Building & Validating Detections with Adversary Intelligence

BsidesCharm Workshop

April 30, 2023

Scott Small, Director of Cyber Threat Intelligence

TIDAL

Agenda

- Logistics & Summary
- Infostealer Threat Landscape
- Practical, Threat-Informed Detection & Validation
  - Guidance, Resources, & Workflows for 3 Example Cases:
    - Applying CTI for Quick Defensive Gap Identification
    - Emulating & Detecting a Top CTI Technique
    - Spotting an Outlier

Workshop Logistics

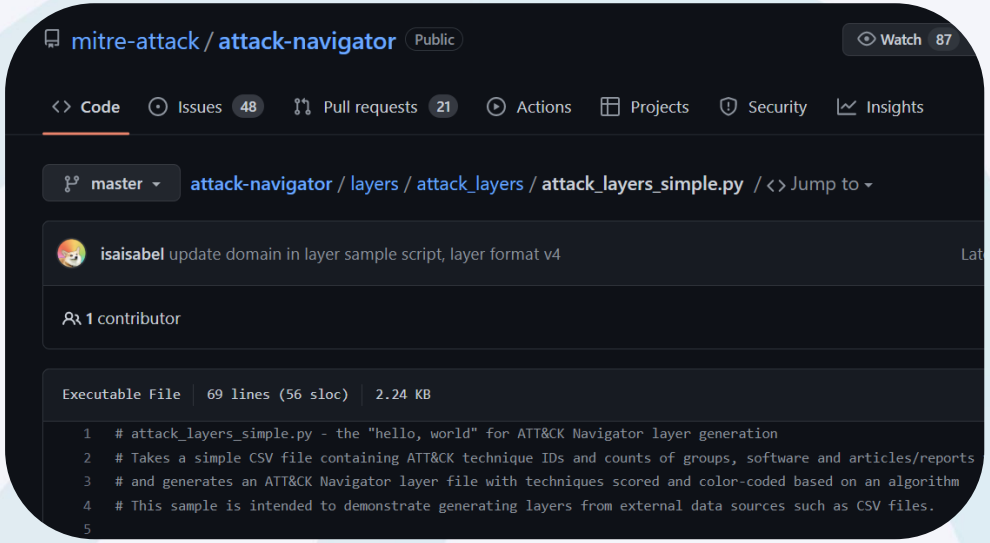
Primary focus: *Exposure to* many tools & resources

- CTI tools, Testing/Simulation tools, Detection Tools (all optional)

See handout if you want to go hands-on

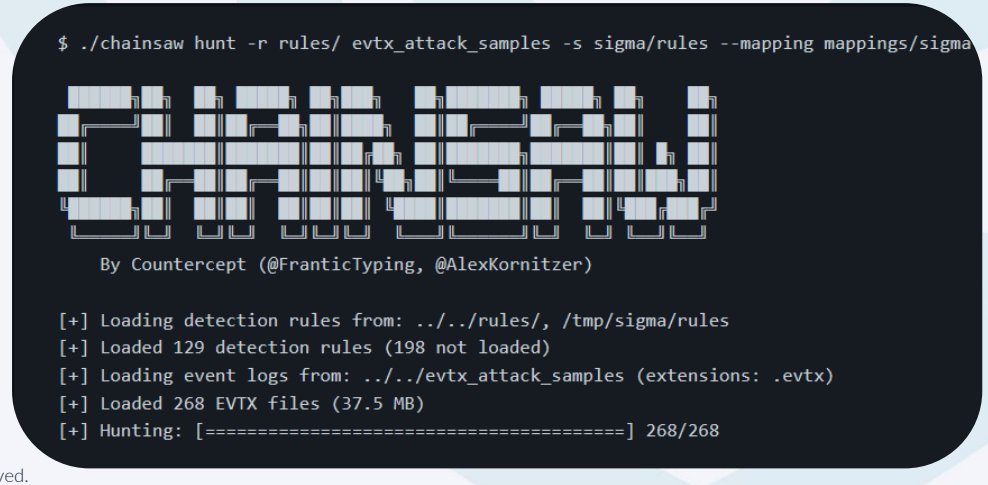
Start big downloads (VirtualBox environment) now

At least one break (aiming to end early)



Atomic Red Team

Sigma Public Repository



TIDAL

whoami

Career intelligence researcher & analyst

- Purple teamer
- OSINT + data viz

Expanding my “technical” skill & understanding through practical applications

- MITRE ATT&CK®, Atomics, Sigma, logging

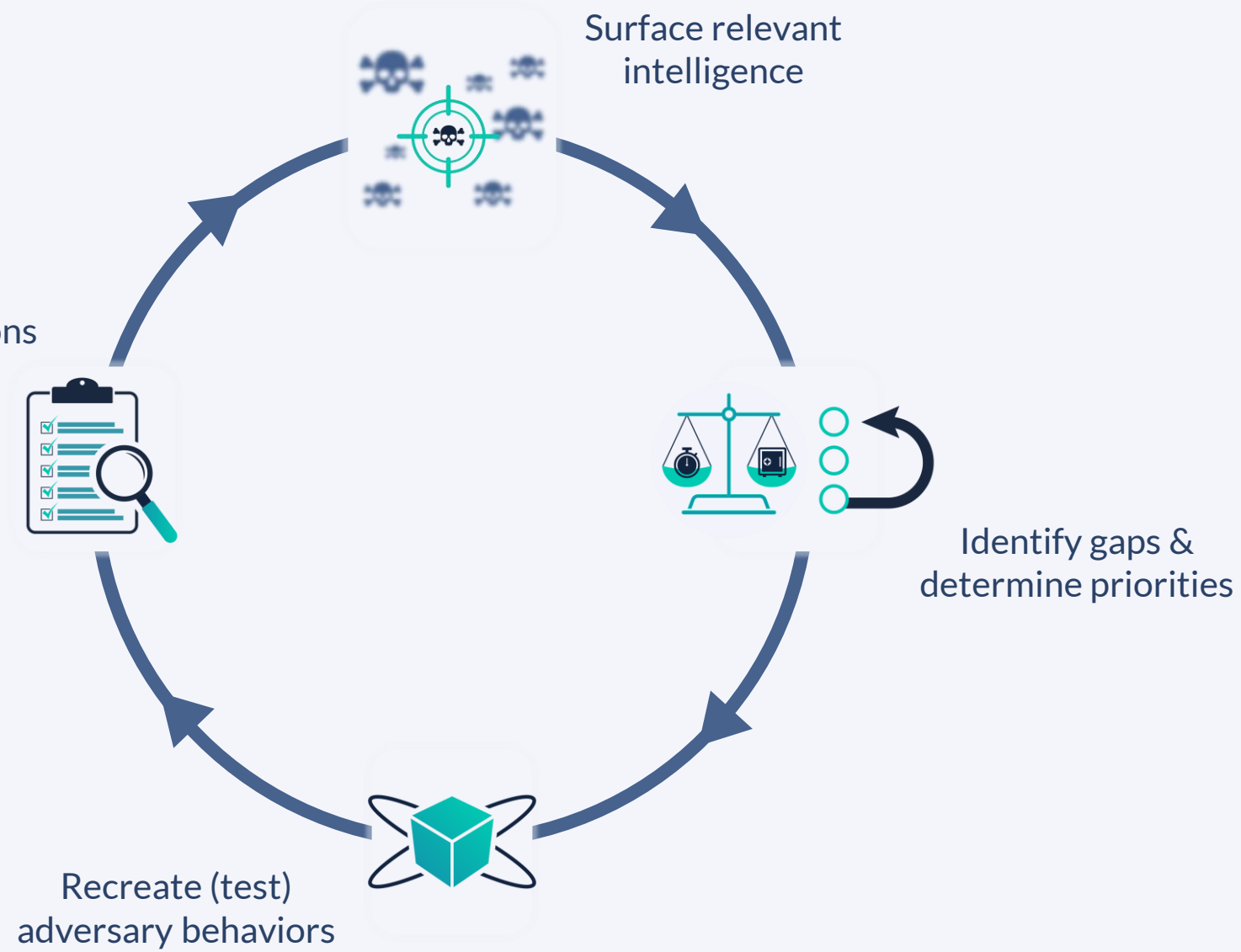
Cyber Threat Intelligence Director @ Tidal Cyber

- Threat-Informed Defense: *Systematic application & deep understanding of adversary tradecraft and technology to assess, organize, and optimize your defenses*

TIDAL

THREAT-INFORMED DEFENSE

Threat-Informed Detection Validation (Micro Purple Teaming)



*It's about the **mindset***

TIDAL

Benefits (& Limitations) of the Approach

Provides focus in an extremely wide (and growing) threat landscape

- Prioritize relevant threats, de-escalate would-be fires, alleviate burnout!

Expedites workflows, while retaining relevance

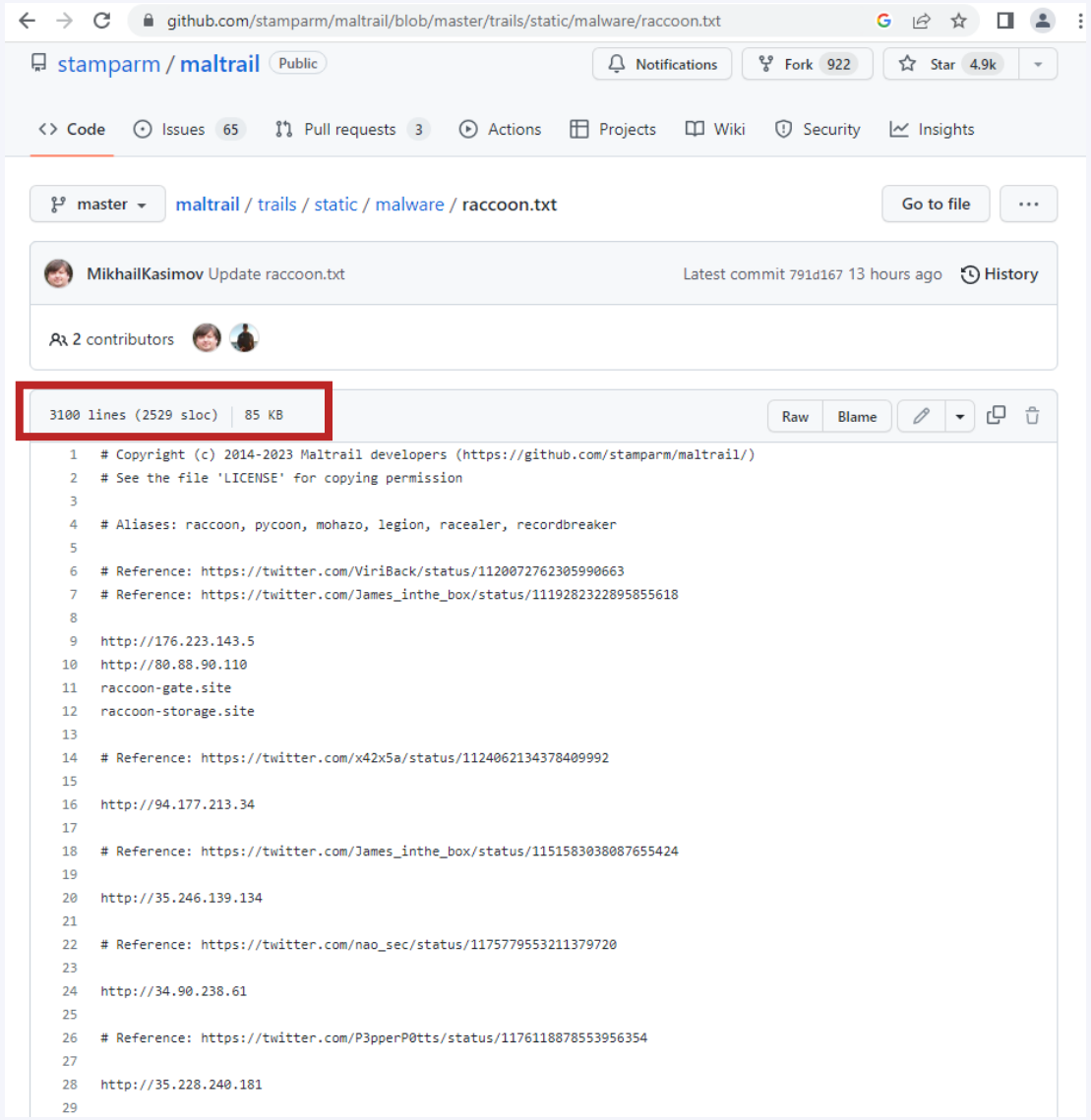
A step towards “proactive”?

Gateway & springboard for further skill development

Not a silver bullet (nothing is)

The Value of TTP Intelligence

IOCs



TTPs

Major Infostealers: Top Common TTPs

Infostealer Family	First Samples Observed	MITRE ATT&CK® Technique Count
RisePro Stealer	December 2022	18
StrelaStealer	November 2022	6
BlueFox Stealer	September 2022	17
Aurora Stealer	September 2022	17
Rhadamanthys Stealer	August 2022	22
Erbium Stealer	July 2022	33
DuckTail	July 2022	21
Raccoon Stealer v2.0	June 2022	19
RecordBreaker	June 2022	14
Prynt Infostealer	April 2022	24
BlackGuard Stealer	April 2022	16
Mars Stealer	February 2022	10
RedLine Stealer	March 2020	41
Raccoon Stealer	April 2019	41
Vidar	December 2018	14
LokiBot	2015	27

TIDAL

A Serious Threat for Enterprises

Infostealer Threat Landscape

TIDAL

THREAT-INFORMED DEFENSE

What are Infostealers?

Information- & credential-stealing malware ("infostealers")

- Usernames, PWs, cookies, tokens, financial details (esp. crypto), user/system info

Most often malware-as-a-service ("MaaS")

A low-cost & low-skill entry point into profitable cybercrime, driving up adoption

A **rich underground ecosystem has developed** to support infostealers

- Malware developers, team administrators, traffic generators, log parsers/distributors, **automated marketplaces** for stolen credential resale

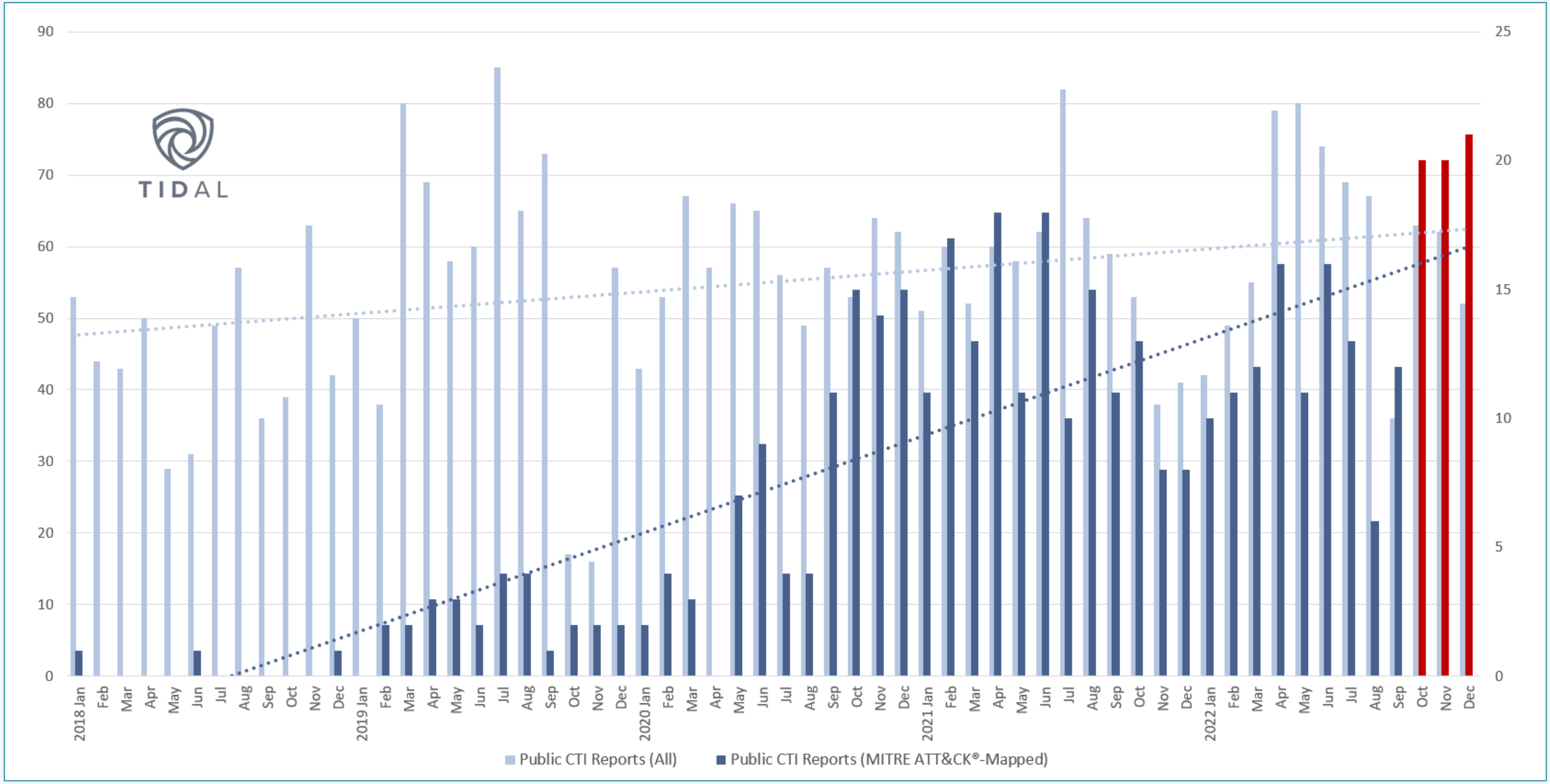
Pose a rising threat to **"high-value" targets**, including small, medium, & large businesses & organizations

TTP Evolution: Regular stealer development & evolution makes indicator-based approaches to defense challenging

Major & Emerging Infostealers CTI Summary

Infostealer Family	First Samples Observed	MITRE ATT&CK® Technique Count
RisePro Stealer	December 2022	18
StrelaStealer	November 2022	6
BlueFox Stealer	September 2022	17
Aurora Stealer	September 2022	17
Rhadamanthys Stealer	August 2022	6
Erbium Stealer	July 2022	33
DuckTail	July 2022	21
Raccoon Stealer v2.0	June 2022	19
RecordBreaker	June 2022	14
Prynt Infostealer	April 2022	24
BlackGuard Stealer	April 2022	16
Mars Stealer	February 2022	10
RedLine Stealer	March 2020	41
Raccoon Stealer	April 2019	41
Vidar	December 2018	14
LokiBot*	2015	27

*Only family currently in ATT&CK



A Practical Approach

Threat-Informed Detection & Validation

Setup: CTI Aggregation to Drive Prioritization

https://www.tidalcyber.com/blog/big-game-stealing-part-1-the-infostealer-landscape-rising-infostealer-threats-to-businesses-w

Big-Game Stealing: Increasing Infostealer Threat to "High-Value" Targets

Including Small, Medium, & Large Businesses & Organizations

Increased Intent

Infostealer-derived credentials linked to actors who compromised multiple major brands in 2022

Underground marketplaces catering to high-value log sales

Established "big-game" actors seeking infostealer capabilities

X

Increased Opportunity

Increasing impersonation of legitimate software for infostealer initial infections, including popular business tools:

Communication/Messaging
Remote Access
Password Management
Programming
Browsers/Updates

X

Increased Capability

Cookie theft capabilities in current strains enable session hijacking

Emerging families have new abilities to:

Steal MFA tokens

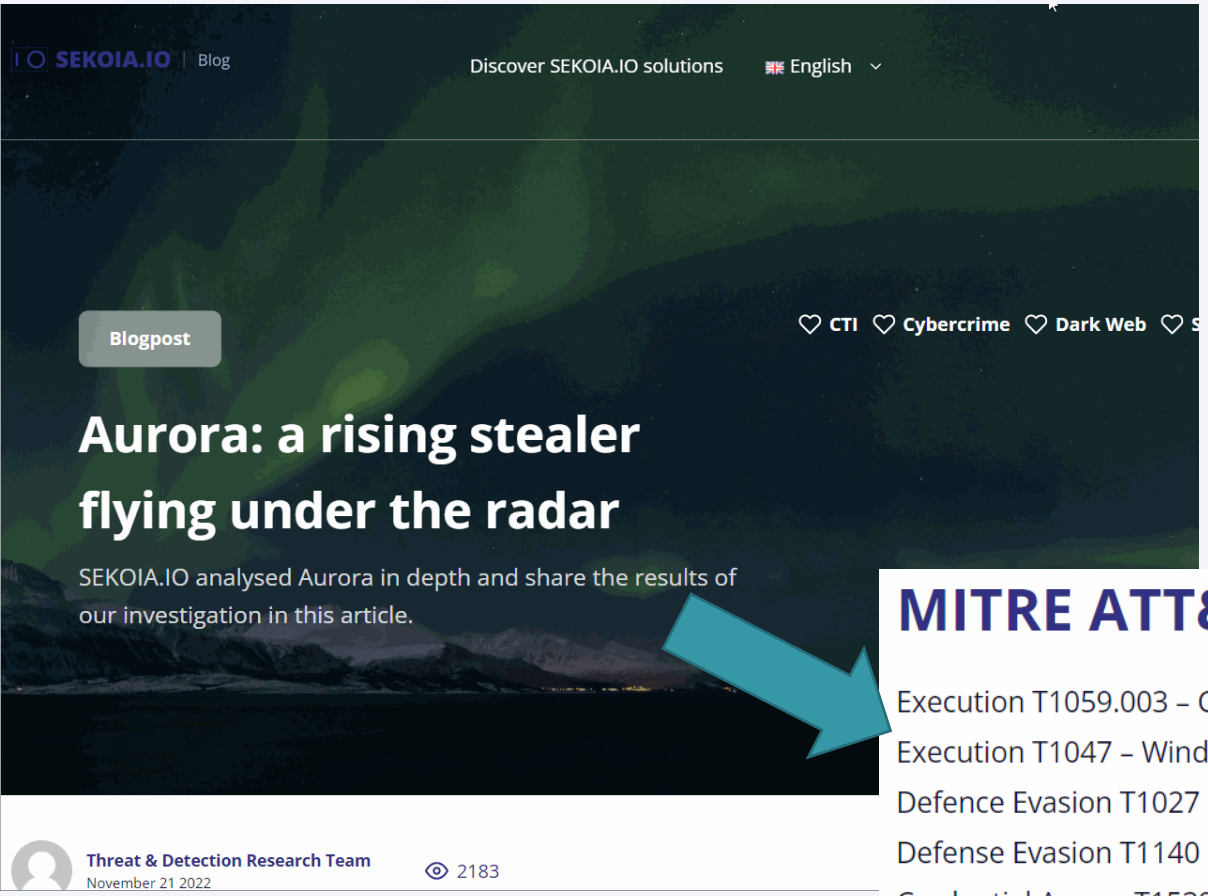
Target email accounts

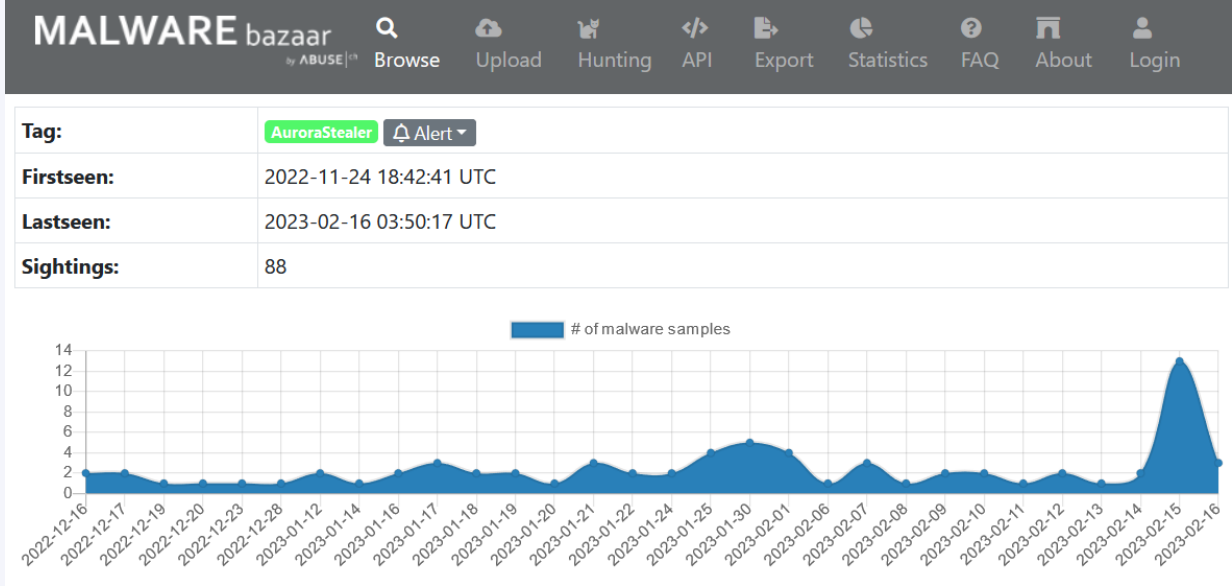
Increased evasion of advanced/enterprise security tools

=

Increased Threat

TIDAL





MITRE ATT&CK TTPs

Execution T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Execution T1047 – Windows Management Instrumentation
Defence Evasion T1027 – Obfuscated Files or Information
Defense Evasion T1140 – Deobfuscate/Decode Files or Information
Credential Access T1539 – Steal Web Session Cookie
Credential Access T1555.003 – Credentials from Password Stores: Credentials from Web Browsers
Discovery T1012 – Query Registry
Discovery T1082 – System Information Discovery
Discovery T1083 – File and Directory Discovery
Discovery T1614 – System Location Discovery
Collection T1005 – Data from Local System
Collection T1113 – Screen Capture

MITRE ATT&CK TTPs

Execution T1059.003 – Command and Scripting Interpreter: Windows Command Shell

Execution T1047 – Windows Management Instrumentation

Defence Evasion T1027 – Obfuscated Files or Information

Defense Evasion T1140 – Deobfuscate/Decode Files or Information

Credential Access T1539 – Steal Web Session Cookie

Credential Access T1555.003 – Credentials from Password Stores: Credentials from Web Browsers

Discovery T1012 – Query Registry

Discovery T1082 – System Information Discovery

Discovery T1083 – File and Directory Discovery

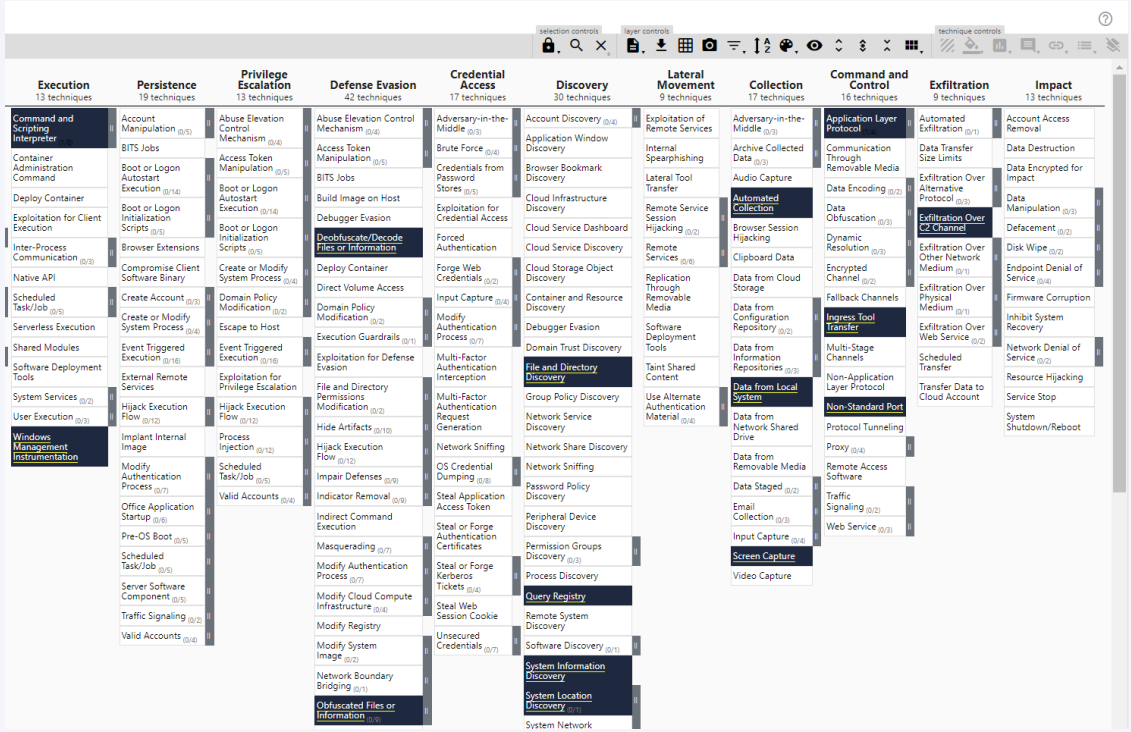
Discovery T1614 – System Location Discovery

Collection T1005 – Data from Local System

Collection T1113 – Screen Capture

Essential tool in the arsenal!

MITRE ATT&CK script: csv to Navigator json
https://github.com/mitre-attack/attack-navigator/blob/master/layers/attack_layers/attack_layers_simple.py



	A	B
1	techID	count
2	T1566	1
3	T1204	1
4	T1555	1
5	T1539	1
6	T1552	1
7	T1113	1
8	T1087	1
9	T1518	1
10	T1057	1
11	T1124	1
12	T1007	1
13	T1614	1
14	T1120	1
15	T1571	1
16	T1095	1
17	T1041	1

attack_layers_simple.py*

*Consider additional fields, like:

tactic
comment

redline_techniques.json


```
{
  "name": "redline_techniques",
  "versions": {
    "attack": "11",
    "navigator": "4.6.1",
    "layer": "4.3"
  },
  "domain": "enterprise-attack",
  "description": "Heatmap of instances of ATT&CK techniques.",
  "techniques": [
    {
      "techniqueID": "T1566",
      "score": 1
    },
    {
      "techniqueID": "T1204",
      "score": 1
    },
    {
      "techniqueID": "T1555",
      "score": 1
    },
    {
      "techniqueID": "T1539",
      "score": 1
    },
    {
      "techniqueID": "T1552",
      "score": 1
    },
    {
      "techniqueID": "T1113",
      "score": 1
    },
    {
      "techniqueID": "T1087",
      "score": 1
    },
    {
      "techniqueID": "T1518",
      "score": 1
    },
    {
      "techniqueID": "T1057",
```


JSON file

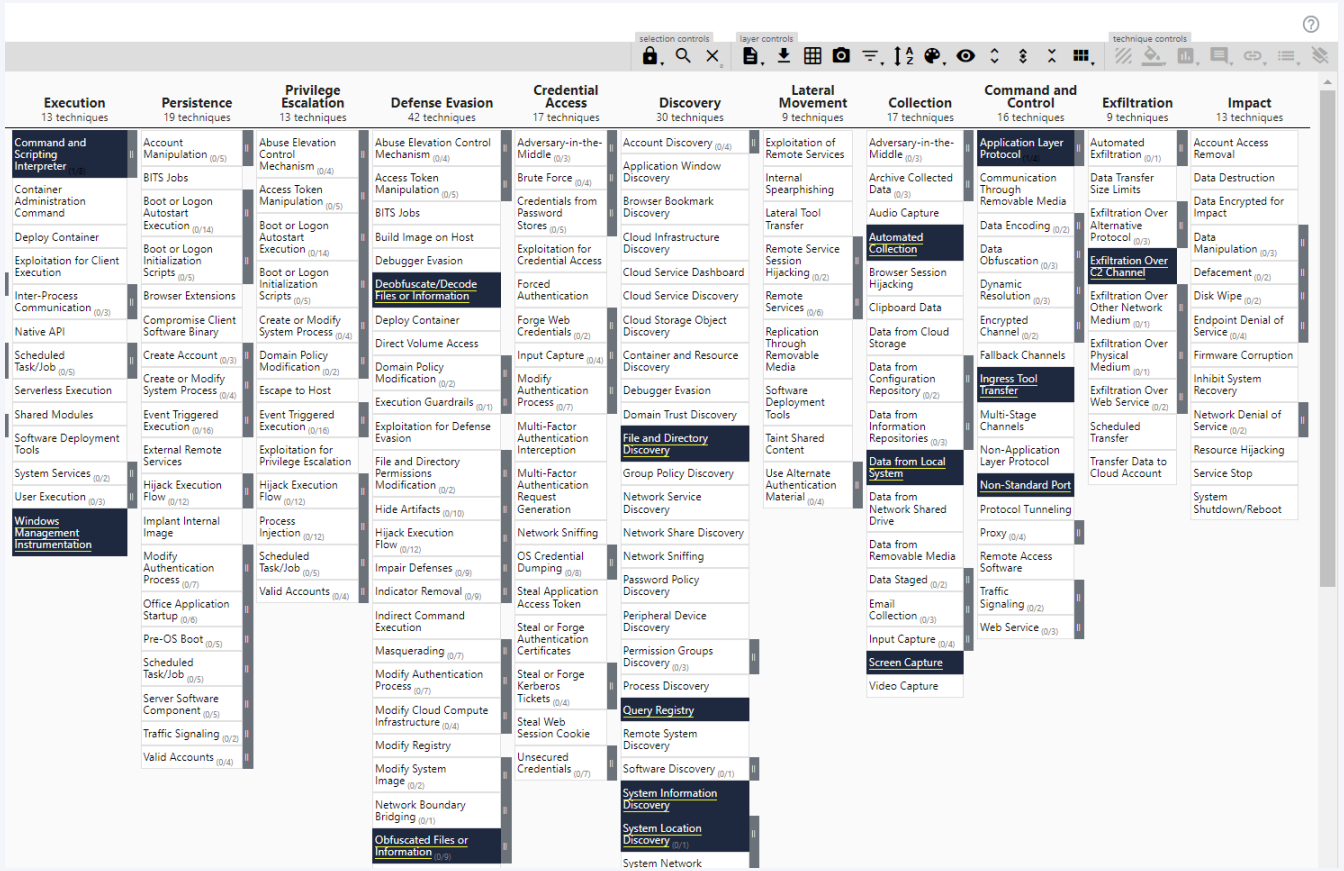
TIDAL

redline_techniques.json


```
{
  "name": "redline_techniques",
  "versions": {
    "attack": "11",
    "navigator": "4.6.1",
    "layer": "4.3"
  },
  "domain": "enterprise-attack",
  "description": "Heatmap of instances of ATT&CK techniques.",
  "techniques": [
    {
      "techniqueID": "T1566",
      "score": 1
    },
    {
      "techniqueID": "T1204",
      "score": 1
    },
    {
      "techniqueID": "T1555",
      "score": 1
    },
    {
      "techniqueID": "T1539",
      "score": 1
    },
    {
      "techniqueID": "T1552",
      "score": 1
    },
    {
      "techniqueID": "T1113",
      "score": 1
    },
    {
      "techniqueID": "T1087",
      "score": 1
    },
    {
      "techniqueID": "T1518",
      "score": 1
    },
    {
      "techniqueID": "T1057",
```

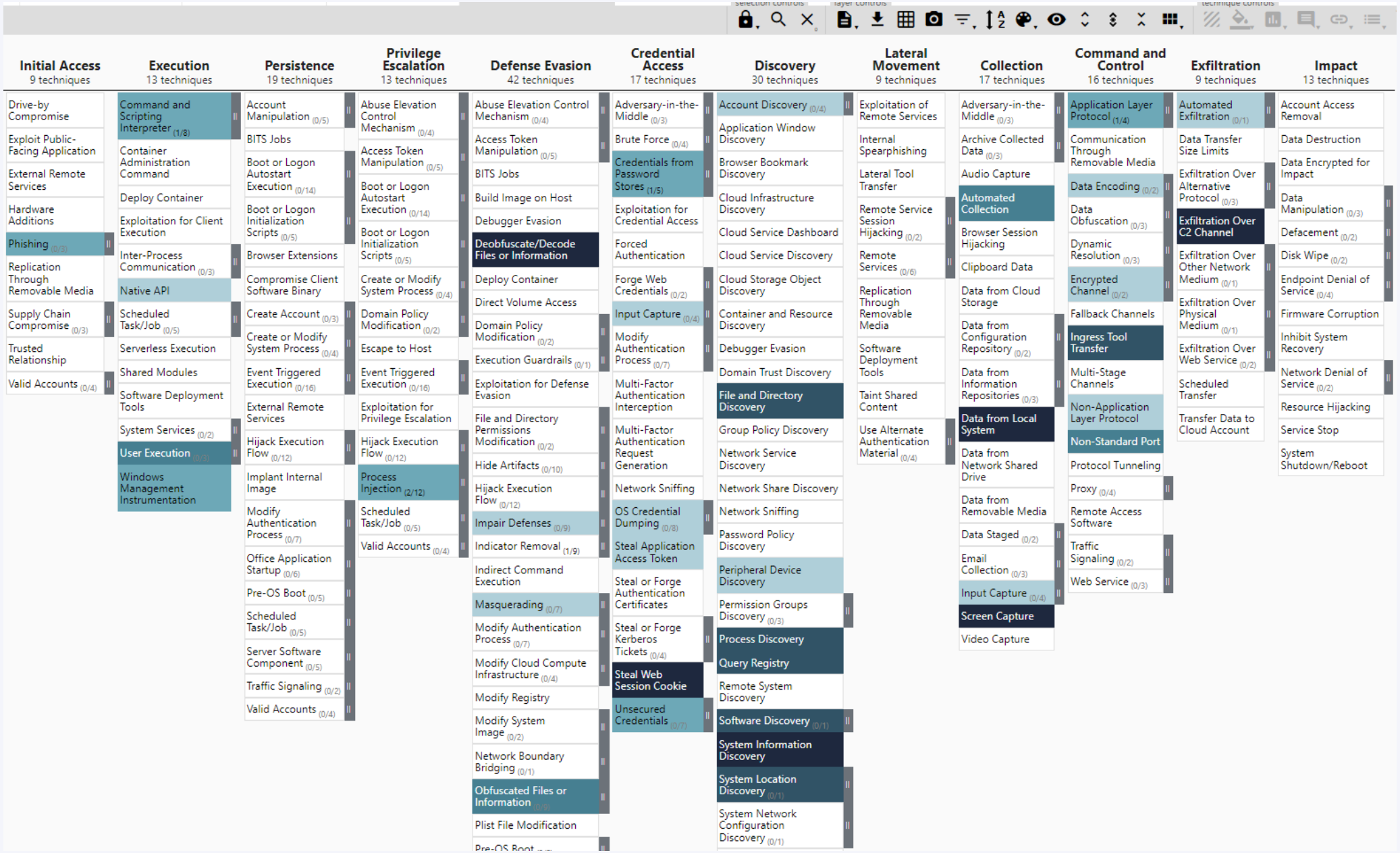

JSON file

Import custom Technique Set



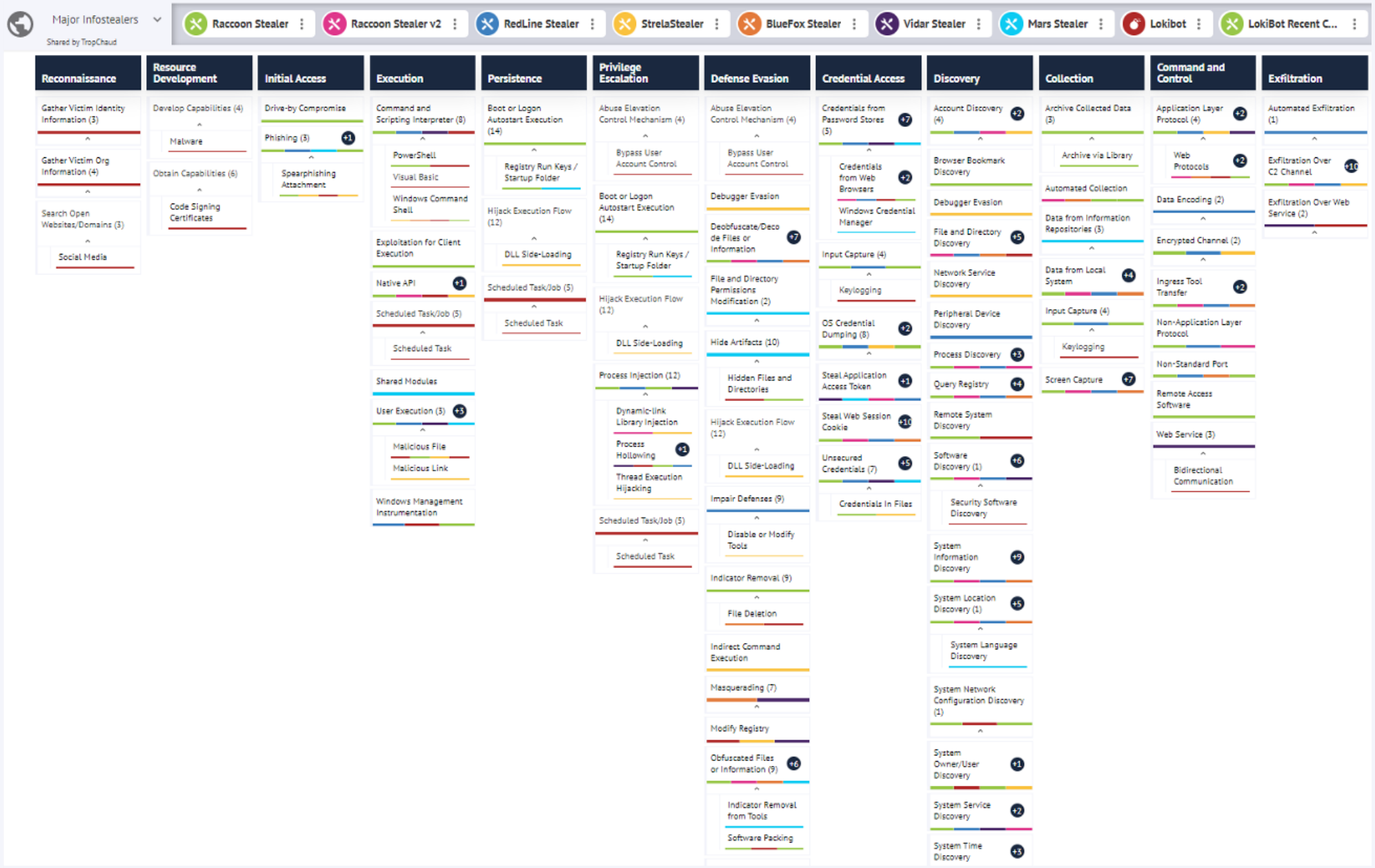
TIDAL

Scale it!



TIDAL

Scale it! app.tidalcyber.com/community-spotlight > “Major Infostealers” Matrix



TIDAL

Major & Emerging Infostealers

Summary of Select TTPs

How to prioritize?

Technique "density" is a great start, but just one approach

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1539	**Steal Web Session Cookie**	Credential Access	20	2	2	2
T1555.003	**Credentials from Web Browsers**	Credential Access	19	4	3	16
T1082	**System Information Discovery**	Discovery	16	4	14	24
T1027	**Obfuscated Files or Information**	Defense Evasion	15	4	84	8
T1113	**Screen Capture**	Collection	14	2	6	6
T1518	**Software Discovery**	Discovery	14	5	2	6
T1041	**Exfiltration Over C2 Channel**	Exfiltration	13	5	3	1
T1083	**File and Directory Discovery**	Discovery	12	3	17	6
T1057	**Process Discovery**	Discovery	11	3	5	5
T1204	**User Execution**	Execution	11	11	8	0
T1528	**Steal Application Access Token**	Credential Access	10	1	10	1
T1614	**System Location Discovery**	Discovery	9	4	0	0
T1012	**Query Registry**	Discovery	8	4	10	2
T1218.011	**Rundll32**	Defense Evasion	1	4	32	13

Example 1: Applying CTI for Quick Defensive Gap Identification

Importance of gap identification

Original dataset:

(Potential) Gap identified!

TIDAL

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1539	Steal Web Session Cookie	Credential Access	20	2	1	2
T1555.003	Credentials from Web Browsers	Credential Access	19	4	3	16
T1082	System Information Discovery	Discovery	16	4	14	24
T1027	Obfuscated Files or Information	Defense Evasion	15	4	84	8
T1113	Screen Capture	Collection	14	2	6	6
T1518	Software Discovery	Discovery	14	5	2	6
T1041	Exfiltration Over C2 Channel	Exfiltration	13	5	3	1
T1083	File and Directory Discovery	Discovery	12	3	17	6
T1057	Process Discovery	Discovery	11	3	5	5
T1204	User Execution	Execution	11	11	8	0
T1528	Steal Application Access Token	Credential Access	10	1	10	1
T1614	System Location Discovery	Discovery	9	4	0	0
T1012	Query Registry	Discovery	8	4	10	2
T1218.011	Rundll32	Defense Evasion	1	4	32	13

Red Team Tools

Simulating Adversary Behavior & Observing Tested Techniques

Atomic Red Team How-To

github.com/redcanaryco/atomic-red-team

Product Solutions Open Source Pricing Search Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.3k Star 7k

Code Issues 17 Pull requests 2 Actions Wiki Security Insights

master 94 branches 0 tags Go to file Code

Atomic Red Team doc generator Generated docs from job=generate-docs branch=mast... 054d751 yesterday 4,745 commits

.github	minor adjustment to how workflows are triggered (#1905)	8 months ago
atomic_red_team	Generate Indexes for Cloud Atomics (#2075)	5 months ago
atomics	Generated docs from job=generate-docs branch=master [ci skip]	yesterday
bin	bump nav version (#2261)	2 weeks ago
static	adding demo gif (#2051)	5 months ago
.gitignore	AWS Cloud atomics (#1457)	last year
CODE_OF_CONDUCT.md	Update CODE_OF_CONDUCT.md (#1934)	8 months ago
Gemfile	Add microsite (#250)	4 years ago
LICENSE.txt	move bin scripts into bin, apis into atomic-red-team	4 years ago
README.md	Add OpenSource Badge (#2277)	4 days ago
atomic-red-team.gemspec	Update atomic-red-team.gemspec (#1719)	last year

README.md

Open Source Security Index
Top-20 fastest-growing security projects

Atomic Red Team

About

Small and highly portable detection tests based on MITRE's ATT&CK.

mitre mitre-attack

Readme
MIT license
Code of conduct
7k stars
308 watching
2.3k forks

Releases

No releases published

Packages

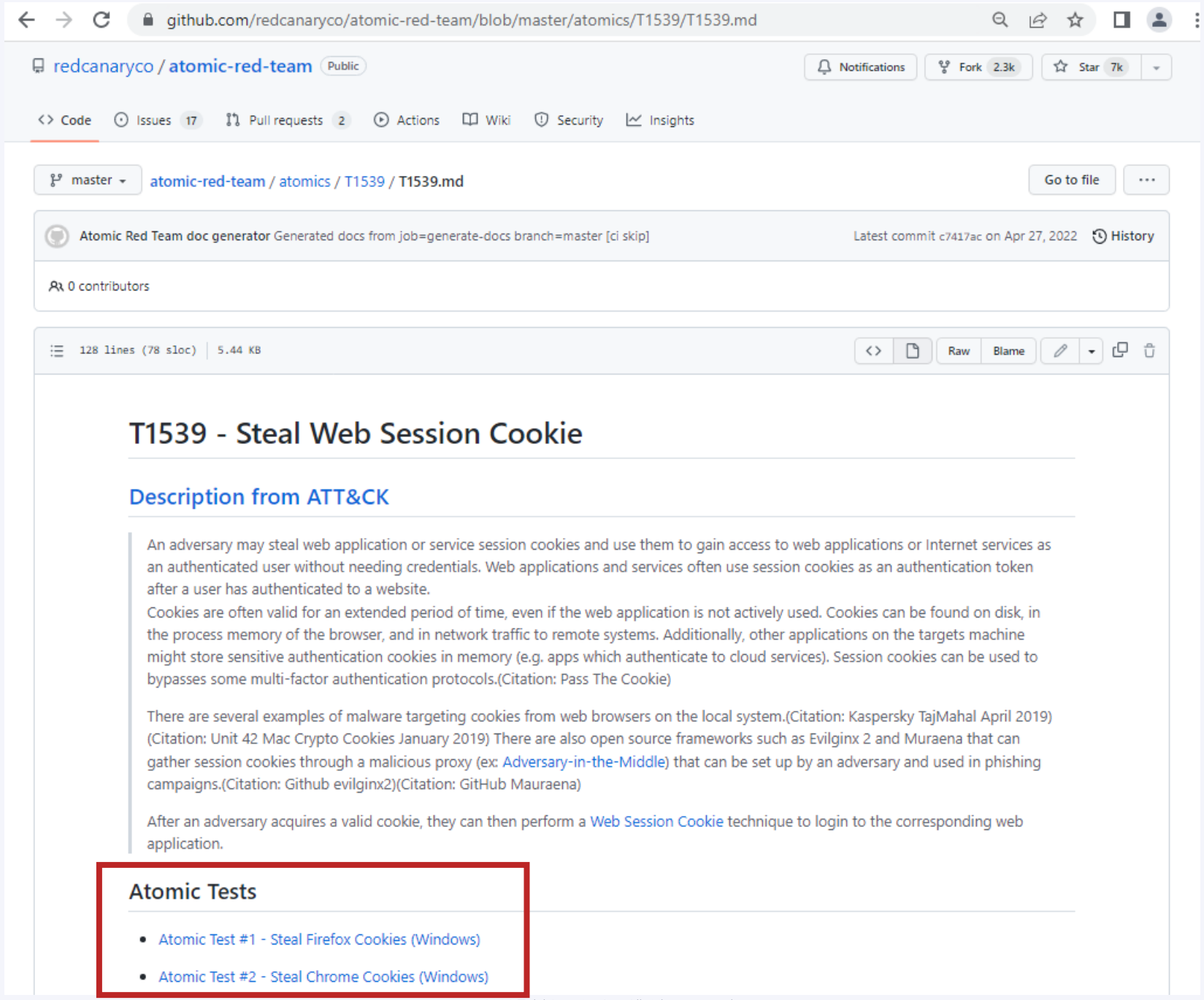
No packages published

Contributors 286

+ 275 contributors

Languages

TIDAL



TIDAL

github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1539/T1539.md#atomic-test-1---steal-firefox-cookies-windows

128 lines (78 sloc) | 5.44 KB

Raw Blame

Atomic Test #1 - Steal Firefox Cookies (Windows)

This test queries Firefox's cookies.sqlite database to steal the cookie data contained within it, similar to Zloader/Zbot's cookie theft function. Note: If Firefox is running, the process will be killed to ensure that the DB file isn't locked. See https://www.malwarebytes.com/resources/files/2020/05/the-silent-night-zloader-zbot_final.pdf.

Supported Platforms: Windows

auto_generated_guid: 4b437357-f4e9-4c84-9fa6-9bcee6f826aa

Inputs:

Name	Description	Type	Default Value
sqlite3_path	Path to sqlite3	Path	$env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe
output_file	Filepath to output cookies	Path	$env:temp\T1539FirefoxCookies.txt

Attack Commands: Run with `powershell`!

```
stop-process -name "firefox" -force -erroraction silentlycontinue
$CookieDBLocation = get-childitem -path "$env:appdata\Mozilla\Firefox\Profiles\*\cookies.sqlite"
"select host, name, value, path, expiry, isSecure, isHttpOnly, sameSite from [moz_cookies];" | cmd /c #{sqlite3_path} "$CookieDBLocat
```

Cleanup Commands:

```
remove-item #{output_file} -erroraction silentlycontinue
```

Dependencies: Run with `powershell`!

Description: Sqlite3 must exist at (#{sqlite3_path})

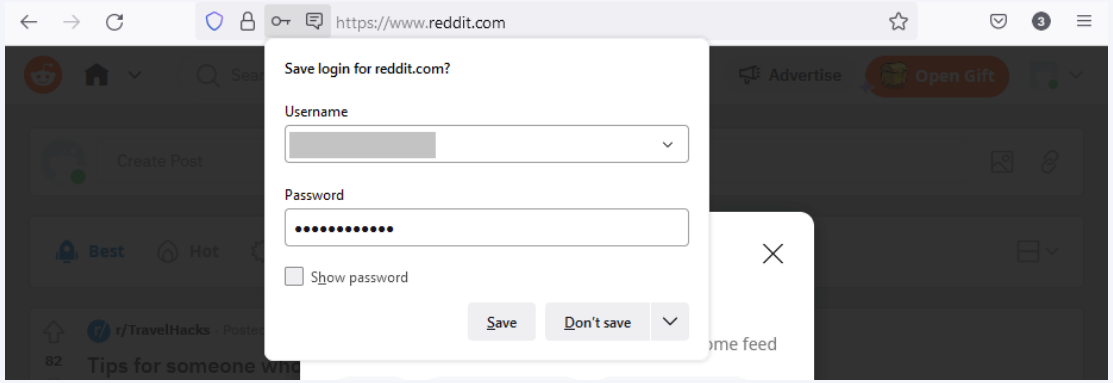
Check Prereq Commands:

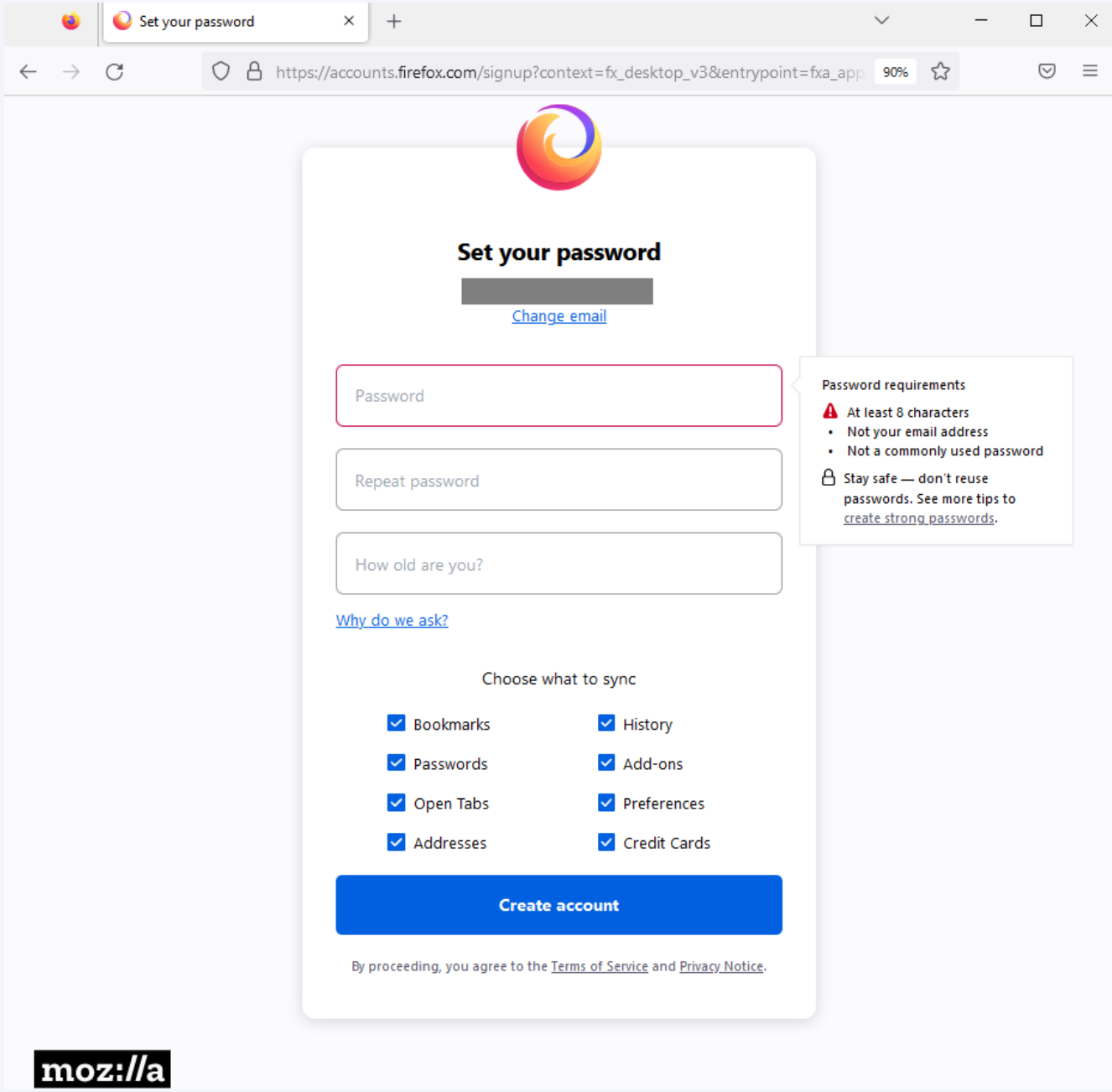
```
if (Test-Path #{sqlite3_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://www.sqlite.org/2022/sqlite-tools-win32-x86-3380200.zip" -OutFile "$env:temp\sqlite.zip"
Expand-Archive -path "$env:temp\sqlite.zip" -destinationpath "$env:temp\" -force
```

TIDAL





TIDAL

moz://a

Getting Started with Atomic Red Team testing

Invoke-AtomicRedTeam wiki: https://github.com/redcanaryco/invoke-atomicredteam/wiki

TIDAL

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
PS C:\Users\User> Invoke-AtomicTest T1539 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Steal Web Session Cookie T1539
Atomic Test Name: Steal Firefox Cookies (Windows)
Atomic Test Number: 1
Atomic Test GUID: 4b437357-f4e9-4c84-9fa6-9bcee6f826aa
Description: This test queries Firefox's cookies.sqlite database to steal the cookie data contained within it, similar to Zloader/Zbot's cookie
 theft function.  Note: If Firefox is running, the process will be killed to ensure that the DB file isn't locked.  See https://www.malwarebyte
s.com/resources/files/2020/05/the-silent-night-zloader-zbot_final.pdf.

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
stop-process -name "firefox" -force -erroraction silentlycontinue
$CookieDBLocation = get-childitem -path "$env:appdata\Mozilla\Firefox\Profiles\*\cookies.sqlite"
"select host, name, value, path, expiry, isSecure, isHttpOnly, sameSite from [moz_cookies];" | cmd /c #{sqlite3_path} "$CookieDBLocation" | out
-file -filepath "#{output_file}"
Command (with inputs):
stop-process -name "firefox" -force -erroraction silentlycontinue
$CookieDBLocation = get-childitem -path "$env:appdata\Mozilla\Firefox\Profiles\*\cookies.sqlite"
"select host, name, value, path, expiry, isSecure, isHttpOnly, sameSite from [moz_cookies];" | cmd /c $env:temp\sqlite-tools-win32-x86-3380200\
sqlite3.exe "$CookieDBLocation" | out-file -filepath "$env:temp\T1539FirefoxCookies.txt"

Cleanup Commands:
Command:
remove-item #{output_file} -erroraction silentlycontinue
Command (with inputs):
remove-item $env:temp\T1539FirefoxCookies.txt -erroraction silentlycontinue

Dependencies:
Description: Sqlite3 must exist at ($env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe)
Check Prereq Command:
if (Test-Path #{sqlite3_path}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path $env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe) {exit 0} else {exit 1}
Get Prereq Command:
Invoke-WebRequest "https://www.sqlite.org/2022/sqlite-tools-win32-x86-3380200.zip" -OutFile "$env:temp\sqlite.zip"
Expand-Archive -path "$env:temp\sqlite.zip" -destinationpath "$env:temp\" -force
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
Technique: Steal Web Session Cookie T1539
Atomic Test Name: Steal Chrome Cookies (Windows)
Atomic Test Number: 2
Atomic Test GUID: 26a6b840-4943-4965-8df5-ef1f9a282440
```

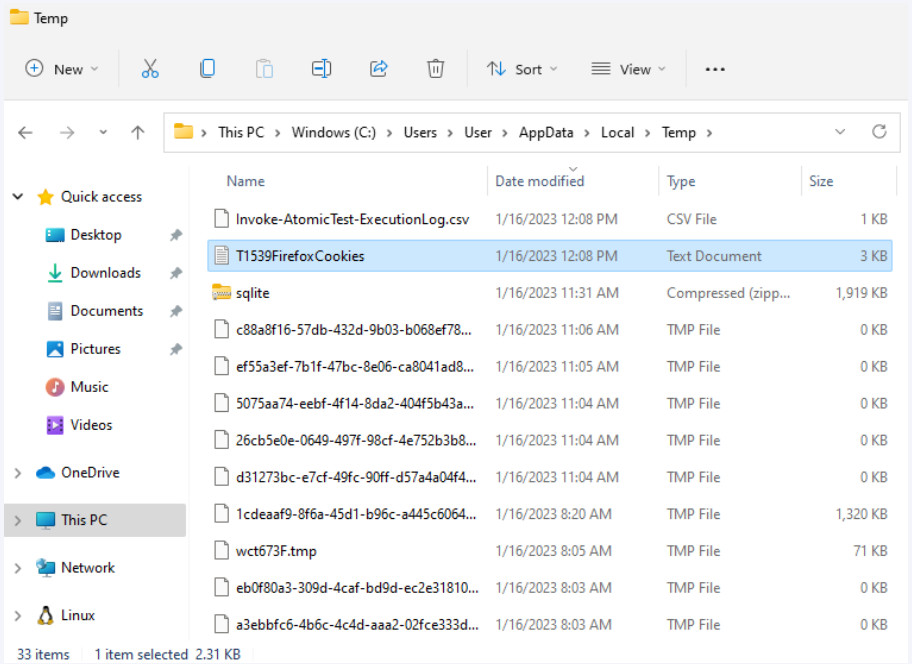
Carrying out a real-world adversary attack / technique

```
PS C:\Users\User> Invoke-AtomicTest T1539 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1539-1 Steal Firefox Cookies (Windows)
Attempting to satisfy prereq: Sqlite3 must exist at ($env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe)
Prereq successfully met: Sqlite3 must exist at ($env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe)
GetPrereq's for: T1539-2 Steal Chrome Cookies (Windows)
Attempting to satisfy prereq: Sqlite3 must exist at ($env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe)
Prereq already met: Sqlite3 must exist at ($env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe)
PS C:\Users\User>
```

```
PS C:\Users\User> Invoke-AtomicTest T1539 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1539-1 Steal Firefox Cookies (Windows)
Done executing test: T1539-1 Steal Firefox Cookies (Windows)
PS C:\Users\User>
```



TIDAL

Blue/Purple Team Tools

Closing the Gap: Closing Gaps With (Validated!) Detections

TIDAL

THREAT-INFORMED DEFENSE

Logging With Sysmon

Sysmon v14.13

Article • 11/28/2022 • 15 minutes to read • 9 contributors

Feedback

By Mark Russinovich and Thomas Garnier

Published: November 28, 2022

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

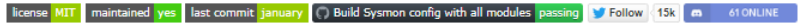
Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

TIDAL

github.com/olafhartong/sysmon-modular

README.md

sysmon-modular | A Sysmon configuration repository for everybody to customise



This is a Microsoft Sysinternals Sysmon download here configuration repository, set up modular for easier maintenance and generation of specific configs.

Please keep in mind that any of these configurations should be considered a starting point, tuning per environment is **strongly** recommended.

The sysmonconfig.xml within the repo is automatically generated after a successful merge by the PowerShell script and a successful load by Sysmon in an Azure Pipeline run. More info on how to generate a custom config, incorporating your own modules here

Pre-Grenerated configurations

Type	Config	Description
default	sysmonconfig.xml	This is the balanced configuration, most used, more information here
verbose	sysmonconfig-excludes-only.xml	This is the very verbose configuration, all events are included, only the exclusion modules are applied. This should not be used in production without validation, will generate a significant amount of data and might impact performance. More information here
super verbose	sysmonconfig-research.xml	A configuration with extreme verbosity. The log volume expected from this file is significantly high, really DO NOT USE IN PRODUCTION! This config is only for research, this will use way more CPU/Memory. Only enable prior to running the to be investigated technique, when done load a lighter config.
MDE augment	sysmonconfig-mde-augmentation.xml	A configuration to augment Defender for Endpoint, intended to augment the information and have as little overlap as possible. This is based on the default/balanced config and will *not generate all events* for Sysmon, there are comments in the config. In the benefit of IR, consider using the excludes only config and only ingest the enriching events. (Blog with more rationale soon)

Index

github.com/SwiftOnSecurity/sysmon-config

Product Solutions Open Source Pricing Search Sign in Sign up

SwiftOnSecurity / sysmon-config Public

Notifications Fork 1.5k Star 3.9k

Code Issues 42 Pull requests 25 Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

SwiftOnSecurity Merge pull request #151 from Neo23x0/patch-8 ... 1836897 on Oct 16, 2021 173 commits

.gitignore	d	3 years ago
README.md	Update README.md	2 years ago
sysmonconfig-export.xml	Merge pull request #151 from Neo23x0/patch-8	last year

README.md

sysmon-config | A Sysmon configuration file for everybody to fork

This is a Microsoft Sysinternals Sysmon configuration file template with default high-quality event tracing.

The file should function as a great starting point for system change monitoring in a self-contained and accessible package. This configuration and results should give you a good idea of what's possible for Sysmon. Note that this does not track things like authentication and other Windows events that are also vital for incident investigation.

sysmonconfig-export.xml

Because virtually every line is commented and sections are marked with explanations, it should also function as a tutorial for Sysmon and a guide to critical monitoring areas in Windows systems.

- For a far more exhaustive and detailed approach to Sysmon configuration from a different approach, see also sysmon-modular by @olafhartong, which can act as a superset of sysmon-config.
- Sysmon is a compliment to native Windows logging abilities, not a replacement for it. For valuable advice on these configurations, see MalwareArchaeology Logging Cheat Sheets by @HackerHurricane.

Note: Exact syntax and filtering choices in the configuration are highly deliberate in what they target, and to have as little performance impact as possible. Sysmon's filtering abilities are different than the built-in Windows auditing features, so often a different approach is taken than the normal static listing of paths.

About

Sysmon configuration file template with default high-quality event tracing

windows monitoring logging sysmon threat-hunting threatintel netsec sysinternals

Readme
3.9k stars
354 watching
1.5k forks

Releases

No releases published

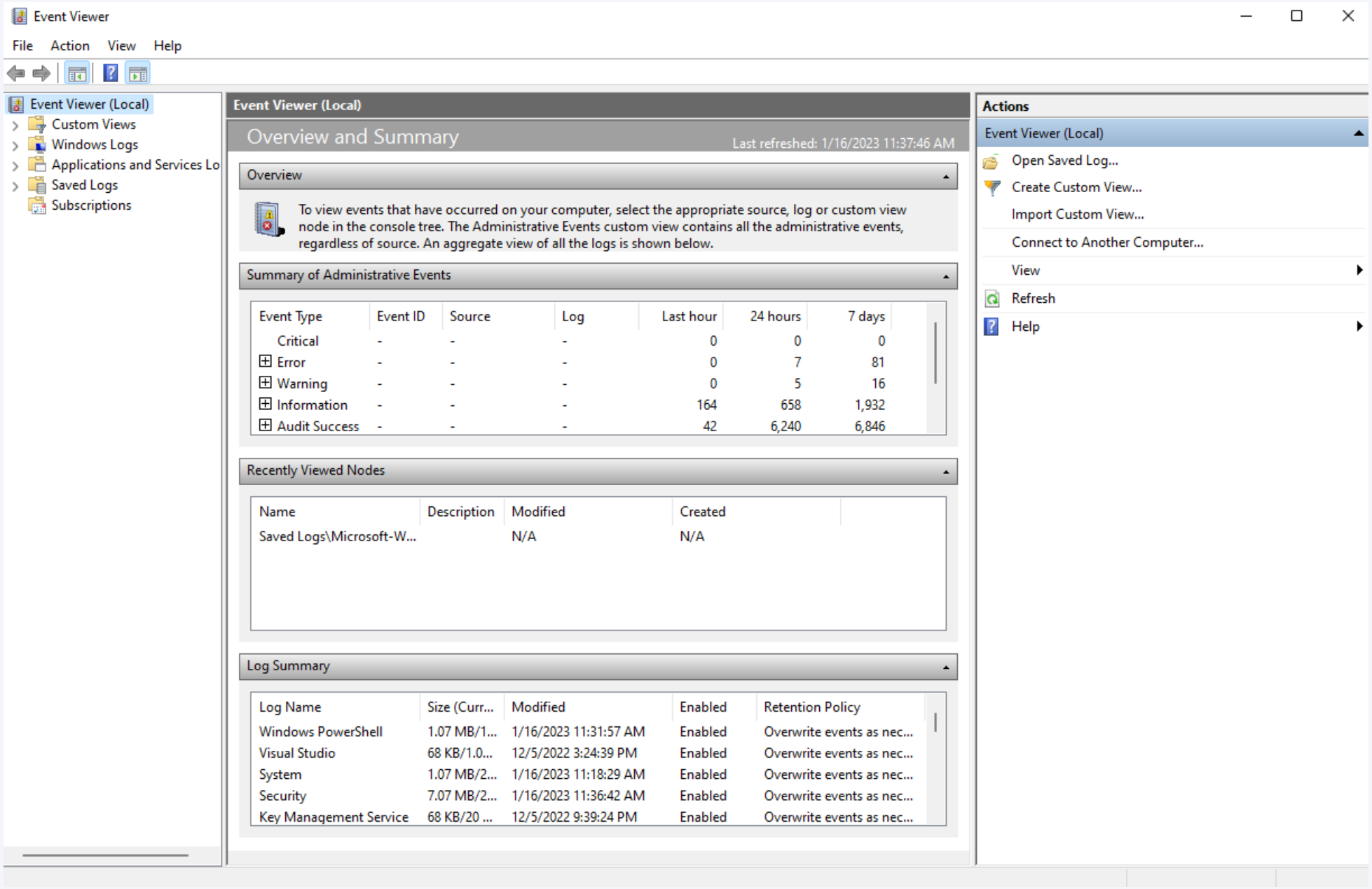
Packages

No packages published

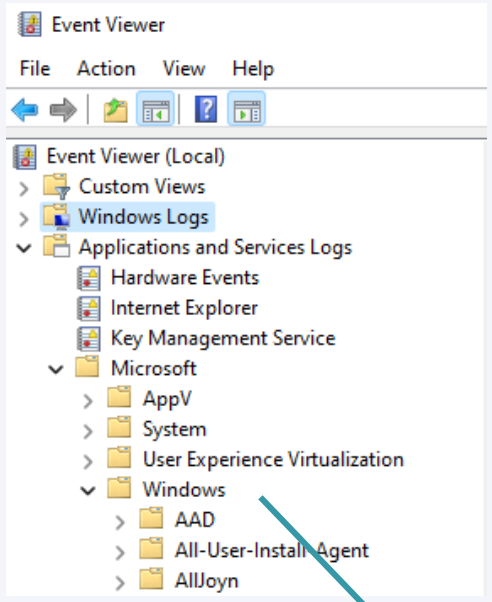
Contributors 18

+ 7 contributors

TIDAL



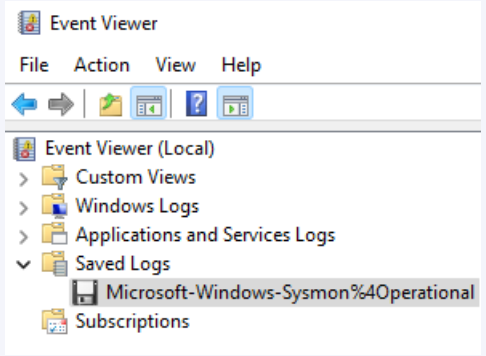
TIDAL

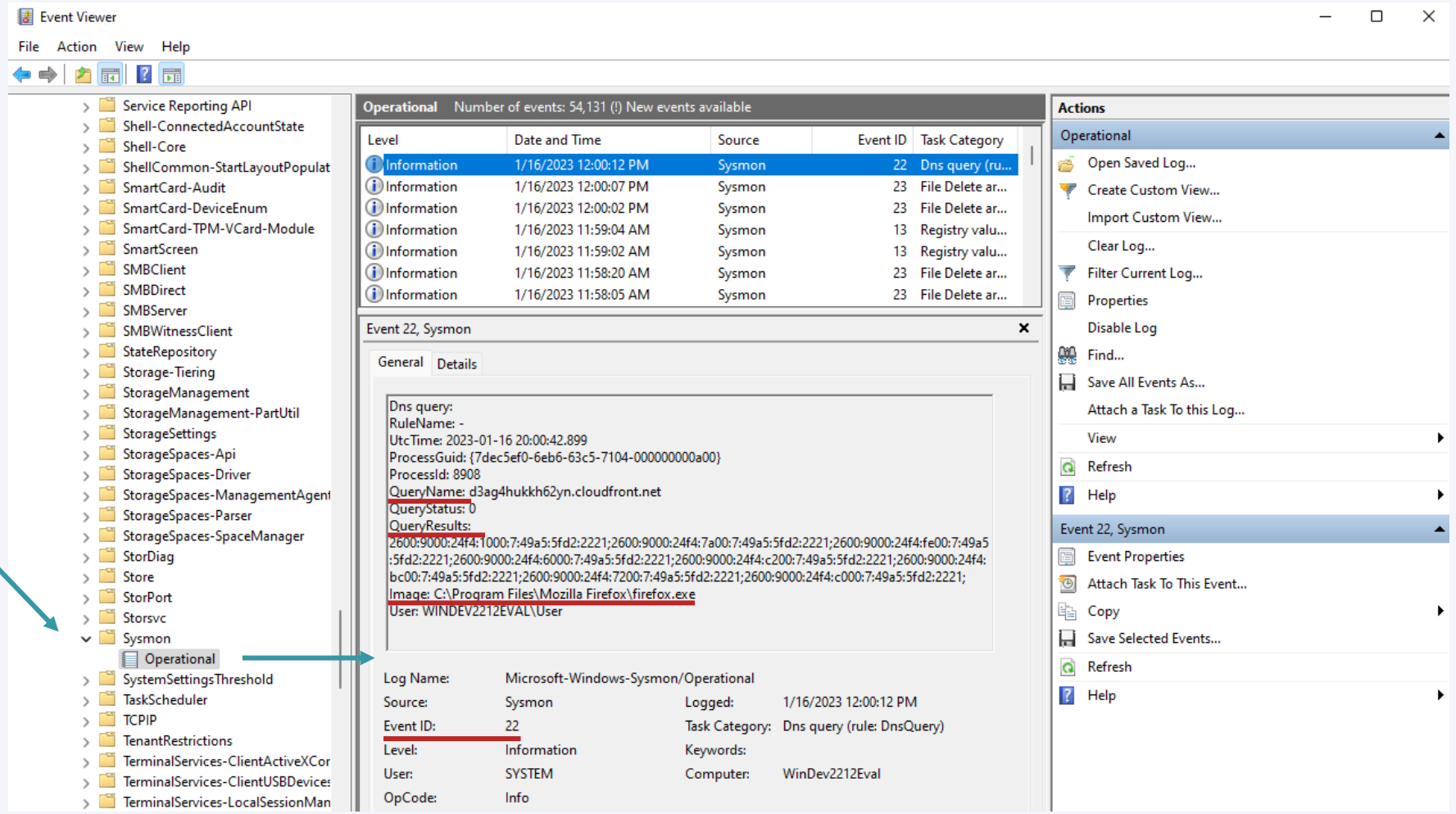


This path ↑

OR

This path ↓





TIDAL

Sigma Rules

github.com/SigmaHQ/sigma

README.md

Python 97.6% Makefile 1.6%
Other 0.8%

Sigma Rule Tests passing

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

1. Sigma rule specification in the Sigma-Specification repository
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules

TIDAL

YAML File

Filename

To keep the file names interoperable use the following:

- Length between 10 and 70 characters
- Lowercase
- No special characters only letters (a-z) and digits (0-9)
- Use `_` instead of a space
- Use `.yml` as a file extension

example:

- lnx_auditd_change_file_time_attr.yml
- web_cve_2022_33891_spark_shell_command_injection.yml
- sysmon_file_block_exe.yml

Data

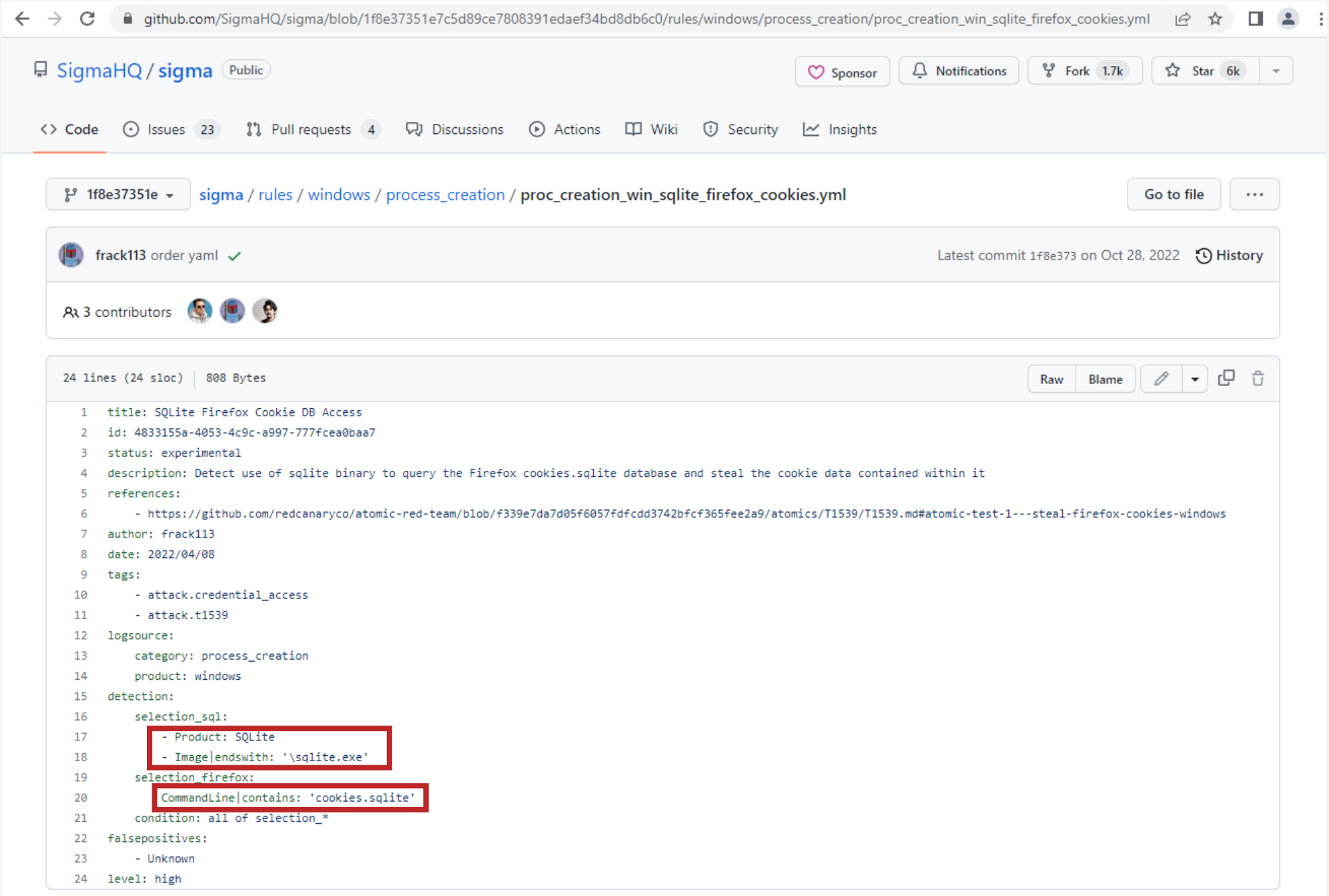
The rule files are written in yaml format
To keep the rules interoperable use the following:

- UTF-8
- LF for the line break (the Windows native editor uses CR-LF)
- Indentation of 4 spaces
- Lowercase keys (e.g. title, id, etc.)
- Single quotes `'` for strings and numeric values don't use any quotes (if the string contains a single quote, double quotes may be used instead)

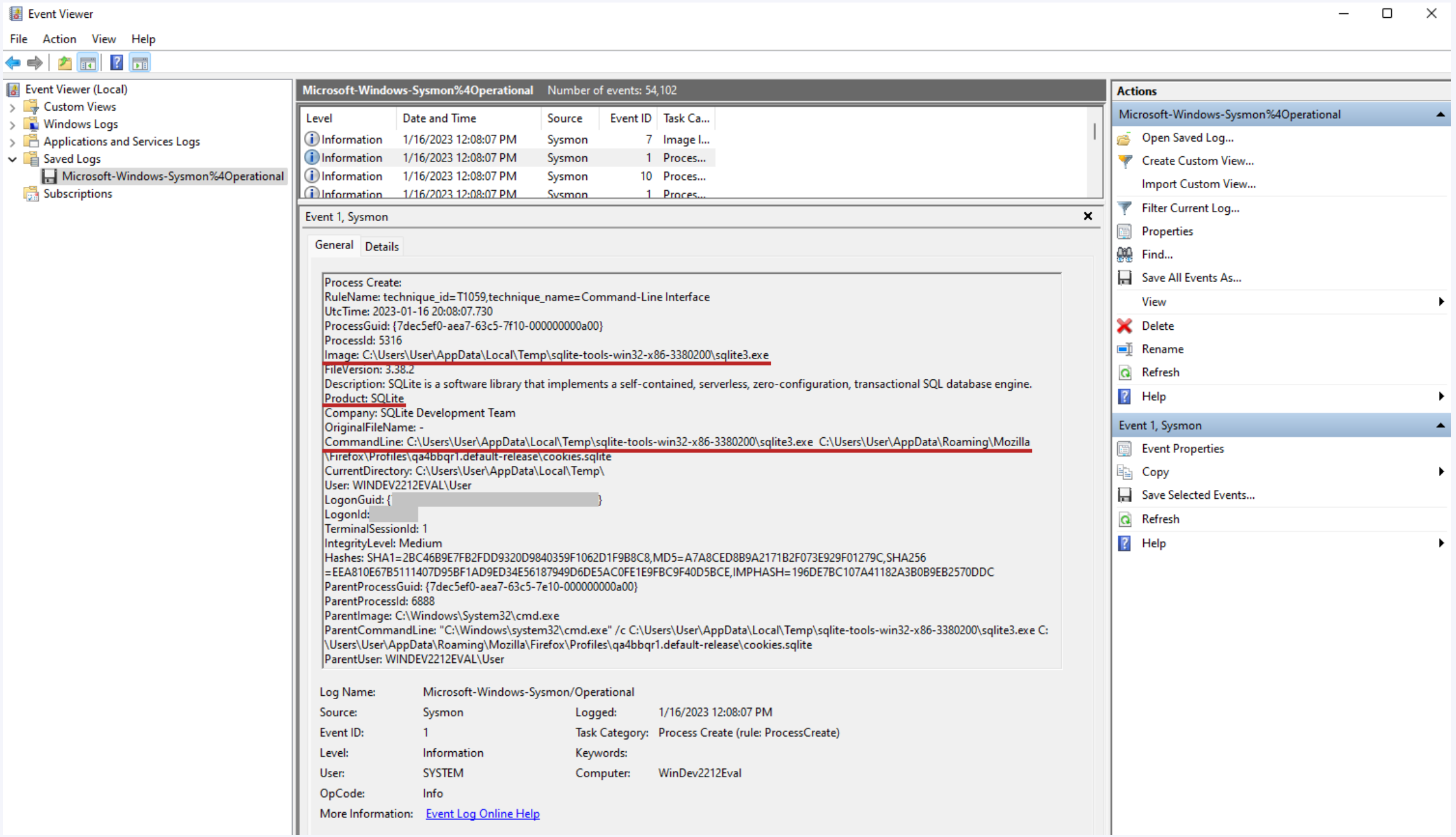
Simple Sigma example

```
title: Whoami Execution
description: Detects a whoami.exe execution
references:
      - https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
author: Florian Roth
date: 2019/10/23
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image: 'C:\Windows\System32\whoami.exe'
    condition: selection
level: high
```

TIDAL



TIDAL



Real results!

TIDAL

#goals

#goals

#goals

Let’s build something new!
With adversary intelligence

#goals

#goals

#goals

TIDAL

github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1539/T1539.md#atomic-test-2---steal-chrome-cookies-windows

128 lines (78 sloc) | 5.44 KB

Raw Blame

Atomic Test #2 - Steal Chrome Cookies (Windows)

This test queries Chrome's SQLite database to steal the encrypted cookie data, designed to function similarly to Zloader/Zbot's cookie theft function. Once an adversary obtains the encrypted cookie info, they could go on to decrypt the encrypted value, potentially allowing for session theft. Note: If Chrome is running, the process will be killed to ensure that the DB file isn't locked. See https://www.malwarebytes.com/resources/files/2020/05/the-silent-night-zloader-zbot_final.pdf.

Supported Platforms: Windows

auto_generated_guid: 26a6b840-4943-4965-8df5-ef1f9a282440

Inputs:

Name	Description	Type	Default Value
cookie_db	Filepath for Chrome cookies database	String	$env:localappdata\Google\Chrome\User Data\Default\Network\Cookies
sqlite3_path	Path to sqlite3	Path	$env:temp\sqlite-tools-win32-x86-3380200\sqlite3.exe
output_file	Filepath to output cookies	Path	$env:temp\T1539ChromeCookies.txt

Attack Commands: Run with `powershell`!

```
stop-process -name "chrome" -force -erroraction silentlycontinue
"select host_key, name, encrypted_value, path, expires_utc, is_secure, is_httponly from [Cookies];" | cmd /c #{sqlite3_path} #{cooki
```

Cleanup Commands:

```
remove-item #{output_file}
```

Dependencies: Run with `powershell`!

Description: Sqlite3 must exist at (#{sqlite3_path})

Check Prereq Commands:

```
if (Test-Path #{sqlite3_path}) {exit 0} else {exit 1}
```

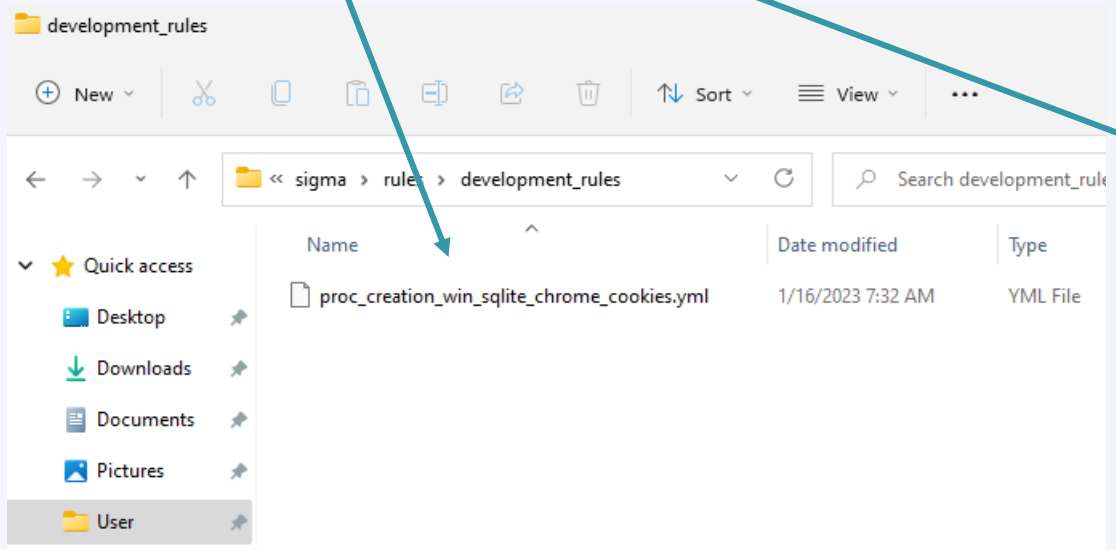
Get Prereq Commands:

```
Invoke-WebRequest "https://www.sqlite.org/2022/sqlite-tools-win32-x86-3380200.zip" -OutFile "$env:temp\sqlite.zip"
```

TIDAL

```
PS C:\Users\User> Invoke-AtomicTest T1539 -TestNumbers 2
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1539-2 Steal Chrome Cookies (Windows)
Done executing test: T1539-2 Steal Chrome Cookies (Windows)
PS C:\Users\User>
```



Microsoft-Windows-Sysmon%4Operational Number of events: 54,073

Level	Date and Time	Source	Event ID	Task Ca...
Information	1/16/2023 12:36:57 PM	Sysmon	1	Proces...
Information	1/16/2023 12:36:57 PM	Sysmon	10	Proces...
Information	1/16/2023 12:36:57 PM	Sysmon	1	Proces...

Event 1, Sysmon

General Details

```
Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime: 2023-01-16 20:36:57.993
ProcessGuid: {7dec5ef0-b569-63c5-c210-000000000a00}
ProcessId: 6856
Image: C:\Users\User\AppData\Local\Temp\sqlite-tools-win32-x86-3380200\sqlite3.exe
FileVersion: 3.38.2
Description: SQLite is a software library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.
Product: SQLite
Company: SQLite Development Team
OriginalFileName: -
CommandLine: C:\Users\User\AppData\Local\Temp\sqlite-tools-win32-x86-3380200\sqlite3.exe  "C:\Users\User\AppData\Local\Google
\Chrome\User Data\Default\Network\Cookies"
CurrentDirectory: C:\Users\User\AppData\Local\Temp\
User: WINDEV2212EVAL\User
LogonGuid:
LogonId:
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=2BC46B9E7FB2FDD9320D9840359F1062D1F9B8C8,MD5=A7A8CED8B9A2171B2F073E929F01279C,SHA256
=EEA810E67B5111407D95BF1AD9ED34E56187949D6DE5AC0FE1E9FBC9F40D5BCE,IMPHASH=196DE7BC107A41182A3B0B9EB2570DDC
ParentProcessGuid: {7dec5ef0-b569-63c5-c110-000000000a00}
ParentProcessId: 2900
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe" /c C:\Users\User\AppData\Local\Temp\sqlite-tools-win32-x86-3380200\sqlite3.exe "C:
\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies"
ParentUser: WINDEV2212EVAL\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	1/16/2023 12:36:57 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WinDev2212Eval
OpCode:	Info		
More Information:	Event Log Online Help		

TIDAL

proc_creation_win_sqlite_chrome_cookies.yml

```yaml
title: SQLite Chrome Cookie DB Access
id: 24c77512-782b-448a-8950-eddb0785fc71
status: experimental
description: Detect use of sqlite binary to query the Chrome Cookies database and steal the cookie data contair
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T15
author: TropChaud
date: 2022/12/19
tags:
    - attack.credential_access
    - attack.t1539
logsource:
    category: process_creation
    product: windows
detection:
    selection_sql:
        - Product: SQLite
        - Image|endswith:
            - '\sqlite.exe'
            - '\sqlite3.exe'
    selection_chrome:
        CommandLine|contains:
            - '\Google\Chrome\User Data\Default\Network\Cookies' # Latest chrome versions
            - '\Google\Chrome\User Data\Default\Cookies' # Older chrome versions
    condition: all of selection_*
falsepositives:
    - Unknown
level: high
```

TIDAL

Real-Time, Straightforward Detection With Chainsaw

github.com/withsecurelabs/chainsaw

WithSecureLabs / chainsaw Public

Notifications | Fork 163 | Star 1.8k

Code | Issues 3 | Pull requests | Discussions | Actions | Projects | Wiki | Security | Insights

master | 7 branches | 29 tags | Go to file | Code

fscc-alexkornitzer fix: broken tests due to new fields being brought in 202148c 3 days ago 230 commits

.github/workflows	chore: updating runner to create zip	6 months ago
images	docs: building out README and help output for v2 release	6 months ago
mappings	tweak: update todo message in mft mapping	4 months ago
rules	chore: update severity levels for chainsaw rules	6 months ago
src	fix: don't panic on an invalid tau key value pair	3 days ago
tests	fix: broken tests due to new fields being brought in	3 days ago
.gitignore	chore: updating .gitignore file and adding Alex Kornitzer to Cargo to...	last year
.gitmodules	Initial public commit	last year
Cargo.lock	build: bump to version 2.3.1	3 days ago
Cargo.toml	build: bump to version 2.3.1	3 days ago
LICENCE	Initial public commit	last year
README.md	docs: cleaning readme and examples	3 months ago

README.md

Rapidly Search and Hunt through Windows Forensic Artefacts

About

Rapidly Search and Hunt through Windows Forensic Artefacts

windows | rust | security | attack | detection | logs | forensics | dfir | threat-hunting | sigma | blueteam | chainsaw | countercept

Readme

GPL-3.0 license

1.8k stars

41 watching

163 forks

Releases 28

v2.3.1 Latest

3 days ago

+ 27 releases

Packages

No packages published

Used by 104

+ 96

Contributors 7

TIDAL

CHAINSAW

By Countercept (@FranticTyping, @AlexKornitzer)

github.com/WithSecureLabs/chainsaw/wiki

Product Solutions Open Source Pricing Search Sign in Sign up

WithSecureLabs / chainsaw Public

Notifications Fork 163 Star 1.8k

Code Issues 3 Pull requests Discussions Actions Projects Wiki Security Insights

Home

James D edited this page on Jul 6, 2022 · 2 revisions

Welcome to the Chainsaw Wiki!

Chainsaw provides a powerful 'first-response' capability to quickly identify threats within Windows event logs. It offers a generic and fast method of searching through event logs for keywords, and by identifying threats using built-in support for Sigma detection rules, and via custom Chainsaw detection rules.

Features

- 🎯 Hunt for threats using Sigma detection rules and custom Chainsaw detection rules
- 🔍 Search and extract event log records by string matching, and regex patterns
- ⚡ Lightning fast, written in rust, wrapping the EVTX parser library by @OBenamram
- 🪶 Clean and lightweight execution and output formats without unnecessary bloat
- 🔥 Document tagging (detection logic matching) provided by the TAU Engine Library
- 📄 Output results in a variety of formats, such as ASCII table format, CSV format, and JSON format
- 💻 Can be run on MacOS, Linux and Windows

Pages 3

Chainsaw Wiki

Overview

- Why Chainsaw?
- How Does Chainsaw Work?
- Sigma Rule Support

Usage

- Quick Start
- Searching
- Hunting
- Output Options

Chainsaw Rules

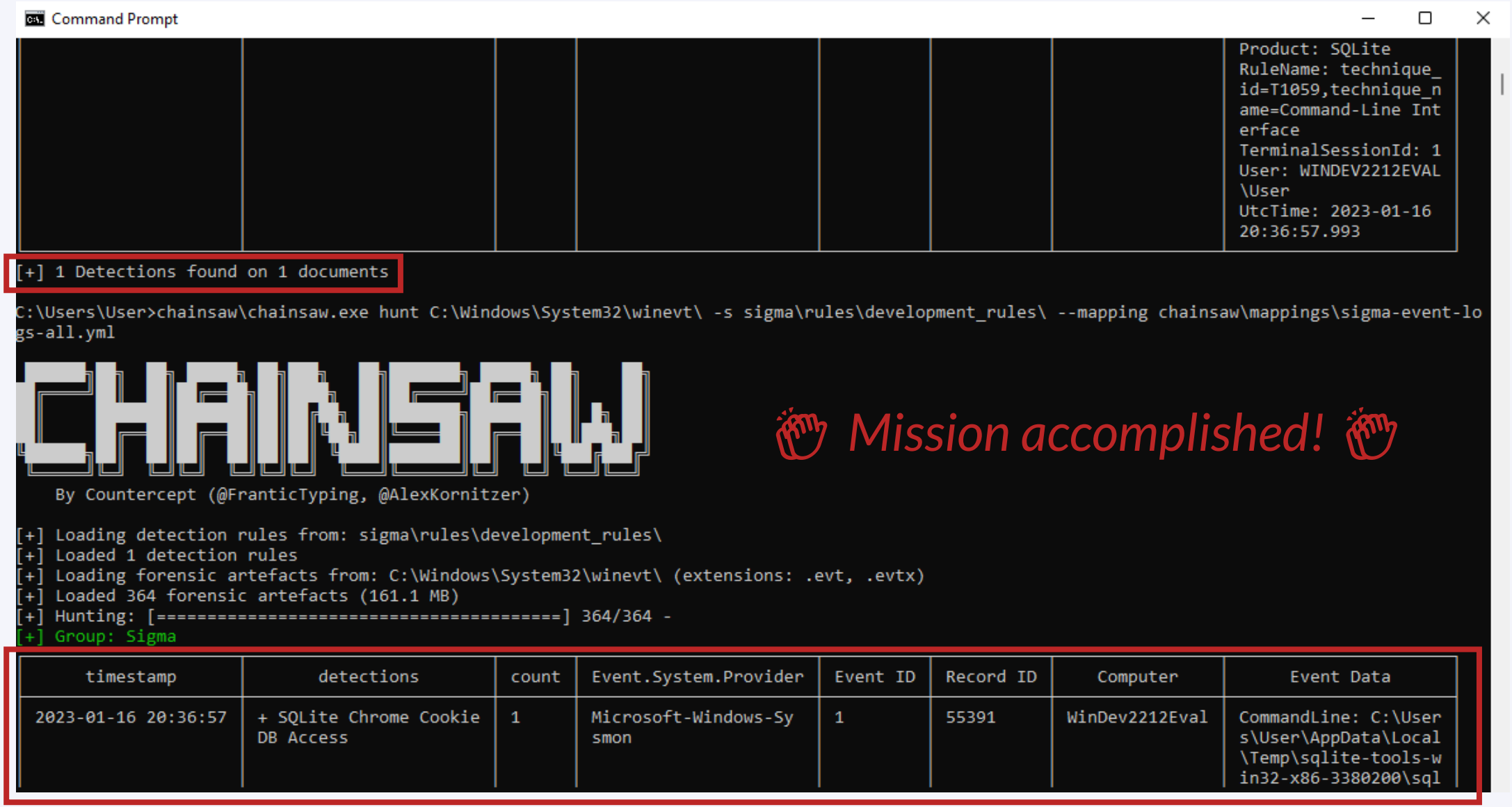
Contributing

- Supporting Additional Rules

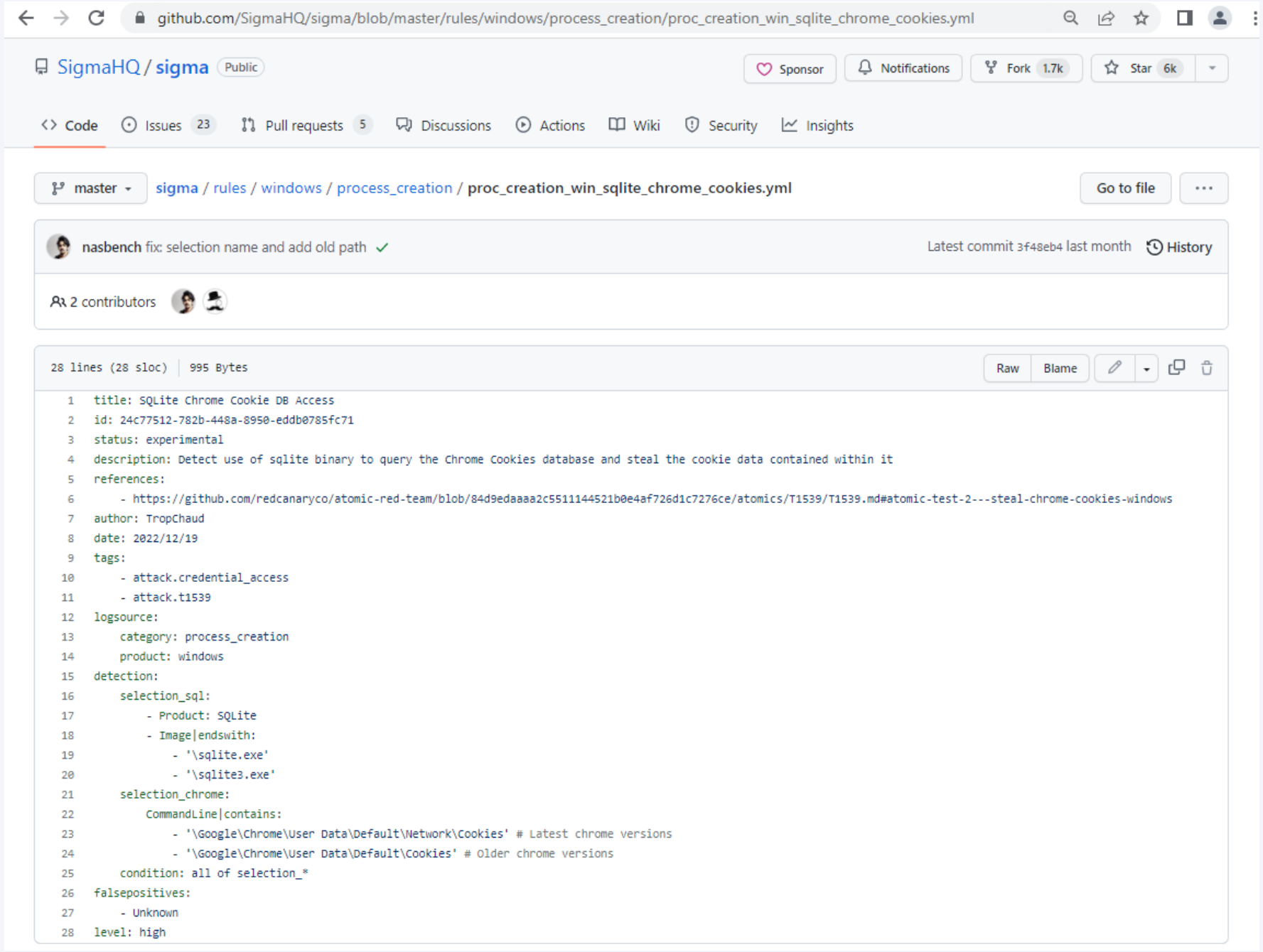
Clone this wiki locally

https://github.com/WithSecureLabs/

TIDAL



TIDAL



TIDAL

Example 2: Emulating & Detecting (Instances of) a Top CTI Technique

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1539	Steal Web Session Cookie	Credential Access	20	2	2	2
T1555.003	Credentials from Web Browsers	Credential Access	19	4	3	16
T1082	System Information Discovery	Discovery	16	4	14	24
T1027	Obfuscated Files or Information	Defense Evasion	15	4	84	8
T1113	Screen Capture	Collection	14	2	6	6
T1518	Software Discovery	Discovery	14	5	2	6
T1041	Exfiltration Over C2 Channel	Exfiltration	13	5	3	1
T1083	File and Directory Discovery	Discovery	12	3	17	6
T1057	Process Discovery	Discovery	11	3	5	5
T1204	User Execution	Execution	11	11	8	0
T1528	Steal Application Access Token	Credential Access	10	1	10	1
T1614	System Location Discovery	Discovery	9	4	0	0
T1012	Query Registry	Discovery	8	4	10	2
T1218.011	Rundll32	Defense Evasion	1	4	32	13

TIDAL

SEKOIA.IO | Blog

To fingerprint the host, Aurora executes three commands on the infected host:

- `wmic os get Caption`
- `wmic path win32_VideoController get name`
- `wmic cpu get name`

Atomic Test #25 - System Information Discovery with WMIC

Identify system information with the WMI command-line (WMIC) utility. Upon execution, various system information will be displayed, including: OS, CPU, GPU, and disk drive names; memory capacity; display resolution; and baseboard, BIOS, and GPU driver products/versions. https://nwgat.ninja/getting-system-information-with-wmic-on-windows/ Elements of this test were observed in the wild used by Aurora Stealer in late 2022 and early 2023, as highlighted in public reporting: https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar https://blog.cyble.com/2023/01/18/aurora-a-stealer-using-shapeshifting-tactics/

Supported Platforms: Windows

auto_generated_guid: 8851b73a-3624-4bf7-8704-aa312411565c

Attack Commands: Run with `command_prompt`!

```
wmic cpu get name
wmic MEMPHYSICAL get MaxCapacity
wmic baseboard get product
wmic baseboard get version
wmic bios get SMBIOSBIOSVersion
wmic path win32_VideoController get name
wmic path win32_VideoController get DriverVersion
wmic path win32_VideoController get VideoModeDescription
wmic OS get Caption,OSArchitecture,Version
wmic DISKDRIVE get Caption
```

New test driven by CTI!

Invoke-AtomicRedTeam wiki:
https://github.com/redcanaryco/invoke-atomicredteam/wiki

```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -TestNumbers 25
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1082-25 System Information Discovery with WMIC
Name
12th Gen Intel(R) Core(TM) i7-12700H
Product
VirtualBox
Version
1.2
SMBIOSBIOSVersion
VirtualBox
Name
VirtualBox Graphics Adapter (WDDM)
DriverVersion
6.1.40.4048
VideoModeDescription
1920 x 1065 x 4294967296 colors
Caption                                  OSArchitecture  Version
Microsoft Windows 11 Enterprise Evaluation  64-bit          10.0.22000
Caption
VBOX HARDDISK
No Instance(s) Available.
Done executing test: T1082-25 System Information Discovery with WMIC
PS C:\Windows\system32>
```

```
01:36:55.680

[+] 20 Detections found on 20 documents

C:\Users\User>chainsaw\chainsaw.exe hunt C:\Windows\System32\winevt\ -s sigma\rules\target_tests\ --mapping chainsaw\mappings\sigma-event-logs-all.yml

CHAINSAW
    By Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: sigma\rules\target_tests\
[+] Loaded 1 detection rules
[+] Loading forensic artefacts from: C:\Windows\System32\winevt\ (extensions: .evtx, .evt)
[+] Loaded 370 forensic artefacts (116.2 MB)
[+] Hunting: [========================================] 370/370 -
[+] Group: Sigma
```

timestamp	detections	count	Event.System.Provider	Event ID	Recor
2023-04-30 18:12:22	+ Potential System Information Discovery Via Wmic.EXE	1	Microsoft-Windows-Sysmon	1	20402

```
Description: WMI Commandline U
tility
FileVersion: 10.0.22621.1 (Win
Build.160101.0800)
Hashes: SHA1=CC3C648E9265A68A7
E6032076E44413CDD1B10F9,MD5=35
3D78C55DA2BC6D95F00C923D0CD0A4
,SHA256=993A2E38A27807096F75E8
```

SIGMA

Example 3: Spotting an Outlier Technique

Technique Preview

Rundll32

VIEW DETAILS

ID: T1218.011
Tactic(s): Defense Evasion
Platform(s): Windows
Parent-Technique: System Binary Proxy Execution

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: `rundll32.exe {DLLname, DLLfunction}`)....

20	59
Groups	Software
4	32
Data Sources	Analytics

Vendors

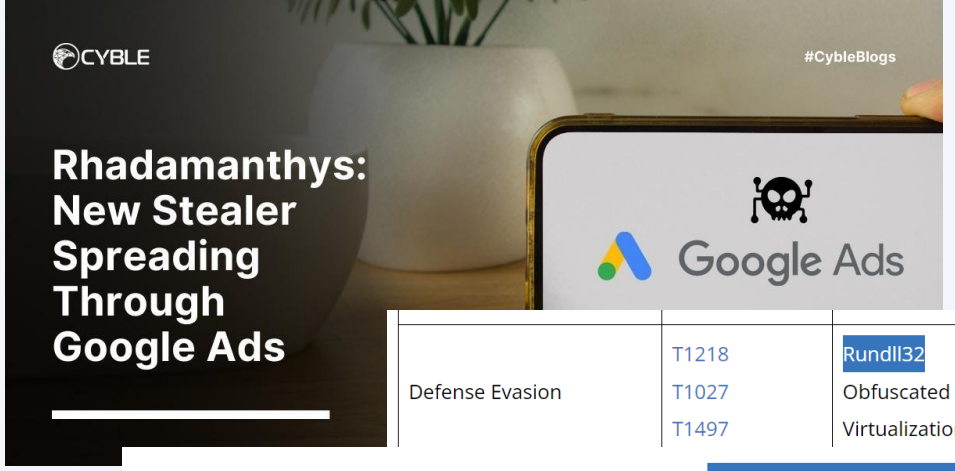
Filter By : Test | Detect | Protect

Atomic Red Team | AttackIQ | Cybereason | Elastic | FourCore | IBM Security | Olaf Hartong | Saf

Labels

Filter By : All(1) | Technique Set(1)

Rhadamant...



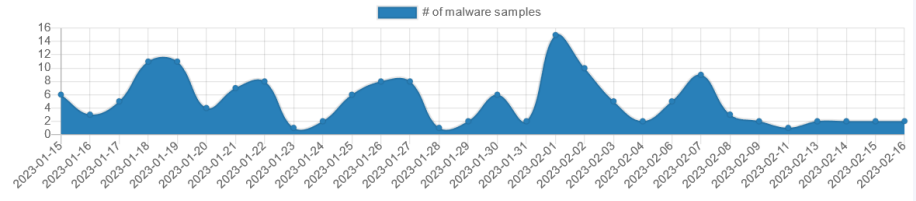
Defense Evasion	T1218	Rundll32
	T1027	Obfuscated Files or Information
	T1497	Virtualization/Sandbox Evasion

After the check, the shellcode further drops a DLL file named "nsis_unsibcfb0.dll" in the *%temp%* folder and launches it using the "rundll32.exe" with specific parameters shown in the figure below.

Widely used, but not by these recent stealers

MALWARE bazaar by ABUSE.CH | Browse | Upload | Hunting | API | Export | Statistics | FAQ | About | Login

Tag:	Rhadamanthys Alert
Firstseen:	2022-12-27 09:11:04 UTC
Lastseen:	2023-02-16 08:40:03 UTC
Sightings:	168



github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_malware_rhadamanthys_steal...yml

SigmaHQ / sigma Public | Sponsor | Fork 1.8k | Star 6.1k

Code | Issues 22 | Pull requests 7 | Discussions | Actions | Wiki | Security | Insights

master | sigma / rules / windows / process_creation / proc_creation_win_malware_rhadamanthys_stealer...yml | Go to file

nasbench feat: more fixes and updates | Latest commit 68f0833 2 weeks ago | History

1 contributor

30 lines (30 sloc) | 1.12 KB | Raw | Blame

```
title: Rhadamanthys Stealer Module Launch Via Rundll32.EXE
id: 5cdbc2e8-86dd-43df-9a1a-200d4745fba5
status: experimental
description: Detects the use of Rundll32 to launch an NSIS module that serves as the main stealer capability of Rhadamanthys infostealer, as observed in reports and samples in
references:
    - https://elis531989.medium.com/dancing-with-shellcodes-analyzing-rhadamanthys-stealer-3c4986966a88
    - https://blog.cyble.com/2023/01/12/rhadamanthys-new-stealer-spreading-through-google-ads/
    - https://www.joesandbox.com/analysis/790122/0/html
    - https://twitter.com/anfam17/status/1607477672057208835
author: TropChaud
date: 2023/01/26
modified: 2023/02/05
tags:
    - attack.defense_evasion
    - attack.t1218.011
logsource:
    category: process_creation
    product: windows
detection:
    selection_rundll32:
        - OriginalFileName: 'RUNDLL32.EXE'
        - Image|endswith: '\rundll32.exe'
    selection_dll:
        CommandLine|contains: 'nsis_uns'
    selection_export_function:
        CommandLine|contains: 'PrintUIEntry'
    condition: all of selection_*
falsepositives:
    - Unknown
```

SIGMA

TIDAL

Thank You!

- Huge thanks to the **Atomic Red Team** & **Sigma repository** maintainers, and OSS tool (**Chainsaw**) producers/contributors!
- Tidal Community Edition: app.tidalcyber.com
- Tidal Blog: tidalcyber.com/blog
- Engage with Us!
  - **Tidal Community Slack** (reach out for a current link)
  - **LinkedIn**: Tidal Cyber / Scott Small
  - **Mastodon**: infosec.exchange/@tidalcyber / infosec.exchange/@IntelScott
  - **Twitter**: @TidalCyber / @IntelScott
  - **Reddit**: u/TropChaud (Scott)
  - **Email**: contact@tidalcyber.com / scott.small@tidalcyber.com

TIDAL