

Practical Detections w/ Sigma

Presented By:
Tyler Casey

Whoami



Lead Detection Engineer & Deputy of SCYTHE
Labs

- Blue Teamer
- DCO Analyst
- Threat Hunter
- Incident Responder



@1qazCasey



/tyler-j-casey

Table of *contents*

01

Sigma

What is it?

Why do I care?

02

Rules 101

Reading
Creating
Standardizing

03

Rule Translation

Sigma → tool of choice,
easy as 1,2,3..

04

Labs

Prac App
Botsv1 Dataset

01 Sigma

"The shareable detection format
for security professionals."
- SigmaHQ



<https://sigmahq.io/>

Detection Sharing

What It Was (is)



SIEM (Tool) Specific

Manually translate
Non-standard format



Silo

Limited sharing means:
Never leaves organization
Never leaves Notepad

Detection Sharing

What It ~~Could~~ Should Be



Centralized Repo
SigmaHQ Github
Internal Repository



Standard Format

Shareable
Repeatable



Tool Agnostic

Splunk
Elastic Stack
CrowdStrike EDR
Microsoft Sentinel

Sigma HQ

The screenshot shows a GitHub repository page for the 'sigma' repository, which is public. The search bar at the top contains the query '7zip'. A dropdown menu is open over the search results, highlighting a file named 'rules/windows/process_creation/proc_creation_win_7zip_exfil_dmp_files.yml'. The repository has 26 branches and 40 tags. The commit history shows 16,050 commits. The commits listed are:

- rules/windows/process_creation/proc_creation_win_7zip_exfil_dmp_files.yml - Go to file (9 hours ago)
- rules/windows/process_creation/proc_creation_win_7zip_password_extraction.yml
- rules/windows/process_creation/proc_creation_win_7zip_password_compression.yml
- rules-emerging-threats/2021/Malware/Conti/proc_creation_win_malware_conti_7zip.yml
- rules-emerging-threats/2022/Exploits/CVE-2022-29072/proc_creation_win_exploit_cve_2022_29072_7zip.yml
- rules-emerging-threats/2017/TA/Lazarus/proc_creation_win_apt_lazarus_binary_masquerading.yml
- rules-compliance chore: move more rules (10 months ago)
- rules-dfir chore: move more rules (10 months ago)
- rules-emerging-threats Merge PR #4714 from @douglasrose75 - Add Rule Coverin... (last week)
- rules-placeholder Merge PR #4681 from @nasbench - Add Missing Ref & Tags (2 weeks ago)
- rules-threat-hunting Merge PR #4698 from @swachchhanda000 - Added rules th... (3 days ago)
- rules Merge PR #4721 from @MalGamy - Add UA used by RedCu... (9 hours ago)

<https://github.com/SigmaHQ/sigma>
<https://detection.fyi>

02



Rules 101

Create it, Standardize it, Read it

PowerShell - IWR

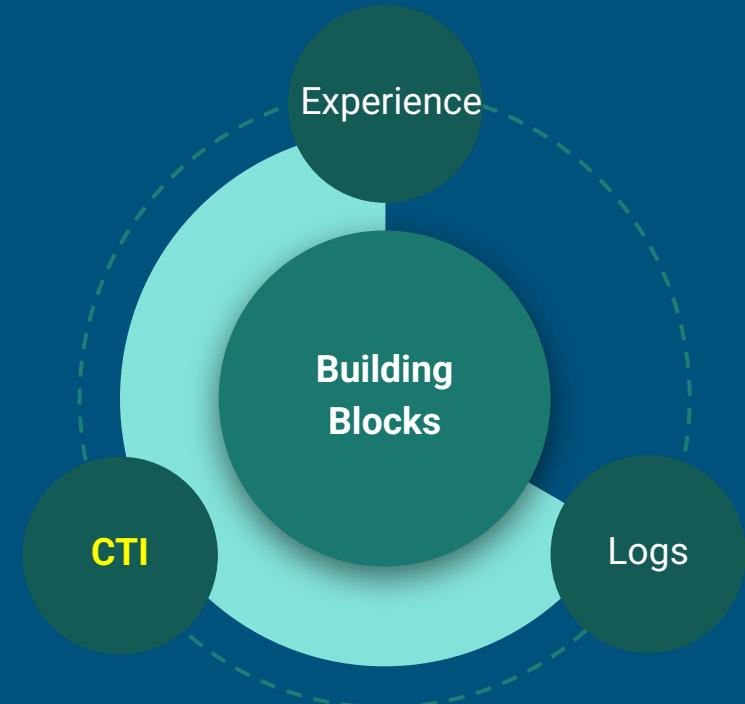
```
title: Potential DLL File Download Via PowerShell Invoke-WebRequest
id: 0f0450f3-8b47-441e-a31b-15a91dc243e2
status: test
description: Detects potential DLL files being downloaded using the PowerShell Invoke-WebRequest cmdlet
references:
  - https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
author: Florian Roth (Nextron Systems), Hieu Tran
date: 2023/03/13
tags:
  - attack.command_and_control
  - attack.execution
  - attack.t1059.001
  - attack.t1105
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    CommandLine|contains:
      - 'Invoke-WebRequest'
      - 'IWR'
    CommandLine|contains|all:
      - 'http'
      - 'OutFile'
      - '.dll'
  condition: selection
falsepositives:
  - Unknown
level: medium
```

Indicator Sources

Enable Automatic Logon

Registry Key	Value	Data
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultUserName	<username>
	DefaultDomainName	<domain name>
	DefaultPassword	<password>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a>



Where Can I Find “Quality”CTI?

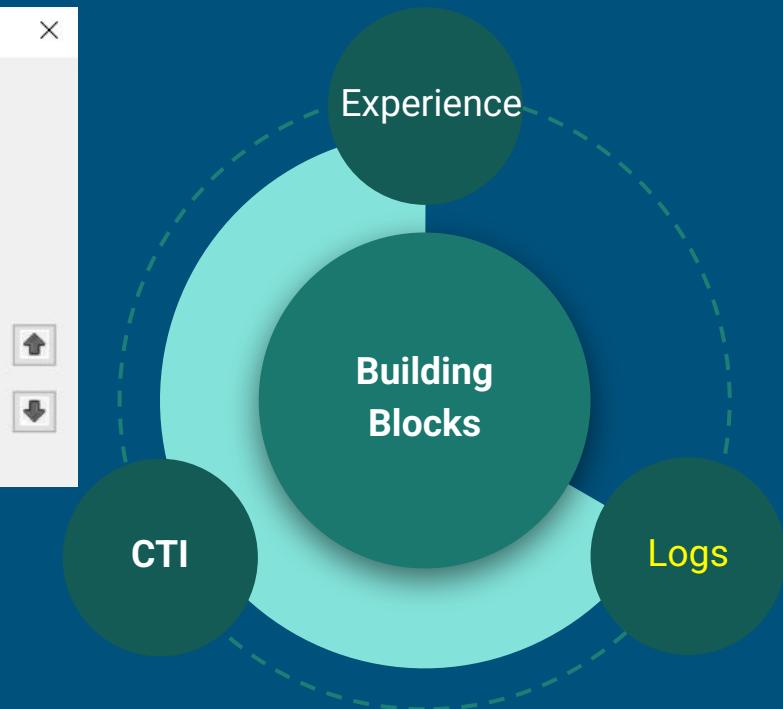
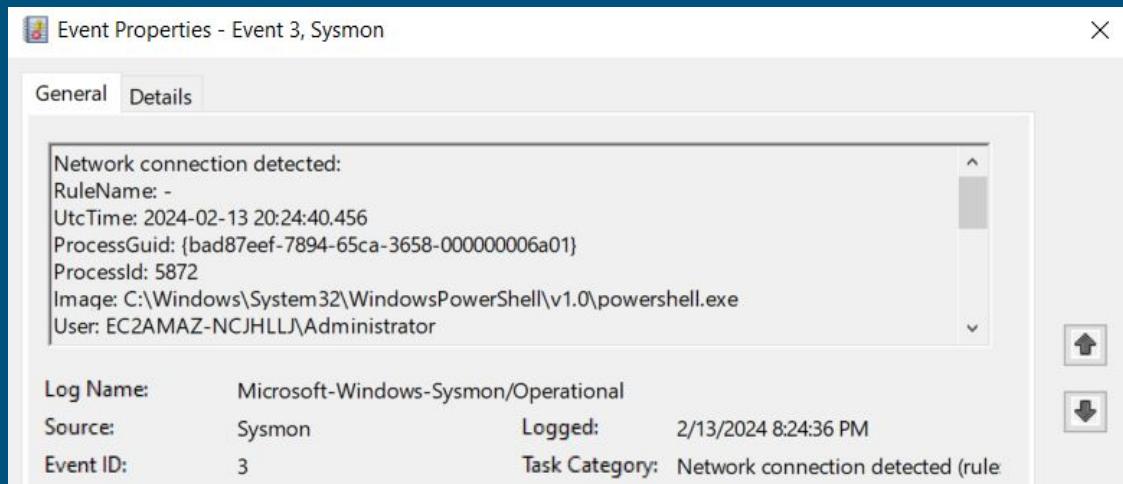
- [CISA Alerts & Advisories](#)
- [DFIR Report](#)
- [Google T.A.G](#)
- [Infosecn1nja Start.me](#)
- [MITRE ATT&CK](#)
- [Unit 42](#)

The screenshot displays a grid of threat intelligence feeds from the start.me platform. The feeds are categorized as follows:

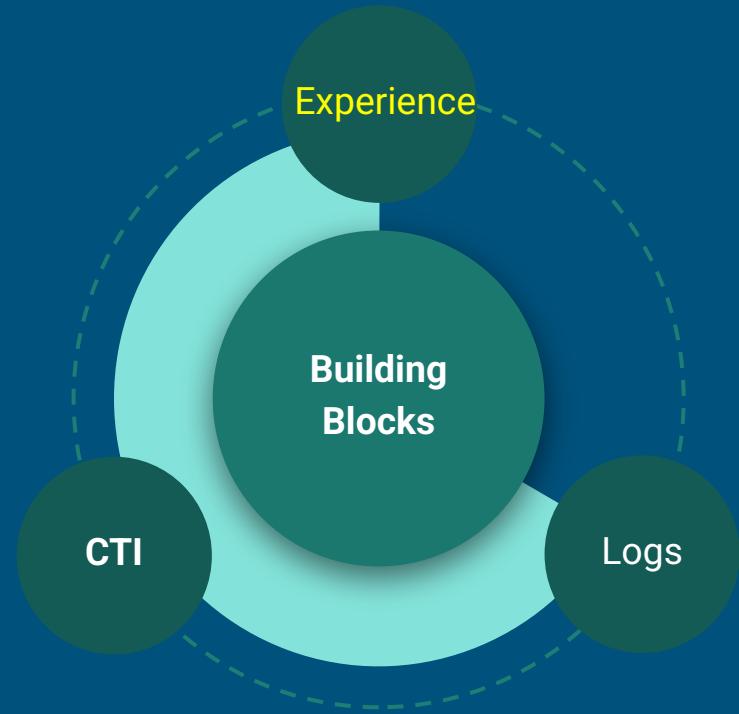
- Mandiant:** Includes articles like "Chinese Espionage Group UNC3886 Found Exploit...", "Cutting Edge: Suspected APT Targets Ivanti Connect ...", "Hundreds of Thousands of Dollars Worth of Solana ...", "The Defender's Advantage Cyber Snapshot, Issue 5 ...", and "Opening a Can of Whoop Ads: Detecting and Disrup...".
- Kaspersky:** Includes articles like "Cracked software beats gold: new macOS backdoor ...", "Dark web threats and dark market predictions for 20...", "A lightweight method to detect potential iOS malware", "Operation Triangulation: The last (hardware) mystery", and "Windows CLFS and five exploits used by ransomwar...".
- MSRC & MSTIC:** Includes articles like "Microsoft addresses App Installer abuse", "Azure Serial Console Attack and Defense - Part 2", "Introducing the Microsoft Defender Bounty Program", "Celebrating ten years of the Microsoft Bug Bounty p...", and "Reflecting on 20 years of Patch Tuesday".
- The DFIR Report:** Includes articles like "Lets Open(Dir) Some Presents: An Analysis of a Persi...", "SQL Brute Force Leads to BlueSky Ransomware", "NetSupport Intrusion Results in Domain Compromise", "From ScreenConnect to Hive Ransomware in 61 hours", and "HTML Smuggling Leads to Domain Wide Ransomware".
- CrowdStrike:** Includes articles like "CrowdStrike Demonstrates Cloud Security Leadershi...", "CrowdStrike's View on the New U.S. Policy for Artifici...", "Eliminate Repetitive Tasks and Accelerate Response ...", "The Difference Between Securing Custom-Developed ...", and "Endpoint and Identity Security: A Critical Combinatio...".
- Unit 42:** Includes articles like "Parrot TDS: A Persistent and Evolving Malware Camp...", "Threat Brief: Ivanti Vulnerabilities CVE-2023-46805 a...", "Financial Fraud APK Campaign", "Medusa Ransomware Turning Your Files into Stone", and "Tackling Anti-Analysis Techniques of GuLoader and ...".
- Ransomware Statistic 2023:** A world map showing ransomware statistics.
- News Analysis:** Includes news items from various sources such as "EFF adds Street Surveillance Hub so Americans can c...", "New macOS Malware Targets Cracked Apps", "Introducing Wordfence CLI 3.0.1: Now With Automat...", "Scans/Exploit Attempts for Atlassian Confluence RCE...", and "UK Expansion of Sophos Partnership with Cowbell".
- Cybereason:** Includes news items like "What's on the Smartest Cybersecurity Minds for 202...", "THREAT ALERT: CITRIXBLEED (CVE-2023-4966)", "Malicious Life Podcast: Volt Typhoon", "THREAT ALERT: Dlvu Variant Delivered by Loader Ma...", and "2024 Cybersecurity Predictions - Generative AI Resh...".

<https://start.me/p/wMrA5z/cyber-threat-intelligence>

Indicator Sources



Indicator Sources





Sigma Fields

title

Short title of what you are making this detection for, do not use the word "detects"

id

Unique ID, uncoder.io / sigconverter will generate one for you

status

Experimental, until tested

description

Detail what the rule is looking for, start with "Detects ..."

references

List references

author

Separate by comma
Can also put @handle



Sigma Fields

date

Date of rule creation
Also a modified date field

*tags

ATT&CK, CAR, CVE, TLP

*logsource

Annotate where the logs
are coming from

*detection

Use selections and
conditions to detect

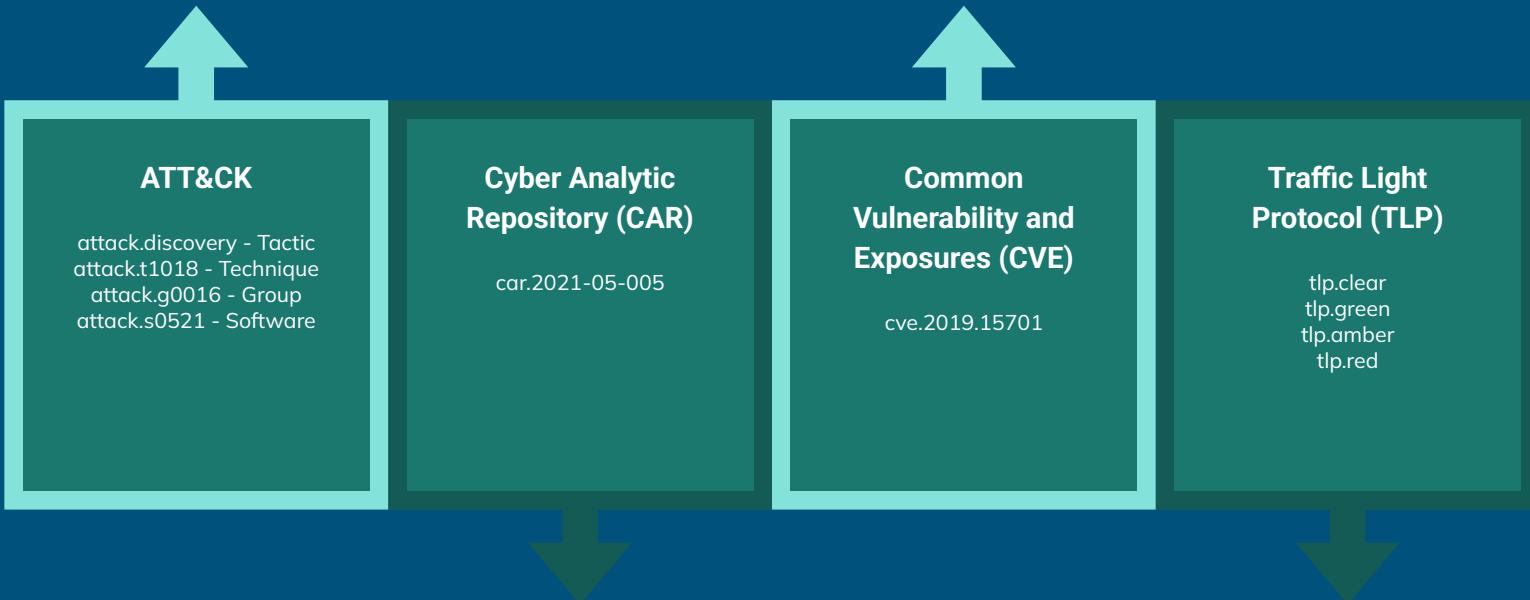
falsepositives

Why might this detection
create false positives?

level

Level of this alert: info, low,
medium, high, critical

Standards: Tags



Standards: Logsource

Product:

- windows
- zeek
- aws

Category:

- process_creation
- network_connection
- registry_add

Service:

- http
- wmi
- cloudtrail

```
logsource:  
    product: windows  
    category: process_creation
```

```
logsource:  
    product: linux  
    service: guacamole
```

```
logsource:  
    product: aws  
    service: cloudtrail
```

<https://github.com/SigmaHQ/sigma-specification/blob/main/specification/sigma-appendix-taxonomy.md>

Standards: Filename

Generally: [category|service]_product_action.yml

- proc_creation_win_7zip_exfil_dmp_files.yml
- file_delete_win_delete_backup_file.yml
- net_connection_lnx_back_connect_shell_dev.yml
- file_access_win_susp_gpo_access_file.yml



The screenshot shows a GitHub repository interface. At the top, it displays the path: sigma / rules / windows / network_connection /. Below this, there is a list of files in the directory:

- net_connection_win_addinutil.yml
- net_connection_win_certutil_initiated_connection.yml
- net_connection_win_dllhost_non_local_ip.yml

A merge pull request from the user **nasbench** is shown above the file list, with the commit message "Merge PR #4702 from @nasbench - Rule tuning and updates".

<https://github.com/SigmaHQ/sigma-specification/blob/main/sigmahq-sigmafilename-convention.md>

proc_creation_win_7zip_password_compression.yml

title: Compress Data and Lock With Password for Exfiltration With 7-ZIP

id: 9fbf5927-5261-4284-a71d-f681029ea574

status: test

description: An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities

references:

author: frack113

date: 2021-07-27

modified: 2023-03-13

tags:

- attack.collection
- attack.t1560.001

logsource:

category: process_creation

product: windows

detection:

selection_img:

- Description|contains: '7-Zip'

- Image|endswith:

- '\7z.exe'
- '\7zr.exe'
- '\7za.exe'

- OriginalFileName:

- '7z.exe'
- '7za.exe'

selection_password:

CommandLine|contains: '-p'

selection_action:

CommandLine|contains:

- 'a'
- 'u'

condition: all of selection_*

falsepositives:

- Legitimate activity is expected since compressing files with a password is common.

level: medium

Detection Logic

selection_img



Description contains 7-Zip
OR Image endswith 7z.exe OR 7zr.exe OR 7za.exe
OR OriginalFileName is 7z.exe OR 7za.exe

selection_password



CommandLine contains '-p'

selection_action



CommandLine contains either 'a' **OR** 'u'

condition: all of selection_*

03

Rule Translation

Make it actionable!

SIGCONVERTER

sigconverter.io
sigma rule converter



Backend:

splunk

Format:

default

Pipeline:

select pipelines...

CLI:

```
sigma convert --without-pipeline -t splunk -f default rule.yml
```

rule.yml pipeline.yml

```
title: Compress Data and Lock With Password for Exfiltration With 7-ZIP
id: 9ffbf927-5261-4284-a71d-f681029ea574
status: test
description: An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities
references:
  - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
author: frack113
date: 2021/07/27
modified: 2023/03/13
tags:
  - attack.collection
  - attack.t1560.001
logsource:
  category: process_creation
  product: windows
detection:
  selection_img:
    - Description|contains: '7-Zip'
    - Image|endswith:
      - '\7z.exe'
      - '\7zr.exe'
      - '\7za.exe'
    - OriginalFileName:
      - '7z.exe'
      - '7za.exe'
```

query

```
Description="*7-zip*" OR Image IN ("*\7z.exe", "*\7zr.exe", "*\7za.exe") OR OriginalFileName IN ("7z.exe", "7za.exe") CommandLine="* -p*" CommandLine IN ("* a **", "* u **")
```

To Install: pip3 install sigma-cli

Detected!

splunk>enterprise Apps ▾

Tyler Casey

Search Analytics Datasets Reports Alerts Dashboards

New Search

```
1 index=main
2 source=WinEventLog:*
3 AND ((Description="*7-Zip*" OR (Image="*\7z.exe" OR Image="*\7zr.exe" OR Image="*\7za.exe"))
4 OR (OriginalFileName="7z.exe" OR OriginalFileName="7za.exe"))
5 AND CommandLine="* -p*" AND (CommandLine="* a *" OR CommandLine="* u *"))
6 | table Description Image CommandLine
```

✓ 3 events (2/15/24 6:21:00.000 PM to 2/15/24 7:21:02.000 PM) No Event Sampling ▾

Events (3) Patterns Statistics (3) Visualization

20 Per Page ▾ Format Preview ▾

Description	Image	CommandLine
7-Zip Console	C:\Program Files\7-Zip\7z.exe	"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! C:\Users\Administrator\Desktop\recon.txt C:\exfil.7z
7-Zip Console	C:\Program Files\7-Zip\7z.exe	"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! C:\Users\Administrator\Desktop\recon.txt C:\exfil.7z
7-Zip Console	C:\Program Files\7-Zip\7z.exe	"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! exfil.7z C:\Users\Administrator\Desktop\recon.txt

Lab(s) Time!

02*



Rules 201

Create it, Standardize it, Read it...
CORRELATE IT

Correlated Sigma Rules

- Most Sigma rules describe **single events**
- **Correlation rules** detect threats by linking **multiple related events**
- Focus on **patterns over time**, not isolated logs
- Used to identify complex attacks that evade simple detections



```
rules/windows_failed_login_single_user.yml
yaml
1   title: Windows Failed Logon Event
2   + name: failed_logon # Rule Reference
3   description: Detects failed logon events on Windows systems.
4   logsource:
5     product: windows
6     service: security
7   detection:
8     selection:
9       EventID: 4625
10    condition: selection
11  ---
12  title: Multiple failed logons for a single user (possible brute force attack)
13  correlation:
14    type: event_count
15    rules:
16      - failed_logon # Referenced here
17    group-by:
18      - TargetUserName
19      - TargetDomainName
20    timespan: 5m
21    condition:
22      gte: 10
```

How do they work?

```
title: Windows Failed Logon Event
name: failed_logon
status: test
description: |
    Detects failed logon events on Windows systems.
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4625
filter:
    SubjectUserName|endswith: $
condition: selection and not filter
---
```

```
title: Multiple failed logons for a single user (possible
brute force attack)
status: test
correlation:
    type: event_count
rules:
    - failed_logon
group-by:
    - TargetUserName
    - TargetDomainName
timespan: 5m
condition:
    gte: 10
```

THANK YOU



@1qazCasey



/tyler-j-casey