

Building & Validating Detections with Adversary Intelligence

BsidesCharm Workshop

April 30, 2023

Scott Small, Director of Cyber Threat Intelligence



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

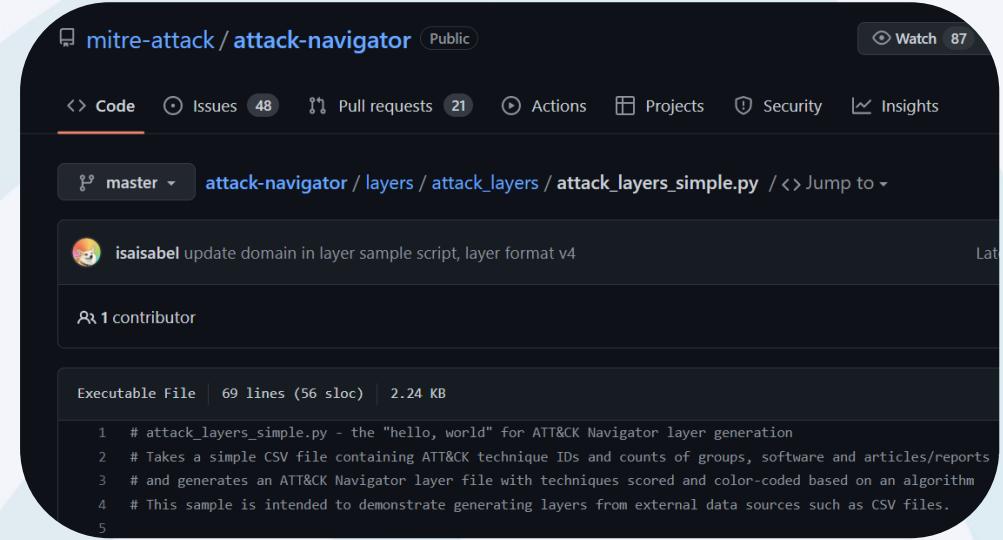
Primary focus: *Exposure to many tools & resources*

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

See handout if you want to go hands-on

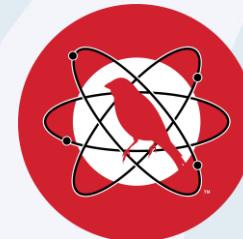
Start big downloads (VirtualBox environment) now

At least one break (aiming to end early)



A screenshot of a GitHub repository page for 'mitre-attack / attack-navigator'. The repository has 48 issues, 21 pull requests, and 87 watchers. The current branch is 'master'. The file 'attack_layers_simple.py' is shown, which is an executable file with 69 lines (56 sloc) and 2.24 KB in size. The code is a script for generating ATT&CK Navigator layers from CSV files.

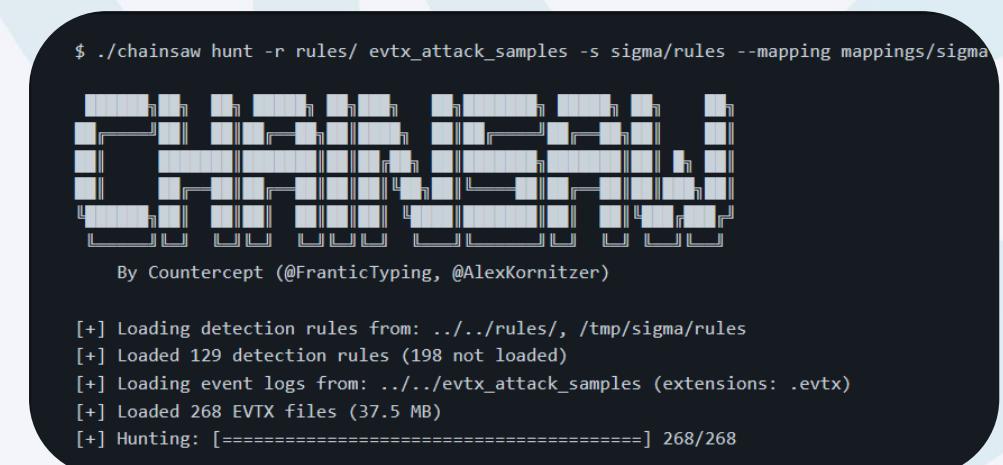
```
1 # attack_layers_simple.py - the "hello, world" for ATT&CK Navigator layer generation
2 # Takes a simple CSV file containing ATT&CK technique IDs and counts of groups, software and articles/reports
3 # and generates an ATT&CK Navigator layer file with techniques scored and color-coded based on an algorithm
4 # This sample is intended to demonstrate generating layers from external data sources such as CSV files.
5
```



Atomic Red Team



Sigma Public Repository



A terminal window showing the execution of the 'chainsaw' tool. The command run is \$./chainsaw hunt -r rules/ evtx_attack_samples -s sigma/rules --mapping mappings/sigma. The output shows the tool loading detection rules and event logs, and performing a hunting operation on EVTX files.

```
$ ./chainsaw hunt -r rules/ evtx_attack_samples -s sigma/rules --mapping mappings/sigma
[+] Loading detection rules from: ../../rules/, /tmp/sigma/rules
[+] Loaded 129 detection rules (198 not loaded)
[+] Loading event logs from: ../../evtx_attack_samples (extensions: .evtx)
[+] Loaded 268 EVTIX files (37.5 MB)
[+] Hunting: [=====] 268/268
```

whoami

Career intelligence researcher & analyst

- Purple teamer
- OSINT + data viz

Expanding my “technical” skill & understanding through practical applications

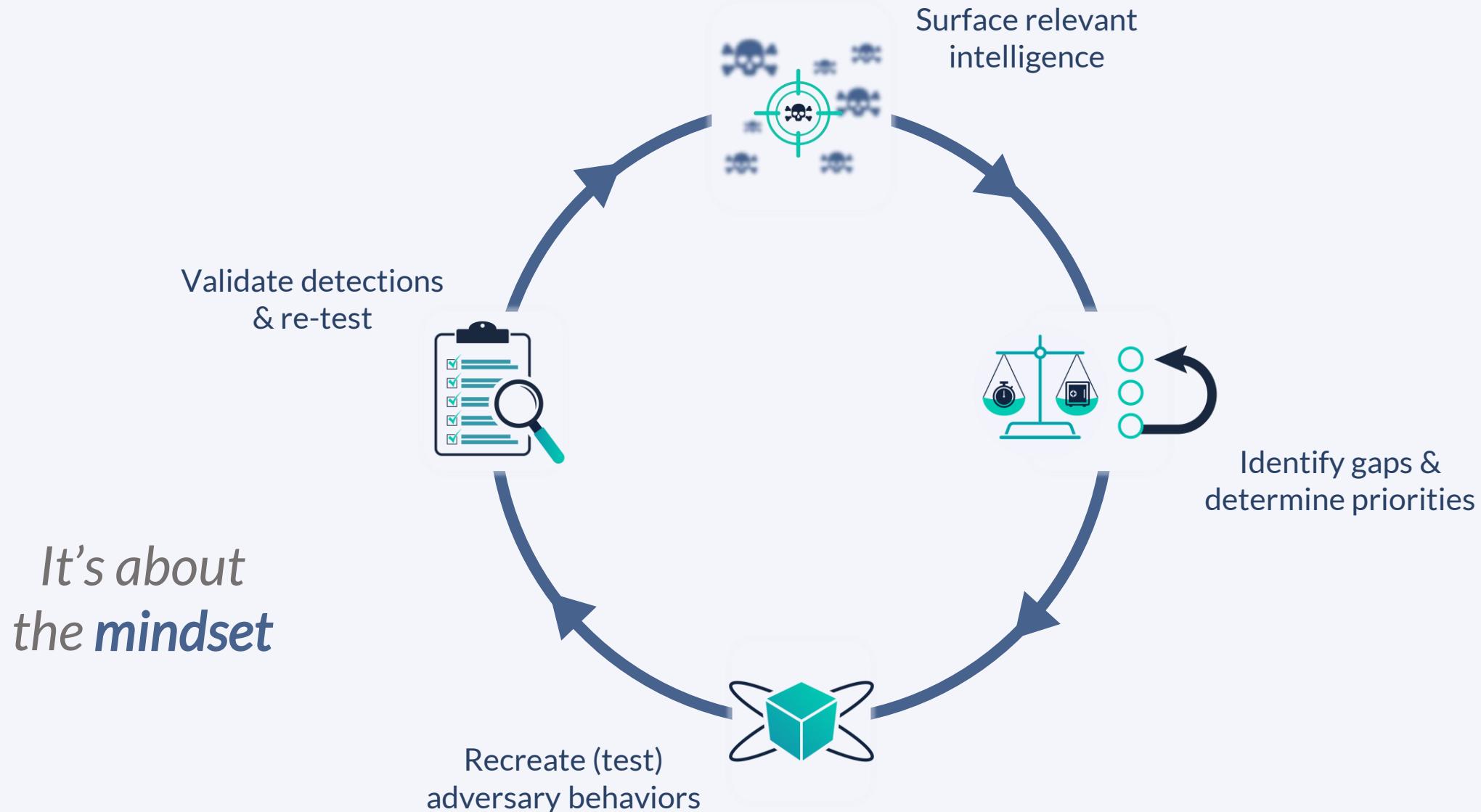
- MITRE ATT&CK®, Atomics, Sigma, logging

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*



Threat-Informed Detection Validation (Micro Purple Teaming)



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

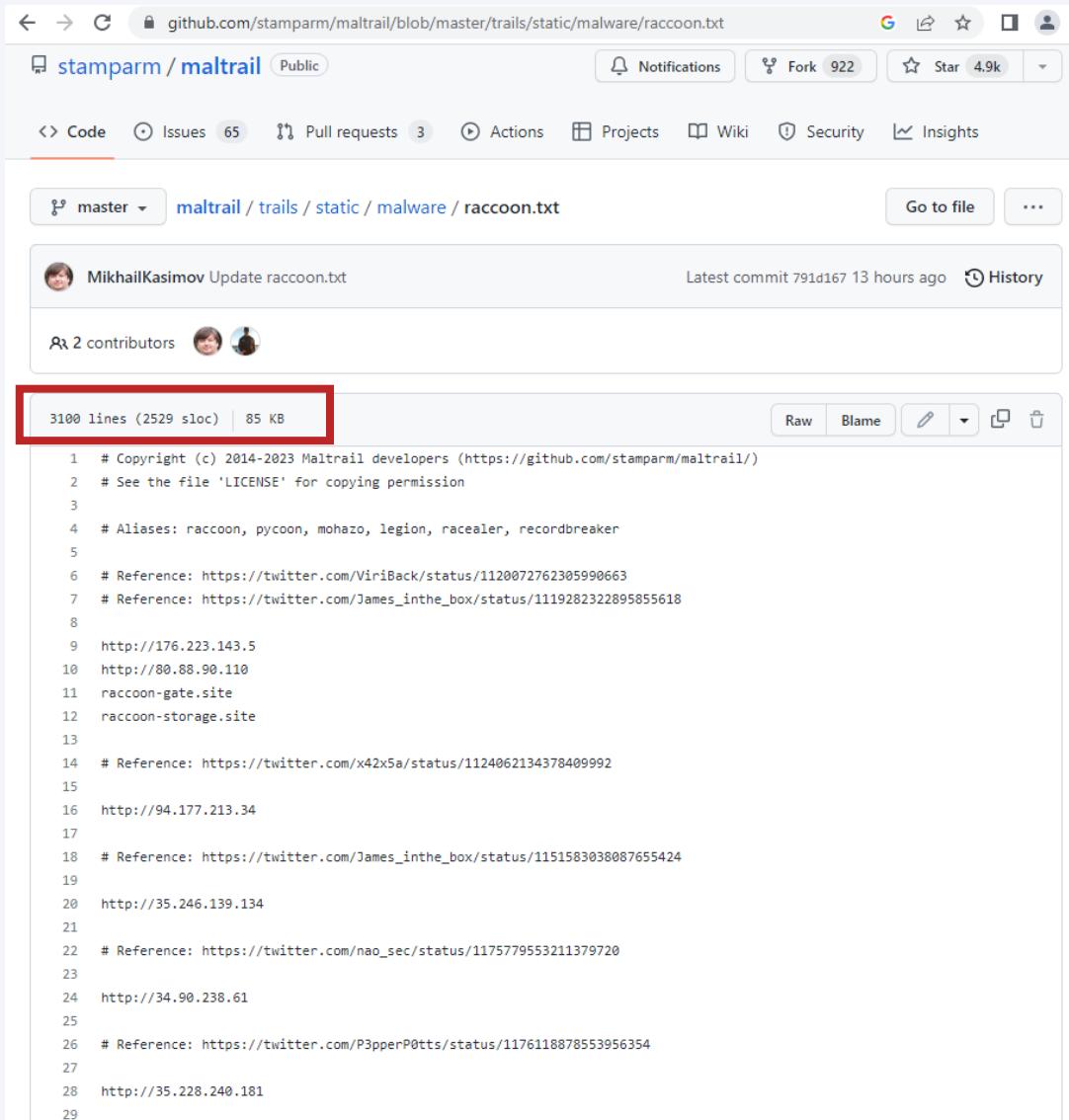
A step towards “proactive”?

Gateway & springboard for further skill development

Not a silver bullet (nothing is)

The Value of TTP Intelligence

IOCs | TTPs



A screenshot of a GitHub repository page for 'stamparm / maltrail'. The page shows the 'Code' tab selected, with a file named 'raccoon.txt' open. The file content is a list of URLs, starting with '# Copyright (c) 2014-2023 Maltrail developers (<https://github.com/stamparm/maltrail/>)'. A red box highlights the first line of the file content.

```
1 # Copyright (c) 2014-2023 Maltrail developers (https://github.com/stamparm/maltrail/)
2 # See the file 'LICENSE' for copying permission
3
4 # Aliases: raccoon, pycoon, mohazo, legion, racealer, recordbreaker
5
6 # Reference: https://twitter.com/ViriBack/status/1120072762305990663
7 # Reference: https://twitter.com/James\_inthe\_box/status/1119282322895855618
8
9 http://176.223.143.5
10 http://80.88.90.110
11 raccoon-gate.site
12 raccoon-storage.site
13
14 # Reference: https://twitter.com/x42x5a/status/1124062134378409992
15
16 http://94.177.213.34
17
18 # Reference: https://twitter.com/James\_inthe\_box/status/1151583038087655424
19
20 http://35.246.139.134
21
22 # Reference: https://twitter.com/nao\_sec/status/1175779553211379720
23
24 http://34.90.238.61
25
26 # Reference: https://twitter.com/P3pperP0tts/status/1176118878553956354
27
28 http://35.228.240.181
29
```

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



A Serious Threat for Enterprises Infostealer Threat Landscape



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

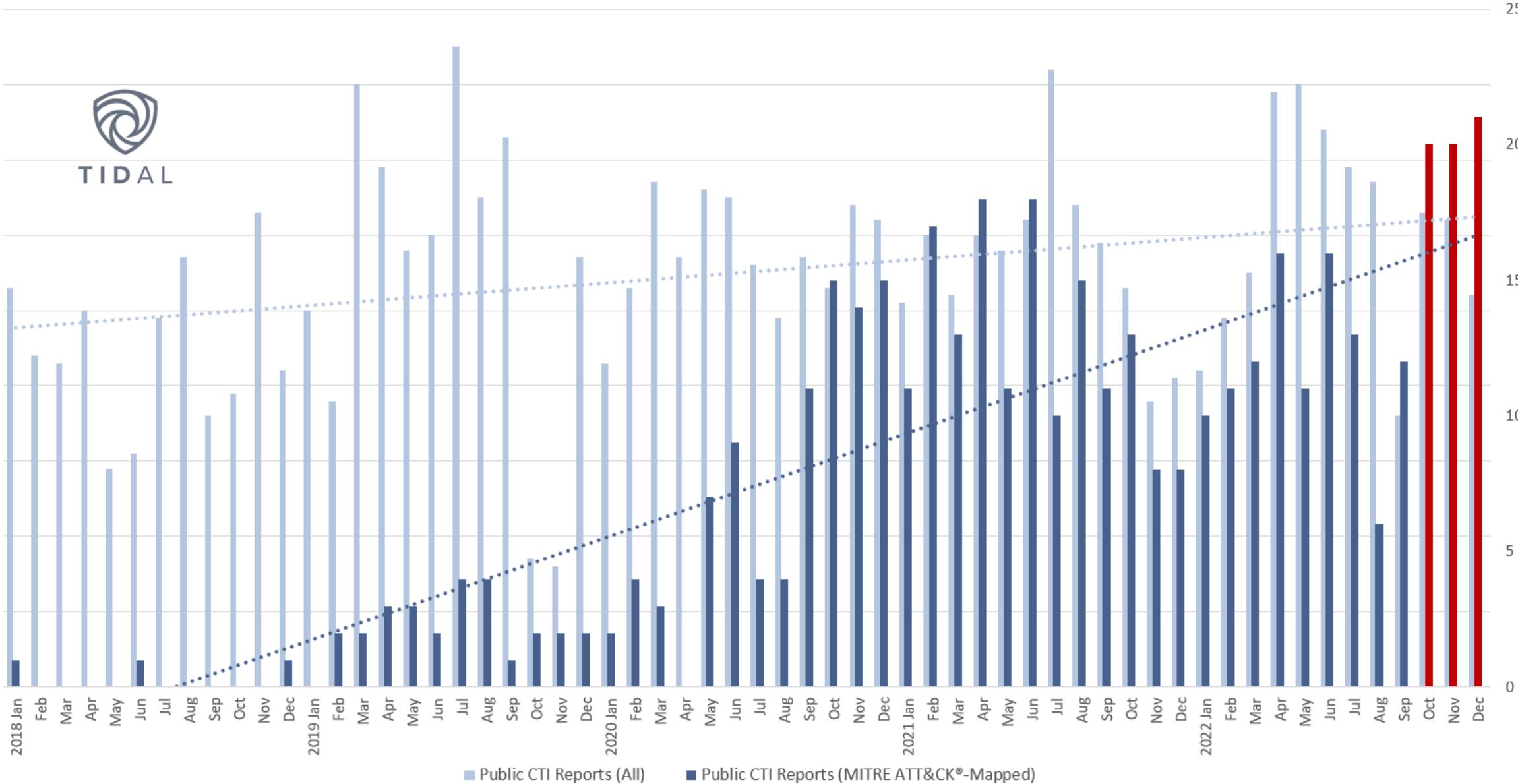
Pose a rising threat to “high-value” targets, including small, medium, & large businesses & organizations

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

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

Increased Opportunity



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

Communication/Messaging
Remote Access
Password Management
Programming
Browsers/Updates

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



SEKOIA.IO | Blog

Discover SEKOIA.IO solutions English

Blogpost

Aurora: a rising stealer flying under the radar

SEKOIA.IO analysed Aurora in depth and share the results of our investigation in this article.



Threat & Detection Research Team
November 21 2022

2183

MALWARE bazaar by ABUSE^{cty}

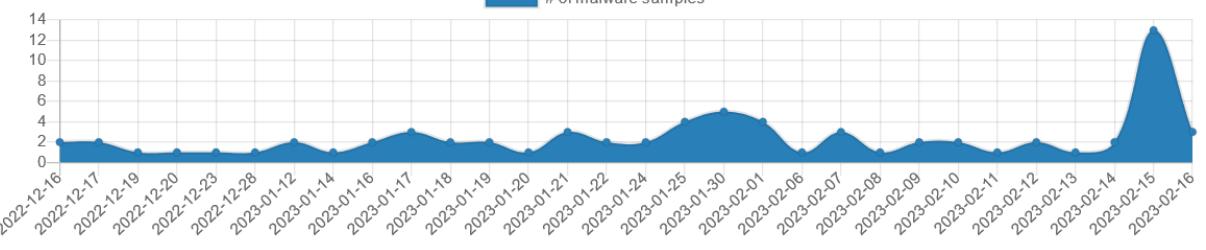
Tag: **AuroraStealer** Alert

Firstseen: 2022-11-24 18:42:41 UTC

Lastseen: 2023-02-16 03:50:17 UTC

Sightings: 88

of malware samples



Date	# of malware samples
2022-12-16	2
2022-12-17	1
2022-12-19	1
2022-12-20	1
2022-12-23	1
2022-12-28	1
2023-01-12	2
2023-01-14	2
2023-01-16	3
2023-01-17	3
2023-01-18	3
2023-01-19	3
2023-01-20	3
2023-01-21	3
2023-01-24	3
2023-01-30	5
2023-02-01	3
2023-02-06	3
2023-02-07	3
2023-02-08	3
2023-02-10	3
2023-02-11	3
2023-02-12	3
2023-02-13	3
2023-02-14	14
2023-02-15	12

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

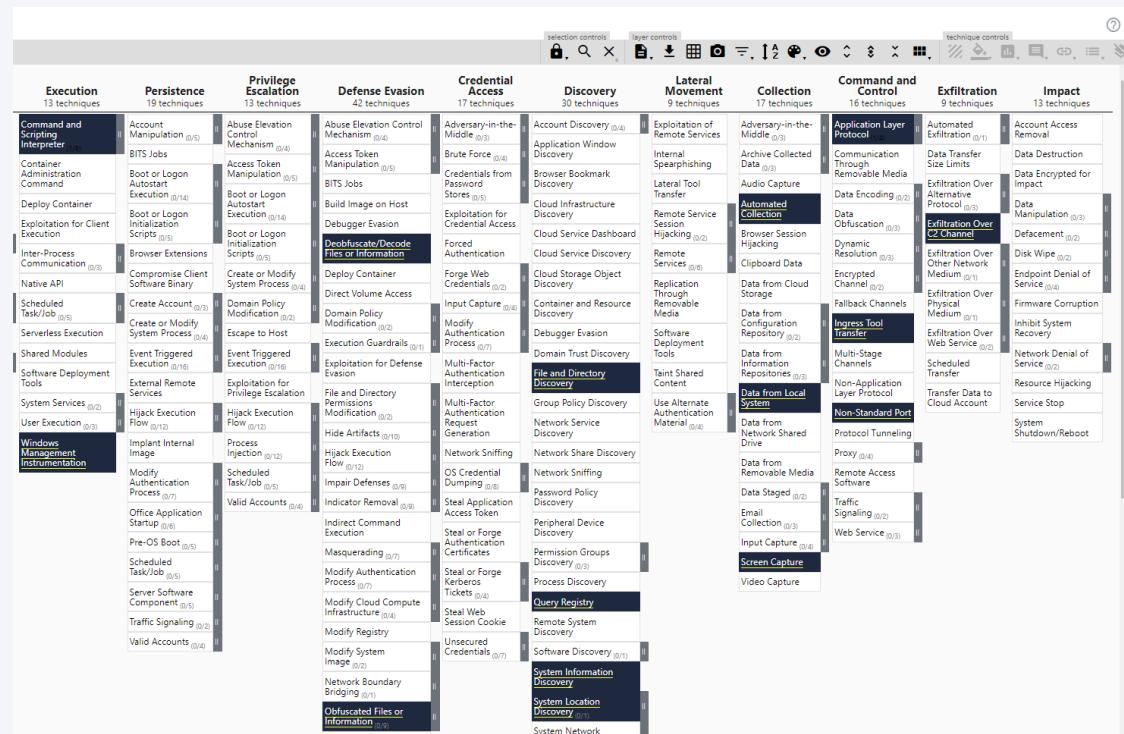
Collection T1113 – Screen Capture

Essential tool in the arsenal!

MITRE ATT&CK script: csv to Navigator json

<https://github.com/mitre-attack/attack-patterns>

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
1  [
2    {
3      "name": "redline_techniques",
4      "versions": {
5        "attack": "11",
6        "navigator": "4.6.1",
7        "layer": "4.3"
8      },
9      "domain": "enterprise-attack",
10     "description": "Heatmap of instances of ATT&CK techniques.",
11     "techniques": [
12       {
13         "techniqueID": "T1566",
14         "score": 1
15       },
16       {
17         "techniqueID": "T1204",
18         "score": 1
19       },
20       {
21         "techniqueID": "T1555",
22         "score": 1
23       },
24       {
25         "techniqueID": "T1539",
26         "score": 1
27       },
28       {
29         "techniqueID": "T1552",
30         "score": 1
31       },
32       {
33         "techniqueID": "T1113",
34         "score": 1
35       },
36       {
37         "techniqueID": "T1087",
38         "score": 1
39       },
40       {
41         "techniqueID": "T1518",
42         "score": 1
43       },
44       {
45         "techniqueID": "T1057",
46         "score": 1
47       }
48     ]
49   }
50 ]
51 
```

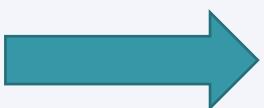
JSON file

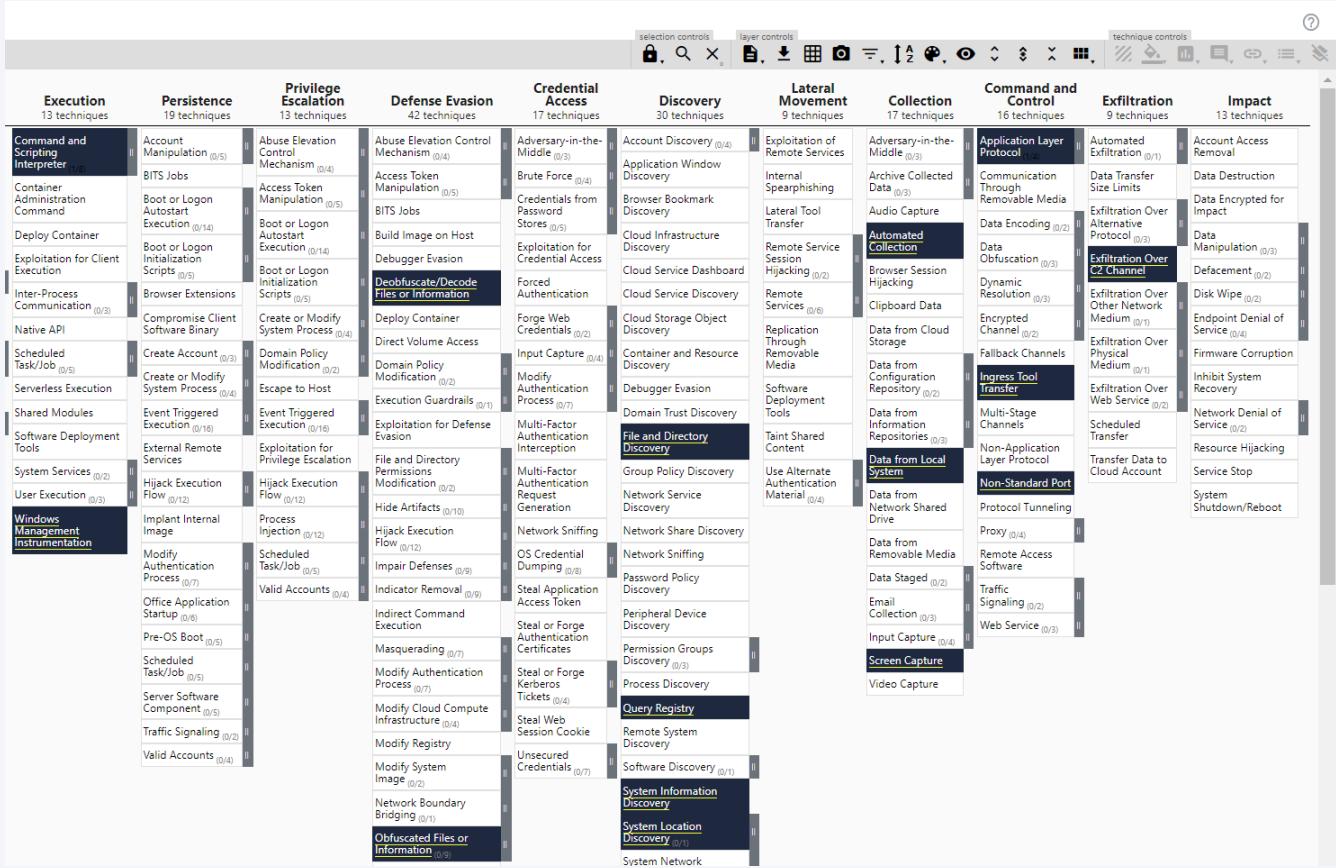
```

redline_techniques.json
1 {
2   "name": "redline_techniques",
3   "versions": {
4     "attack": "11",
5     "navigator": "4.6.1",
6     "layer": "4.3"
7   },
8   "domain": "enterprise-attack",
9   "description": "Heatmap of instances of ATT&CK techniques.",
10  "techniques": [
11    {
12      "techniqueID": "T1566",
13      "score": 1
14    },
15    {
16      "techniqueID": "T1204",
17      "score": 1
18    },
19    {
20      "techniqueID": "T1555",
21      "score": 1
22    },
23    {
24      "techniqueID": "T1539",
25      "score": 1
26    },
27    {
28      "techniqueID": "T1552",
29      "score": 1
30    },
31    {
32      "techniqueID": "T1113",
33      "score": 1
34    },
35    {
36      "techniqueID": "T1087",
37      "score": 1
38    },
39    {
40      "techniqueID": "T1518",
41      "score": 1
42    },
43    {
44      "techniqueID": "T1057",
45    }
46  ]
47}

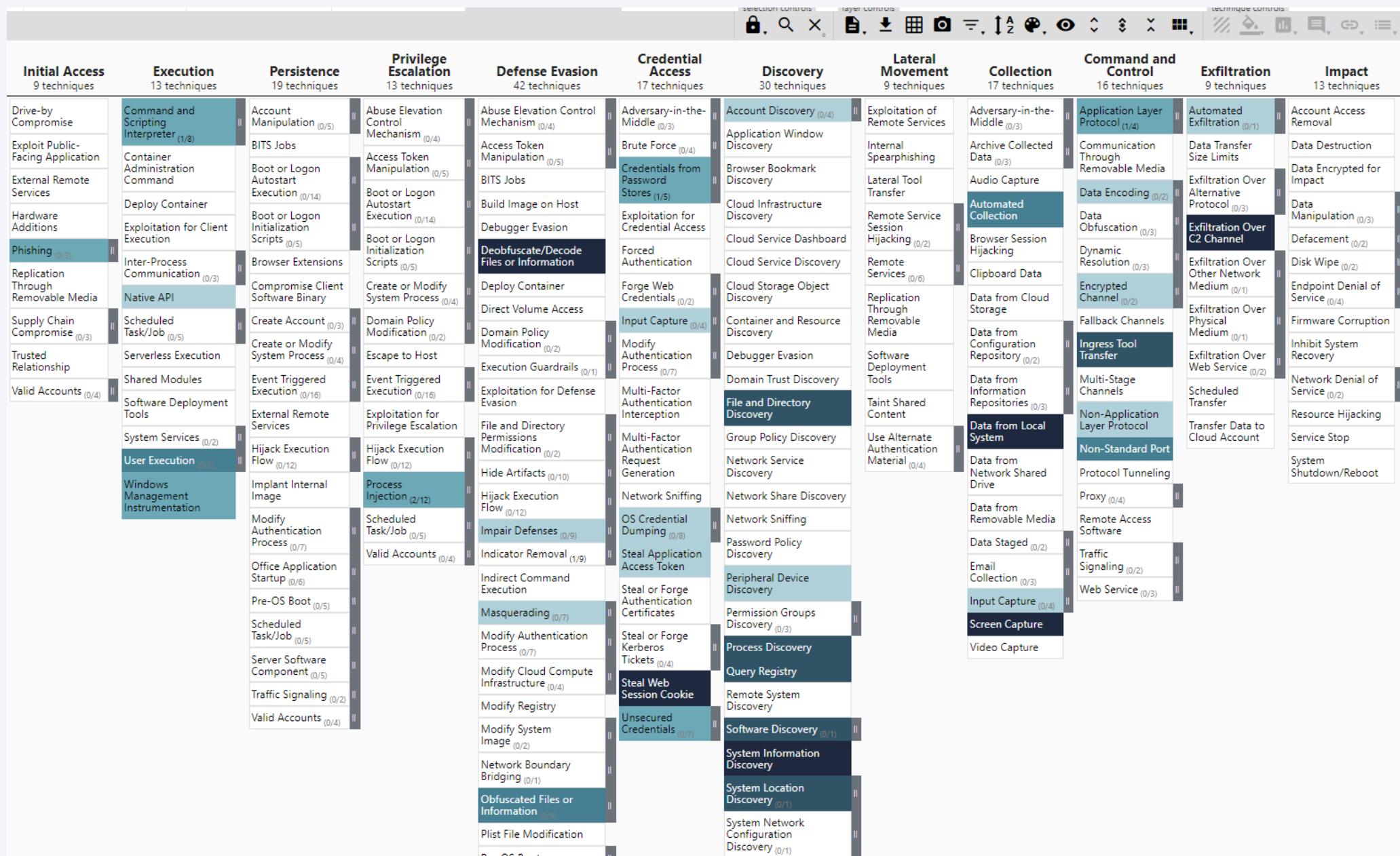
```

JSON file

 Import custom Technique Set

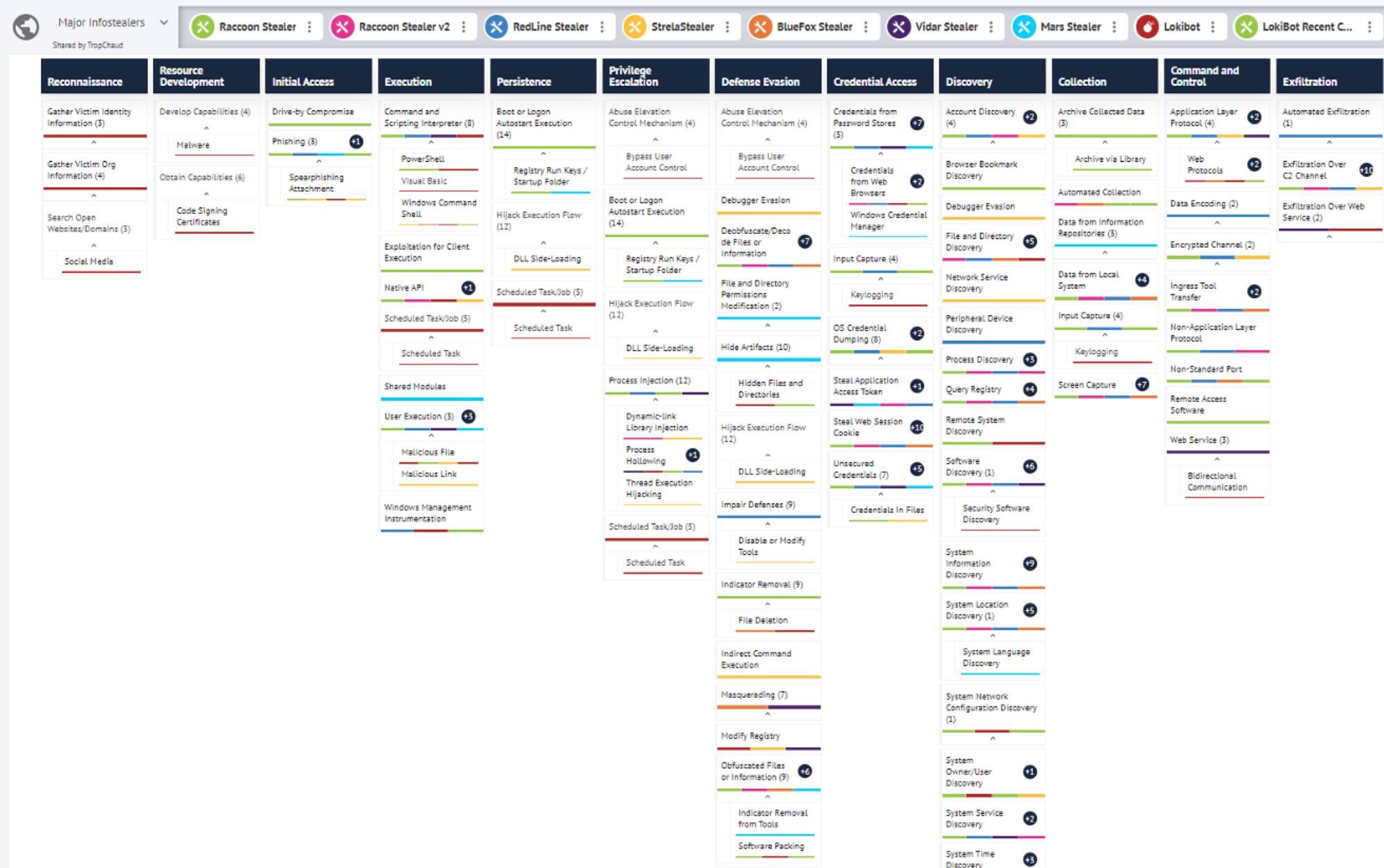


Scale it!



TIDAL

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



Major & Emerging
Info stealers
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!

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

redcanaryco / atomic-red-team Public

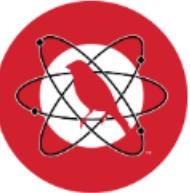
Code Issues 17 Pull requests 2 Actions Wiki Security Insights

master 94 branches 0 tags Go to file Code

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

Search Sign in Sign up

Notifications Fork 2.3k Star 7k

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



github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1539/T1539.md

redcanaryco / atomic-red-team (Public)

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

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 \(Windows\)](#)

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

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:

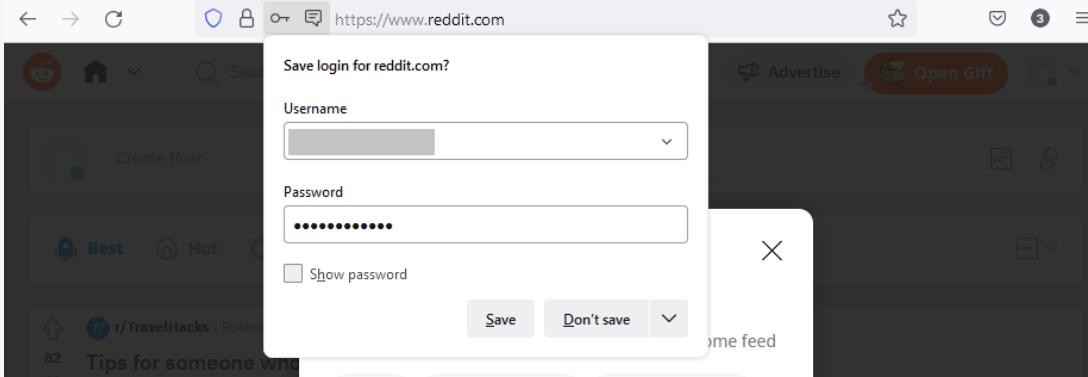
```
if (Test-Path #{$sqlite3_path}) {exit 0} else {exit 1}
```

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



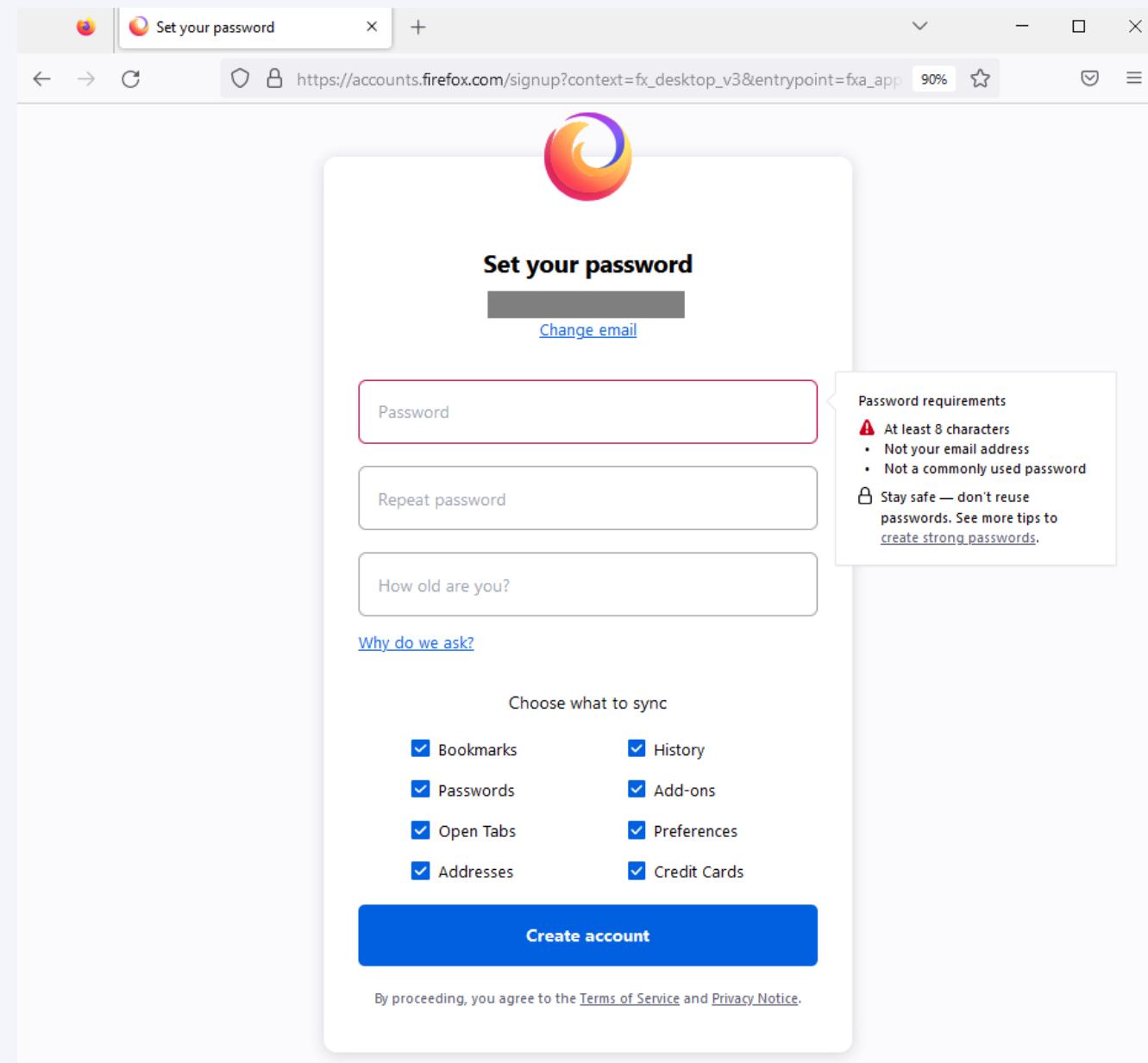
Save login for reddit.com?

Username

Password

Show password

Save Don't save



Set your password

[Change email](#)

Password

Repeat password

How old are you?

[Why do we ask?](#)

Choose what to sync

<input checked="" type="checkbox"/> Bookmarks	<input checked="" type="checkbox"/> History
<input checked="" type="checkbox"/> Passwords	<input checked="" type="checkbox"/> Add-ons
<input checked="" type="checkbox"/> Open Tabs	<input checked="" type="checkbox"/> Preferences
<input checked="" type="checkbox"/> Addresses	<input checked="" type="checkbox"/> Credit Cards

[Create account](#)

By proceeding, you agree to the [Terms of Service](#) and [Privacy Notice](#).



TIDAL

moz://a

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.ps1" -Force
PS C:\Users\User> Invoke-AtomicTest T1539 -ShowDetails
PathToAtomsicsFolder = 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.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
```

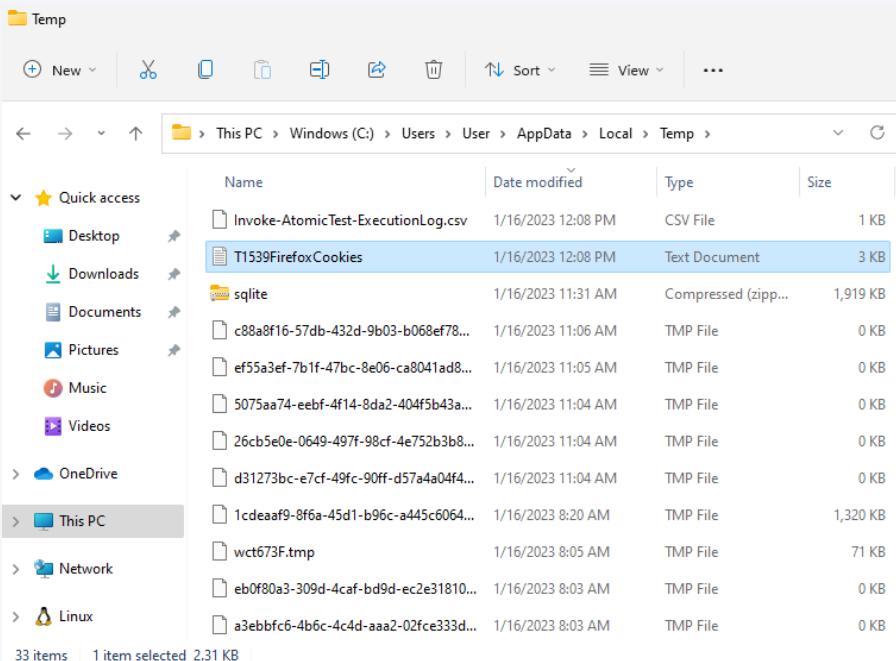
Carrying out a real-world adversary attack / technique

```
PS C:\Users\User> Invoke-AtomicTest T1539 -GetPrereqs
PathToAtomsicsFolder = 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
PathToAtomsicsFolder = 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



Logging With Sysmon





Filter by title

- Home
- Downloads
 - Downloads
 - > File and Disk Utilities
 - > Networking Utilities
 - > Process Utilities
- Security Utilities
 - Security Utilities
 - Autologon
 - LogonSessions
 - NewSID
 - PsLoggedOn
 - PsLogList
 - RootkitRevealer
 - Sysmon
- > System Information
- > Miscellaneous
- Sysinternals Suite
- Microsoft Store
- Community

[Download PDF](#)[Learn](#) / [Sysinternals](#) / [Downloads](#) /[+](#) [Edit](#) [⋮](#)

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage

[Show more ▾](#)

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

README.md

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

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

This is a Microsoft Sysinternals [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



 Event Viewer

File Action View Help

◀ ▶   

Event Viewer (Local)

- > Custom Views
- > Windows Logs
- > Applications and Services Logs
- > Saved Logs
- > Subscriptions

Event Viewer (Local)

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...

Actions

Event Viewer (Local) ▾

-  Open Saved Log...
-  Create Custom View...
- Import Custom View...
- Connect to Another Computer...

View

 Refresh

 Help



Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs**
- Applications and Services Logs
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - Microsoft
 - AppV
 - System
 - User Experience Virtualization
 - Windows
 - AAD
 - All-User-Install Agent
 - AllJoyn

This path ↑

OR

This path ↓

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
- Applications and Services Logs
- Saved Logs
 - Microsoft-Windows-Sysmon%4Operational**
- Subscriptions

Event Viewer

File Action View Help

Service Reporting API

Shell-ConnectedAccountState

Shell-Core

ShellCommon-StartLayoutPopulat

SmartCard-Audit

SmartCard-DeviceEnum

SmartCard-TPM-VCard-Module

SmartScreen

SMBClient

SMBDirect

SMBServer

SMBWitnessClient

StateRepository

Storage-Tiering

StorageManagement

StorageManagement-PartUtil

StorageSettings

StorageSpaces-Api

StorageSpaces-Driver

StorageSpaces-ManagementAgent

StorageSpaces-Parser

StorageSpaces-SpaceManager

StorDiag

Store

StorPort

Storsvc

Sysmon

- Operational**
- SystemSettingsThreshold
- TaskScheduler
- TCP/IP
- TenantRestrictions
- TerminalServices-ClientActiveXCor
- TerminalServices-ClientUSBDevice
- TerminalServices-LocalSessionMan

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

General Details

Dns query:
 RuleName: -
 UtcTime: 2023-01-16 20:00:42.899
 ProcessGuid: {7dec5ef0-6eb6-63c5-7104-00000000a00}
 ProcessId: 8908
 QueryName: d3ag4hukkh62yn.cloudfront.net
 QueryStatus: 0
 QueryResults:
 2600:9000:24f4:1000:7:49a5:5fd2:2221;2600:9000:24f4:7:a00:7:49a5:5fd2:2221;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
 Event ID: 22
 Level: Information
 User: SYSTEM
 OpCode: Info
 Logged: 1/16/2023 12:00:12 PM
 Task Category: Dns query (rule: DnsQuery)
 Keywords:
 Computer: WinDev2212Eval

Actions

Operational

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 22, Sysmon

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help



TIDAL

Sigma Rules

github.com/SigmaHQ/sigma

README.md

Sigma Rule Tests passing

 SIGMA

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



The diagram illustrates the workflow of the Sigma project. It starts with the **Sigma Format**, described as a "Generic Signature Description". This format is processed by the **Sigma Converter**, which "Applies Predefined and Custom Field Mapping". The converter outputs to three different query formats: **Elastic Search Queries**, **Splunk Searches**, and an ellipsis (...).



TIDAL

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_audited_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



frack113 order yaml ✓

Latest commit 1f8e373 on Oct 28, 2022 History

 3 contributors

24 lines (24 sloc) | 808 Bytes

Raw Blame

1 / 1

四

四

```
1 title: SQLite Firefox Cookie DB Access
2 id: 4833155a-4053-4c9c-a997-777fceabaa7
3 status: experimental
4 description: Detect use of sqlite binary to query the Firefox cookies.sqlite database and steal the cookie data contained within it
5 references:
6   - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1539/T1539.md#atomic-test-1---steal-firefox-cookies-windows
7 author: frack113
8 date: 2022/04/08
9 tags:
10   - attack.credential_access
11   - attack.t1539
12 logsource:
13   category: process_creation
14   product: windows
15 detection:
16   selection_sql:
17     - Product: SQLite
18     - Image|endswith: '\sqlite.exe'
19   selection_firefox:
20     CommandLine|contains: 'cookies.sqlite'
21 condition: all of selection_*
22 falsepositives:
23   - Unknown
24 level: high
```

Event Viewer

File Action View Help



Microsoft-Windows-Sysmon%4Operational Number of events: 54,102

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

Event 1, Sysmon

General Details

Process Create:
 RuleName: technique_id=T1059,technique_name=Command-Line Interface
 UtcTime: 2023-01-16 20:08:07.730
 ProcessGuid: {7dec5ef0-aea7-63c5-7f10-00000000a00}
 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: {
 LogonId:
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: SHA1=2BC46B9E7FB2FDD9320D9840359F1062D1F9B8C8,MD5=A7A8CED8B9A2171B2F073E929F01279C,SHA256=EEA80E67B511407D95BF1AD9ED34E56187949D6DE5AC0FE1E9FBC9F40D5BCE,IMPHASH=196DE7BC107A41182A3B0B9EB2570DDC
 ParentProcessGuid: {7dec5ef0-aea7-63c5-7e10-00000000a00}
 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](#)

Actions

Microsoft-Windows-Sysmon%4Operational

Open Saved Log...

Create Custom View...

Import Custom View...

Filter Current Log...

Properties

Find...

Save All Events As...

View

Delete

Rename

Refresh

Help

Event 1, Sysmon

Event Properties

Copy

Save Selected Events...

Refresh

Help

Real results!



TIDAL

#goals

#goals

#goals

Let's build something new!
With adversary intelligence

#goals

#goals

#goals



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

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} #{cookie_db} .dump | findstr /B /C:"host_key" > $env:temp\T1539ChromeCookies.txt
```

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:

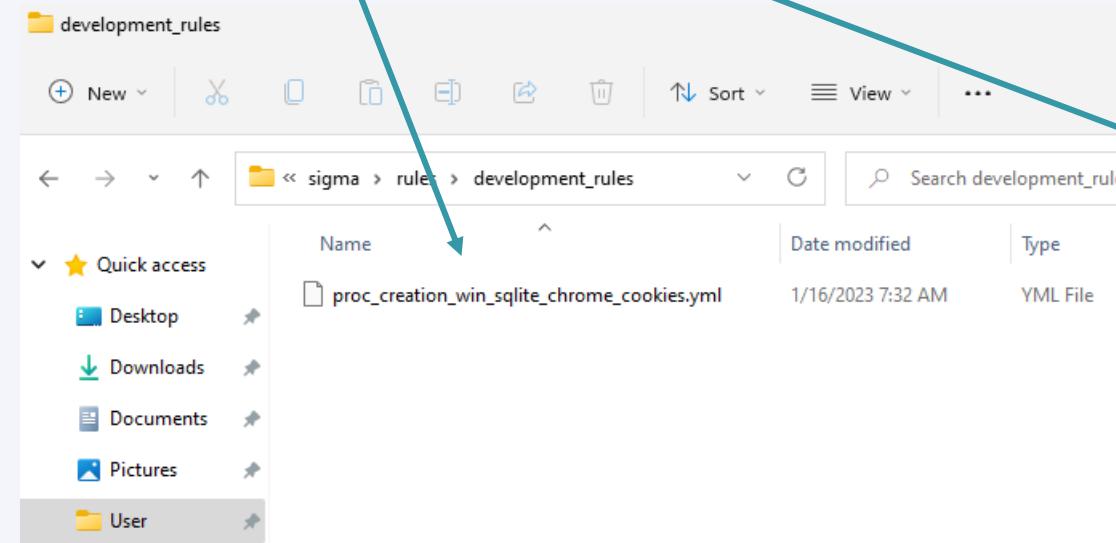
```
Invoke-WebRequest "https://www.sqlite.org/2022/sqlite-tools-win32-x86-3380200.zip" -outfile "$env:temp\sqlite.zip"
```

```

PS C:\Users\User> Invoke-AtomicTest T1539 -TestNumbers 2
PathToAtomsicsFolder = 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	Process...
Information	1/16/2023 12:36:57 PM	Sysmon	10	Process...
Information	1/16/2023 12:36:57 PM	Sysmon	1	Process...

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-c210-00000000a00}
 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-c110-00000000a00}
 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
1  title: SQLite Chrome Cookie DB Access
2  id: 24c77512-782b-448a-8950-eddb0785fc71
3  status: experimental
4  description: Detect use of sqlite binary to query the Chrome Cookies database and steal the cookie data contained within.
5  references:
6    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T1539/proc\_creation\_win\_sqlite\_chrome\_cookies.yml
7  author: TropChaud
8  date: 2022/12/19
9  tags:
10   - attack.credential_access
11   - attack.t1539
12  logsource:
13    category: process_creation
14    product: windows
15  detection:
16    selection_sql:
17      - Product: SQLite
18      - Image|endswith:
19        - '\sqlite.exe'
20        - '\sqlite3.exe'
21    selection_chrome:
22      CommandLine|contains:
23        - '\Google\Chrome\User Data\Default\Network\Cookies' # Latest chrome versions
24        - '\Google\Chrome\User Data\Default\Cookies' # Older chrome versions
25    condition: all of selection_*
26  falsepositives:
27    - Unknown
28  level: high
```



Real-Time, Straightforward Detection With Chainsaw



github.com/withsecurelabs/chainsaw

WithSecureLabs / chainsaw Public

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

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

Contributors 7

© 2023 Tidal Security, Inc. All rights reserved.





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!

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/>

© 2023 Tidal Security, Inc. All rights reserved.



TIDAL

```

Command Prompt
Product: SQLite
RuleName: technique_id=T1059,technique_name=Command-Line Interface
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-logs-all.yml

CHAINSAW
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 DB Access 1       Microsoft-Windows-Sysmon 1       55391     WinDev2212Eval CommandLine: C:\Users\User\AppData\Local\Temp\sqlite-tools-win32-x86-3380200\sql

```

 *Mission accomplished!*



TIDAL

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

SigmaHQ / sigma Public

Code Issues Pull requests Discussions Actions Wiki Security Insights

master sigma / rules / windows / process_creation / proc_creation_win_sqlite_chrome_cookies.yml Go to file ...

nasbench fix: selection name and add old path ✓ Latest commit 3f48eb4 last month History

2 contributors

28 lines (28 sloc) | 995 Bytes Raw Blame

```
1 title: SQLite Chrome Cookie DB Access
2 id: 24c77512-782b-448a-8950-eddb0785fc71
3 status: experimental
4 description: Detect use of sqlite binary to query the Chrome Cookies database and steal the cookie data contained within it
5 references:
6   - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T1539/T1539.md#atomic-test-2---steal-chrome-cookies-windows
7 author: TropChaud
8 date: 2022/12/19
9 tags:
10   - attack.credential_access
11   - attack.t1539
12 logsources:
13   category: process_creation
14   product: windows
15 detection:
16   selection_sql:
17     - Product: SQLite
18     - Image|endswith:
19       - '\sqlite.exe'
20       - '\sqlite3.exe'
21   selection_chrome:
22     CommandLine|contains:
23       - '\Google\Chrome\User Data\Default\Network\Cookies' # Latest chrome versions
24       - '\Google\Chrome\User Data\Default\Cookies' # Older chrome versions
25   condition: all of selection_*
26 falsepositives:
27   - Unknown
28 level: high
```



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



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`

Invoke-AtomicRedTeam wiki:

<https://github.com/redcanaryco/invoke-atomicredteam/wiki>

```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -TestNumbers 25
>>
PathToAtomsicsFolder = 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>
```



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!



```
[+] 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 RecordID
2023-04-30 18:12:22 + Potential System Information Discovery Via Wmic.EXE 1 Microsoft-Windows-Sysmon 1 20402

Filepath: C:\Windows\System32\winevt\eventlog.xml
Description: WMI Commandline Utility
FileVersion: 10.0.22621.1 (WinBuild.160101.0800)
Hashes: SHA1=CC3648E9265AG68A7
E6932076E44413CD01B10F9, MD5=35
3D78C55DA2BC6D95F00C923D0C0044
,SHA256=993A2E38A27887096F75E8
```



Example 3: Spotting an Outlier Technique

Technique Preview

Rundll32

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}....

Vendors

Filter By : Test Detect Protect



ATTACK IQ

cybereason

elastic

FourCore

IBM Security



Labels

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



Widely used, but not by these recent stealers

MALWARE bazaar

by ABUSE

Search

Browse

Upload

Hunting

API

Export

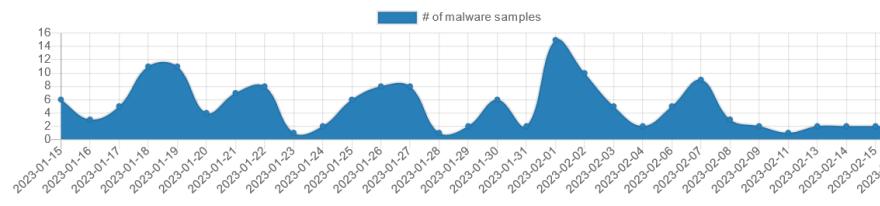
Statistics

FAQ

About

Login

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



A screenshot of a dashboard interface. At the top right is a teal button labeled "VIEW DETAILS". Below it are four boxes: "20 Groups", "59 Software", "4 Data Sources", and "32 Analytics". A large blue arrow points from the "Software" box towards the "SIGMA" GitHub page.

A screenshot of a Cyble blog post titled "Rhadamanthys: New Stealer Spreading Through Google Ads". The post includes a photo of a smartphone displaying a Google Ads interface with a skull icon. It lists three techniques: T1218, T1027, and T1497, under the categories "Defense Evasion" and "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.

A screenshot of a GitHub repository for Sigma rules. The specific file shown is "sigma/rules/windows/process_creation/proc_creation_win_malware_rhadamanthys_steler.yml". The code defines a rule to detect the use of Rundll32 to launch an NSIS module, which serves as the main stealer capability of Rhadamanthys info-stealer. The rule includes URLs for references and a detection section using Sigma's selection functions.

```
title: Rhadamanthys Stealer Module Launch Via Rundll32.EXE
id: 5cdcc2e8-86dd-43df-9a1a-200d4745fb85
status: experimental
description: Detects the use of Rundll32 to launch an NSIS module that serves as the main stealer capability of Rhadamanthys info-stealer, 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: TropChad
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_0ll:
    Commandline|contains: 'nsis_uns'
  selection_export_function:
    Commandline|contains: 'PrintUIEntry'
  condition: all of selection_
  falsepositives:
    - Unknown
```



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**: [@tidalcyber](https://infosec.exchange/@tidalcyber) / [@IntelScott](https://infosec.exchange/@IntelScott)
 - **Twitter**: @TidalCyber / @IntelScott
 - **Reddit**: u/TropChaud (Scott)
 - **Email**: contact@tidalcyber.com / scott.small@tidalcyber.com

