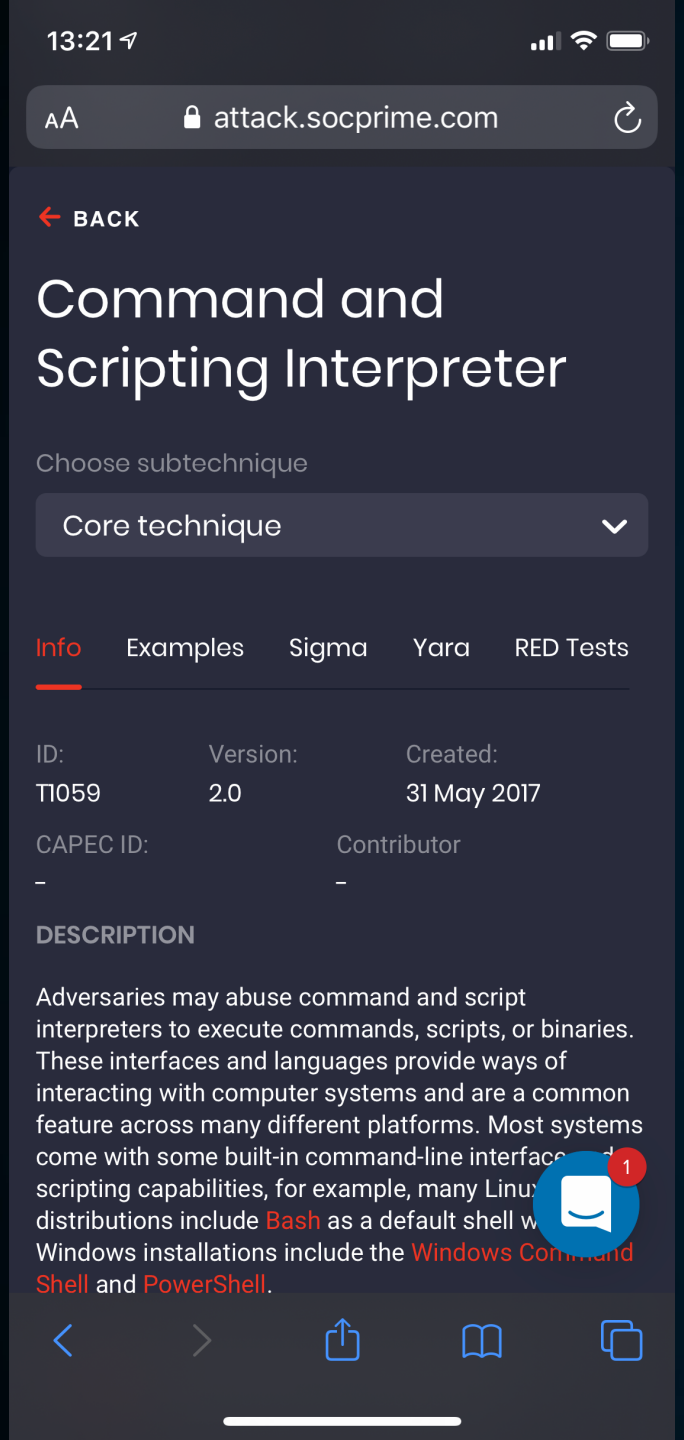
Release | Filter | Year

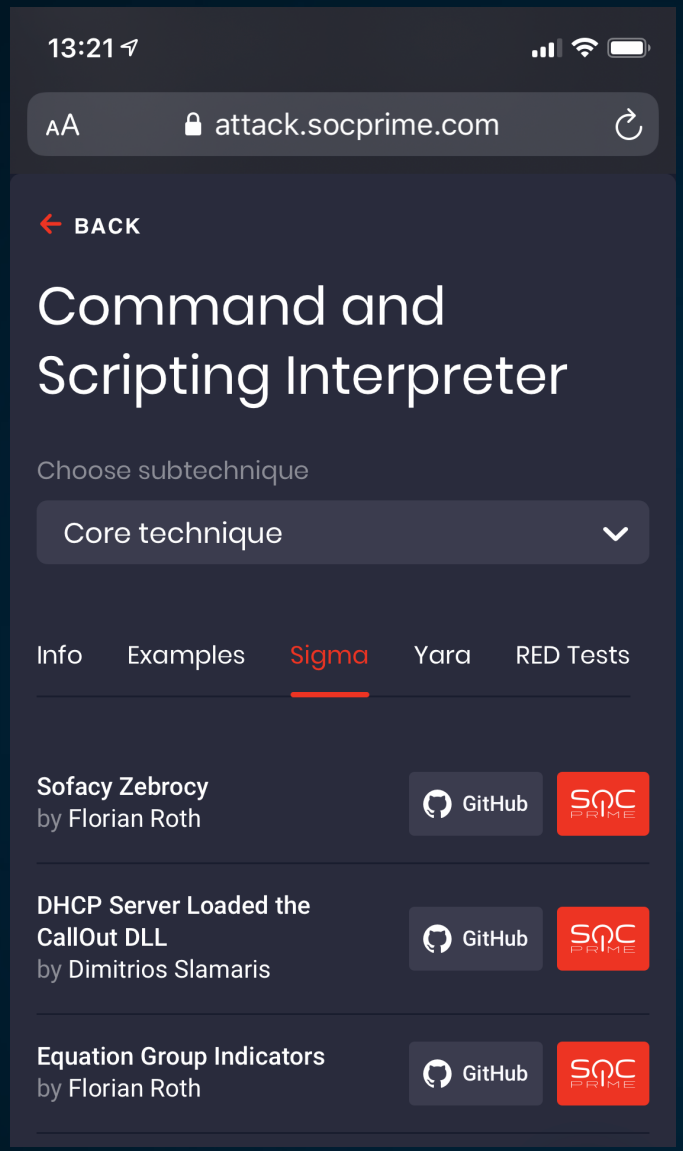


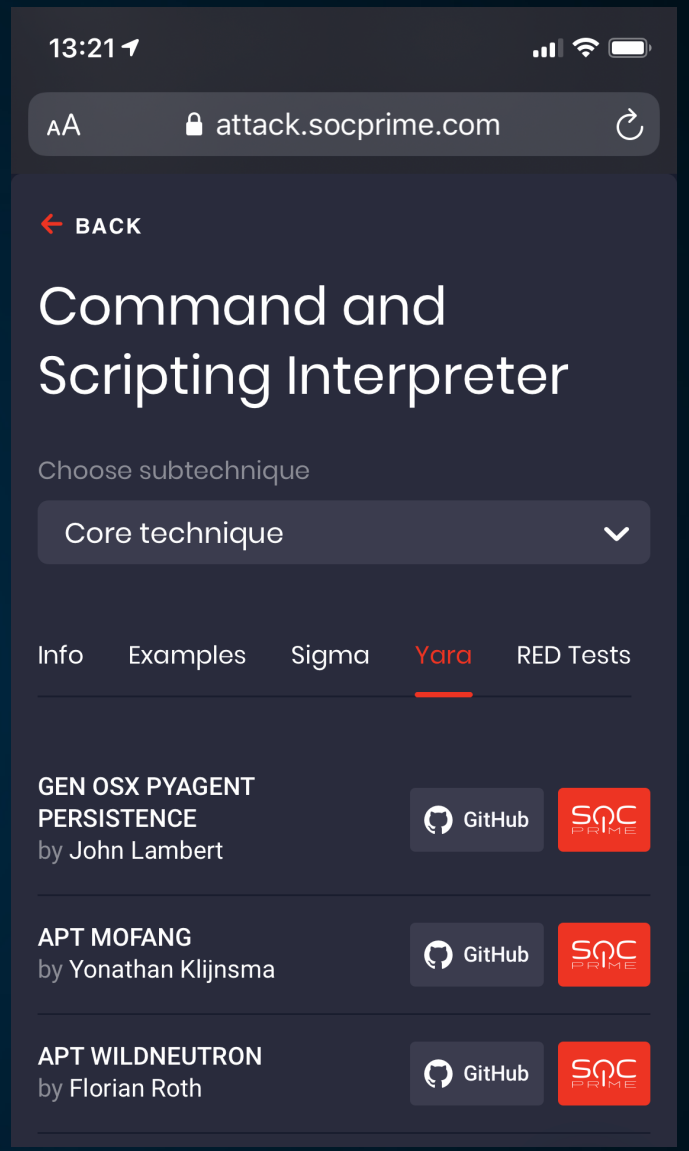
SOC PRIME

Sub-Techniques


PRODUCTS
SOLUTIONS
SERVICES
COMPANY
SIGN IN
SIGN UP
All
Phishing TTP
Zoom
Work From Home
Panda APT
Bear APT
e.g. APT28, PowerShell
TACTICS (12)
Initial Access
9 techniques
Execution
10 techniques
Persistence
18 techniques
Privilege Escalation
12 techniques
Defense Evasion
34 techniques
Credential Access
14 techniques
Discovery
23 techniques
Lateral Movement
9 techniques
Collection
16 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques
TECHNIQUES (10)
Command and Scripting Interpreter
Rules 17
Examples 35
Subtechniques 6
Exploitation for Client Execution
Rules 4
Examples 25
Subtechniques 0
Inter-Process Communication
Rules 0
Examples 0
Subtechniques 2
Native API
Rules 0
Examples 21
Subtechniques 0
Scheduled Task/Job
Rules 9
Examples 1
Subtechniques 5
Shared Modules
Rules 0
Examples 4
Subtechniques 0
Command and Scripting Interpreter
Choose subtechnique
Core technique
Info
Examples
Sigma
Yara
RED Tests
ID: T1059
Version: 2.0
Created: 31 May 2017
CAPEC ID: -
Contributor -
DESCRIPTION
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, many Linux distributions include Bash as a default shell while Windows installations include the Windows Command Shell and PowerShell.
There are also additional third-party interpreters, such as Python, that may also be cross-platform.
Tactics:
Execution
Permission Required:
User
Platforms:
Linux, Windows, macOS
Data Sources
PowerShell logs, Process command-line parameters, Process monitoring, Windows Registry, Windows event logs
DETECTION
Command-line and scripting activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools.
MITRE | ATT&CK
MAR 31, 2020

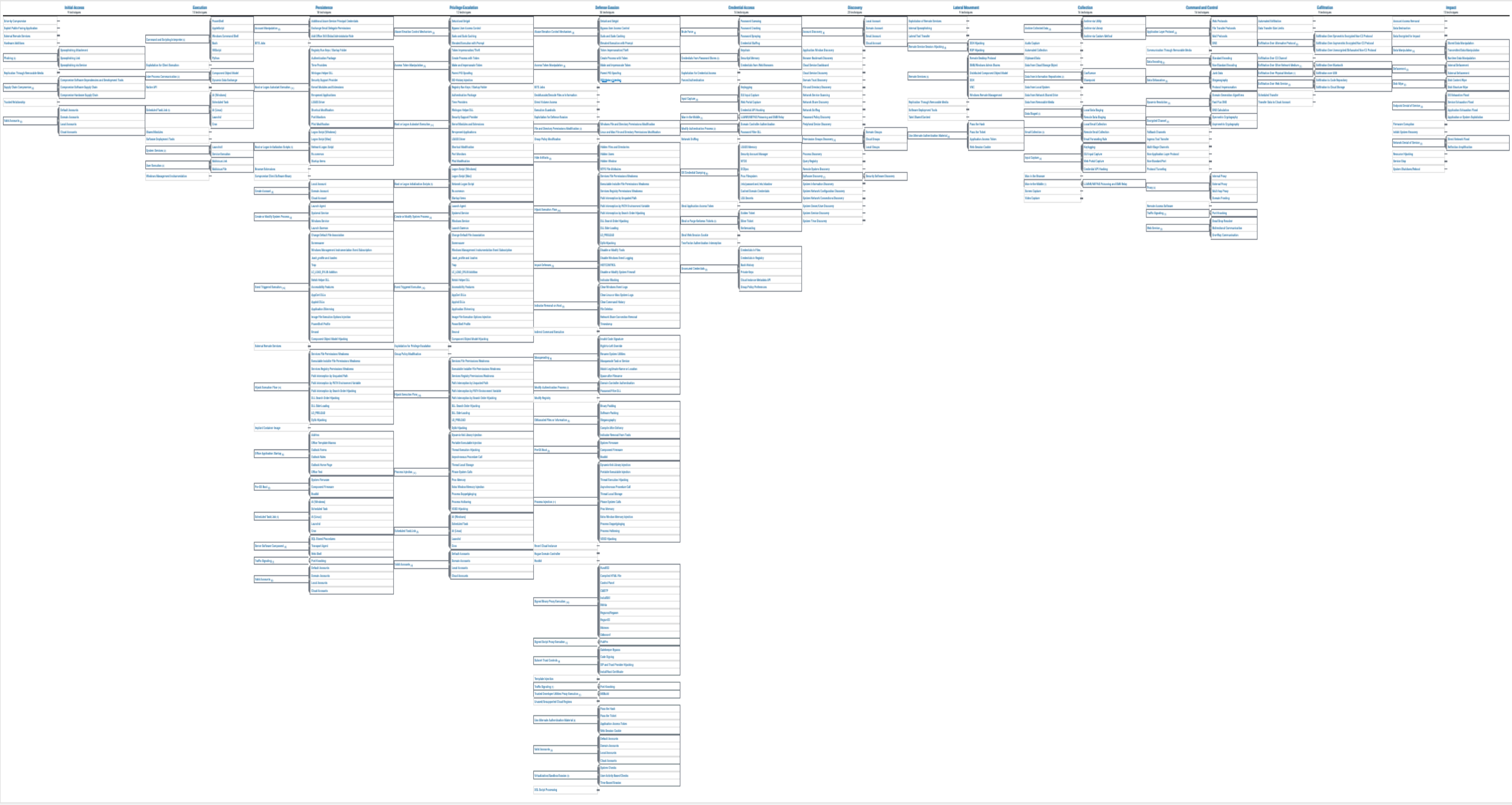

13:21
AA
attack.socprime.com
BACK
Command and Scripting Interpreter
Choose subtechnique
Core technique
Info
Examples
Sigma
Yara
RED Tests
ID:
T1059
Version:
2.0
Created:
31 May 2017
CAPEC ID:
-
Contributor
-
DESCRIPTION
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, many Linux distributions include Bash as a default shell while Windows installations include the Windows Command Shell and PowerShell.
1


13:21
AA
attack.socprime.com
BACK
Command and Scripting Interpreter
Choose subtechnique
Core technique
Info
Examples
Sigma
Yara
RED Tests
Sofacy Zebrocy
by Florian Roth
GitHub
DHCP Server Loaded the CallOut DLL
by Dimitrios Slamaris
GitHub
Equation Group Indicators
by Florian Roth
GitHub


13:21
AA
attack.socprime.com
BACK
Command and Scripting Interpreter
Choose subtechnique
Core technique
Info
Examples
Sigma
Yara
RED Tests
GEN OSX PYAGENT PERSISTENCE
by John Lambert
GitHub
APT MOFANG
by Yonathan Klijnsma
GitHub
APT WILDNEUTRON
by Florian Roth
GitHub

ATT&CK Matrix for Enterprise

layouts: - show sub-techniques hide sub-techniques



V • T • E

Periodic table

18x9

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	Alkali metals	Alkaline earth metals													Pnictogens	Chalcogens	Halogens	Noble gases
Period 1	Hydrogen 1 H 1.008																	Helium 2 He 4.0026
2	Lithium 3 Li 6.94	Beryllium 4 Be 9.0122											Boron 5 B 10.81	Carbon 6 C 12.011	Nitrogen 7 N 14.007	Oxygen 8 O 15.999	Fluorine 9 F 18.998	Neon 10 Ne 20.180
3	Sodium 11 Na 22.990	Magnesium 12 Mg 24.305											Aluminium 13 Al 26.982	Silicon 14 Si 28.085	Phosphorus 15 P 30.974	Sulfur 16 S 32.06	Chlorine 17 Cl 35.45	Argon 18 Ar 39.95
4	Potassium 19 K 39.098	Calcium 20 Ca 40.078	Scandium 21 Sc 44.956	Titanium 22 Ti 47.867	Vanadium 23 V 50.942	Chromium 24 Cr 51.996	Manganese 25 Mn 54.938	Iron 26 Fe 55.845	Cobalt 27 Co 58.933	Nickel 28 Ni 58.693	Copper 29 Cu 63.546	Zinc 30 Zn 65.38	Gallium 31 Ga 69.723	Germanium 32 Ge 72.630	Arsenic 33 As 74.922	Selenium 34 Se 78.971	Bromine 35 Br 79.904	Krypton 36 Kr 83.798
5	Rubidium 37 Rb 85.468	Strontium 38 Sr 87.62	Yttrium 39 Y 88.906	Zirconium 40 Zr 91.224	Niobium 41 Nb 92.906	Molybdenum 42 Mo 95.95	Technetium 43 Tc [97]	Ruthenium 44 Ru 101.07	Rhodium 45 Rh 102.91	Palladium 46 Pd 106.42	Silver 47 Ag 107.87	Cadmium 48 Cd 112.41	Indium 49 In 114.82	Tin 50 Sn 118.71	Antimony 51 Sb 121.76	Tellurium 52 Te 127.60	Iodine 53 I 126.90	Xenon 54 Xe 131.29
6	Caesium 55 Cs 132.91	Barium 56 Ba 137.33	Lanthanum 57 La 138.91	Hafnium 72 Hf 178.49	Tantalum 73 Ta 180.95	Tungsten 74 W 183.84	Rhenium 75 Re 186.21	Osmium 76 Os 190.23	Iridium 77 Ir 192.22	Platinum 78 Pt 195.08	Gold 79 Au 196.97	Mercury 80 Hg 200.59	Thallium 81 Tl 204.38	Lead 82 Pb 207.2	Bismuth 83 Bi 208.98	Polonium 84 Po [209]	Astatine 85 At [210]	Radon 86 Rn [222]
7	Francium 87 Fr [223]	Radium 88 Ra [226]	Actinium 89 Ac [227]	Rutherfordium 104 Rf [267]	Dubnium 105 Db [268]	Seaborgium 106 Sg [269]	Bohrium 107 Bh [270]	Hassium 108 Hs [269]	Meitnerium 109 Mt [278]	Darmstadtium 110 Ds [281]	Roentgenium 111 Rg [282]	Copernicium 112 Cn [285]	Nihonium 113 Nh [286]	Flerovium 114 Fl [289]	Moscovium 115 Mc [290]	Livermorium 116 Lv [293]	Tennessine 117 Ts [294]	Oganesson 118 Og [294]
*				Cerium 58 Ce 140.12	Praseodymium 59 Pr 140.91	Neodymium 60 Nd 144.24	Promethium 61 Pm [145]	Samarium 62 Sm 150.36	Europium 63 Eu 151.96	Gadolinium 64 Gd 157.25	Terbium 65 Tb 158.93	Dysprosium 66 Dy 162.50	Holmium 67 Ho 164.93	Erbium 68 Er 167.26	Thulium 69 Tm 168.93	Ytterbium 70 Yb 173.05	Lutetium 71 Lu 174.97	
‡				Thorium 90 Th 232.04	Protactinium 91 Pa 231.04	Uranium 92 U 238.03	Neptunium 93 Np [237]	Plutonium 94 Pu [244]	Americium 95 Am [243]	Curium 96 Cm [247]	Berkelium 97 Bk [247]	Californium 98 Cf [251]	Einsteinium 99 Es [252]	Fermium 100 Fm [257]	Mendelevium 101 Md [258]	Nobelium 102 No [259]	Lawrencium 103 Lr [266]	

1 (red)=Gas | 3 (black)=Solid | 80 (green)=Liquid | 109 (gray)=Unknown **Color of the atomic number** shows state of matter (at 0 °C and 1 atm)

Primordial | From decay | Synthetic **Border** shows natural occurrence of the element

Standard atomic weight $A_{r,\,std}(E)$[4] Ca: 40.078 — Formal short value, rounded (no uncertainty)[5]
Po: [209] — mass number of the most stable isotope

Background color shows subcategory in the metal–metalloid–nonmetal trend:

Metal						Metalloid	Nonmetal		Unknown chemical properties
Alkali metal	Alkaline earth metal	Lanthanide	Actinide	Transition metal	Post-transition metal		Reactive nonmetal	Noble gas	

Transpose the matrix, Tactics move to horizontal

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

12x32

Terms used consistently, Tactics cropped from Technique names

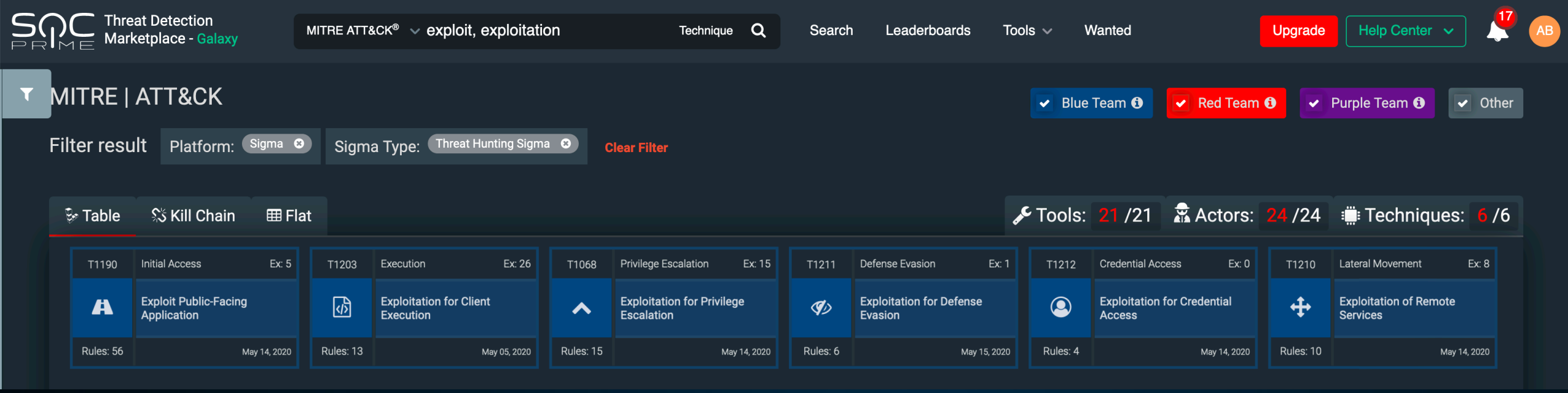
Initial Access	Drive-by Compromise	Exploit	Remote Services	Hardware Additions	Phishing	Removable Media	Supply Chain Compromise	Trusted Relationship	Valid Accounts																								
Execution	Command and Scripting Interpreter	Exploit	Inter-Process Communication	Native API	Scheduled Task/Job	Shared Modules	Software Deployment Tools	System Services	User Execution	WMI																							
Persistence	Account Manipulation	BITS Jobs	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Browser Extensions	Compromise Client Software Binary	Create Account	Create or Modify System Process	Event Triggered Execution	Remote Services	Hijack Execution Flow	Office Application Startup	Pre-OS Boot	Scheduled Task/Job	Server Software Component	Traffic Signaling	Valid Accounts																
Privilege Escalation	Abuse Elevation Control Mechanism	Access Token Manipulation	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Create or Modify System Process	Event Triggered Execution	Exploit	Group Policy Modification	Hijack Execution Flow	Process Injection	Scheduled Task/Job	Valid Accounts																					
Defense Evasion	Abuse Elevation Control Mechanism	Access Token Manipulation	BITS Jobs	Decode Information	Direct Volume Access	Execution Guardrails	Exploit	File and Directory Permissions Modification	Group Policy Modification	Hide Artifacts	Hijack Execution Flow	Impair Defenses	Indicator Removal on Host	Indirect Command Execution	Masquerading	Modify Authentication Process	Modify Registry	Obfuscated Information	Pre-OS Boot	Process Injection	Rogue Domain Controller	Rootkit	Signed Binary Proxy Execution	Signed Script Proxy Execution	Subvert Trust Controls	Template Injection	Traffic Signaling	Trusted Developer Utilities Proxy Execution	Use Alternate Authentication Material	Valid Accounts	Virtualization / Sandbox Evasion	XSL Script Processing
Credential Access	Brute Force	Credentials from Password Stores	Exploit	Forced Authentication	Input Capture	Man-in-the-Middle	Modify Authentication Process	Network Sniffing	OS Credential Dumping	Kerberos	Steal Web Session Cookie	2FA Interception	Unsecured Credentials																			
Discovery	Accounts	Application Window	Browser Bookmark	Domain Trust	File and Directory	Network Service Scanning	Network Share	Network Sniffing	Password Policy	Peripheral Device	Permission Groups	Process Listing	Query Registry	Remote System	Software	System Information	System Network Configuration	System Network Connections	System Owner / User	System Services	System Time											
Lateral Movement	Exploit	Phishing	Tool Transfer	Remote Service Session Hijacking	Remote Services	Removable Media	Software Deployment Tools	Taint Shared Content	Use Alternate Authentication Material																							
Collection	Archive Collected Data	Audio Capture	Automated Collection	Clipboard Data	Data from Information Repositories	Data from Local System	Data from Network Shared Drive	Data from Removable Media	Data Staged	Email	Input Capture	Man in the Browser	Man-in-the-Middle	Screen Capture	Video Capture																	
Command and Control	Application Layer Protocol	Removable Media	Data Encoding	Data Obfuscation	Dynamic Resolution	Encrypted Channel	Fallback Channels	Ingress Tool Transfer	Multi-Stage Channels	Non-Application Layer Protocol	Non-Standard Port	Protocol Tunneling	Proxy	Remote Access Software	Traffic Signaling	Web Service																
Exfiltration	Automated Exfiltration	Data Transfer Size Limits	Alternative Protocol	C2 Channel	Other Network Medium	Physical Medium	Web Service	Scheduled Transfer																								
Impact	Account Access Removal	Data Destruction	Data Encrypted for Impact	Data Manipulation	Defacement	Disk Wipe	Endpoint DoS	Firmware Corruption	Inhibit System Recovery	Network Denial of Service	Resource Hijacking	Service Stop	System Shutdown / Reboot																			

Discovery: idea on sub-techniques

Host Parameters		User Data	Network Specifics
Software	Accounts	Browser Bookmark	Domain Trust
System Information	File and Directory	Application Window	Password Policy
System Network Configuration	Peripheral Device	System Owner / User	Network Sniffing
System Services	Permission Groups		Remote System
System Time	Process Listing		
System Network Connections	Query Registry		

Credential Access: idea on sub-techniques

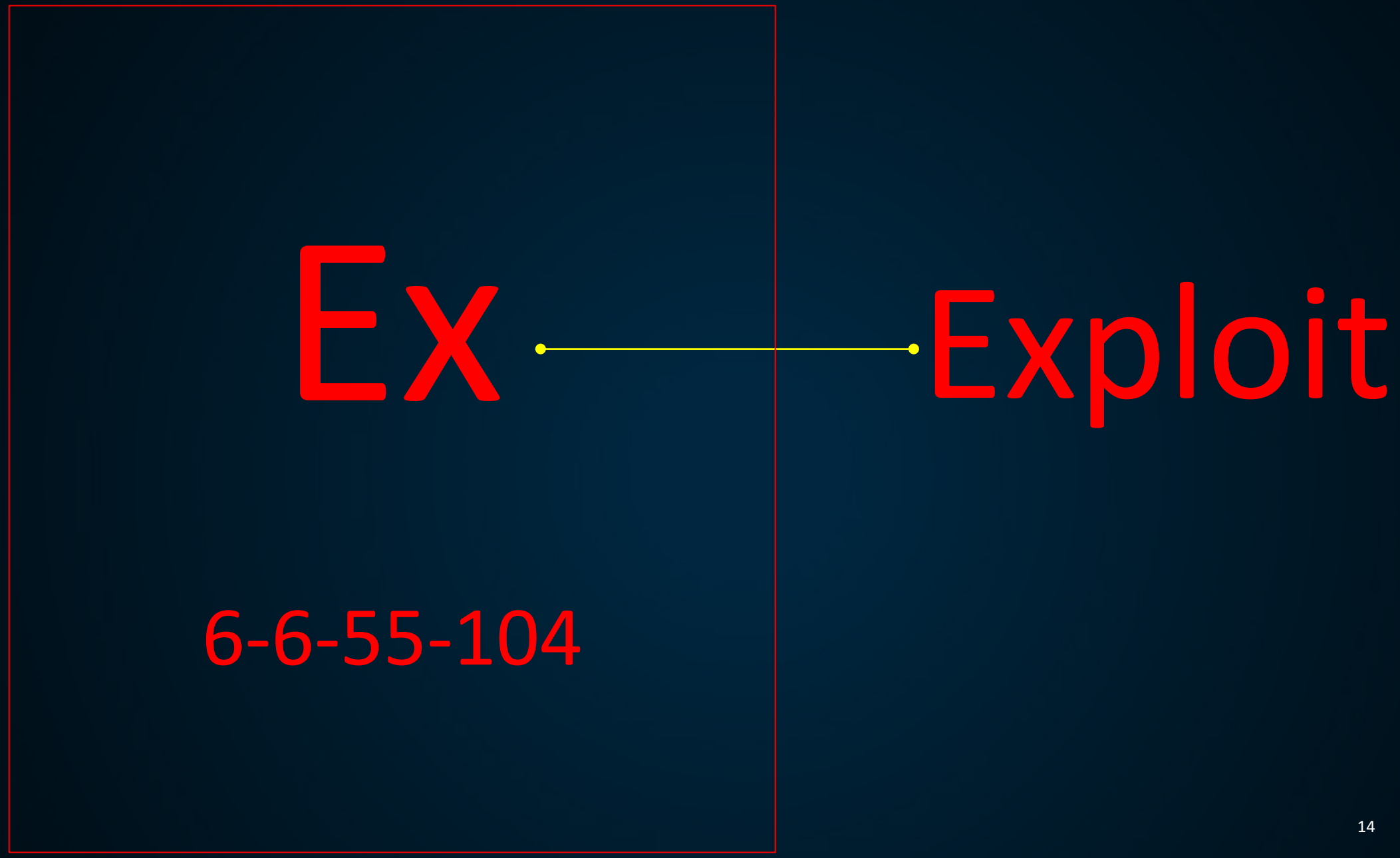
Clear Text Credentials	**Credential Extraction**							
Unsecured Credentials	OS Credential Dumping	LSASS Memory	NTDS	DCSync	Proc Filesystem	/etc/passwd and /etc/shadow	Cached Domain Credentials	LSA Secrets
Network Sniffing	Credentials from Password Stores	Keychain	Securityd Memory	Credentials from Web Browsers				



6 Tactics
6 Techniques, #5 has 0 examples
55 examples
104 Sigma rules on behavior

Tactics	Techniques	Examples	Sigma
6	6	55	104

Exploit code = 6-6-55-104


Ex
Exploit
6-6-55-104

Phantom techniques

T1153	Execution	Ex: 0
	Source	
Rules: 0		

T1019	Persistence	Ex: 3
	System Firmware	
Rules: 0		

T1157	Privilege Escalation	Ex: 0
	Dylib Hijacking	
Rules: 0		

T1480	Defense Evasion	Ex: 2
	Execution Guardrails	
Rules: 0		

T1111	Credential Access	Ex: 1
	Two-Factor Authentication Interception	
Rules: 0		

T1538	Discovery	Ex: 0
	Cloud Service Dashboard	
Rules: 0		

T1184	Lateral Movement	Ex: 1
	SSH Hijacking	
Rules: 0		

T1052	Exfiltration	Ex: 5
	Exfiltration Over Physical Medium	
Rules: 0		

T1529	Impact	Ex: 6
	System Shutdown/Reboot	
Rules: 0		

T1162	Persistence	Ex: 1
	Login Item	
Rules: 0		

T1514	Privilege Escalation	Ex: 1
	Elevated Execution with Prompt	
Rules: 0		

T1109	Defense Evasion	Ex: 1
	Component Firmware	
Rules: 0		

T1167	Credential Access	Ex: 1
	Securityd Memory	
Rules: 0		

T1534	Lateral Movement	Ex: 0
	Internal Spearphishing	
Rules: 0		

T1537	Exfiltration	Ex: 0
	Transfer Data to Cloud Account	
Rules: 0		

T1157	Persistence	Ex: 0
	Dylib Hijacking	
Rules: 0		

T1502	Privilege Escalation	Ex: 1
	Parent PID Spoofing	
Rules: 0		

T1502	Defense Evasion	Ex: 1
	Parent PID Spoofing	
Rules: 0		

T1522	Credential Access	Ex: 0
	Cloud Instance Metadata API	
Rules: 0		

T1506	Lateral Movement	Ex: 0
	Web Session Cookie	
Rules: 0		

T1525	Persistence	Ex: 0
	Implant Container Image	
Rules: 0		

T1519	Privilege Escalation	Ex: 0
	Emond	
Rules: 0		

T1006	Defense Evasion	Ex: 0
	File System Logical Offsets	
Rules: 0		

T1109	Persistence	Ex: 1
	Component Firmware	
Rules: 0		

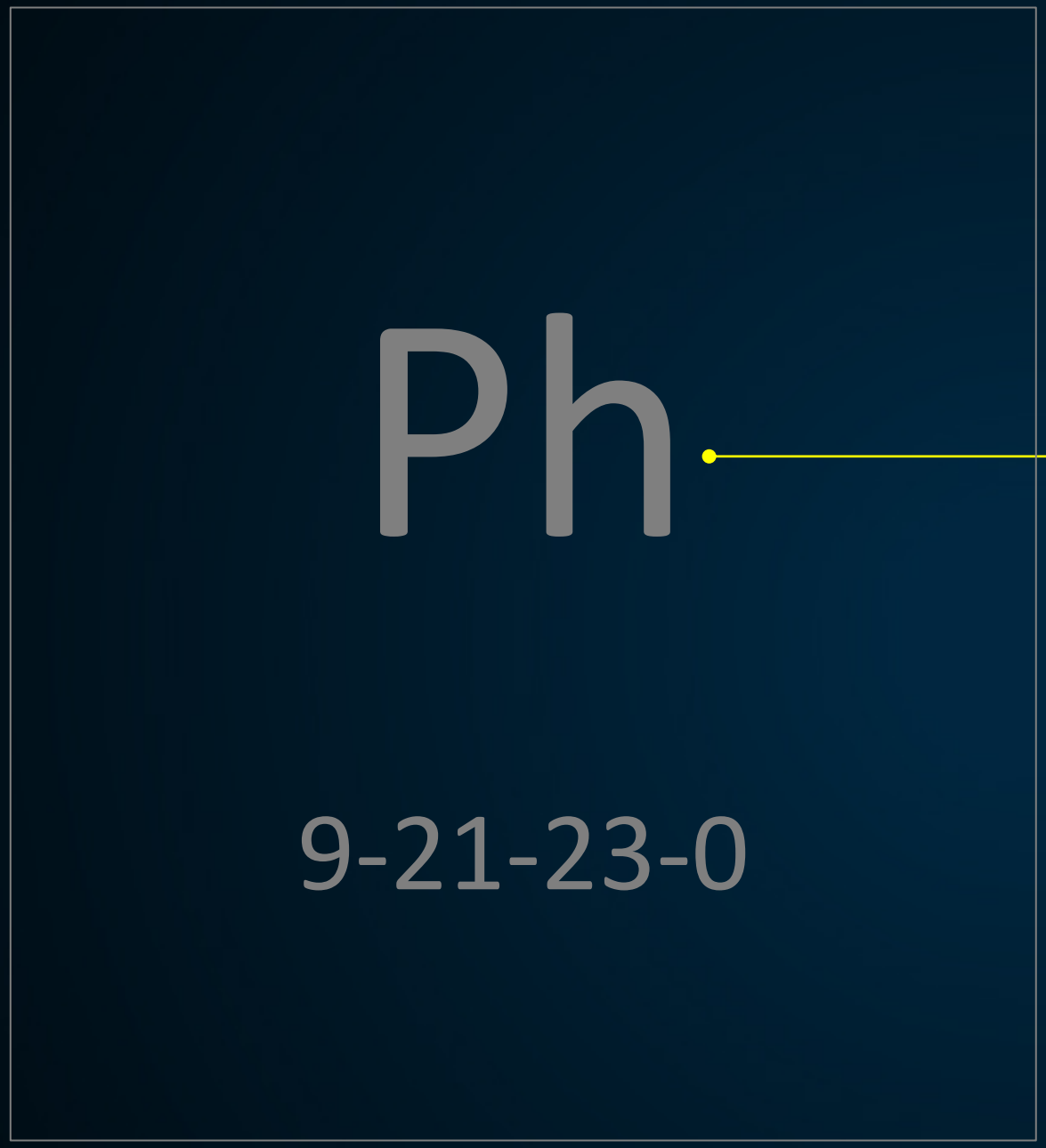
T1536	Defense Evasion	Ex: 0
	Revert Cloud Instance	
Rules: 0		

T1519	Persistence	Ex: 0
	Emond	
Rules: 0		

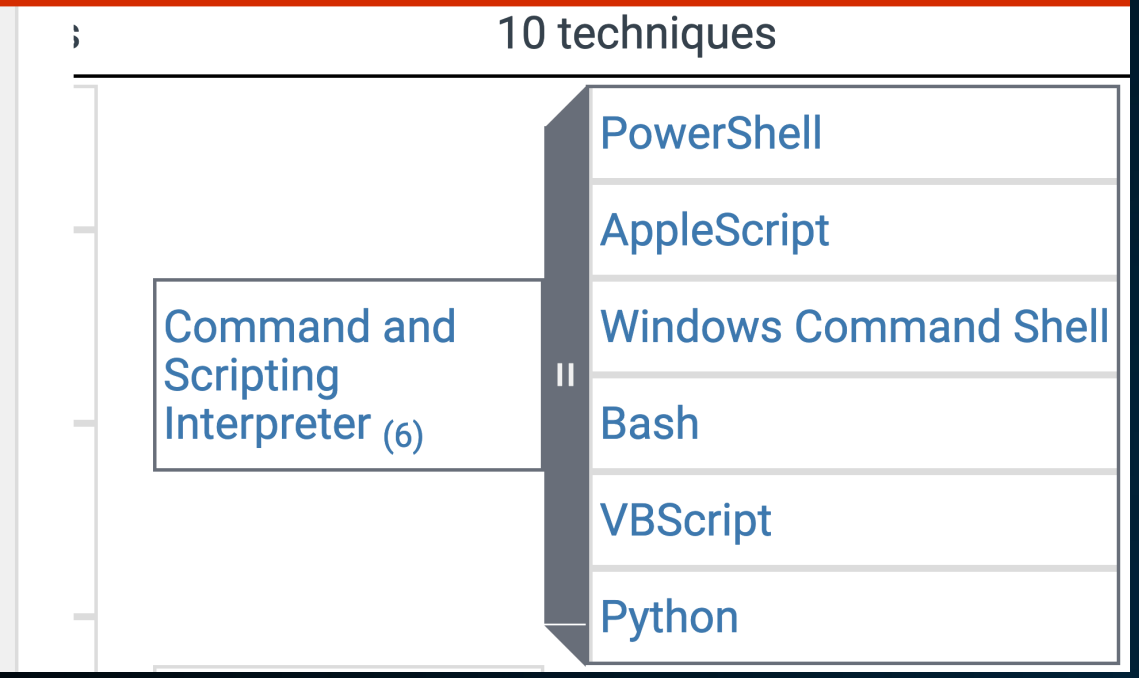
T1535	Defense Evasion	Ex: 0
	Unused/Unsupported Cloud Regions	
Rules: 0		

T1506	Defense Evasion	Ex: 0
	Web Session Cookie	
Rules: 0		

21 total, 23 examples, 0 sigma


Ph
Phantom
9-21-23-0

MITRE | ATT&CK®



C#

.NET

Command Interpreter
1 Tactic
1 Technique
285 examples
280 Sigma rules,

CI — Command Interpreter

1-2-285-280

CyberElements

Ex	Cl	Ph
6-6-55-104	1-2-285-280	9-21-23-0

Prioritized by Sightings, Examples and Sigma count

								<------ More Examples and Threat Hunting / Behavior based detection logic <---- | ----> Less or No Examples or no Detection Logic -------->									
Tactics	**Example Agnostic**							**Example Count and Threat Hunting based**									
Initial Access	Exploit	Remote Services	Valid Accounts	Drive-by Compromise	Phishing	Removable Media	Supply Chain Compromise	Hardware Additions	Trusted Relationship								
Execution	Exploit	Command Interpreter	WMI	Scheduled Task	User Execution	System Services	Native API	Inter-Process Communication	Shared Modules	Software Deployment Tools							
Persistence		Remote Services	Valid Accounts	Create Account	Scheduled Task	Create or Modify System Process	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Office Application Startup	Account Manipulation	Event Triggered Execution	Browser Extensions	BITS Jobs	Server Software Component	Hijack Execution Flow	Compromise Client Software Binary	Pre-OS Boot	Traffic Signaling
Discovery		Host Parameters	User Data	Network Specifics	Network Share	Network Service Scanning											
Privilege Escalation	Exploit	Valid Accounts	Scheduled Task	Process Injection	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Create or Modify System Process	Event Triggered Execution	Group Policy Modification	Hijack Execution Flow	Abuse Elevation Control Mechanism	Access Token Manipulation					
Defense Evasion	Exploit	Trusted Developer Utilities Proxy Execution	Valid Accounts	Obfuscated Information	Modify Registry	Process Injection	Access Token Manipulation	Subvert Trust Controls	Abuse Elevation Control Mechanism	Modify Authentication Process	Direct Volume Access	BITS Jobs	Execution Guardrails	File and Directory Permissions Modification	Group Policy Modification	Hide Artifacts	Indirect Command Execution	
		Masquerading	Indicator Removal on Host	Decode Information	Signed Binary Proxy Execution	Signed Script Proxy Execution	Impair Defenses	Hijack Execution Flow	Rootkit	Pre-OS Boot	Template Injection	Traffic Signaling	Use Alternate Authentication Material	XSL Script Processing	Virtualization / Sandbox Evasion	Rogue Domain Controller		
Credential Access	Exploit	Clear Text Credentials	Brute Force	Credential Extraction	Kerberos	Man-in-the-Middle	Removable Media	Forced Authentication	Modify Authentication Process	Input Capture	Web Session Cookie	2FA Interception						
Lateral Movement	Exploit	Remote Services	Lateral Tool Transfer (ex Remote File Copy)	Use Alternate Authentication Material	Removable Media	Phishing	Taint Shared Content	Software Deployment Tools	Remote Service Session Hijacking									
Collection		Data from Local System	Data from Network Shared Drive	Email	Man-in-the-Middle	Removable Media	Data from Information Repositories	Archive Collected Data	Data Staged	Man in the Browser	Input Capture	Clipboard Data	Screen Capture	Video Capture	Audio Capture	Automated Collection		
Command and Control			Application Layer Protocol	Ingress Tool Transfer (ex Remote File Copy)	Data Obfuscation	Web Service	Data Encoding	Encrypted Channel	Proxy	Fallback Channels	Non-Application Layer Protocol	Non-Standard Port	Protocol Tunneling	Dynamic Resolution	Remote Access Software	Traffic Signaling	Multi-Stage Channels	
Exfiltration		C2 Channel	Alternative Protocol	Web Service	Automated Exfiltration	Data Transfer Size Limits	Other Network Medium	Scheduled Transfer	Physical Medium									
Impact		Data Encrypted for Impact	Service Stop	Network Denial of Service	Account Access Removal	Data Manipulation	Data Destruction	System Shutdown / Reboot	Defacement	Disk Wipe	Endpoint DoS	Inhibit System Recovery	Resource Hijacking	Firmware Corruption				

ATT&CK® BLOG ARCHIVES GETTING STARTED | ATT&CK

Automating Mapping to ATT&CK: The Threat Report ATT&CK Mapper (TRAM) Tool

Sarah Yoder Following
Dec 20, 2019 · 7 min read

TRAM is a web-based tool that automates the extraction of adversary behaviors for the purpose of mapping them to ATT&CK.

ATT&CK® BLOG ARCHIVES GETTING STARTED | ATT&CK

Building an ATT&CK Sightings Ecosystem

John Wunder Follow
Feb 28, 2019 · 3 min read

People love that ATT&CK is driven by real data. It's not a theoretical set of possible things adversaries **could** do, it's a compendium of things adversaries have **actually** done.

SOC PRIME

Do not exclude.
Prioritize.

/Be safe

twitter @andriinb

SOC PRIME

Sigma @ ATT&CK for Cloud

Filter result | Platform: Sigma | Cloud: AWS | Azure | Azure AD | GCP | Office 365 | SaaS | Sigma Type: Threat Hunting Sigma | Compliance

111 Rules | 111 Sigma Rules | 20 Log Sources | 3 Tools | 10 Actors | 36 Techniques

101 | 10 | 111

Recommended

Possible SCAM/SPAM or Phishing via Calendar (via gsuite)

95 16 0

by: SOC Prime Team Type: Rule Released: 22 Oct 2019

Updated: 9 Apr 2020

Details | View

Context

10 Jun 2019 #threatintel

17 Jun 2019 Media

Severity (via gsuite)	Rule	1
Interactive Logon to Server Systems	Rule	1
GCP Service Account Created (via gcpaudit)	Rule	1
Possible PowerUpSQL module usage (via cmdline)	Rule	1
AWS Root Credentials	Rule	1
Network Successful login with Built-in Accounts	Rule	1
Azure AD Failed Logins	Rule	1
Multiple Failed Logins with Different Accounts from Single Source System	Rule	1
Remote access to SSH, FTP, SFTP applications	Rule	1

T1192	Initial Access	Ex: 21	T1136	Persistence	Ex: 16
Spearphishing Link			Create Account		
Rules: 20		May 18, 2020	Rules: 9		Apr 16, 2020
T1189	Initial Access	Ex: 16	T1098	Persistence	Ex: 7
Drive-by Compromise			Account Manipulation		
Rules: 5		Apr 01, 2020	Rules: 37		Apr 30, 2020
T1190	Initial Access	Ex: 5	T1108	Persistence	Ex: 8
Exploit Public-Facing Application			Redundant Access		
Rules: 56		May 18, 2020	Rules: 3		May 14, 2020

T1108	Defense Evasi				
Redundant A					
Rules: 3					
T1527	Defense Evasi				
Application A					
Rules: 4					
T1536	Defense Evasi				
Revert Cloud					
Rules: 0					