Big-Game Stealing

Practical Detection Engineering & Validation for an Underrated Threat

Amsterdam 2023 FIRST Technical Colloquium

April 2023

Scott Small, Director of Cyber Threat Intelligence

TIDAL

Agenda

- Benefits (& Limitations) of the Approach
- Infostealer Threat Landscape
- Practical, Threat-Informed Detection & Validation
  - Guidance, Resources, & Workflows for 3 Example Cases:
    - Emulating & Detecting a Top CTI Technique
    - Spotting an Outlier
    - Branching Out: Technique Variations

whoami

Career intelligence researcher & analyst

- Purple teamer
- OSINT + data viz

Expanding my “technical” skill & understanding through practical applications

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

Cyber Threat Intelligence Director @ Tidal Cyber

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

TIDAL

THREAT-INFORMED DEFENSE

Threat-Informed Detection & Validation

Benefits (& Limitations) of the Approach

TIDAL

THREAT-INFORMED DEFENSE

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)

A Serious Threat for Enterprises

Infostealer Threat Landscape

TIDAL

THREAT-INFORMED DEFENSE

What are Infostealers?

Information- & credential-stealing malware (“infostealers”)

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

Most often malware-as-a-service (“MaaS”)

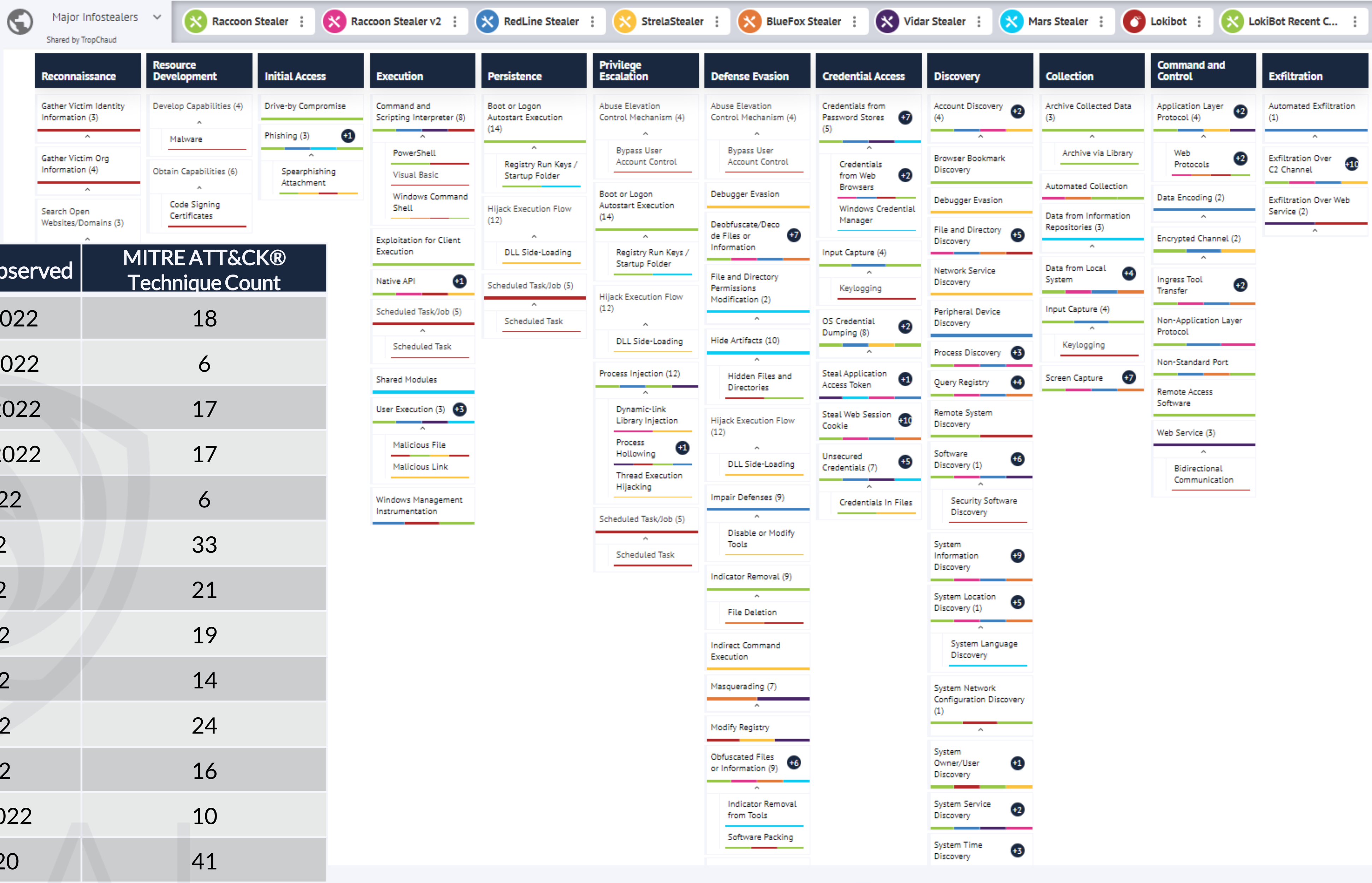
A low-cost & low-skill entry point into profitable cybercrime, driving up adoption

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

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

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

Major & Emerging Infostealers Technique 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)

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)

*Only family currently in ATT&CK

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

app.tidalcyber.com > Community Spotlight

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

Including Small, Medium, & Large Businesses & Organizations

Increased Intent

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

Underground marketplaces catering to high-value log sales

Established “big-game” actors seeking infostealer capabilities

X

Increased Opportunity

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

Communication/Messaging
Remote Access
Password Management
Programming
Browsers/Updates

X

Increased Capability

Cookie theft capabilities in most current strains enable session hijacking

Emerging families have new abilities to:

Steal MFA tokens

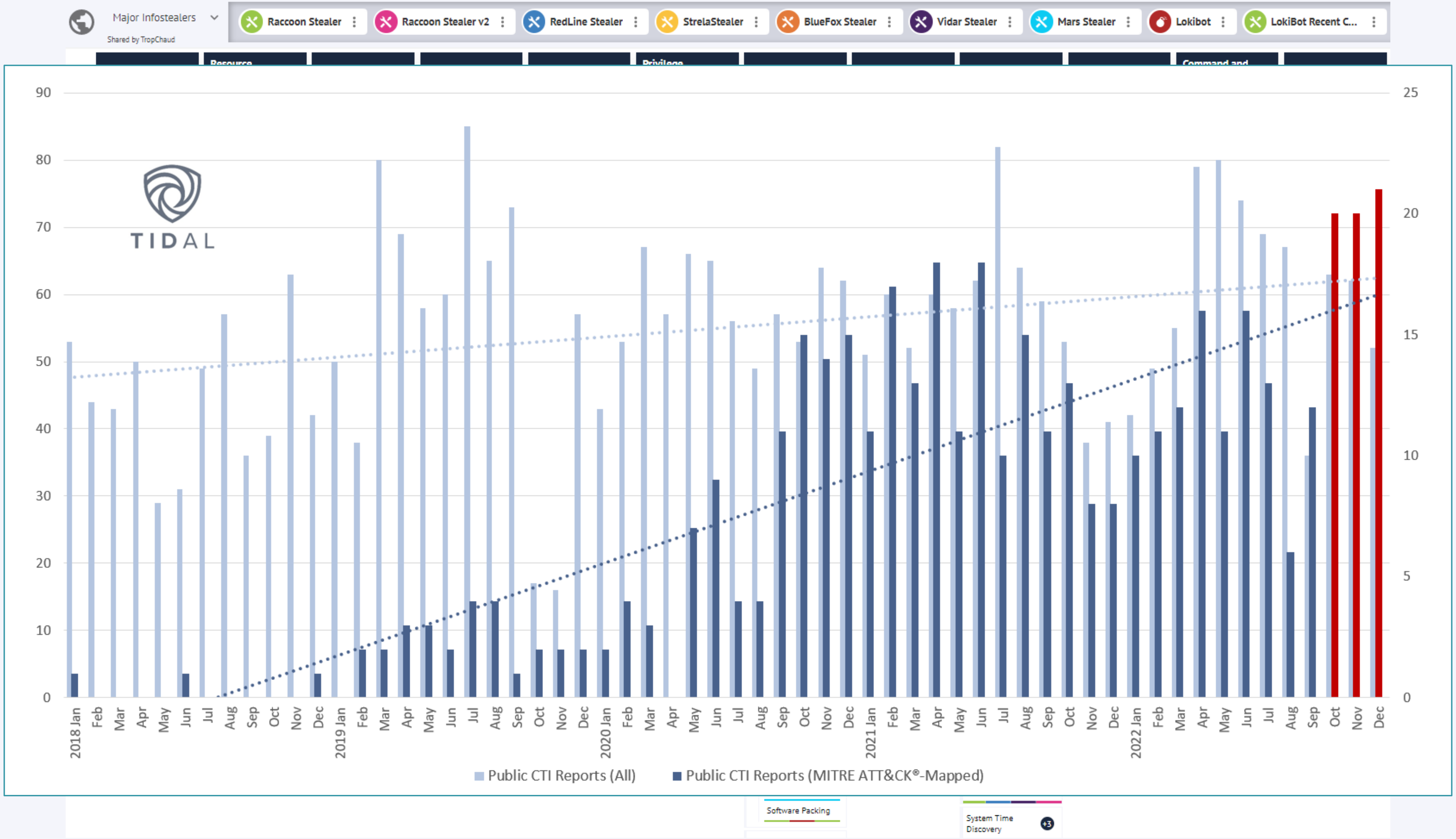
Target email accounts

Increased evasion of advanced/enterprise security tools

=

Increased Threat

“But they’re just Techniques”?!?



A Practical Approach

Threat-Informed Detection & Validation

TIDAL

THREAT-INFORMED DEFENSE

Major & Emerging Infostealers

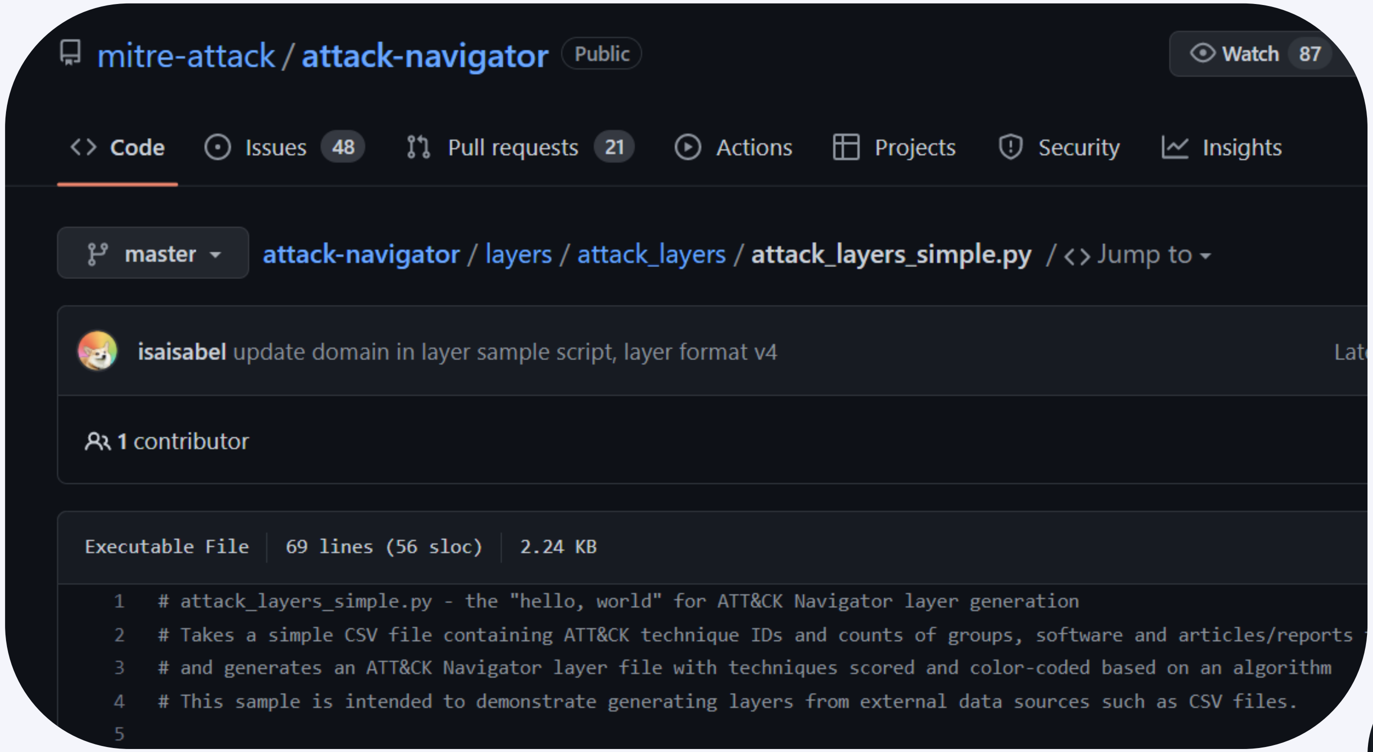
Summary of Select TTPs

How to prioritize?

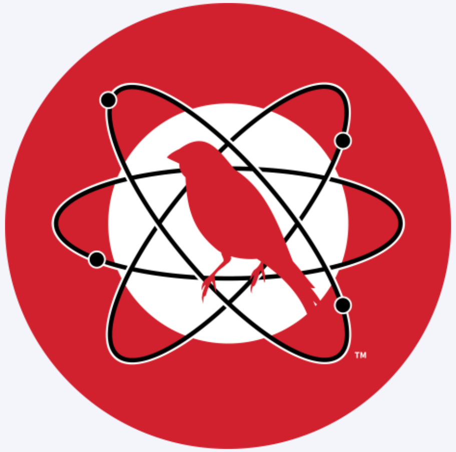
Technique "density" is a great start, but just one approach

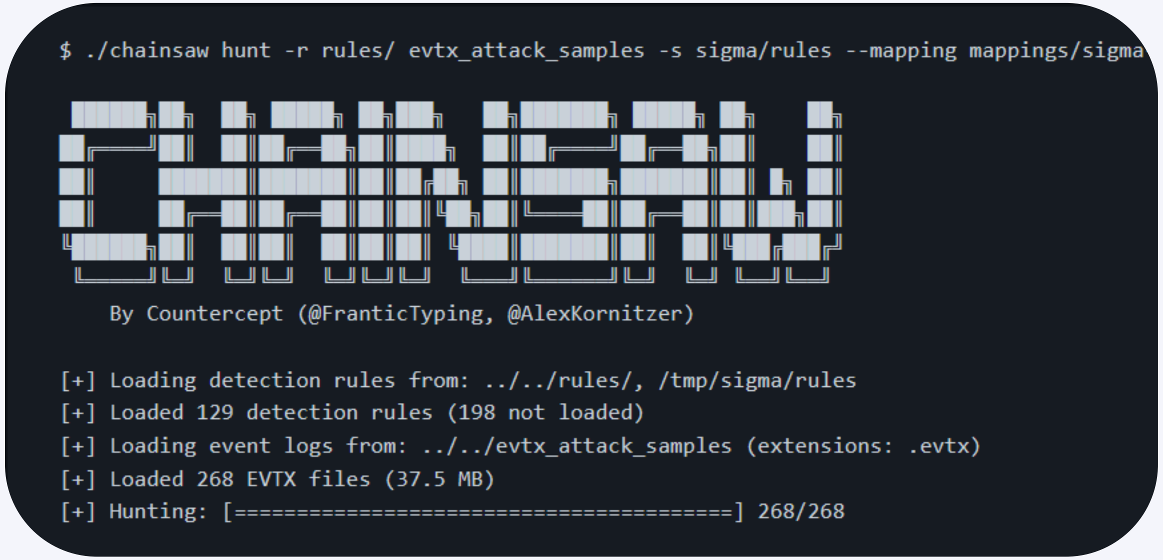
Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1539	**Steal Web Session Cookie**	Credential Access	20	2	2	2
T1555.003	**Credentials from Web Browsers**	Credential Access	19	4	3	16
T1082	**System Information Discovery**	Discovery	16	4	14	24
T1027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

Threat-Informed Detection & Validation: Tools for Getting Started


mitre-attack / attack-navigator Public
Watch 87
Code
Issues 48
Pull requests 21
Actions
Projects
Security
Insights
master
attack-navigator / layers / attack_layers / attack_layers_simple.py / <> Jump to
isaisabel update domain in layer sample script, layer format v4
Lat
1 contributor
Executable File
69 lines (56 sloc)
2.24 KB

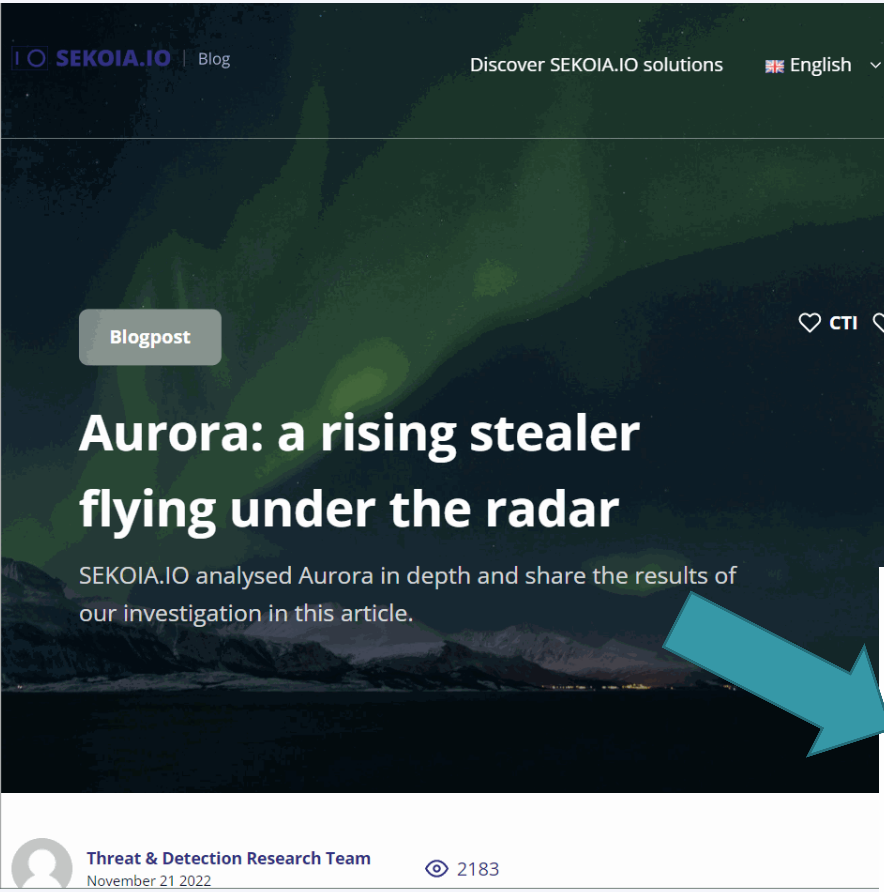
```
# attack_layers_simple.py - the "hello, world" for ATT&CK Navigator layer generation
# Takes a simple CSV file containing ATT&CK technique IDs and counts of groups, software and articles/reports
# and generates an ATT&CK Navigator layer file with techniques scored and color-coded based on an algorithm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





```
$ ./chainsaw hunt -r rules/ evtx_attack_samples -s sigma/rules --mapping mappings/sigma

    By Countercept (@FranticTyping, @AlexKornitzer)

[+] 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 EVTX files (37.5 MB)
[+] Hunting: [========================================] 268/268
```

Example 1: Emulating & Detecting (Instances of) a Top CTI Technique

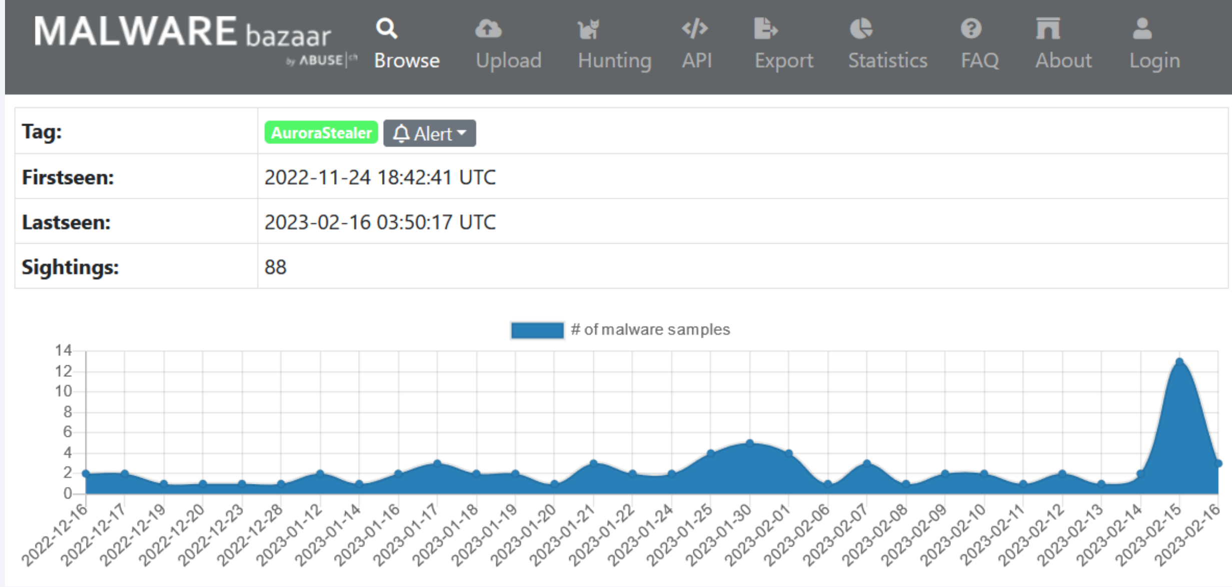


Aurora: a rising stealer flying under the radar

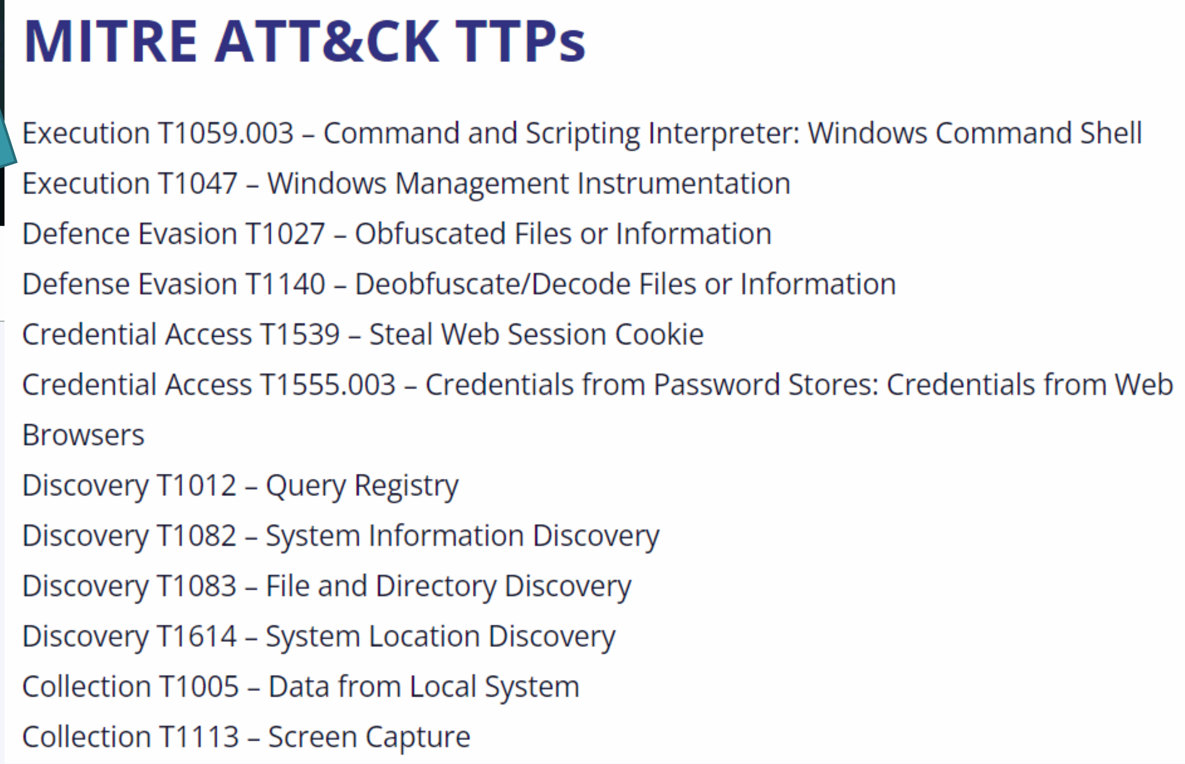
SEKOIA.IO analysed Aurora in depth and share the results of our investigation in this article.

Threat & Detection Research Team
November 21 2022

2183



Tag:	AuroraStealer Alert
Firstseen:	2022-11-24 18:42:41 UTC
Lastseen:	2023-02-16 03:50:17 UTC
Sightings:	88



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

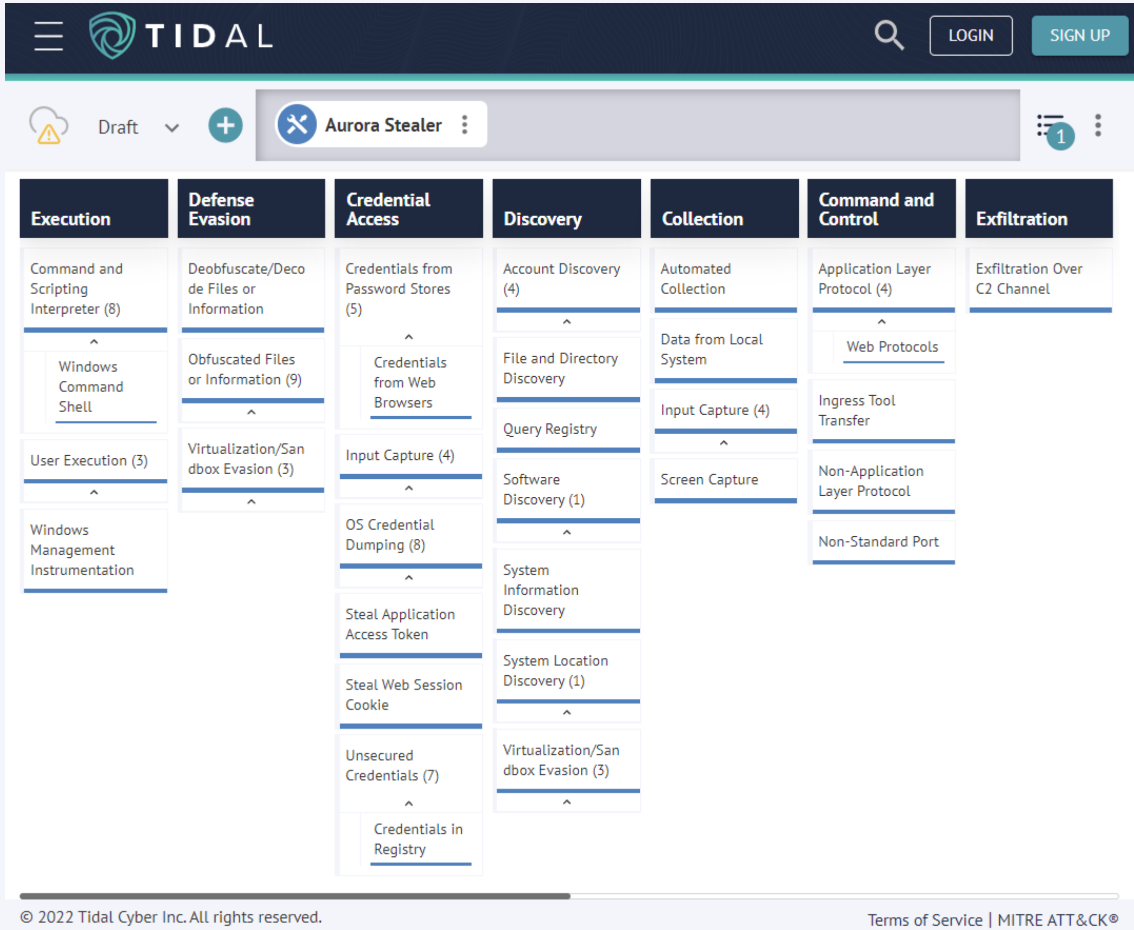
Discovery T1083 – File and Directory Discovery

Discovery T1614 – System Location Discovery

Collection T1005 – Data from Local System

Collection T1113 – Screen Capture

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



Execution
- Command and Scripting Interpreter (8)
  - Windows Command Shell
- User Execution (3)
- Windows Management Instrumentation

Defense Evasion
- Deobfuscate/Decode Files or Information
- Obfuscated Files or Information (9)
- Virtualization/Sandbox Evasion (3)

Credential Access
- Credentials from Password Stores (5)
  - Credentials from Web Browsers
- Input Capture (4)
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal Web Session Cookie
- Unsecured Credentials (7)
  - Credentials in Registry

Discovery
- Account Discovery (4)
- File and Directory Discovery
- Query Registry
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- Virtualization/Sandbox Evasion (3)

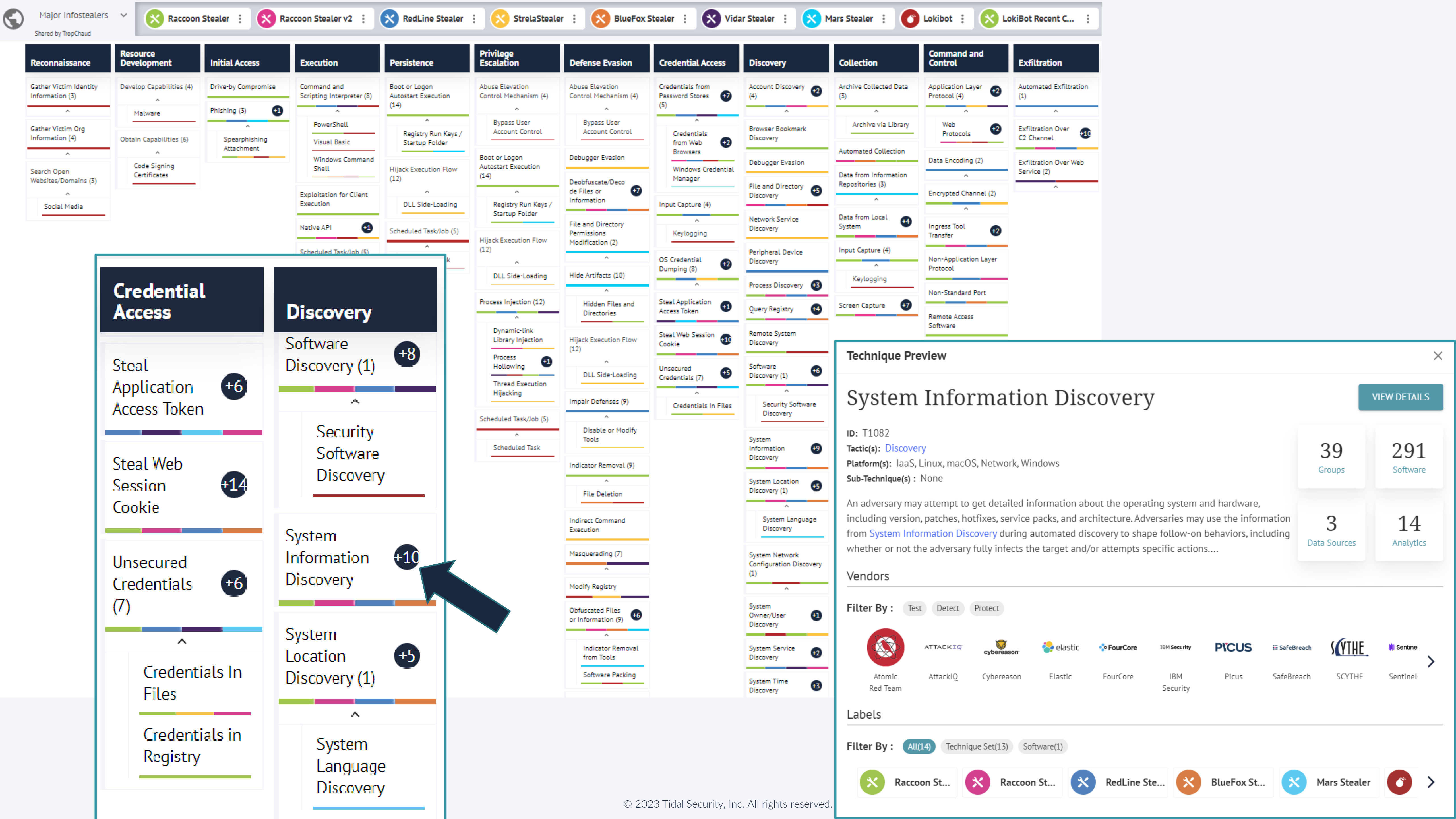
Collection
- Automated Collection
- Data from Local System
- Input Capture (4)
- Screen Capture

Command and Control
- Application Layer Protocol (4)
  - Web Protocols
- Ingress Tool Transfer
- Non-Application Layer Protocol
- Non-Standard Port

Exfiltration
- Exfiltration Over C2 Channel

© 2022 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®



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)

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

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

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

Credential Access
- Steal Application Access Token +6
- Steal Web Session Cookie +14
- Unsecured Credentials (7) +6
- Credentials In Files
- Credentials in Registry

Discovery
- Software Discovery (1) +8
- Security Software Discovery
- System Information Discovery +10
- System Location Discovery (1) +5
- System Language Discovery

Technique Preview ×

System Information Discovery VIEW DETAILS

ID: T1082
Tactic(s): Discovery
Platform(s): IaaS, Linux, macOS, Network, Windows
Sub-Technique(s): None

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions....

39 Groups | 291 Software
3 Data Sources | 14 Analytics

Vendors

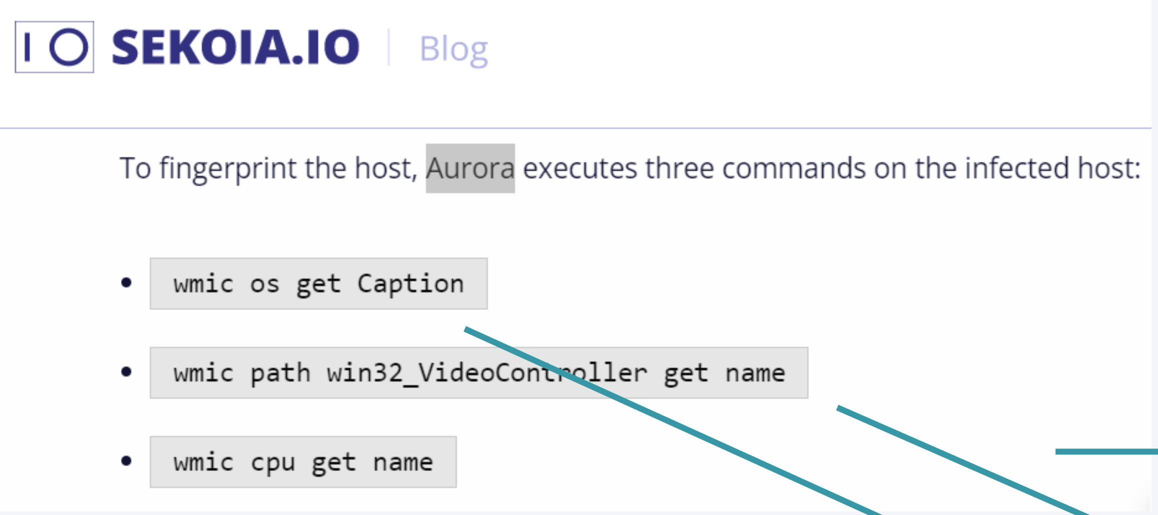
Filter By : Test Detect Protect

Atomic Red Team | AttackIQ | Cybereason | Elastic | FourCore | IBM Security | Picus | SafeBreach | SCYTHE | Sentinel

Labels

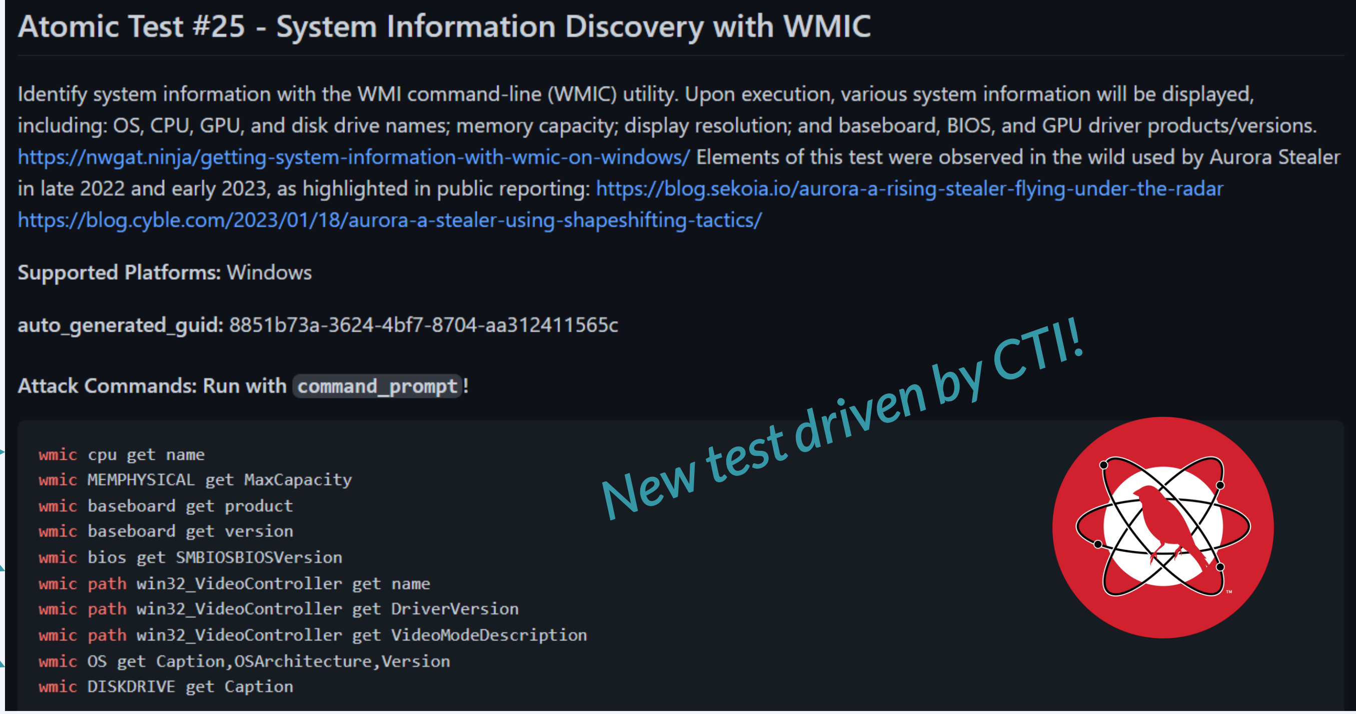
Filter By : All(14) Technique Set(13) Software(1)

Raccoon St... | Raccoon St... | RedLine Ste... | BlueFox St... | Mars Stealer



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

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



Atomic Test #25 - System Information Discovery with WMIC

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

Supported Platforms: Windows

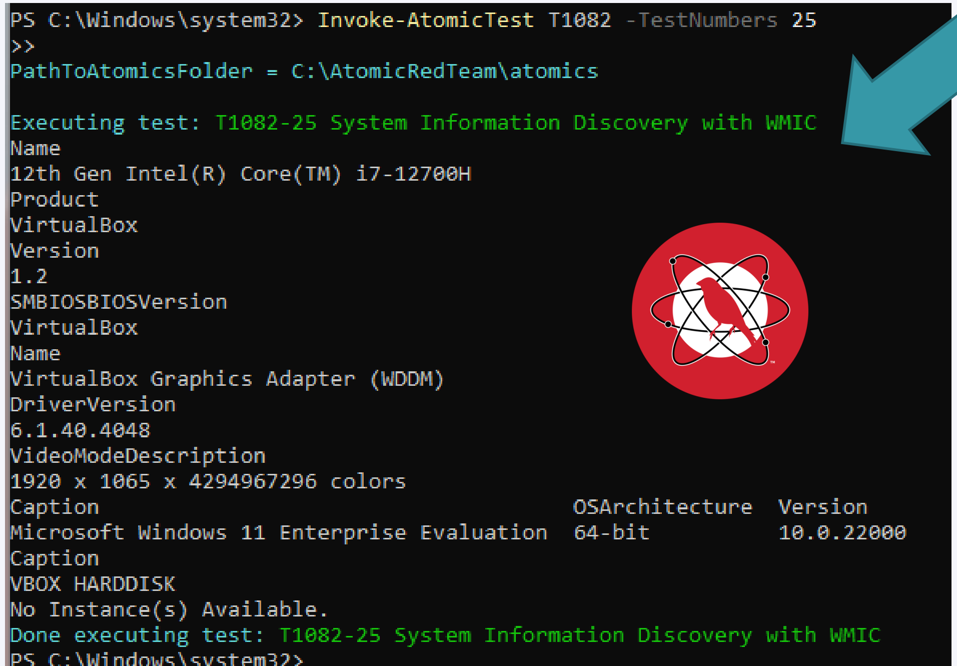
auto_generated_guid: 8851b73a-3624-4bf7-8704-aa312411565c

Attack Commands: Run with `command_prompt`!

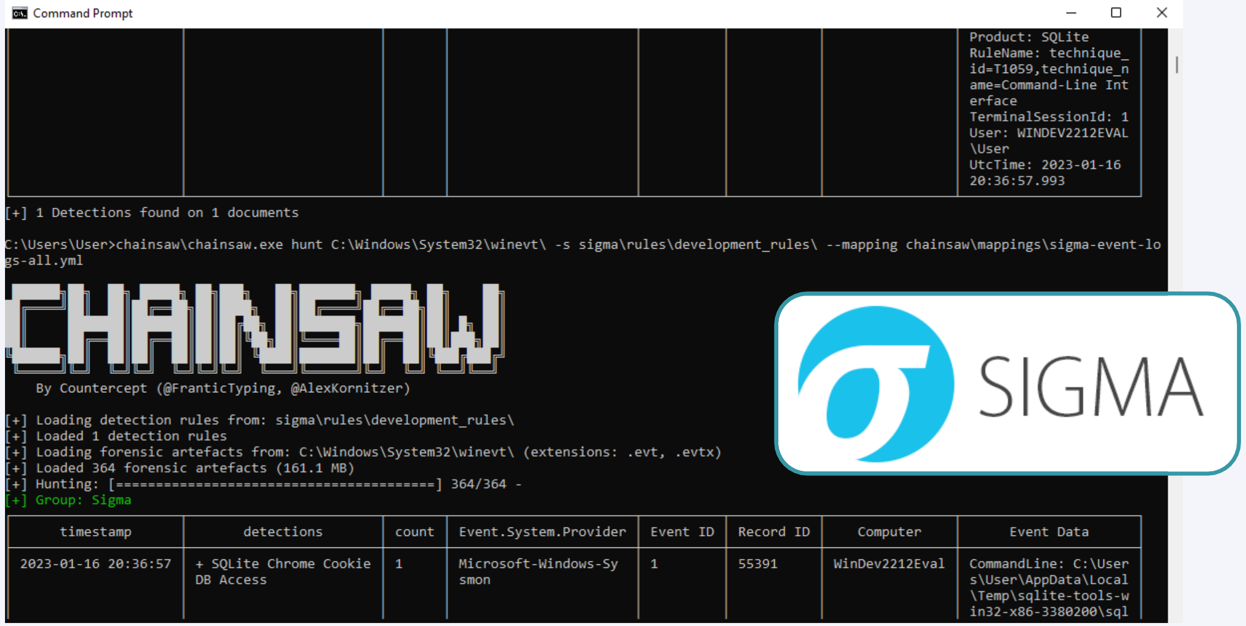
```
wmic cpu get name
wmic MEMPHYSICAL get MaxCapacity
wmic baseboard get product
wmic baseboard get version
wmic bios get SMBIOSBIOSVersion
wmic path win32_VideoController get name
wmic path win32_VideoController get DriverVersion
wmic path win32_VideoController get VideoModeDescription
wmic OS get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

New test driven by CTI!

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



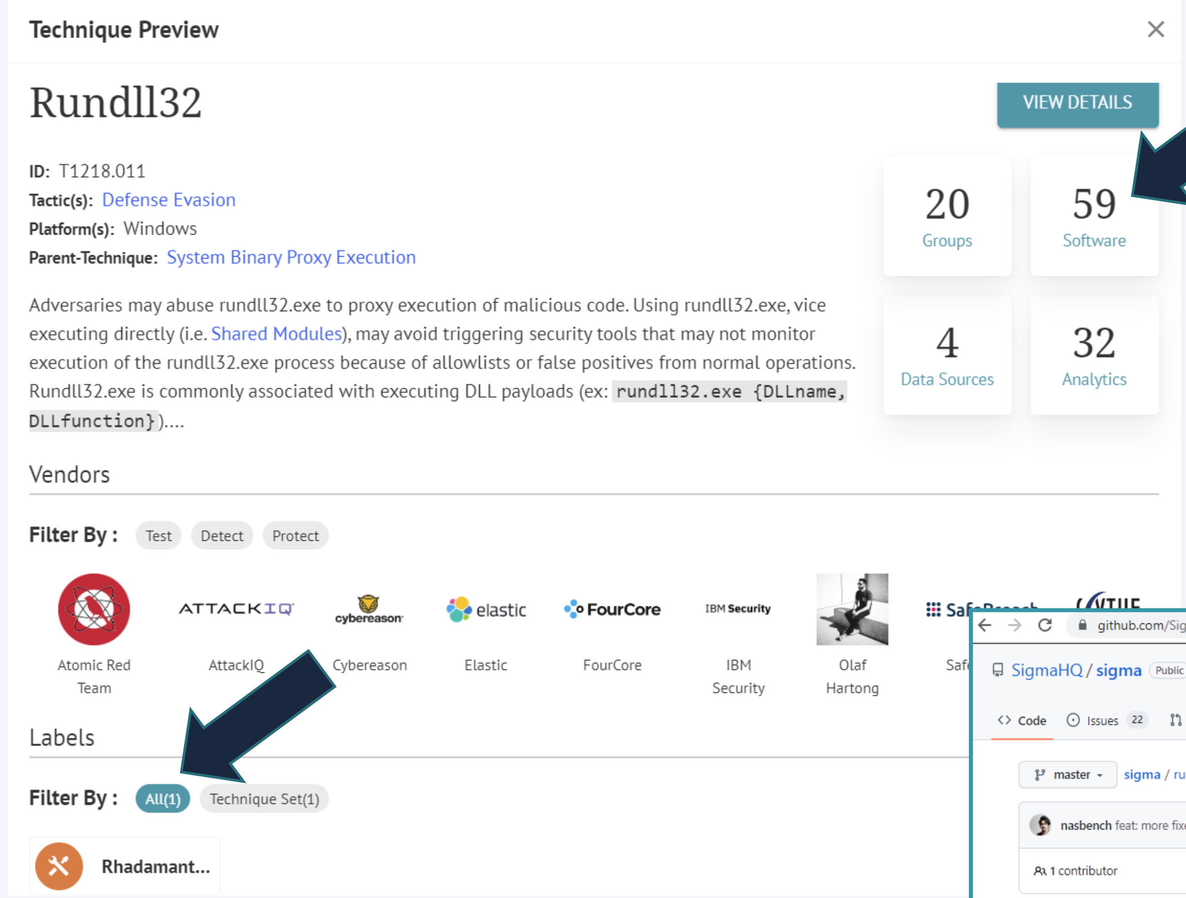
```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -TestNumbers 25
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

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



```
                                                  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

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

Example 2: Spotting an Outlier Technique



Technique Preview

Rundll32

VIEW DETAILS

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

20 Groups	59 Software
4 Data Sources	32 Analytics

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}`)....

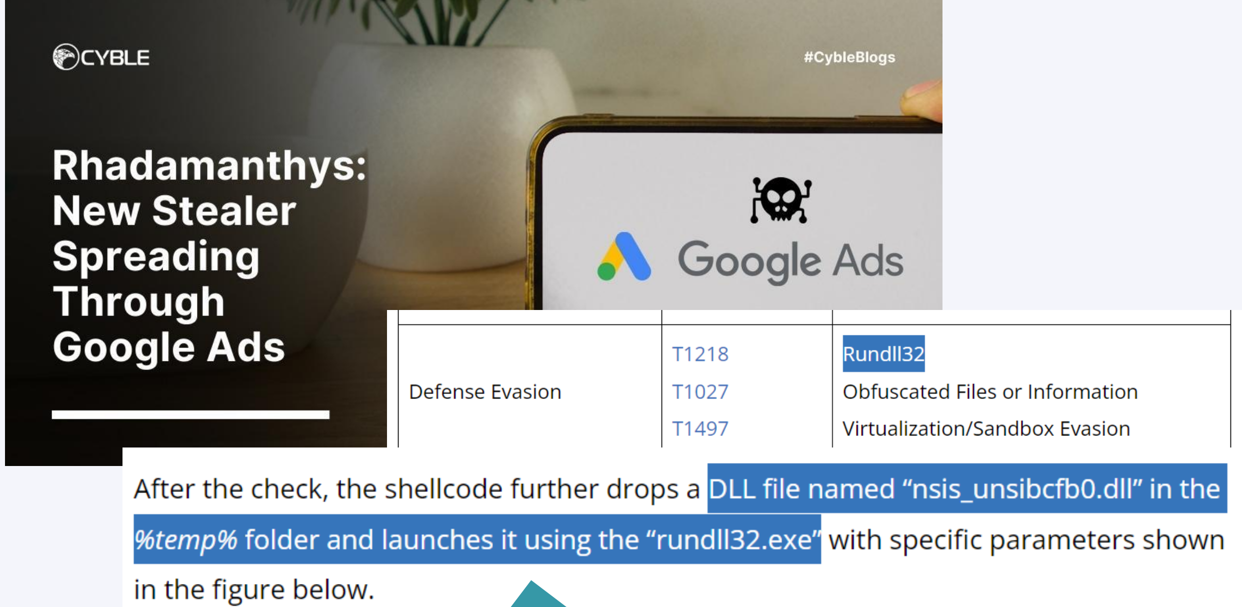
Vendors

Filter By : Test Detect Protect

Labels

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

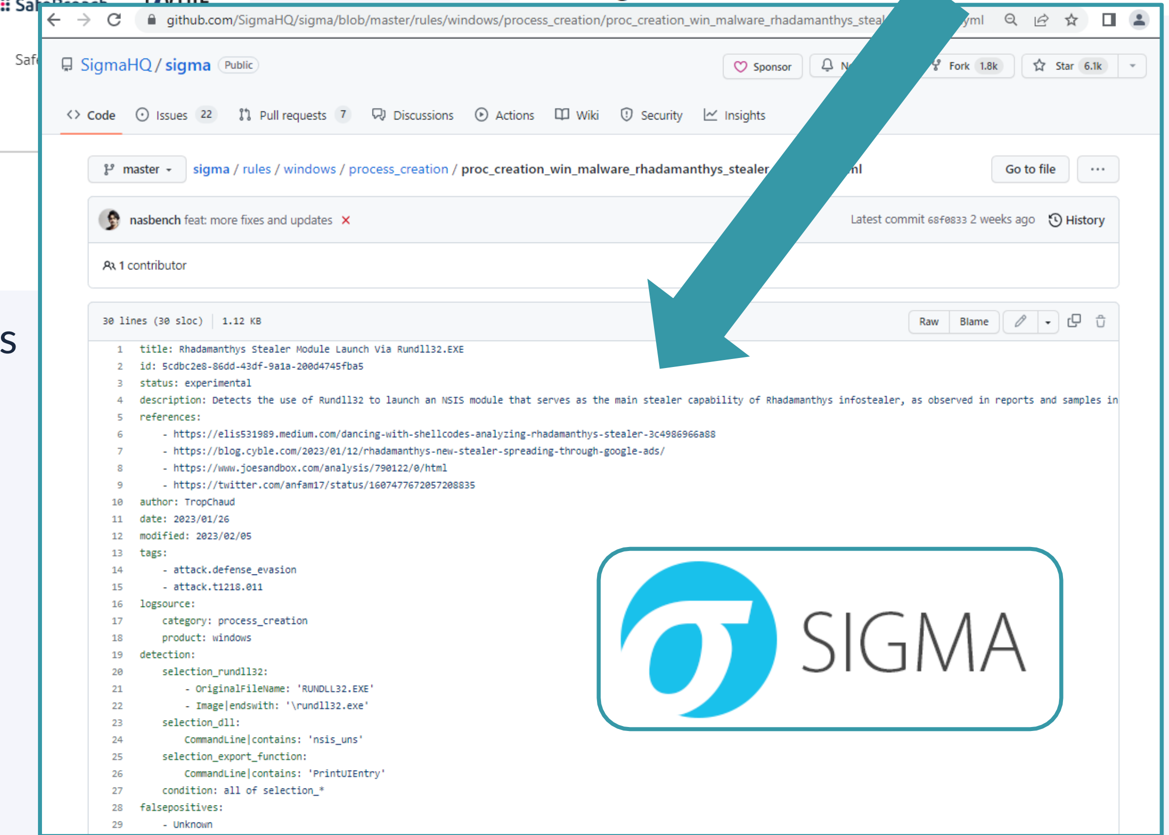
Rhadamant...



Rhadamanthys: New Stealer Spreading Through Google Ads

Defense Evasion	T1218 T1027 T1497	Rundll32 Obfuscated Files or Information 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.



sigma / rules / windows / process_creation / proc_creation_win_malware_rhadamanthys_stealer...ml

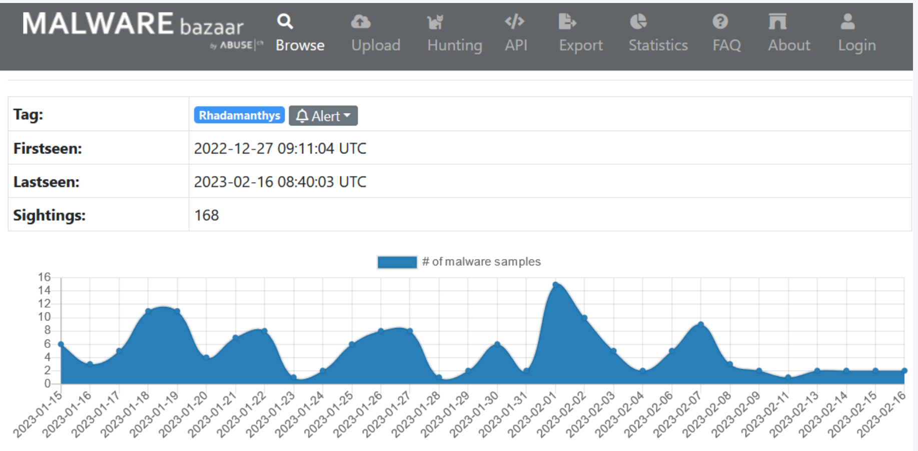
nasbench feat: more fixes and updates ✕ Latest commit 68f0833 2 weeks ago History

1 contributor

30 lines (30 sloc) 1.12 KB

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

Widely used, but not by these recent stealers

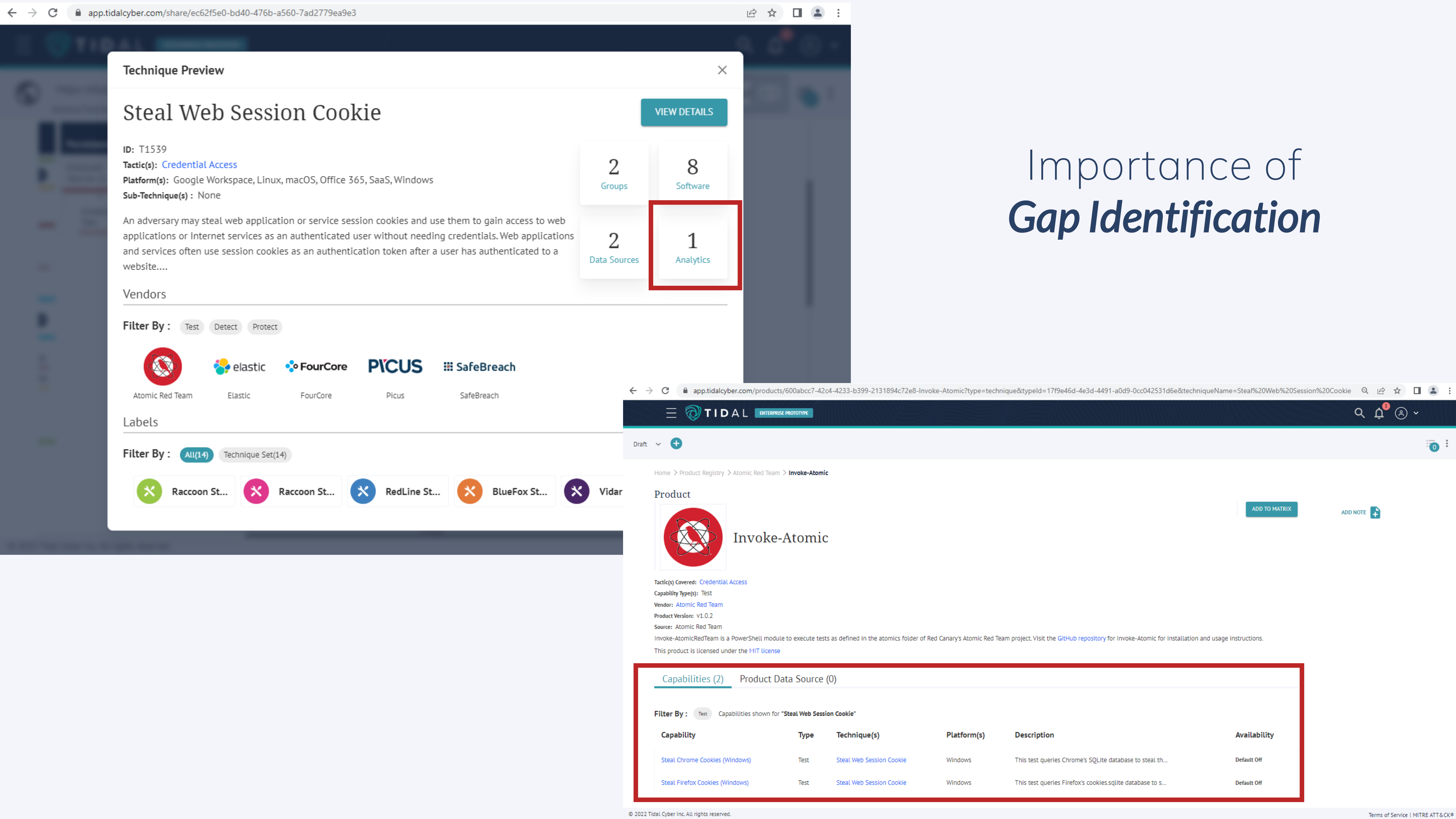


Tag:	Rhadamanthys
Firstseen:	2022-12-27 09:11:04 UTC
Lastseen:	2023-02-16 08:40:03 UTC
Sightings:	168

TIDAL

Example 3: Technique Variation (Expanding Beyond Emulation)

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

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

Product

Invoke-Atomic

ADD TO MATRIX
ADD NOTE

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

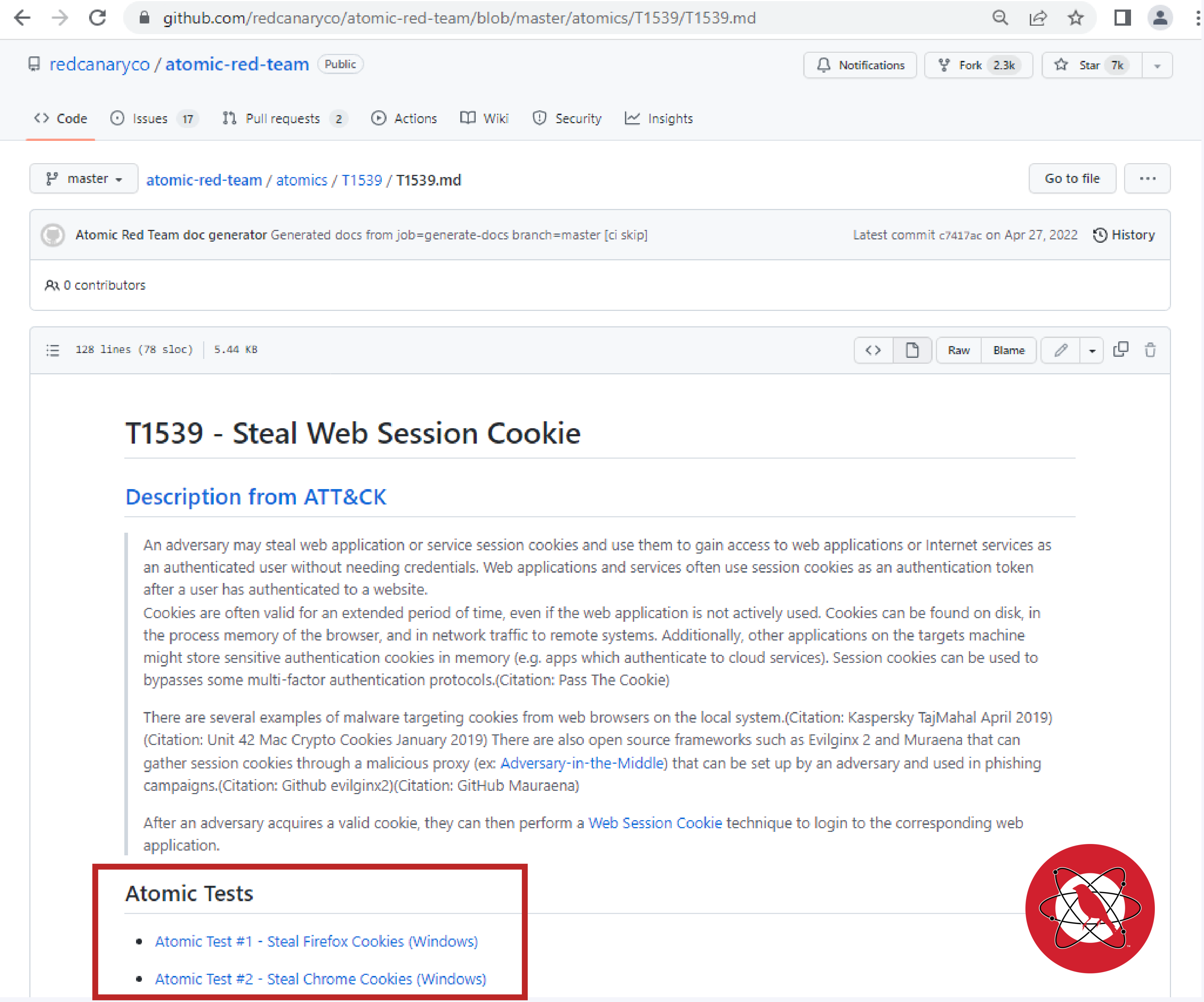
Capabilities (2) Product Data Source (0)

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®


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
Raw
Blame

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

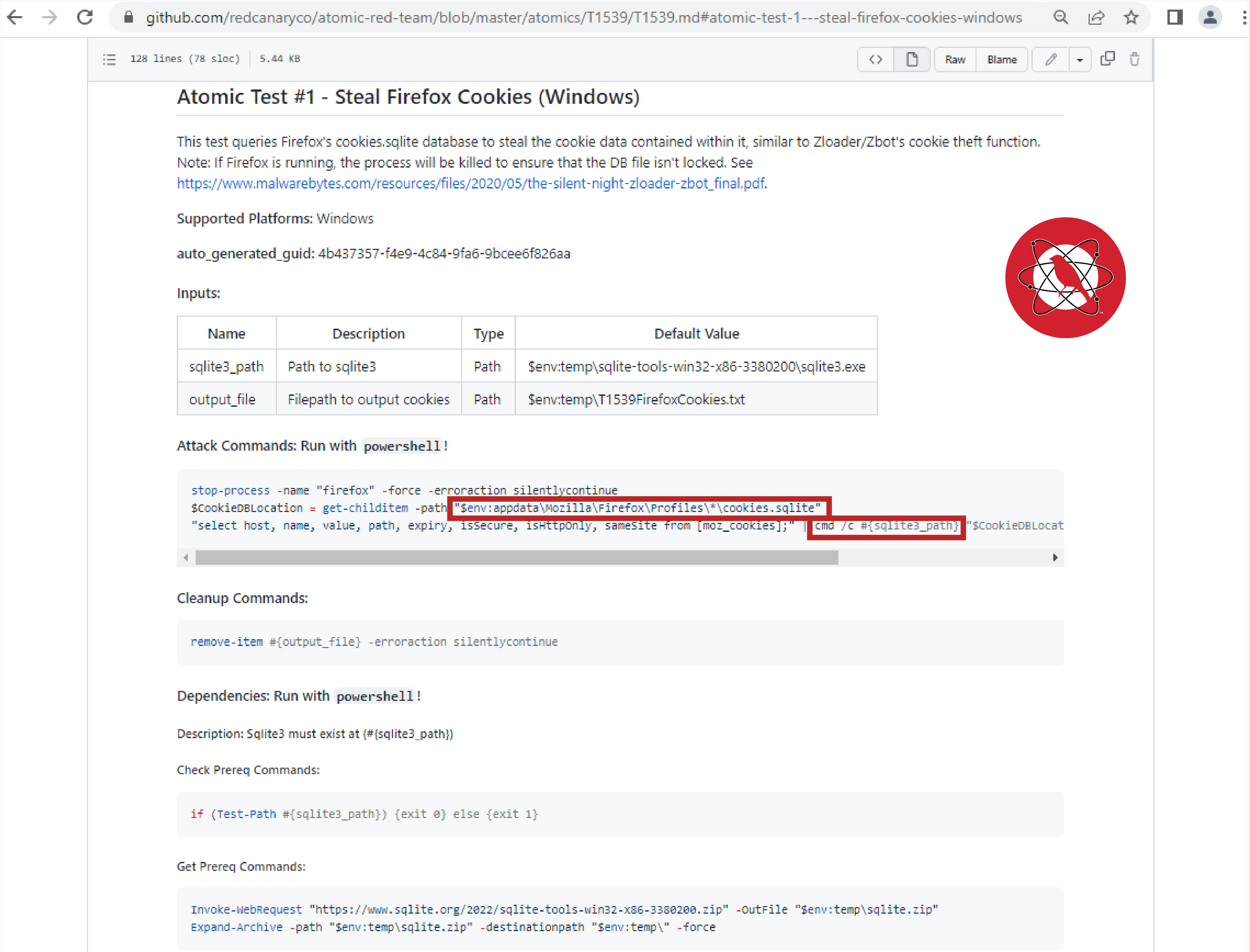
T1539 - Steal Web Session Cookie

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
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`!

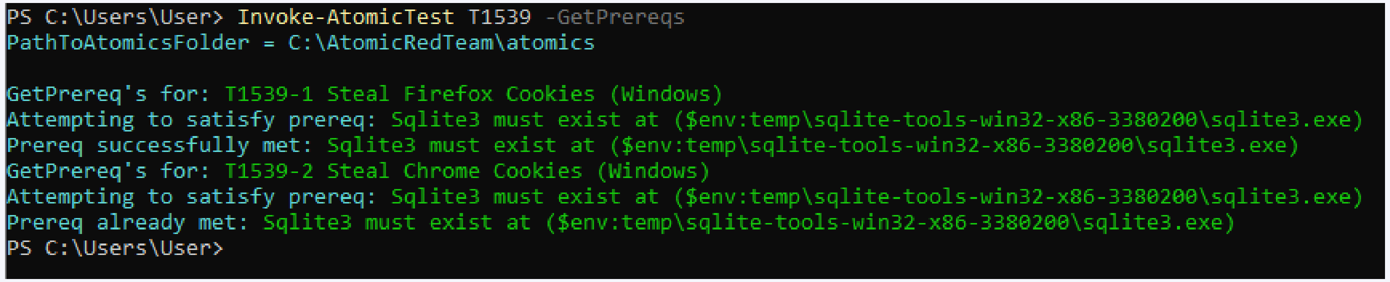
Description: Sqlite3 must exist at (#{sqlite3_path})

Check Prereq Commands:

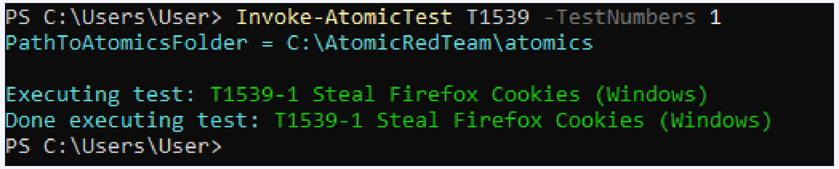
```
if (Test-Path #{sqlite3_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

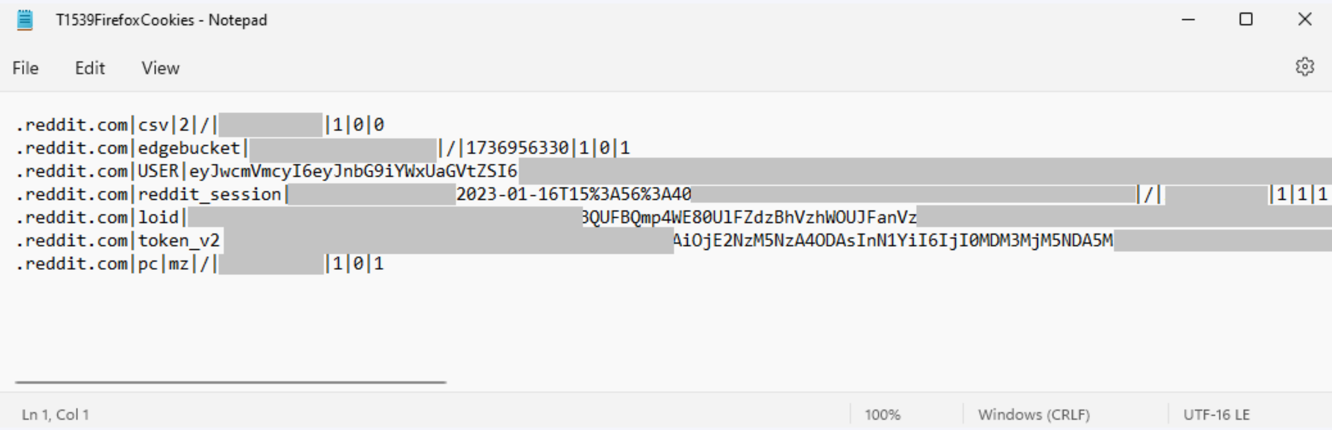
```
Invoke-WebRequest "https://www.sqlite.org/2022/sqlite-tools-win32-x86-3380200.zip" -OutFile "$env:temp\sqlite.zip"
Expand-Archive -path "$env:temp\sqlite.zip" -destinationpath "$env:temp\" -force
```



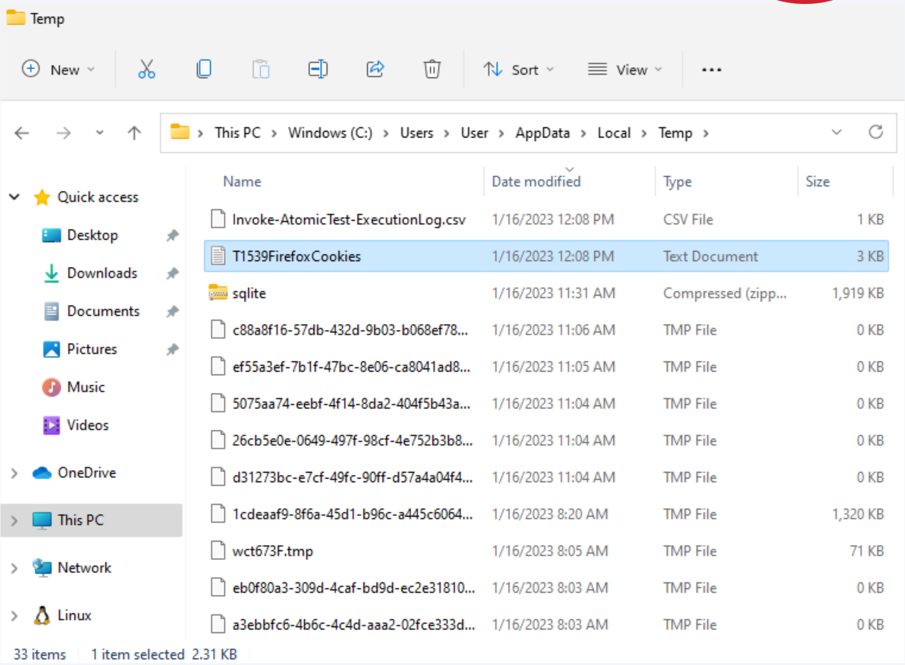
```
PS C:\Users\User> Invoke-AtomicTest T1539 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

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>
```



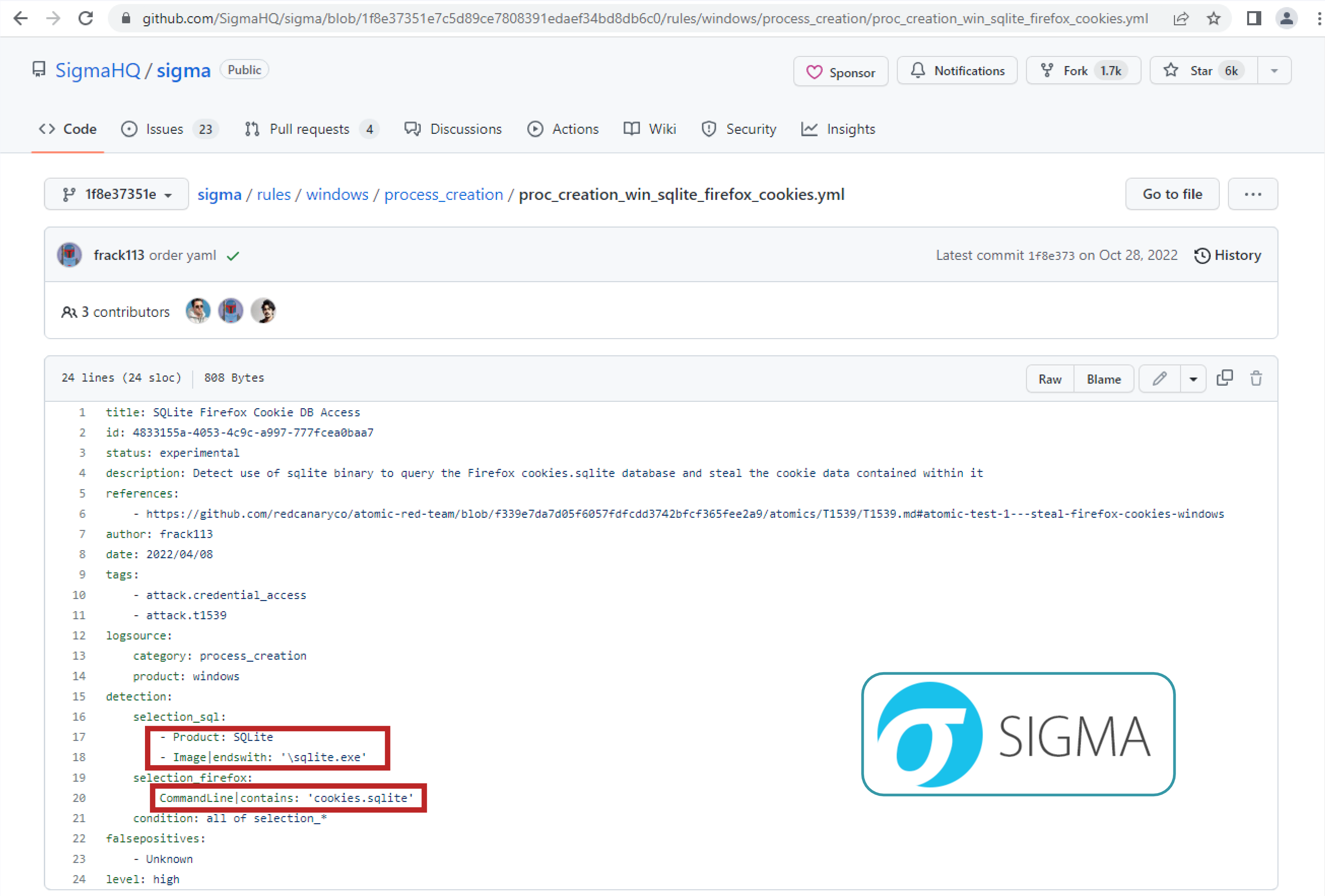
```
PS C:\Users\User> Invoke-AtomicTest T1539 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

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



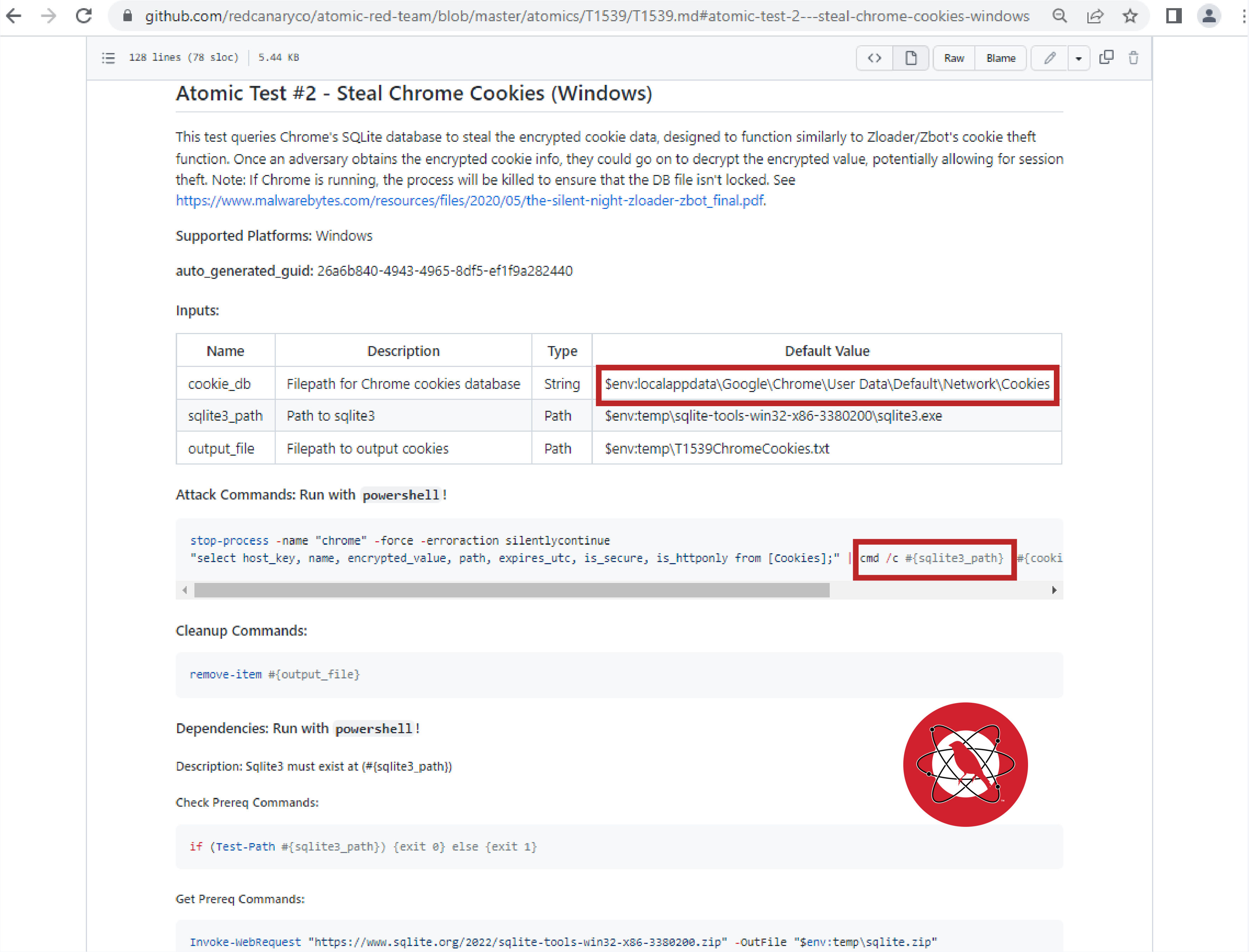
```
.reddit.com|csv|2|/|[redacted]|1|0|0
.reddit.com|edgebucket|[redacted]|/|1736956330|1|0|1
.reddit.com|USER|eyJwcmVmcyI6eyJnbG9iYWxUaGVtZSI6[redacted]
.reddit.com|reddit_session|[redacted]2023-01-16T15%3A56%3A40[redacted]|/|[redacted]|1|1|1
.reddit.com|loid|[redacted]3QUFBQmp4WE80UlFZdzBhVzhWOUJFanVz[redacted]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



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


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
frack113 order yaml ✓
Latest commit 1f8e373 on Oct 28, 2022
History
3 contributors
24 lines (24 sloc) | 808 Bytes
Raw
Blame
SIGMA

```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
```



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`!

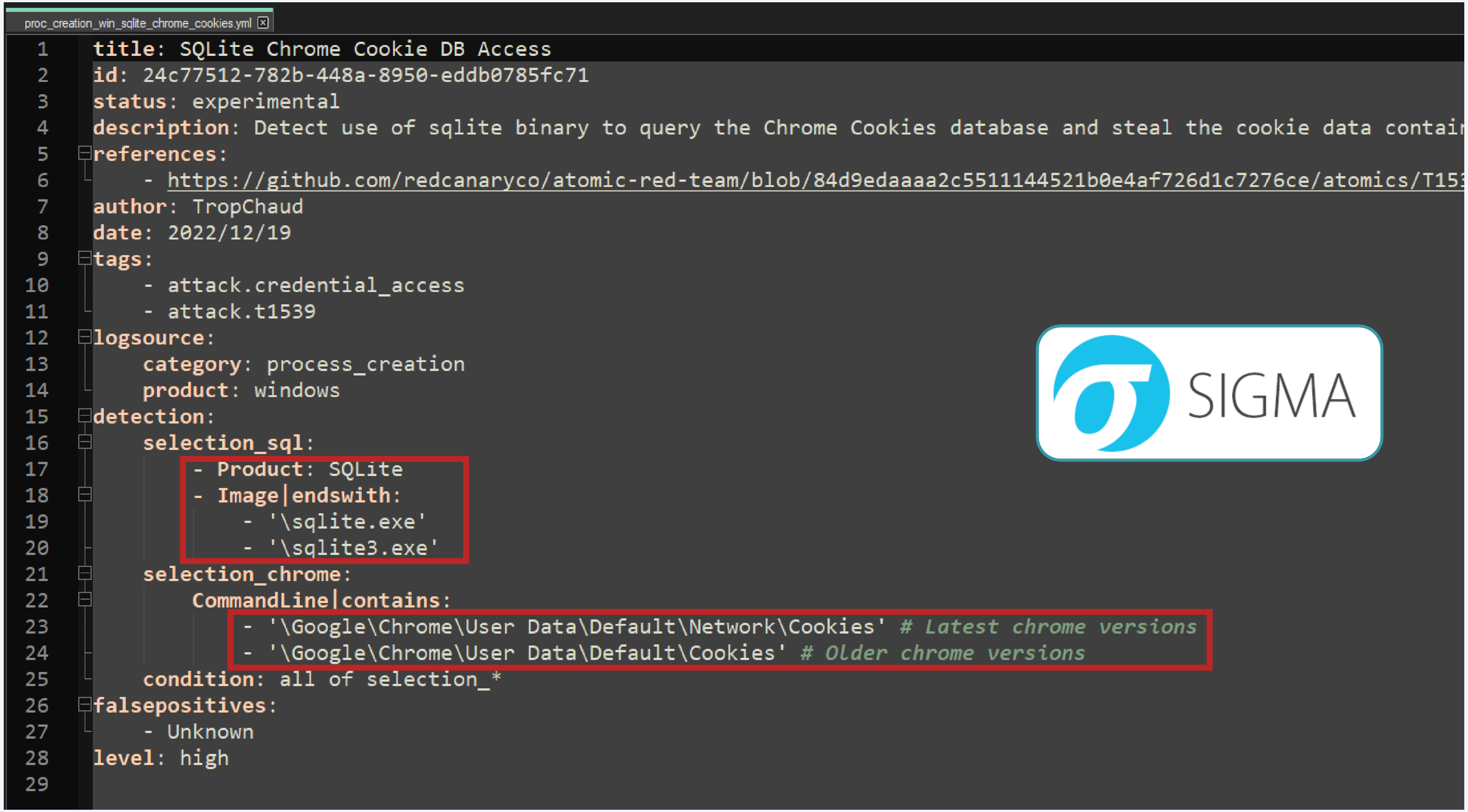
Description: Sqlite3 must exist at (#{sqlite3_path})

Check Prereq Commands:

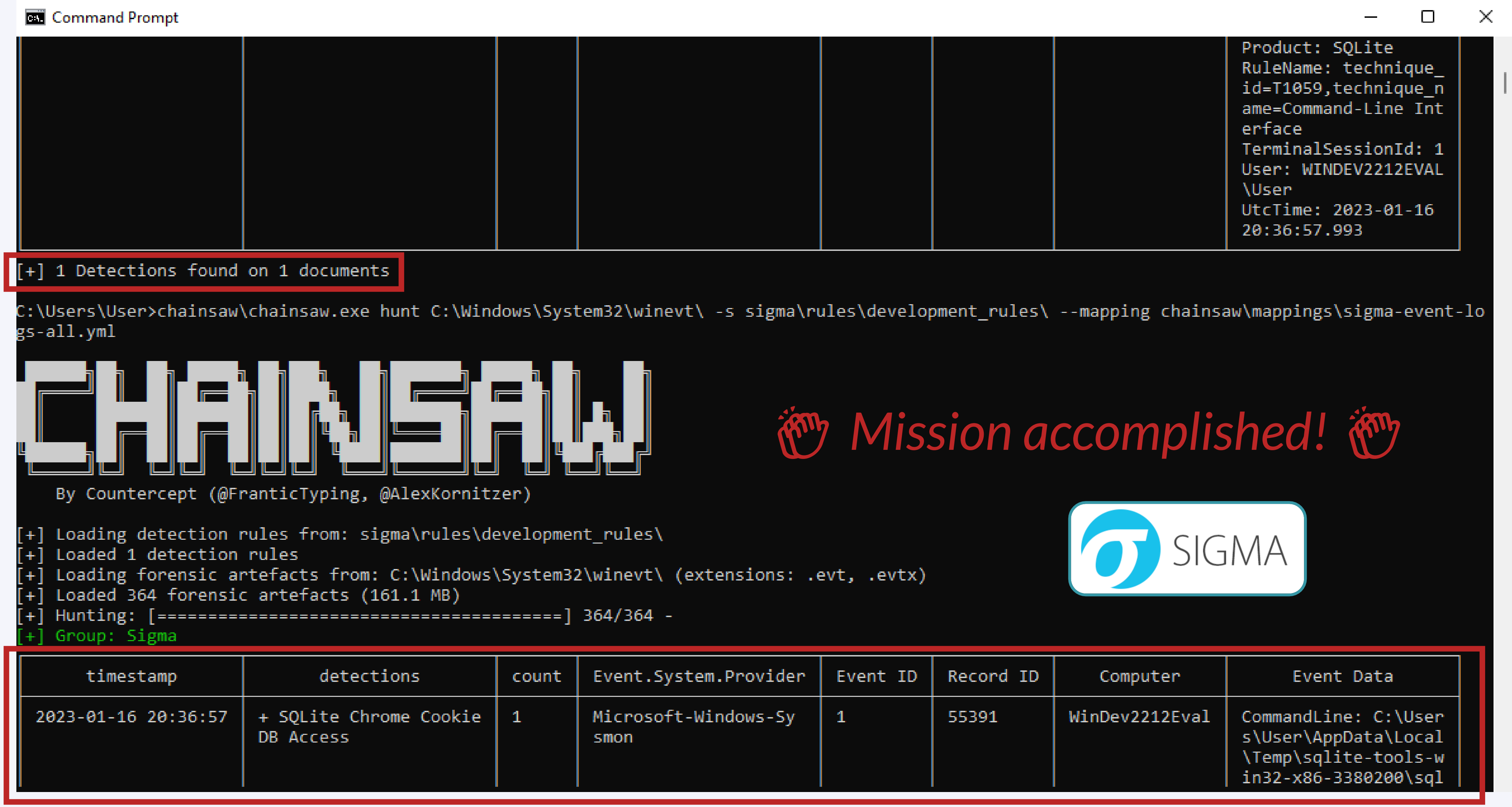
```
if (Test-Path #{sqlite3_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

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



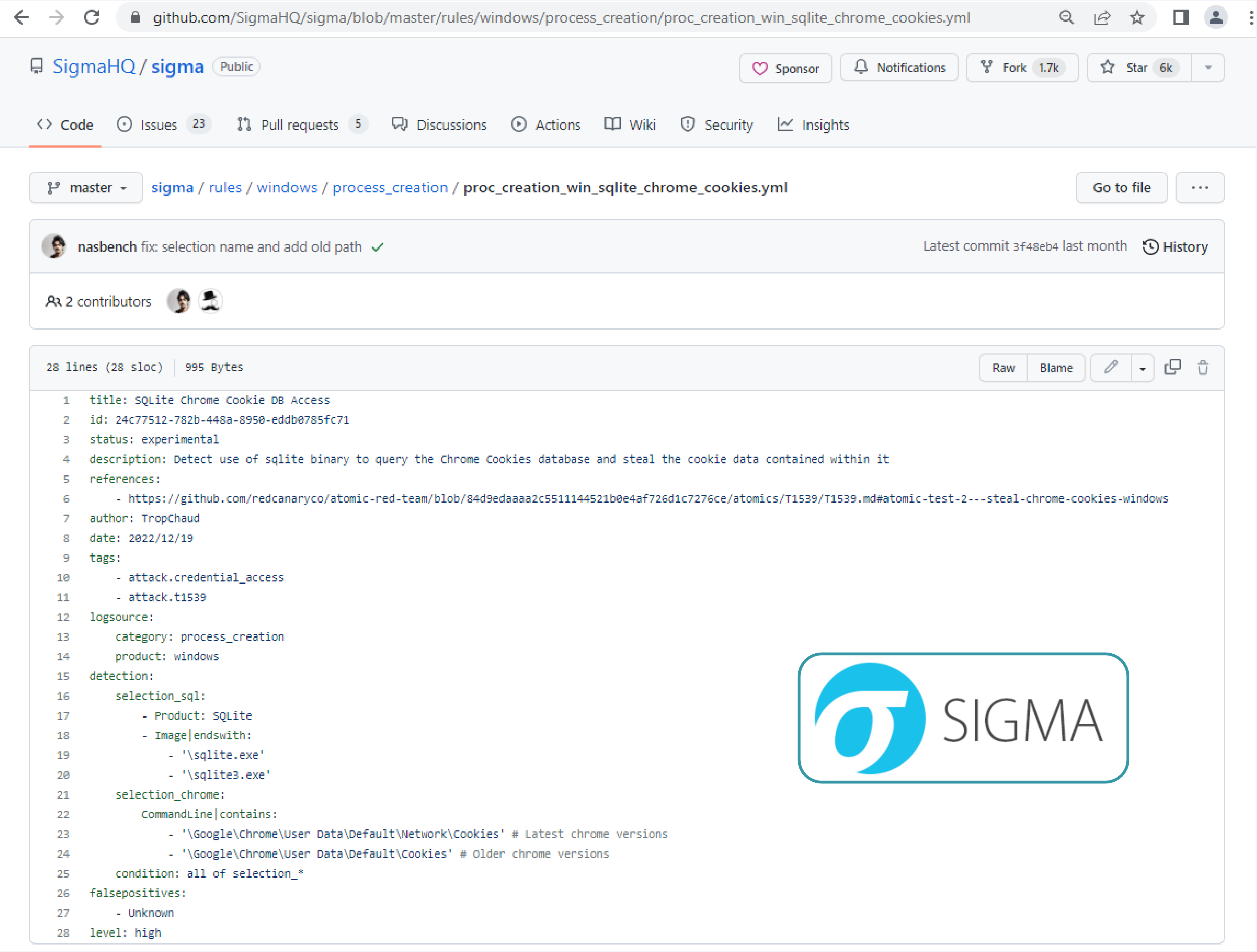
```yaml
title: SQLite Chrome Cookie DB Access
id: 24c77512-782b-448a-8950-eddb0785fc71
status: experimental
description: Detect use of sqlite binary to query the Chrome Cookies database and steal the cookie data contai
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T15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

```



```
|                 |                   |      |                   |        |          |            | 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!

SIGMA


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
nasbench fix: selection name and add old path ✓
Latest commit 3f48eb4 last month
History
2 contributors
28 lines (28 sloc) | 995 Bytes
Raw
Blame
SIGMA

```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
```

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**
  - **LinkedIn**: Tidal Cyber / Scott Small
  - **Mastodon**: infosec.exchange/@tidalcyber / infosec.exchange/@IntelScott
  - **Twitter**: @TidalCyber / @IntelScott
  - **Email**: contact@tidalcyber.com / scott.small@tidalcyber.com

TIDAL