

How to Conduct Threat Hunts Without a Threat Hunt Team

Jeremy Ang

About Me

- Senior Threat Intelligence Analyst at Intercontinental Exchange, Inc
- 10+ years of experience in Cybersecurity
- Threat Intelligence and Hunting, Incident Response and Digital Forensics, and Vulnerability Management
- CISSP, GCFA, GREM, GDAT, GCTI, GMON, GCIH and GOSI
- Volunteers as a mentor with (ISC)2 Singapore and member of AiSP's CTI SIG
- Opinions expressed in this presentation are solely my own and do not represent the views or opinions of my employer

Agenda

- Detection Engineering VS Threat Hunting
- Threat Hunting Frameworks
- Project DEPTH
- Quick Wins
- Key Takeaways

2 Sides, Same Coin

Detection Engineering

- Reactive approach
- Detect/respond to known threats
- False positives
- Automated
- Alert-Informed, IOCs

Threat Hunting

- Proactive approach
- Hunt Search for previously unknown threats
 - False negatives

Evil

U

- Manual, hypothesis-driven
- Threat-Informed, TTPs





Source: https://www.splunk.com/en_us/blog/learn/threat-hunting.html

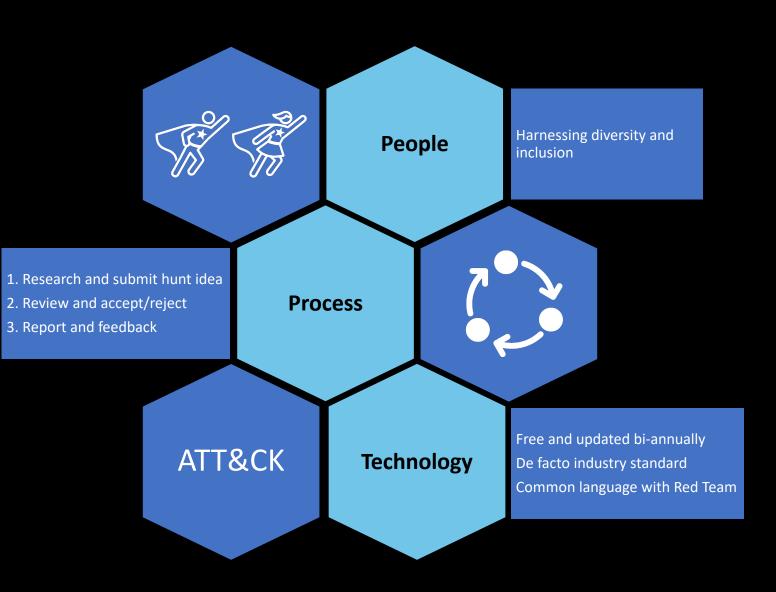
ATT&CK

- A common language for Blue, Red, Purple team
- Classify adversary behavior, identify security gaps
- Context is key

Reconnaissance 10 techniques	Resource Development 8 techniques	t Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques		Privilege Escalation 14 techniques		acti	cs	
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration	Account Manipulation (6)	n	Abuse Elevation Control Mechanism (5)				
Gather Victim Host	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting	BITS Jobs	-	Access Token	1.			
Gather Victim Identity	Compromise Accounts (3)	Exploit Public-Facing Application	Interpreter (9)		Registry Run Keys / Startup Folder	Manipulation (5)	"			
Information (3)	Compromise Infrastructure (7)	External Remote	Container Administration Command		Authentication Package	Account Manipulation (6)				
Gather Victim Network	Develop Capabilities (4)	Services	Deploy Container			Boot of Logon Autostart Execution 140				
Gather Victim Org	Establish Accounts (3)	Hardware Additions	Exploitation for Client		Winlogon Helper DLL	Boot or Logon		Pro	ocedures	
Information (4)	Obtain Capabilities (6)	Phishing (4)	Execution		Security Support Provider	Initialization Sch, ts (5)	"	ID	Name	Description
Phishing for Information (4)	Stage Capabilities (6)	Replication Through Removable Media	Inter-Process		Kernel Modules and Extensions	Create or Modify System		S0045	ADVSTORESHELL	ADVSTORESHELL achieves persistence by adding itself to the
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain	Communication (3)	Boot or Logon Autostart	Re-opened Applications	Process (4) Domain Policy		00040	ADVOTORESHEEL	HKCU/SOFTWARE/Microsoft/Windows/CurrentVersion/Run Registry key.[5][6][7]
Search Open Technical Databases (5)		Compromise (3)	Scheduled Task/Job (5)	Execution (14)	LSASS Driver	Modification (2)	"	S0331	Agent Tesla	Agent Tesla can add itself to the Registry as a startup program to establish persistence. ^{[8][9]}
Search Open		Trusted Relationship	Serverless Execution		Shortcut Modification	Escape to Host		S1025	Amadey	Amadey has changed the Startup folder to the one containing its executable by overwriting the registry
Websites/Domains (3)		Valid Accounts (4)	Shared Modules		Port Monitors	Event Triggered			,	keys. ^{[10][11]}
Search Victim-Owned Websites	-		Software Deployment Tools		Print Processors	Execution (16) Exploitation for Privilege		S1074	ANDROMEDA	ANDROMEDA can establish persistence by dropping a sample of itself to C:\ProgramData\Local
					XDG Autostart Entries	Exploitation for Privilege Escalation				Settings\Temp\mskmde.com and adding a Registry run key to execute every time a user logs on. ^[12]
			System Services (2)			Hijack Execution				Source: https://attack.mitre.org/techniques/T1547/001
			User Execution (3) Windows Management		Login Items	Flow (12)				Source: https://attack.initre.org/techniques/1134//001
			Instrumentation	Boot or Logon Initialization Scripts (5)		Process Injection (12) Scheduled Task/Job (5)				
				- (0)		(-)				
				Browser Extensions		Valid Accounts (4)	<u> </u>			
				Techniques,	Sub-techniques					

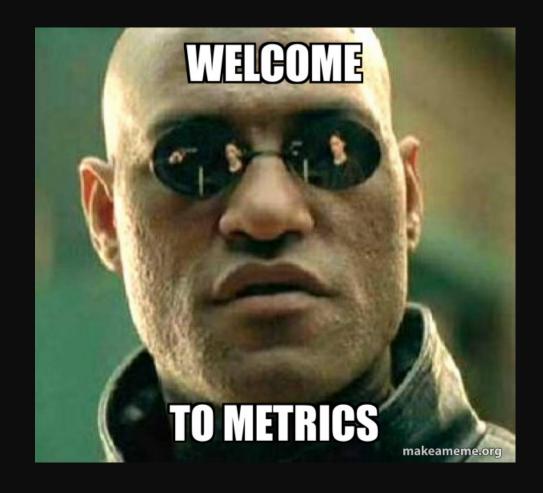
Project DEPTH

Defense in DEPTH



Measuring the DEPTH

- Initiated 27 unique threat hunting use-cases
- Implemented 13 detection alerts from threat hunt submissions
- Detection and mitigation across 20 ATT&CK techniques and sub-techniques
 - ✓ T1036.002: Masquerading: Right-to-Left Override
 - ✓ T1070.001: Indicator Removal: Clear Windows Event Logs
 - ✓ T1218.002: System Binary Proxy Execution: Control Panel
- Identified other issues like insufficient logging and monitoring, outdated/EOL systems, etc.



Quick Wins

RMM tools

- Remember SolarWinds in 2020?
- Rise in popularity amongst threat actors
 - LOTL as a legitimate software with signed certs and exclusion paths
 - Bypass admin privilege requirements and software management control policies
- Used as C2 and to maintain persistence on a victim's network [T1219] and perform lateral movement [T1072]
- More than 100 and counting...

Procedure Examples

ID	Name	Description
C0015	C0015	During C0015, the threat actors installed the AnyDesk remote desktop application onto the compromised network. ^[4]
C0018	C0018	During C0018, the threat actors used AnyDesk to transfer tools between systems. ^{[5][6]}
C0027	C0027	During C0027, Scattered Spider directed victims to run remote monitoring and management (RMM) tools. [7]
S0030	Carbanak	Carbanak has a plugin for VNC and Ammyy Admin Tool. ^[8]
G0008	Carbanak	Carbanak used legitimate programs such as AmmyyAdmin and Team Viewer for remote interactive C2 to target systems. ^[9]
G0080	Cobalt Group	Cobalt Group used the Ammyy Admin tool as well as TeamViewer for remote access, including to preserve remote access if a Cobalt Strike module was lost. ^{[10][11][12]}
G0105	DarkVishnya	DarkVishnya used DameWare Mini Remote Control for lateral movement. ^[13]
S0384	Dridex	Dridex contains a module for VNC. ^[14]

Source: https://attack.mitre.org/techniques/T1219/

Hunt for RMM tools

- Mitigations:
 - Application Control Policy
 - MFA
- Detections:
 - Network-based Monitoring for known domains or ports (AnyDesk:6568, TeamViewer:5938)
 - Host-based Monitoring for processes (anydesk.exe, teamviewer.exe) initiated by RMM tools
 - Host-based Monitoring for file certificates (SignerSubjectName=philandro Software GmbH, TeamViewer GmbH)
- Consider maintaining a repository of RMM tools

Name	Associated Threat	Domain	Port	Process	Is this approved?	Detection
AnyDesk	ALPHV, Scattered Spider	anydesk.com	6568	anydesk.exe	No	Yes
TeamViewer	ALPHV, BazarCall, Scattered Spider	teamviewer.com	5938	teamviewer. exe	Yes	Yes

Top 5 ATT&CK Techniques

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

	help changelog theme •	
Create New Layer	Create a new empty layer	~
Open Existing Layer	Load a layer from your computer or a URL	~
Create Layer from Other Layers	Select layers to inherit properties from	~
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	~

- 1) From a CTI perspective, review threat actors of interest to your organization and pick the top 5:
 - Top actors by Big 4
 - Top fincrime/ransomware actors
- 2) Using Navigator, apply different layers of the threat actors' TTPs together
- 3) Extract the top 5 techniques that overlap and implement detections

Scattered Spider (G1015) $\,\, imes\,$

									r controls	₽, ⊙ ≎		A A A A A A A A A A A A A A A A A A A	▋, ⇔, ≔, 🔌 🛛
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration	Account Manipulation (3/6)	Abuse Elevation Control	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the- Middle	Account Discovery (2/4)	Exploitation of Remote Services	Adversary-in- the-Middle	Application Layer Protocol (0/4)	Automated Exfiltration	Account Access II Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command Command and	BITS Jobs	Mechanism (0/5) Access Token	Access Token Manipulation	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication	(0/1) Data Transfer	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Accounts (0/3)	Exploit Public- Facing	Scripting Interpreter _(0/9)	Boot or Logon Autostart II Execution	Manipulation I	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	(0/3) Audio Capture	Removable Media Content Injection	Size Limits Exfiltration	Data Encrypted for Impact
Gather Victim Network Information II	Compromise Infrastructure (0/7)	Application	Container Administration	Boot or Logon	Account Manipulation I	Build Image on Host	(0/6) Exploitation for	Cloud Infrastructure Discovery	Remote Service	Automated	Data Encoding (0/2)	Over I Alternative	Data Manipulation
(0/6) Gather Victim Org	Develop Capabilities (0/4)	External Remote Services	Command Deploy Container	Initialization II Scripts (0/5)	(3/6) Boot or Logon	Debugger Evasion Deobfuscate/Decode Files	Credential Access Forced	Cloud Service Dashboard	Session Hijacking I	I Collection Browser Session	Data Obfuscation	Protocol (0/3) Exfiltration	Defacement (0/2)
Information (0/4) " Phishing for	Establish Accounts	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Autostart I Execution (0/14)	or Information Deploy Container	Authentication Forge Web	Cloud Service Discovery Cloud Storage Object	Remote Services	Hijacking Clipboard Data	Dynamic Resolution	Over C2 Channel	Disk Wipe (0/2)
Information (2/4)	Obtain Capabilities (1/6)	Phishing (1/4)	Inter-Process Communication	Compromise Client Software Binary	Boot or Logon Initialization I Scripts	Direct Volume Access	Credentials (0/2)	Discovery Container and Resource	Replication Through Removable Media	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Other Network	Service (0/4)
Sources (0/2) Search Open	Stage Capabilities	Replication Through Removable	(0/3) Native API	Create Account	Create or Modify System	Domain Policy Modification (0/2)	I (0/4) Modify	Discovery Debugger Evasion	Software Deployment Tools	Data from Configuration	(0/2) Fallback Channels	Medium (0/1)	Firmware Corruption
Technical Databases	(0/6)	Media	Scheduled	(0/3) Create or Modify	Process (0/4)	Execution Guardrails (0/1)	Authentication Process (0/8)	Device Driver Discovery	Taint Shared	Repository (0/2)	Ingress Tool Transfer	Over Physical Medium (0/1)	Inhibit System Recovery
Search Open Websites/Domains II		Supply Chain Compromise II	Task/Job _(0/5) Serverless	System Process	Domain Policy Modification I	Exploitation for Defense Evasion	Multi-Factor Authentication	Domain Trust Discovery	Content Use Alternate	Data from Information Repositories (1/3)	II Multi-Stage Channels	Exfiltration Over Web	Network Denial of
(0/3) Search Victim-Owned		Trusted Relationship	Execution Shared Modules	Event Triggered Execution (0/16)	Escape to Host	File and Directory Permissions Modification	Interception Multi-Factor	File and Directory Discovery	Authentication I Material (0/4)	Data from Local System	Non-Application Laver Protocol	Service (0/4)	Resource Hijacking
Websites		Valid Accounts	Software Deployment Tools	External Remote Services	Event Triggered Execution (0/16)	Hide Artifacts (0/11)	Authentication Request Generation	Group Policy Discovery		Data from Network Shared	Non-Standard Port	Transfer Transfer Data	Service Stop System
		(1/4)	System Services	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation	Hijack Execution Flow	Network Sniffing	Network Service		Drive Data from	Protocol Tunneling	to Cloud Account	Shutdown/Reboot
			(0/2) User Execution (0/3)	Implant Internal I Image	Hijack Execution	Impair Defenses (0/11)	I OS Credential Dumping (1/8)	Discovery Network Share Discovery		Removable Media	Proxy (0/4) Remote Access	1	
			Windows Management	Modify Authentication II	Flow (0/12) Process	Impersonation Indicator Removal	Steal Application Access Token	Network Sniffing		Data Staged (0/2)	II Traffic Signaling		
			Instrumentation	Process (0/8) Office Application	Injection (0/12) Scheduled	Indirect Command Execution	Steal or Forge Authentication	Password Policy Discovery Peripheral Device		Email Collection (0/3)	II (0/2) Web Service		
				Startup (0/6)	Task/Job (0/5)	Masquerading (0/9)	Certificates	Discovery		Input Capture	1	·	
				Power Settings	Valid Accounts	Modify Authentication	Steal or Forge Kerberos Tickets	Permission Groups	1	Screen Capture			

 \odot

								selection controls layer	^{controls} , ±, =, ‡≵	₽,⊙ ≎ €	tech : ::::::::::::::::::::::::::::::::::
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques
To techniques Active Scanning (1/3) Gather Victim Host information (0/4) Gather Victim Identity information (1/3) Gather Victim Org information (0/4) Sather Victim Org information (0/4) Phishing for information (2/4) Search Closed Sources (0/2) Search Open fechnical Databases Fearch Open Websites/Domains Search Victim-Owned Websites	Acquire Access Acquire Access Acquire infrastructure (2/8) Compromise Accounts (2/3) Compromise Infrastructure (1/7) Develop Capabilities (2/4) Establish Accounts (1/3) Obtain Capabilities (2/6) Stage Capabilities (1/6) I	Content Injection Drive-by Compromise Exploit Public- Facing Application External Remote Services Hardware Additions Phishing (4/4) I Replication Through Removable Media Supply Chain Compromise (1/3) Trusted Relationship	Cloud Administration Command and Scripting Interpreter (6/9) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (1/3) Native API Scheduled Task/Job (1/5) Serverless Execution Shared Modules	Account Manipulation (4/6) BITS Jobs Boot or Logon Autostart Execution (1/14) Boot or Logon Initialization Scripts (1/5) Browser Extensions Compromise Client Software Binary Create Account (1/3) Create or Modify System Process (0/4) Event Triggered Execution (2/16) External Remote	Abuse Elevation Control Mechanism (1/5) Access Token Manipulation (2/5) Account Manipulation (4/6) Boot or Logon Autostart Execution (1/14) Boot or Logon Initialization Scripts (1/5) Create or Modify System Process (0/4) Domain Policy Modification (1/2) Escape to Host	Abuse Elevation Control Mechanism (1/5) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Debugger Evasion Debugger Evasion Deblog Container Direct Volume Access Domain Policy Modification (1/2) Execution Guardrails (0/1) Exploitation for Defense File and Directory Permissions Modification [0/2)	Adversary-in-the- Middle ()(3) Brute Force (2/4) Credentials from Password Stores ()(6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2/2) Input Capture ()(4) Modify Authentication Process (1/8) Multi-Factor Authentication Interception	Account Discovery (3/4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Service Discovery Cloud Storage Object Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Scovery	Image: Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (v2) Remote Services (v2) Remote Services (v2) Remote Services (v2) Remote Services (v3) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (3/4)	Adversary-in- the-Middle (0/3) I Archive Collected Data II Archive Collected Data II Audio Capture II Audio Capture II Automated Collection II Browser Session Hijacking II Data from Cloud Storage II Data from Configuration Repository (0/2) II Data from Information Repositories (2/3) II Data from Local System II	Application Layer Protocol (1/4) Communication Through Removable Media Content Injection Data Encoding (1/2) Data Obfuscation (1/3) Dynamic Resolution (1/3) Encrypted Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol
		Valid Accounts (8/4)	Software Deployment Tools System Services (0/2) User Execution (2/3) Windows Management Instrumentation	Services Hijack Execution Flow (0/12) Implant Internal Image Modify Authentication Process (1/8)	Execution (2/16) Exploitation for Privilege Escalation Hijack Execution Flow (0/12) Process Injection (1/12)	Hide Artifacts (0/11) Hijack Execution Flow (0/12) Impair Defenses (3/11) Impersonation Indicator Removal (3/9)	Request Generation Network Sniffing OS Credential Dumping (3/8) Steal Application Access Token	Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery		Data from Network Shared Drive Data from Removable Media Data Staged (1/2) Email Collection	Non-Standard Port Protocol Tunneling Proxy (3/4) Remote Access Software Traffic Signaling (0/2)

about domain Techniques by Threat Groups Enterprise ATT&CK v14					platforms Linux, macOS, Windows, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD				legend 1.0 1.4 1.8 2.2 2.6 3.0				
Re connaiss an ce	Re sour ce De velopm en t	Initial Access	Execution	Persistence	Privilege Escalation	De fen se Eva sion	Credential Access	Disc overy	Lateral Movement	Collection	Comm and and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Adm h Istration	Account Manipulation	Abuse Elevat b n Control Me chanism	Abuse Elevation Control Mechanism	Adversa ry-in- the- Middle	Account Discovery	Exploitation of Remote Services	Adversa ry-in-the-Middle	Application Layer Proto col	Autom ated Exfiltration	Account Access Remo val
GatherVictim	Acquire	Drive-by	Command and	BITS Jobs	Access Token	Access Token	Brute Force	Application	Inte mal	Archive	Comm unicatio n Throug h	Data Transfer	Data
Host In form ation Gath er Victim	Infrastructure Compromise	Comp rom ise Exploit Public-Facing	Scripting Interpret er Conta iner	Boot or Log on	Manipulation Account	Ma nipulation	Cred entials from	Window Discove ry Browser Informatio n	Spear phishing Lat eral	Collected Data	Remo vable M edia Conte nt	Size Limits Exfiltration Over	Destruction Data Encrypted
Ide ntity Info ma tion	Accounts	Application	Administration Comman d	Autostant Execution	Ma nipulation	BITS Jobs	Password Stores	Discovery	Tool T ransf er	Audio Cap ture	Inject b n	Alterna tive Proto col	for Impa ct
Gath er Victim Network Information	Comp rom ise Infr astru cture	Extern al Remote Services	Deploy Conta iner	Boot or Log on Initializat on Scripts	Boot o r Log on Autosta rt Execution	Build Image on Host	Exploitation for Cred ential Access	Cloud Infra structu re Discover y	Remo te Service Session Hijacking	Autom ated Collection	Data Enco ding	Exfiltration Over C2 Chan nel	Data Manipulation
Gath er Victim	Develop	Hard ware	Exploitation for	Browser	Boot or Log on	Debu gger	Fo roed	Cloud Service	Remo te	Browser Session	Data	Exfiltration Over	Deface ment
Org Information Phishing for	Capa bilt è s Establish	Additions	Client Execut b n Inte r-Pro cess	Extension s Compromise Client	Initialization Scripts Create or Modify	E vasion Deob fuscate/ De code	Authen tication Forge Web	Dashboard Cloud Service	Services Replication Through	Hijacking	Obfu scation Dynam ic	Othe r Network Med ium Exfiltration Over	
Info mation	Accounts	Phishing	Communication	Software Bh ary	System Pro cess	Files or in formation	Cred entials	Discovery	Remo vable M edia	Clipboa rd Data	Resolut b n	Physical Medium	Disk Wipe
Search Closed Sources	Obta in Capa bilt is s	Replication Through Removable Media	Native API	Crea te Account	Doma in Policy Mo dification	Deploy Conta iner	Inp ut Captu re	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Sto race	Encrypt ed Chan nel	Exfiltration Over Web Service	Endpoht Denial of Service
Search Open	Stage	Supply Chain	Schedu le d	Crea te or Mod f y		Direct	Mo dify Au thentica tion	Conta iner a nd	Taint	Data from Configuration Repost ory	Falback	Schedule d	Fin ancial
Techn ical Databa ses Search Open	Capa bill is s	Comp rom ise	Task/Job Server less	System Process Event Triggered	Escape t o Host	Volume Access Doms in Policy	Process MultiFactor	Resource Discovery Debugger	Share d Conte nt		Chan nels	Transfer Transfer Data	Th eft Fir mware
Search Open Websites/Do mains		Trusted Relation ship	Server less Execution	Event Triggered Execution	Event Trigger ed Execution	Doma in Policy Mo dification	Mut i Factor Authen tication Intercept on	Evasion	Authen tication Ma terial	Data from Information Repost ories	Ing ress Tool T ransf er	Transfer Data to Clou d Acco unt	Fir mware Corruption
Search Victim -Owned		Valid Accounts	Share d Modules	Extern al	Exploitation for	Execution	Multi Factor Authen tication	Device Drive r		Data from	Mu ti Stage		Inh b it System
Websites			Software	Remote Services Hijack	Privilege Escalat b n Hijack	Guandra its Exploitation for	Requiest Genieration Networik	Discovery Doma in Tru st		Loca I System Data from Network	Chan nels Non-Ap plication		Recove ry Network Denial
			Deploym ent To ols	Execution Row	Execution Row	Defen se Evasion	Sniffing	Discovery		Share d Drive	Laye r P roto col		of Service
			System Services	Imp lant Inte mail I mage	Process Inject b n	File and Directory Permissions Modification	OS Cred ential Dump ing	File and Directory		Data from Removable Media	Non-Standard Port		Resource Hijacking
				Mo dify Au thentica tion	Schedu e d		Steal Application	Group Policy			Proto col		
			User Execution	Process	Task/Jo b	Hide Artifact s	Access Token	Discovery		Data Staged	Tu nneling		Service Stop
			Windows M anag emen t Instrume ntation	Office Application Startup	Va Id Accounts	Hijack Execution Flow	Steal or Forge Auth entication Cert f baites	Log Enumeration		Email Collection	Proxy		System Shutdo wn/Reboot
				Power Sett h gs		Imp air	Steal or Forge	Network Service		Inp ut Captu re	Remo te Access		
						Defen ses	Kerbe ros T bke ts Steal Web	Discover y Network Share			Software Traffic		
				Pre-OSBcot		Imp erson ation	Session Coo kie	Discovery		Screen Capture	Signaling		
				Schedule d Task/Job		Indica tor Removal	Unsecu red Cred entials	Network Sniffing		Video Capture	Web Service		
				Server Software		Ind i ect Com mand		Password Polcy					
				Comp onen t		Execution		Discovery					
				Traffic Signaling		Ma squer ading		Peripheral Device Discove ry					
				Valid Accounts		Mo dify Au thentica tion		Permission					
						Process Mo dify Cloud Co mpute		Groups Discovery Process					
						Infrastru cture		Discovery					
						Mo dify Registry		Que ry Registry					
						Modify		Remo te System					
						System I mage Network Bo unda ry	_	Discover y Software					
						Network Boundary Bridging		Software Discovery					
						Obfu scated Files or Information		System I nform ation					
						or Information Plist File		Discovery System Location					
						Mo dification		Discovery					
						Pre-OSBcot		System Network Configuration Discovery					
						Process		System Ne twork					
						Injection		Connections Discovery					
						Reflective Code Load hg		System O wn en User Discover y					
						Rogu e Doma h		System Service					
						Controller	_	Discovery	_				
						Rootkit		System Tim e Discovery					
								Time Discovery					

ATT&CK Navigator

- Export the layer as JSON and focus on techniques with score=3 or the top 5
 - T1553.002: Subvert Trust Controls: Code Signing
 - T1588.002: Obtain Capabilities: Tool
 - T1105: Ingress Tool Transfer
- Complement with CTID's projects for top technique priority
 - Sightings Ecosystem
 - T1059: Command and Scripting Interpreter
 - T1027: Obfuscated Files or Information
 - T1105: Ingress Tool Transfer
 - Top ATT&CK Techniques
 - Top Ransomware Technique List
- Implement and maintain detections

techniqueID	tactic	score
T1553.002	defense-evasion	3
T1588.002	resource-development	3
т1105	command-and-control	3
T1553.005	defense-evasion	2
т1078.004	defense-evasion	2
T1078.004	persistence	2
Т1078.004	privilege-escalation	2
T1078.004	initial-access	2
т1047	execution	2
T1218.011	defense-evasion	2

SIGHTINGS ECOSYSTEM

A DATA-DRIVEN ANALYSIS OF ATT&CK IN THE WILD

Received 1.6m+ Sightings of 353 unique techniques, from 198 countries, observed between August 2021 and September 2023 2021 - 2023 AUGUST SEPTEMBER





198

SIGHTINGS

UNIQUE TECHNIQUES COUNTRIES

Source: https://mitre-engenuity.org/cybersecurity/center-for-threatinformed-defense/our-work/sightings-ecosystem/

Key Takeaways

- Leverage ATT&CK to achieve quick wins
- Organizations without a threat hunt program can kickstart today with the right people, process and technology
- Organizations with a threat hunt program can use ATT&CK to improve detection coverage and mature current hunting capabilities
- Threat hunting is an iterative process so automate where possible
- Marry with Red Team's findings to be cognizant of your organization's overall security posture.