How to Conduct Threat Hunts Without a Threat Hunt Team

Jeremy Ang

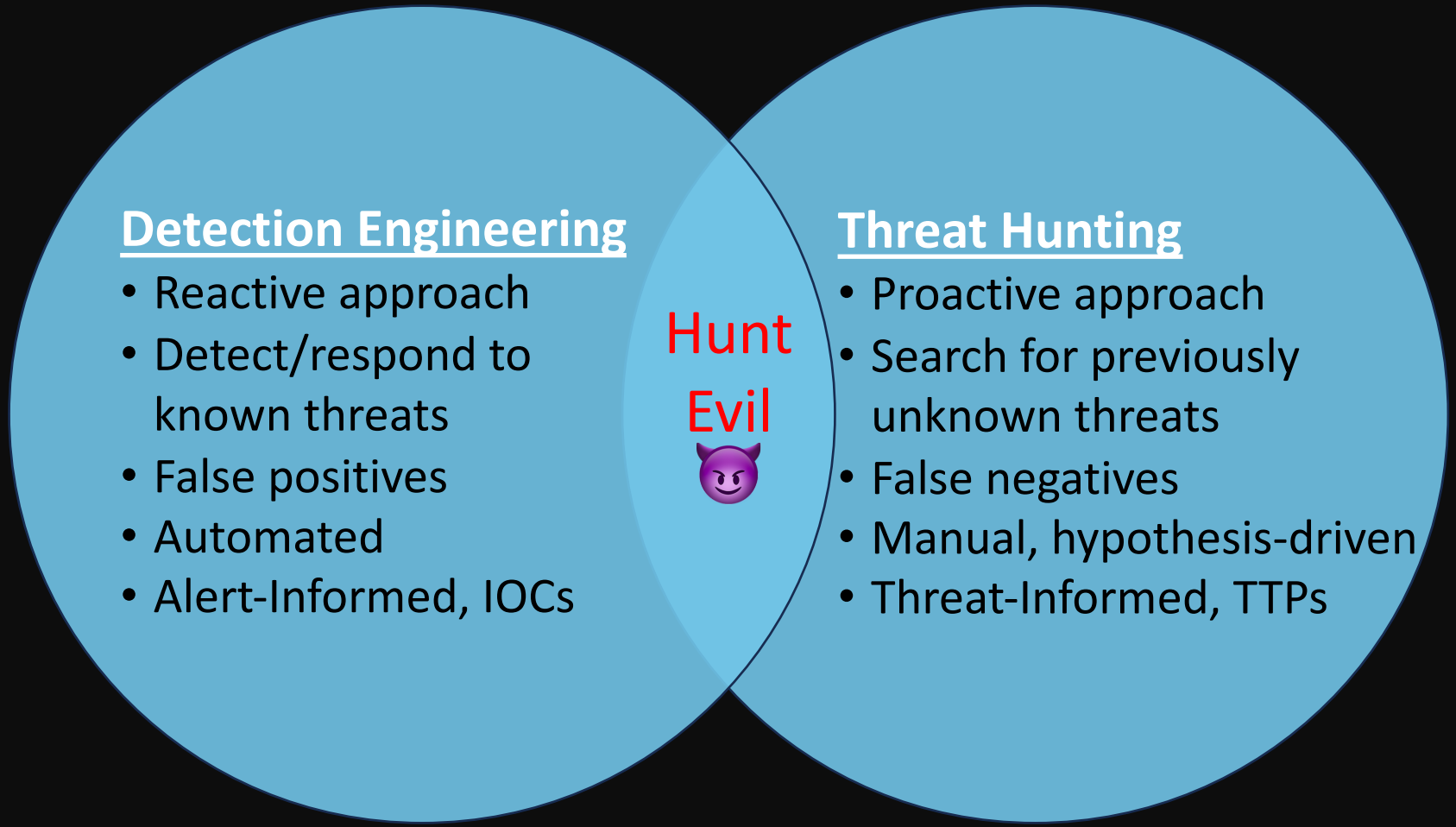
About Me

- 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



Chronicle of Threat Hunting Frameworks

MITRE ATT&CK®
The Pyramid of Pain
2013

2015
Sqrrl Threat Hunting Reference Model

HMM: Hunting Maturity Model

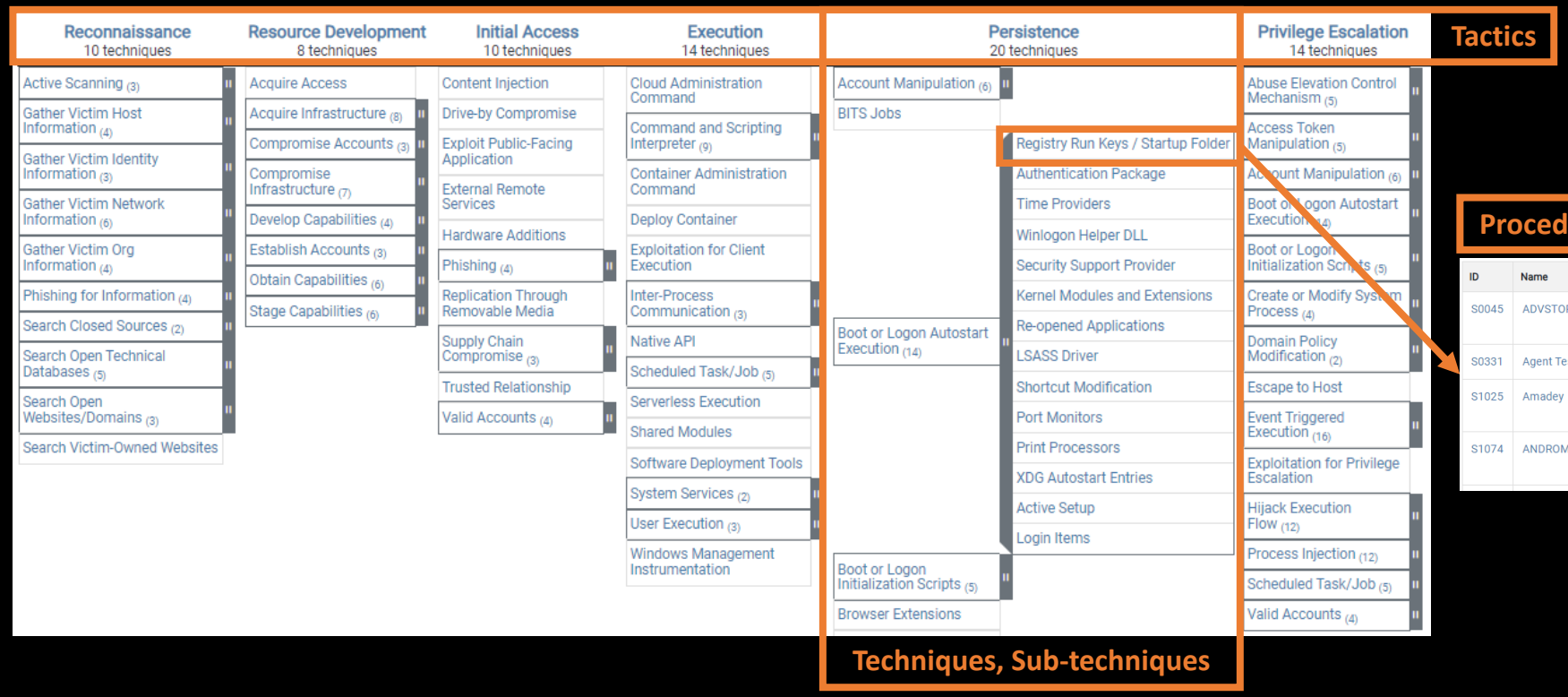
TaHiTI: Targeted Hunting Integrating Threat Intelligence
2018

2023
PEAK: Prepare, Execute & Act with Knowledge

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



Procedures

ID	Name	Description
S0045	ADVSTORESHELL	ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[5][6][7]
S0331	Agent Tesla	Agent Tesla can add itself to the Registry as a startup program to establish persistence.[8][9]
S1025	Amadey	Amadey has changed the Startup folder to the one containing its executable by overwriting the registry keys.[10][11]
S1074	ANDROMEDA	ANDROMEDA can establish persistence by dropping a sample of itself to `C:\ProgramData\Local Settings\Temp\mskmde.com` and adding a Registry run key to execute every time a user logs on.[12]

Source: https://attack.mitre.org/techniques/T1547/001

Project DEPTH

Defense in DEPTH

People

Harnessing diversity and inclusion

1. Research and submit hunt idea
2. Review and accept/reject
3. Report and feedback

Process

ATT&CK

Technology

Free and updated bi-annually
De facto industry standard
Common language with Red Team

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]

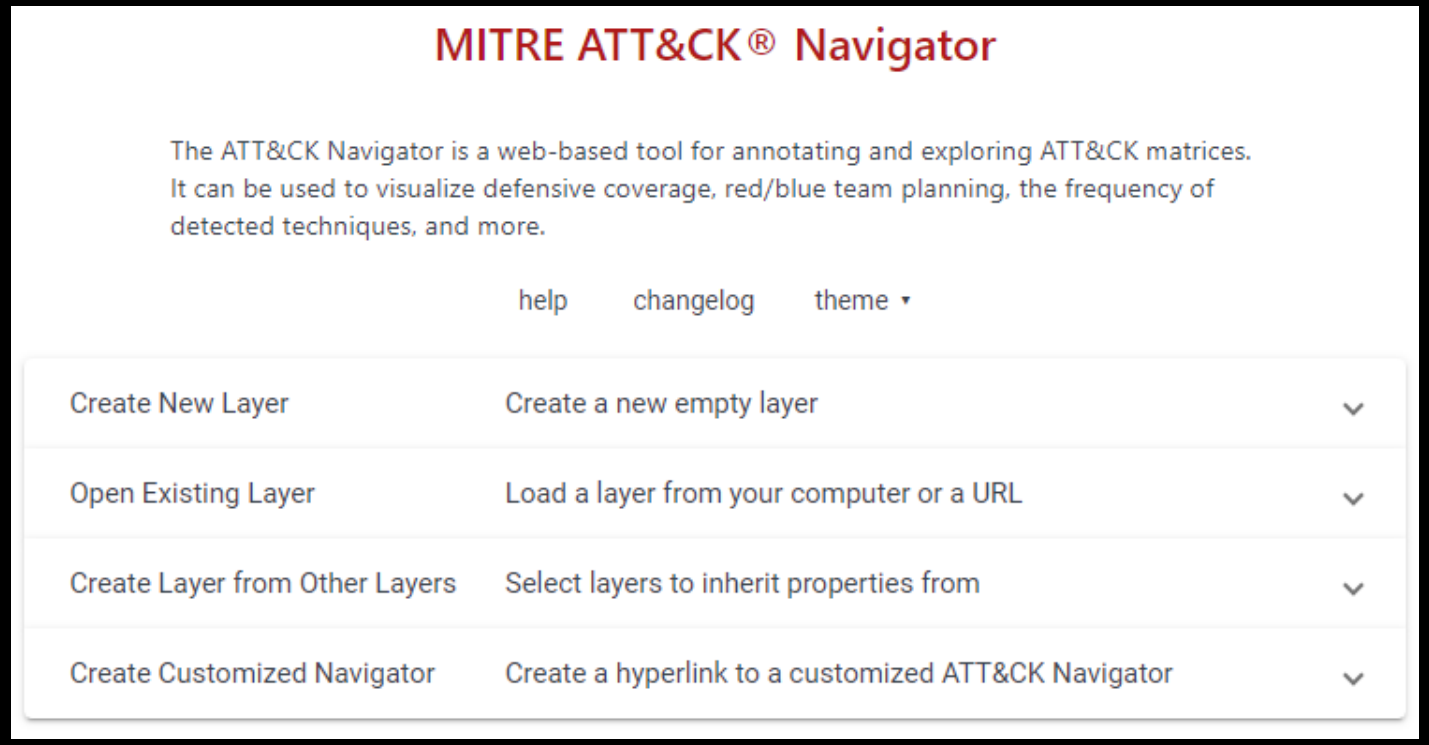
Source: https://attack.mitre.org/techniques/T1219/

Hunt for RMM tools

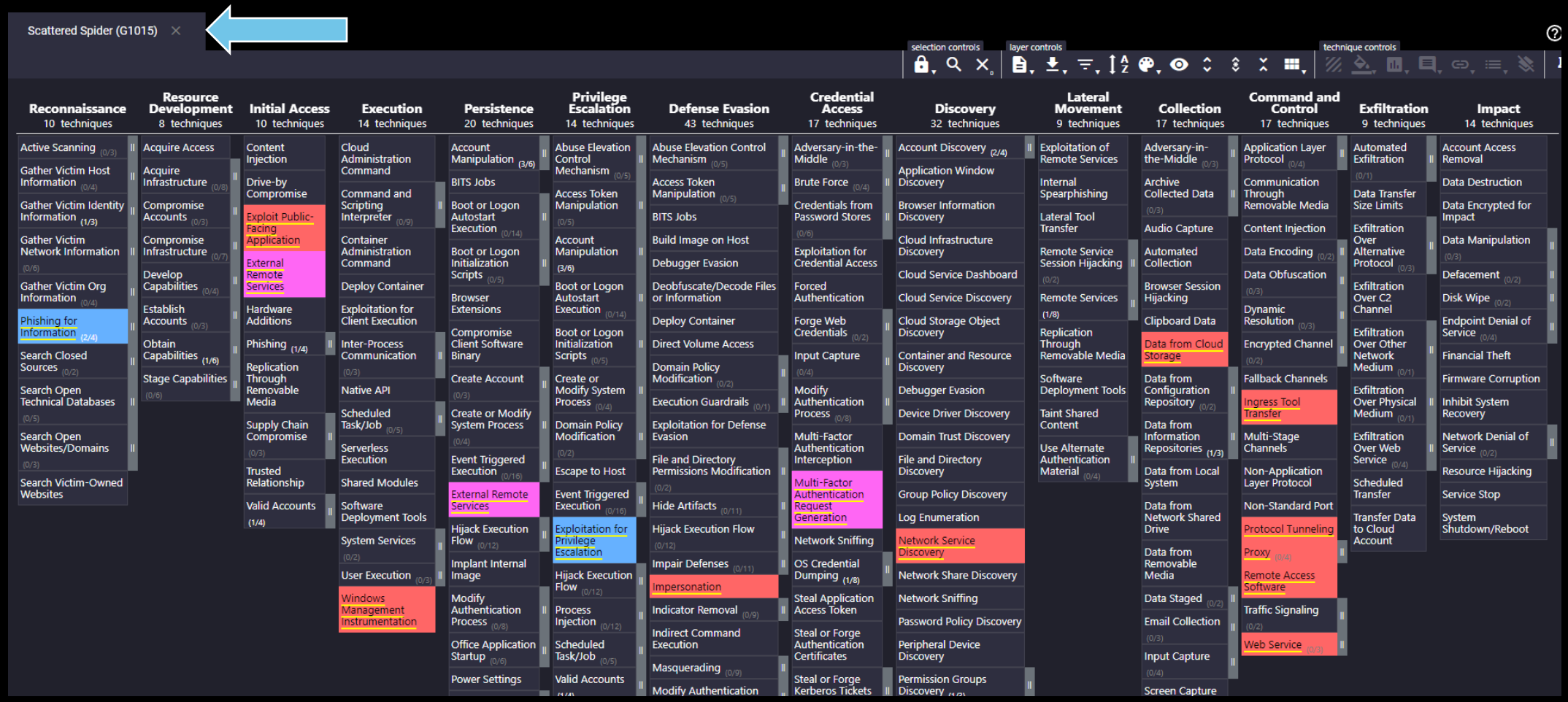
- Mitigations:
  - Application Control Policy
  - MFA
- Detections:
  - Network-based - Monitoring for known domains or ports (AnyDesk:6568, TeamViewer:5938)
  - Host-based - Monitoring for processes (anydesk.exe, teamviewer.exe) initiated by RMM tools
  - Host-based – Monitoring for file certificates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

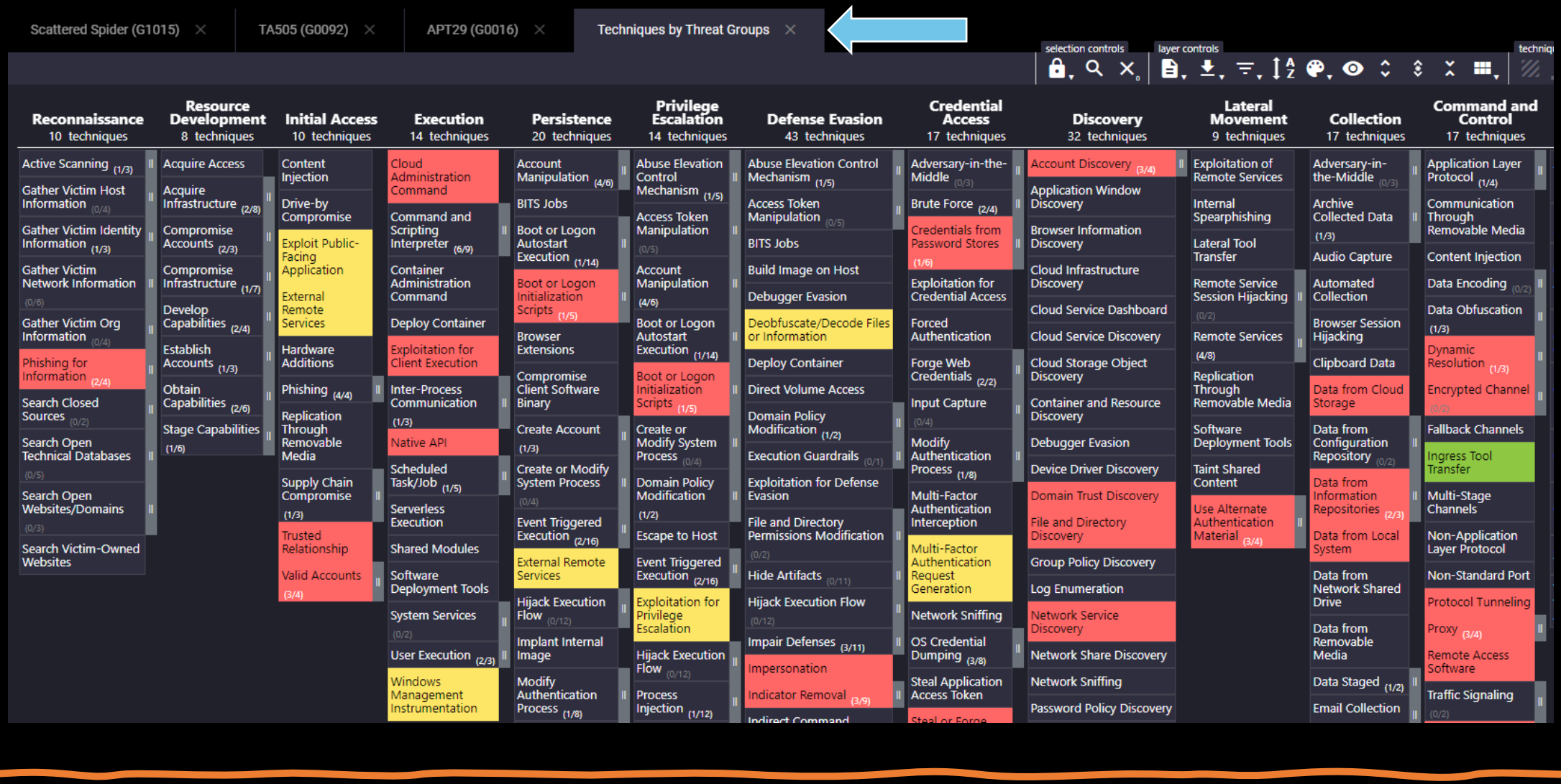
Name	Associated Threat	Domain	Port	Process	Is this approved?	Detection
AnyDesk	ALPHV, Scattered Spider	anydesk.com	6568	anydesk.exe	No	Yes
TeamViewer	ALPHV, BazarCall, Scattered Spider	teamviewer.com	5938	teamviewer.exe	Yes	Yes

Top 5 ATT&CK Techniques



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


Scattered Spider (G1015)
TA505 (G0092)
APT29 (G0016)
Techniques by Threat Groups
selection controls
layer controls
Reconnaissance
10 techniques
Active Scanning (1/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (1/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (2/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Resource Development
8 techniques
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)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4/4)
Replication Through Removable Media
Supply Chain Compromise (1/3)
Trusted Relationship
Valid Accounts (3/4)
Execution
14 techniques
Cloud Administration Command
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
Software Deployment Tools
System Services (0/2)
User Execution (2/3)
Windows Management Instrumentation
Persistence
20 techniques
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 Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (1/8)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (1/5)
Access Token Manipulation (0/5)
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
Event Triggered Execution (2/16)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (1/12)
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (1/5)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (1/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/11)
Hijack Execution Flow (0/12)
Impair Defenses (3/11)
Impersonation
Indicator Removal (3/9)
Indirect Command
Credential Access
17 techniques
Adversary-in-the-Middle (0/3)
Brute Force (2/4)
Credentials from Password Stores (1/6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2/2)
Input Capture (0/4)
Modify Authentication Process (1/8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (3/8)
Steal Application Access Token
Steal or Forge
Discovery
32 techniques
Account Discovery (3/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (4/8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (3/4)
Collection
17 techniques
Adversary-in-the-Middle (0/3)
Archive Collected Data (1/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (2/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (1/2)
Email Collection
Command and Control
17 techniques
Application Layer Protocol (1/4)
Communication Through Removable Media
Content Injection
Data Encoding (0/2)
Data Obfuscation (1/3)
Dynamic Resolution (1/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (3/4)
Remote Access Software
Traffic Signaling (0/2)

about

Techniques by Threat Groups

domain

Enterprise ATT&CK v14

platforms

Linux, macOS, Windows, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD

legend

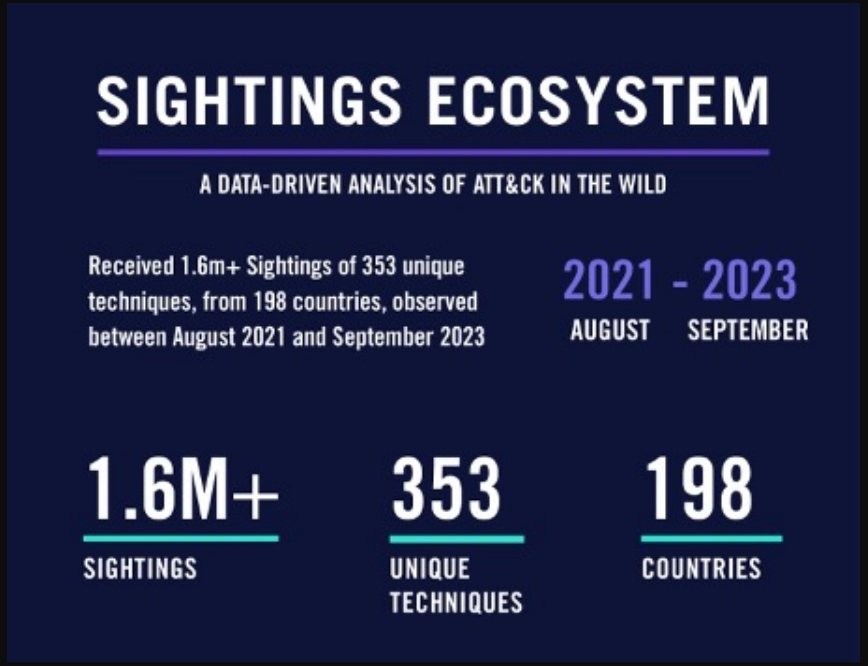
1.0 1.4 1.8 2.2 2.6 3.0

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 Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains		Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			System Services	Implant Internal Image	Process Injection	File and Directory Permissions Modification	OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	Proxy		System Shutdown/Reboot
				Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Web Service		
				Server Software Component		Indirect Command Execution		Password Policy Discovery					
				Traffic Signaling		Masquerading		Peripheral Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute Infrastructure		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		System Network Configuration Discovery					
						Process Injection		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					

ATT&CK Navigator

techniqueID	tactic	score
T1553.002	defense-evasion	3
T1588.002	resource-development	3
T1105	command-and-control	3
T1553.005	defense-evasion	2
T1078.004	defense-evasion	2
T1078.004	persistence	2
T1078.004	privilege-escalation	2
T1078.004	initial-access	2
T1047	execution	2
T1218.011	defense-evasion	2

- 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



Source: https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-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.