Becoming a Proactive Defender

SCYTHE

Chris Peacock – Principal Detection Engineer

SCYTHE

Raytheon Intelligence & Space

GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

- Network Engineer
- SOC Analyst
- Threat Hunter
- Detection Engineer
- CTI Analyst
- Incident Responder
- Purple Team Lead
- GCTI, GCFA, GCED
- MITRE ATT&CK Contributor
- Sigma Contributor
- LOLBAS Contributor

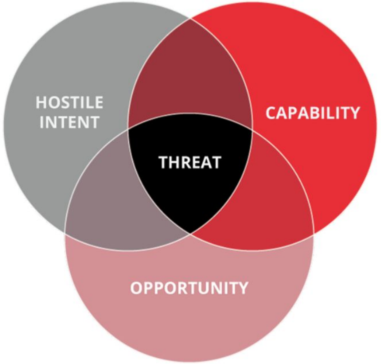
Starting Path

- Started Cyber Classes
  - Lab Guides vs Reality. Here’s an ASA have fun.
- Helpdesk
  - What do end users do and how can we support them?
- CompTIA Net+ & Network Engineer
  - PCAPs, Data Points, DNS, Internal vs External IP ranges.
- CompTIA Security+ & SOC1/2
  - Becoming blue/purple
- GCED to Threat Hunter
  - Diving deeper and evolving

Find Malware Fallacy

- Look for malware and remove it.
- Fails to look at attack paths and understand LOLBAS.
- Fails to understand the human threat behind attacks.

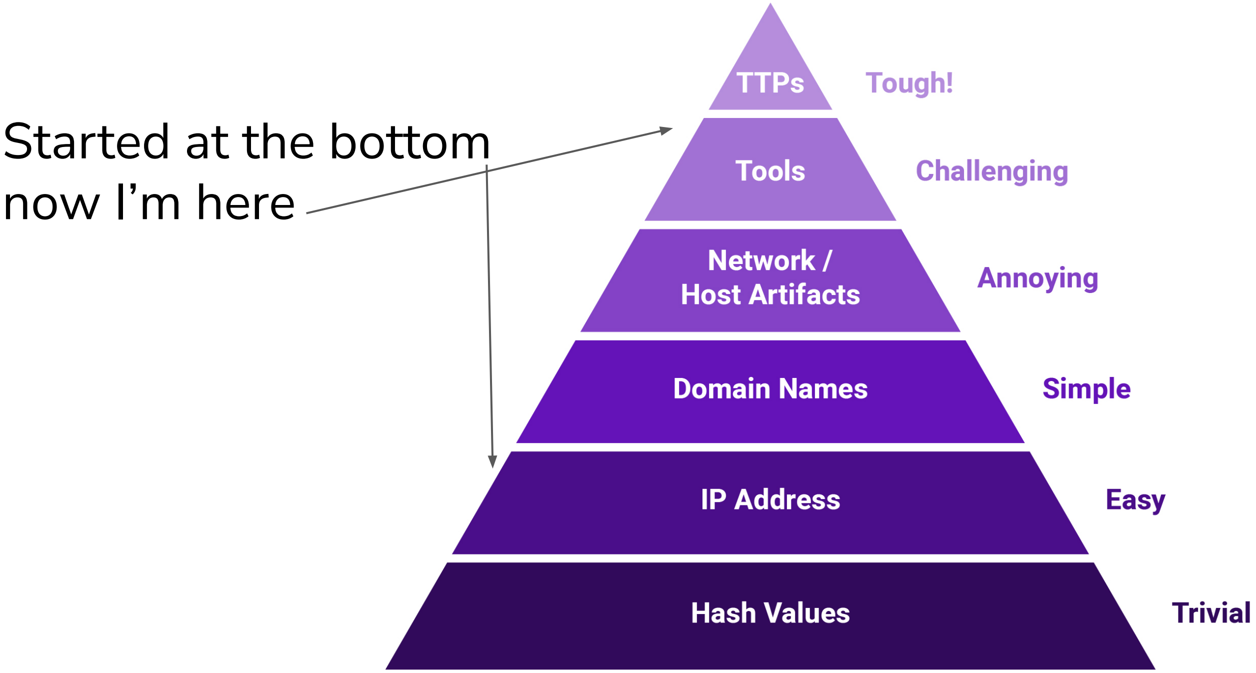
It's not malware it's a human or organization



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

Pyramid of Pain

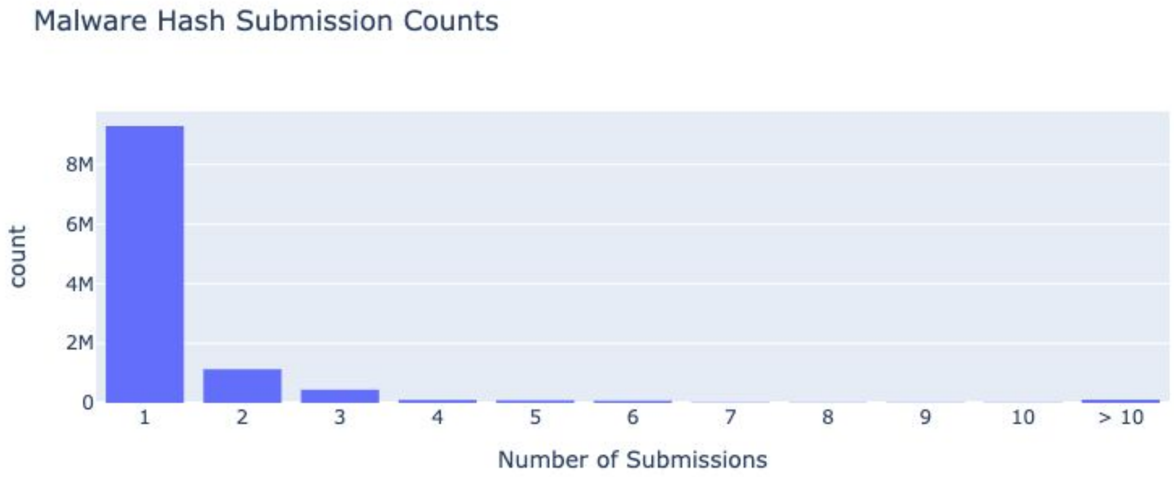
David Bianco: *http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html*



Started at the bottom now I'm here

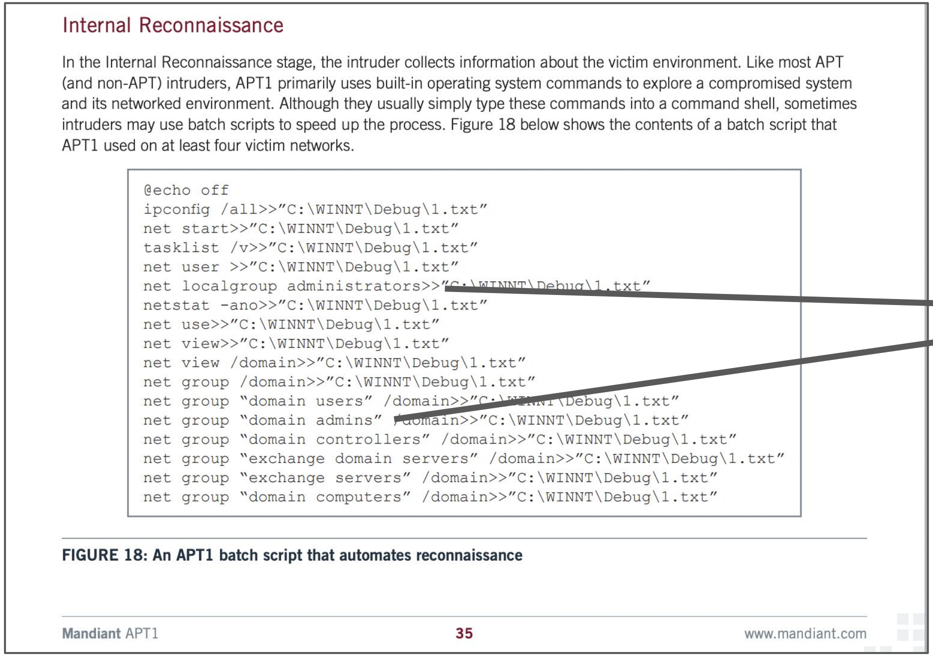
See, Hash Checks Aren't All That

"(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

We Stink at Behaviors: APT1 & Conti



Internal Reconnaissance

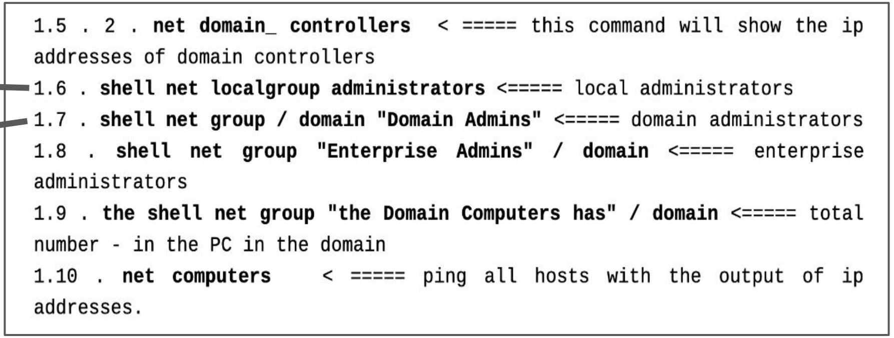
In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands 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

Mandiant APT1 35 www.mandiant.com

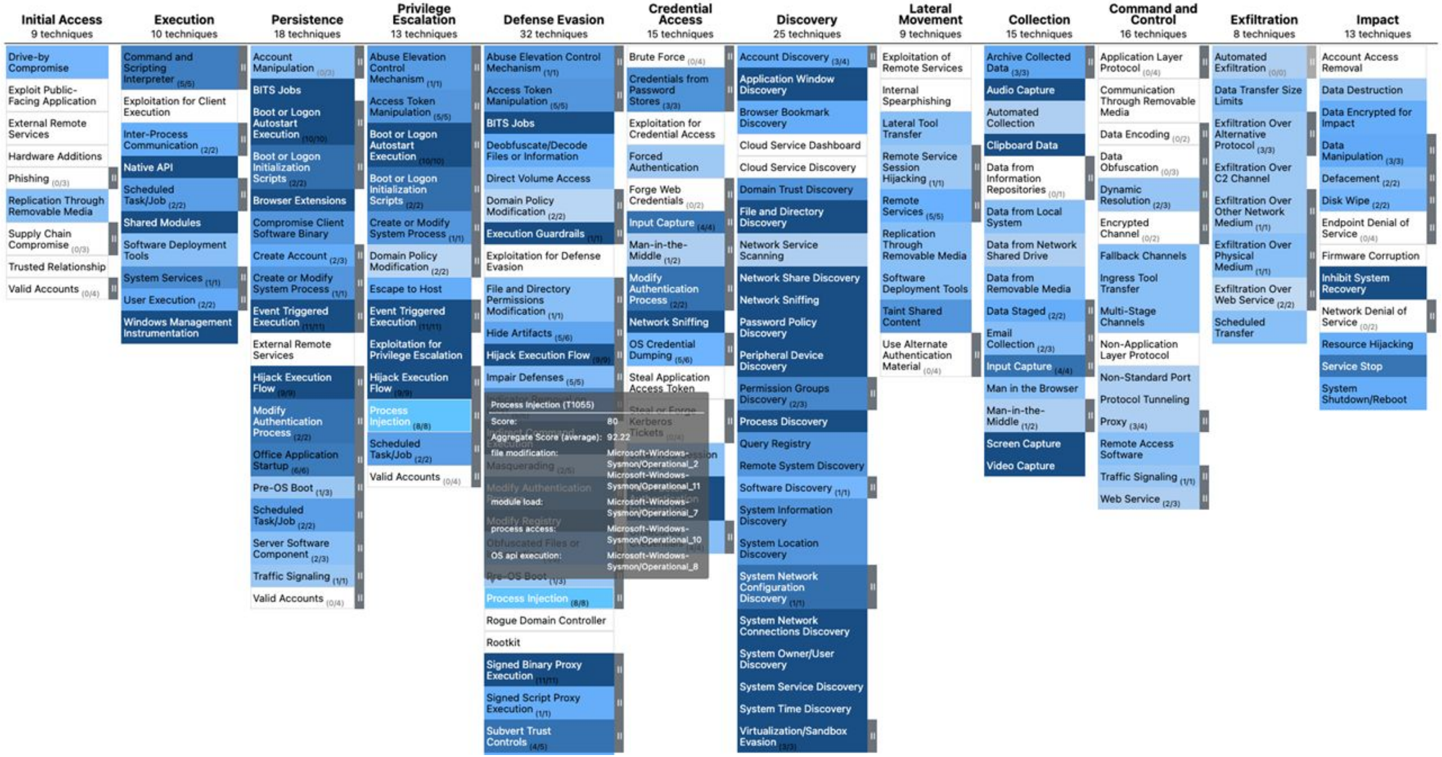
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf



```
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

Behaviors like Techniques? ATT&CK Check Box Fallacy



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
10 techniques

- Command and Scripting Interpreter (5/5)
- Exploitation for Client Execution
- Inter-Process Communication (2/2)
- Native API
- Scheduled Task/Job (2/2)
- Shared Modules
- Software Deployment Tools
- System Services (1/1)
- User Execution (2/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/3)
- BITS Jobs
- Boot or Logon Autostart Execution (10/10)
- Boot or Logon Initialization Scripts (2/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (2/3)
- Create or Modify System Process (1/1)
- Event Triggered Execution (11/11)
- External Remote Services
- Hijack Execution Flow (9/9)
- Modify Authentication Process (2/2)
- Office Application Startup (6/6)
- Pre-OS Boot (1/3)
- Scheduled Task/Job (2/2)
- Server Software Component (2/3)
- Traffic Signaling (1/1)
- Valid Accounts (0/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (1/1)
- Access Token Manipulation (5/5)
- Boot or Logon Autostart Execution (10/10)
- Boot or Logon Initialization Scripts (2/2)
- Create or Modify System Process (1/1)
- Domain Policy Modification (2/2)
- Escape to Host
- Event Triggered Execution (11/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (9/9)
- Process Injection (8/8)
- Scheduled Task/Job (2/2)
- Valid Accounts (0/4)

Defense Evasion
32 techniques

- Abuse Elevation Control Mechanism (1/1)
- Access Token Manipulation (5/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (2/2)
- Execution Guardrails (1/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (1/1)
- Hide Artifacts (5/6)
- Hijack Execution Flow (9/9)
- Impair Defenses (5/5)
- Indicator Removal on
- Indirect Command Execution
- Masquerading (2/5)
- Modify Authentication
- Modify Registry
- Obfuscated Files or
- Pre-OS Boot (1/3)
- Process Injection (8/8)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11/11)
- Signed Script Proxy Execution (1/1)
- Subvert Trust Controls (4/5)

Credential Access
15 techniques

- Brute Force (0/4)
- Credentials from Password Stores (3/3)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (4/4)
- Man-in-the-Middle (1/2)
- Modify Authentication Process (2/2)
- Network Sniffing
- OS Credential Dumping (5/6)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Unsecured Credentials (4/4)

Discovery
25 techniques

- Account Discovery (3/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (2/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1/1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (1/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3/3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (1/1)
- Remote Services (5/5)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
15 techniques

- Archive Collected Data (3/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories (0/1)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2/2)
- Email Collection (2/3)
- Input Capture (4/4)
- Man in the Browser
- Man-in-the-Middle (1/2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (2/3)
- 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 (1/1)
- Web Service (2/3)

Exfiltration
8 techniques

- Automated Exfiltration (0/0)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1/1)
- Exfiltration Over Physical Medium (1/1)
- Exfiltration Over Web Service (2/2)
- Scheduled Transfer

Impact
13 techniques

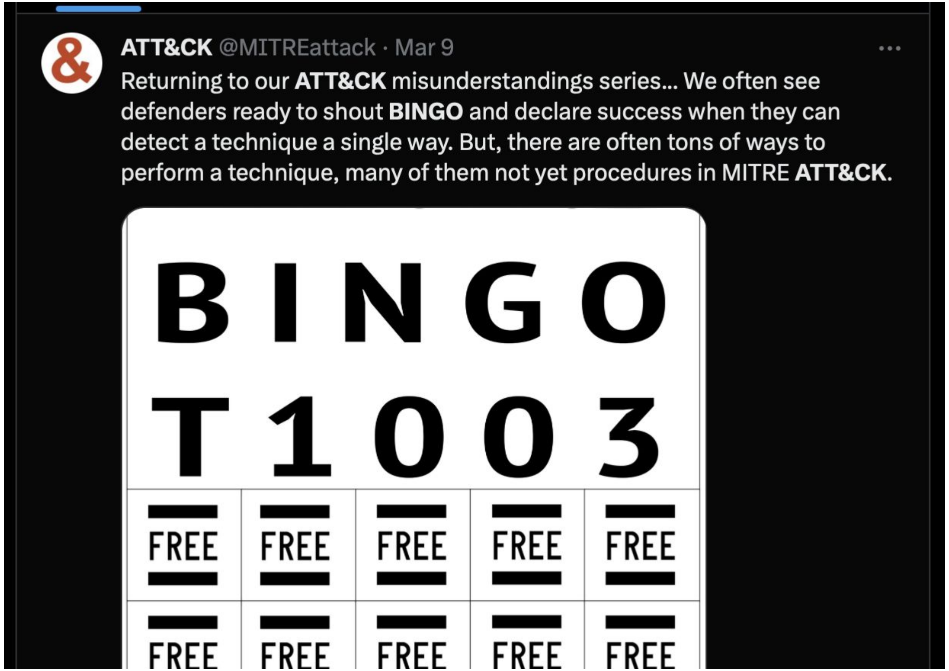
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3/3)
- Defacement (2/2)
- Disk Wipe (2/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Process Injection (T1055)

Score:	80
Aggregate Score (average):	92.22
file modification:	Microsoft-Windows-Sysmon/Operational_2 Microsoft-Windows-Sysmon/Operational_11
module load:	Microsoft-Windows-Sysmon/Operational_7
process access:	Microsoft-Windows-Sysmon/Operational_10
OS api execution:	Microsoft-Windows-Sysmon/Operational_8

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

STOP Shouting BINGO



ATT&CK @MITREattack · Mar 9

Returning to our **ATT&CK** misunderstandings series... We often see defenders ready to shout **BINGO** and declare success when they can detect a technique a single way. But, there are often tons of ways to perform a technique, many of them not yet procedures in MITRE **ATT&CK**.

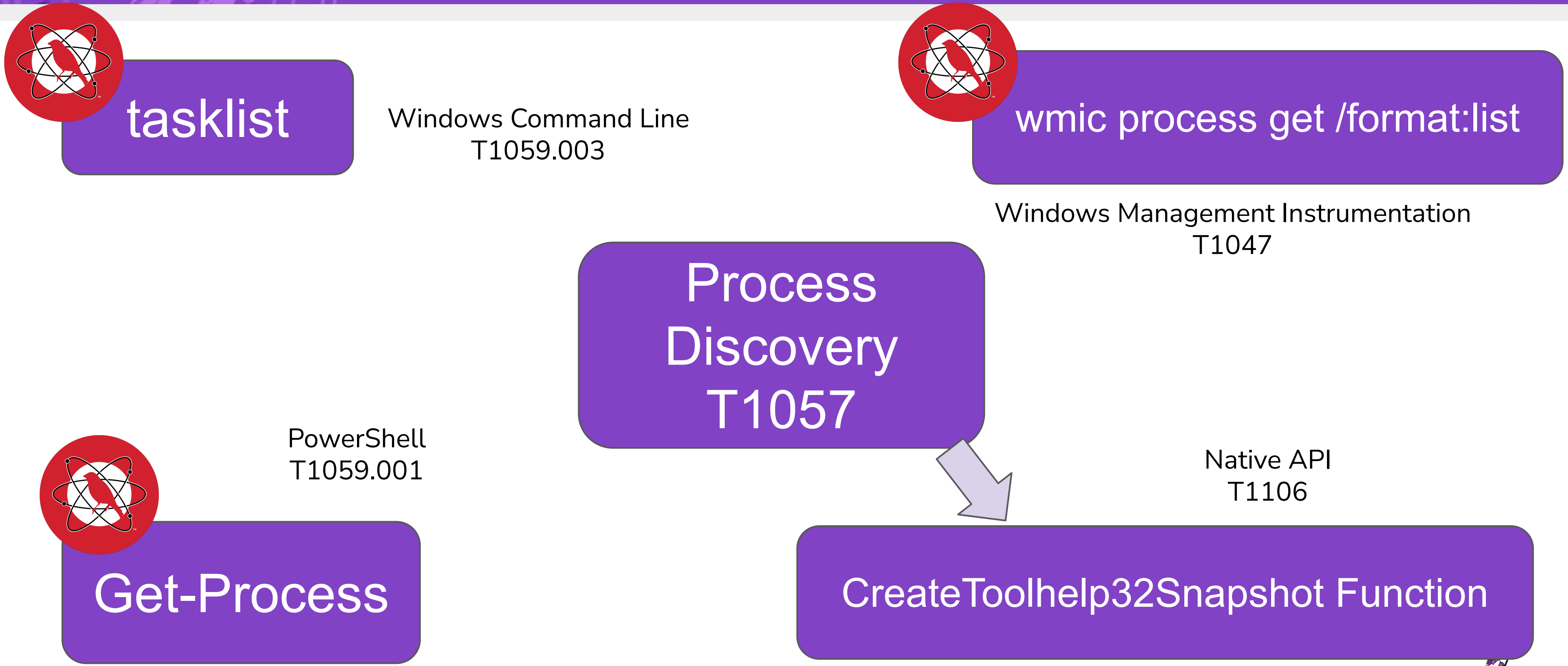
Who’s seen a report with Technique IDs?

SCYTHE

Who’s seen a report with what procedures were mapped to those Technique IDs?

SCYTHE

Procedure Assumption



tasklist

Windows Command Line
T1059.003

wmic process get /format:list

Windows Management Instrumentation
T1047

Process Discovery
T1057

PowerShell
T1059.001

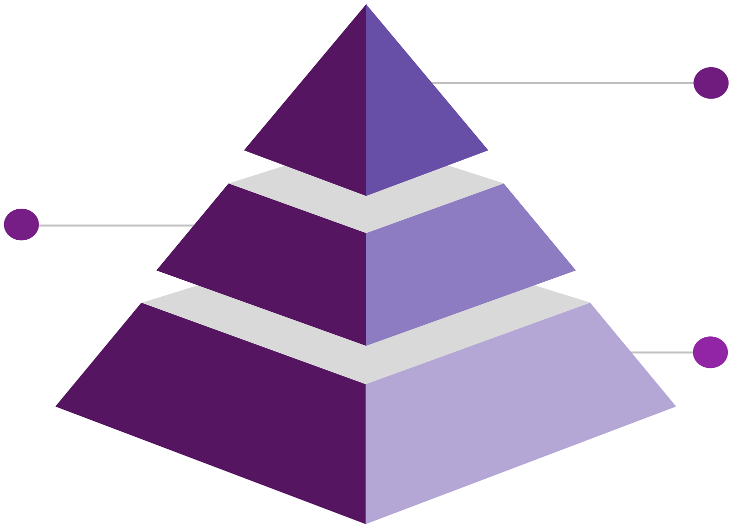
Get-Process

Native API
T1106

CreateToolhelp32Snapshot Function

Procedures

- How the adversary conducts their techniques
  - Best for emulation and detection validation
  - T1059.001 PowerShell & T1190: Exploit Public-Facing Application



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

Techniques
T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics
TA006 - Credential Access

How can I be more proactive?

IcedID Initial Discovery			
Procedure		Alert	Alert Level & Notes
1	ipconfig /all	✗	• No Alert • One Sigma Recommendation
2	systeminfo	✗	• No Alert • One Sigma Recommendation
3	whoami /groups	✓	• Low Alert • Tune if needed & Raise Alert Level • Two Sigma Recommendations
4	net config workstation	✗	• No Alert • One Sigma Recommendation
5	net use	✗	• No Alert • One Sigma Recommendation

How can I be more proactive?

Procedure		Alert	Level & Sigma
6	cmd /c echo %userdomain%	✗	• No Alert • Engineer custom alerts for ○ “echo <my_domain_name_here>” ○ “/c”
7	nltest /domain_trusts	✗	• No Alert • One Sigma Recommendation
8	nltest /domain_trusts /all_trusts	✗	• No Alert • Two Sigma Recommendations
9	net view /all /domain	✓	• Low Alert • Change to High/Critical • Two Sigma Recommendations
10	net view /all	✓	• Low Alert • Change to High/Critical • Two Sigma Recommendations

Proactive Keys

- What are my threats doing?
  - ISO Smuggling, Rundll32, Renamed LOLBAS?
- How do my defenses stand up to them?
  - What do I block, alert, and respond to?
- What can I do to improve my defenses?
- The best teacher is the adversary.
  - The adversary always gets a vote.
- Adapt, Adapt, Adapt.
  - It’s a cat and mouse game.

Common Mistakes

- PowerShell
- Rundll32
- Mshta
- Mimikatz on DC
- Renamed Binary

Get in the Film Room
&
Scrimmage

SCYTHE