MAGNET FORENSICS®

# Triage & Beyond: How Magnet Forensics Powers Incident Response

Doug Metz, Senior Security Forensics Specialist

10 October 2024

# Doug Metz, MCFE, GCFA, GCFE, GREM

- Joined Magnet in 2021
- Incident Response Manager
- HTCIA, Delaware Valley Chapter
- BakerStreetForensics.com

doug.metz@magnetforensics.com

**Cyber Unpacked**

Exploring enterprise DFIR

HTCIA

Delaware Valley - Philadelphia

BAKER STREET FORENSICS

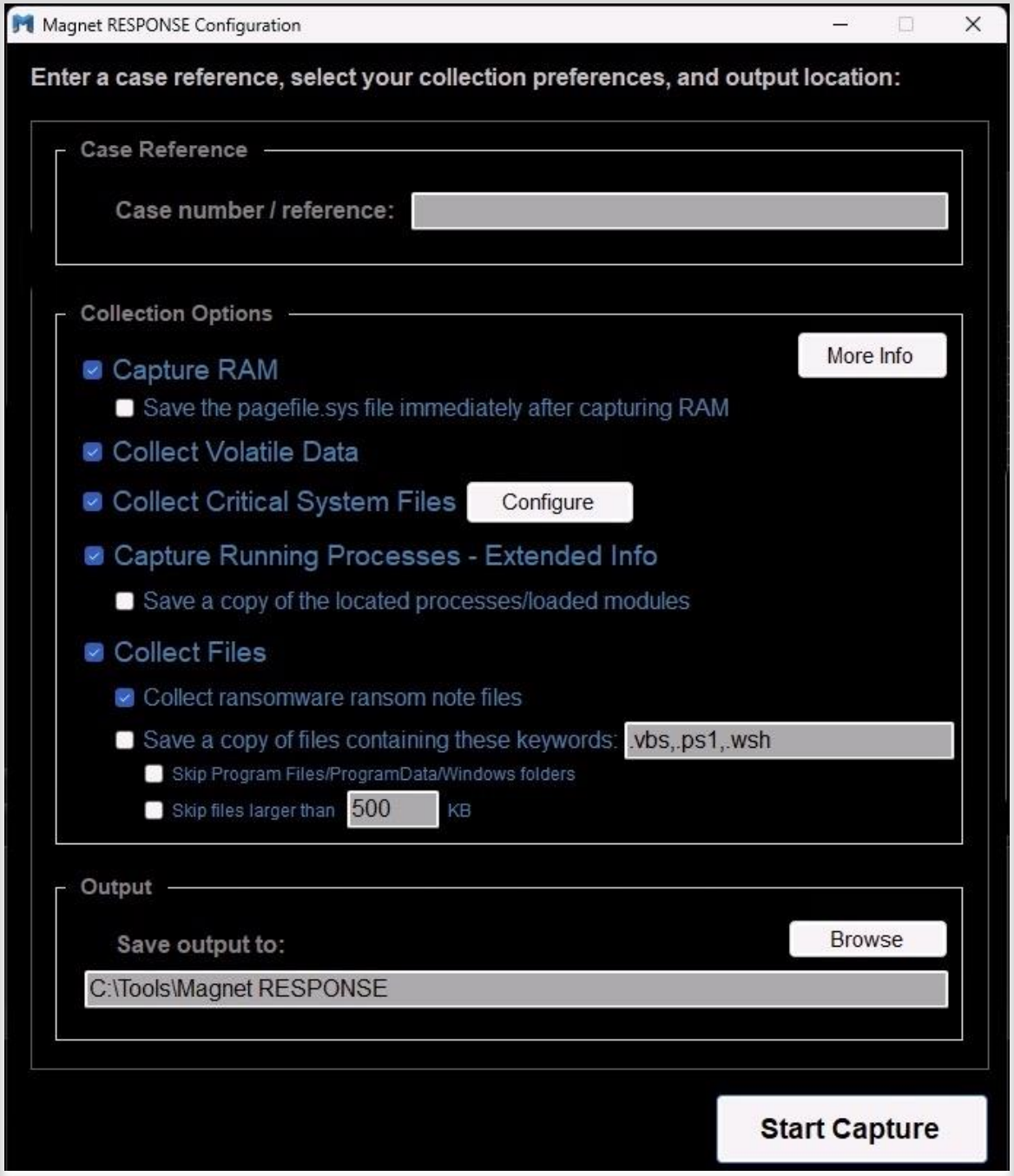
D . F . I . R .

# Triage in DFIR

- Incident Identification
- Impact Assessment
- Urgency Classification
- Containment and Mitigation
- Resource Allocation

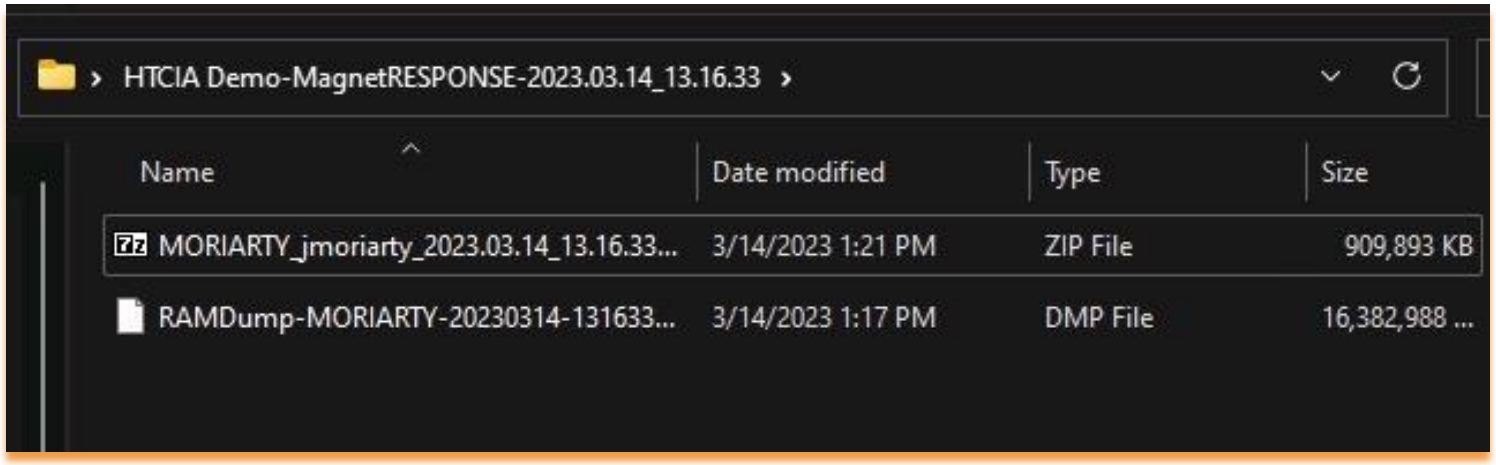
# Magnet RESPONSE

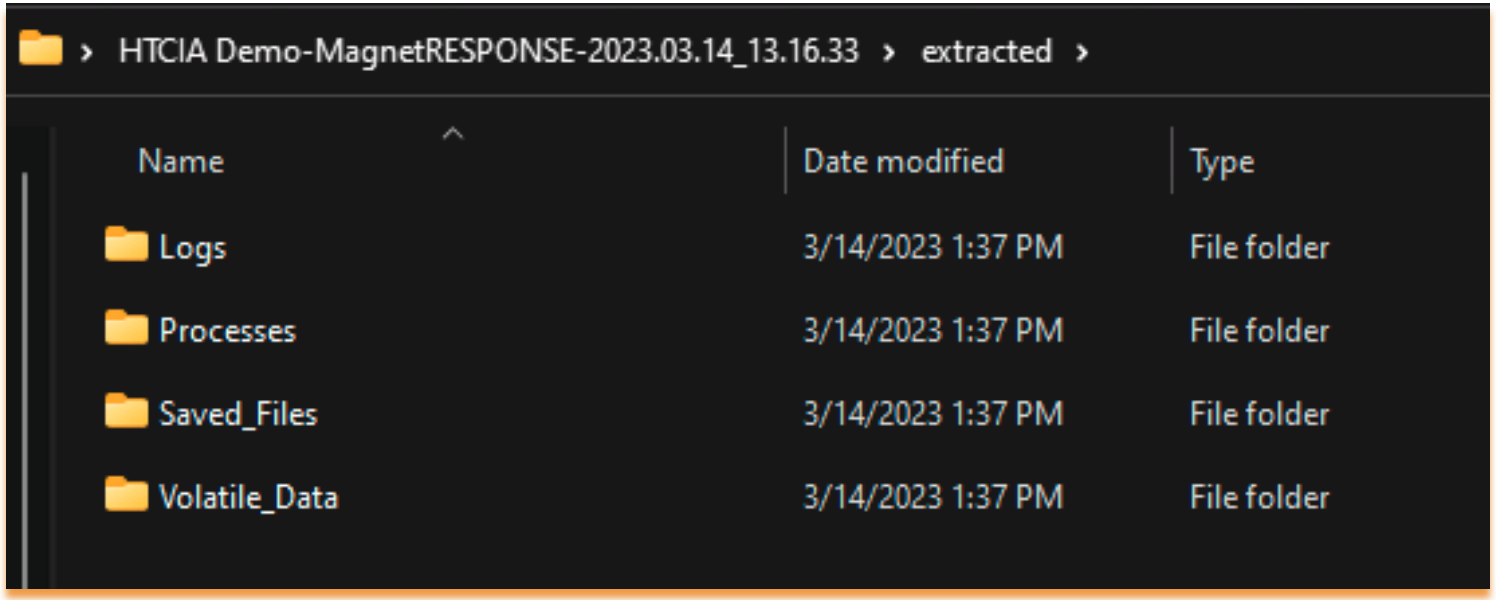
- Free triage collection tool
- Intuitive interface
- Collects RAM, Volatile info and Operating System artifacts



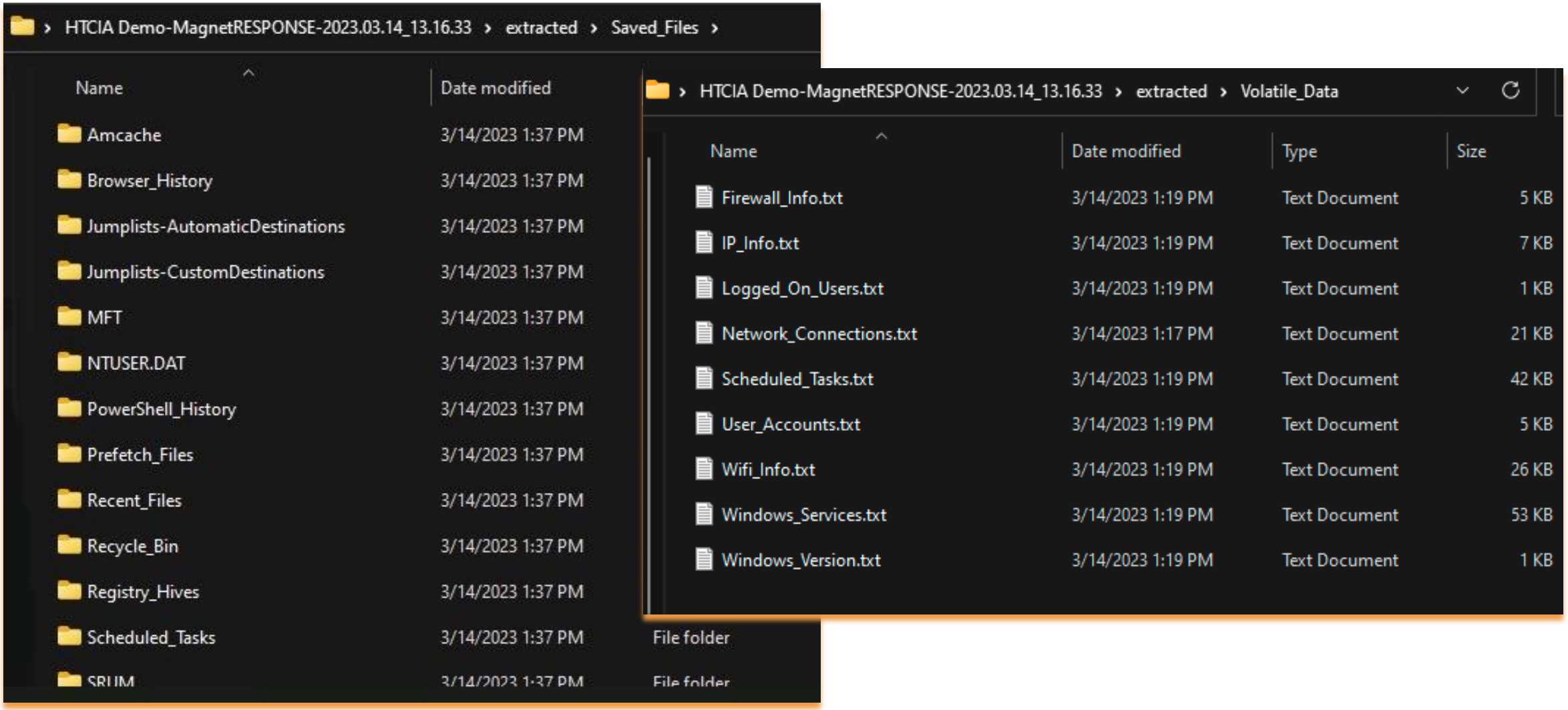
# Simplified Memory Capture


# Magnet RESPONSE Output

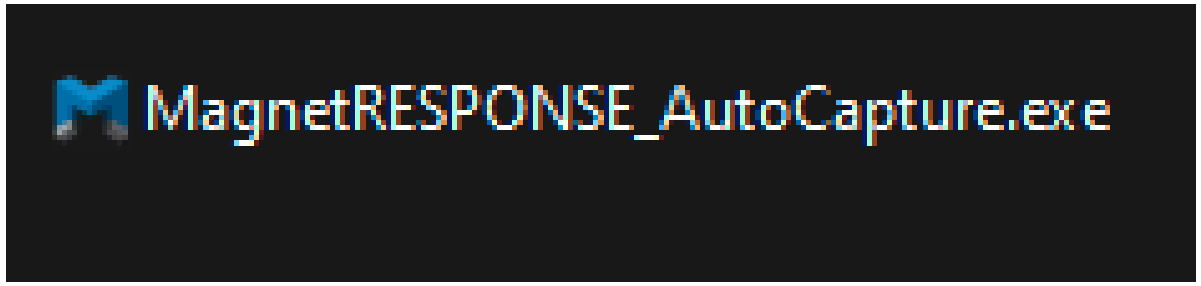


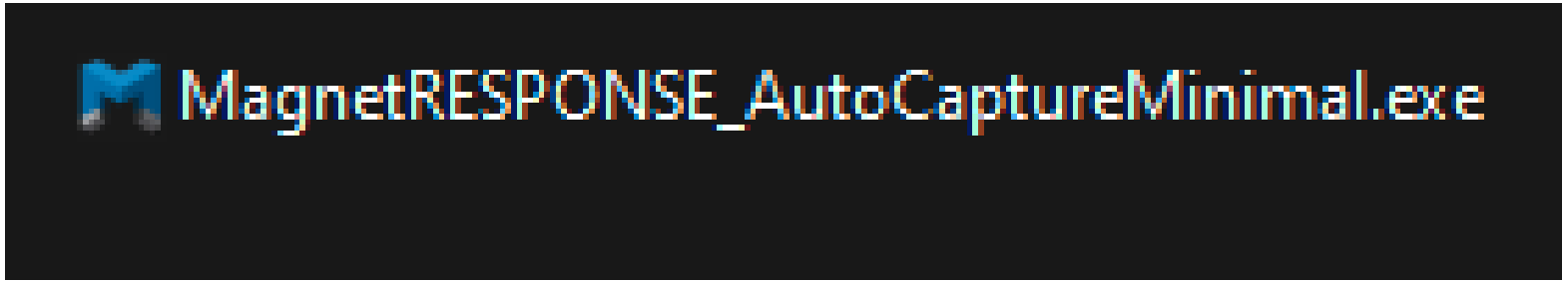



# Magnet RESPONSE Output

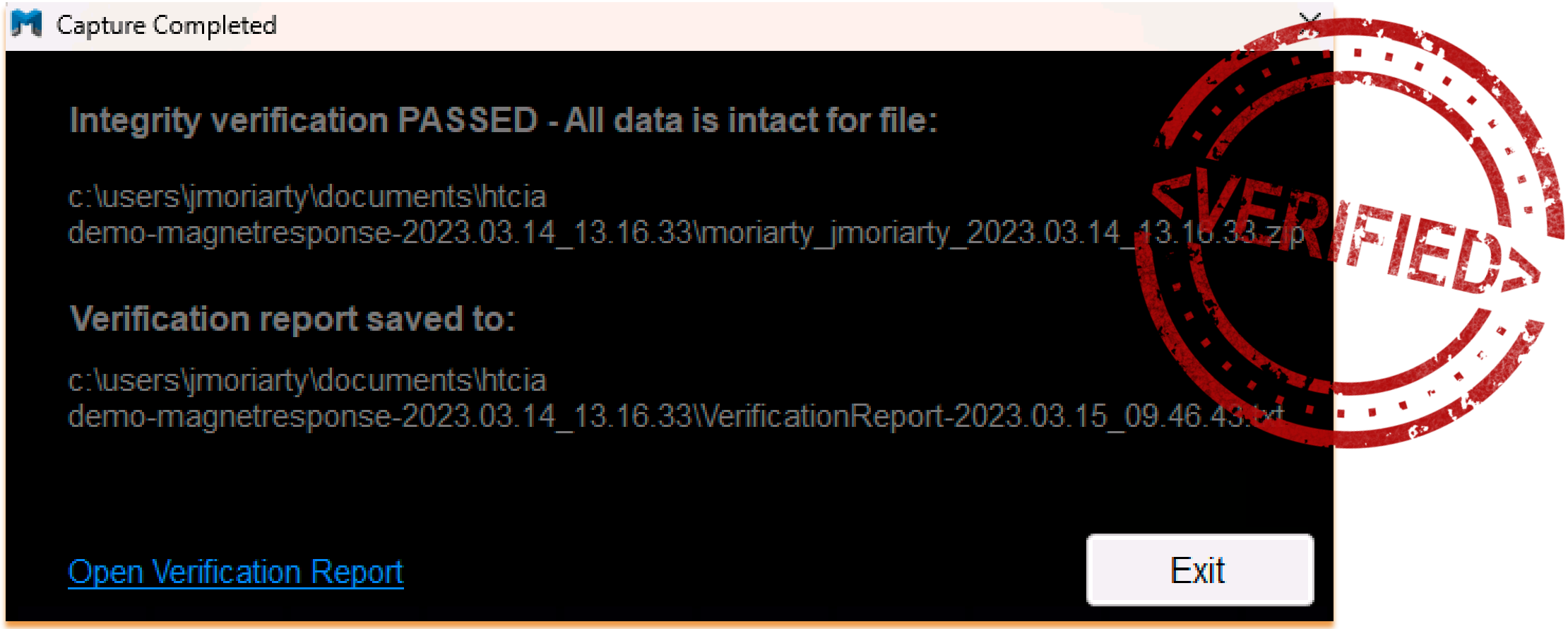


# Auto Collect Options



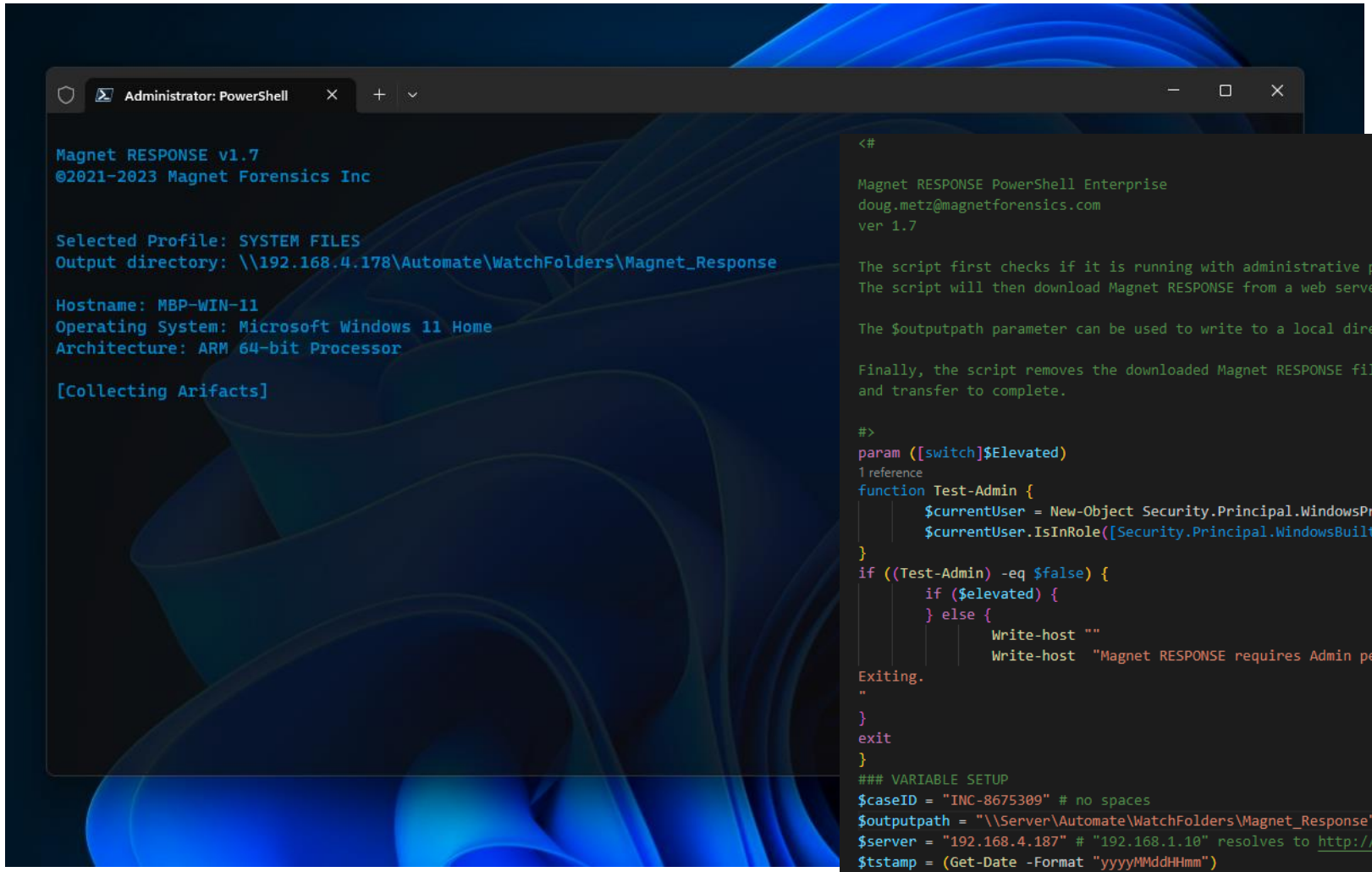
# Verifying a Capture Package



# Magnet RESPONSE CLI

| | |
|---|---|
| /captureram | - Enables RAM capture |
| /capturepagefile | - Enables capture of pagefile.sys file |
| /capturevolatile | - Enables volatile data capture |
| /capturesystemfiles | - Enables critical system file collection |
| /captureextendedprocessinfo | - Enables extended info capture for running processes/loaded modules |
| /saveprocfiles | - Enables saving copies of running processes/loaded modules. Must be used with /captureextendedprocessinfo switch |
| /capturefiles:<keyword.csv> | - Enables scanning for files with filenames containing specified keywords e.g. /capturefiles:secret,badfile,.vbs,confidential |
| /skipsystemfolders | - Indicates that the Program Files/ProgramData/Windows folders should be skipped when searching for files based on filename keywords. Must be used with /capturefiles |
| /maxsize:<file size in KB> | - Indicates the maximum file size to collect from hits found using /capturefiles – any files above this size are skipped e.g. /maxsize:500 |
| /captureransomnotes | - Enables the ransomware ransom note collection |
| /silent | - No GUI output to screen |

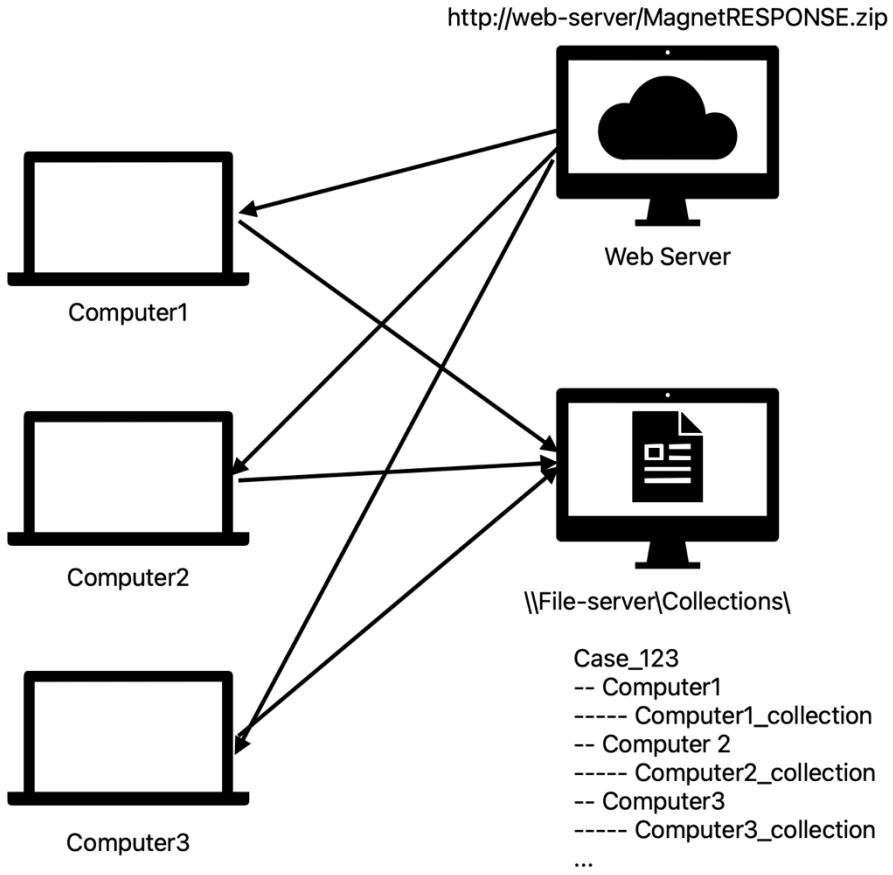
# Magnet RESPONSE PowerShell




```
<#

Magnet RESPONSE PowerShell Enterprise
doug.metz@magnetforensics.com
ver 1.7

The script first checks if it is running with administrative permissions and exits if not.
The script will then download Magnet RESPONSE from a web server, extract it, and run with the specified options.

The $outputpath parameter can be used to write to a local directory `C:Temp`, `D:\Output` or network `\\Server\Share`.

Finally, the script removes the downloaded Magnet RESPONSE files and prints the time taken for the collection
and transfer to complete.

#>
param ([switch]$Elevated)
1 reference
function Test-Admin {
        $currentUser = New-Object Security.Principal.WindowsPrincipal $([Security.Principal.WindowsIdentity]::GetCurrent())
        $currentUser.IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator)
}
if ((Test-Admin) -eq $false) {
        if ($elevated) {
        } else {
                Write-host ""
                Write-host  "Magnet RESPONSE requires Admin permissions.
Exiting.
"
}
exit
}
### VARIABLE SETUP
$caseID = "INC-8675309" # no spaces
$outputpath = "\\Server\Automate\WatchFolders\Magnet_Response" # Update to reflect output destination. C:\Temp R:\Output \\Server\Share
$server = "192.168.4.187" # "192.168.1.10" resolves to http://192.168.1.10/MagnetRESPONSE.zip
$tstamp = (Get-Date -Format "yyyyMMddHHmm")
#######
```

# Magnet RESPONSE PowerShell

- Web server hosting MagnetRESPONSE.zip
- File server with folder share for collections



# Case Variables

```
### VARIABLE SETUP
$caseID = "demo-161" # no spaces
$outputpath = ”\\server\share" # Update to reflect output destination.
$server = "192.168.4.187" # "192.168.4.187" resolves to http://192.168.4.187/MagnetRESPONSE.zip
```

$caseID – Name of your case or incident. (no spaces)

$outputpath – Where the collection output is sent

$server – Address for web server hosting MagnetRESPONSE.zip

# Collection Profiles

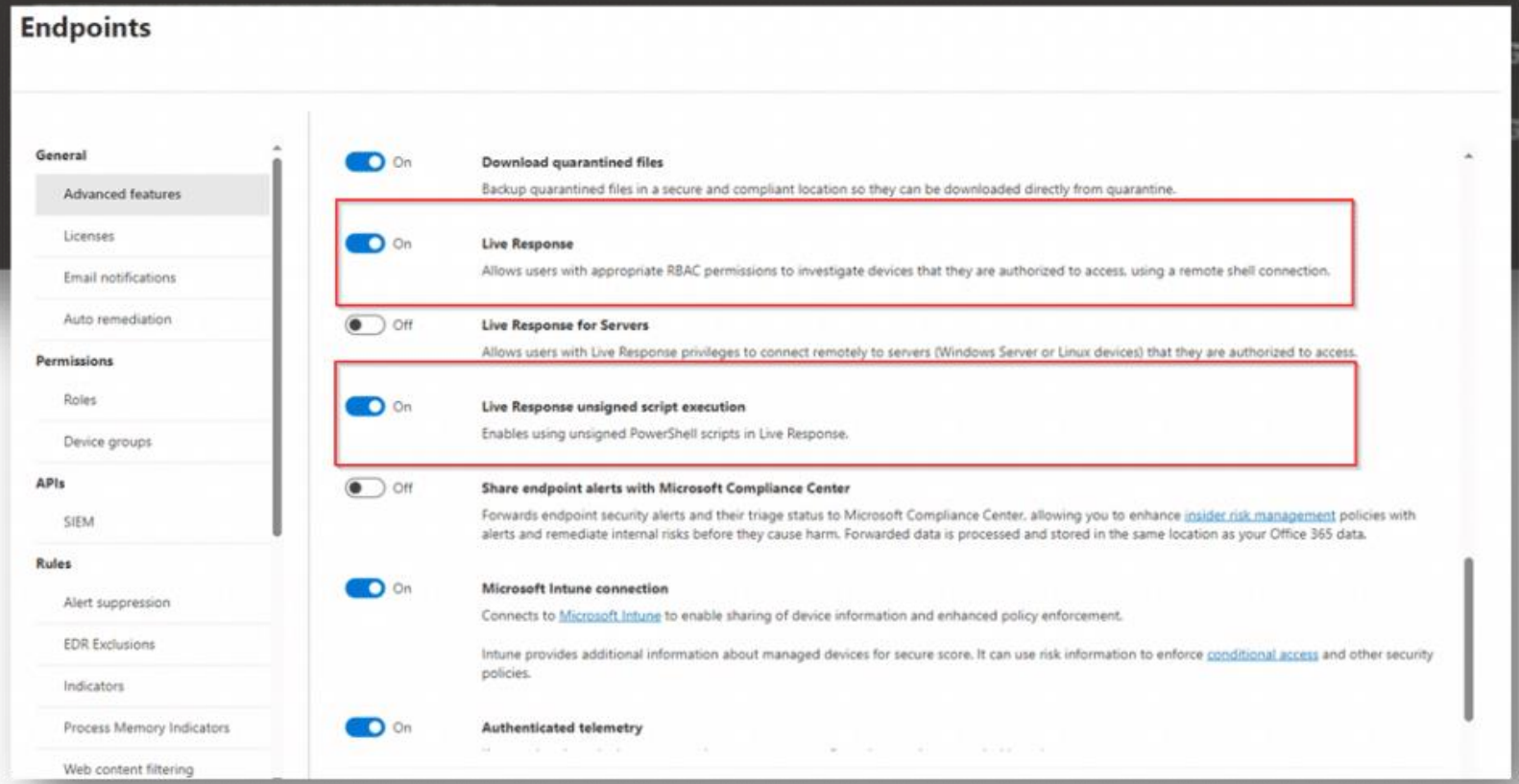
```
#### Extended Process Capture
<#
$profileName = "EXTENDED PROCESS CAPTURE"
$arguments = "/capturevolatile /captureextendedprocessinfo /saveprocfiles"
#>
#### Systen Files

$profileName = "SYSTEM FILES"
$arguments = "/capturesystemfiles"
#>
#### Just RAM
<#
$profileName = "CAPTURE RAM"
$arguments = "/captureram"
#>
```

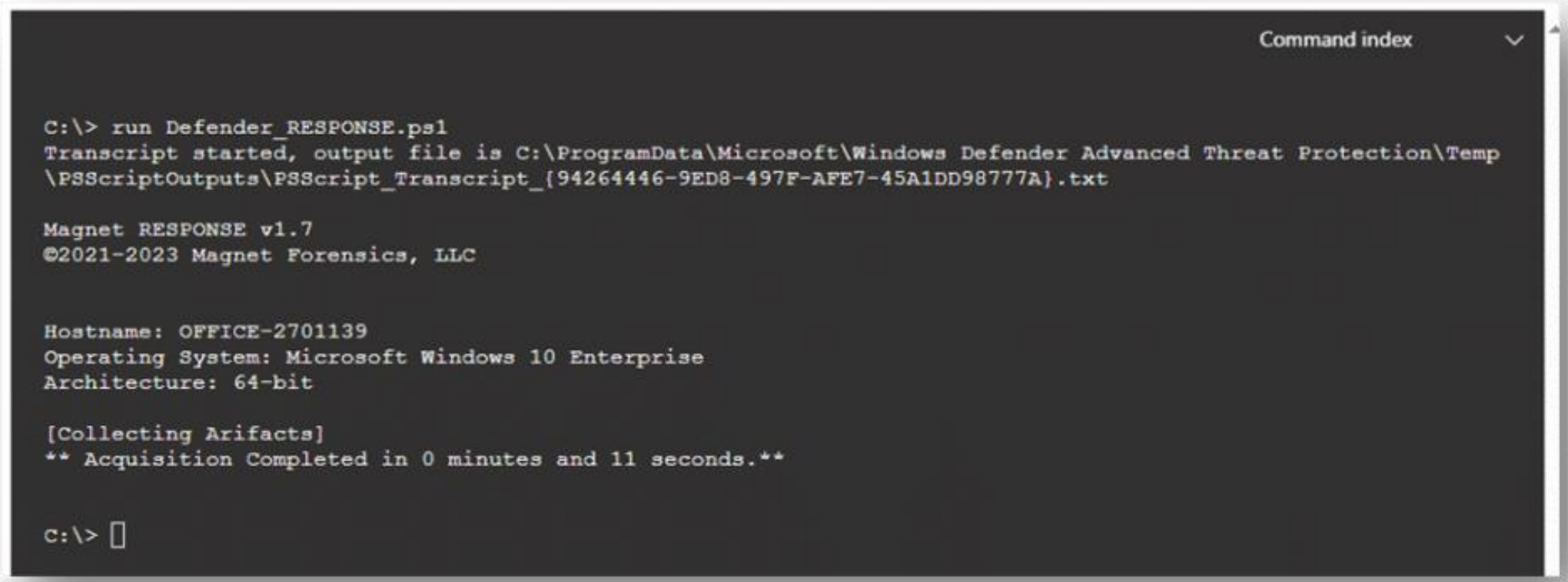
# Magnet RESPONSE and

**Microsoft Defender**
for Endpoint

# Defender_RESPONSE.ps1

```
C:\> library
File name                Description      Parameters      Parameters description  Uploaded on
                                  Uploaded by
========================  ============  ==========  ============================  ================================
Defender_RESPONSE.ps1                                                              GMT
-0500 (Eastern Standard Time)
MagnetRESPONSE.exe                                                                 GMT
-0500 (Eastern Standard Time)
```






Retrieving the Data from the Defender console:

Once the script finishes, the zipped output will be saved to "C:\Temp\RESPONSE" on the remote machine.

- Navigate to the output folder using the command — cd c:\Temp\RESPONSE
- List files using the "dir" command
- Copy the zip filename
- Download <filename.zip>

```
    .',;::ccccc:;.                        ...''''''..'.
   .;cccllllooooddxc.                  .';clooddoolcc::;:;.
   .:cccllllooooddxo.                .,coxxxxxdl:,'..
   'ccccclllooooddd'             .,,'lxkxxxo:'.
   'ccccclllooooddd'         .,:lxOkl,;oxo,.
   ':ccccllloooodddo.      .:dkOOOOkkd;''.
   .:ccccllloooooddo.   ..;lxkOOOOOkkkd;
   .;ccccllloooooddc:coxkkkkOOOOOOx:.
    'ccccllloooooddddxxxxkkkkOOOOx:.
     ,ccclllooooddddxxxxxkkkxlc,.
      ':lllloooooddddxxxxxoc;.
        .';:cloodddddolc:,..
            ''''''''''
```

# CyberPipe


```
CyberPipe IR Collection Script v5.0
https://github.com/dwmetz/CyberPipe
@dwmetz | ©2024 bakerstreetforensics.com


Mapping network drive...
Drive is mapped.
Collections directory exists.
Host directory created.


Running MAGNET Response...


Magnet RESPONSE v1.7
©2021-2024 Magnet Forensics Inc


Hostname:           MORIARTY
Operating System:   Microsoft Windows 11 Pro
Architecture:       64-bit
Selected Profile:   Volatile (testing)
Output Directory:   \Collections\MORIARTY-202402131644


Collecting Artifacts...
```

# CyberPipe (v5)

**Functions:**

- Capture a memory image with MAGNET DumpIt for Windows, (x32, x64, ARM64), or MAGNET RAM Capture on legacy systems;
- Create a Triage collection with MAGNET Response;
- Check for encrypted disks with Encrypted Disk Detector;
- Recover the active BitLocker Recovery key;
- Save all artifacts, output, and audit logs to USB or source network drive.

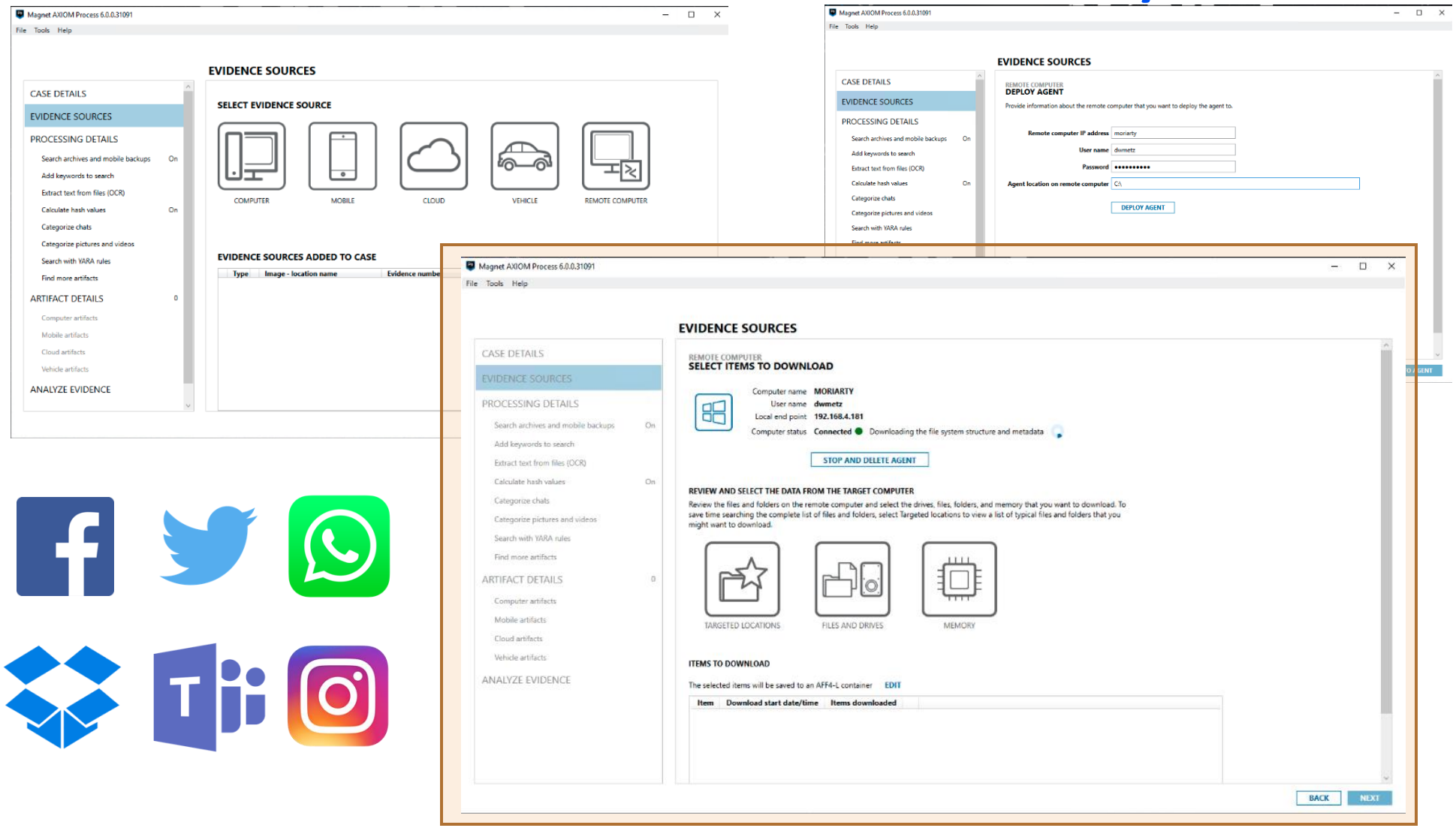
**Collection Profiles:**

- Volatile Artifacts
- Triage Collection (Volatile, RAM, Pagefile, Triage artifacts)
- Just RAM
- RAM & Pagefile
- or build your own using the RESPONSE CLI options

**Prerequisites:**

- MAGNET Response
- MAGNET Encrypted Disk Detector

# Remote Collections with AXIOM Cyber



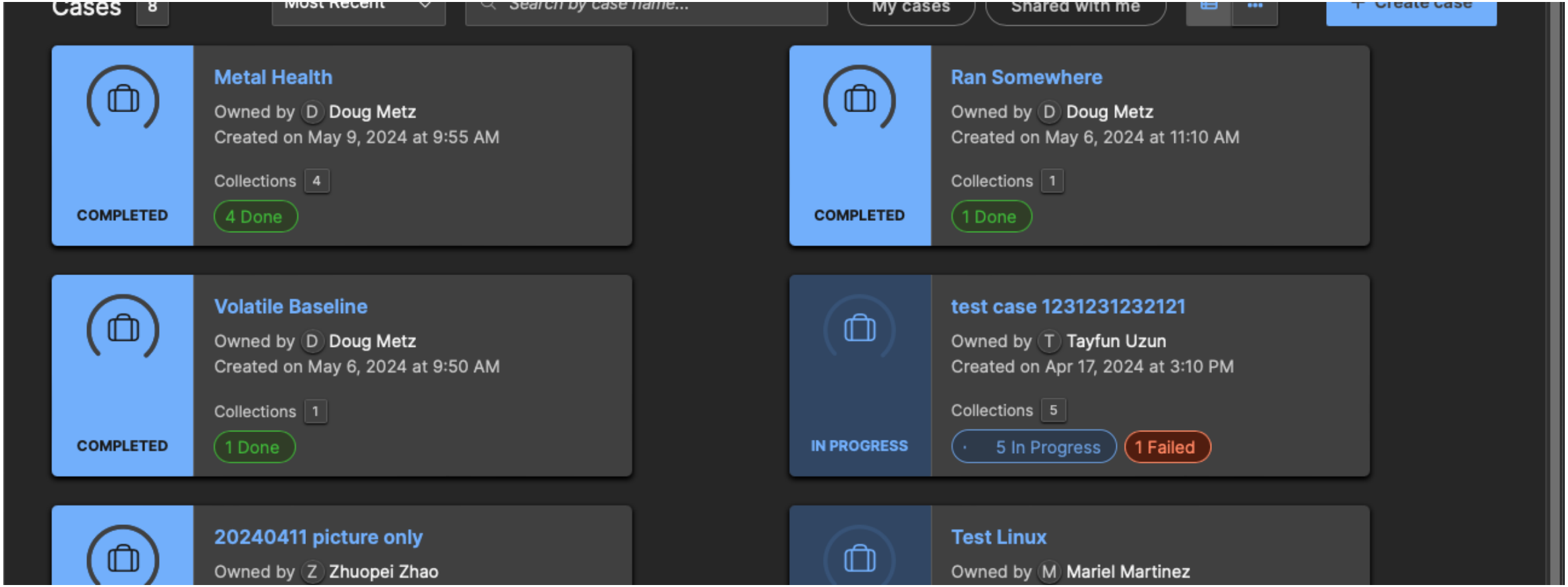

Office 365

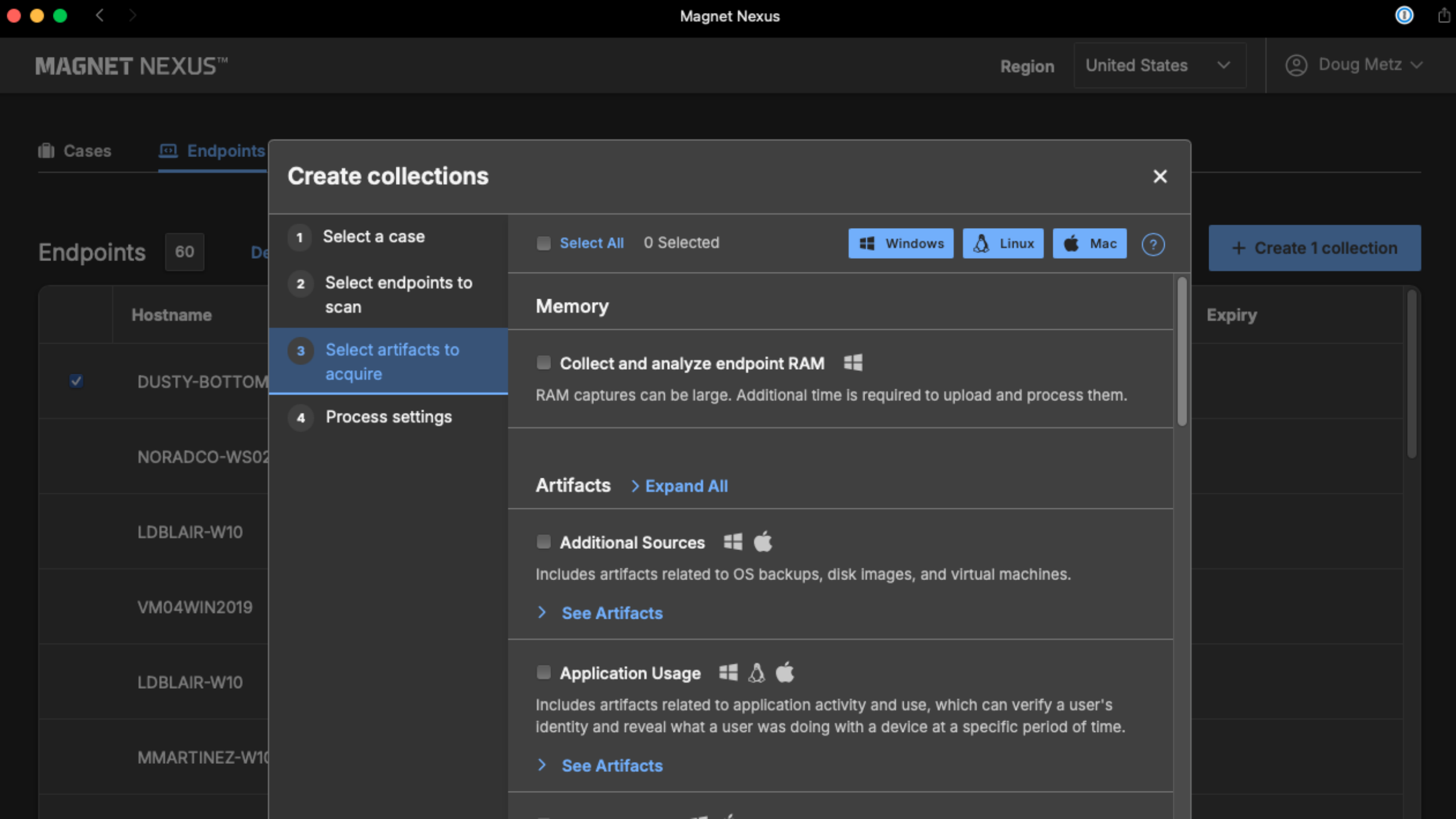
iOS

aws

MAGNET FORENSICS®

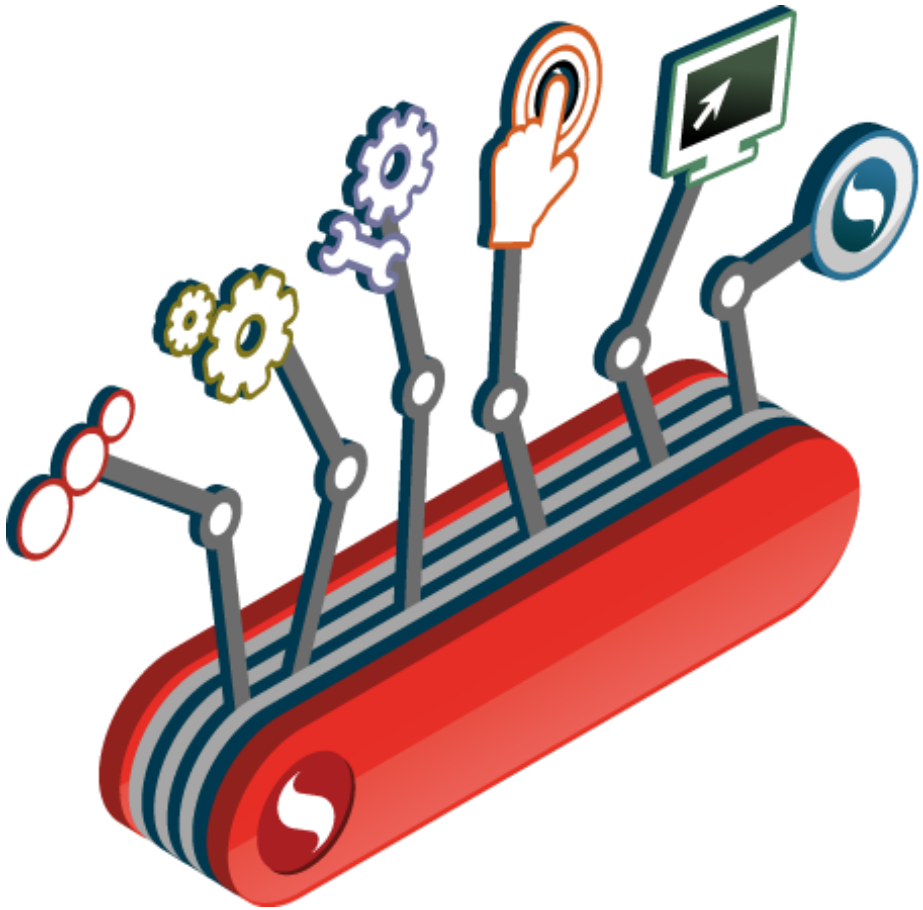
# Remote Collections (and Analysis) with Magnet NEXUS




Magnet Nexus
MAGNET NEXUS™
Region
United States
Doug Metz
Cases
Endpoints
Endpoints
60
+ Create 1 collection
Hostname
Expiry
DUSTY-BOTTOM
NORADCO-WS02
LDBLAIR-W10
VM04WIN2019
LDBLAIR-W10
MMARTINEZ-W10
Create collections
1 Select a case
2 Select endpoints to scan
3 Select artifacts to acquire
4 Process settings
Select All
0 Selected
Windows
Linux
Mac
Memory
Collect and analyze endpoint RAM
RAM captures can be large. Additional time is required to upload and process them.
Artifacts
Expand All
Additional Sources
Includes artifacts related to OS backups, disk images, and virtual machines.
See Artifacts
Application Usage
Includes artifacts related to application activity and use, which can verify a user's identity and reveal what a user was doing with a device at a specific period of time.
See Artifacts

# YARA

"The pattern matching Swiss army knife for malware researchers (and everyone else)."



# Components of YARA Rules

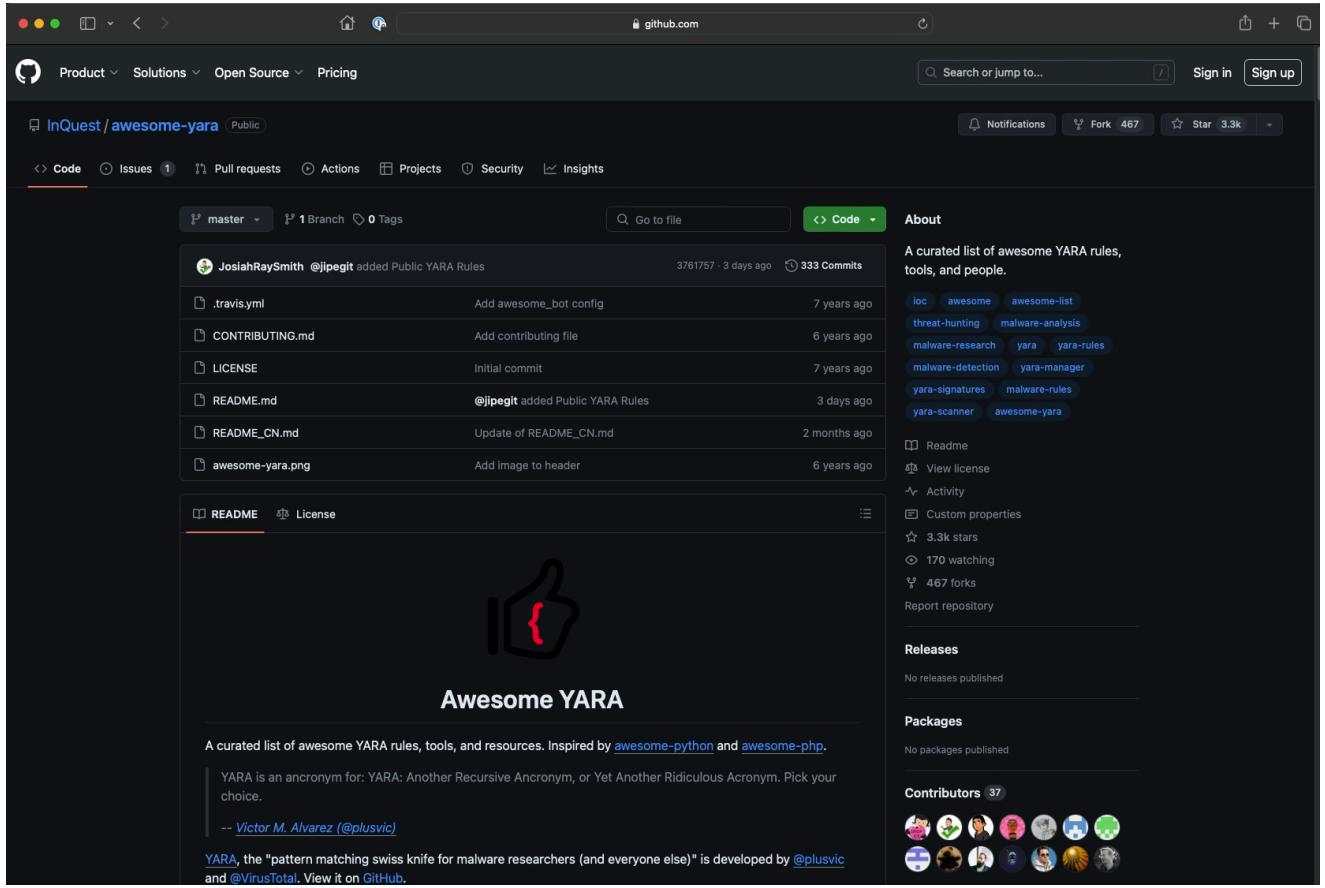
1. * Rule Name: Name of the rule. (Avoid spaces.)
2. Metadata: Details describing the sample and/or conditions the rule was written to detect for, author information, references, etc.
3. Strings: text patterns identified in the sample (ascii, wide, HEX, Base64…)
4. * Condition: The pattern or patterns that must be present in a file or process for the rule to trigger

* Required

# Example YARA Rule

```
rule Detect_Malware {
    meta:
        description = "Detects a specific malware family"
        author = "Your Name"

    strings:
        $string1 = "malware_indicator_1"
        $string2 = "malware_indicator_2"

    condition:
        $string1 and $string2
}
```

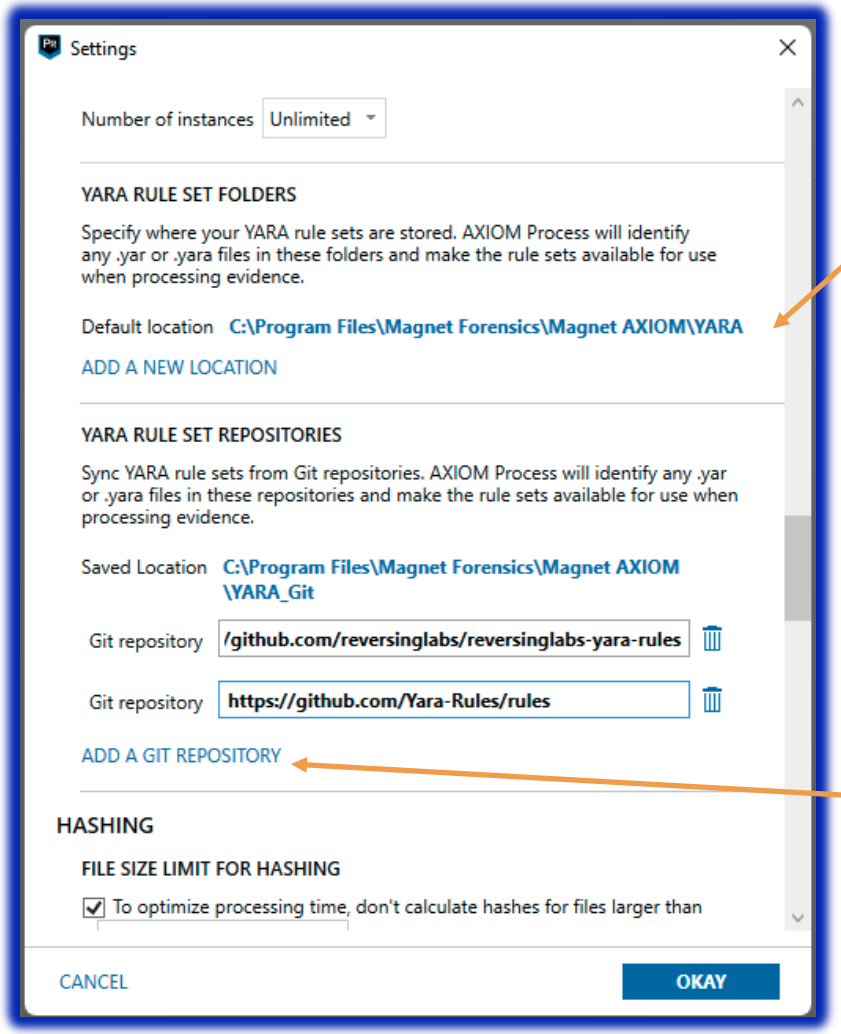
# YARA Sources




# YARA Rules In

# MAGNET AXIOM CYBER™

# YARA Repository Configuration




Manually add or remove rules from this folder

Sync additional GitHub repositories

## SEARCH WITH YARA RULES

CASE DETAILS

EVIDENCE SOURCES 2

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search On
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Search with YARA rules
- Find more artifacts

ARTIFACT DETAILS 214

- Mobile artifacts
- Cloud artifacts
- Computer artifacts 214 of 264
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

### YARA RULE SETS

Use YARA rules to identify matching files. You can import YARA rule sets from a folder containing .yar or .yara files, or you can manually add YARA rule sets.

**NOTE:** Running several YARA rule sets at once might increase scan times.

Reading YARA rule sets from 1 synced folder(s) and 2 Git repo(s). EDIT

*Search by name or source path...*

# New YARA Rules

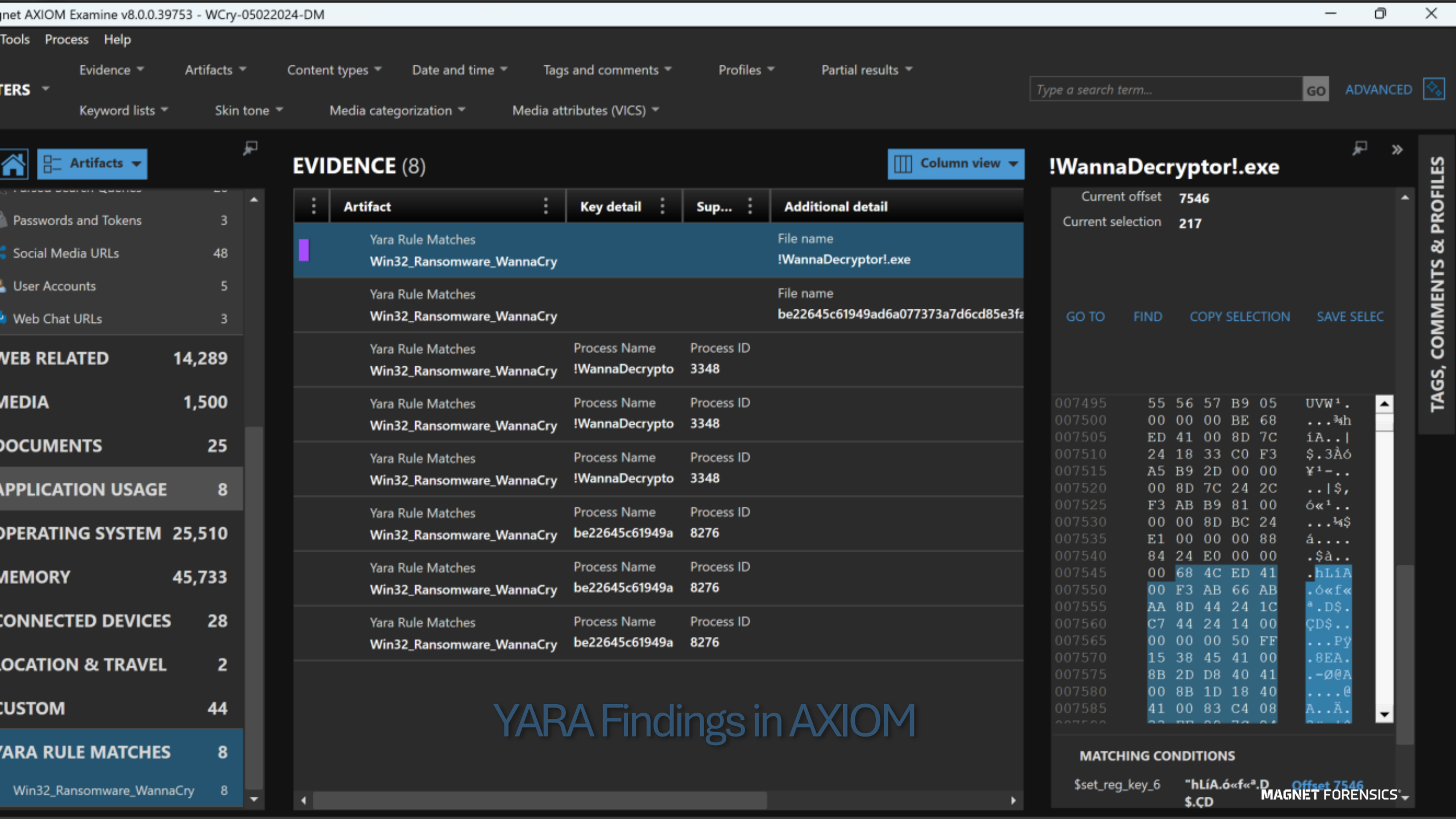
SELECT ALL ADD NEW RULE SET REFRESH SYNC WITH GIT

Rules selected: 0

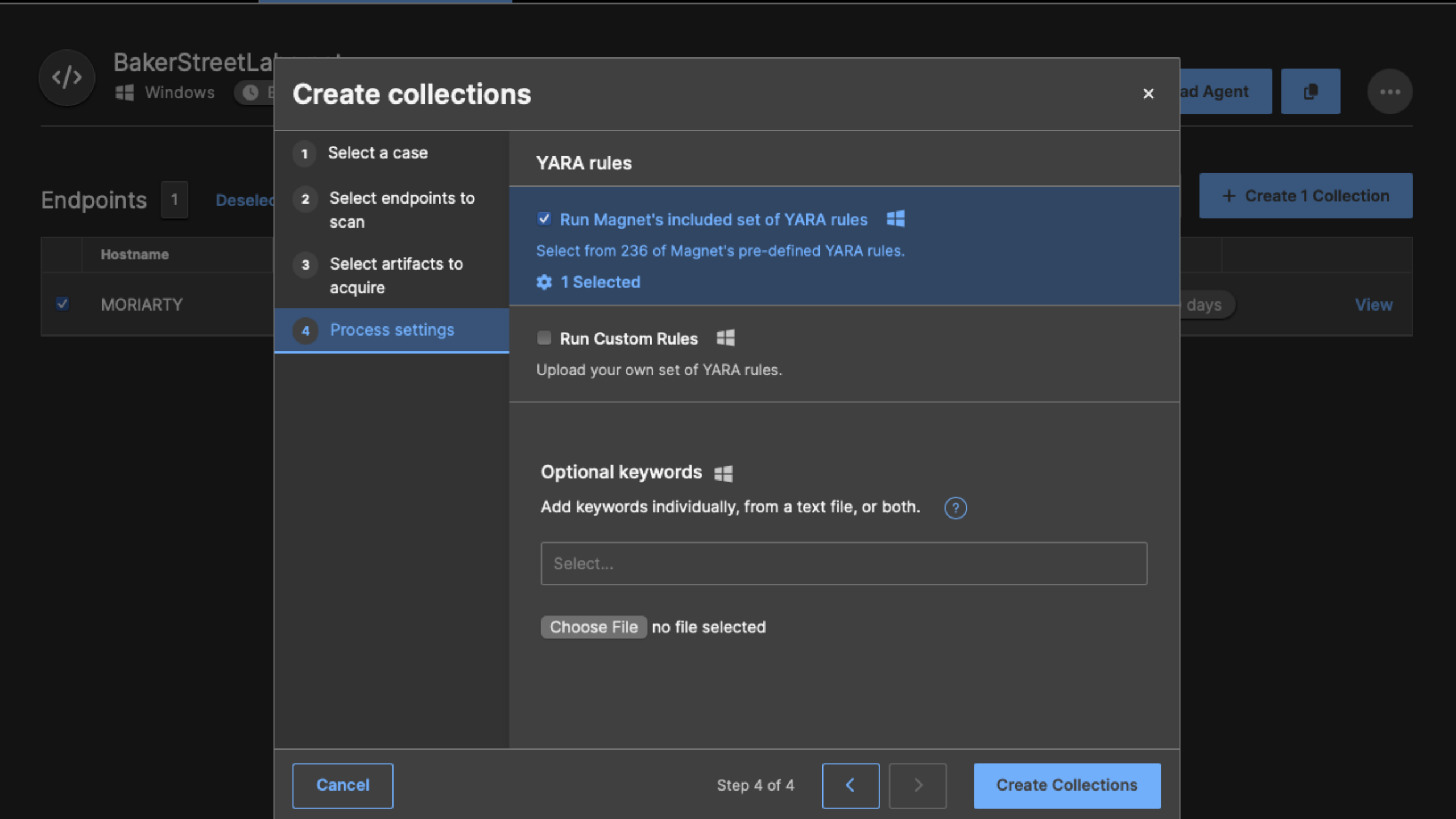
| Enabled | Rule set name | Source path | Source | Date created |
|---|---|---|---|---|
| ☐ | Win32.Ransomware.Ladon.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | JJencode.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers | Git | 12/8/2023 10:49:32 AM |
| ☐ | Win32.Ransomware.LeChiffre.ya... | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | packer.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers | Git | 12/8/2023 10:49:32 AM |
| ☐ | Win32.Ransomware.LockBit.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | Win32.Ransomware.Lolkek.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | Win32.Ransomware.LooCipher.... | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | packer_compiler_signatures.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers | Git | 12/8/2023 10:49:32 AM |
| ☐ | Win32.Ransomware.Lorenz.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | Win32.Ransomware.Mafia.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | peid.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers | Git | 12/8/2023 10:49:32 AM |
| ☐ | Win32.Ransomware.Magniber.y... | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | tweetable-polyglot-png.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers | Git | 12/8/2023 10:49:33 AM |
| ☐ | Win32.Ransomware.Major.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |
| ☐ | Win32.Ransomware.Makop.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | Magnet Forensics | 12/13/2022 3:14:57 PM |

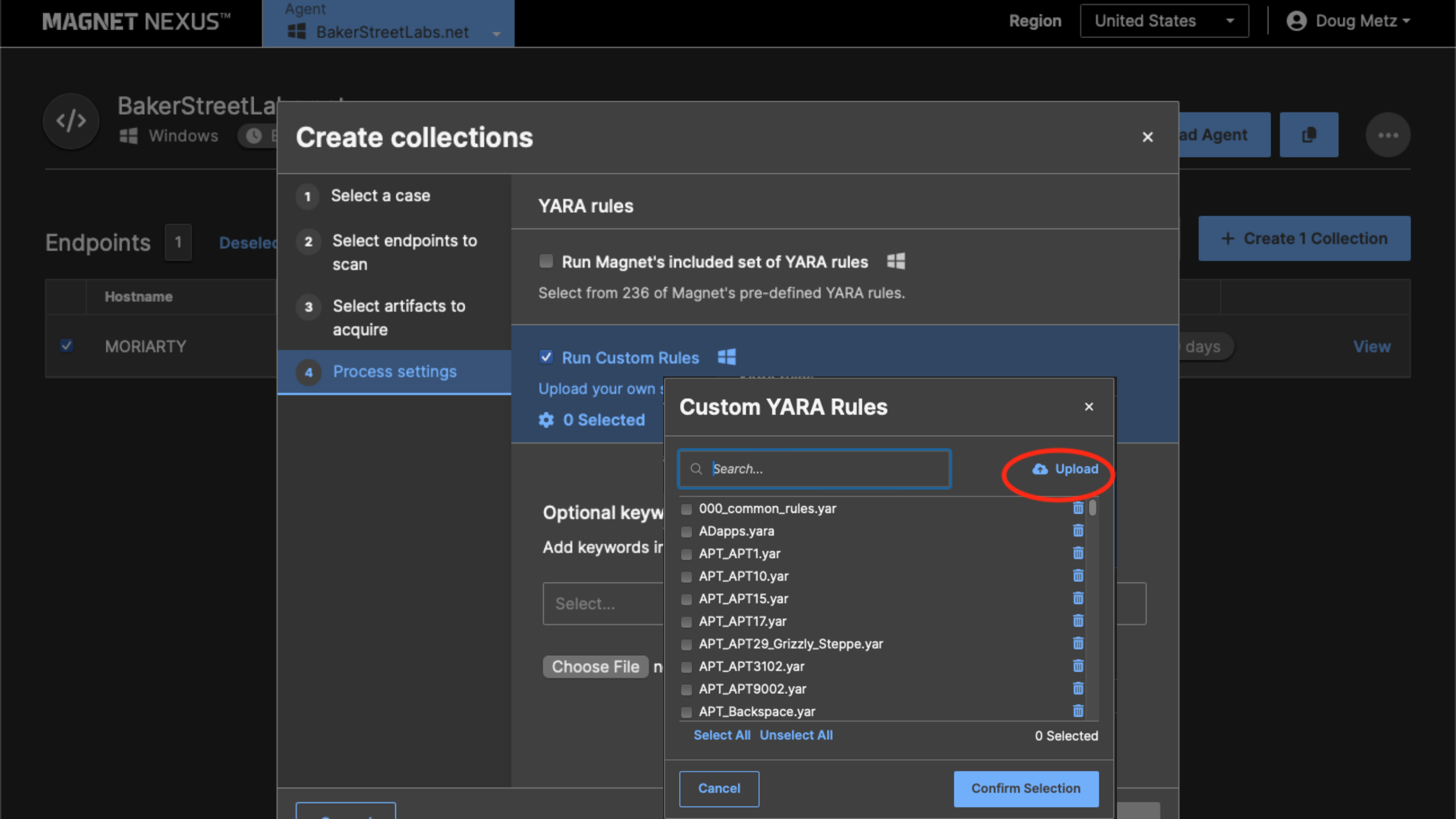
Search with YARA rules ! On

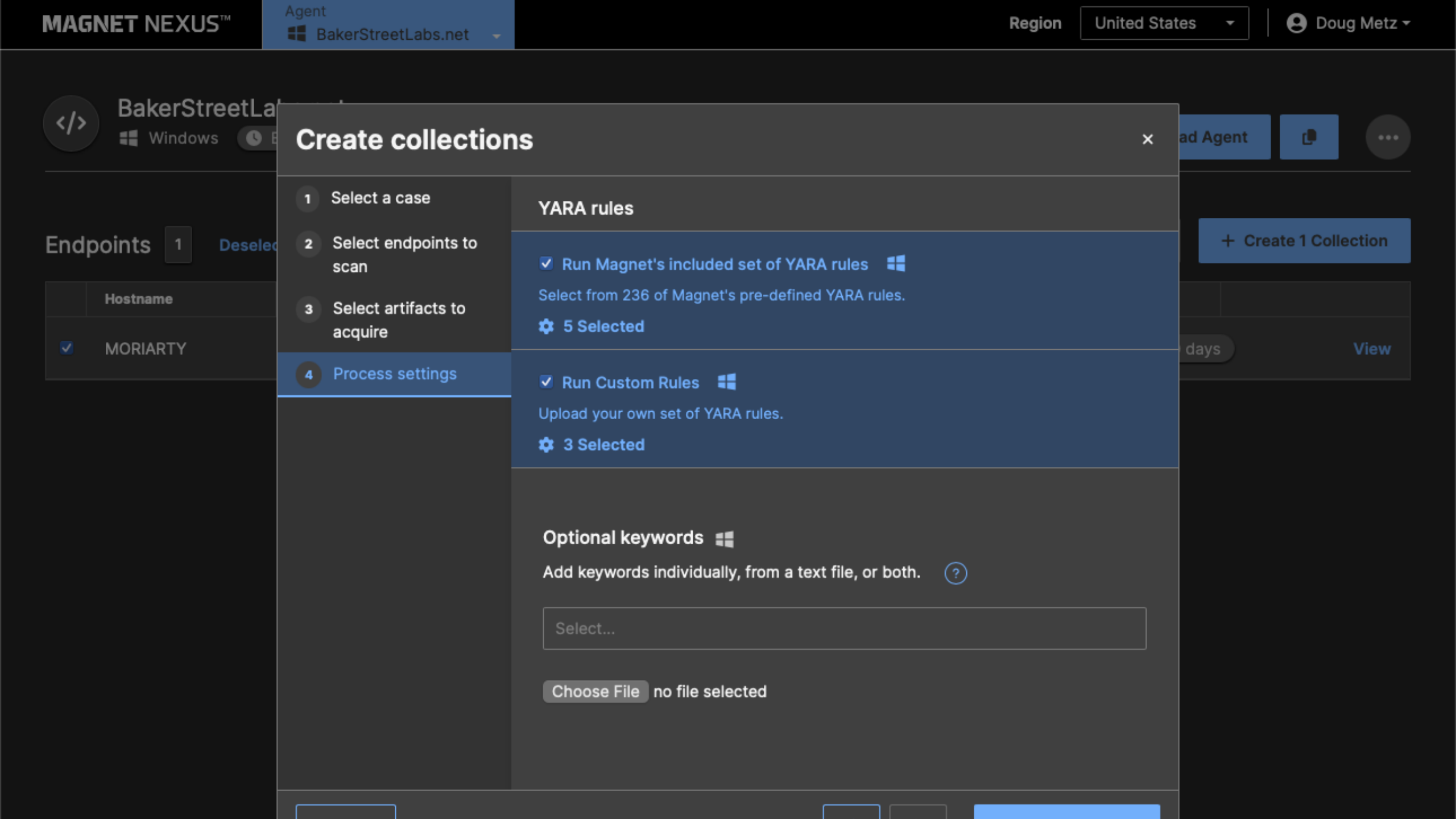
BACK


gnet AXIOM Examine v8.0.0.39753 - WCry-05022024-DM
Tools Process Help
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results
TERS
Keyword lists Skin tone Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
Passwords and Tokens 3
Social Media URLs 48
User Accounts 5
Web Chat URLs 3
WEB RELATED 14,289
MEDIA 1,500
DOCUMENTS 25
APPLICATION USAGE 8
OPERATING SYSTEM 25,510
MEMORY 45,733
CONNECTED DEVICES 28
LOCATION & TRAVEL 2
CUSTOM 44
YARA RULE MATCHES 8
Win32_Ransomware_WannaCry 8
EVIDENCE (8)
Column view
Artifact
Key detail
Sup...
Additional detail
Yara Rule Matches
Win32_Ransomware_WannaCry
File name
!WannaDecryptor!.exe
Yara Rule Matches
Win32_Ransomware_WannaCry
File name
be22645c61949ad6a077373a7d6cd85e3fa
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
!WannaDecrypto
Process ID
3348
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
!WannaDecrypto
Process ID
3348
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
!WannaDecrypto
Process ID
3348
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
be22645c61949a
Process ID
8276
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
be22645c61949a
Process ID
8276
Yara Rule Matches
Win32_Ransomware_WannaCry
Process Name
be22645c61949a
Process ID
8276
YARA Findings in AXIOM
!WannaDecryptor!.exe
Current offset 7546
Current selection 217
GO TO
FIND
COPY SELECTION
SAVE SELEC
007495 55 56 57 B9 05 UVW¹.
007500 00 00 00 BE 68 ...¾h
007505 ED 41 00 8D 7C íA..|
007510 24 18 33 C0 F3 $.3Àó
007515 A5 B9 2D 00 00 ¥¹-..
007520 00 8D 7C 24 2C ..|$,
007525 F3 AB B9 81 00 ó«¹..
007530 00 00 8D BC 24 ...¼$
007535 E1 00 00 00 88 á....
007540 84 24 E0 00 00 .$à..
007545 00 68 4C ED 41 .hLíA
007550 00 F3 AB 66 AB .ó«f«
007555 AA 8D 44 24 1C ª.D$.
007560 C7 44 24 14 00 ÇD$..
007565 00 00 00 50 FF ...Pÿ
007570 15 38 45 41 00 .8EA.
007575 8B 2D D8 40 41 .-Ø@A
007580 00 8B 1D 18 40 ....@
007585 41 00 83 C4 08 A..Ä.
MATCHING CONDITIONS
$set_reg_key_6 "hLíA.ó«f«ª.D $.ÇD Offset 7546
TAGS, COMMENTS & PROFILES
MAGNET FORENSICS

# YARA Rules In


Create collections
1 Select a case
2 Select endpoints to scan
3 Select artifacts to acquire
4 Process settings
YARA rules
Run Magnet's included set of YARA rules
Select from 236 of Magnet's pre-defined YARA rules.
1 Selected
Run Custom Rules
Upload your own set of YARA rules.
Optional keywords
Add keywords individually, from a text file, or both.
Select...
Choose File
no file selected
Cancel
Step 4 of 4
Create Collections
Endpoints
Create 1 Collection
Hostname
MORIARTY
View


MAGNET NEXUS™
Agent
BakerStreetLabs.net
Region
United States
Doug Metz
Windows
Endpoints
1
Hostname
MORIARTY
+ Create 1 Collection
View
Create collections
1 Select a case
2 Select endpoints to scan
3 Select artifacts to acquire
4 Process settings
YARA rules
Run Magnet's included set of YARA rules
Select from 236 of Magnet's pre-defined YARA rules.
Run Custom Rules
0 Selected
Optional keyw
Add keywords ir
Select...
Choose File
Custom YARA Rules
Search...
Upload
000_common_rules.yar
ADapps.yara
APT_APT1.yar
APT_APT10.yar
APT_APT15.yar
APT_APT17.yar
APT_APT29_Grizzly_Steppe.yar
APT_APT3102.yar
APT_APT9002.yar
APT_Backspace.yar
Select All
Unselect All
0 Selected
Cancel
Confirm Selection


MAGNET NEXUS™
Agent
BakerStreetLabs.net
Region
United States
Doug Metz
Windows
ad Agent
Endpoints
1
Deselec
+ Create 1 Collection
Hostname
MORIARTY
days
View
Create collections
1 Select a case
2 Select endpoints to scan
3 Select artifacts to acquire
4 Process settings
YARA rules
Run Magnet's included set of YARA rules
Select from 236 of Magnet's pre-defined YARA rules.
5 Selected
Run Custom Rules
Upload your own set of YARA rules.
3 Selected
Optional keywords
Add keywords individually, from a text file, or both.
Select...
Choose File
no file selected

Scanning...

## Artifacts

- Application Usage 85
- Connected Devices 236
- Indicators of compromise 1
  - Yara Rules 1
- Operating System 546321
- Refined Results 641
- Volatile Artifacts 1420

# Yara Rules

| Tag | File Name | File Size (Bytes) | Matching Conditions |
|---|---|---|---|
| | C:\Users\dwmetz\Downloads\EmployeeSalaries2024.xls.exe | 229376 | $main_1, $main_5, $ent |

YARA RULES

## Hit Details

File Name:
**C:\Users\dwmetz\Downloads\EmployeeSalaries2024.xls.exe**

File Size (Bytes):
**229376**

Matching Conditions:
**$main_1, $main_5, $entrypoint_all**

Matched Rules:
**Win32_Ransomware_WannaCry**

+ Tag


MITRE
ATT&CK™

layer

selection controls | layer controls | technique controls

## Reconnaissance
10 techniques

- tive Scanning (0/3)
- ther Victim Host ormation (0/4)
- ther Victim Identity ormation (0/3)
- ther Victim Network ormation (0/6)
- ther Victim Org ormation (0/4)
- ishing for Information (0/4)
- arch Closed Sources (0/2)
- arch Open Technical tabases (0/5)
- arch Open bsites/Domains (0/3)
- arch Victim-Owned bsites

## Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/8)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/7)
- Stage Capabilities (0/6)

## Initial Access
10 techniques

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

## Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (0/10)
- 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 (0/6)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Host Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/5)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (0/13)
- Implant Internal Image
- Modify Authentication Process (0/9)
- Office Application Startup (0/6)
- Power Settings
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

## Privilege Escalation
14 techniques

- Abuse Elevation Control Mechanism (0/6)
- Access Token Manipulation (0/5)
- Account Manipulation (0/6)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/5)
- Domain or Tenant Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/13)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

## Defense Evasion
43 techniques

- Abuse Elevation Control Mechanism (0/6)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/12)
- Hijack Execution Flow (0/13)
- Impair Defenses (0/11)
- Impersonation
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/9)
- Modify Authentication Process (0/9)
- Modify Cloud Compute Infrastructure (0/5)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/13)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (0/6)
- System Binary Proxy Execution (0/14)
- System Script Proxy Execution (0/2)
- Template Injection

## 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 (0/9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/8)

## Discovery
32 techniques

- Account Discovery (0/4)
- 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 (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

## Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/8)
- 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 (0/3)
- 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
- Video Capture

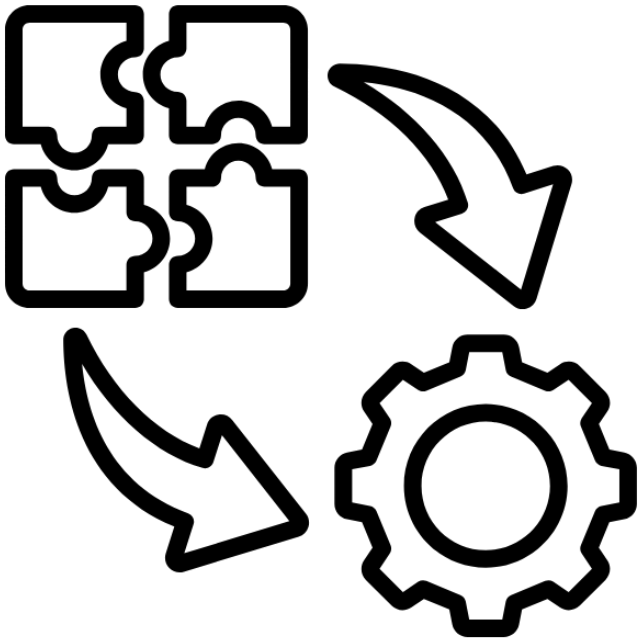
## Command and Control
18 techniques

- 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
- Hide Infrastructure
- 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

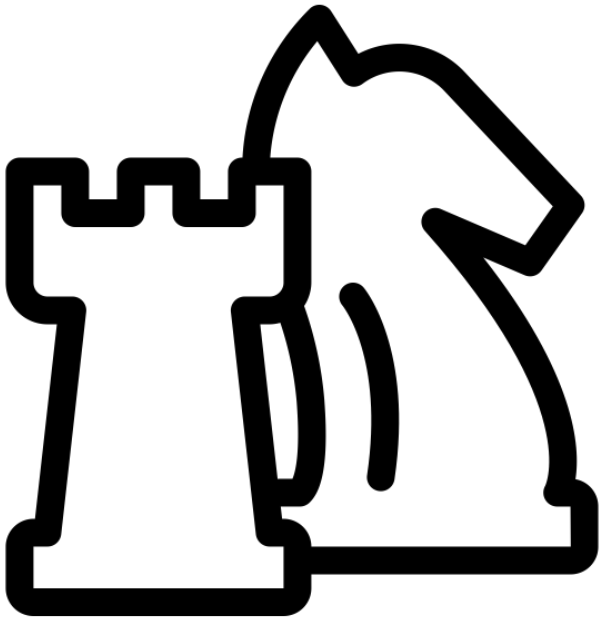
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/4)
- Scheduled Transfer
- Transfer Data to Cloud Account

# Key Components of MITRE ATT&CK



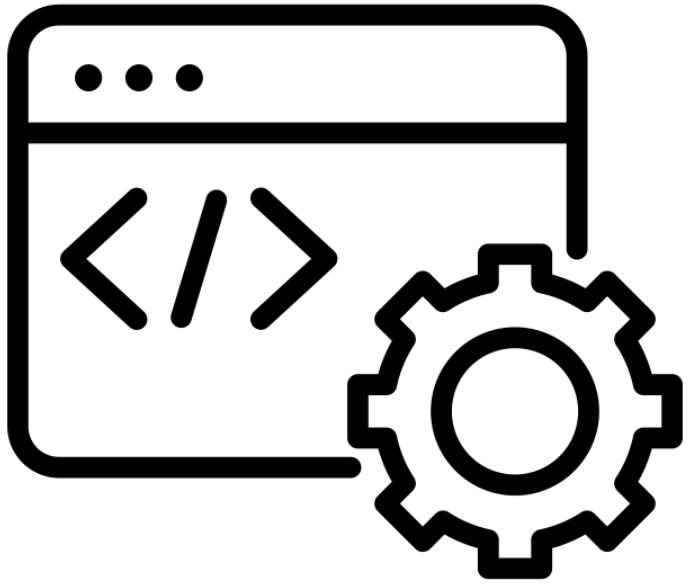
- Tactics
- Techniques
- Sub-techniques
- Procedures
- Mitigations
- Detections

# Tactics



- High level objective or goals
- Each tactic represents a phase in attack lifecycle
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control (C2)
  - Exfiltration
  - Impact

# Techniques

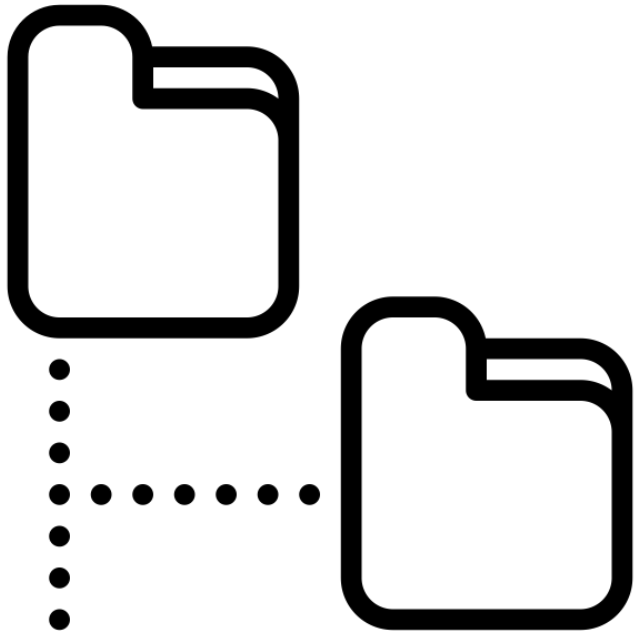


- Specific Methods or Procedures
- Each technique linked to a tactic

*Example:*

- Tactic: TA0002 - Execution
  - Technique: T1059 – Command and Scripting Interpreter

# Sub-techniques

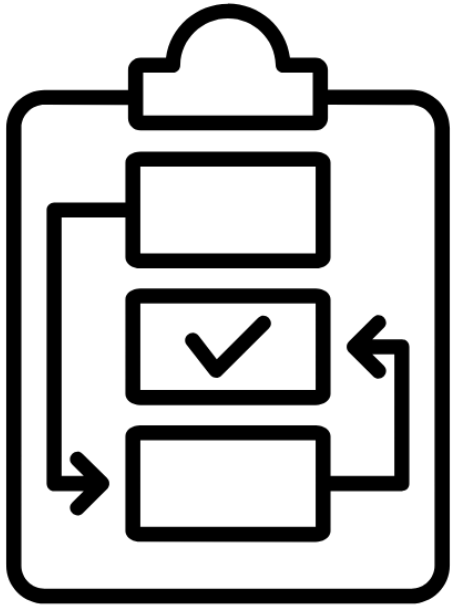


- More granular
- Provides detail on how it can be executed
- Each technique linked to a tactic

*Example:*

- Tactic: TA0002 - Execution
  - Technique: T1059 – Command and Scripting Interpreter
    - Sub-technique: T1059.001 PowerShell

# Procedures



- refer to the actual implementations or instances of techniques observed in real-world attacks

*Example:*

- Tactic: TA0002 - Execution
  - Technique: T1059 – Command and Scripting Interpreter
    - Sub-technique: T1059.001 PowerShell
      - Procedure: G0073 APT19 used PowerShell commands to execute payloads

# Mitigations

- Defensive Measures

*Example:*

- Mitigation: M1038 Execution Prevention

Use application control where appropriate. PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., Add-Type).

# Detections

- How to identify and detect techniques

*Example:*
- Detection: DS0009 Execution Prevention
- Data source: Process
- Data component: Process Creation

Monitor for newly executed processes that may abuse PowerShell commands and scripts …

# Detections

DETECTION: DS0009 Execution Prevention

Monitor for newly executed processes that may abuse PowerShell commands and scripts for execution. PowerShell is a scripting environment included with Windows that is used by both attackers and administrators. Execution of PowerShell scripts in most Windows versions is opaque and not typically secured by antivirus which makes using PowerShell an easy way to circumvent security measures. This analytic detects execution of PowerShell scripts.

Powershell can be used to hide monitored command line execution such as:

net usesc start

Note: - The logic for Analytic 1 is based around detecting on non-interactive Powershell sessions (i.e., those not launched by a user through explorer.exe). This may lead to false positives when used in a production environment, so we recommend tuning any such analytics by including additional logic (e.g., looking for suspicious parent processes) that helps filter such events.- The logic for Analytic 2 is based around detecting on remote Powershell sessions. PowerShell can be used over WinRM to remotely run commands on a host. When a remote PowerShell session starts, svchost.exe executes wsmprovhost.exe.

Analytic 1 - Non-interactive Powershell Sessions

(source="*WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="*WinEventLog:Security" EventCode="4688") Image="powershell.exe" AND ParentImage!="explorer.exe"

Analytic 2 - Remote Powershell Sessions

(source="*WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="*WinEventLog:Security" EventCode="4688") Image="wsmprovhost.exe" AND ParentImage="svchost.exe"

Analytic 3 - Powershell Execution

(source="*WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") Image="C:*Windows\\powershell.exe" ParentImage!="C:\Windows\explorer.exe"|stats values(CommandLine) as "Command Lines" values(ParentImage) as "Parent Images" by ComputerName

# Key Features of Sigma Rules

- Sigma Rules
  - Platform Agnostic
  - Structured Format
  - Flexibility
  - Community Driven

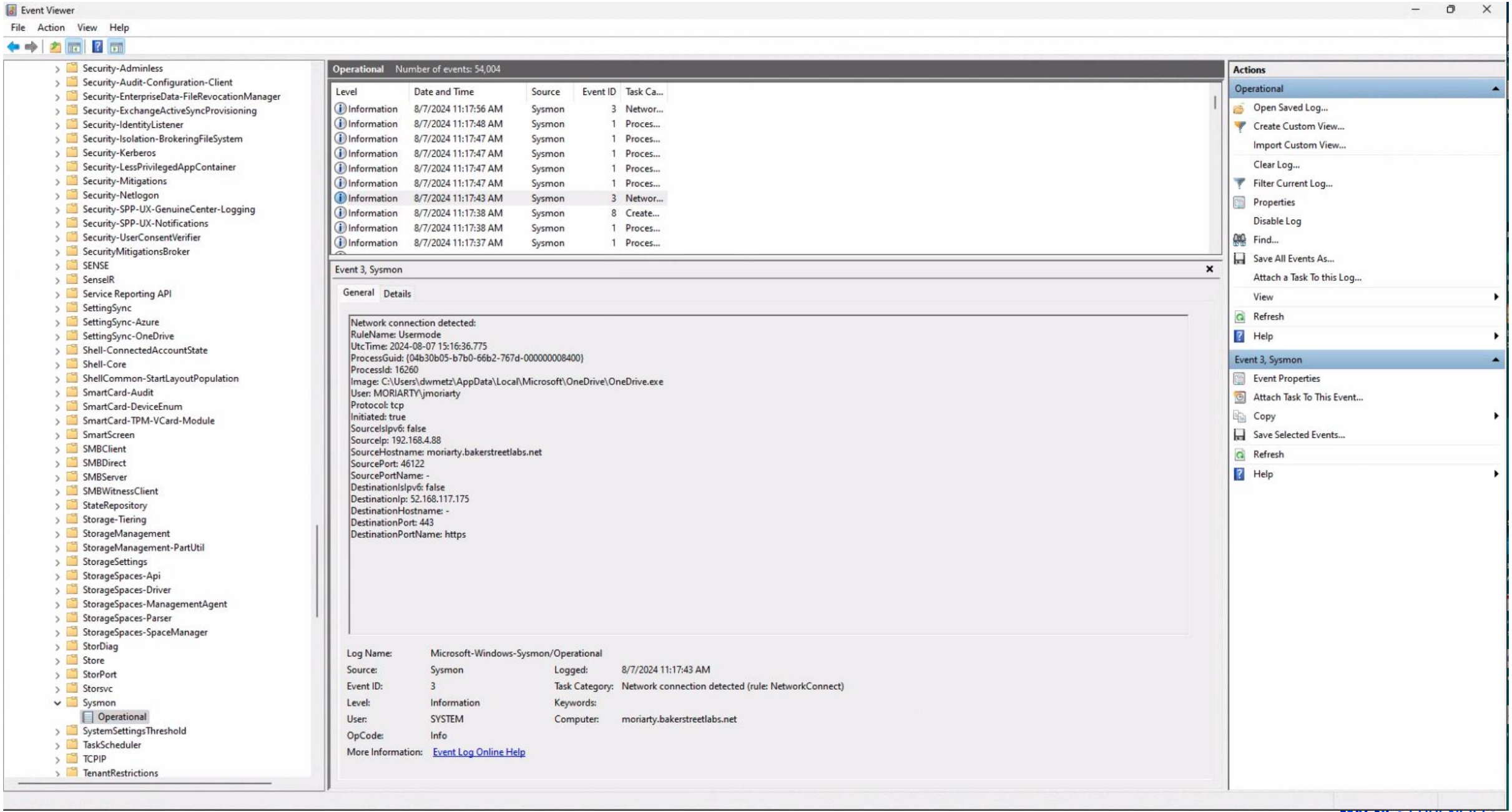
***"Sigma is for logs, what YARA is for files."***

```yaml
title: Vshadow used to delete Volume Shadow Copies
id: 3a57232d-8d26-44f5-8fe6-b2f662513772
status: experimental
description: Detects the usage of the LOLBAS vshadow.exe to delete volume shadow copies.
references:
    - https://lolbas-project.github.io/lolbas/OtherMSBinaries/Vshadow/
    - https://learn.microsoft.com/en-us/windows/win32/vss/vshadow-tool-and-sample
author: Doug Metz '@dwmetz'
date: 2024/06/21
```
Add Tag
```yaml
tags:
    - attack.t1490
logsource:
    category: process_creation
    product: windows
```
Look Up
```yaml
detection:
    fileName:
        winlog.event_data.OriginalFileName: vshadow.exe
    delete_commands:
        CommandLine|contains:
            - vshadow -da
            - vshadow -do
            - vshadow *-dx
            - vshadow *-ds
    condition: fileName and delete_commands
falsepositives:
    - Unknown
level: critical
```

# Sigma Rule Conversion

```
winlog.channel:Microsoft\-Windows\-Sysmon\/Operational AND (winlog.event_id:1 AND
(winlog.event_data.OriginalFileName:vshadow.exe AND (winlog.event_data.CommandLine:
("*vshadow\ \-da*" OR "*vshadow\ \-do*" OR "*vshadow\ *\-dx*" OR "*vshadow\ *\-
ds*"))))
```

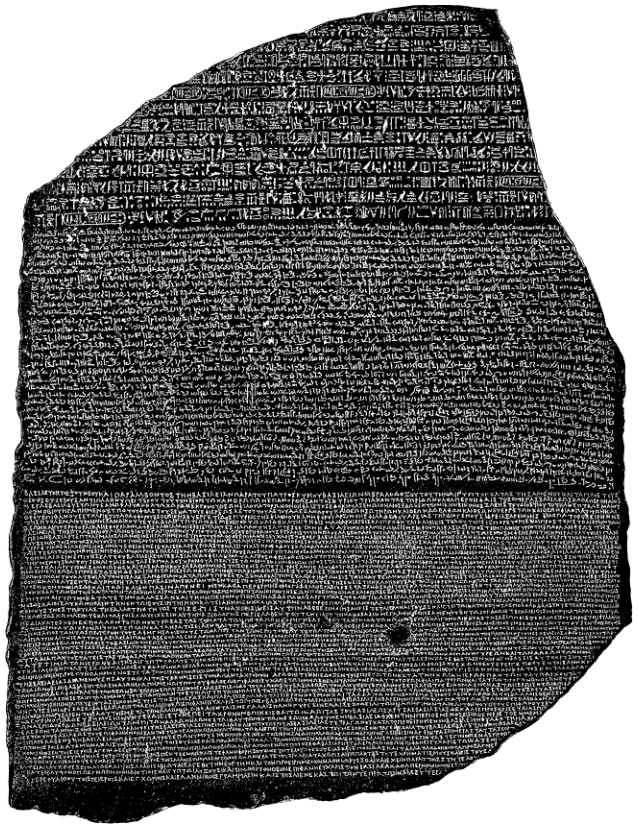
Previously shown Sigma rule converted to Elastic query



# Knowing Your Enemy with TTPs

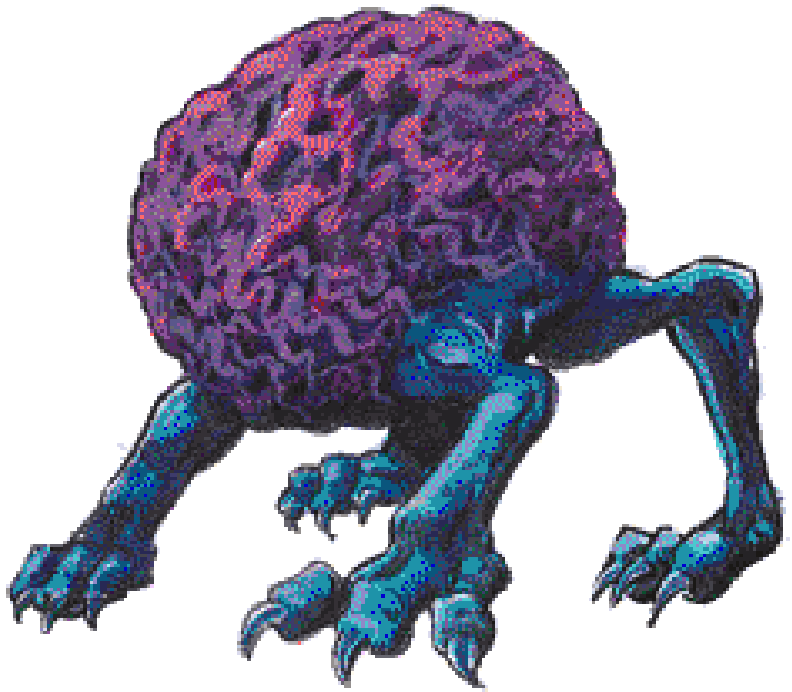
- Predictive Capabilities
- Tailored Defenses

# Advantages of a Common Security Language



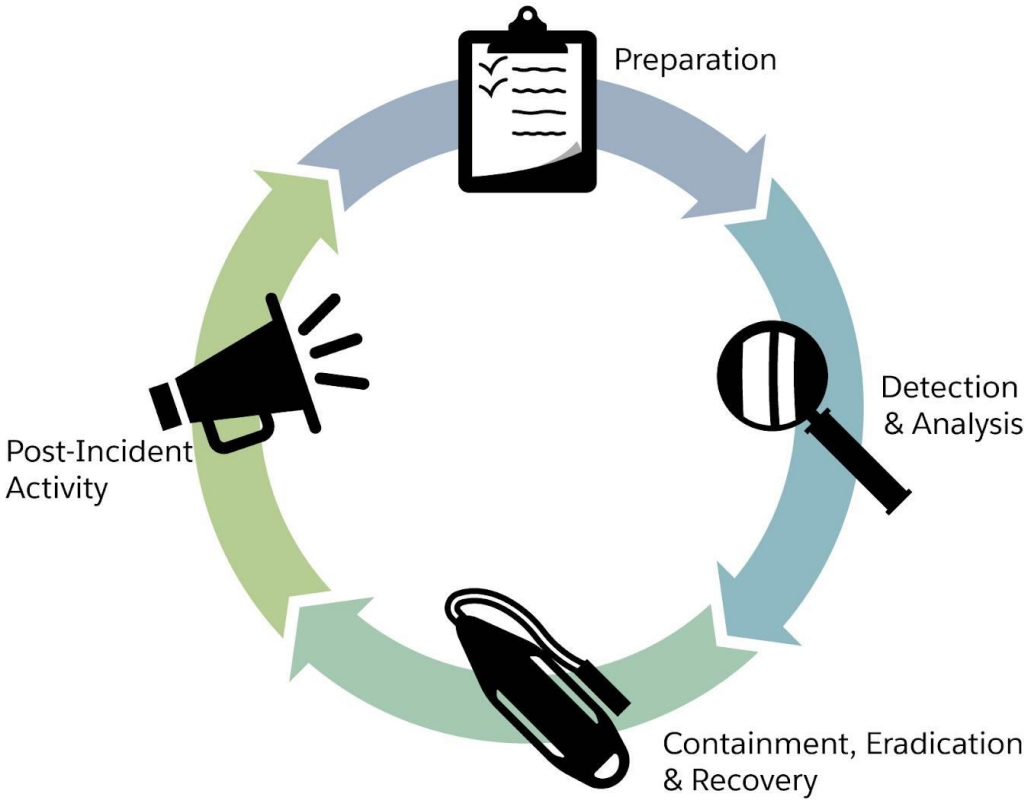
- Improved Collaboration
- Consistent Reporting
- Training and Awareness

# Improving Your Threat Intelligence



- Contextual Awareness
- Proactive Defense
- Enhanced Analysis

# How MITRE ATT&CK Supports Post-Incident Analysis




- Root Cause Analysis
- Lessons Learned
- Improved Incident Response Plans

# MAGNET AXIOM CYBER™

AND

# MITRE ATT&CK™

CASE DETAILS

EVIDENCE SOURCES 1

PROCESSING DETAILS

- Search archives and mobile backups: On
- Decode file-based encryption
- Add keywords to search
- Extract text from files (OCR)
- Calculate hashes and find matches: On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Identify TTPs and malware
- Find more artifacts

ARTIFACT DETAILS 207

- Mobile artifacts
- Cloud artifacts
- Computer artifacts: 207 of 269
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

## IDENTIFY TTPS USING MITRE ATT&CK® FRAMEWORK

Axiom Process can use SIGMA rules to identify TTPs using the MITRE ATT&CK® framework. For a listing of the rules that can be applied, see SIGMA rules GitHub.

**NOTE:** You must download the sigma_core.zip prior to using SIGMA rules. For detailed steps on how to download the sigma_core.zip, see Download sigma_core.zip from SigmaHQ.

sigma_core.zip - release r2024-05-13 - successfully applied. Click EDIT to provide an updated sigma_core.zip. EDIT

☐ Use SIGMA rules to identify TTPs

## YARA RULE SETS

Use YARA rules to identify matching files. You can import YARA rule sets from a folder containing .yar or .yara files, or you can manually add YARA rule sets.

**NOTE:** Running several YARA rule sets at once might increase scan times.

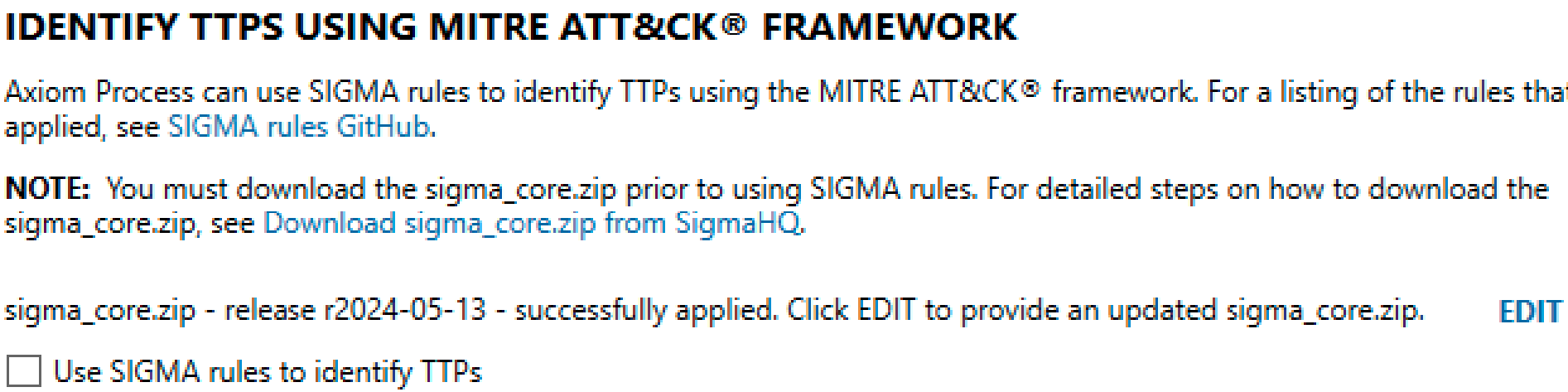
Reading YARA rule sets from 1 synced folder(s). EDIT

*Search by name or source path...*

SELECT ALL ADD NEW RULE SET REFRESH

| Enabled | Rule set name | Source path | Source | Date created |
|---|---|---|---|---|
| ☐ | Email_generic_phishing.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA | User | 7/17/2024 12:21:02 PM |
| ☐ | Linux.Virus.Vit.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Awfull.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Cmay.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.DeadCode.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Elerad.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Greenp.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Mocket.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Virus.Negt.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Trojan.CaddyWiper.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |
| ☐ | Win32.Trojan.Dridex.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | User | 12/29/2022 10:22:21 AM |

# Axiom Cyber and MITRE ATT&CK



File Tools Process Help

FILTERS | Evidence | Artifacts | Content types | Date and time | Tags and comments | Profiles | Partial results | Keyword lists | Skin tone | Media categorization | Media attributes (VICS) | CLEAR FILTERS | Type a search term...

Artifacts

| | |
|---|---|
| WEB RELATED | 10 |
| MEDIA | 9 |
| DOCUMENTS | 3 |
| OPERATING SYSTEM | 37,579 |
| CONNECTED DEVICES | 12 |
| MITRE ATT&CK | 2,498 |
| TA0001 Initial Access | 66 |
| TA0002 Execution | 328 |
| TA0003 Persistence | 115 |
| TA0004 Privilege Escalation | 738 |
| TA0005 Defense Evasion | 857 |
| TA0006 Credential Access | 325 |
| TA0007 Discovery | 8 |
| TA0008 Lateral Movement | 25 |
| TA0011 Command and Control | 28 |
| TA0040 Impact | 8 |
| KEYWORD SNIPPETS | 9,839 |

## MATCHING RESULTS (328 of 328)

Column view

## TA0002 Execution

| Tactic | Technique | SIGMA rule title |
|---|---|---|
| TA0002 Execution | T1021.003 Remote Services: Distributed Component... | MMC20 Lateral Move |
| TA0002 Execution | T1047 Windows Management Instrumentation | Suspicious Process Cr |
| TA0002 Execution | T1047 Windows Management Instrumentation | Suspicious Process Cr |
| TA0002 Execution | T1047 Windows Management Instrumentation | Suspicious Microsoft |
| TA0002 Execution | T1047 Windows Management Instrumentation | Suspicious Microsoft |
| TA0002 Execution | T1047 Windows Management Instrumentation | Suspicious Microsoft |
| TA0002 Execution | T1053.005 Scheduled Task/Job: Scheduled Task | Suspicious Schtasks S |
| TA0002 Execution | T1053.005 Scheduled Task/Job: Scheduled Task | Suspicious Schtasks S |
| TA0002 Execution | T1055.012 Process Injection: Process Hollowing | HackTool - CACTUST( |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Windows Defender Tl |
| TA0002 Execution | T1059 Command and Scripting Interpreter | PowerShell Downloac |

## DETAILS

### ARTIFACT INFORMATION

| | |
|---|---|
| Tactic | **TA0002 Execution** |
| Technique | **T1053.005 Scheduled Task/Job: Scheduled Task** |
| SIGMA rule title | **Suspicious Schtasks Schedule Types** |
| SIGMA rule description | **Detects scheduled task creations or modification on a suspicious schedule type** |
| SIGMA rule creation date | **09/09/2022 00:00:00** |
| SIGMA rule author | **Nasreddine Bencherchali (Nextron Systems)** |
| SIGMA rule path | **C:\Users\dmetz\OneDrive - Magnet Forensics Inc\Desktop\AXIOM - MITRE\MITREATTACK\rules\windows\process_creation\proc_creation_win_schtasks_schedule_type.yml** |
| Artifact type | TA0002 Execution |
| Item ID | 19855 |
| Original artifact | Windows Event Logs |

Magnet AXIOM Examine v8.3.2.41393 - MITRE-EVTX-SAMPLES

File Tools Process Help

FILTERS | Evidence | Artifacts | Content types | Date and time | Tags and comments | Profiles | Partial results | Keyword lists | Skin tone | Media categorization | Media attributes (VICS) | CLEAR FILTERS | Type a search term... | GO | ADVANCED

Artifacts

MATCHING RESULTS 50,057
REFINED RESULTS 107
Identifiers - Device 24
Identifiers - People 83
WEB RELATED 10
MEDIA 9
DOCUMENTS 3
OPERATING SYSTEM 37,579
CONNECTED DEVICES 12
MITRE ATT&CK® 2,498
TA0001 Initial Access 66
TA0002 Execution 328
TA0003 Persistence 115
TA0004 Privilege Escalation 738
TA0005 Defense Evasion 857
TA0006 Credential Access 325
TA0007 Discovery 8
TA0008 Lateral Movement 25
TA0011 Command and Control 28
TA0040 Impact 8
KEYWORD SNIPPETS 9,839

## MATCHING RESULTS (328 of 328)

Column view

| Tactic | Technique | SIGMA rule title | SIGMA rule description |
|---|---|---|---|
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Parent in Public Folder Suspicious Process | This rule detects suspicious processes with parent i.. |
| TA0002 Execution | T1564 Hide Artifacts | Parent in Public Folder Suspicious Process | This rule detects suspicious processes with parent i.. |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From Suspicious Paths | Detects usage of the "wusa.exe" (Windows Update S |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Com | |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Com | |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Parent in Public Folder Suspicious Pro | |
| TA0002 Execution | T1564 Hide Artifacts | Parent in Public Folder Suspicious Pro | |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From S | |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Com | |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Com | |
| TA0002 Execution | | Wusa.EXE Extracting Cab Files From S | |
| TA0002 Execution | T1059 Command and Scripting Interpreter | Parent in Public Folder Suspicious Pro | |
| TA0002 Execution | T1564 Hide Artifacts | Parent in Public Folder Suspicious Pro | |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | | PsExec Service Child Process Execution as LOCAL SY... | Detects suspicious launch of the PSEXESVC service c |
| TA0002 Execution | T1053.005 Scheduled Task/Job: Scheduled Task | Suspicious Schtasks Schedule Types | Detects scheduled task creations or modification on |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |
| TA0002 Execution | T1059.003 Command and Scripting Interpreter: Win... | Operator Bloopers Cobalt Strike Commands | Detects use of Cobalt Strike commands accidentally. |

## TA0002 Execution

EVTX-Samples

### DETAILS

ARTIFACT INFORMATION

| | |
|---|---|
| Tactic | TA0002 Execution |
| Technique | T1053.005 Scheduled Task/Job: Scheduled Task |
| SIGMA rule title | Suspicious Schtasks Schedule Types |
| SIGMA rule description | Detects scheduled task creations or modification on a suspicious schedule type |
| SIGMA rule creation date | 09/09/2022 00:00:00 |
| SIGMA rule author | Nasreddine Bencherchali (Nextron Systems) |
| SIGMA rule path | C:\Users\dmetz\OneDrive - Magnet Forensics Inc \Desktop\AXIOM - MITRE\MITREATTACK\rules \windows\process_creation \proc_creation_win_schtasks_schedule_type.yml |
| Artifact type | TA0002 Execution |
| Item ID | 19855 |

Item ID 19855

Original artifact Windows Event Logs

EVIDENCE INFORMATION

### MITRE ATT&CK®

```
title: Suspicious Schtasks Schedule Types
id: 24c8392b-aa3c-46b7-a545-43f71657fe98
related:
    - id: 7a02e22e-b885-4404-b38b-1ddc7e65258a
      type: similar
status: test
description: Detects scheduled task creations or
modification on a suspicious schedule type
```

TAGS, COMMENTS & PROFILES

Time zone UTC+0:00

9:55 AM 8/9/2024

MAGNET Exhibit Builder v1.3.0.818 - D:\Cases\Exhibit_Builder\MITRE ATT&CK Findings.mfeb

File Tools Help

## CONTENTS

### MAIN BODY

*As you add headings to your report, they will appear here. For easier navigation, start your document with a TITLE style, followed by H1, H2, H3, and so on.*

### APPENDICES

*Any external documents you insert will be added here.*

## REPORT

Table Tools

Home Insert Page Layout References Review Design Layout

Paste Cut Copy Format Painter — Clipboard

Segoe UI 12 — Font

Paragraph

Find/Replace Enable Spell Check Find Next Error — Editing & Proofing

Quick Styles Change Styles — Styles

### TA0001 Initial Access

#### ARTIFACT INFORMATION

| | |
|---|---|
| Tactic | TA0001 Initial Access |
| Technique | T1566.001 Phishing: Spearphishing Attachment |
| SIGMA rule title | HTML Help HH.EXE Suspicious Child Process |
| SIGMA rule description | Detects a suspicious child process of a Microsoft HTML Help (HH.exe) |
| SIGMA rule path | C:\Users\dmetz\OneDrive - Magnet Forensics Inc\Desktop\AXIOM - MITRE\MITREATTACK\rules\windows\process_creation\proc_creation_win_hh_html_help_susp_child_process.yml |
| Artifact | Windows Event Logs |
| Artifact ID | 13308 |

#### EVIDENCE INFORMATION

| | |
|---|---|
| Source | EVTX-Samples.zip\D\EVTX-ATTACK-SAMPLES\Execution\Sysmon_Exec_CompiledHTML.evtx |
| Recovery method | Unknown |
| Deleted source | |
| Location | File Offset 10712 |

100%

## DATA SOURCES

Type a search term...

ARTIFACTS (338) EXTERNAL FILES EVIDEN

Filter by Sort by Artif

TA0001 INITIAL ACCESS
Tactic
TA0001 Initial Access
Technique
T1566.001 Phishing: Spearphishing
SIGMA rule title
HTML Help HH.EXE Suspicious Child

TA0003 PERSISTENCE
Tactic
TA0003 Persistence
Technique
T1547.010 Boot or Logon Autostart
SIGMA rule title
Default RDP Port Changed to Non S

TA0006 CREDENTIAL ACCESS
Tactic
TA0006 Credential Access
Technique
T1133 External Remote Services
SIGMA rule title
External Remote SMB Logon from P

TA0006 CREDENTIAL ACCESS
Tactic
TA0006 Credential Access
Technique
T1078 Valid Accounts
SIGMA rule title
External Remote SMB Logon from P

TA0006 CREDENTIAL ACCESS
Tactic
TA0006 Credential Access
Technique
T1110 Brute Force
SIGMA rule title
External Remote SMB Logon from P

TA0006 CREDENTIAL ACCESS

MAGNET FORENSICS®

# Speed is Power

# TRIAGE & BEYOND: HOW MAGNET FORENSICS POWERS INCIDENT RESPONSE

Resources:

## Free Tools

Magnet Response:

https://www.magnetforensics.com/resources/magnet-response/

Microsoft Sysmon:

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Sigma CLI: https://github.com/SigmaHQ/sigma-cli

Strings (Mac, Linux): *included in operating system*

Strings (Windows):

https://learn.microsoft.com/en-us/sysinternals/downloads/strings

VS Code Sigma Extension:
https://marketplace.visualstudio.com/items?itemName=humpalum.sigma

## PowerShell & Python

CyberPipe: https://github.com/dwmetz/CyberPipe

Defender Response PowerShell:
https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

Ginsu: https://github.com/dwmetz/ginsu

Magnet Response PowerShell:
https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

Strings2Yara: https://github.com/dwmetz/Toolbox/blob/main/Strings2Yara.py

## Repositories

Awesome YARA: https://github.com/InQuest/awesome-yara

Sigma Rules: https://github.com/SigmaHQ/sigma/releases

YARA-Forge: https://yarahq.github.io

## Products

Magnet Axiom Cyber:

https://www.magnetforensics.com/products/magnet-axiom-cyber/

Magnet Exhibit Builder:

https://www.magnetforensics.com/blog/elevate-your-digital-forensics-reports-with-magnet-exhibit-builder/

Magnet Nexus: https://magnetnexus.com

## References

Baker Street Forensics https://bakerstreetforensics.com

Cyber Unpacked: https://www.magnetforensics.com/cyber-unpacked/

HTCIA - High Tech Crime Investigators Association https://www.htcia.org

Magnet Response CLI Guide: https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell/blob/main/Magnet_RESPONSE_CLI_Guide.pdf

MITRE ATT&CK: https://attack.mitre.org

Sigma Detection Format: https://sigmahq.io

YARA: https://virustotal.github.io/yara

# Thank You

MAGNET FORENSICS®