GRIMMCon 0×7

Control Validation Compass

Intelligence for Improved Security Validation

Scott Small

Cybersecurity practitioner /
consultant / therapist /
field guide

OSINT & tech for risk reduction

twitter.com/IntelScott

github.com/TropChaud

MITRE ATT&CK™

Catalog of adversary behavior

Ends

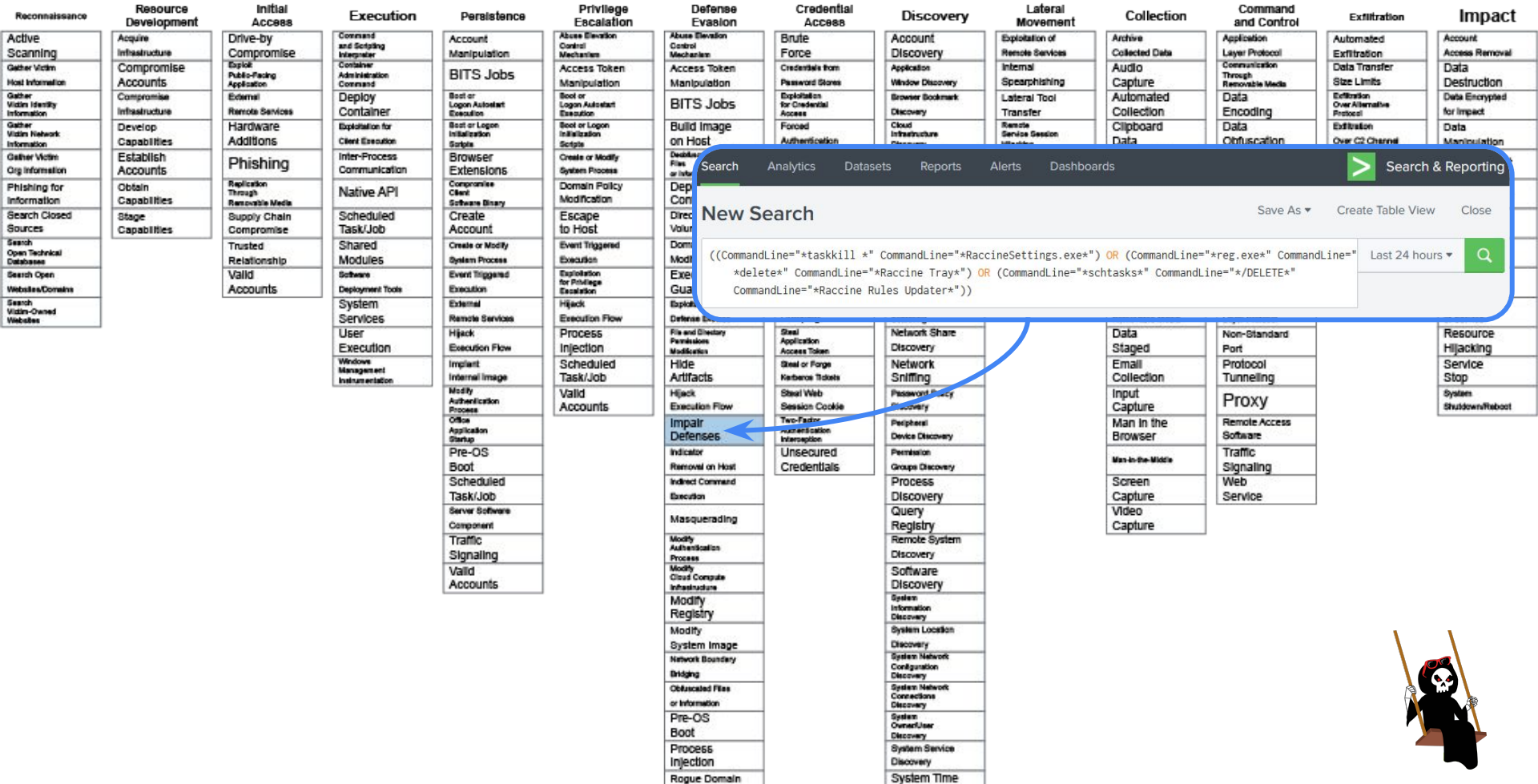
Means

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	and Scripting Interpreter	Account Manipulation	Control Mechanism	Control Mechanism	Adversary-in-the-Middle	Account Discovery	Remote Services
Exploit Public Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing
External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking
Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media
Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools
Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content
Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material
	System Services	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Request Generation	Domain Trust Discovery	
	User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	
	Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions Modification	OS Credential Dumping	Group Policy Discovery	
		Modify Authentication Process	Valid Accounts	Hide Artifacts	Steal Application Access Token	Network Service Discovery	
		Office Application Startup		Hijack Execution Flow	Steal or Forge Kerberos Tickets	Network Share Discovery	
		Pre-OS Boot		Impair Defenses	Steal Web Session Cookie	Network Sniffing	
		Scheduled Task/Job		Indicator Removal on Host	Unsecured Credentials	Password Policy Discovery	
		Server Software		Indirect Command		Peripheral	

Hunting for Post-Exploitation Stage Attacks with Elastic Stack and the MITRE ATT&CK Framework:

https://www.youtube.com/watch?v=PdCQChYrxXg

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	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
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	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
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	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
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Input Capture	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Man-in-the-Middle	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal Application Access Token	Network Share Discovery		Data Staged	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal or Forge Kerberos Tickets	Network Sniffing		Email Collection	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Steal Web Session Cookie	Password Policy Discovery		Input Capture	Proxy		System Shutdown/Reboot
				Office Application Startup		Impair Defenses	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Permission Groups Discovery		Man-in-the-Middle	Traffic Signaling		
				Scheduled Task/Job		Indirect Command Execution		Process Discovery		Screen Capture	Web Service		
				Server Software Component		Masquerading		Query Registry		Video Capture			
				Traffic Signaling		Modify Authentication Process		Remote System Discovery					
				Valid Accounts		Modify Cloud Compute Infrastructure		Software Discovery					
						Modify Registry		System Information Discovery					
						Modify System Image		System Location Discovery					
						Network Boundary Bridging		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		System Time					


Reconnaissance
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites
Resource Development
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
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
Container Administration Command
Deploy Container
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
Implant Internal Image
Modify Authentication Process
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
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal on Host
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information
Pre-OS Boot
Process Injection
Rogue Domain
Credential Access
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Steal Application Access Token
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure
Network Share Discovery
Network Sniffing
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session
Collection
Archive Collected Data
Audio Capture
Automated Collection
Clipboard Data
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
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
Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Resource Hijacking
Service Stop
System Shutdown/Reboot
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
((CommandLine="*taskkill *" CommandLine="*RaccineSettings.exe*") OR (CommandLine="*reg.exe*" CommandLine="*delete*" CommandLine="*Raccine Tray*") OR (CommandLine="*schtasks*" CommandLine="*/DELETE*" CommandLine="*Raccine Rules Updater*"))
Last 24 hours

```
index=__your_sysmon_index__ EventCode=1 Image="C:\\Windows\\*\\powershell.exe" ParentImage!="C
    :\\Windows\\explorer.exe"|stats values(CommandLine) as "Command Lines" values(ParentImage) as "Pa
    Images" by ComputerName
```

```
(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" (DestinationPort="3389" EventCode="3" Initiated="true") NOT ((Image="*\\mstsc.exe" OR Image="*\\RTSApp.exe" OR Image="
    *\\RTS2App.exe" OR Image="*\\RDCMan.exe" OR Image="*\\ws_TunnelService.exe" OR Image="*\\RSSensor.exe" OR Image="*\\RemoteDesktopManagerFree.exe" OR Image="*\\RemoteDesktopManager
    .exe" OR Image="*\\RemoteDesktopManager64.exe" OR Image="*\\mRemoteNG.exe" OR Image="*\\mRemote.exe" OR Image="*\\Terminals.exe" OR Image="*\\spiceworks-finder.exe" OR Image="
    *\\FSDiscovery.exe" OR Image="*\\FSAssessment.exe" OR Image="*\\MobaRTE.exe" OR Image="*\\chrome.exe" OR Image="*\\thor.exe" OR Image="*\\thor64.exe")))
```

```
(source="WinEventLog:Security" EventCode="4704" (Message="*SeEnableDelegationPrivilege*"))
```

```
(source="WinEventLog:Security" (EventCode="4625" OR EventCode="4776") (Status="0xC000006F" OR Status="0xC0000070" OR Status="0xC0000413" OR Status="0xC000018C" OR Status
    ="0xC000015B"))
```

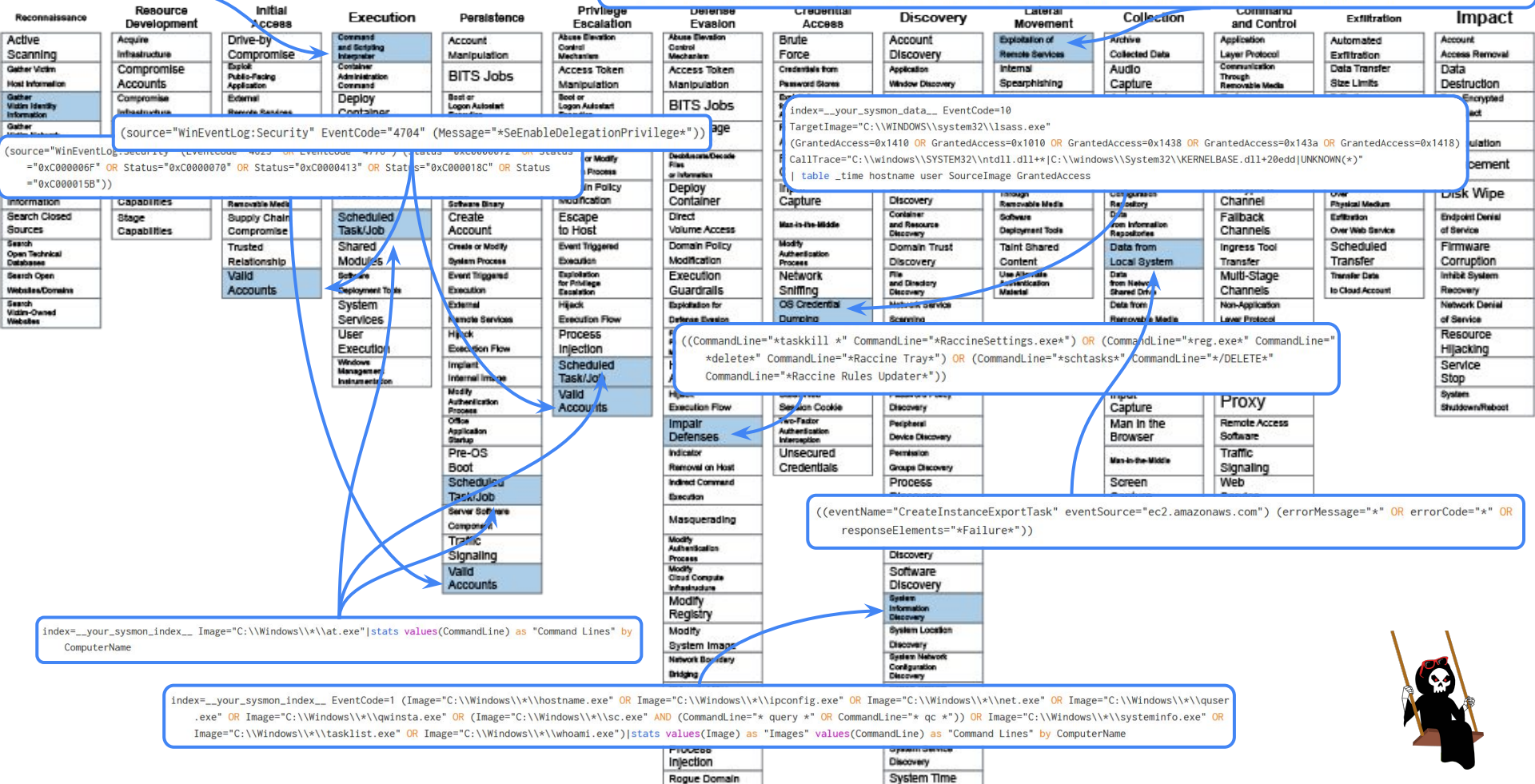
```
index=__your_sysmon_data__ EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
| table _time hostname user SourceImage GrantedAccess
```

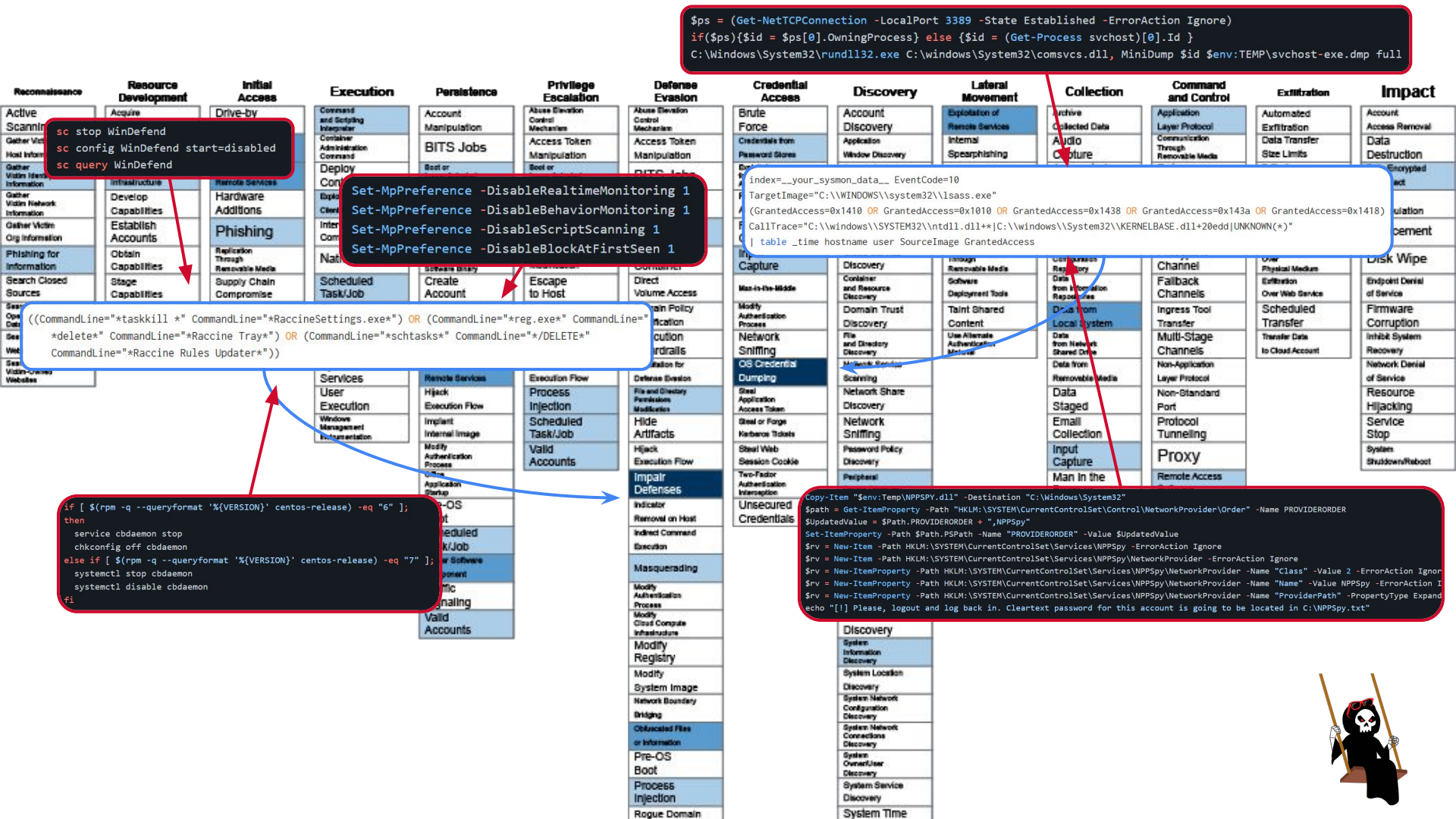
```
((CommandLine="*taskkill *" CommandLine="*RaccineSettings.exe*") OR (CommandLine="*reg.exe*" CommandLine="
    *delete*" CommandLine="*Raccine Tray*") OR (CommandLine="*schtasks*" CommandLine="*/DELETE*"
    CommandLine="*Raccine Rules Updater*"))
```

```
((eventName="CreateInstanceExportTask" eventSource="ec2.amazonaws.com") (errorMessage="*" OR errorCode="*" OR
    responseElements="*Failure*"))
```

```
index=__your_sysmon_index__ Image="C:\\Windows\\*\\at.exe"|stats values(CommandLine) as "Command Lines" by
    ComputerName
```

```
index=__your_sysmon_index__ EventCode=1 (Image="C:\\Windows\\*\\hostname.exe" OR Image="C:\\Windows\\*\\ipconfig.exe" OR Image="C:\\Windows\\*\\net.exe" OR Image="C:\\Windows\\*\\quser
    .exe" OR Image="C:\\Windows\\*\\qwinsta.exe" OR (Image="C:\\Windows\\*\\sc.exe" AND (CommandLine="* query *" OR CommandLine="* qc *")) OR Image="C:\\Windows\\*\\systeminfo.exe" OR
    Image="C:\\Windows\\*\\tasklist.exe" OR Image="C:\\Windows\\*\\whoami.exe")|stats values(Image) as "Images" values(CommandLine) as "Command Lines" by ComputerName
```




$ps = (Get-NetTCPConnection -LocalPort 3389 -State Established -ErrorAction Ignore)
if($ps){$id = $ps[0].OwningProcess} else {$id = (Get-Process svchost)[0].Id }
C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump $id $env:TEMP\svchost-exe.dmp full
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
sc stop WinDefend
sc config WinDefend start=disabled
sc query WinDefend
Set-MpPreference -DisableRealtimeMonitoring 1
Set-MpPreference -DisableBehaviorMonitoring 1
Set-MpPreference -DisableScriptScanning 1
Set-MpPreference -DisableBlockAtFirstSeen 1
index=__your_sysmon_data__ EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
| table _time hostname user SourceImage GrantedAccess
((CommandLine="*taskkill *" CommandLine="*RaccineSettings.exe*") OR (CommandLine="*reg.exe*" CommandLine="*delete* CommandLine="*Raccine Tray*") OR (CommandLine="*schtasks*" CommandLine="*/DELETE*" CommandLine="*Raccine Rules Updater*"))
if [$(rpm -q --queryformat '%{VERSION}' centos-release) -eq "6"];
then
service cbdaemon stop
chkconfig off cbdaemon
else if [$(rpm -q --queryformat '%{VERSION}' centos-release) -eq "7"];
systemctl stop cbdaemon
systemctl disable cbdaemon
fi
Copy-Item "$env:Temp\NPPSPY.dll" -Destination "C:\Windows\System32"
$path = Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order" -Name PROVIDERORDER
$UpdatedValue = $Path.PROVIDERORDER + ",NPPSpy"
Set-ItemProperty -Path $Path.PSPath -Name "PROVIDERORDER" -Value $UpdatedValue
$rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy -ErrorAction Ignore
$rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -ErrorAction Ignore
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "Class" -Value 2 -ErrorAction Ignor
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "Name" -Value NPPSpy -ErrorAction I
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "ProviderPath" -PropertyType Expand
echo "[!] Please, logout and log back in. Cleartext password for this account is going to be located in C:\NPPSpy.txt"

Nearly 600 techniques & sub-techniques

9,000+ detection rules, **2,100+** tests

```
index=__your_sysmon_index__ EventCode=1 Image="C:\\Windows\\*\\powershell.exe" ParentImage!="C
    :\\Windows\\explorer.exe"|stats values(CommandLine) as "Command Lines" values(ParentImage) as "Parent
    Images" by ComputerName
```

```
(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" (DestinationPort="3389" EventCode="3" Initiated="true") NOT ((Image="*\\mstsc.exe" OR Image="*\\RTSApp.exe" OR Image="
    *\\RTS2App.exe" OR Image="*\\RDCMan.exe" OR Image="*\\ws_TunnelService.exe" OR Image="*\\RSSensor.exe" OR Image="*\\RemoteDesktopManagerFree.exe" OR Image="*\\RemoteDesktopManager
    .exe" OR Image="*\\RemoteDesktopManager64.exe" OR Image="*\\mRemoteNG.exe" OR Image="*\\mRemote.exe" OR Image="*\\Terminals.exe" OR Image="*\\spiceworks-finder.exe" OR Image="
    *\\FSDiscovery.exe" OR Image="*\\FSAssessment.exe" OR Image="*\\MobaRTE.exe" OR Image="*\\chrome.exe" OR Image="*\\thor.exe" OR Image="*\\thor64.exe")))
```

```
index=__your_sysmon_data__ EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
| table _time hostname user SourceImage GrantedAccess
```

```
(source="WinEventLog:Security" EventCode="4704" (Message="*SeEnableDelegationPrivilege*"))
```

```
(source="WinEventLog:Security" (EventCode="4625" OR EventCode="4776") (Status="0xC0000072" OR Status
    ="0xC000006F" OR Status="0xC0000070" OR Status="0xC0000413" OR Status="0xC000018C" OR Status
    ="0xC000015B"))
```

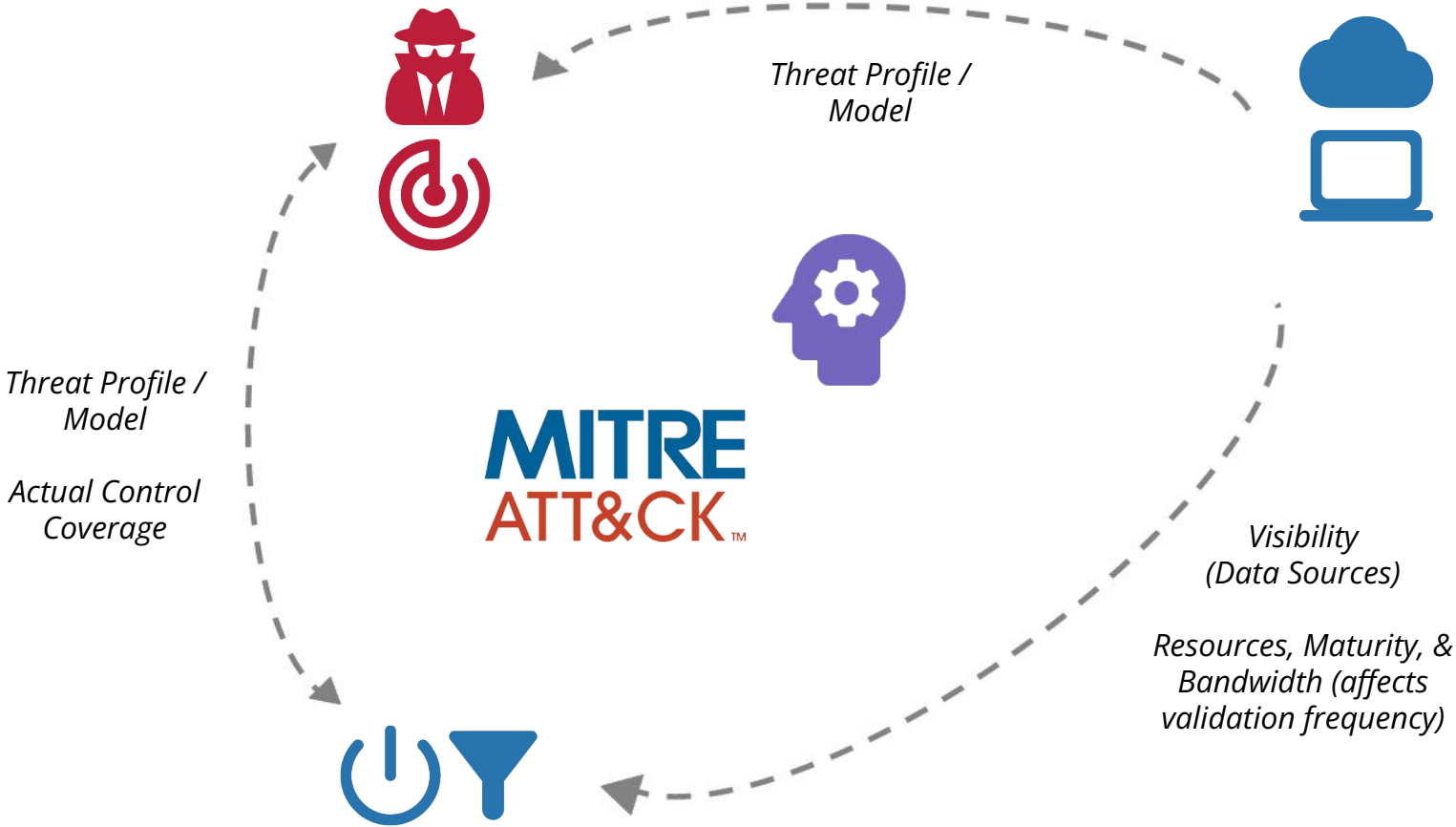
```
((CommandLine="*taskkill *" CommandLine="*RaccineSettings.exe*") OR (CommandLine="*reg.exe* CommandLine="
    *delete* CommandLine="*Raccine Tray*") OR (CommandLine="*schtasks* CommandLine="*/DELETE*"
    CommandLine="*Raccine Rules Updater*"))
```

```
((eventName="CreateInstanceExportTask" eventSource="ec2.amazonaws.com") (errorMessage="*" OR errorCode="*" OR
    responseElements="*Failure*"))
```

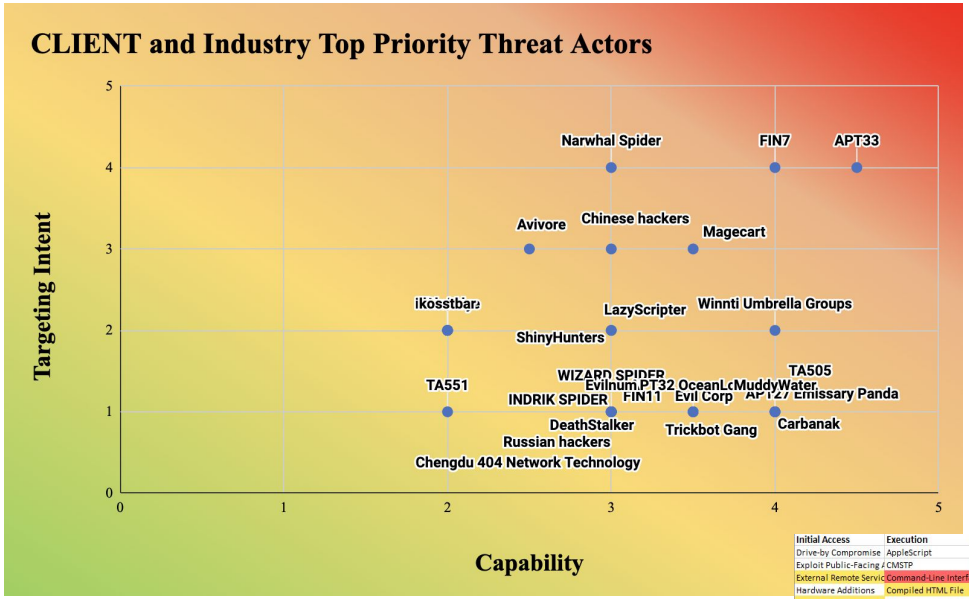
```
index=__your_sysmon_index__ Image="C:\\Windows\\*\\at.exe"|stats values(CommandLine) as "Command Lines" by
    ComputerName
```

```
index=__your_sysmon_index__ EventCode=1 (Image="C:\\Windows\\*\\hostname.exe" OR Image="C:\\Windows\\*\\ipconfig.exe" OR Image="C:\\Windows\\*\\net.exe" OR Image="C:\\Windows\\*\\quser
    .exe" OR Image="C:\\Windows\\*\\qwinsta.exe" OR (Image="C:\\Windows\\*\\sc.exe" AND (CommandLine="* query *" OR CommandLine="* qc *")) OR Image="C:\\Windows\\*\\systeminfo.exe" OR
    Image="C:\\Windows\\*\\tasklist.exe" OR Image="C:\\Windows\\*\\whoami.exe")|stats values(Image) as "Images" values(CommandLine) as "Command Lines" by ComputerName
```

Prioritizing Detections: Risk Profiling



Resistance Isn't Futile - Katie Nickels (Shmoocon 2020):
https://www.youtube.com/watch?v=b0ShMaKDidU



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Contr	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bas	Access Token Manipul	Access Token Manipul	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Remov
Exploit Public-Facing A	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window D	Application Deployme	Automated Collection	Communication Throu	Data Compressed	Data Destruction
External Remote Servic	Command-Line Interfa	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Dis	Component Object Mo	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Imp
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account C	Credential Dumping	Domain Trust Discover	Exploitation of Remote	Data from Information	Custom Command and	Data Transfer Size Limi	Defacement
Replication Through R	Component Object Mo	AppInit DLLs	Application Shimming	Clear Command Histor	Credentials from Web	File and Directory Disc	Internal Spearphishing	Data from Local Syster	Custom Cryptographic	Exfiltration Over Alterr	Disk Content Wipe
Spearphishing Attachi	Control Panel Items	Application Shimming	Bypass User Account C	CMSTP	Credentials in Files	Network Service Scann	Logon Scripts	Data from Network Sha	Data Encoding	Exfiltration Over Comm	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchang	Authentication Packag	DLL Search Order Hijac	Code Signing	Credentials in Registry	Network Share Discove	Pass the Hash	Data from Removable I	Data Obfuscation	Exfiltration Over Other	Endpoint Denial of Ser
Spearphishing via Ser	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Crede	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physi	Firmware Corruption
Supply Chain Compror	Execution through Mod	Bootkit	Elevated Execution wit	Compiled HTML File	Forced Authentication	Password Policy Disco	Remote Desktop Protoc	Email Collection	Domain Generation Al	Scheduled Transfer	Inhibit System Recover
Trusted Relationship	Exploitation for Client	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Disc	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Serv
Valid Accounts	Graphical User Interfa	Change Default File As	Exploitation for Privile	Component Object Mo	Input Capture	Permission Groups Dis	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory	Connection Proxy	Input Prompt	Process Discovery	Replication Through R	Screen Capture	Multi-Stage Channels		Runtime Data Manipul
	Launchctl	Component Object Mo	File System Permissior	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discov	SSH Hijacking		Multilayer Encryption		Stored Data Manipulat
	LSASS Driver	DLL Search Order Hijac	Image File Execution O	Deobfuscate/Decode F	LLMNR/NBT-NS Poison	Security Software Disc	Taint Shared Content		Port Knocking		System Shutdown/Rebo
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Too	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Man
	PowerShell	Emond	New Service	DLL Search Order Hijac	Password Filter DLL	System Information Di	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Servic	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Config	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissior	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Direc	Plist Modification	Exploitation for Defens	Steal Web Session Coo	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory	Two-Factor Authentica	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution O	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Ex	Kernel Modules and Ex	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Ex	Launch Agent	Service Registry Permi	Gatekeeper Bypass							
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Additic	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Sudo	Hidden Window							
	Trusted Developer Util	Login Item	Sudo Caching	HISTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Managemen	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Remote Man	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							

https://github.com/splunk/security_content

README.md

Splunk Security Content

Welcome to the Splunk Security Content

This project gives you access to our repository of A
on tactics, techniques and procedures (TTPs), map
Martin Cyber Kill Chain, and CIS Controls. They incl
Splunk Phantom playbooks (where available)—all d
respond to threats.

Get Content

The latest Splunk Security Content can be obtainec

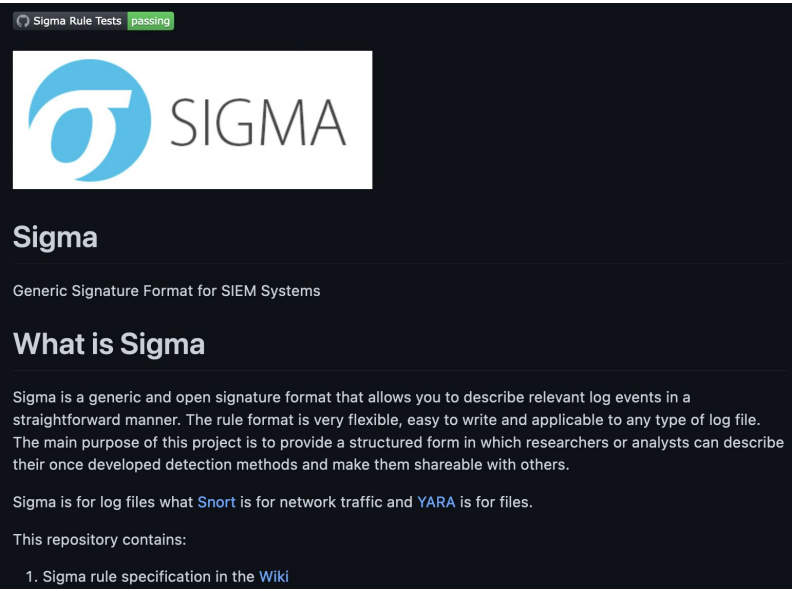
SSE App

Grab the latest release of Splunk Security Essential
it from splunkbase, it is a Splunk Supported App. S
content release, this is the **preferred way** to get co

```yaml
name: AdsiSearcher Account Discovery
id: de7fcadc-04f3-11ec-a241-acde48001122
version: 1
date: '2021-08-24'
author: Teoderick Contreras, Mauricio Velazco, Splunk
type: TTP
datamodel: []
description: The following analytic utilizes PowerShell Script Block Logging (EventCode=4104)
  to identify the `[Adsisearcher]` type accelerator being used to query Active Directory
  for domain groups. Red Teams and adversaries may leverage `[Adsisearcher]` to enumerate
  domain users for situational awareness and Active Directory Discovery.
search: '`powershell` EventCode=4104 Message = "*[adsisearcher]*" Message = "*objectcategory=user*"
  Message = "*.findAll()*" | stats count min(_time) as firstTime max(_time) as lastTime
  by EventCode Message ComputerName User | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
  | `adsisearcher_account_discovery_filter`'
how_to_implement: The following Hunting analytic requires PowerShell operational logs
  to be imported. Modify the powershell macro as needed to match the sourcetype or
  add index. This analytic is specific to 4104, or PowerShell Script Block Logging.
known_false_positives: Administrators or power users may use this command for troubleshooting.
references:
- https://attack.mitre.org/techniques/T1087/002/
- https://www.blackhillsinfosec.com/red-blue-purple/
- https://devblogs.microsoft.com/scripting/use-the-powershell-adsisearcher-type-accelerator-to-search-active-directory/
tags:
  analytic_story:
  - Industroyer2
  - Active Directory Discovery
  confidence: 50
  context:
  - Source:Endpoint
  - Stage:Discovery
  dataset:
  - https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techniques/T1087.002/AD_discovery/wi
  impact: 50
  kill_chain_phases:
  - Reconnaissance
  message: powershell process having commandline $Message$ for user enumeration
  mitre_attack_id:
  - T1087.002
  - T1087
  observable:
  - name: ComputerName
```

techID	techName	splunk
T1001	Data Obfuscation	
T1001.001	Junk Data	
T1001.002	Steganography	
T1001.003	Protocol Impersonation	
T1003	OS Credential Dumping	41
T1003.001	LSASS Memory	14
T1003.002	Security Account Manage	12
T1003.003	NTDS	7
T1003.004	LSA Secrets	
T1003.005	Cached Domain Credenti	
T1003.006	DCSync	
T1003.007	Proc Filesystem	
T1003.008	/etc/passwd and /etc/sha	1
T1005	Data from Local System	1
T1006	Direct Volume Access	
T1007	System Service Discovery	2
T1008	Fallback Channels	
T1010	Application Window Disc	
T1011	Exfiltration Over Other N	
T1011.001	Exfiltration Over Bluetoo	
T1012	Query Registry	1
T1014	Rootkit	
T1016	System Network Configu	3
T1016.001	Internet Connection Disc	1
T1018	Remote System Discover	15
T1020	Automated Exfiltration	5
T1020.001	Traffic Duplication	
T1021	Remote Services	19
T1021.001	Remote Desktop Protoco	2
T1021.002	SMB/Windows Admin Sh	6
T1021.003	Distributed Component C	5
T1021.004	SSH	

https://github.com/SigmaHQ/sigma



techID	techName	splunk	sigma
T1001	Data Obfuscation		
T1001.001	Junk Data		
T1001.002	Steganography		
T1001.003	Protocol Impersonation		3
T1003	OS Credential Dumping	41	14
T1003.001	LSASS Memory	14	62
T1003.002	Security Account Manage	12	27
T1003.003	NTDS	7	18
T1003.004	LSA Secrets		12
T1003.005	Cached Domain Credenti		8
T1003.006	DCSync		8
T1003.007	Proc Filesystem		1
T1003.008	/etc/passwd and /etc/sha	1	
T1005	Data from Local System	1	7
T1006	Direct Volume Access		1
T1007	System Service Discovery	2	3
T1008	Fallback Channels		2
T1010	Application Window Disc		1
T1011	Exfiltration Over Other N		
T1011.001	Exfiltration Over Bluetoo		
T1012	Query Registry	1	11
T1014	Rootkit		
T1016	System Network Configu	3	8
T1016.001	Internet Connection Disc	1	
T1018	Remote System Discover	15	14
T1020	Automated Exfiltration	5	5
T1020.001	Traffic Duplication		
T1021	Remote Services	19	2
T1021.001	Remote Desktop Protoco	2	11
T1021.002	SMB/Windows Admin Sh	6	30
T1021.003	Distributed Component C	5	8
T1021.004	SSH		

DeTT&CT

https://github.com/rabobank-cdc/DeTTECT

techID	techName	splunk	splunk	elastic	eql	an	azure	azure	logpoir	proofp	tanium	aws	gcp	car	atc	sigma	playbo	art	car_red	rta	prelude	stockoile	scythe	mitieat	nist	cis	d3fend	engage	policy
T1040	Network Sniffing		3	1			8	1	3		5	5			1	2	7		8			1	1		2	11	11	1	12	3
T1046	Network Service Scannin	2				1	5		28	2		6	1	2	1	1			4	1			3	6	3	11	13		11	3
T1052	Exfiltration Over Physical								2																2	10	8	1	11	3
T1078	Valid Accounts	53		38			16		24			8			6	2					1		15		3	24	46	12	11	3
T1083	File and Directory Discov	1		1			2		5		2				1	8			4			4	33					11	2
T1020	Automated Exfiltration	3		1					6			3			2	6			1				3					8	10	2
T1135	Network Share Discovery	3	2	2	2		1	2	2						2	7			7		1	2	2	5	1	3			10	2
T1007	System Service Discovery	2	1					1	3					2	1	3	1		2	1	1	1	1	11					9	2
T1011	Exfiltration Over Other N														1														9	3
T1029	Scheduled Transfer											1		1						1			1		1	7	1	8	9	3
T1041	Exfiltration Over C2 Chan						2		8		22	3			2	3			1			3	1	19	1	5	1	12	9	3
T1048	Exfiltration Over Alternat	15		2			8		5		2	4			4	18			3						3	12	8	13	9	3
T1072	Software Deployment To	1					3					1				1			2			2			9	24	42	5	9	3
T1530	Data from Cloud Storage	2		5			6					8	9												6	33	47		9	3
T1537	Transfer Data to Cloud Ac	2		6			2					1				4							1		3	20	14		9	3
T1567	Exfiltration Over Web Ser	2					2		1			2				4			1						1	3		9	9	3
T1005	Data from Local System	1		2			2				1					6						2	6	8					8	2
T1016	System Network Configu	3	1	2	2		1	1	2		3			2		8			8	1	1	2	7	39					8	2
T1030	Data Transfer Size Limits								1							2			1				1		1	7	1	8	8	3
T1047	Windows Management In	1	5	5	2		3	5	9	1	9			3	1	35	3		9		2		2	11	2	8	17		8	3
T1049	System Network Connect	5	1	1	2		1	1	2					1	1	8			4	1	1	4	1	10					8	2
T1068	Exploitation for Privilege	9		1			13		12		3	3		1	3	19								2	4	25	6	6	8	3
T1091	Replication Through Rem								1							1			2						2	10	11	1	8	3
T1092	Communication Through																								2	8	10	1	8	3
T1125	Video Capture						1									1												2	8	2
T1133	External Remote Services			4			1		4			4	1			4			2						4	18	29	13	8	3
T1555	Credentials from Passwo	9		1			7		2		3	1				4			5					1	3	3			8	2
T1602	Data from Configuration						2					1													7	25			8	3
T1003	OS Credential Dumping	67	5	8	6		6	5	48	11	2	1			44	7	5		3			1	1	2	8	21	24	26	7	3
T1018	Remote System Discover	15	2	4	2		2	2	4		3	2	1	1	1	1			14	1	1	3	8	8					7	2
T1033	System Owner/User Disc	8	2	3	2			1	4		4			2	3	13			3	1		1	4	26					7	2
T1039	Data from Network Share	3							1					1		2												1	7	2
T1080	Taint Shared Content						3																		3	10	8	1	7	3
T1087	Account Discovery	56	1	3	2		6	1	8		7	1			8	15					1		9		1	3	2		7	2
T1114	Email Collection	9			1		1		9						1	2						1			3	14	30	10	7	3
T1119	Automated Collection						2		2			1				5			4					1	2	17	8	3	7	3
T1123	Audio Capture	1	1	1	2		1	1	1		2				2	6	1		1									2	7	2
T1219	Remote Access Software			3			3		2			2			2	5														
T1552	Unsecured Credentials	5					6		6		3	7																		
T1566	Phishing	46		3			3		12		2	1																		
T1613	Container and Resource I											1																		
T1057	Process Discovery	2	1	1	2		2	1						2																
T1082	System Information Disco	1	1	4	3		2	1	4					2	1															
T1102	Web Service			1			1																							
T1113	Screen Capture	4		1			3		3																					
T1120	Peripheral Device Discov			1																										
T1132	Data Encoding																													
T1204	User Execution	24		2	1		4		5			31	1																	
T1213	Data from Information Re						5																							
T1217	Browser Bookmark Disco		1				1	1	1																					
T1485	Data Destruction	6		7			6		8		5	6																		

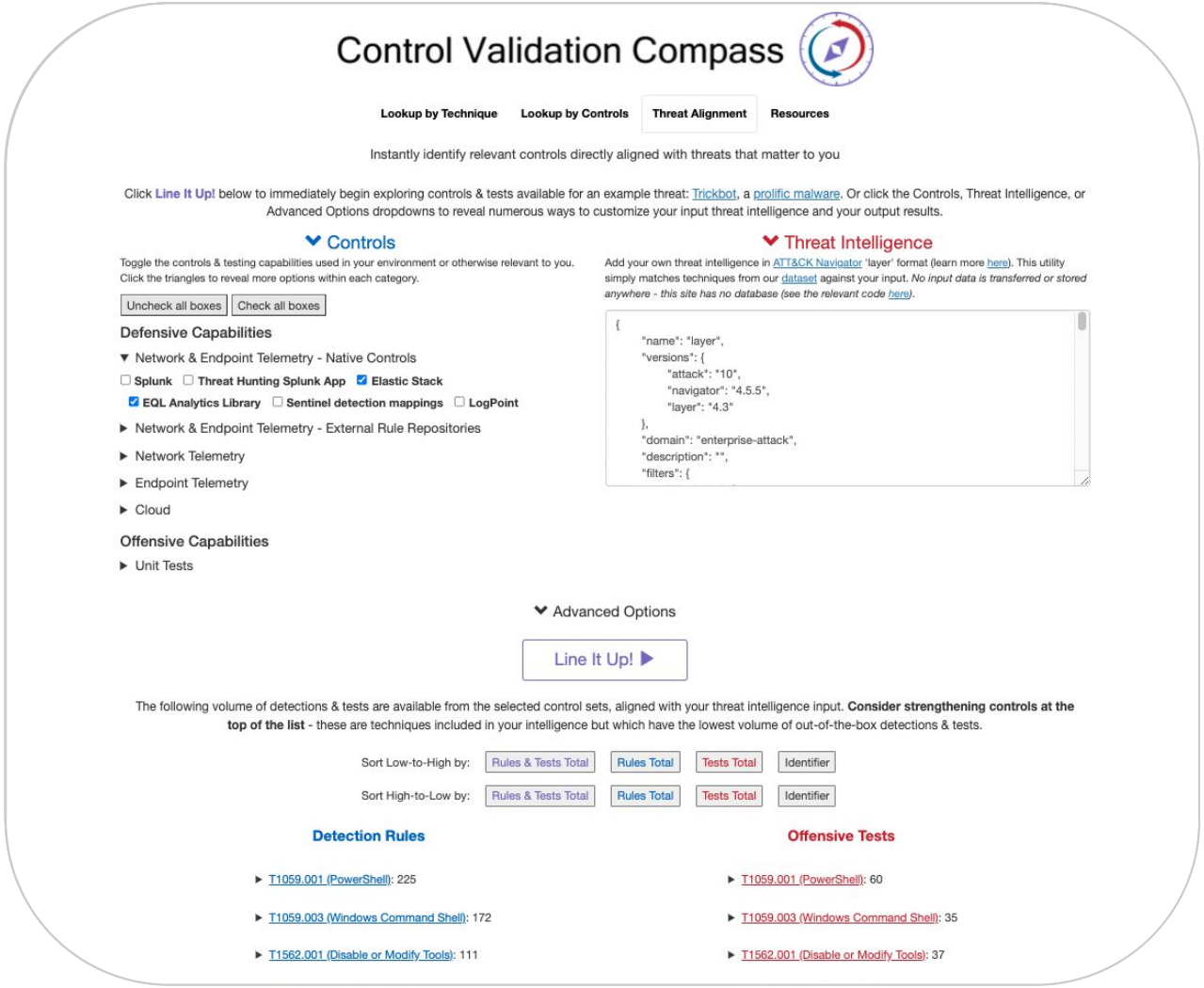
techID	techName	url	estLe	splu	splu	elas	eql	azur	azur	loop	proc	tanii	aws	gcp	car	atc	sigm	playb	art	ar re	rta	reluc	ockp	scyt	mitii	nist	cis	d3fe	enga	polic	dete	test
T1137.005	Outlook Rules	https://at	v					1																	1	2				1	1	0
T1137.006	Add-ins	https://at	v					1				1																1		1	1	1
T1149	LC_MAIN Hijacking	https://at	v																											0	0	0
T1153	Source	https://at	v																											0	0	0
T1175	Component Object M	https://at	v								3																			0	1	0
T1195.001	Compromise Software	https://at	v	2				2																						2	1	0
T1195.002	Compromise Software	https://at	v			4		1																						2	1	0
T1195.003	Compromise Hardwa	https://at	v																											2	0	0
T1204.001	Malicious Link	https://at	v					1				3																		2	1	0
T1204.002	Malicious File	https://at	v	4		4		3		2		28																		3	2	3
T1204.003	Malicious Image	https://at	v	7																										0	1	0
T1205.001	Port Knocking	https://at	v					2		2																				0	1	0
T1213.001	Confluence	https://at	v					1																						2	1	0
T1213.002	Sharepoint	https://at	v					3																						2	1	0
T1213.003	Code Repositories	https://at	v																											0	0	0
T1216.001	PubPrn	https://at	v																											2	0	1
T1218.001	Compiled HTML File	https://at	v	4		2				1		1																		2	2	3
T1218.002	Control Panel	https://at	v	1		1				3		7																		2	1	1
T1218.003	CMSTP	https://at	v	3						4		1																		2	1	1
T1218.004	InstallUtil	https://at	v	5		1				2		3																		2	1	1
T1218.005	Mshta	https://at	v	8		3		1		10		6																		2	1	1
T1218.007	Msiexec	https://at	v	1						1		1																		2	1	1
T1218.008	Odbcconf	https://at	v							1																				2	1	1
T1218.009	Regsvcs/Regasm	https://at	v	6						1		3																		2	1	1
T1218.010	Regsvr32	https://at	v	5		2				2		3																		1	2	1
T1218.011	Rundll32	https://at	v	16		3		1		9		19																		2	2	3
T1218.012	Verclsid	https://at	v	1						1																				2	1	1
T1218.013	Mavinject	https://at	v																											1	0	0
T1218.014	MMC	https://at	v																											1	0	0
T1222.001	Windows File and Dir	https://at	v	1				2		2															2	11				2	2	1
T1222.002	Linux and Mac File a	https://at	v					2				1													2	11				2	2	3
T1480.001	Environmental Keyin	https://at	v																						1					1	0	0
T1484	Domain Policy Modif	https://at	n	4				2		3															3	13				3	1	0
T1484.001	Group Policy Modific	https://at	v					2		2				1																0	1	0
T1484.002	Domain Trust Modific	https://at	v			1		2						4																0	2	1
T1491.001	Internal Defacement	https://at	v					1				3													8		10			2	1	2
T1491.002	External Defacement	https://at	v					1				3															10			2	1	0
T1497.001	System Checks	https://at	v																											2	1	3
T1497.002	User Activity Based C	https://at	v																											0	1	0
T1497.003	Time Based Evasion	https://at	v																											0	0	0
T1498.001	Direct Network Flood	https://at	v					2				4													1	8	9			3	1	0
T1498.002	Reflection Amplificat	https://at	v																											0	0	0

Prioritizing Detections: A Compass to Guide You

Control Validation Compass

controlcompass.github.io

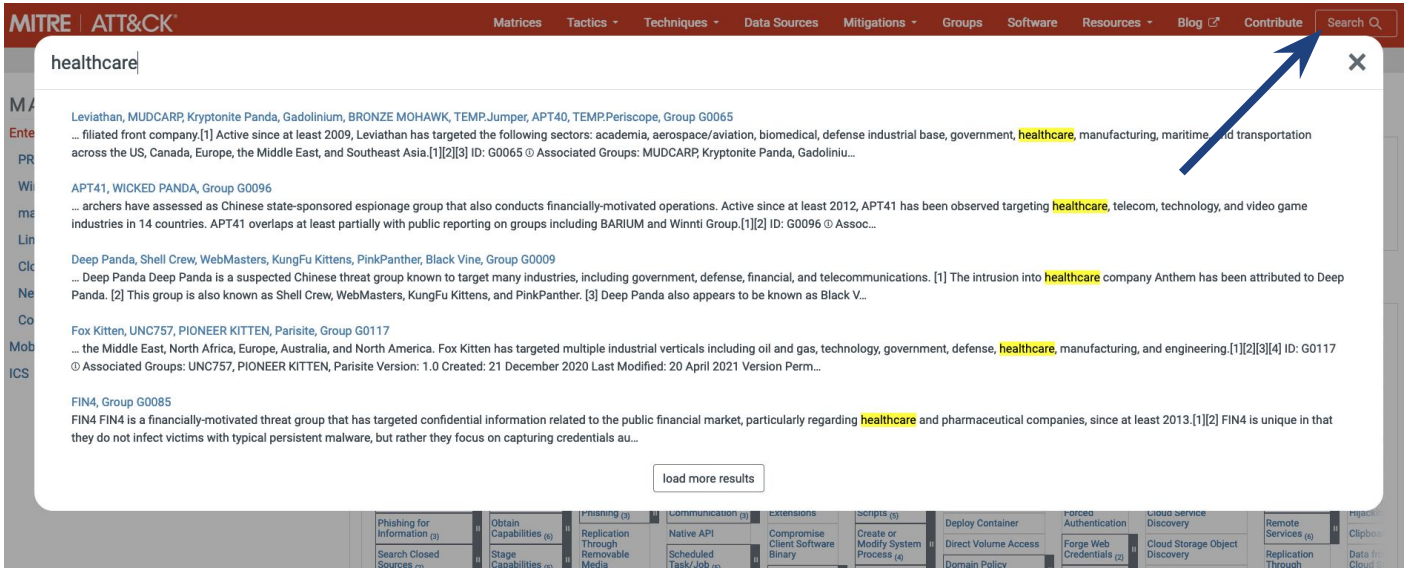
Open source tool pointing cybersecurity teams to **9,000+** publicly-accessible technical and policy controls and **2,100+** offensive security tests, aligned with over **500** common attacker techniques (ATT&CK)



controlcompass.github.io

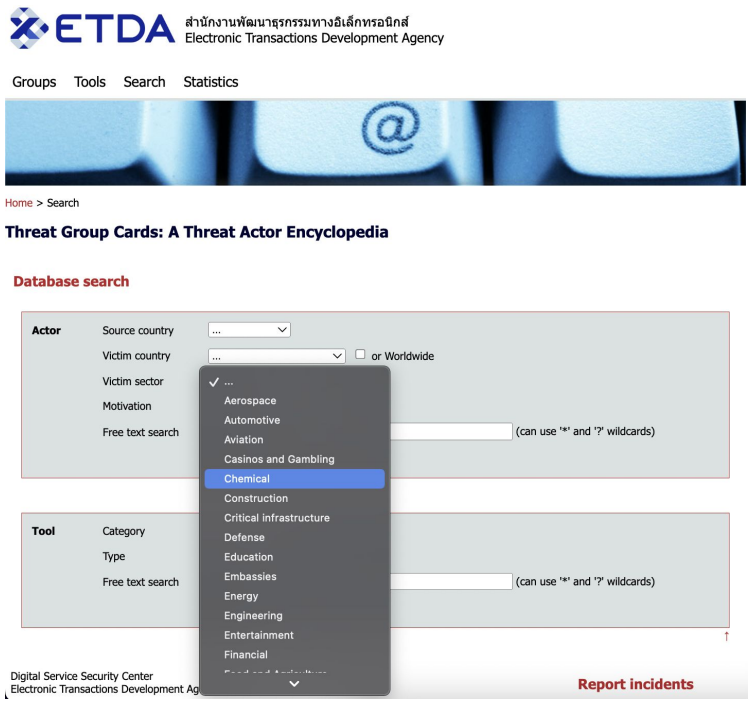
Sourcing TTP-Focused Intelligence

attack.mitre.org



Sourcing TTP-Focused Intelligence

https://apt.etda.or.th/cgi-bin/aptsearch.cgi

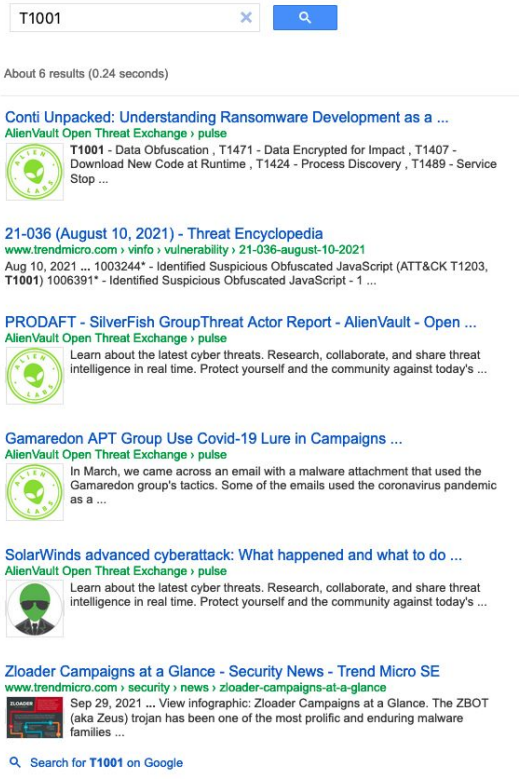


Sourcing TTP-Focused Intelligence

https://www.cisa.gov/uscert/ncas/alerts

Sourcing TTP-Focused Intelligence

https://cse.google.com/cse?cx=003248445720253387346:turlh5vi4xc



Thank You!

Resources

Control Validation Compass

- Web App: https://controlcompass.github.io/
- Dataset & source code: https://github.com/ControlCompass/ControlCompass.github.io

Cyber Adversary Heatmaps

- https://github.com/tropChaud/Cyber-Adversary-Heatmaps
- https://twitter.com/IntelScott

ATT&CK

- Getting Started with ATT&CK
- Hunting with MITRE ATT&CK
- Hunting for Post-Exploitation Stage Attacks with Elastic Stack and the MITRE ATT&CK Framework

Threat Profiling

- Using Threat Intelligence to Focus ATT&CK Activities
- A Practical Approach to Prioritizing Defenses

Control Validation / Assessment Resources

- Prelude
- VECTR
- AttackIQ Academy

Risk

- The Risk Business