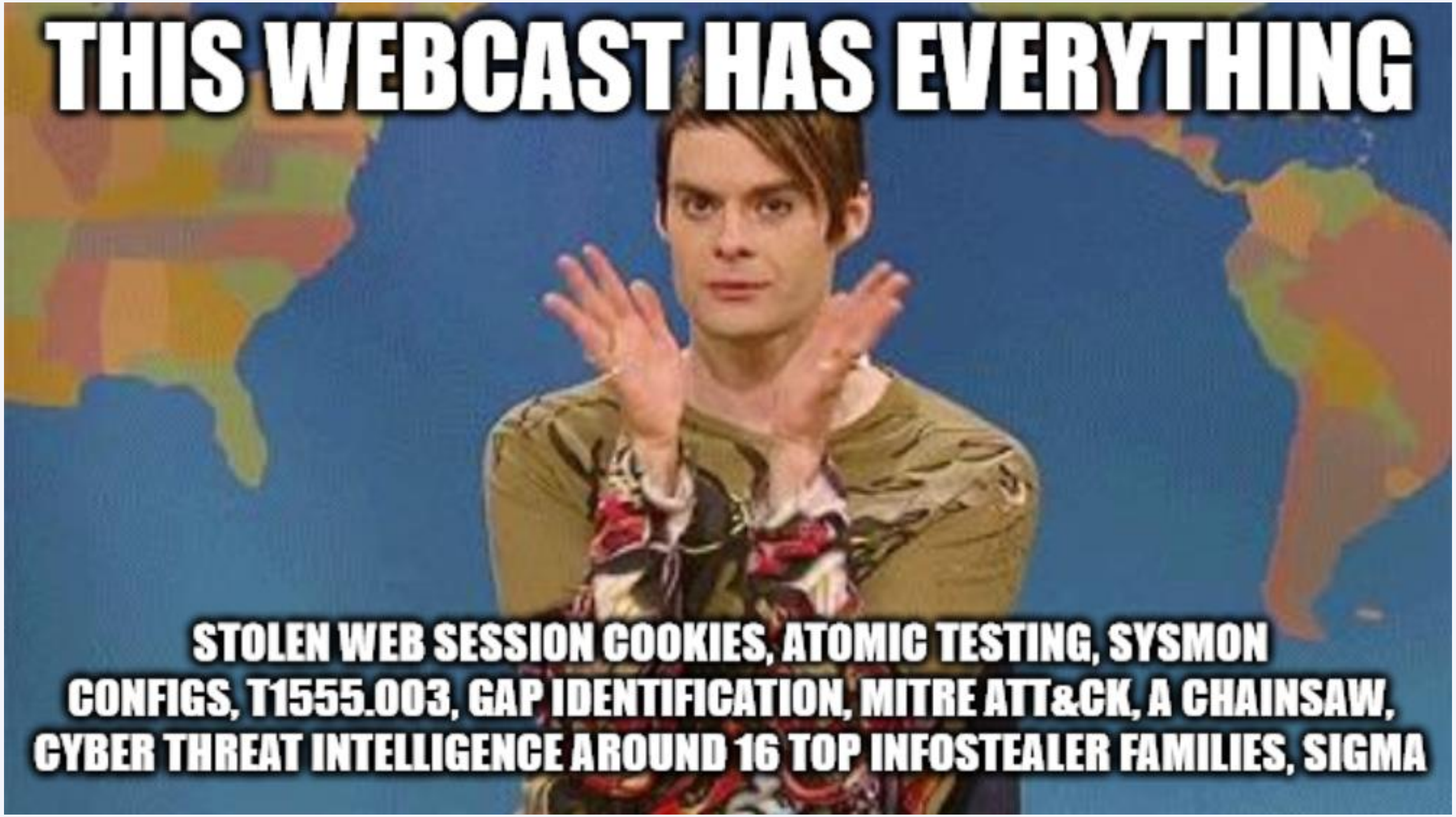
Stealer, No Stealing!
A Practical Guide to Building & Validating Detections With Adversary Intelligence

Adversary Village: Adversary Guru Series

January 17, 2023

Scott Small, Director of Cyber Threat Intelligence

TIDAL


THIS WEBCAST HAS EVERYTHING
STOLEN WEB SESSION COOKIES, ATOMIC TESTING, SYSMON CONFIGS, T1555.003, GAP IDENTIFICATION, MITRE ATT&CK, A CHAINSAW, CYBER THREAT INTELLIGENCE AROUND 16 TOP INFOSTEALER FAMILIES, SIGMA

whoami

Intelligence researcher & analyst, purple teamer, passionate about data viz

Expanding my "technical" skills through practical applications: Python, Javascript, MITRE ATT&CK, detection validation (Atomics + Sigma)

Addicted to sharing original cyber threat content:

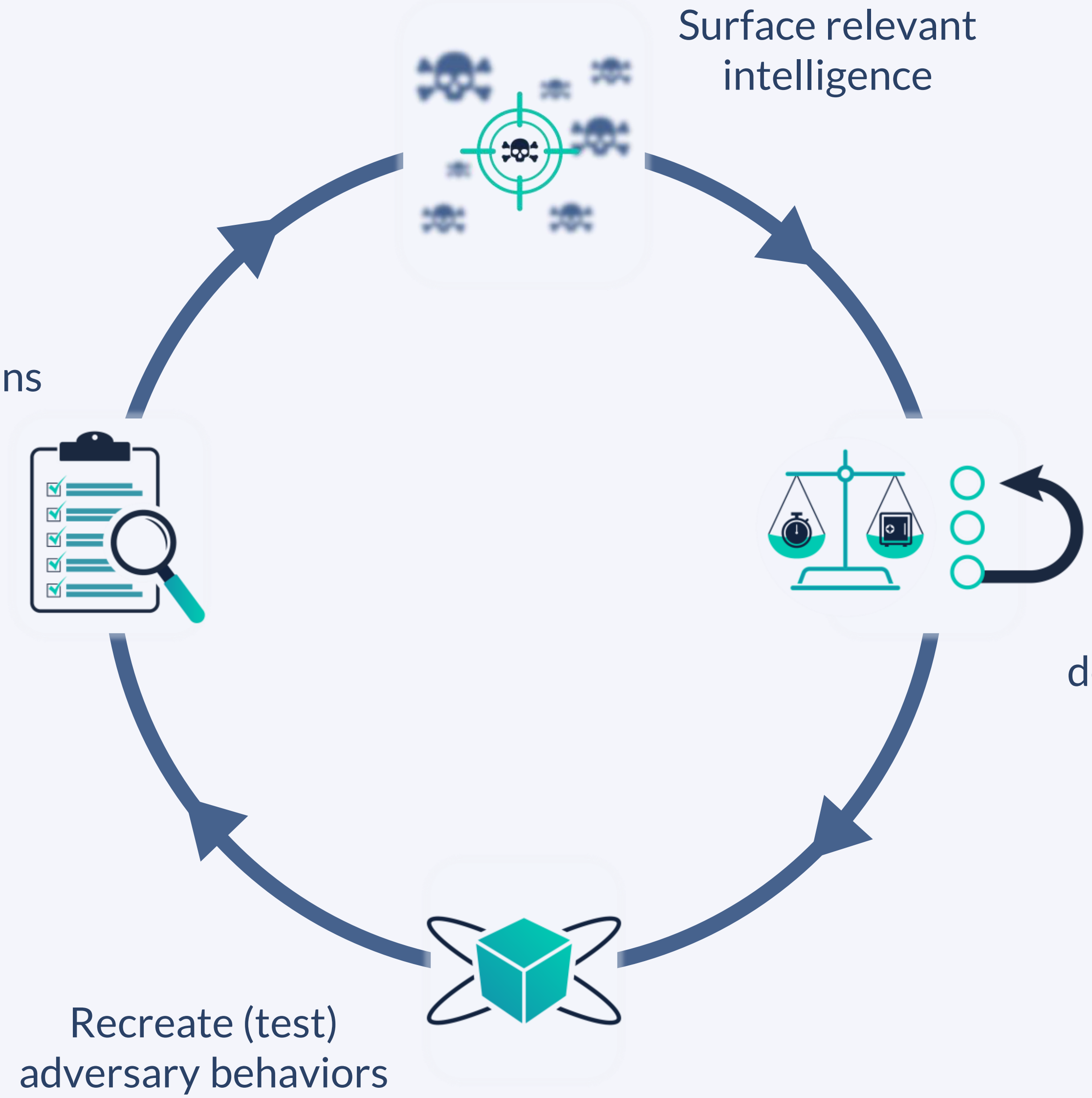
- LinkedIn, Mastodon, Twitter, Reddit
- github.com/TropChaud
- brighttalk.com/channel/19703/

Cyber Threat Intelligence Director @ Tidal Cyber

Troubleshooting extended displays, or evading defenses deep in a target environment?

(Optimistic) Agenda

Threat-Informed Detection Validation (Micro Purple Teaming)

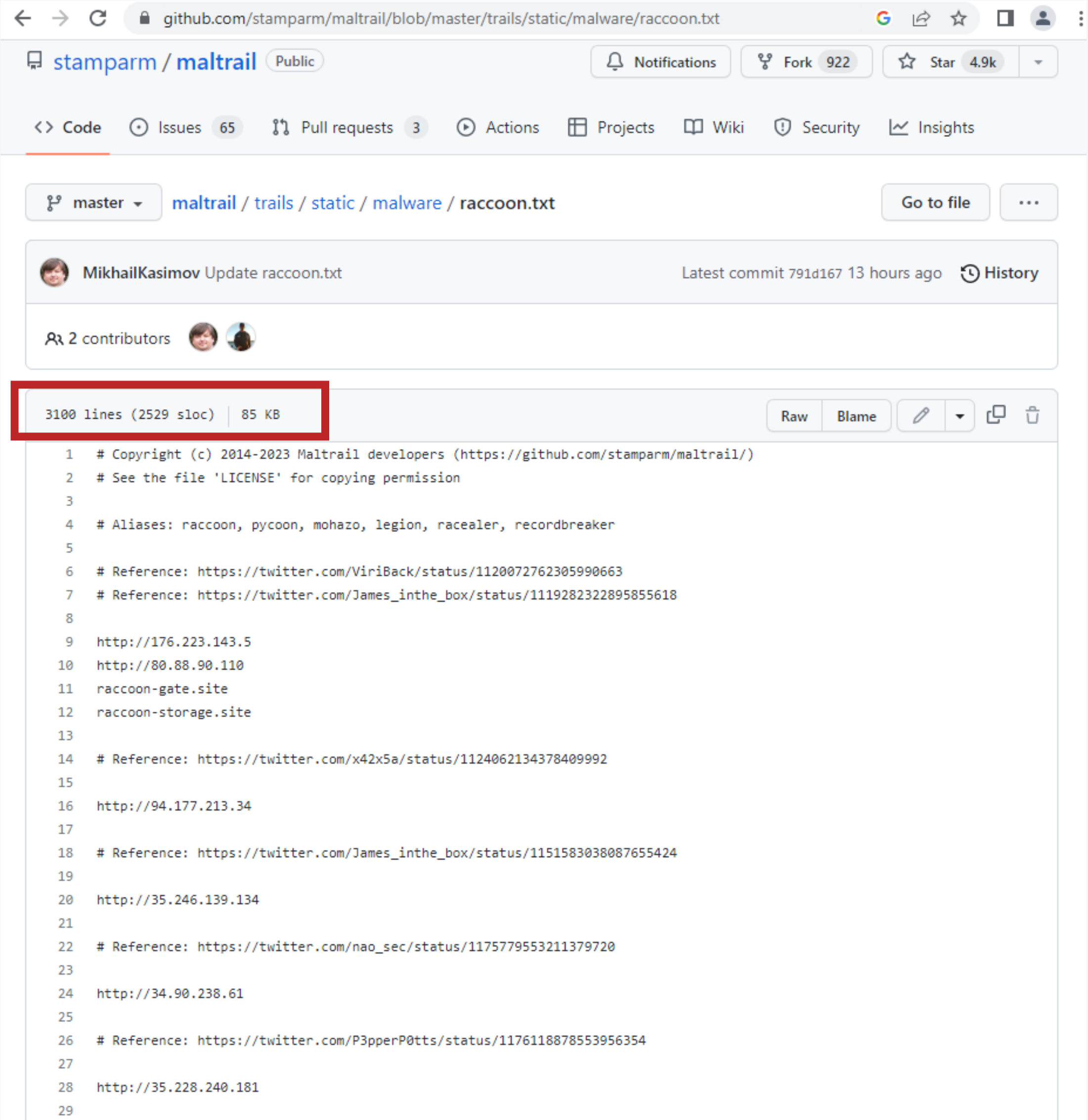

Surface relevant intelligence
Identify gaps & determine priorities
Recreate (test) adversary behaviors
Validate detections & re-test

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

TIDAL

The Value of TTP Intelligence

IOCs


github.com/stamparm/maltrail/blob/master/trails/static/malware/raccoon.txt
stamparm / maltrail Public
Notifications
Fork 922
Star 4.9k
Code
Issues 65
Pull requests 3
Actions
Projects
Wiki
Security
Insights
master
maltrail / trails / static / malware / raccoon.txt
Go to file
MikhailKasimov Update raccoon.txt
Latest commit 791d167 13 hours ago
History
2 contributors
Raw
Blame

3100 lines (2529 sloc) | 85 KB

```
# Copyright (c) 2014-2023 Maltrail developers (https://github.com/stamparm/maltrail/)
# See the file 'LICENSE' for copying permission

# Aliases: raccoon, pycoon, mohazo, legion, racealer, recordbreaker

# Reference: https://twitter.com/ViriBack/status/1120072762305990663
# Reference: https://twitter.com/James_inthe_box/status/1119282322895855618

http://176.223.143.5
http://80.88.90.110
raccoon-gate.site
raccoon-storage.site

# Reference: https://twitter.com/x42x5a/status/1124062134378409992

http://94.177.213.34

# Reference: https://twitter.com/James_inthe_box/status/1151583038087655424

http://35.246.139.134

# Reference: https://twitter.com/nao_sec/status/1175779553211379720

http://34.90.238.61

# Reference: https://twitter.com/P3pperP0tts/status/1176118878553956354

http://35.228.240.181

```

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

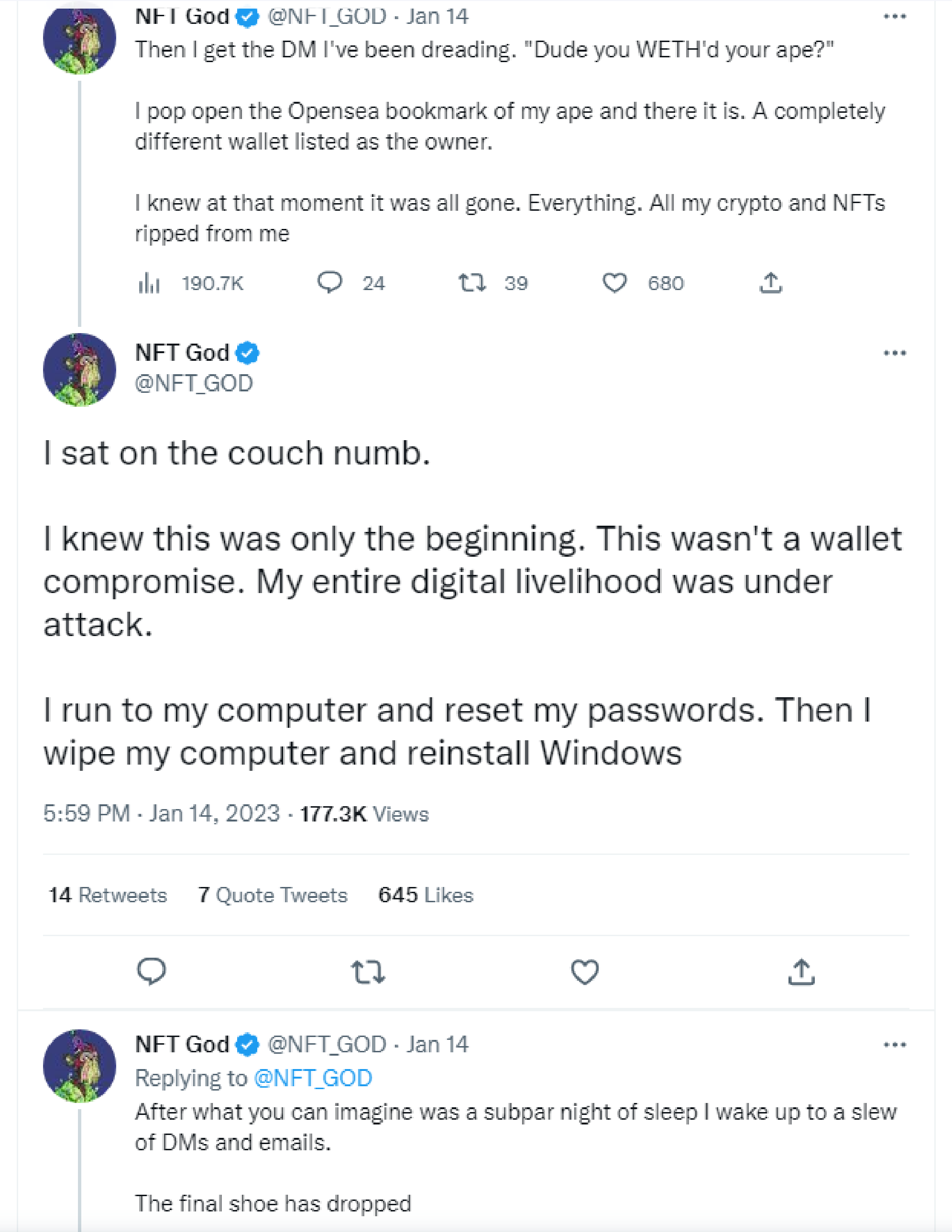
TIDAL

CTI Tools

Applying Cyber Threat Intelligence for Defensive Gap Identification

TIDAL

THREAT-INFORMED DEFENSE



NFT God @NFT_GOD · Jan 14

Then I get the DM I've been dreading. "Dude you WETH'd your ape?"

I pop open the Opensea bookmark of my ape and there it is. A completely different wallet listed as the owner.

I knew at that moment it was all gone. Everything. All my crypto and NFTs ripped from me

190.7K 24 39 680

NFT God
@NFT_GOD

I sat on the couch numb.

I knew this was only the beginning. This wasn't a wallet compromise. My entire digital livelihood was under attack.

I run to my computer and reset my passwords. Then I wipe my computer and reinstall Windows

5:59 PM · Jan 14, 2023 · **177.3K** Views

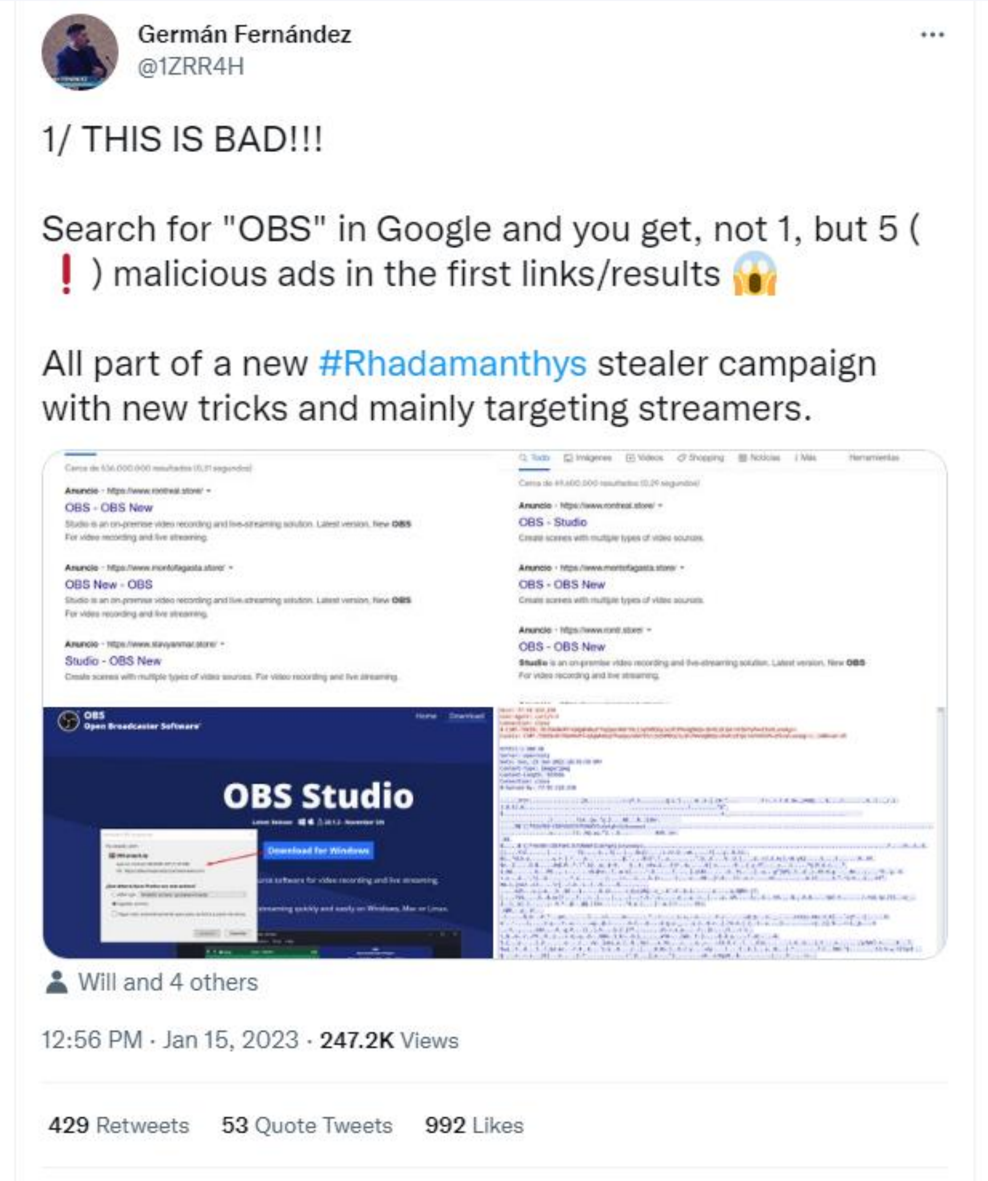
14 Retweets **7** Quote Tweets **645** Likes

NFT God @NFT_GOD · Jan 14

Replying to @NFT_GOD

After what you can imagine was a subpar night of sleep I wake up to a slew of DMs and emails.

The final shoe has dropped



Germán Fernández
@1ZRR4H

1/ THIS IS BAD!!!

Search for "OBS" in Google and you get, not 1, but 5 (❗) malicious ads in the first links/results 😱

All part of a new #Rhadamanthys stealer campaign with new tricks and mainly targeting streamers.

Will and 4 others

12:56 PM · Jan 15, 2023 · **247.2K** Views

429 Retweets **53** Quote Tweets **992** Likes

TIDAL

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 X Increased Opportunity X Increased Capability = Increased Threat

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

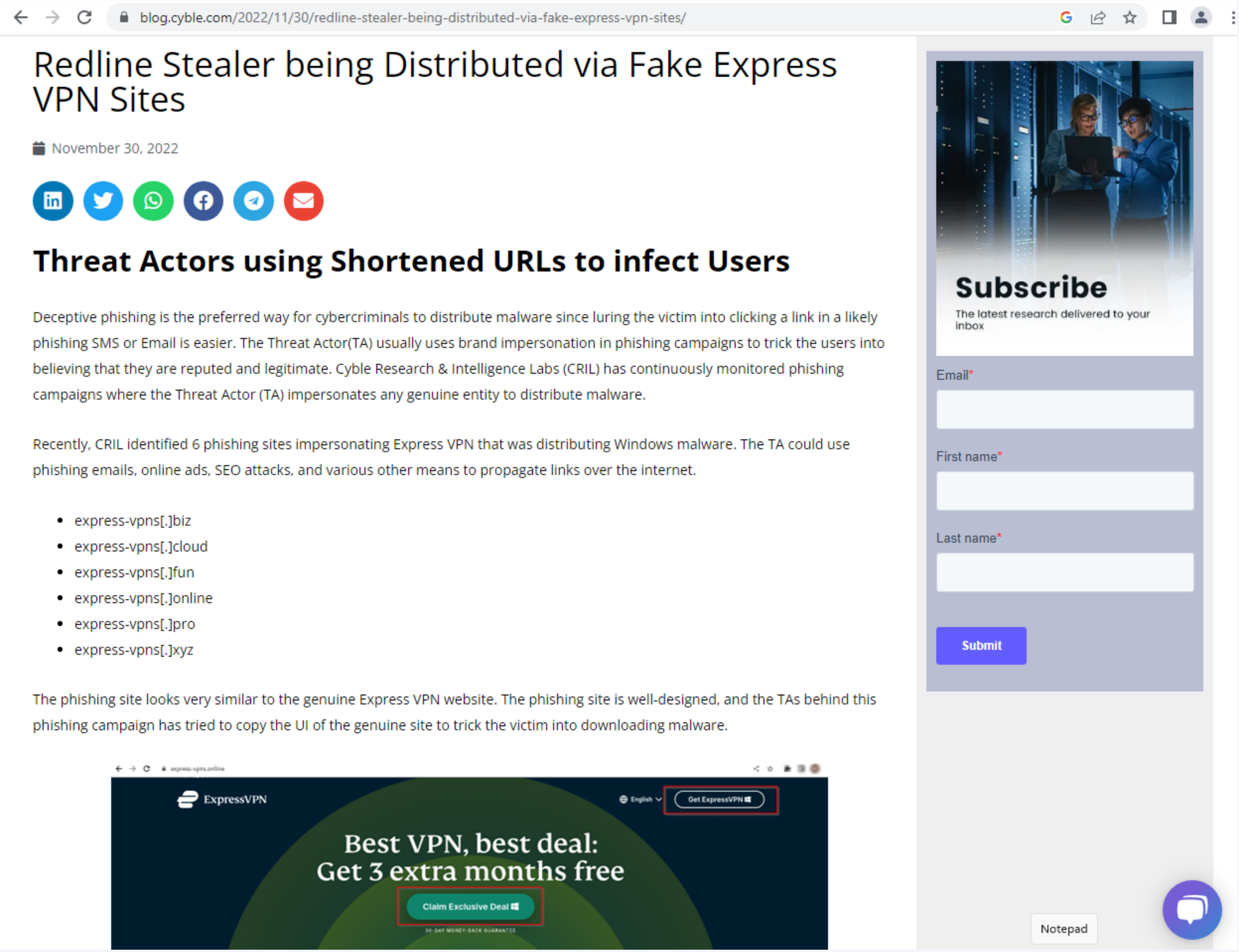
Increased evasion of advanced/enterprise security tools

=

Increased Threat

TIDAL

Recent CTI: https://blog.cyble.com/2022/11/30/redline-stealer-being-distributed-via-fake-express-vpn-sites/



Redline Stealer being Distributed via Fake Express VPN Sites

November 30, 2022

Threat Actors using Shortened URLs to infect Users

Deceptive phishing is the preferred way for cybercriminals to distribute malware since luring the victim into clicking a link in a likely phishing SMS or Email is easier. The Threat Actor(TA) usually uses brand impersonation in phishing campaigns to trick the users into believing that they are reputed and legitimate. Cyble Research & Intelligence Labs (CRIL) has continuously monitored phishing campaigns where the Threat Actor (TA) impersonates any genuine entity to distribute malware.

Recently, CRIL identified 6 phishing sites impersonating Express VPN that was distributing Windows malware. The TA could use phishing emails, online ads, SEO attacks, and various other means to propagate links over the internet.

- express-vpns[.]biz
- express-vpns[.]cloud
- express-vpns[.]fun
- express-vpns[.]online
- express-vpns[.]pro
- express-vpns[.]xyz

The phishing site looks very similar to the genuine Express VPN website. The phishing site is well-designed, and the TAs behind this phishing campaign has tried to copy the UI of the genuine site to trick the victim into downloading malware.

Subscribe

The latest research delivered to your inbox

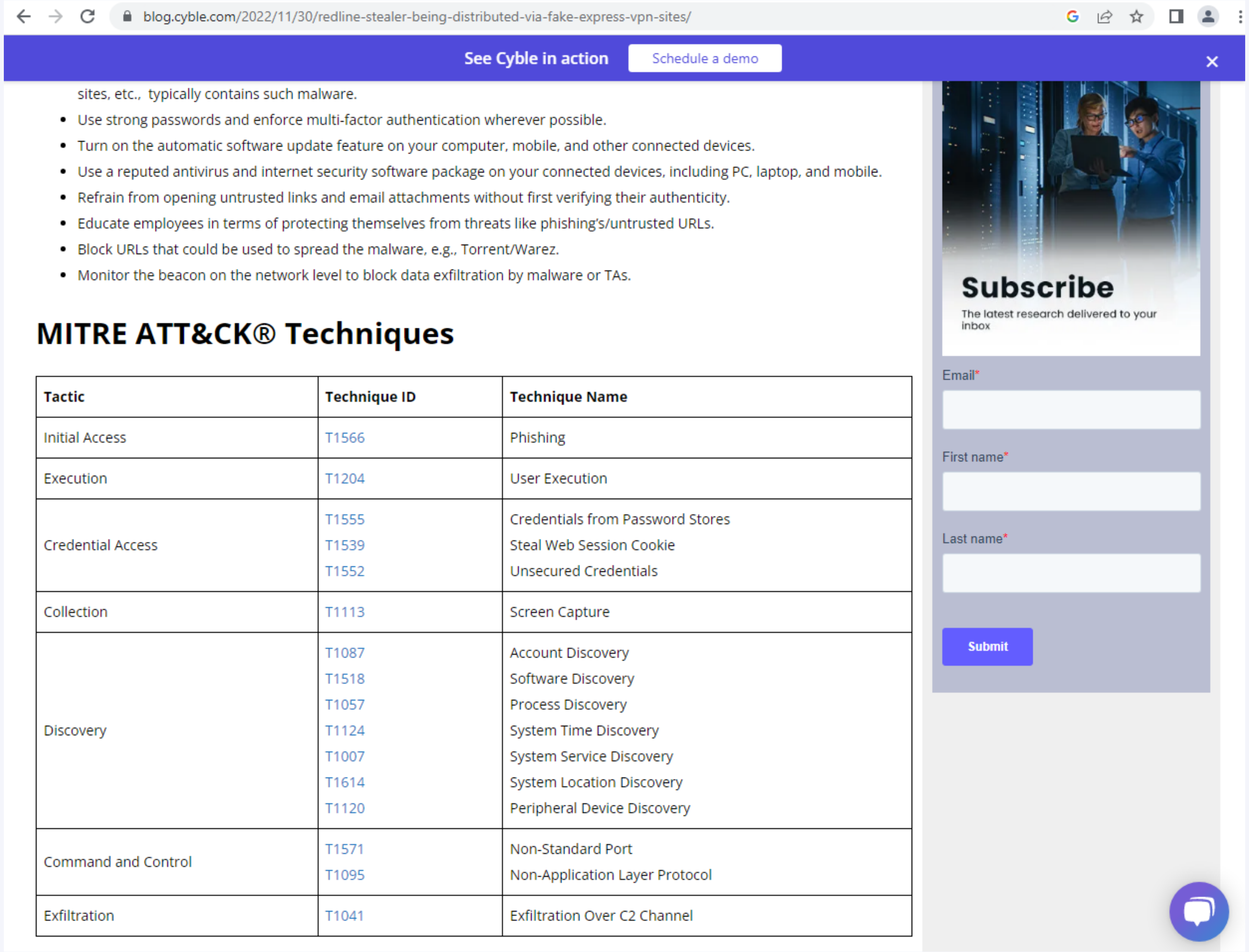
Email*

First name*

Last name*

Submit

Recent CTI: https://blog.cyble.com/2022/11/30/redline-stealer-being-distributed-via-fake-express-vpn-sites/


blog.cyble.com/2022/11/30/redline-stealer-being-distributed-via-fake-express-vpn-sites/
See Cyble in action
Schedule a demo
Subscribe
The latest research delivered to your inbox
Email*
First name*
Last name*
Submit

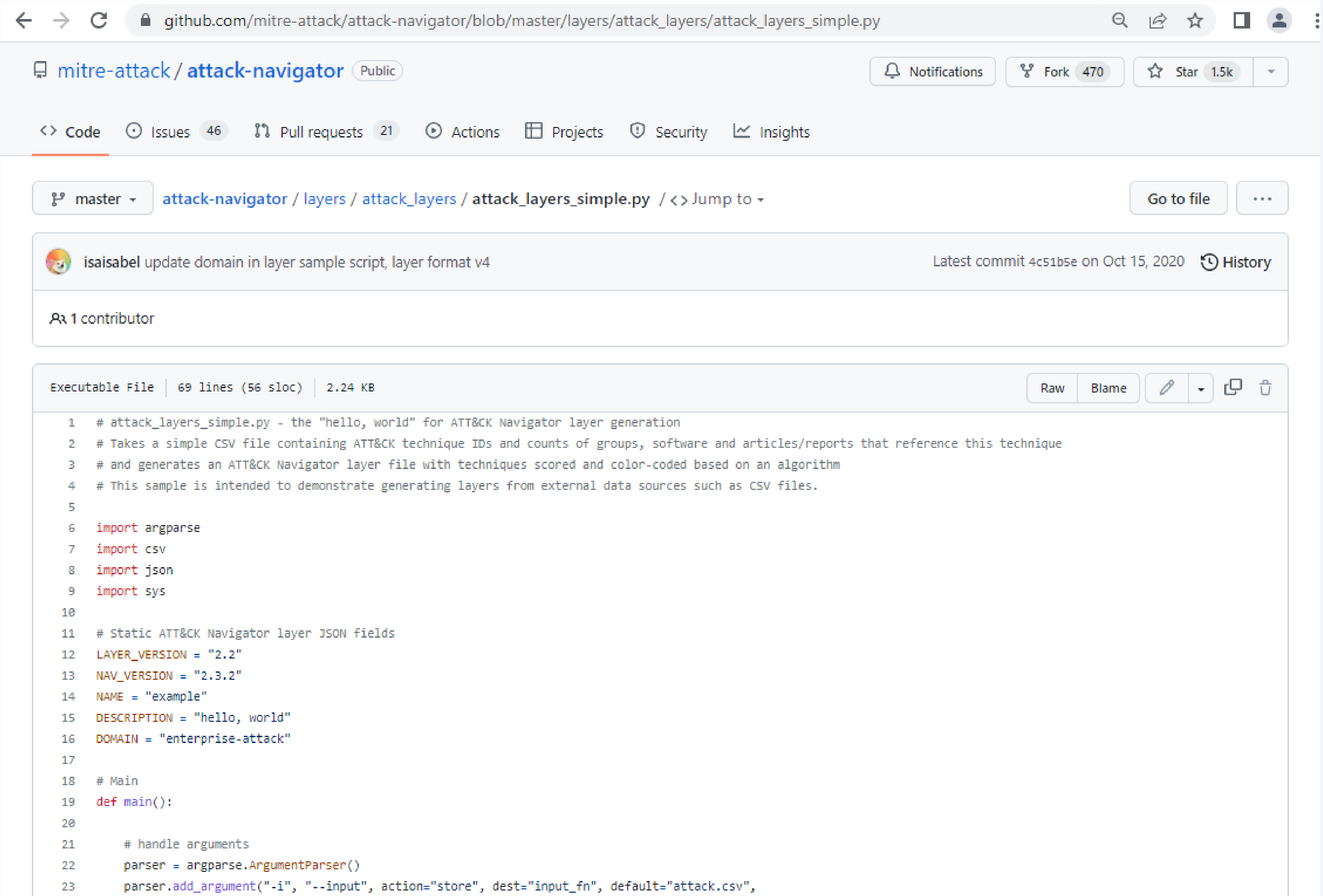
sites, etc., typically contains such malware.

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.

MITRE ATT&CK® Techniques

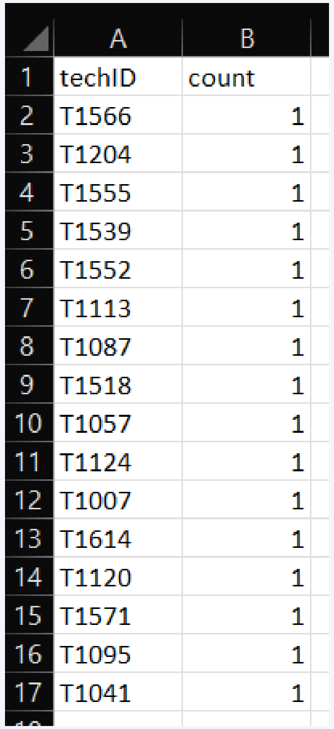
Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Credential Access	T1555 T1539 T1552	Credentials from Password Stores Steal Web Session Cookie Unsecured Credentials
Collection	T1113	Screen Capture
Discovery	T1087 T1518 T1057 T1124 T1007 T1614 T1120	Account Discovery Software Discovery Process Discovery System Time Discovery System Service Discovery System Location Discovery Peripheral Device Discovery
Command and Control	T1571 T1095	Non-Standard Port Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

Essential tool in the arsenal: https://github.com/mitre-attack/attack-navigator/blob/master/layers/attack_layers/attack_layers_simple.py


github.com/mitre-attack/attack-navigator/blob/master/layers/attack_layers/attack_layers_simple.py
mitre-attack / attack-navigator
Public
Notifications
Fork 470
Star 1.5k
Code
Issues 46
Pull requests 21
Actions
Projects
Security
Insights
master
attack-navigator / layers / attack_layers / attack_layers_simple.py / <> Jump to
Go to file
···
History
1 contributor
Executable File
69 lines (56 sloc)
2.24 KB
Raw
Blame

isaisabel update domain in layer sample script, layer format v4 Latest commit 4c51b5e on Oct 15, 2020

```python
# attack_layers_simple.py - the "hello, world" for ATT&CK Navigator layer generation
# Takes a simple CSV file containing ATT&CK technique IDs and counts of groups, software and articles/reports that reference this technique
# and generates an ATT&CK Navigator layer file with techniques scored and color-coded based on an algorithm
# This sample is intended to demonstrate generating layers from external data sources such as CSV files.

import argparse
import csv
import json
import sys

# Static ATT&CK Navigator layer JSON fields
LAYER_VERSION = "2.2"
NAV_VERSION = "2.3.2"
NAME = "example"
DESCRIPTION = "hello, world"
DOMAIN = "enterprise-attack"

# Main
def main():

    # handle arguments
    parser = argparse.ArgumentParser()
    parser.add_argument("-i", "--input", action="store", dest="input_fn", default="attack.csv",
```

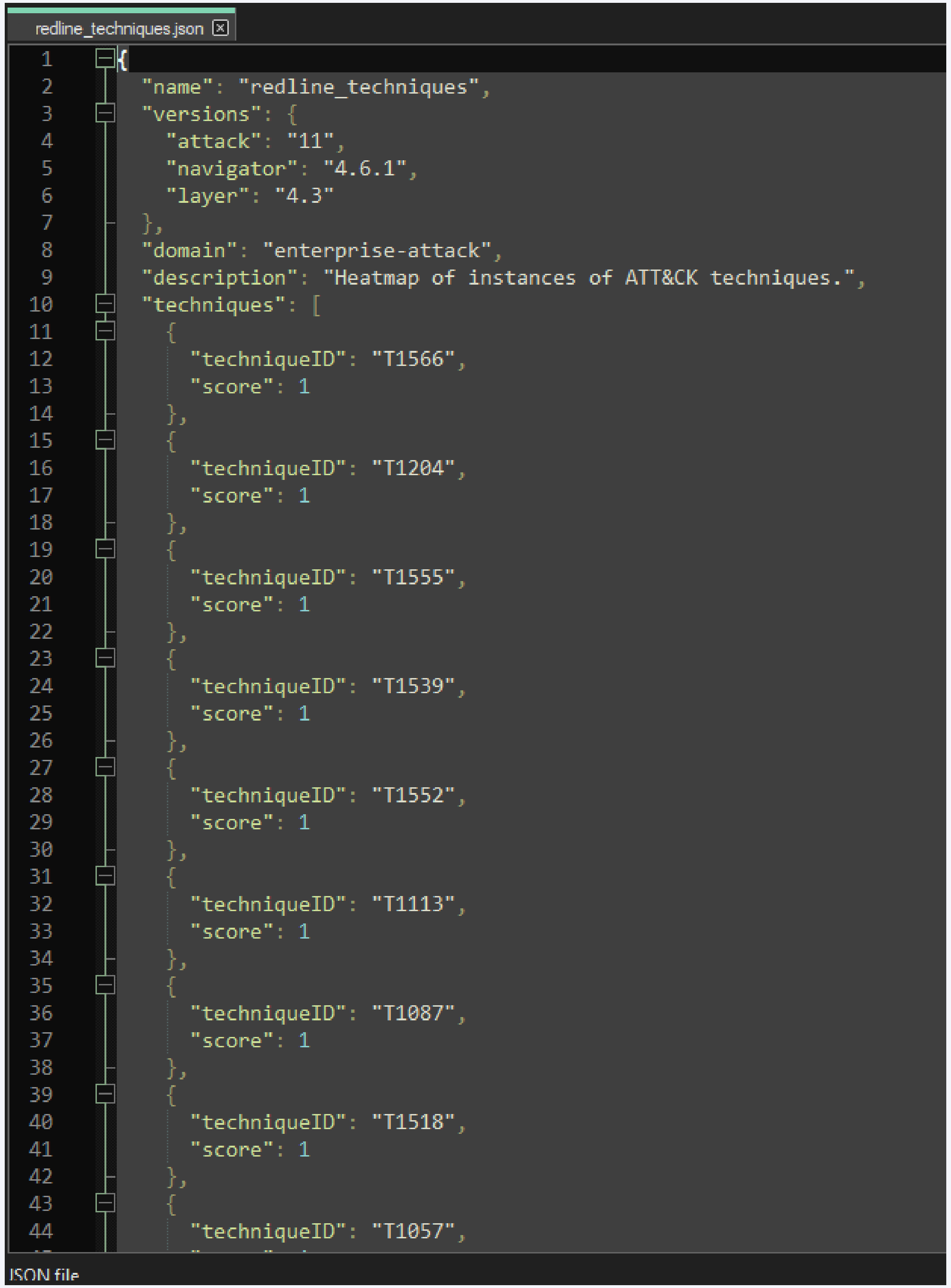


	A	B
1	techID	count
2	T1566	1
3	T1204	1
4	T1555	1
5	T1539	1
6	T1552	1
7	T1113	1
8	T1087	1
9	T1518	1
10	T1057	1
11	T1124	1
12	T1007	1
13	T1614	1
14	T1120	1
15	T1571	1
16	T1095	1
17	T1041	1

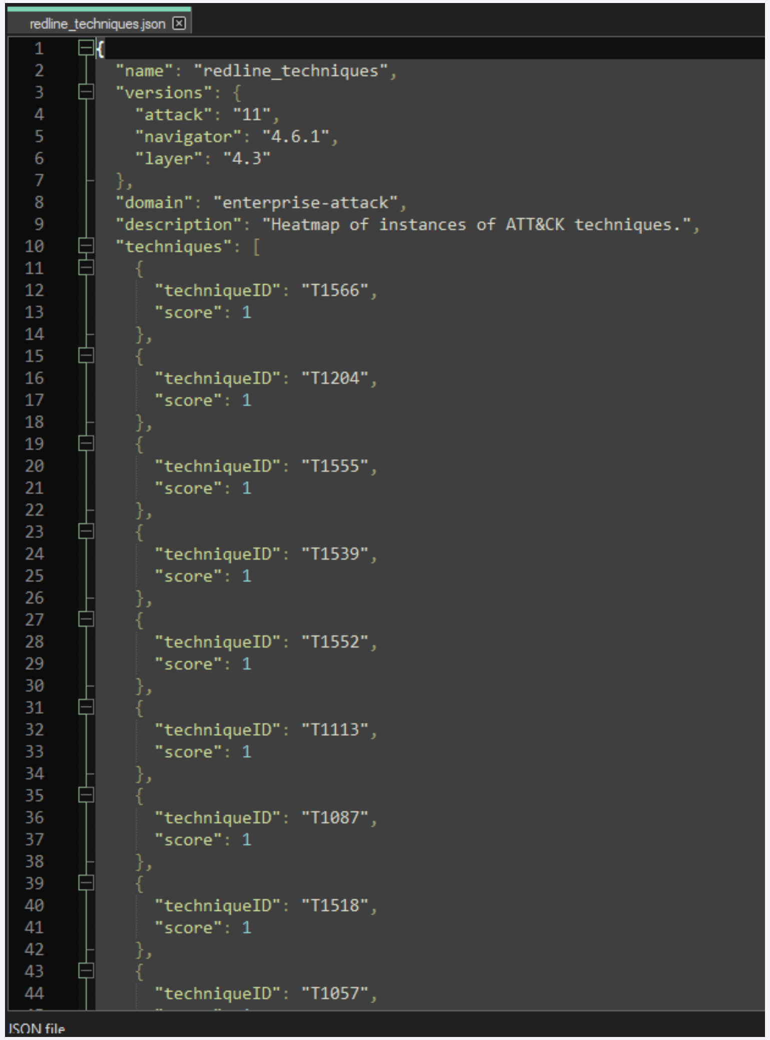
attack_layers_simple.py*

*Consider additional fields, like:

tactic
comment



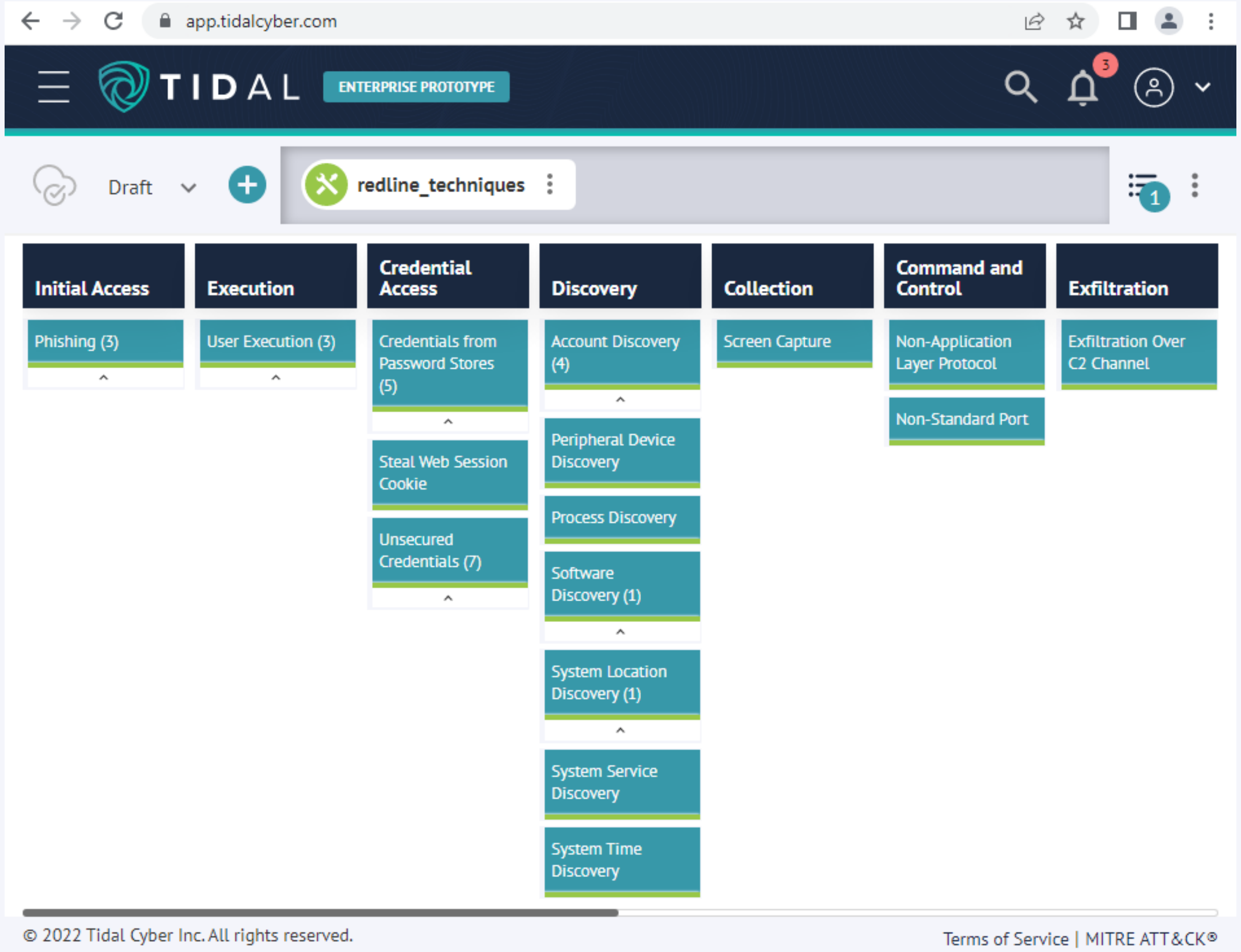
```
{
  "name": "redline_techniques",
  "versions": {
    "attack": "11",
    "navigator": "4.6.1",
    "layer": "4.3"
  },
  "domain": "enterprise-attack",
  "description": "Heatmap of instances of ATT&CK techniques.",
  "techniques": [
    {
      "techniqueID": "T1566",
      "score": 1
    },
  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



```
{
  "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",
```

app.tidalcyber.com

Import custom Technique Set

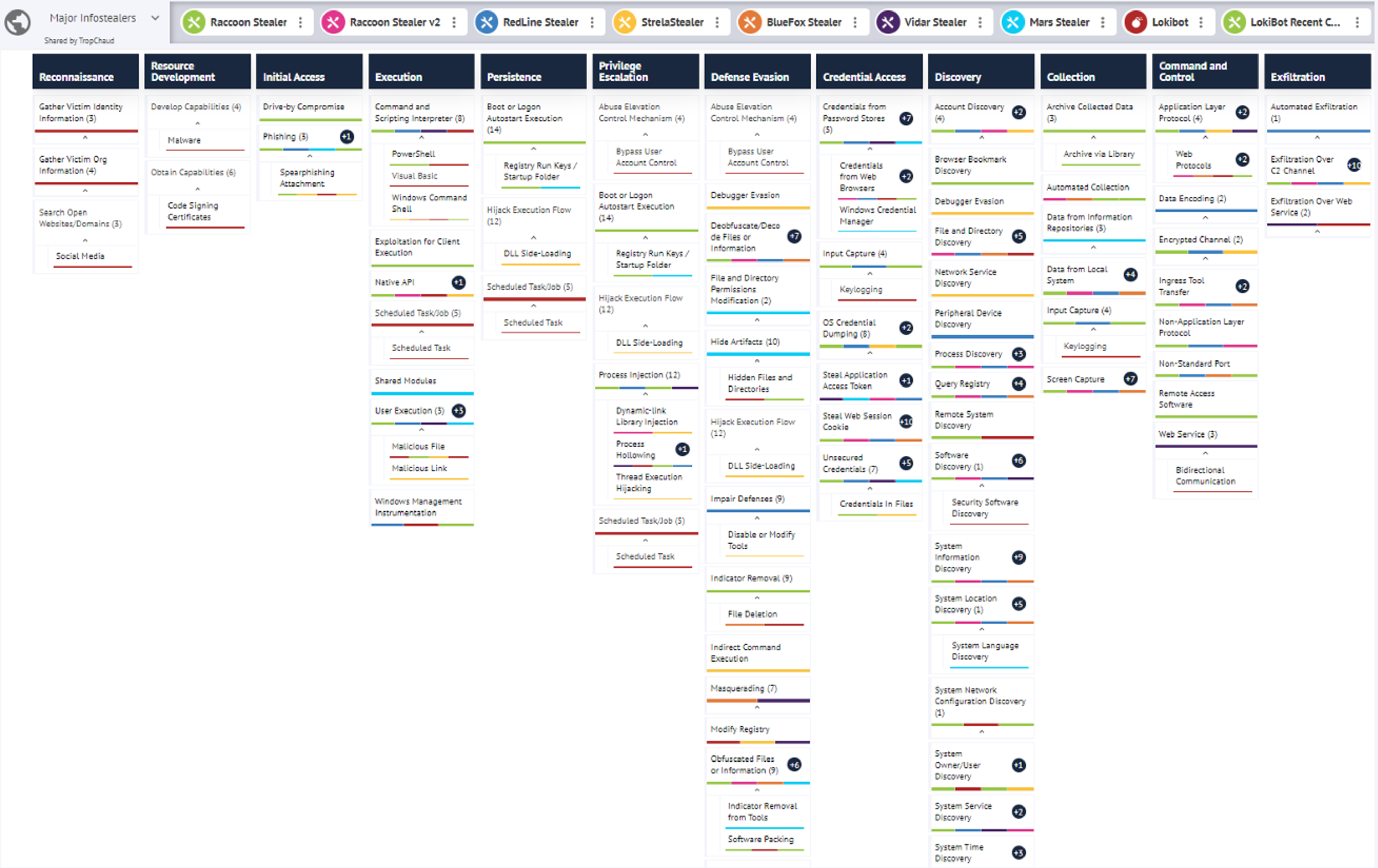


Initial Access	Execution	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Phishing (3)	User Execution (3)	Credentials from Password Stores (5)	Account Discovery (4)	Screen Capture	Non-Application Layer Protocol	Exfiltration Over C2 Channel
		Steal Web Session Cookie	Peripheral Device Discovery		Non-Standard Port	
		Unsecured Credentials (7)	Process Discovery			
			Software Discovery (1)			
			System Location Discovery (1)			
			System Service Discovery			
			System Time Discovery			

© 2022 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®

Scale it! app.tidalcyber.com > Community Spotlight > “Major Infostealers” Matrix



Major Infostealers
Shared by TropChaud

Raccoon Stealer | Raccoon Stealer v2 | RedLine Stealer | StrelaStealer | BlueFox Stealer | Vidar Stealer | Mars Stealer | Lokibot | LokiBot Recent C...

Reconnaissance
- Gather Victim Identity Information (3)
- Gather Victim Org Information (4)
- Search Open Websites/Domains (3)
  - Social Media

Resource Development
- Develop Capabilities (4)
  - Malware
- Obtain Capabilities (6)
  - Code Signing Certificates

Initial Access
- Drive-by Compromise
- Phishing (3) +1
  - Spearphishing Attachment

Execution
- Command and Scripting Interpreter (8)
  - PowerShell
  - Visual Basic
  - Windows Command Shell
- Exploitation for Client Execution
- Native API +1
- Scheduled Task/Job (5)
  - Scheduled Task
- Shared Modules
- User Execution (3) +3
  - Malicious File
  - Malicious Link
- Windows Management Instrumentation

Persistence
- Boot or Logon Autostart Execution (14)
  - Registry Run Keys / Startup Folder
- Hijack Execution Flow (12)
  - DLL Side-Loading
- Scheduled Task/Job (5)
  - Scheduled Task

Privilege Escalation
- Abuse Elevation Control Mechanism (4)
  - Bypass User Account Control
- Boot or Logon Autostart Execution (14)
  - Registry Run Keys / Startup Folder
- Hijack Execution Flow (12)
  - DLL Side-Loading
- Process Injection (12)
  - Dynamic-link Library Injection
  - Process Hollowing +1
  - Thread Execution Hijacking
- Scheduled Task/Job (5)
  - Scheduled Task

Defense Evasion
- Abuse Elevation Control Mechanism (4)
  - Bypass User Account Control
- Debugger Evasion
- Deobfuscate/Decode Files or Information +7
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
  - Hidden Files and Directories
- Hijack Execution Flow (12)
  - DLL Side-Loading
- Impair Defenses (9)
  - Disable or Modify Tools
- Indicator Removal (9)
  - File Deletion
- Indirect Command Execution
- Masquerading (7)
- Modify Registry
- Obfuscated Files or Information (9) +6
  - Indicator Removal from Tools
  - Software Packing

Credential Access
- Credentials from Password Stores (5) +7
  - Credentials from Web Browsers +2
  - Windows Credential Manager
- Input Capture (4)
  - Keylogging
- OS Credential Dumping (8) +2
- Steal Application Access Token +1
- Steal Web Session Cookie +10
- Unsecured Credentials (7) +5
  - Credentials In Files

Discovery
- Account Discovery (4) +2
- Browser Bookmark Discovery
- Debugger Evasion
- File and Directory Discovery +5
- Network Service Discovery
- Peripheral Device Discovery
- Process Discovery +3
- Query Registry +4
- Remote System Discovery
- Software Discovery (1) +6
  - Security Software Discovery
- System Information Discovery +9
- System Location Discovery (1) +5
  - System Language Discovery
- System Network Configuration Discovery (1)
- System Owner/User Discovery +1
- System Service Discovery +2
- System Time Discovery +3

Collection
- Archive Collected Data (3)
  - Archive via Library
- Automated Collection
- Data from Information Repositories (3)
- Data from Local System +4
- Input Capture (4)
  - Keylogging
- Screen Capture +7

Command and Control
- Application Layer Protocol (4) +2
  - Web Protocols +2
- Data Encoding (2)
- Encrypted Channel (2)
- Ingress Tool Transfer +2
- Non-Application Layer Protocol
- Non-Standard Port
- Remote Access Software
- Web Service (3)
  - Bidirectional Communication

Exfiltration
- Automated Exfiltration (1)
- Exfiltration Over C2 Channel +10
- Exfiltration Over Web Service (2)

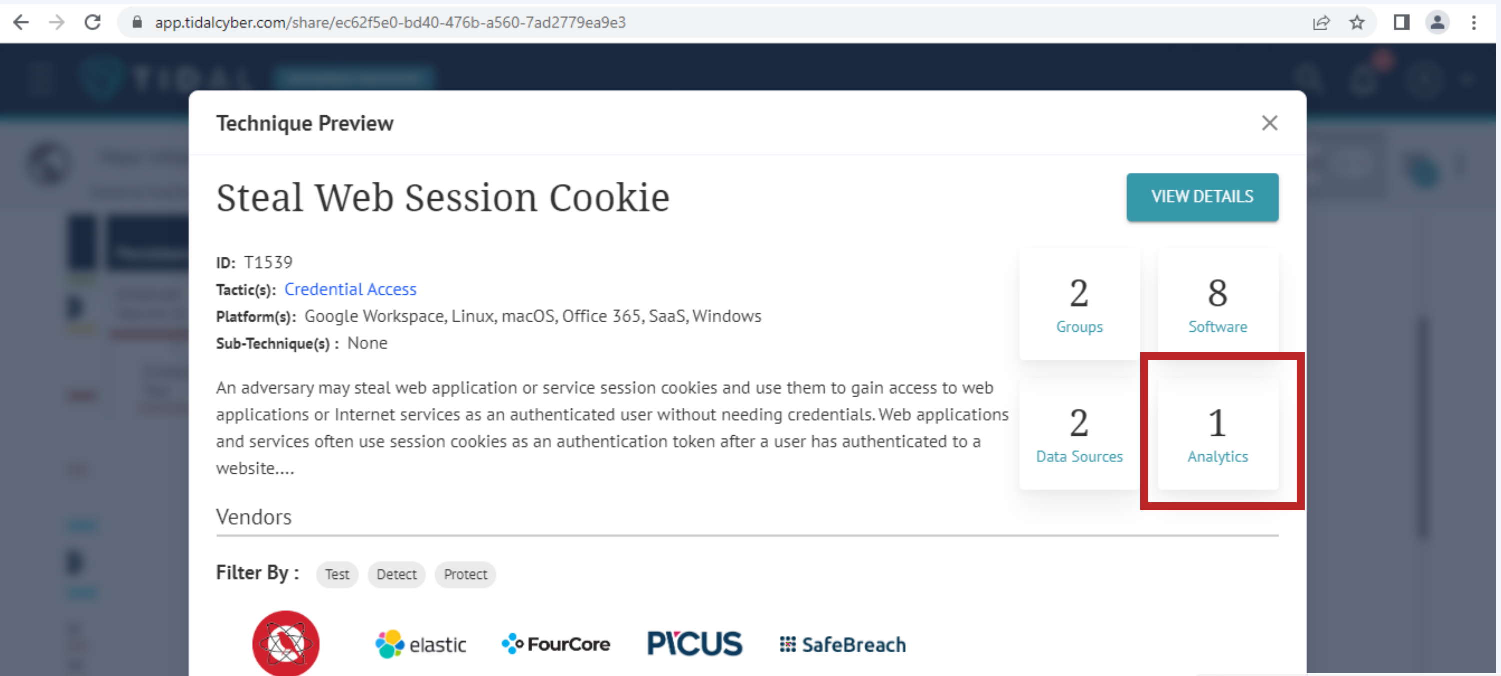
Major Infostealers: Top Common TTPs

How to prioritize??

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

Rank	Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Sources	# Sigma Analytics	# Atomic Tests
1	T1539	**Steal Web Session Cookie**	Credential Access	16	2	1	2
2 (Tie)	T1113	**Screen Capture**	Collection	13	2	6	6
2 (Tie)	T1082	**System Information Discovery**	Discovery	13	3	14	23
3	T1057	**Process Discovery**	Discovery	11	3	5	5
6 (Tie)	T1012	**Query Registry**	Discovery	8	4	10	2
6 (Tie)	T1083	**File and Directory Discovery**	Discovery	8	3	11	6
8	T1007	**System Service Discovery**	Discovery	6	3	3	3
9 (Tie)	T1528	**Steal Application Access Token**	Credential Access	5	1	8	1
9 (Tie)	T1555.003	**Credentials from Web Browsers**	Credential Access	5	4	2	16
9 (Tie)	T1106	**Native API**	Execution	5	2	12	4

Importance of Gap Identification


app.tidalcyber.com/share/ec62f5e0-bd40-476b-a560-7ad2779ea9e3

Technique Preview

Steal Web Session Cookie

VIEW DETAILS

ID: T1539
Tactic(s): Credential Access
Platform(s): Google Workspace, Linux, macOS, Office 365, SaaS, Windows
Sub-Technique(s) : None

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website....

2 Groups
8 Software
2 Data Sources
1 Analytics

Vendors

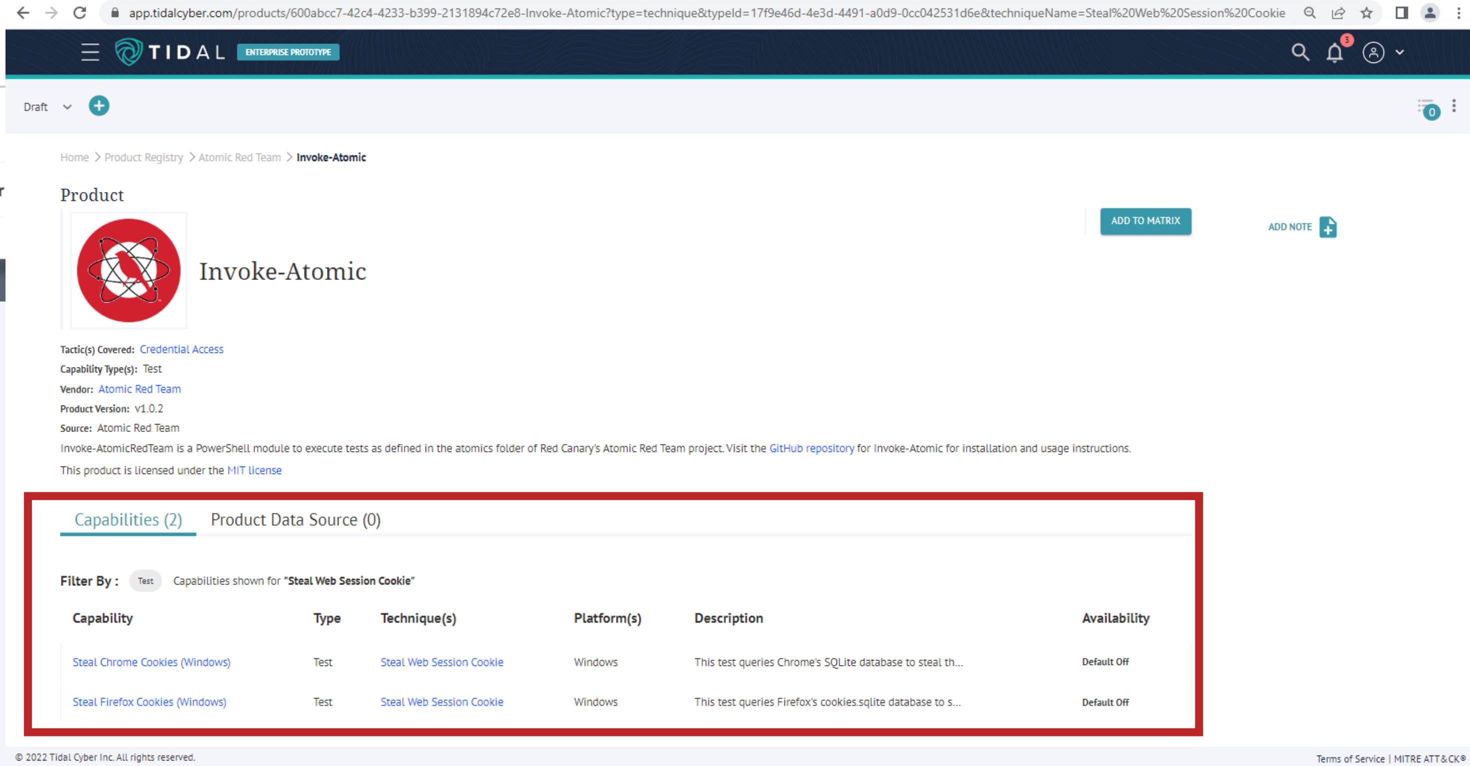
Filter By : Test Detect Protect

Atomic Red Team
Elastic
FourCore
Picus
SafeBreach

Labels

Filter By : All(14) Technique Set(14)

Raccoon St... Raccoon St... RedLine St... BlueFox St... Vidar


app.tidalcyber.com/products/600abcc7-42c4-4233-b399-2131894c72e8-Invoke-Atomic?type=technique&typeId=17f9e46d-4e3d-4491-a0d9-0cc042531d6e&techniqueName=Steal%20Web%20Session%20Cookie
TIDAL
ENTERPRISE PROTOTYPE
Draft

Home > Product Registry > Atomic Red Team > **Invoke-Atomic**

Product

ADD TO MATRIX

ADD NOTE

Invoke-Atomic

Tactic(s) Covered: Credential Access
Capability Type(s): Test
Vendor: Atomic Red Team
Product Version: v1.0.2
Source: Atomic Red Team

Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the atomics folder of Red Canary's Atomic Red Team project. Visit the GitHub repository for Invoke-Atomic for installation and usage instructions.

This product is licensed under the MIT license

Capabilities (2) Product Data Source (0)

Filter By : Test Capabilities shown for **"Steal Web Session Cookie"**

Capability	Type	Technique(s)	Platform(s)	Description	Availability
Steal Chrome Cookies (Windows)	Test	Steal Web Session Cookie	Windows	This test queries Chrome's SQLite database to steal th...	Default Off
Steal Firefox Cookies (Windows)	Test	Steal Web Session Cookie	Windows	This test queries Firefox's cookies.sqlite database to s...	Default Off

© 2022 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®

TIDAL

Major Infostealers: Top Common TTPs

Rank	Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Sources	# Sigma Analytics	# Atomic Tests
1	T1539	**Steal Web Session Cookie**	Credential Access	16	2	1	2
2 (Tie)	T1113	**Screen Capture**	Collection	13	2	6	6
2 (Tie)	T1082	**System Information Discovery**	Discovery	13	3	14	23
3	T1057	**Process Discovery**	Discovery	11	3	5	5
6 (Tie)	T1012	**Query Registry**	Discovery	8	4	10	2
6 (Tie)	T1083	**File and Directory Discovery**	Discovery	8	3	11	6
8	T1007	**System Service Discovery**	Discovery	6	3	3	3
9 (Tie)	T1528	**Steal Application Access Token**	Credential Access	5	1	8	1
9 (Tie)	T1555.003	**Credentials from Web Browsers**	Credential Access	5	4	2	16
9 (Tie)	T1106	**Native API**	Execution	5	2	12	4

Gap identified!!

Red Team Tools

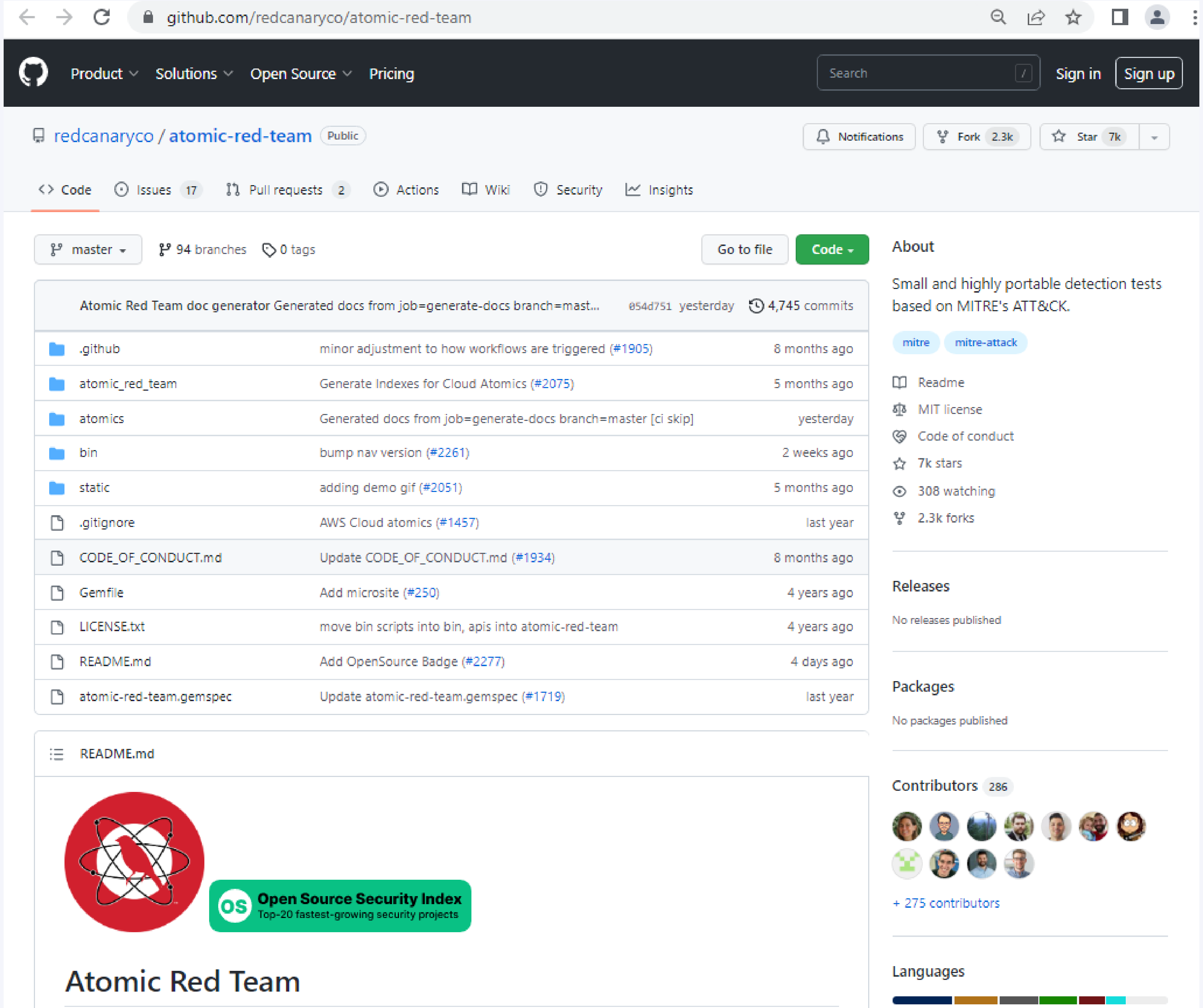
Simulating Adversary Behavior & Observing Tested Techniques

TIDAL

THREAT-INFORMED DEFENSE

Atomic Red Team How-To

TIDAL



Atomic Red Team doc generator Generated docs from job=generate-docs branch=mast... e54d751 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

OS 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.

Releases

No releases published

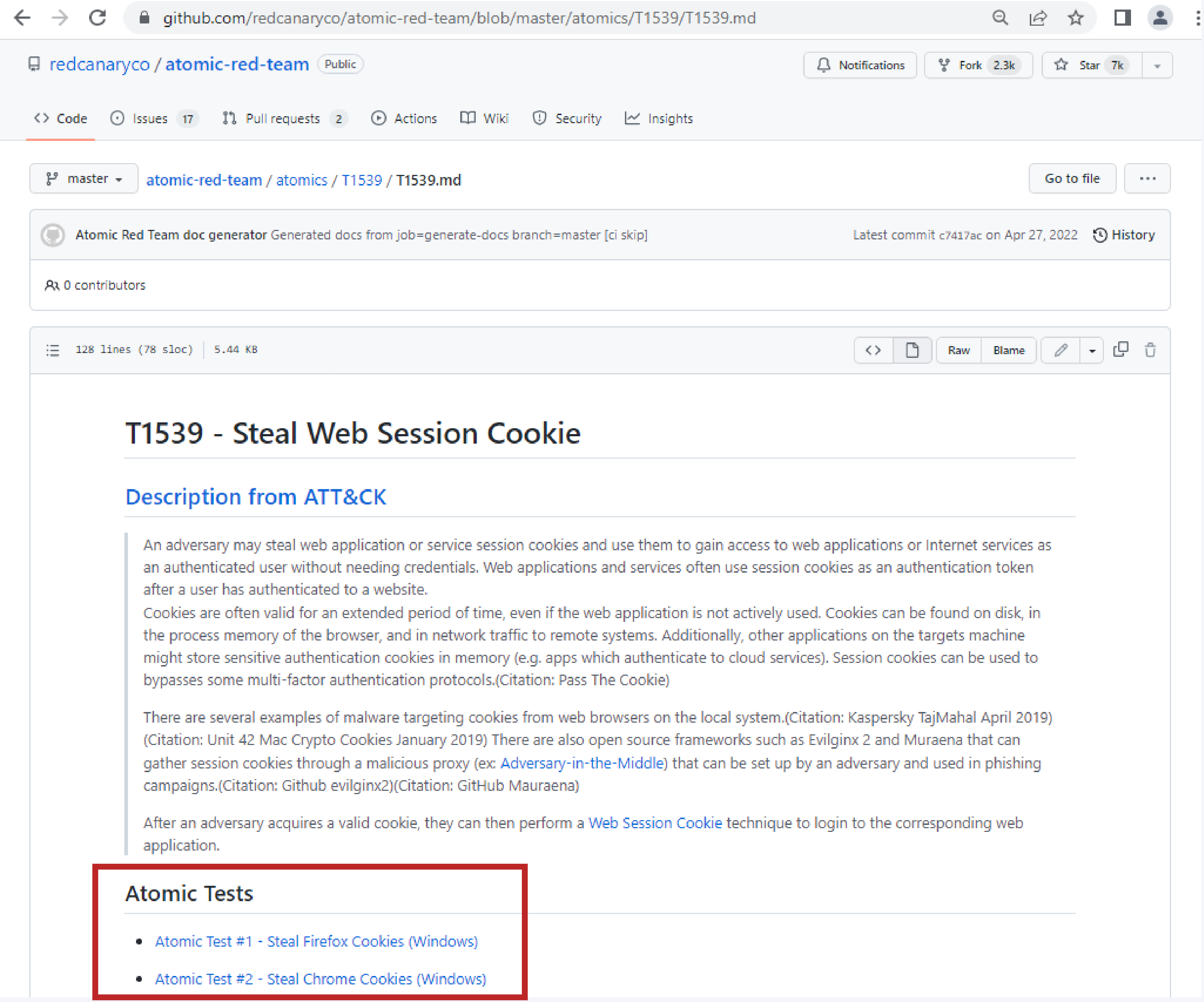
Packages

No packages published

Contributors 286

+ 275 contributors

Languages


github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1539/T1539.md
redcanaryco / atomic-red-team Public
Notifications
Fork 2.3k
Star 7k
Code
Issues 17
Pull requests 2
Actions
Wiki
Security
Insights
master
atomic-red-team / atomics / T1539 / T1539.md
Go to file
Atomic Red Team doc generator Generated docs from job=generate-docs branch=master [ci skip]
Latest commit c7417ac on Apr 27, 2022
History
0 contributors
128 lines (78 sloc) 5.44 KB
Raw
Blame

T1539 - Steal Web Session Cookie

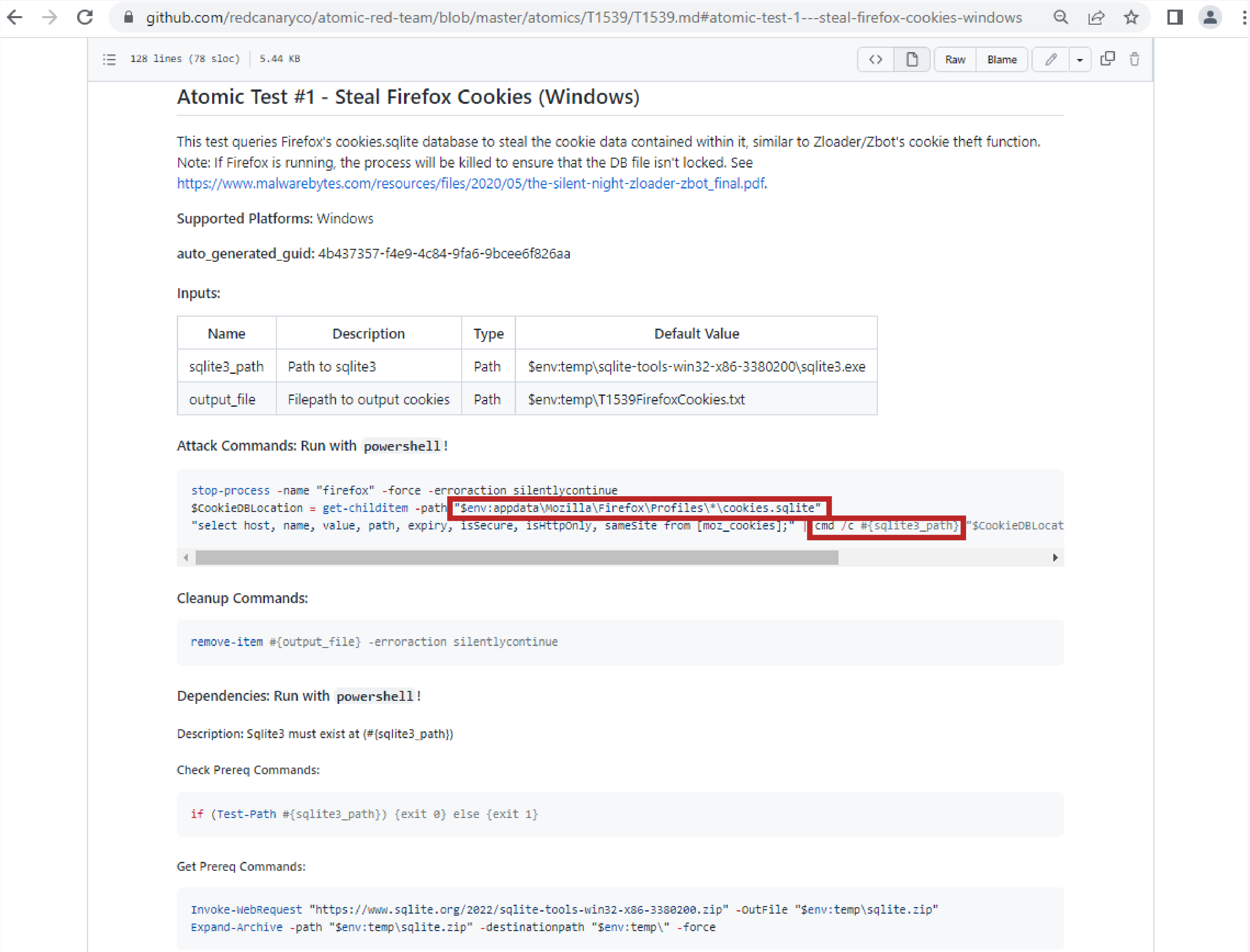
Description from ATT&CK

> An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.
> Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie)
>
> There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as Evilginx 2 and Muraena that can gather session cookies through a malicious proxy (ex: Adversary-in-the-Middle) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena)
>
> After an adversary acquires a valid cookie, they can then perform a Web Session Cookie technique to login to the corresponding web application.

Atomic Tests

- Atomic Test #1 - Steal Firefox Cookies (Windows)
- Atomic Test #2 - Steal Chrome Cookies (Windows)

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`!

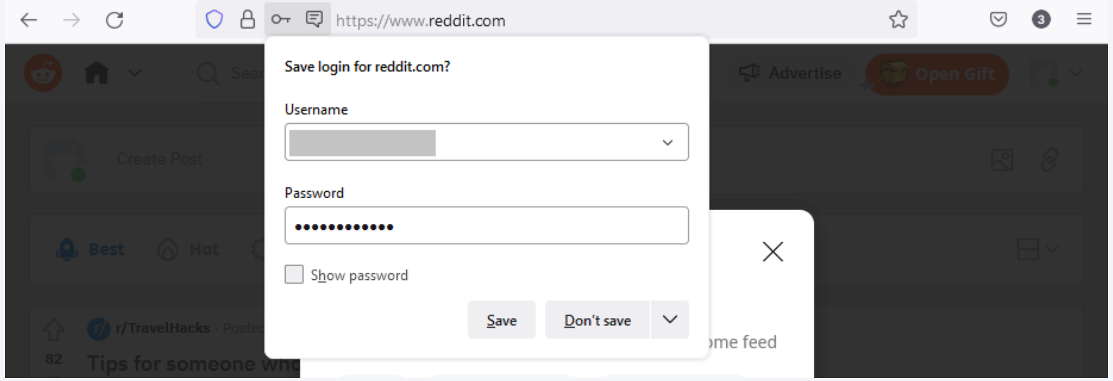
Description: Sqlite3 must exist at (#{sqlite3_path})

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
```



Save login for reddit.com?

Username

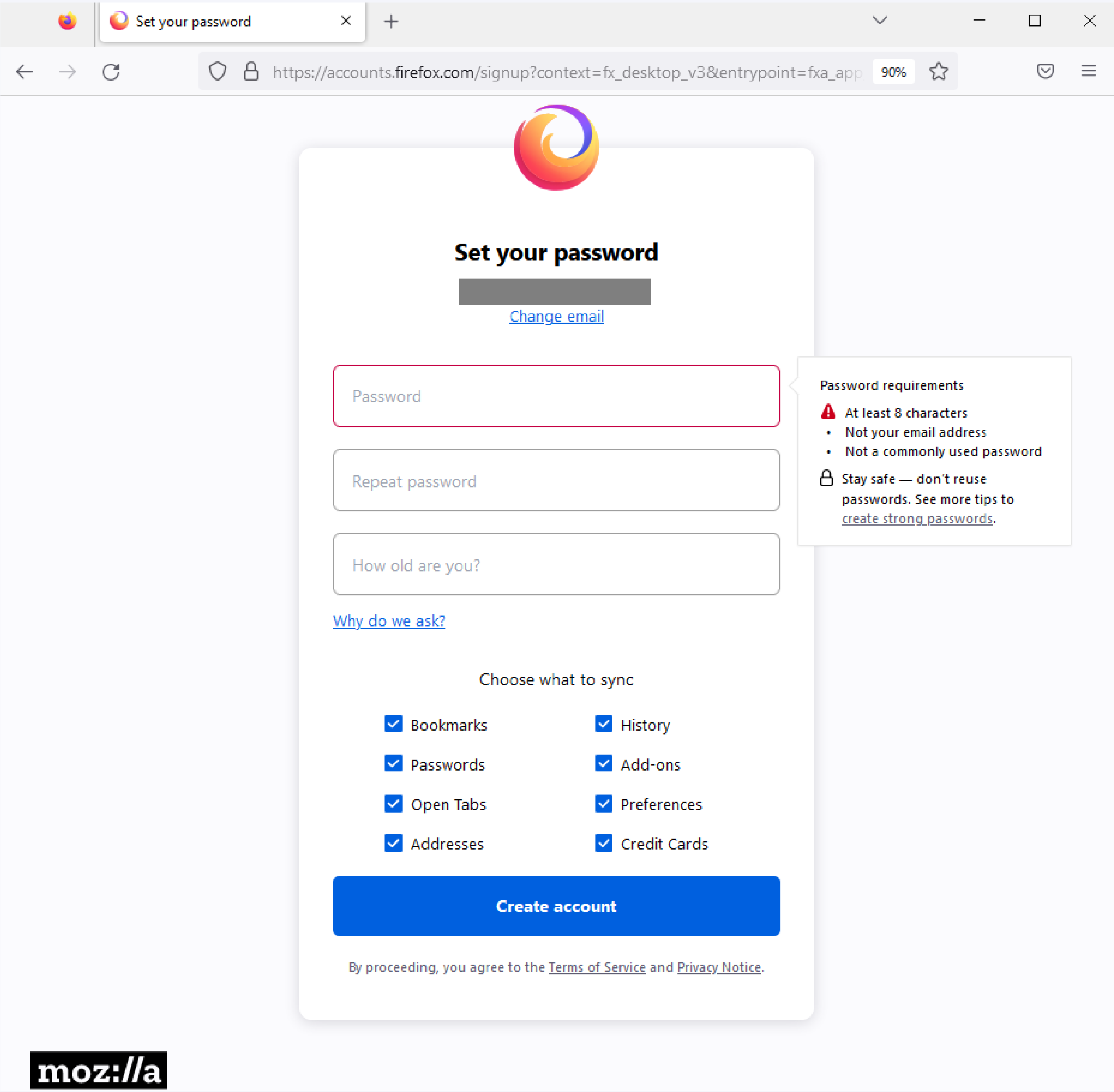
[redacted]

Password

••••••••••••

□ Show password

Save | Don't save


Set your password
https://accounts.firefox.com/signup?context=fx_desktop_v3&entrypoint=fxa_app
90%
moz://a

Set your password

[redacted]

Change email

Password

Repeat password

How old are you?

Why do we ask?

Password requirements

- At least 8 characters
- Not your email address
- Not a commonly used password

Stay safe — don't reuse passwords. See more tips to create strong passwords.

Choose what to sync

☑ Bookmarks ☑ History

☑ Passwords ☑ Add-ons

☑ Open Tabs ☑ Preferences

☑ Addresses ☑ Credit Cards

Create account

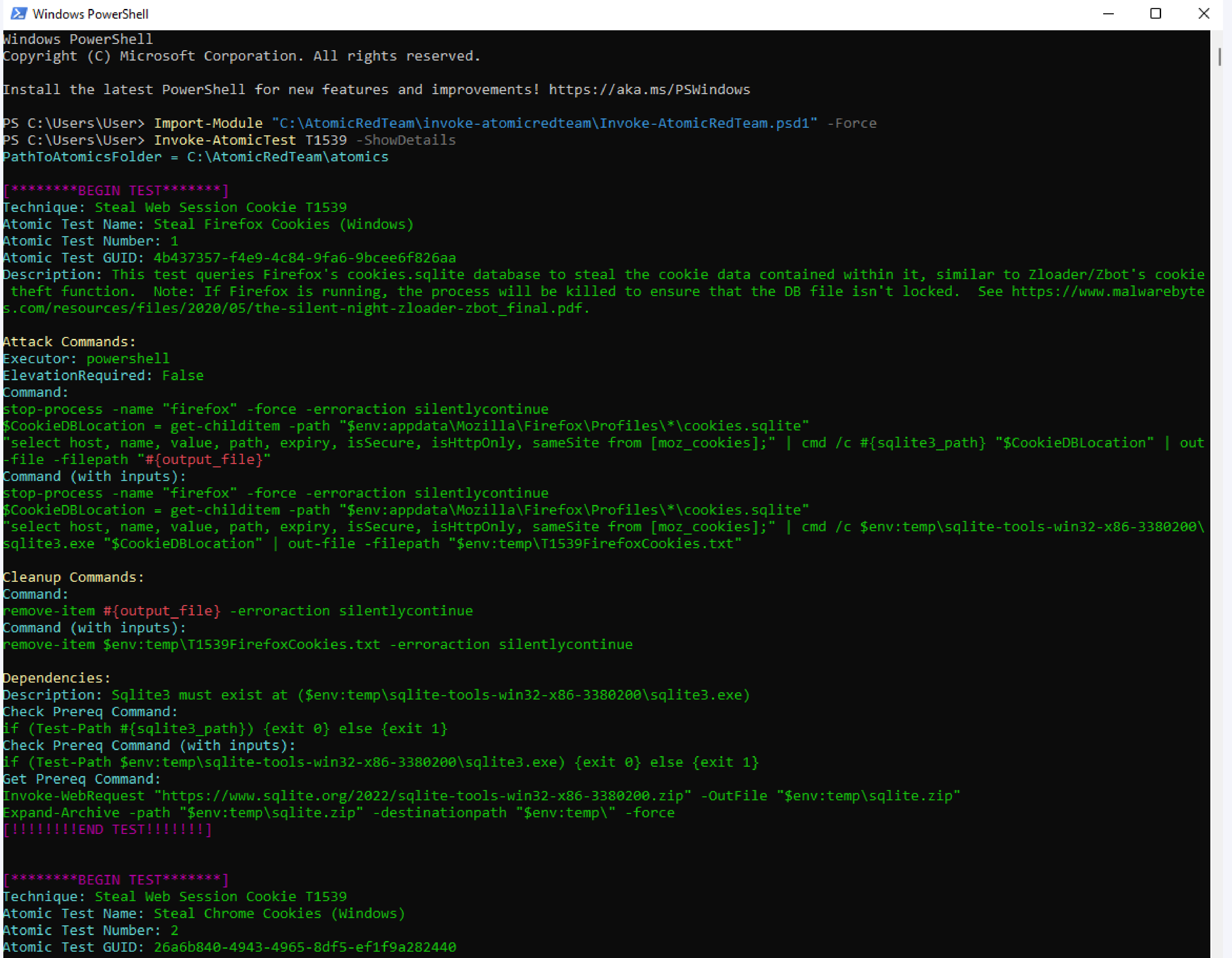
By proceeding, you agree to the Terms of Service and Privacy Notice.

TIDAL

Getting Started with Atomic Red Team testing

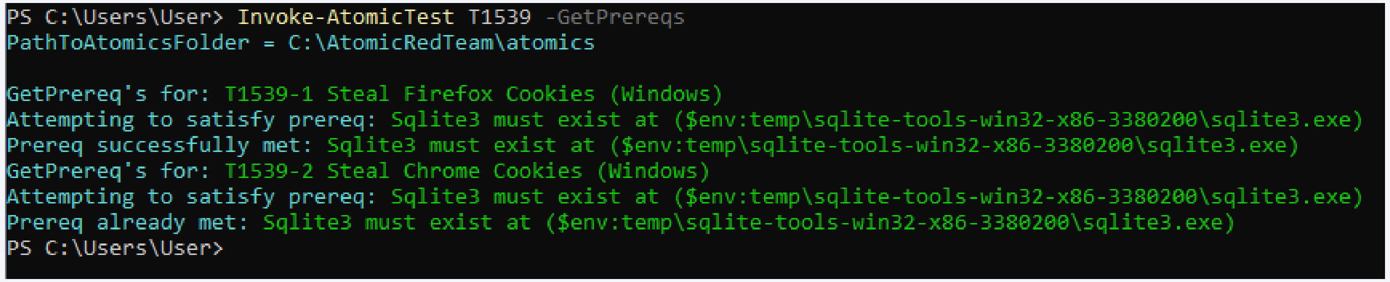
Invoke-AtomicRedTeam wiki: https://github.com/redcanaryco/invoke-atomicredteam/wiki

TIDAL

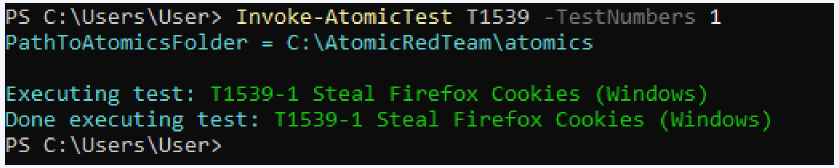


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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
```

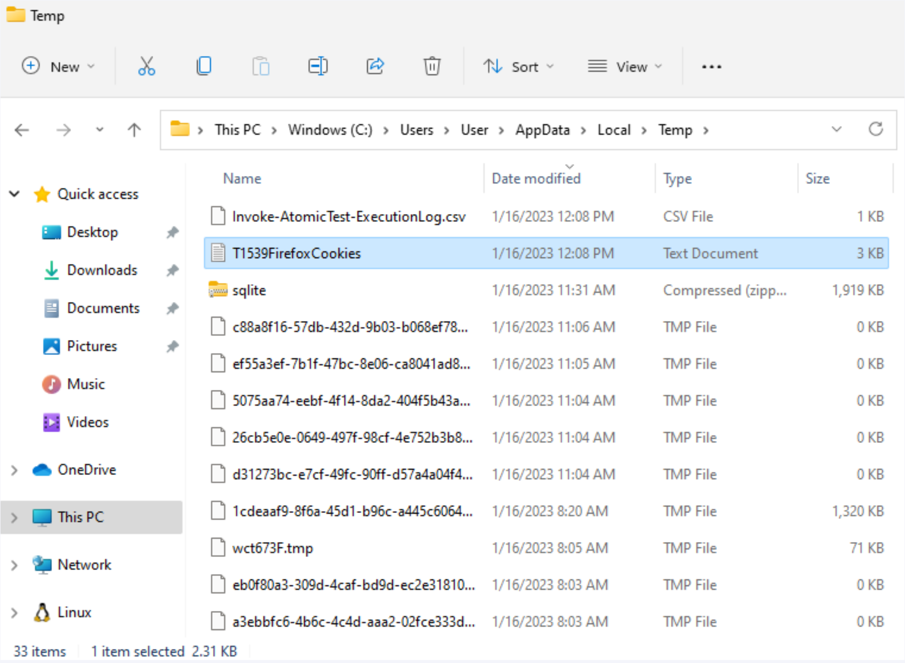
The Fun Stuff!! Carrying out a real-world adversary attack / technique!



```
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>
```



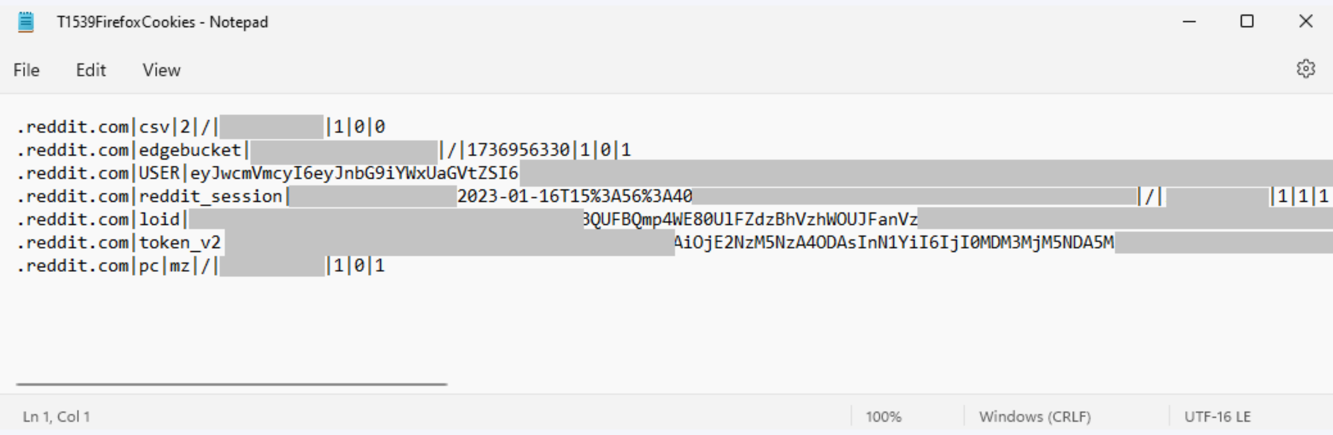
```
PS C:\Users\User> Invoke-AtomicTest T1539 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

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



This PC › Windows (C:) › Users › User › AppData › Local › Temp ›

Name	Date modified	Type	Size
Invoke-AtomicTest-ExecutionLog.csv	1/16/2023 12:08 PM	CSV File	1 KB
T1539FirefoxCookies	1/16/2023 12:08 PM	Text Document	3 KB
sqlite	1/16/2023 11:31 AM	Compressed (zipp...	1,919 KB
c88a8f16-57db-432d-9b03-b068ef78...	1/16/2023 11:06 AM	TMP File	0 KB
ef55a3ef-7b1f-47bc-8e06-ca8041ad8...	1/16/2023 11:05 AM	TMP File	0 KB
5075aa74-eebf-4f14-8da2-404f5b43a...	1/16/2023 11:04 AM	TMP File	0 KB
26cb5e0e-0649-497f-98cf-4e752b3b8...	1/16/2023 11:04 AM	TMP File	0 KB
d31273bc-e7cf-49fc-90ff-d57a4a04f4...	1/16/2023 11:04 AM	TMP File	0 KB
1cdeaaf9-8f6a-45d1-b96c-a445c6064...	1/16/2023 8:20 AM	TMP File	1,320 KB
wct673F.tmp	1/16/2023 8:05 AM	TMP File	71 KB
eb0f80a3-309d-4caf-bd9d-ec2e31810...	1/16/2023 8:03 AM	TMP File	0 KB
a3ebbfc6-4b6c-4c4d-aaa2-02fce333d...	1/16/2023 8:03 AM	TMP File	0 KB

33 items   1 item selected 2.31 KB



```
.reddit.com|csv|2|/|[redacted]|1|0|0
.reddit.com|edgebucket|[redacted]|/|1736956330|1|0|1
.reddit.com|USER|eyJwcmVmcyI6eyJnbG9iYWxUaGVtZSI6[redacted]
.reddit.com|reddit_session|[redacted]2023-01-16T15%3A56%3A40[redacted]|/|[redacted]|1|1|1
.reddit.com|loid|[redacted]3QUFBQmp4WE80UlFZdzBhVzhWOUJFanVz[redacted]
.reddit.com|token_v2[redacted]AiOjE2NzM5NzA4ODAsInN1YiI6IjI0MDM3MjM5NDA5M[redacted]
.reddit.com|pc|mz|/|[redacted]|1|0|1
```

Ln 1, Col 1   100%   Windows (CRLF)   UTF-16 LE

Blue/Purple Team Tools

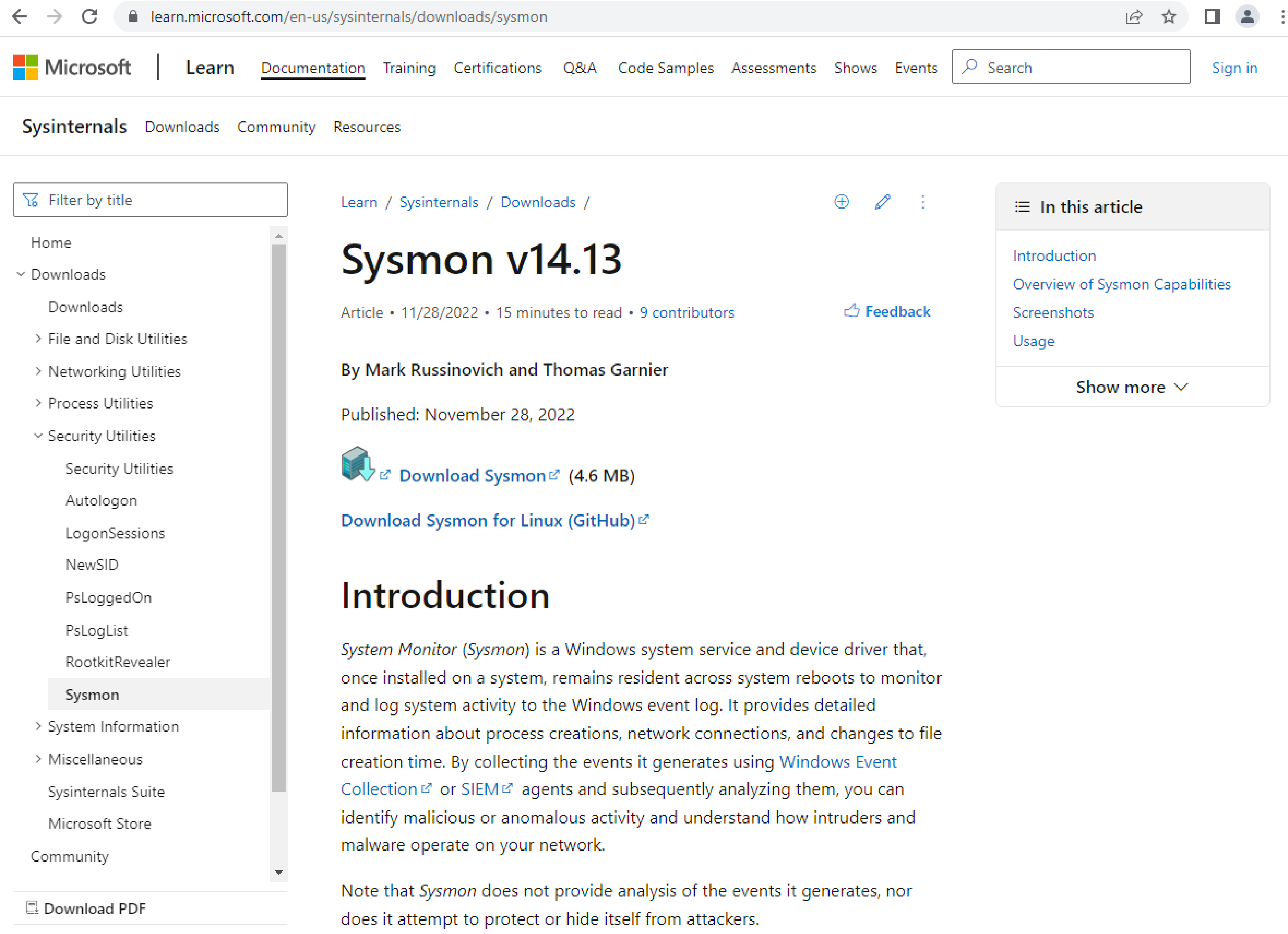
Closing the Gap: Closing Gaps With (Validated!) Detections

TIDAL

THREAT-INFORMED DEFENSE

Logging With Sysmon

TIDAL



Sysmon v14.13

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

By Mark Russinovich and Thomas Garnier

Published: November 28, 2022

Download Sysmon (4.6 MB)

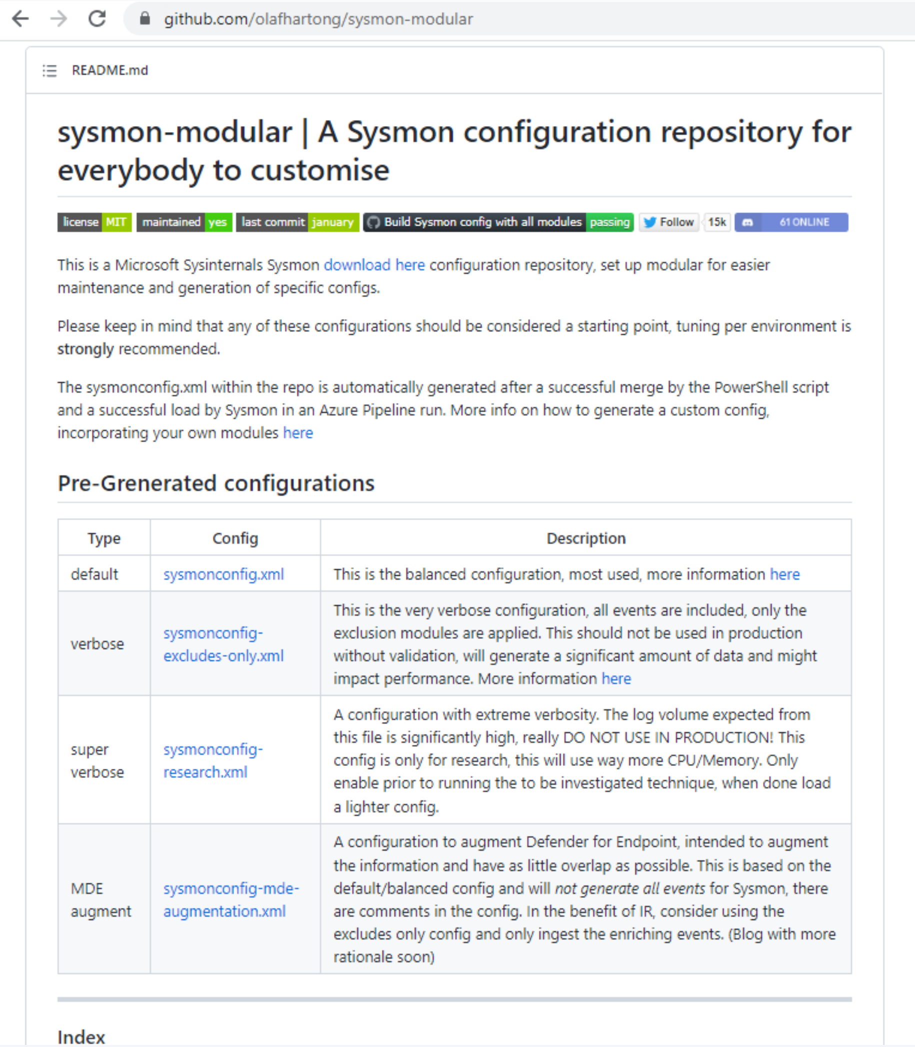
Download Sysmon for Linux (GitHub)

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
license MIT
maintained yes
last commit january
Build Sysmon config with all modules passing
Follow
15k
61 ONLINE

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.

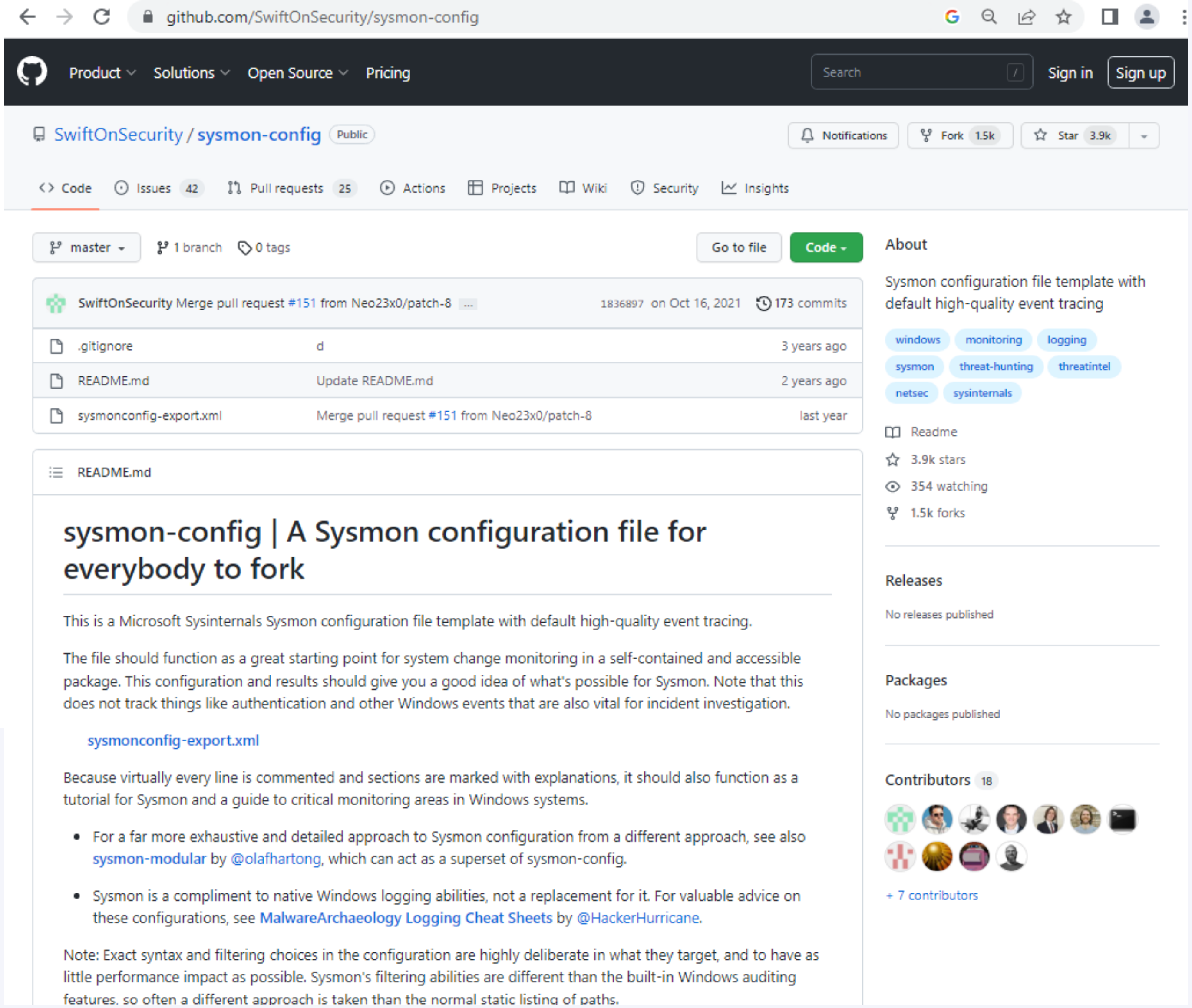
Please keep in mind that any of these configurations should be considered a starting point, tuning per environment is **strongly** recommended.

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



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

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

No releases published

No packages published

+ 7 contributors

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.

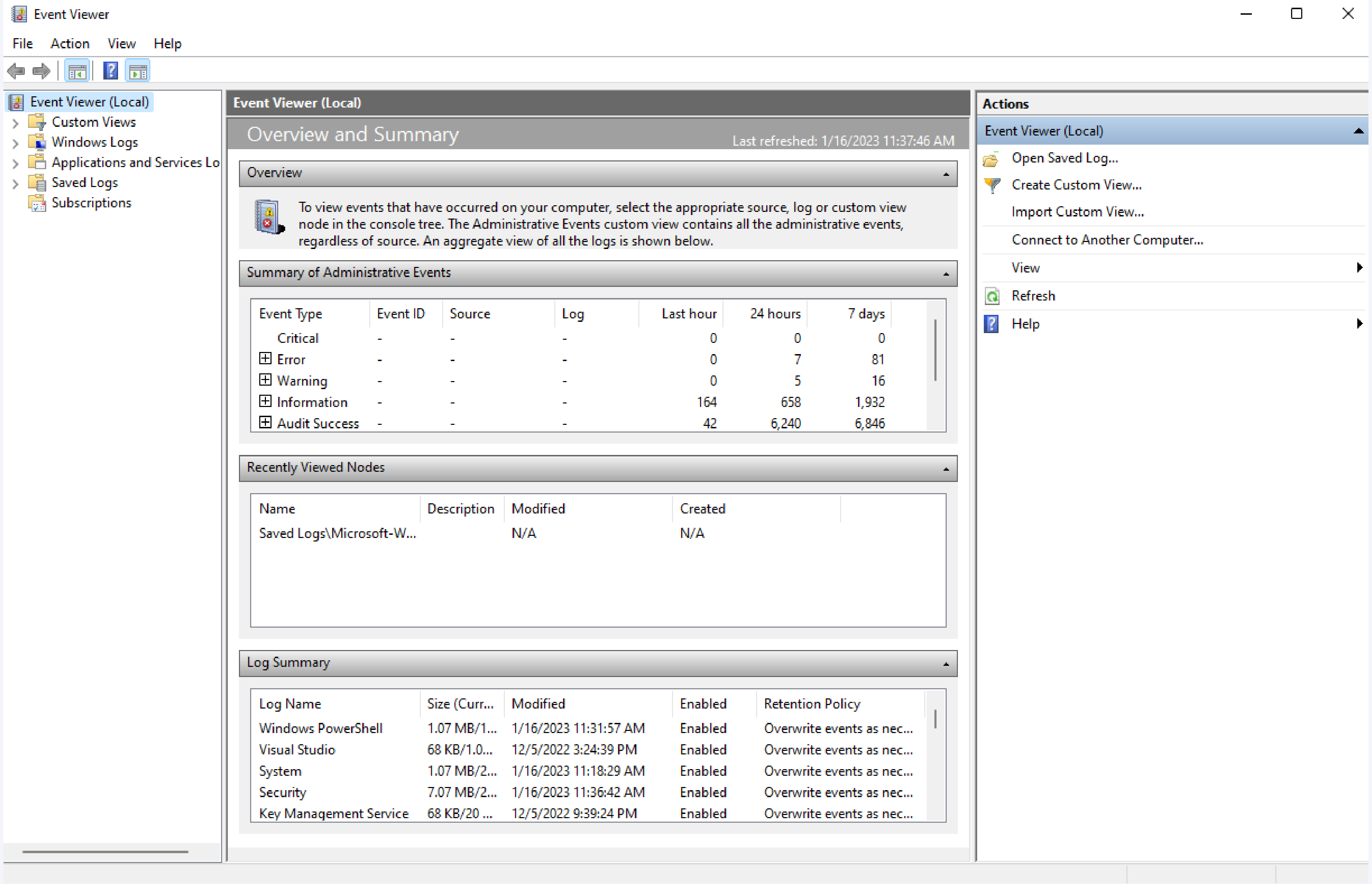
sysmonconfig-export.xml

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.

TIDAL



Overview and Summary

Last refreshed: 1/16/2023 11:37:46 AM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Summary of Administrative Events

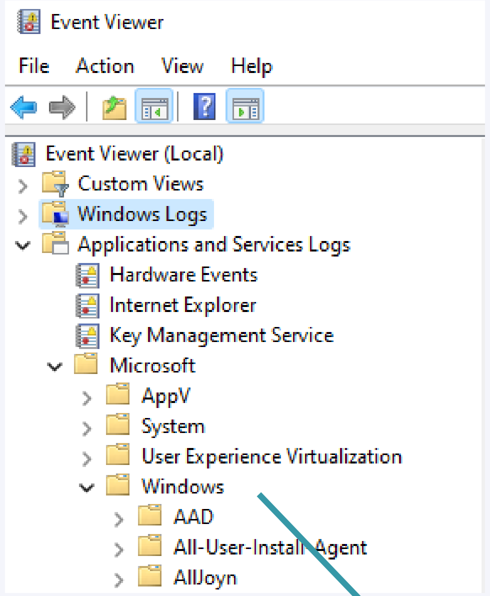
Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	0	7	81
⊞ Warning	-	-	-	0	5	16
⊞ Information	-	-	-	164	658	1,932
⊞ Audit Success	-	-	-	42	6,240	6,846

Recently Viewed Nodes

Name	Description	Modified	Created
Saved Logs\Microsoft-W...		N/A	N/A

Log Summary

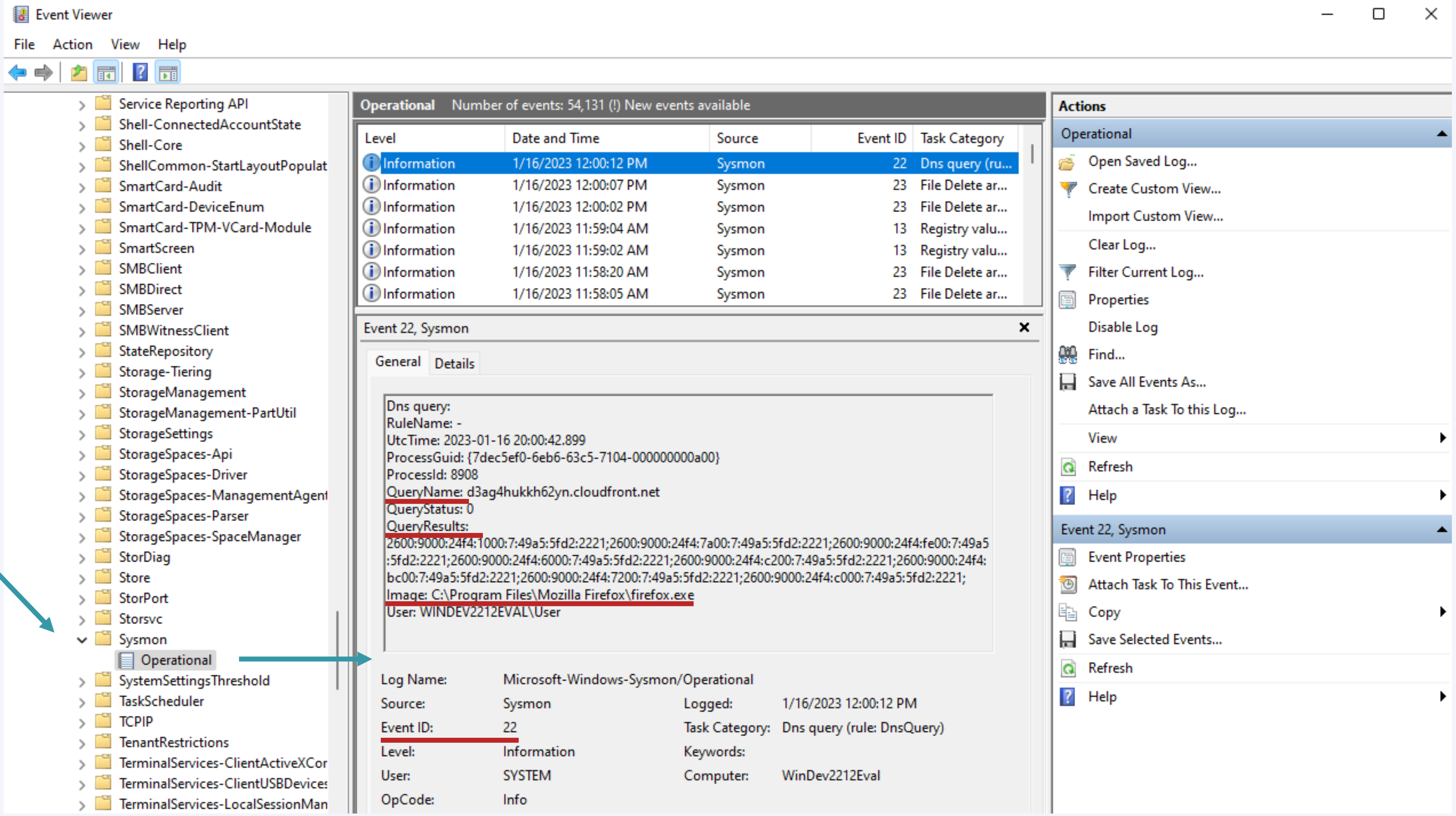
Log Name	Size (Curr...	Modified	Enabled	Retention Policy
Windows PowerShell	1.07 MB/1...	1/16/2023 11:31:57 AM	Enabled	Overwrite events as nec...
Visual Studio	68 KB/1.0...	12/5/2022 3:24:39 PM	Enabled	Overwrite events as nec...
System	1.07 MB/2...	1/16/2023 11:18:29 AM	Enabled	Overwrite events as nec...
Security	7.07 MB/2...	1/16/2023 11:36:42 AM	Enabled	Overwrite events as nec...
Key Management Service	68 KB/20 ...	12/5/2022 9:39:24 PM	Enabled	Overwrite events as nec...



This path ↑

OR

This path ↓



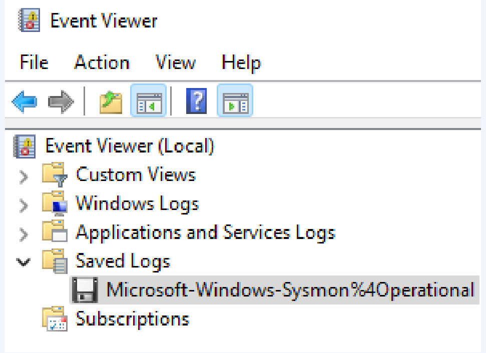
Operational Number of events: 54,131 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	1/16/2023 12:00:12 PM	Sysmon	22	Dns query (ru...
Information	1/16/2023 12:00:07 PM	Sysmon	23	File Delete ar...
Information	1/16/2023 12:00:02 PM	Sysmon	23	File Delete ar...
Information	1/16/2023 11:59:04 AM	Sysmon	13	Registry valu...
Information	1/16/2023 11:59:02 AM	Sysmon	13	Registry valu...
Information	1/16/2023 11:58:20 AM	Sysmon	23	File Delete ar...
Information	1/16/2023 11:58:05 AM	Sysmon	23	File Delete ar...

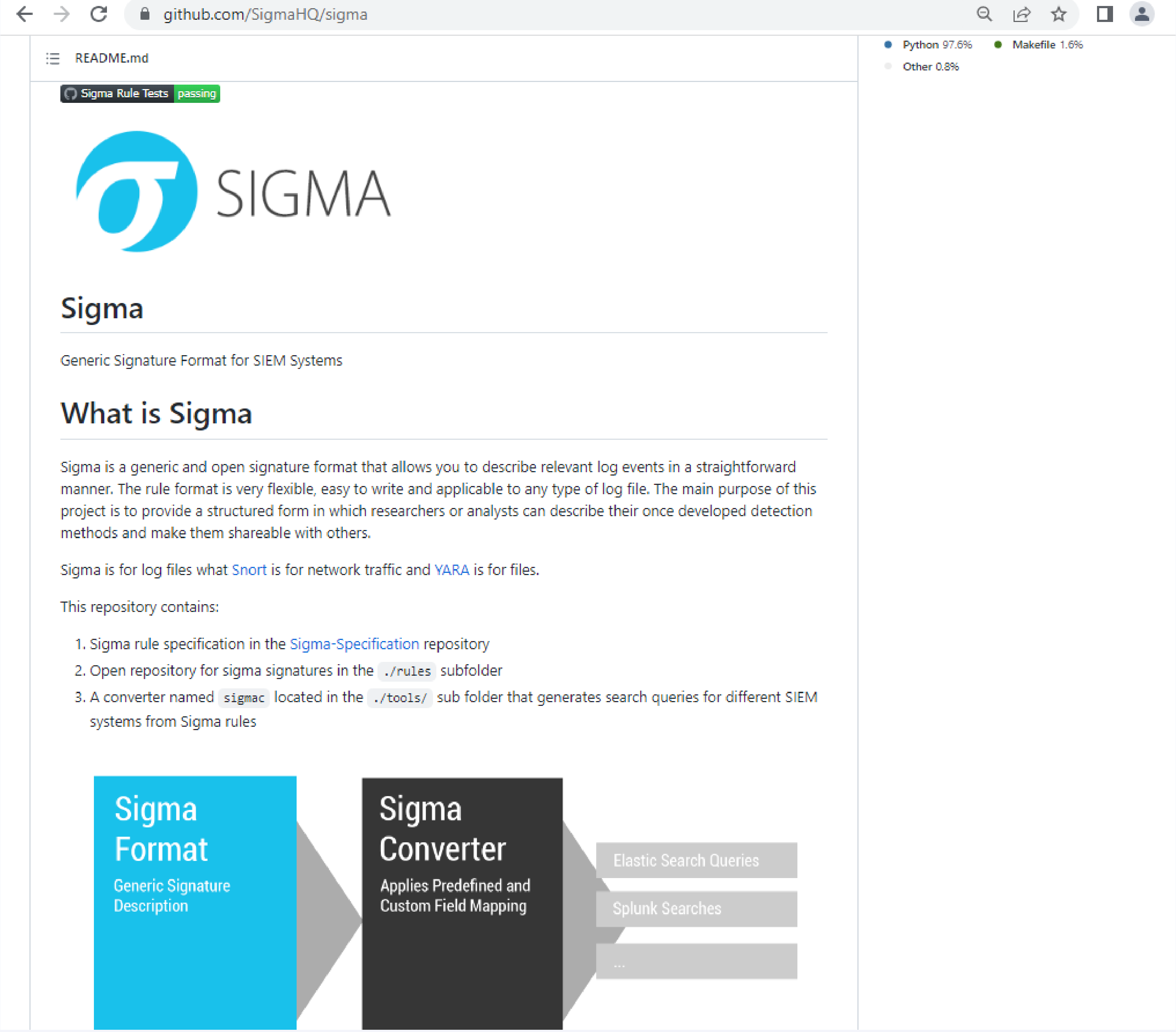
Event 22, Sysmon

```
Dns query:
RuleName: -
UtcTime: 2023-01-16 20:00:42.899
ProcessGuid: {7dec5ef0-6eb6-63c5-7104-000000000a00}
ProcessId: 8908
QueryName: d3ag4hukkh62yn.cloudfront.net
QueryStatus: 0
QueryResults:
2600:9000:24f4:1000:7:49a5:5fd2:2221;2600:9000:24f4:7a00:7:49a5:5fd2:2221;2600:9000:24f4:fe00:7:49a5
:5fd2:2221;2600:9000:24f4:6000:7:49a5:5fd2:2221;2600:9000:24f4:c200:7:49a5:5fd2:2221;2600:9000:24f4:
bc00:7:49a5:5fd2:2221;2600:9000:24f4:7200:7:49a5:5fd2:2221;2600:9000:24f4:c000:7:49a5:5fd2:2221;
Image: C:\Program Files\Mozilla Firefox\firefox.exe
User: WINDEV2212EVAL\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	1/16/2023 12:00:12 PM
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WinDev2212Eval
OpCode:	Info		



Sigma Rules



Sigma

Generic Signature Format for SIEM Systems

What is Sigma

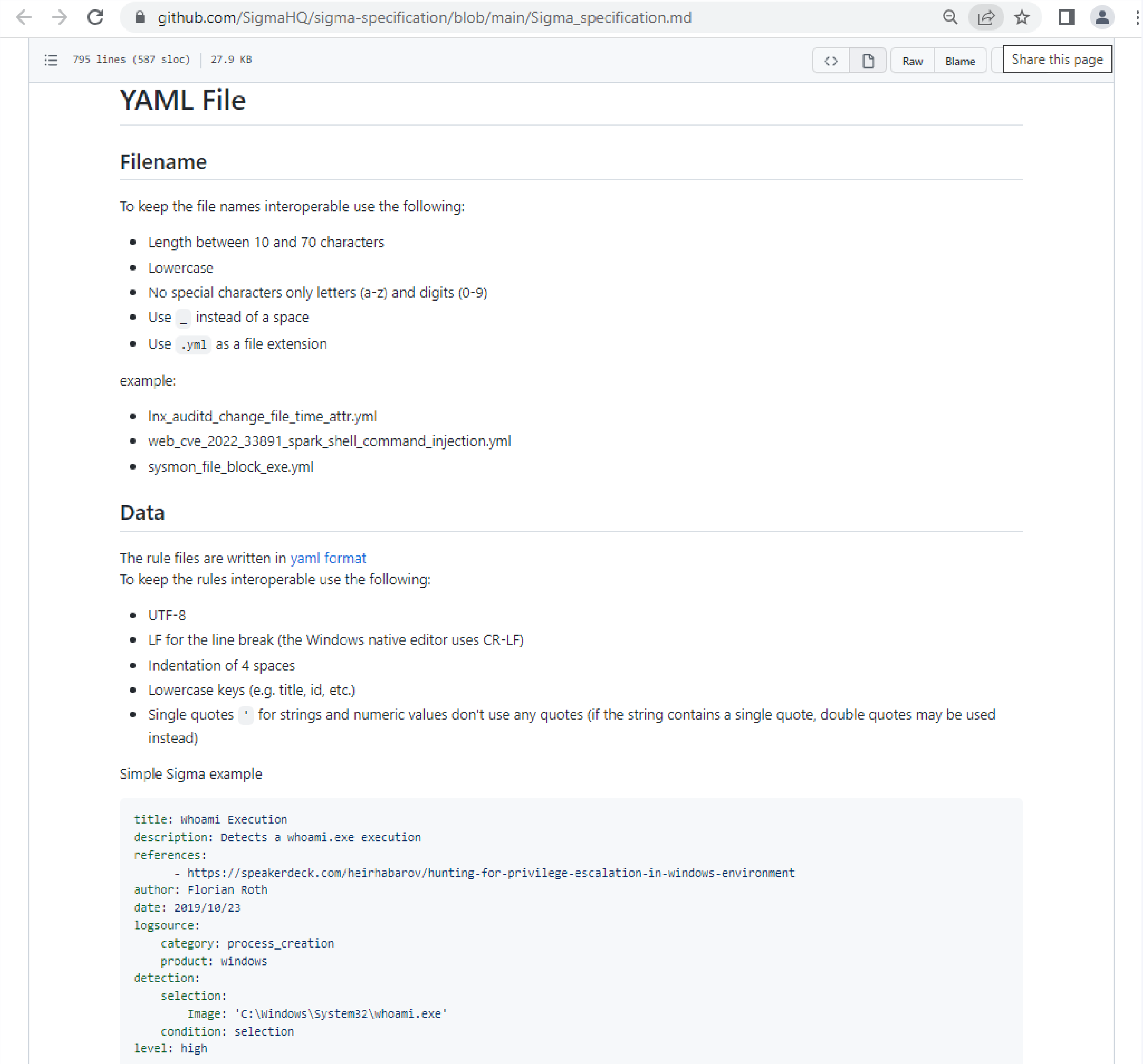
Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts 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

Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...


github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md
795 lines (587 sloc) | 27.9 KB
Raw
Blame
Share this page

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

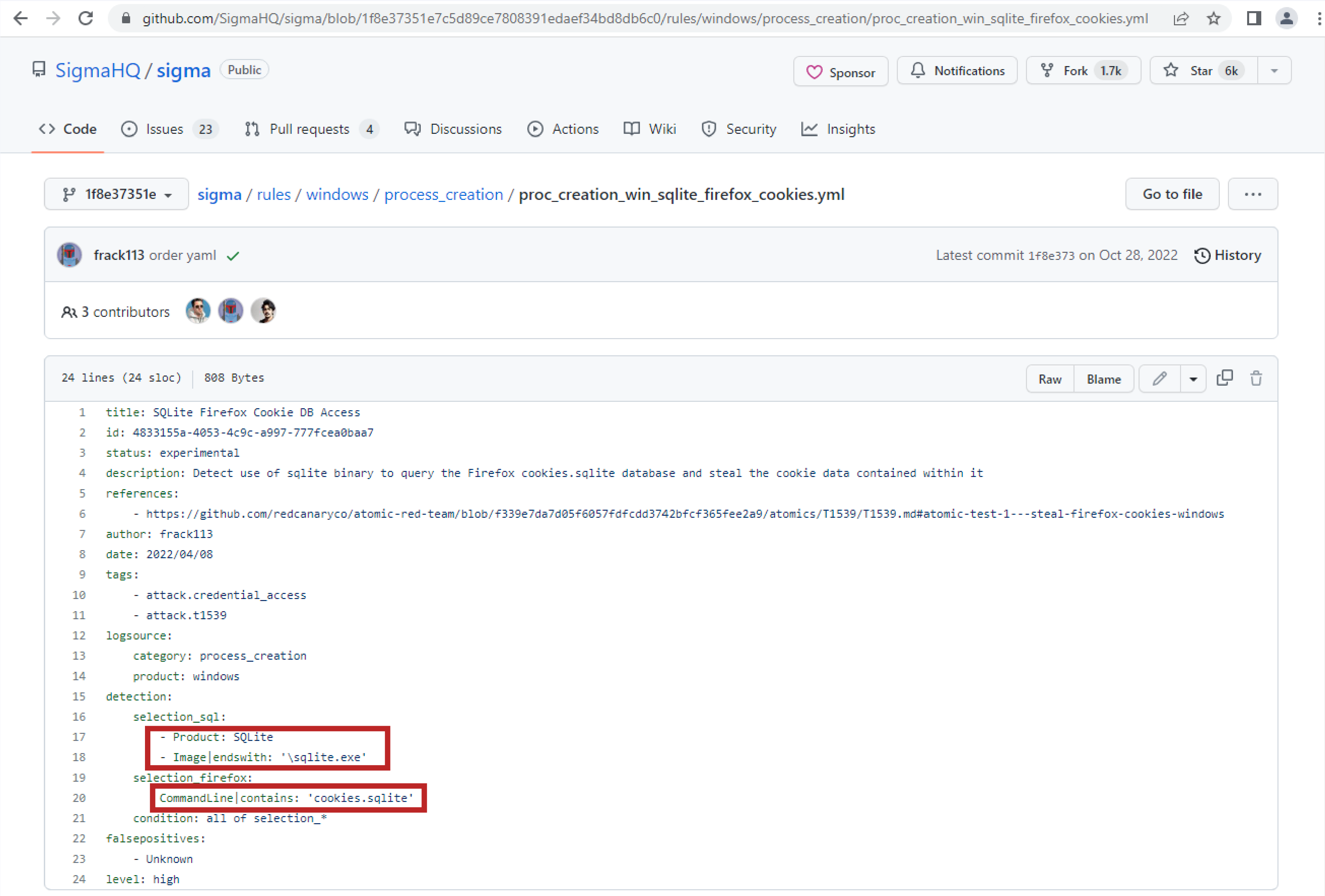
Data

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
```



github.com/SigmaHQ/sigma/blob/1f8e37351e7c5d89ce7808391edaef34bd8db6c0/rules/windows/process_creation/proc_creation_win_sqlite_firefox_cookies.yml
SigmaHQ / sigma
Public
Sponsor
Notifications
Fork 1.7k
Star 6k
Code
Issues 23
Pull requests 4
Discussions
Actions
Wiki
Security
Insights
1f8e37351e
sigma / rules / windows / process_creation / proc_creation_win_sqlite_firefox_cookies.yml
Go to file
History
3 contributors
Raw
Blame

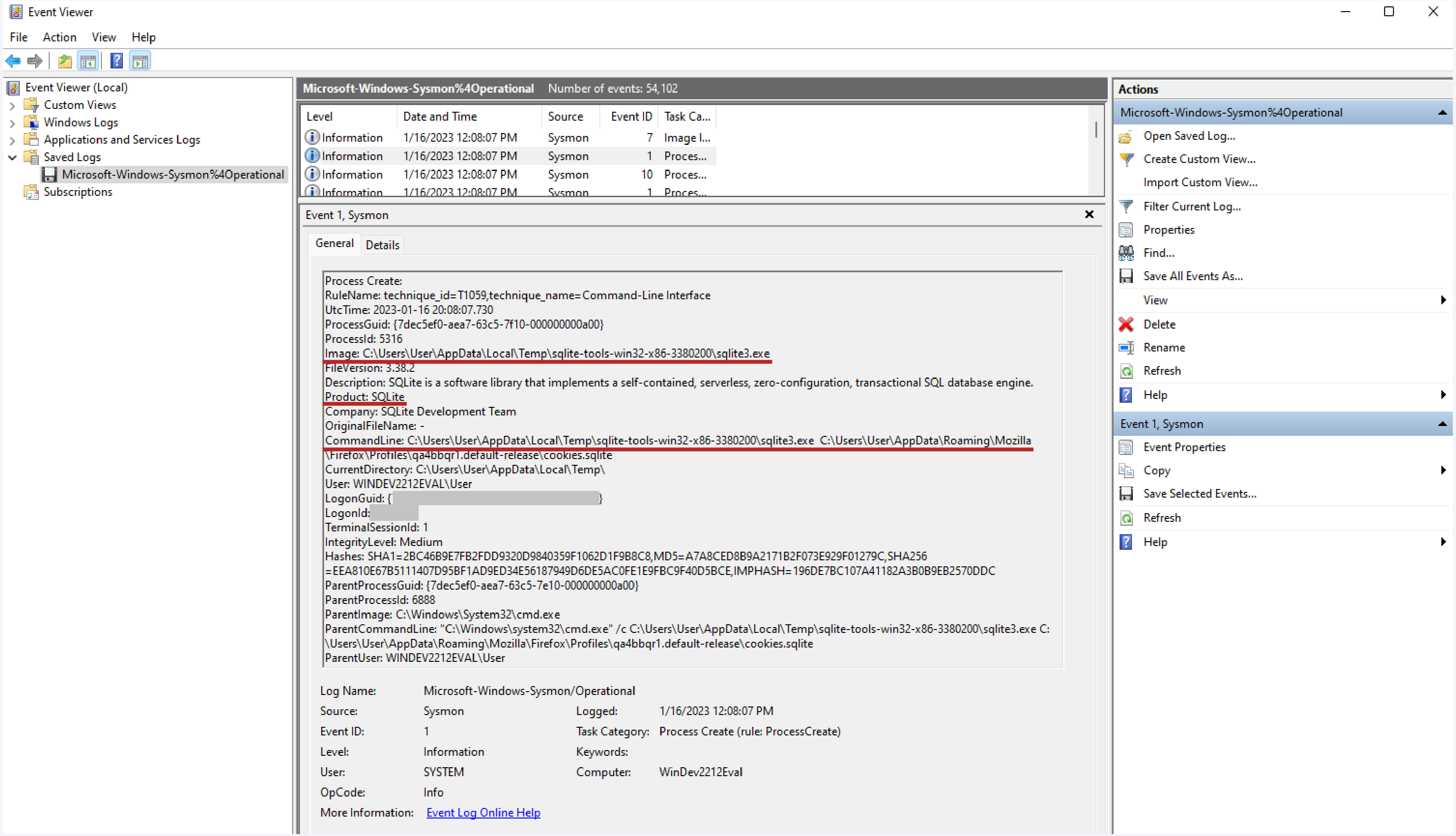
frack113 order yaml ✓

Latest commit 1f8e373 on Oct 28, 2022

24 lines (24 sloc) | 808 Bytes

```yaml
title: SQLite Firefox Cookie DB Access
id: 4833155a-4053-4c9c-a997-777fcea0baa7
status: experimental
description: Detect use of sqlite binary to query the Firefox cookies.sqlite database and steal the cookie data contained within it
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1539/T1539.md#atomic-test-1---steal-firefox-cookies-windows
author: frack113
date: 2022/04/08
tags:
    - attack.credential_access
    - attack.t1539
logsource:
    category: process_creation
    product: windows
detection:
    selection_sql:
        - Product: SQLite
        - Image|endswith: '\sqlite.exe'
    selection_firefox:
        CommandLine|contains: 'cookies.sqlite'
    condition: all of selection_*
falsepositives:
    - Unknown
level: high
```

TIDAL



Level	Date and Time	Source	Event ID	Task Ca...
Information	1/16/2023 12:08:07 PM	Sysmon	7	Image l...
Information	1/16/2023 12:08:07 PM	Sysmon	1	Proces...
Information	1/16/2023 12:08:07 PM	Sysmon	10	Proces...
Information	1/16/2023 12:08:07 PM	Sysmon	1	Proces...

```
Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime: 2023-01-16 20:08:07.730
ProcessGuid: {7dec5ef0-aea7-63c5-7f10-000000000a00}
ProcessId: 5316
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\Roaming\Mozilla
\Firefox\Profiles\qa4bbqr1.default-release\cookies.sqlite
CurrentDirectory: C:\Users\User\AppData\Local\Temp\
User: WINDEV2212EVAL\User
LogonGuid: {[redacted]}
LogonId:[redacted]
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=2BC46B9E7FB2FDD9320D9840359F1062D1F9B8C8,MD5=A7A8CED8B9A2171B2F073E929F01279C,SHA256
=EEA810E67B5111407D95BF1AD9ED34E56187949D6DE5AC0FE1E9FBC9F40D5BCE,IMPHASH=196DE7BC107A41182A3B0B9EB2570DDC
ParentProcessGuid: {7dec5ef0-aea7-63c5-7e10-000000000a00}
ParentProcessId: 6888
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\Roaming\Mozilla\Firefox\Profiles\qa4bbqr1.default-release\cookies.sqlite
ParentUser: WINDEV2212EVAL\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	1/16/2023 12:08:07 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		

Real results!

TIDAL

#goals

#goals

#goals

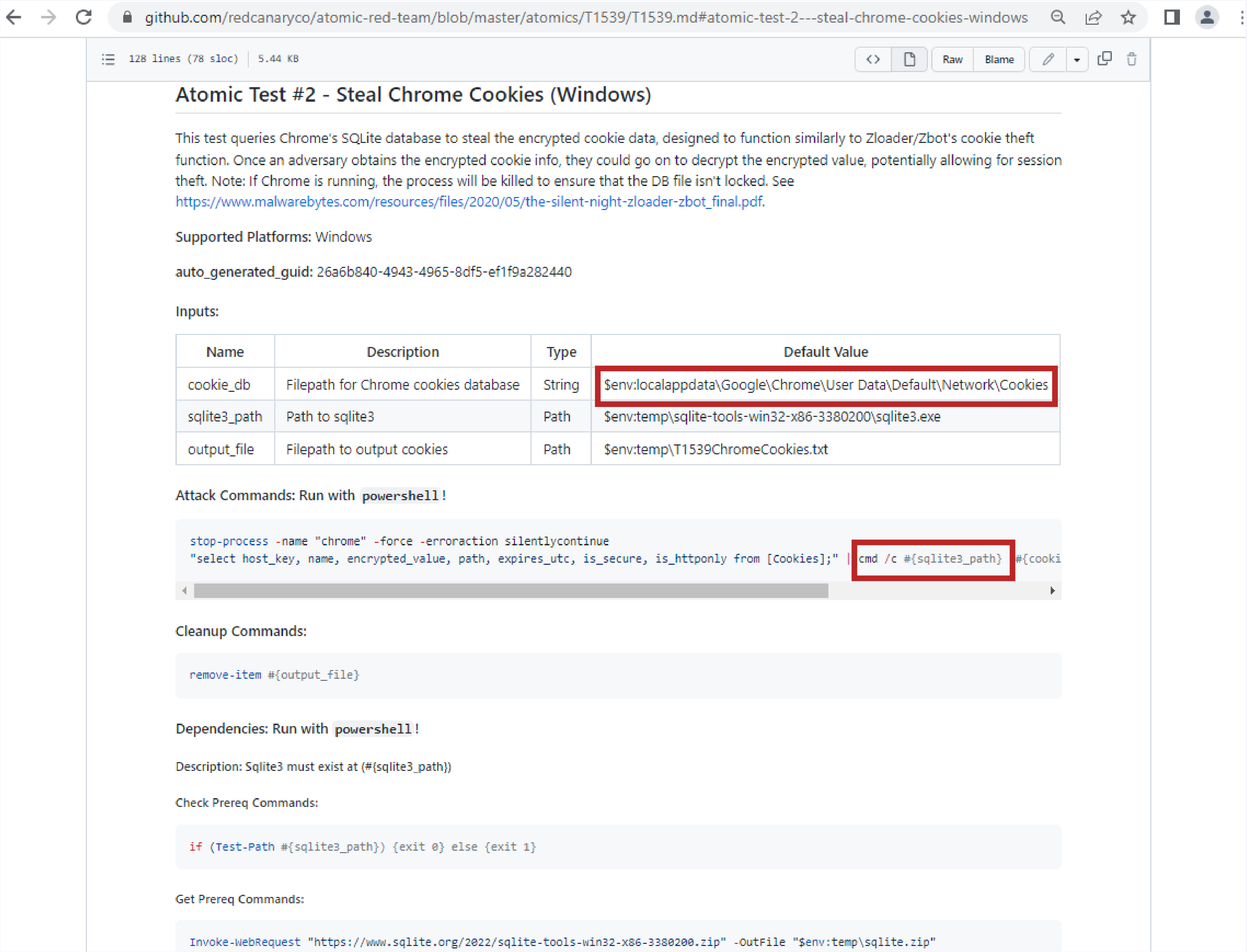
Let’s build something new!
With adversary intelligence

#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})

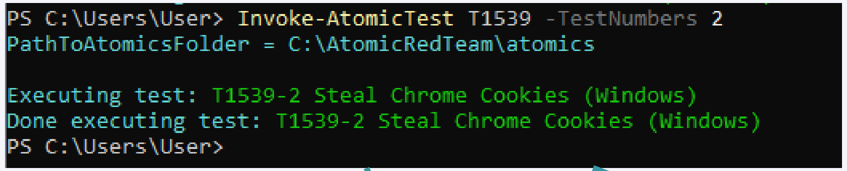
Check Prereq Commands:

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

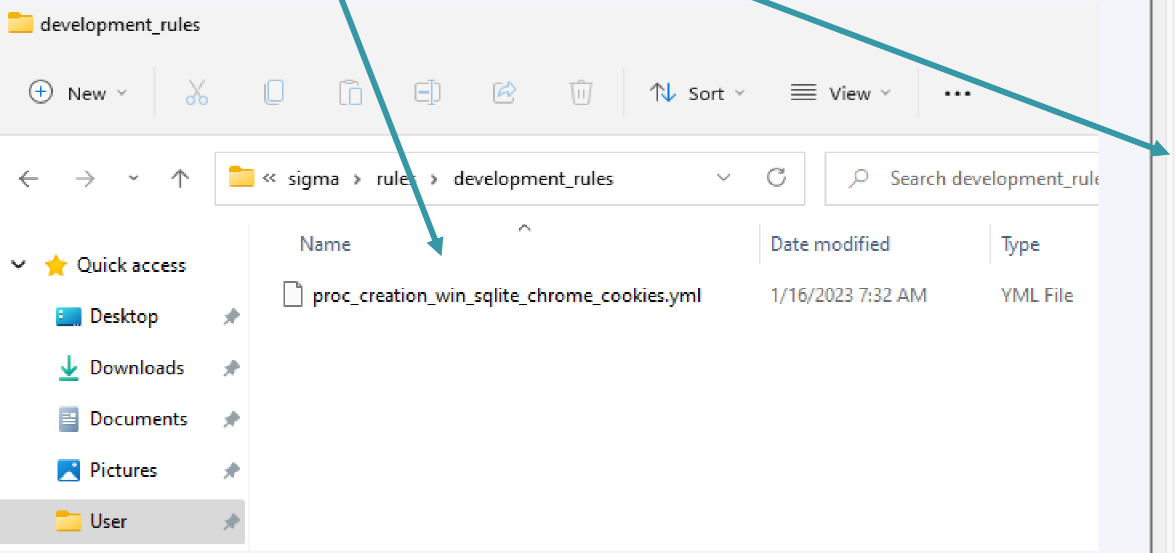
Get Prereq Commands:

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

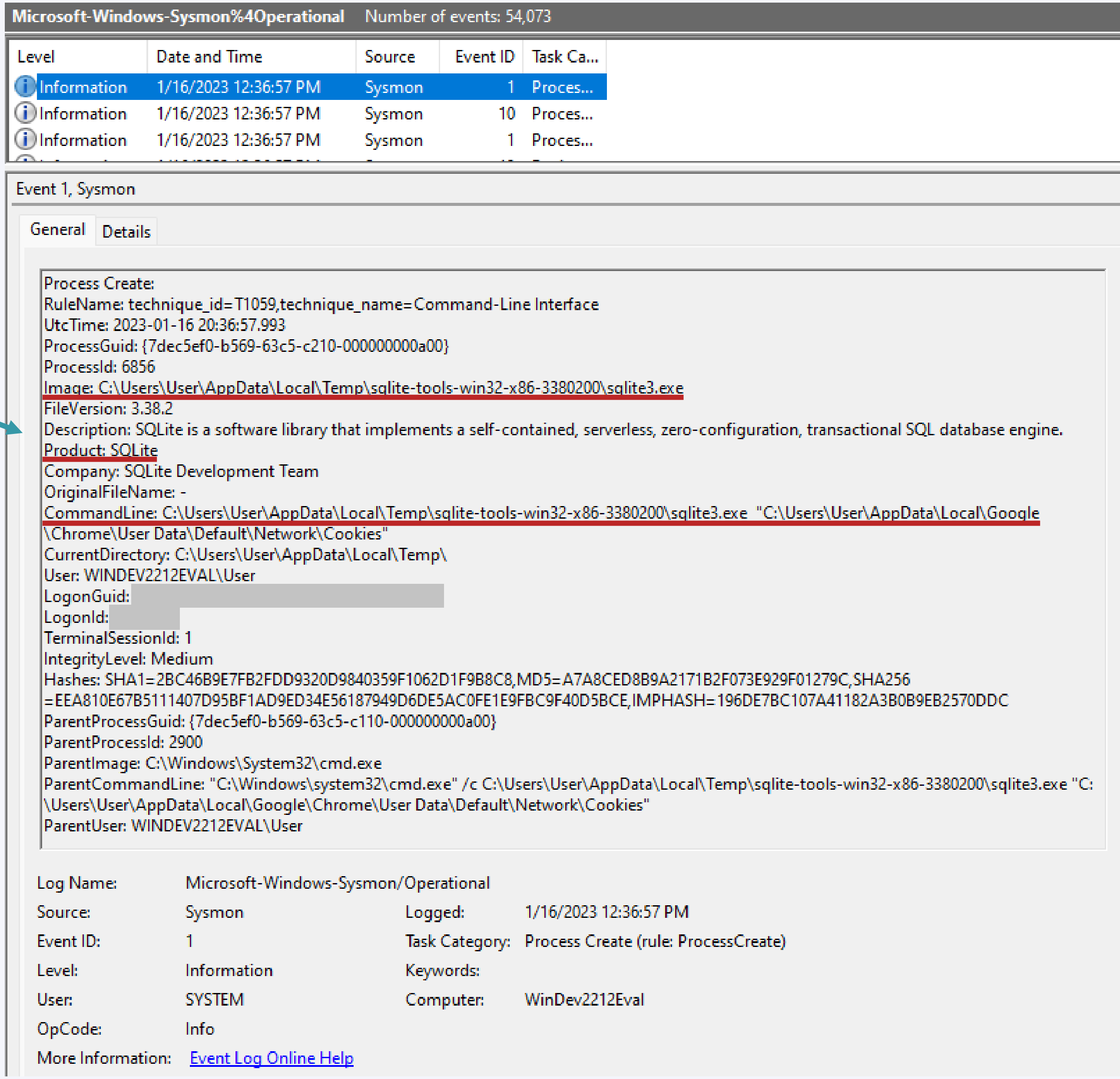
TIDAL



```
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>
```



Name	Date modified	Type
proc_creation_win_sqlite_chrome_cookies.yml	1/16/2023 7:32 AM	YML File



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

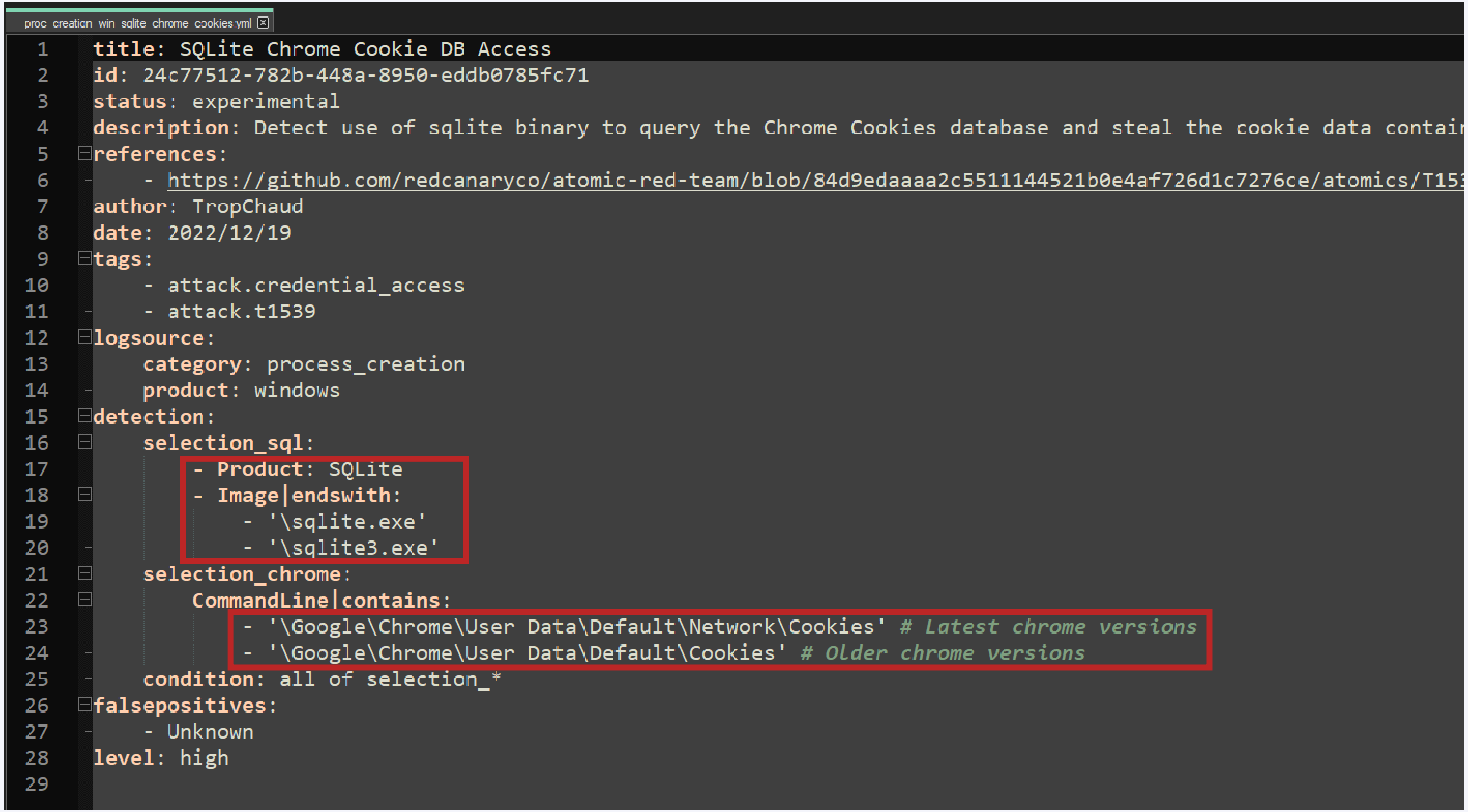
Level	Date and Time	Source	Event ID	Task Ca...
Information	1/16/2023 12:36:57 PM	Sysmon	1	Proces...
Information	1/16/2023 12:36:57 PM	Sysmon	10	Proces...
Information	1/16/2023 12:36:57 PM	Sysmon	1	Proces...

Event 1, Sysmon

```
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: [redacted]
LogonId: [redacted]
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		

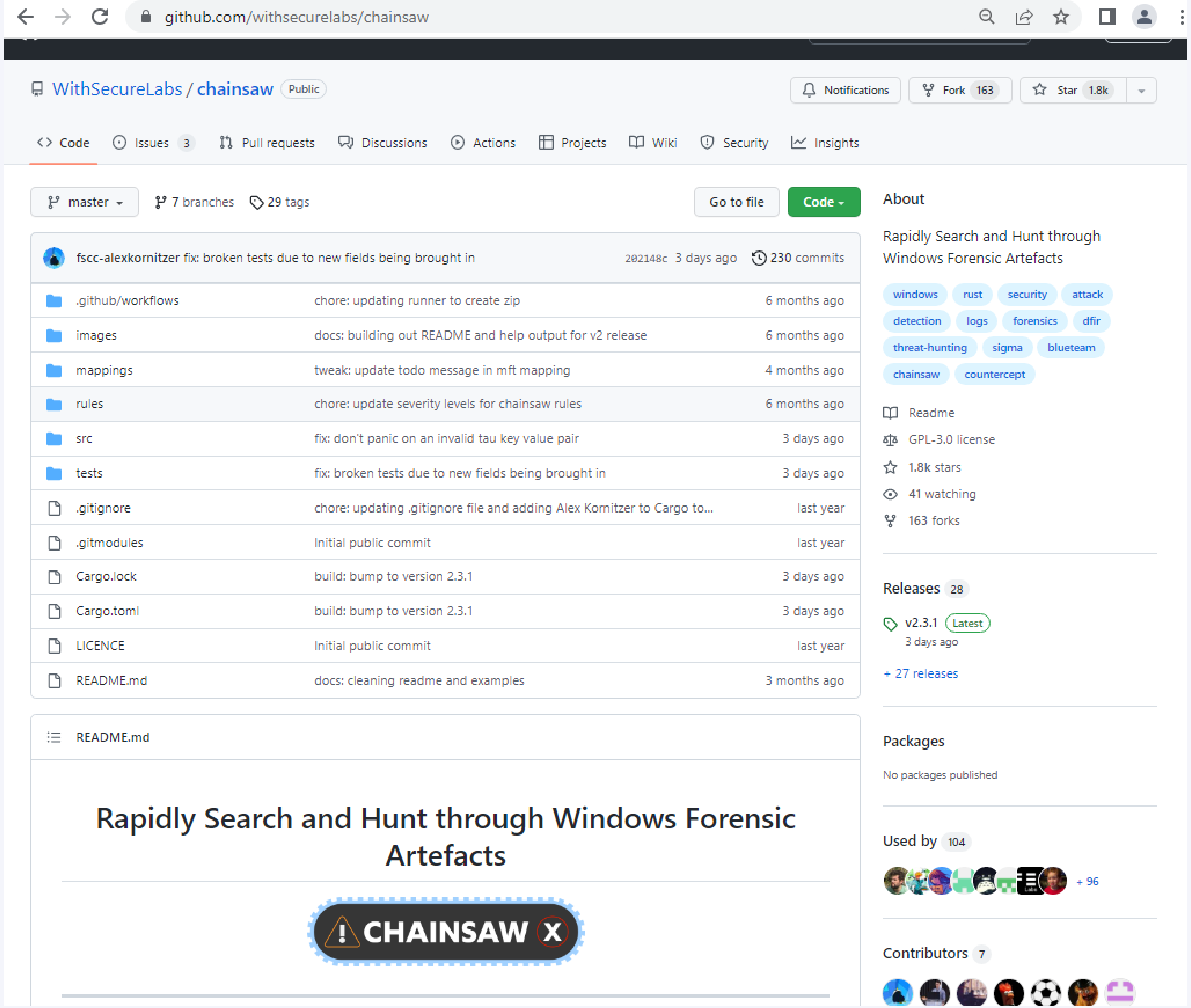
TIDAL



```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 contai
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T153
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
```

Real-Time, Straightforward Detection With Chainsaw

TIDAL



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

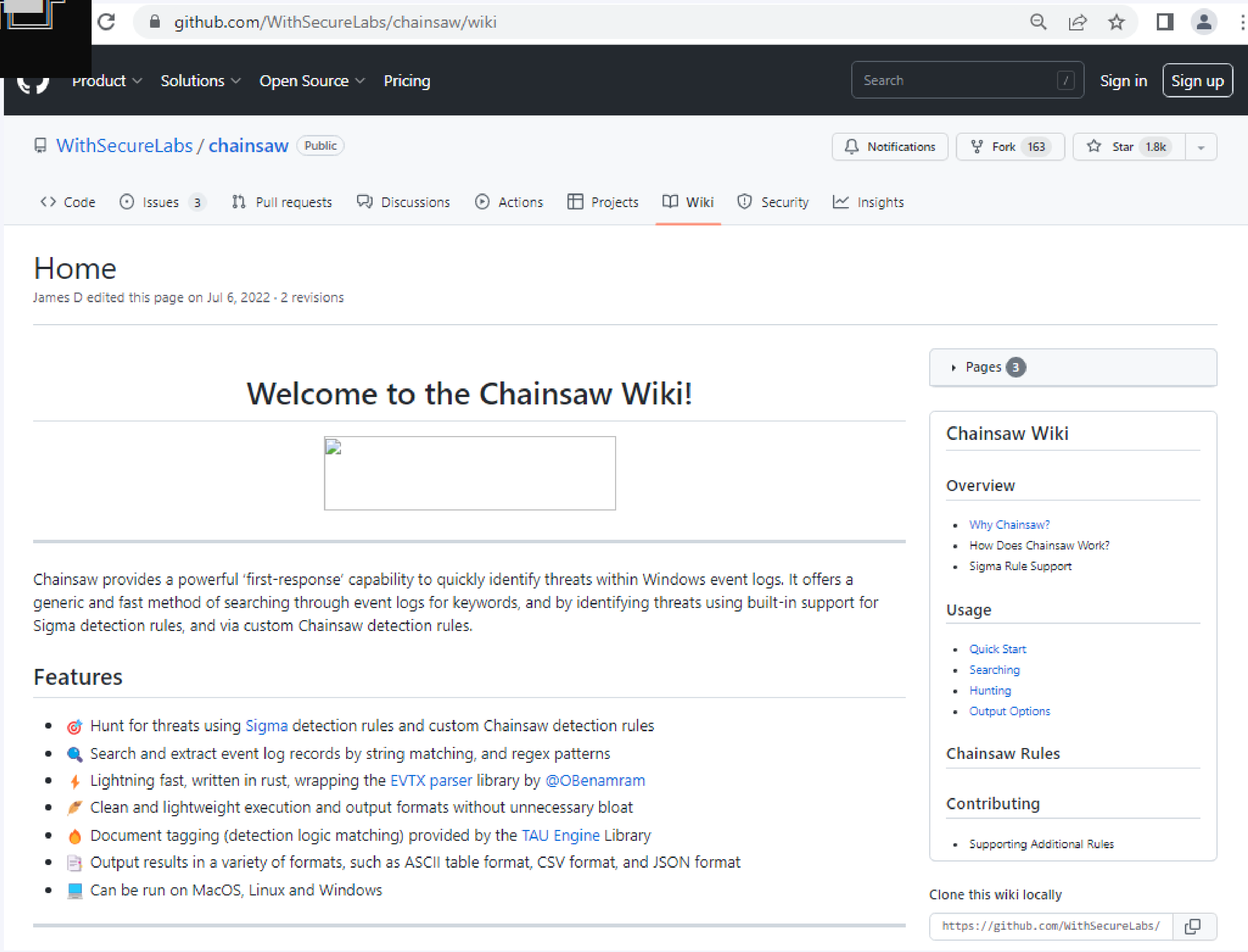
No packages published

Used by 104

+ 96

Contributors 7

```
CHAINSAW
   By Countercept (@FranticTyping, @AlexKornitzer)
```



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

Chainsaw Wiki

Overview

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

Usage

- Quick Start
- Searching
- Hunting
- Output Options

Chainsaw Rules

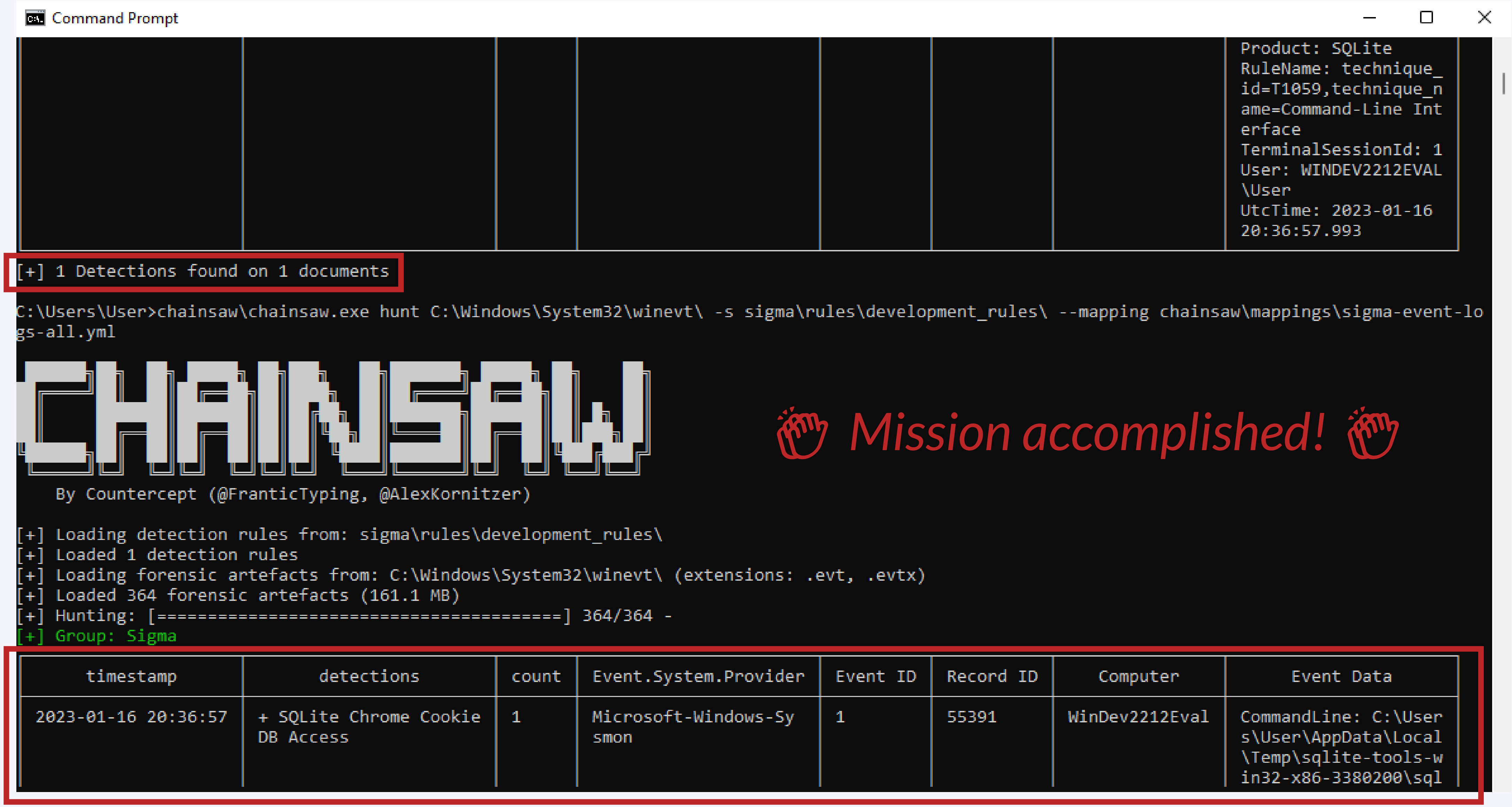
Contributing

- Supporting Additional Rules

Clone this wiki locally

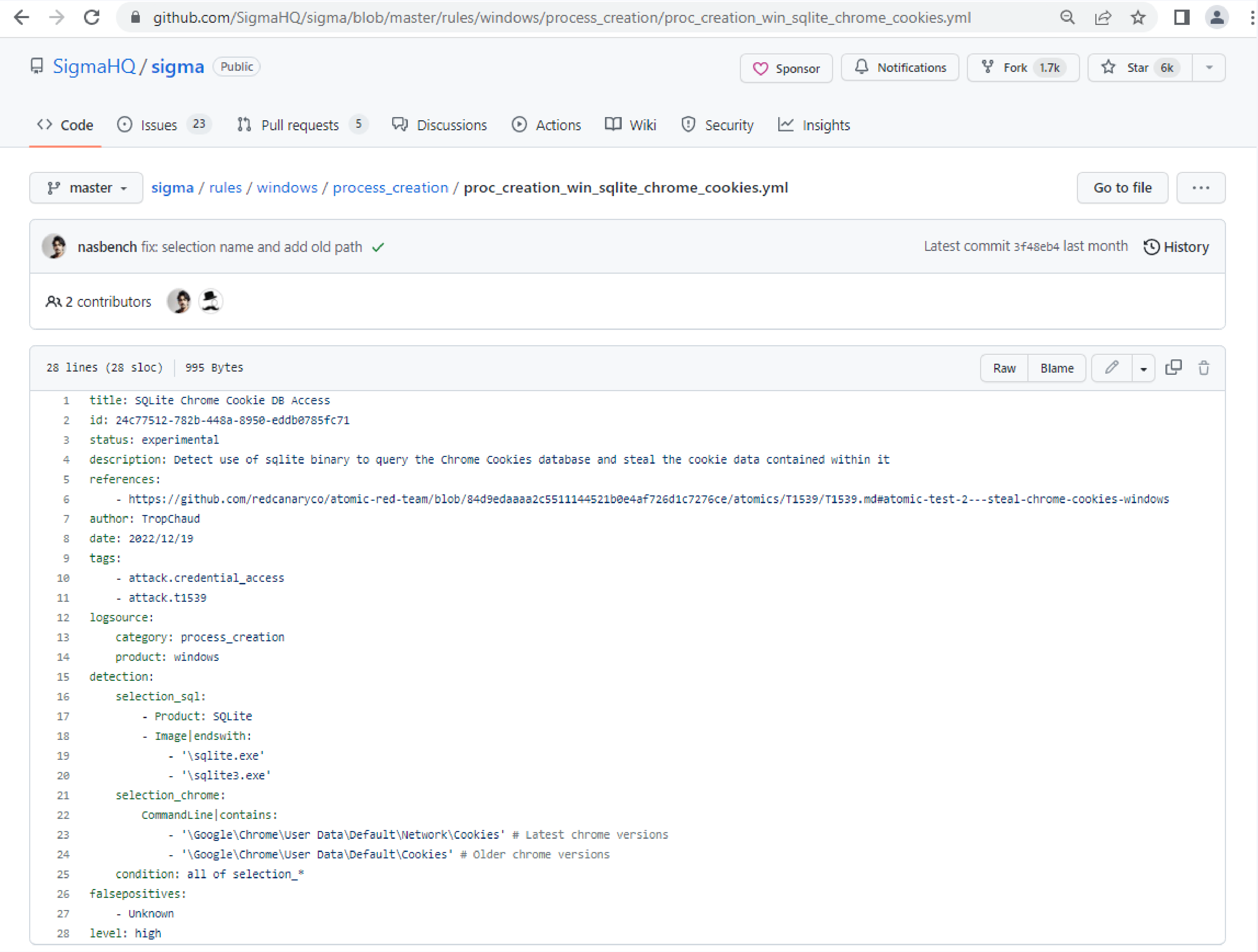
`https://github.com/WithSecureLabs/`

TIDAL



```
│          │           │     │           │        │         │          │ Product: SQLite       │
│          │           │     │           │        │         │          │ RuleName: technique_  │
│          │           │     │           │        │         │          │ id=T1059,technique_n  │
│          │           │     │           │        │         │          │ ame=Command-Line Int  │
│          │           │     │           │        │         │          │ erface                │
│          │           │     │           │        │         │          │ TerminalSessionId: 1  │
│          │           │     │           │        │         │          │ User: WINDEV2212EVAL  │
│          │           │     │           │        │         │          │ \User                 │
│          │           │     │           │        │         │          │ UtcTime: 2023-01-16   │
│          │           │     │           │        │         │          │ 20:36:57.993          │

[+] 1 Detections found on 1 documents

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

    By Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: sigma\rules\development_rules\
[+] Loaded 1 detection rules
[+] Loading forensic artefacts from: C:\Windows\System32\winevt\ (extensions: .evt, .evtx)
[+] Loaded 364 forensic artefacts (161.1 MB)
[+] Hunting: [========================================] 364/364 -
[+] Group: Sigma
│      timestamp      │       detections        │ count │ Event.System.Provider │ Event ID │ Record ID │    Computer     │      Event Data       │
│ 2023-01-16 20:36:57 │ + SQLite Chrome Cookie  │ 1     │ Microsoft-Windows-Sy  │ 1        │ 55391     │ WinDev2212Eval  │ CommandLine: C:\User  │
│                     │ DB Access               │       │ smon                  │          │           │                 │ s\User\AppData\Local  │
│                     │                         │       │                       │          │           │                 │ \Temp\sqlite-tools-w  │
│                     │                         │       │                       │          │           │                 │ in32-x86-3380200\sql  │
```

👏 *Mission accomplished!* 👏


github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_sqlite_chrome_cookies.yml
SigmaHQ / sigma Public
Sponsor
Notifications
Fork 1.7k
Star 6k
Code
Issues 23
Pull requests 5
Discussions
Actions
Wiki
Security
Insights
master
sigma / rules / windows / process_creation / proc_creation_win_sqlite_chrome_cookies.yml
Go to file
Latest commit 3f48eb4 last month
History
2 contributors
28 lines (28 sloc) | 995 Bytes
Raw
Blame

nasbench fix: selection name and add old path ✓

```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 contained within it
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T1539/T1539.md#atomic-test-2---steal-chrome-cookies-windows
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

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