The TTP Pyramid

@SecurePeacock

SCYTHE

Chris Peacock – Adversary Emulation Detection Engineer

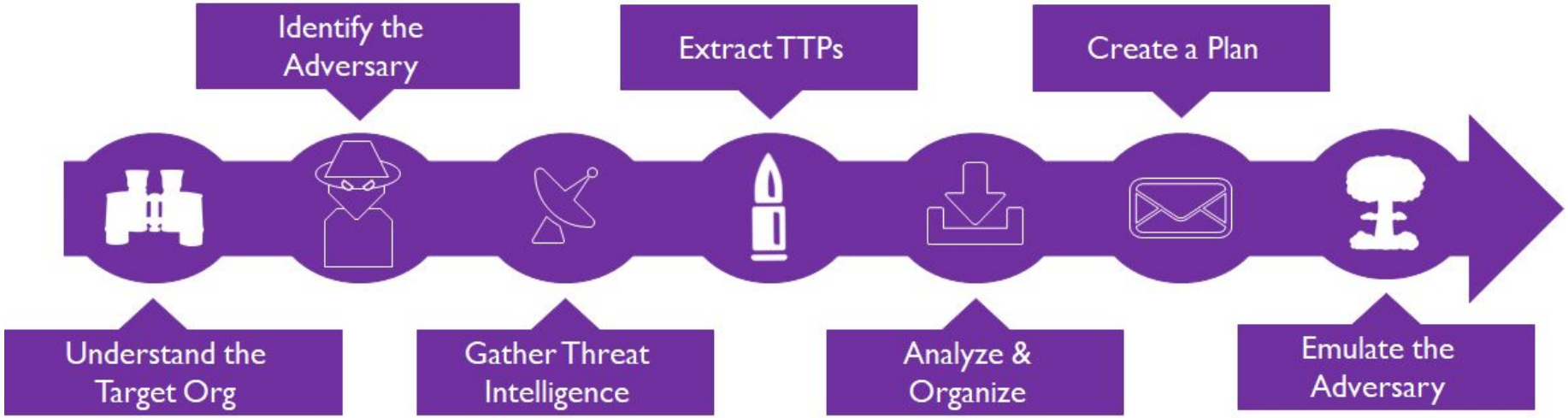
SCYTHE

Raytheon Intelligence & Space

GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

Cyber Threat Intelligence – Purple Process

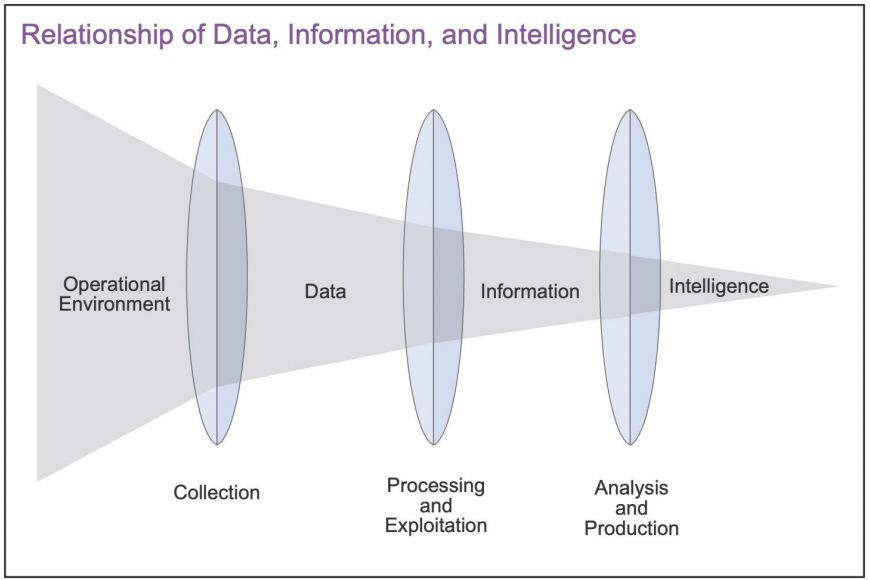


ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Cyber Threat Intelligence

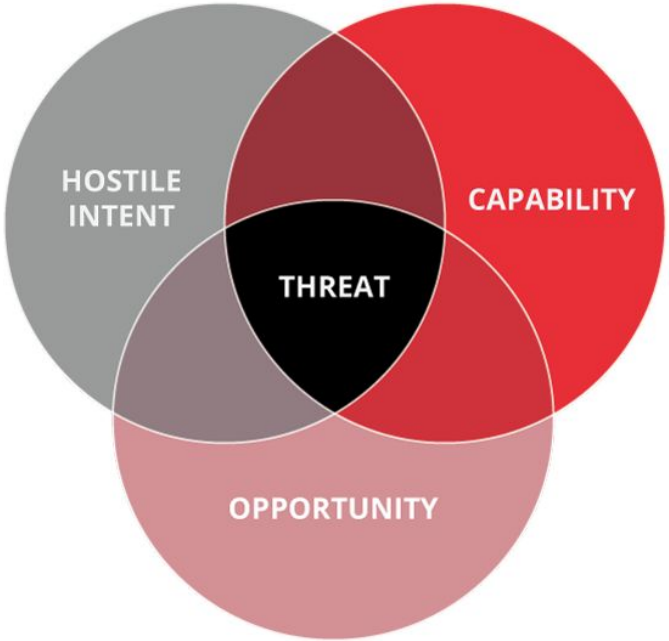
"Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors."

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



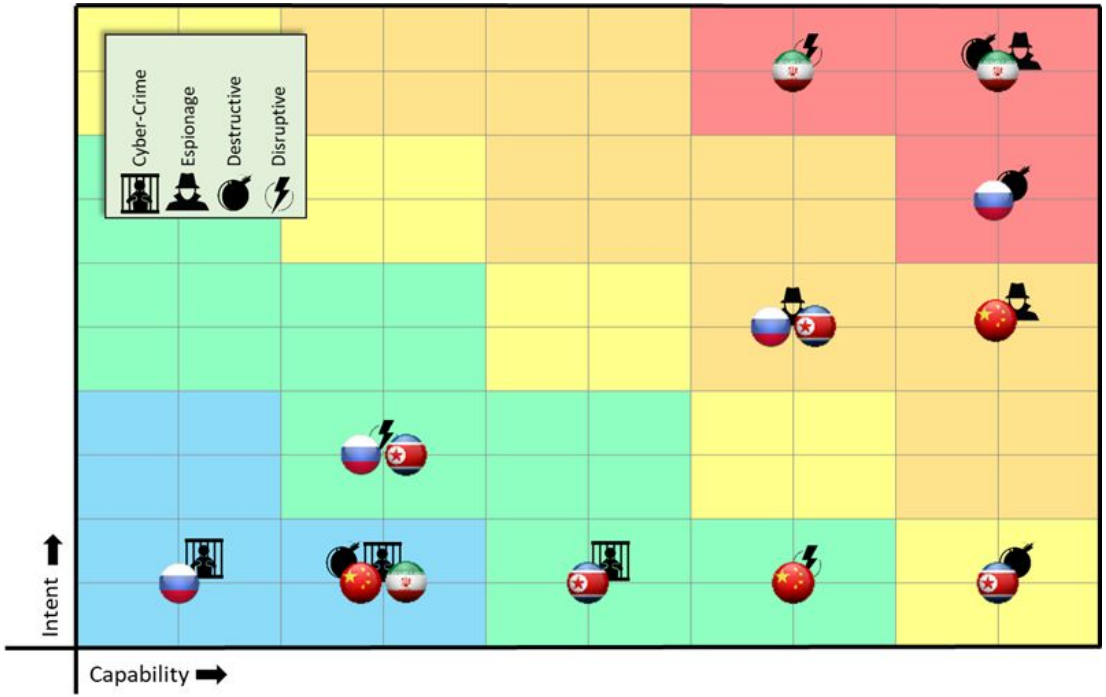
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

What is a threat?



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

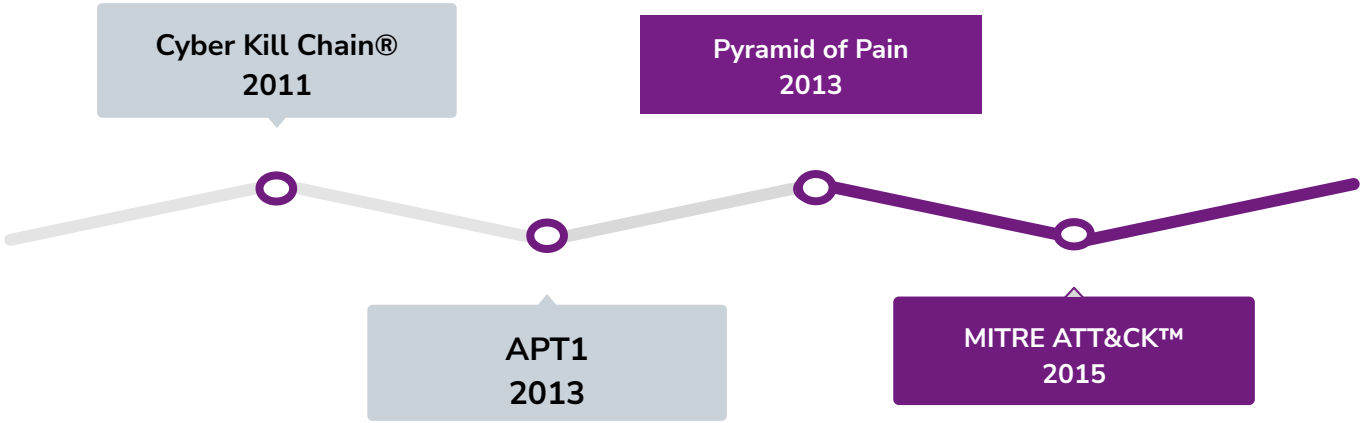
Prioritizing Threats – Threat Box



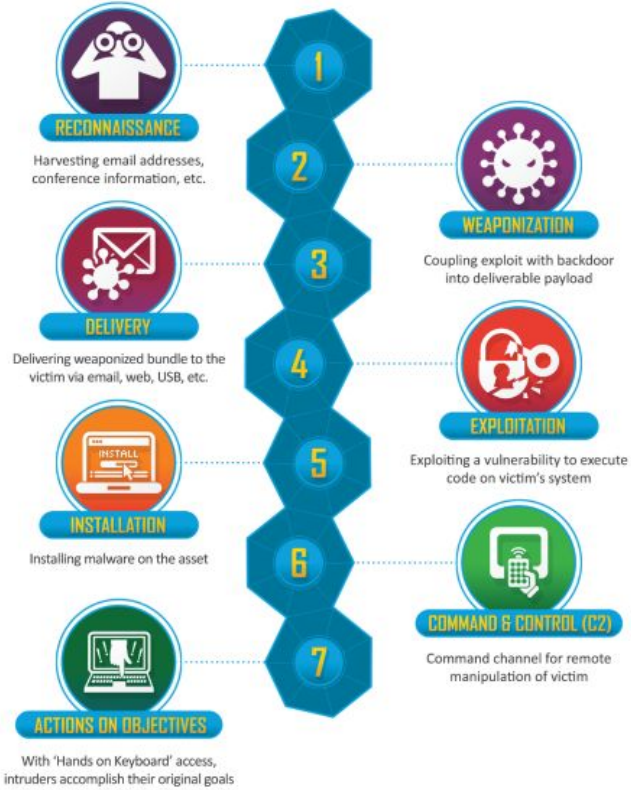
Andy Piazza - Threat Box

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

Intelligence Timeline

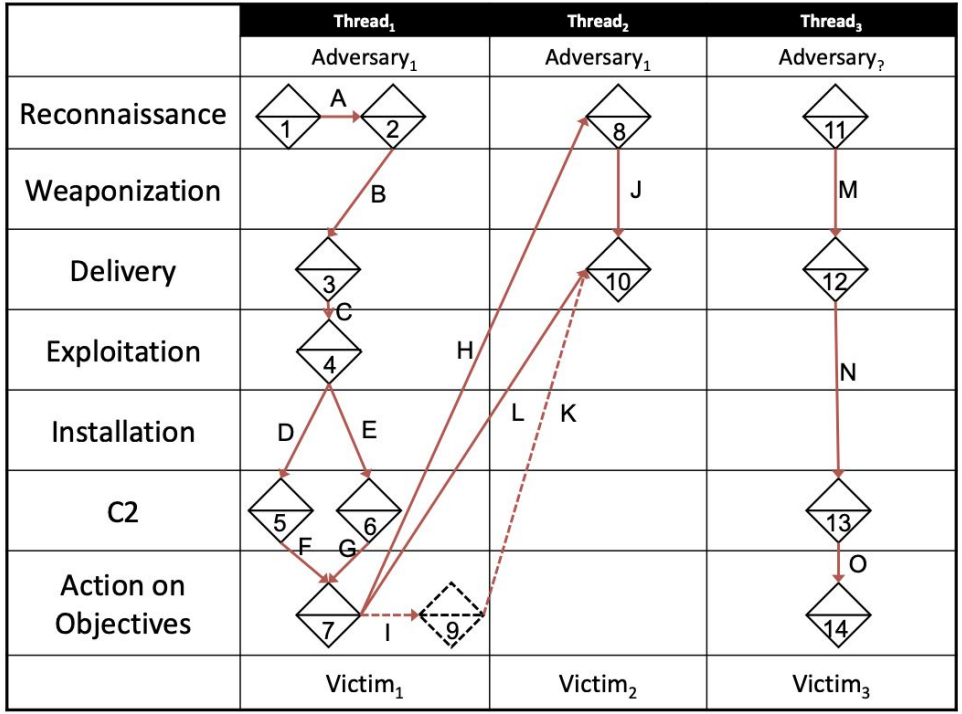


Lockheed Martin Cyber Kill Chain®



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

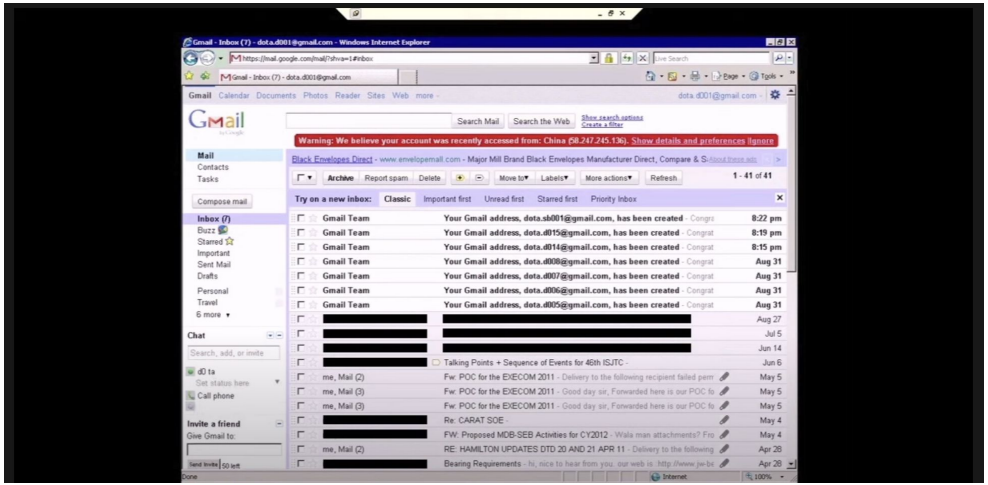
Kill Chain® Plus Diamond Model



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/mYaTCvA2VLQ

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"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

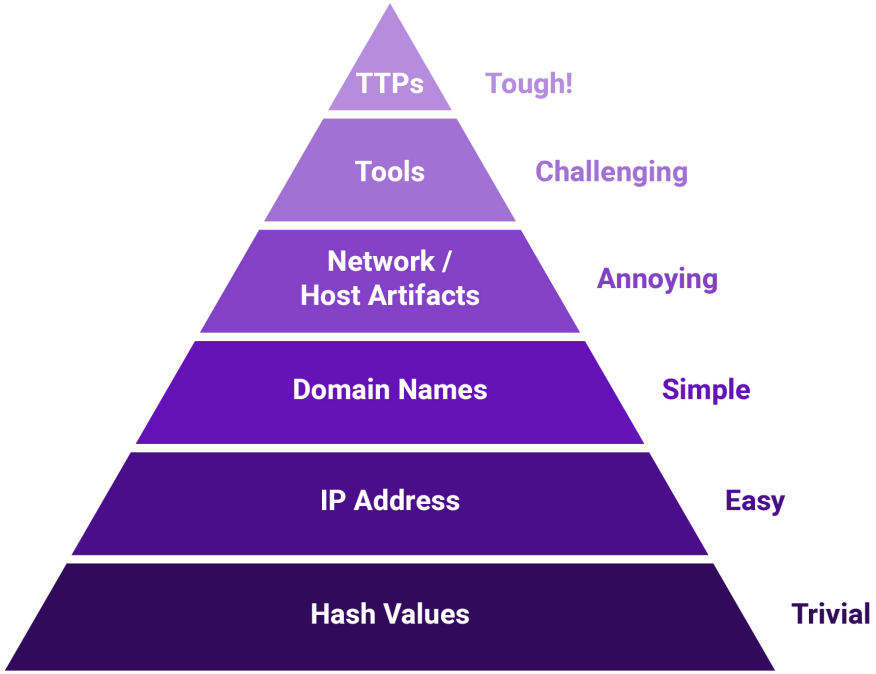
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

```
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.
```

https://github.com/scythe-io/community-threats/blob/master/Conti/Conti_Playbook_Translated.pdf

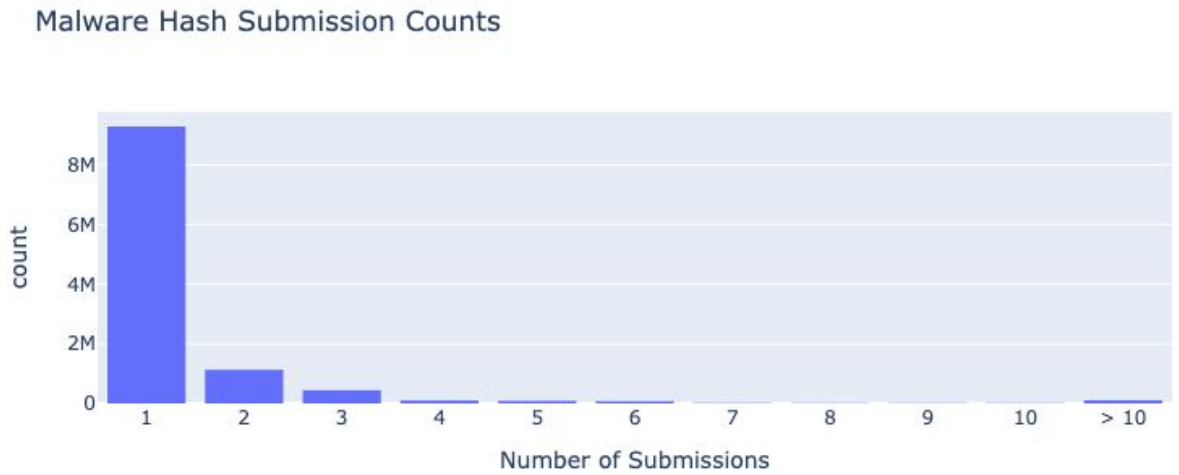
Pyramid of Pain

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

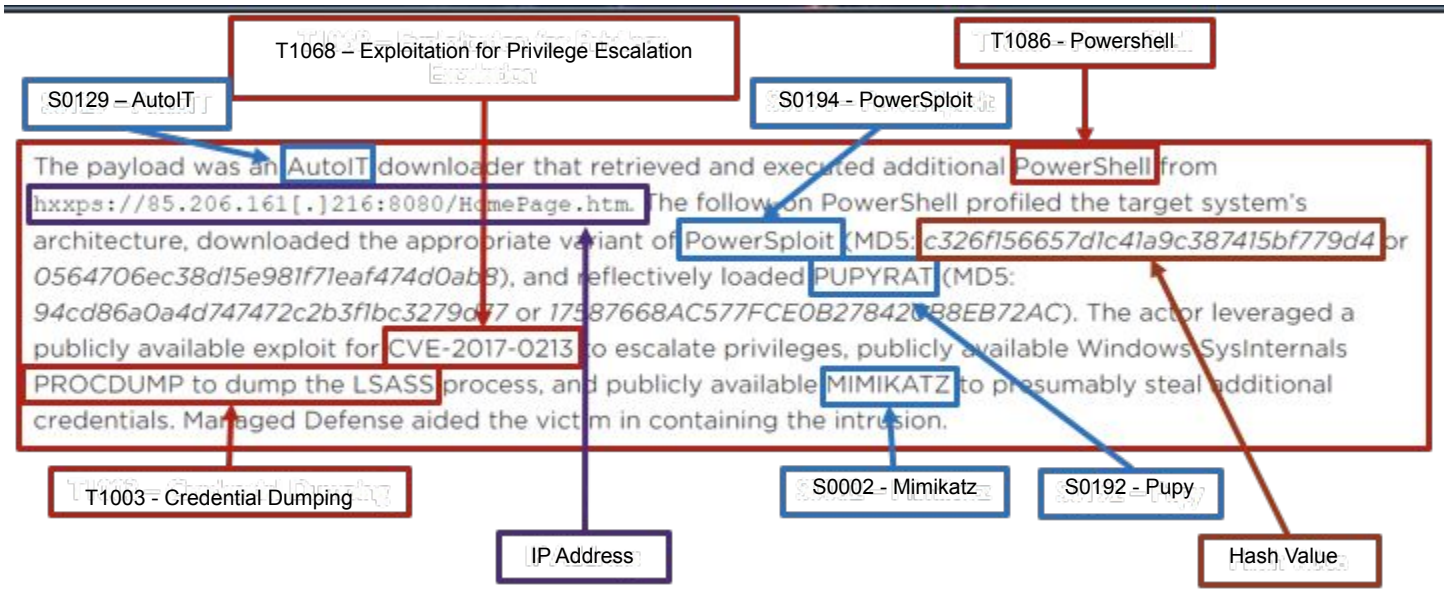


http://detect-respond.blogspot.com/2022/04/stop-using-hashes-for-detection-and.html

ATT&CK™

- 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

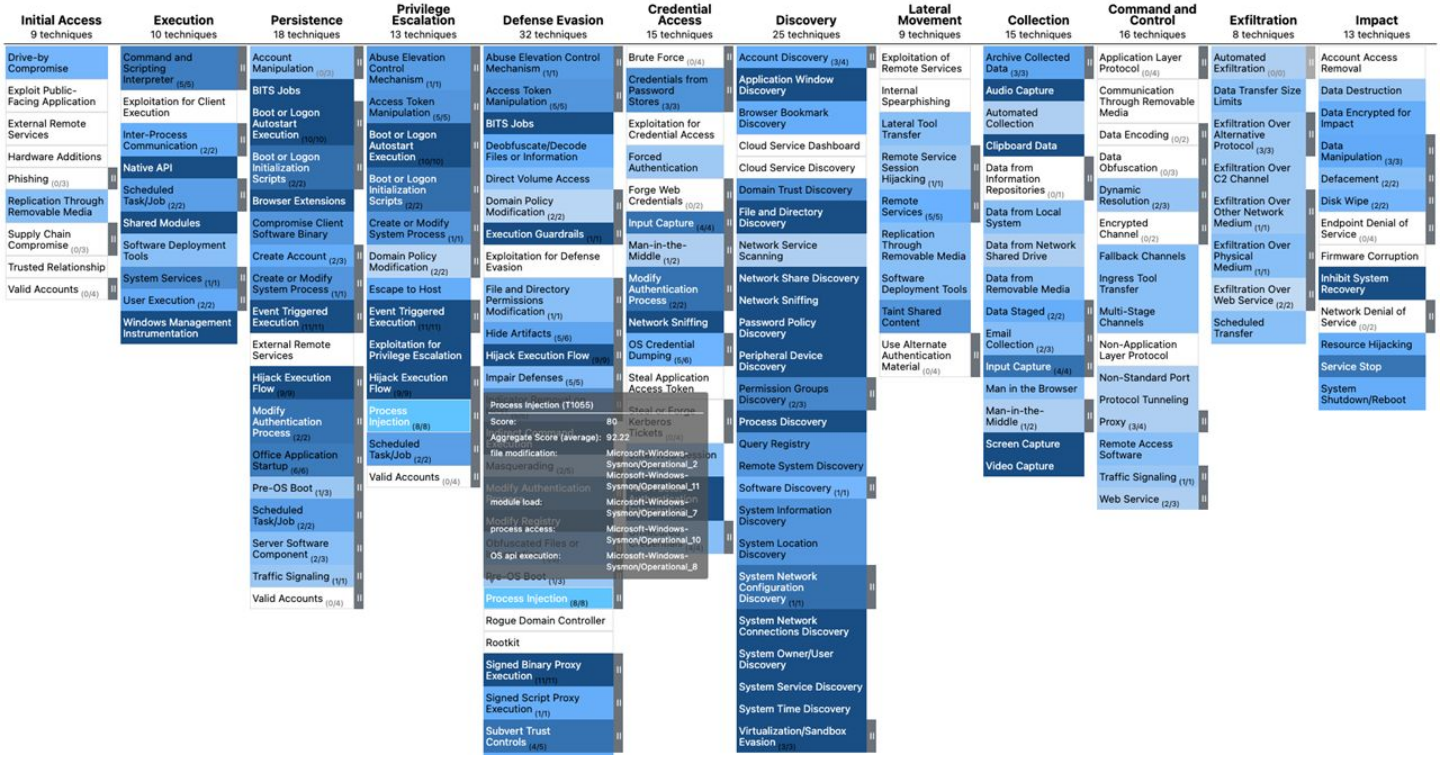


[ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK](#) - Katie Nickels and Cody Thomas

ATT&CK™ Techniques

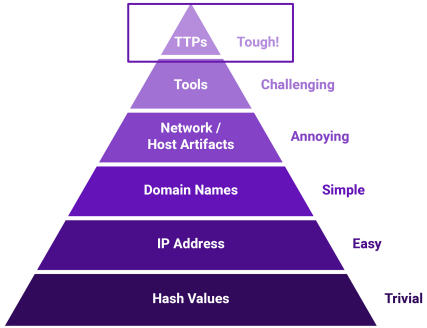
Jamie Williams @jamieantisocial

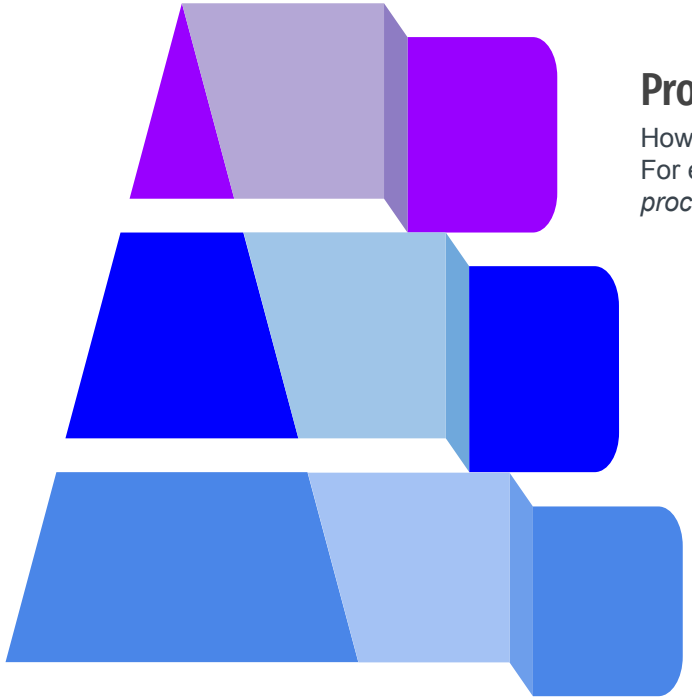
ATT&CK™ Check Box Fallacy



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

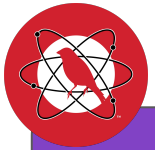
tasklist

Windows Command Line
T1059.003

wmic process get /format:list

Windows Management Instrumentation
T1047

Process Discovery T1057



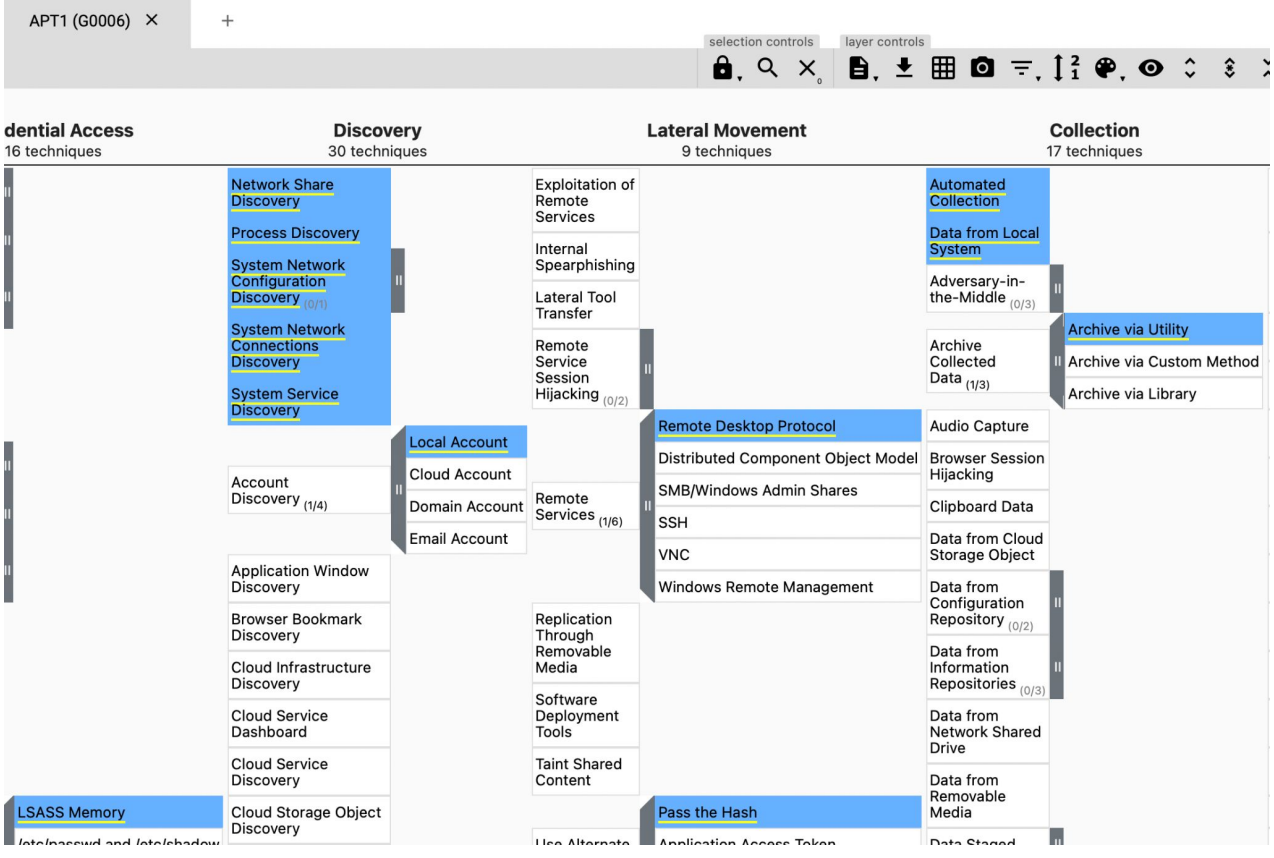
PowerShell
T1059.001

Get-Process

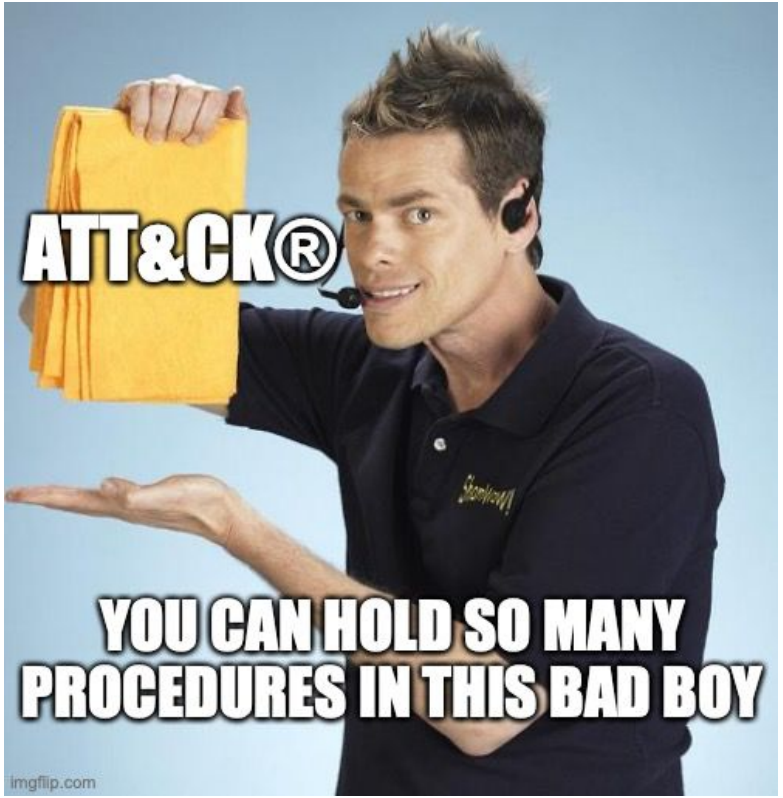
Native API
T1106

CreateToolhelp32Snapshot Function

Procedure Assumption – APT 1 Example

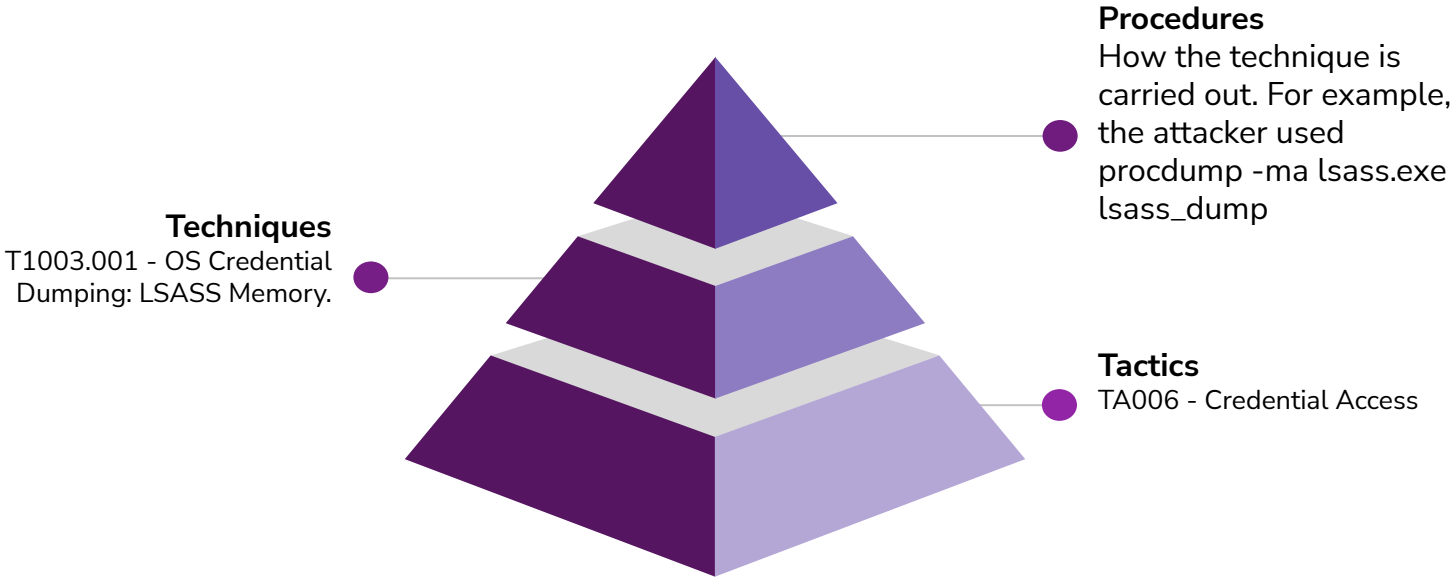


Procedures


ATT&CK®
YOU CAN HOLD SO MANY PROCEDURES IN THIS BAD BOY
imgflip.com

Procedures

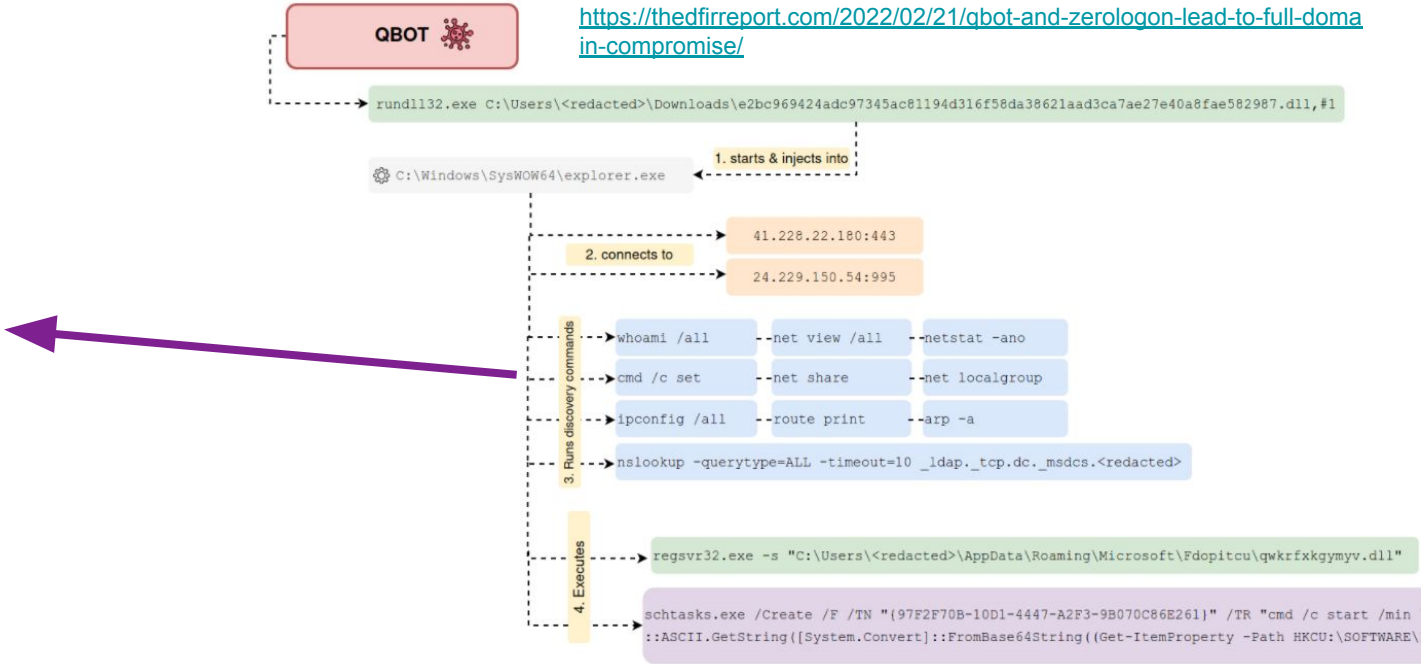
- How the adversary conducts the their techniques
  - Best for emulation and detection validation



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

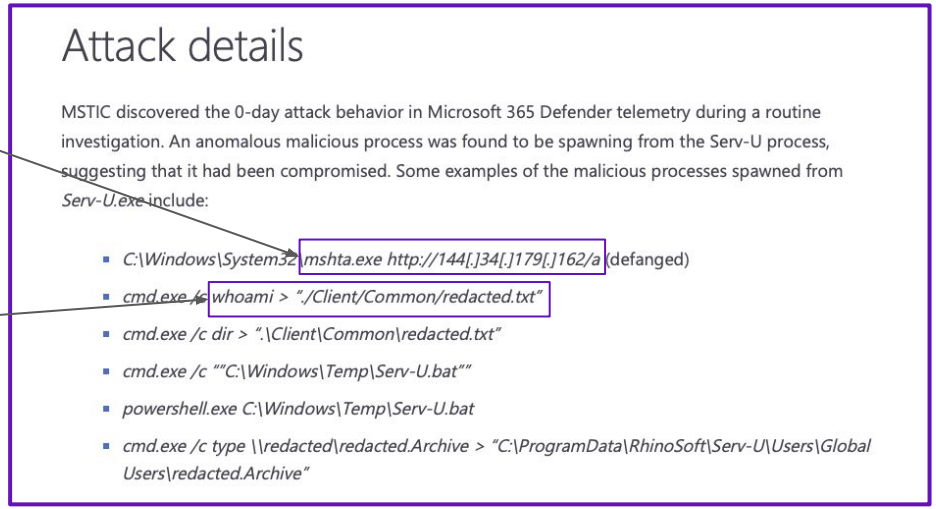
- Focus on the human element and behaviours
  - Training
  - Tools
  - Approved Actions
  - Runbooks
  - Habits
- Conti Playbook Example
  - “In one case, we observed the operator copying and pasting commands from a script, neglecting to provide the actual IPv4 addresses as the required parameter” -TheDFIRReport

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

https://thedfirreport.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



Microsoft MSTIC Blog

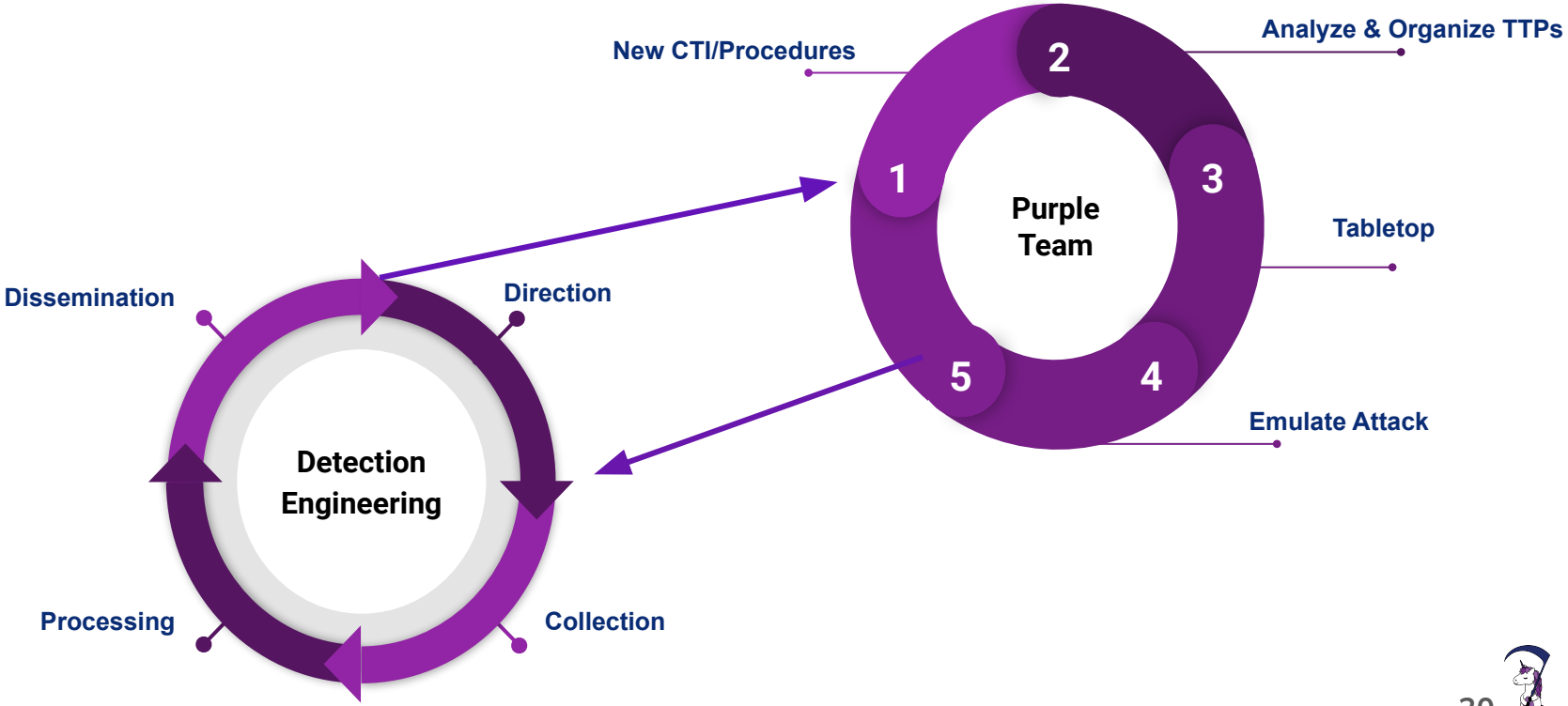
Cyber Threat Intelligence: Collecting

- 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

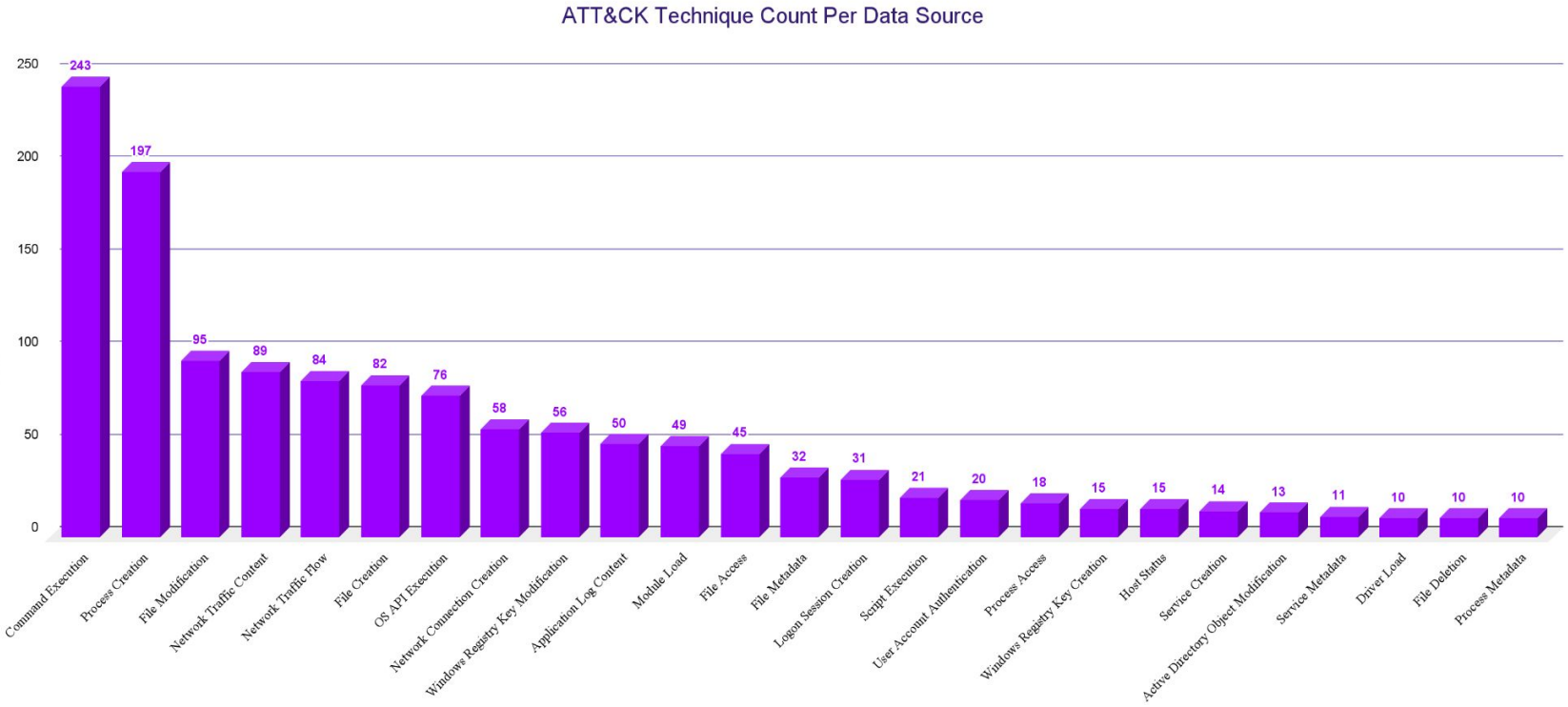
- ATT&CK™ Pivot
  - Procedure -> Technique -> Logs

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/

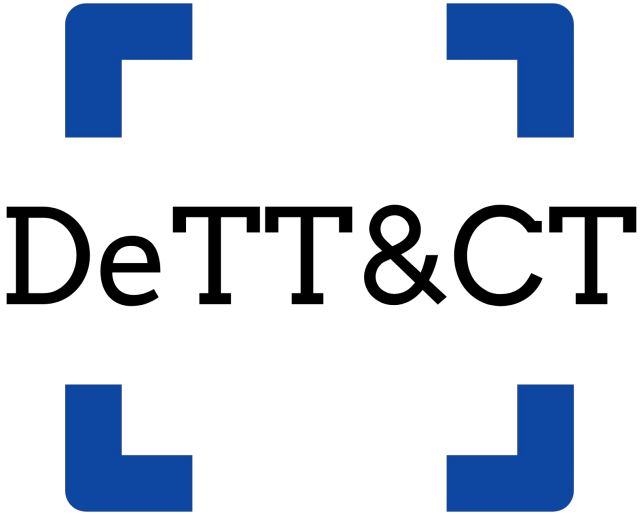
Logging: Prioritization



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

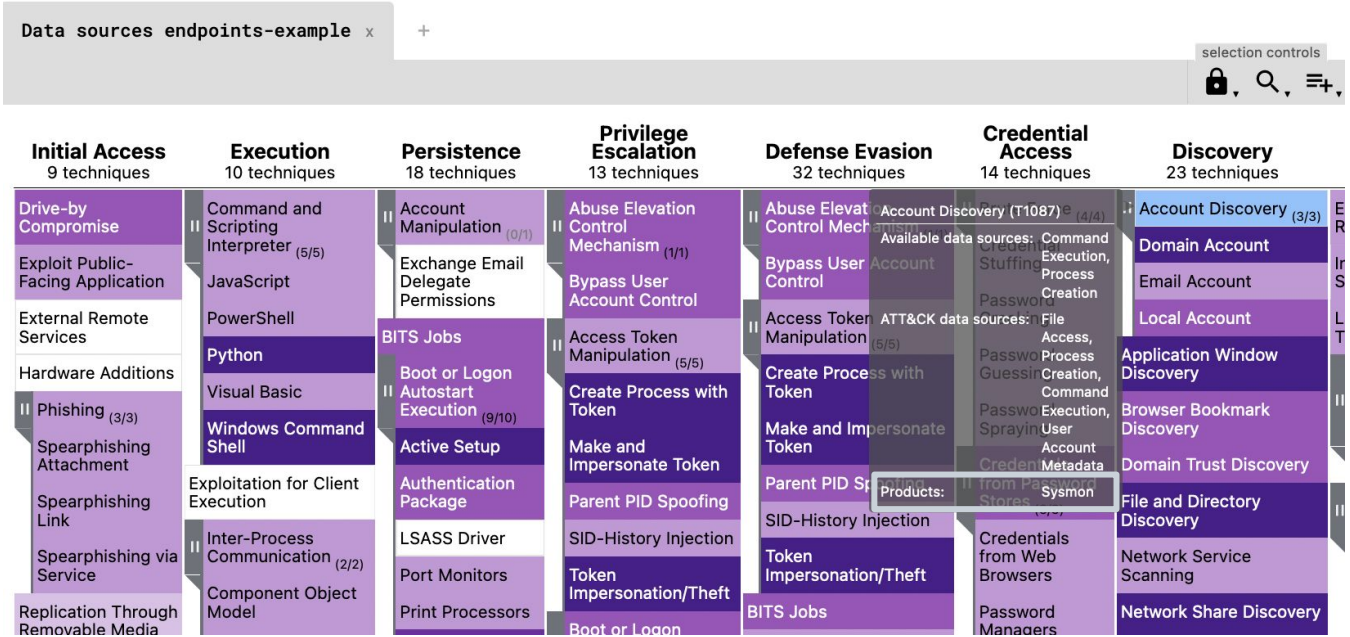
Collection: DeTT&CT

- “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



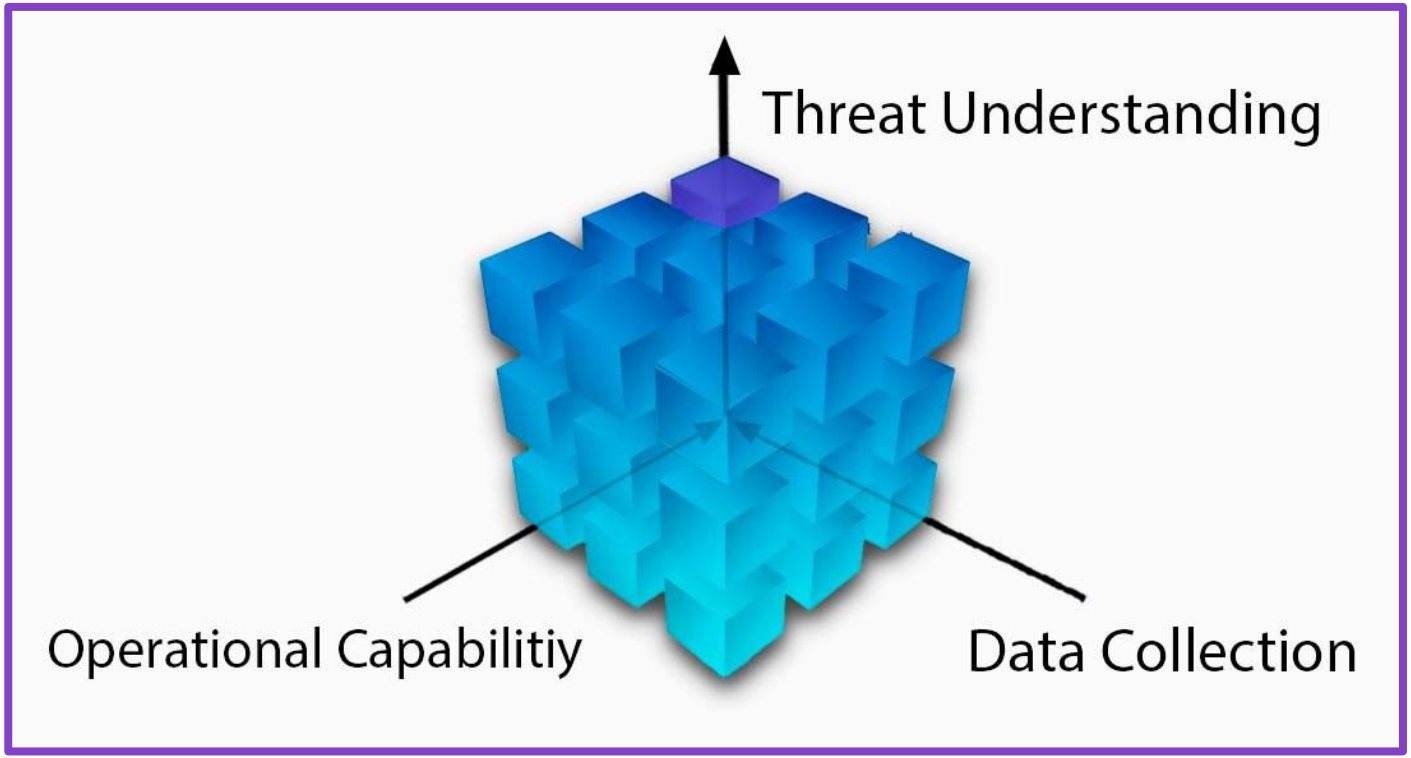
Collection: DeTT&CT

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



https://rabobank-cdc.github.io/dettect-editor/

Detection Drivers



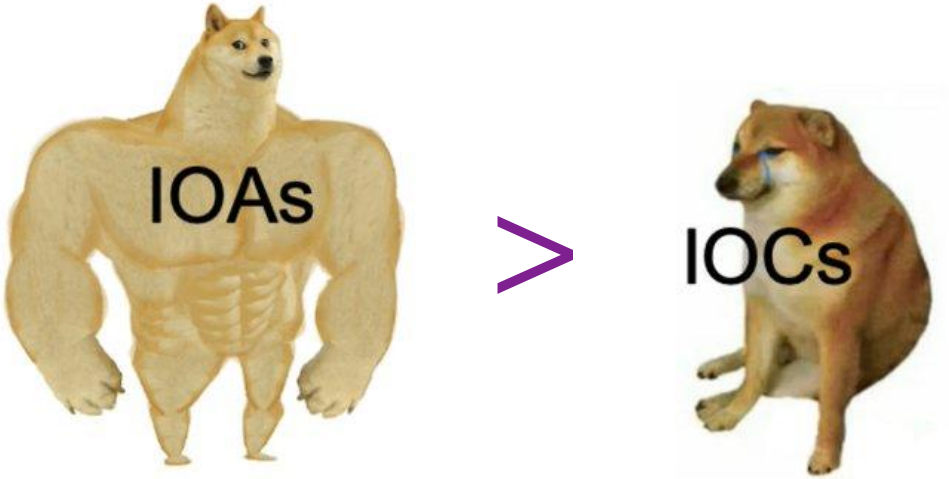
Detection Engineering

- 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-mgbot-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/ioa-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!

SCYTHE