

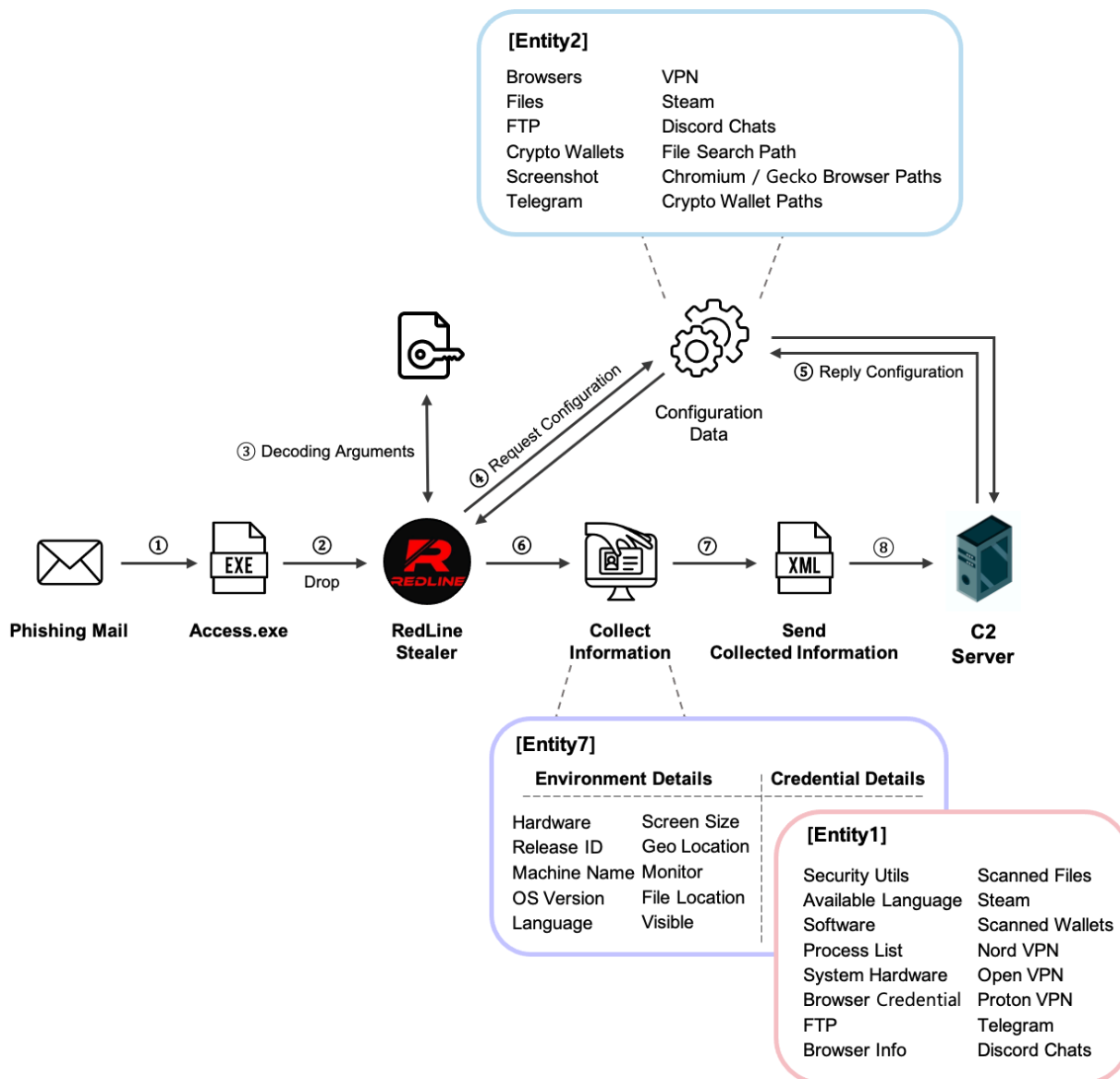
Threat Hunting: Detecting Browser Credential Stealing

[T1555.003]

Archived: 2026-04-02 11:36:50 UTC

Password Managers have seen rapid adoption by organisations as they provide a safe space to store and access your passwords. Native password managers such as [Chrome and Edge Password managers](#) offer users a convenient way of creating secure passwords for different sites without the hassle of remembering each password. As the usage of similar passwords across websites goes down, [threat actors have adopted](#) and have now begun to target these password managers present in your web browser.

Stealers such as Redline are in the news as they provide a low barrier of entry to new cybercriminals, who then use these credentials to provide initial access to other sophisticated groups.



Redline Stealer Operation: Illustration by Jiho Kim | S2W Talon

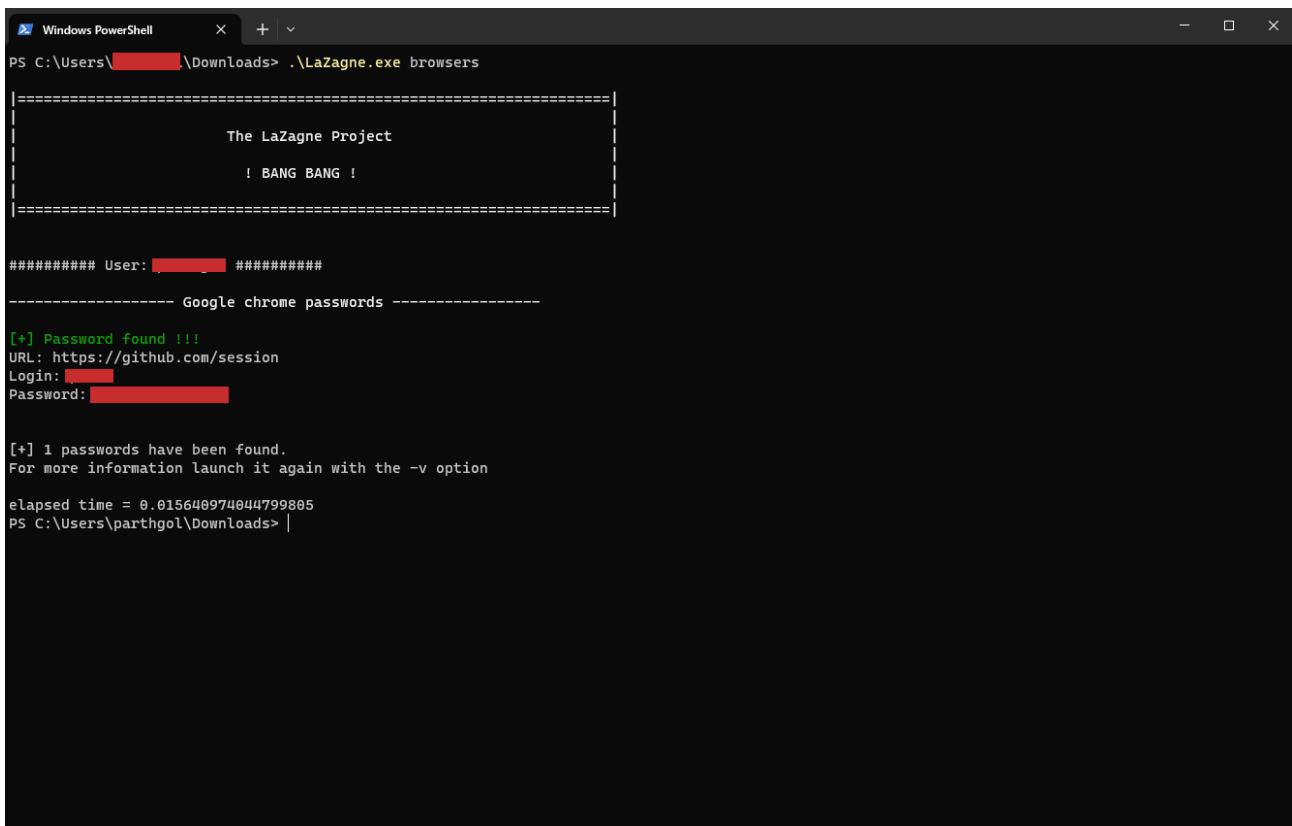
Browser Credential Dumping - MITRE ATT&CK T1555

[Browser Credential dumping](#) is a technique adversaries use to steal credentials from your browsers. People save login credentials in browsers to make the login process faster. Malware such as Redline Stealer, [Zaraza](#) bot, and other info stealers have been actively targeting users and organizations to gain access to browser credentials. These credentials are made available to threat actors who use these credentials to breach various organizations.

This post will showcase how to detect browser credential extraction, weed out false positives, and improve our resilience against this threat.

Tools of the Trade

There are various tools, open source and closed, which adversaries use for stealing credentials from browsers. Tools such as [Lazagne](#) and [HackerBrowserData](#) are open source and provide customizability to advanced attackers, whereas tools such as [Nirsoft's WebBrowserPassView](#) are closed source and cannot be modified easily. Direct integration to C2 Frameworks such as [Metasploit's](#) `post/multi/gather/firefox_creds` and `post/windows/gather/enum_chrome` modules allow quick access to browser passwords for adversaries.



```
Windows PowerShell
PS C:\Users\██████████\Downloads> .\LaZagne.exe browsers

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

##### User: ██████████ #####

----- Google chrome passwords -----

[+] Password found !!!
URL: https://github.com/session
Login: ██████████
Password: ██████████

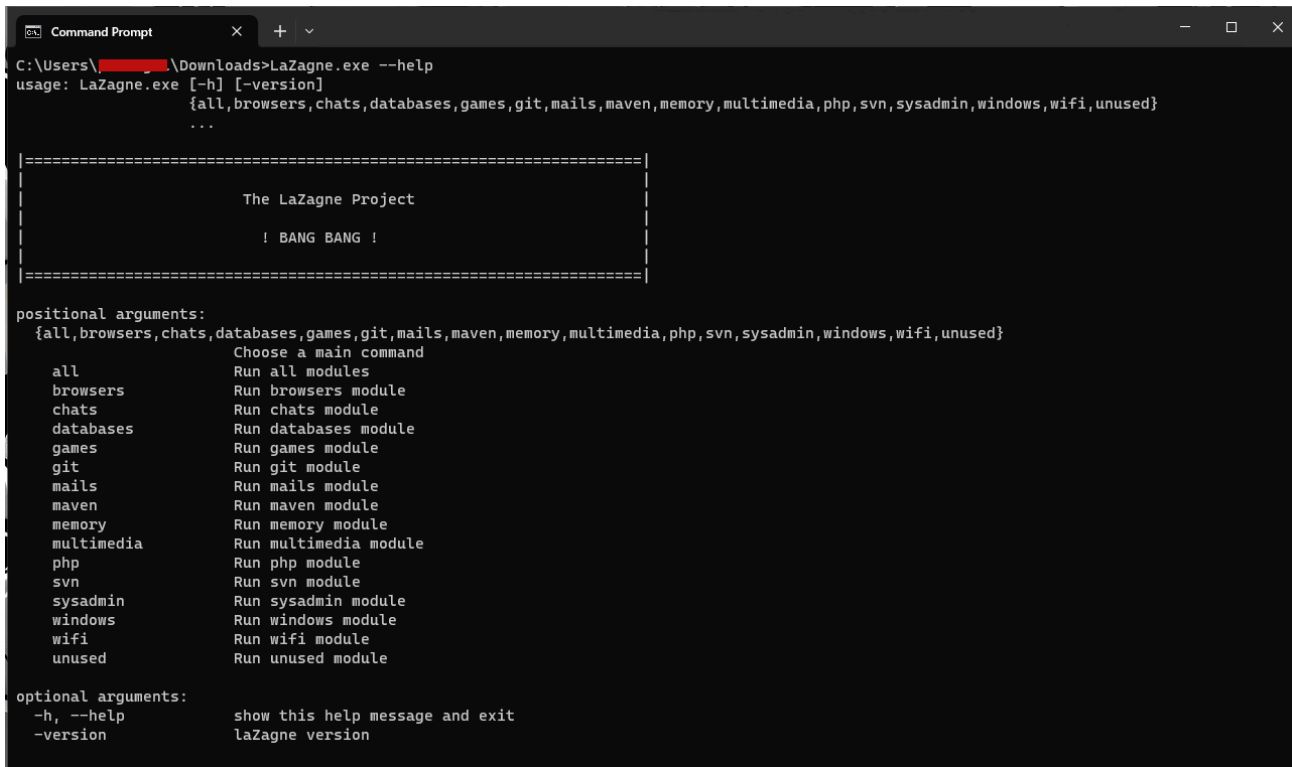
[+] 1 passwords have been found.
For more information launch it again with the -v option

elapsed time = 0.015640974044799805
PS C:\Users\parthgol\Downloads> |
```

Extraction of Browser passwords using lazagne

Methodology

To identify how tools such as Lazagne and HackBrowserData extract browser credentials from a host machine, we can download their source code for examination and find key detection opportunities.



```
C:\Users\...Downloads>Lazagne.exe --help
usage: Lazagne.exe [-h] [-version]
               {all,browsers,chats,databases,games,git,mails,maven,memory,multimedia,php,svn,sysadmin,windows,wifi,unused}
               ...

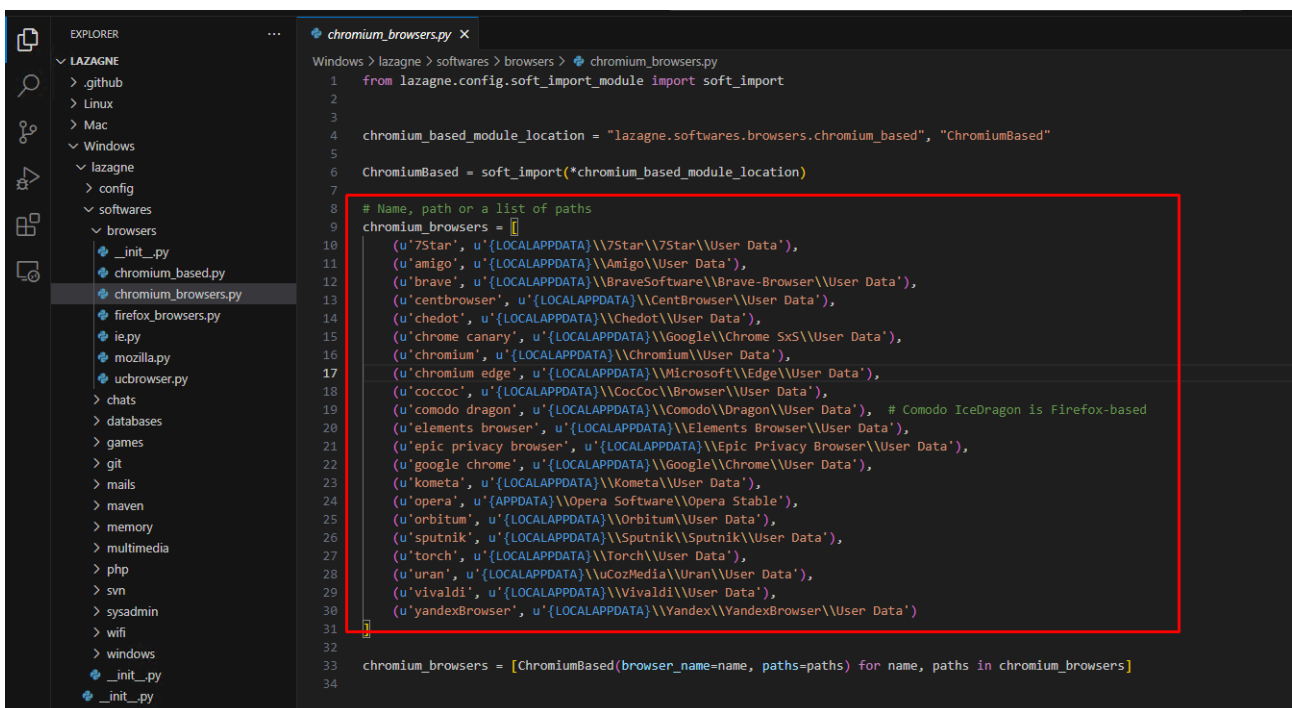
=====
                        The Lazagne Project
                        ! BANG BANG !
=====

positional arguments:
{all,browsers,chats,databases,games,git,mails,maven,memory,multimedia,php,svn,sysadmin,windows,wifi,unused}
    all                Choose a main command
    browsers           Run all modules
    chats              Run browsers module
    databases          Run chats module
    games              Run databases module
    git                Run games module
    mails              Run git module
    maven              Run mails module
    memory             Run maven module
    multimedia         Run memory module
    php                Run multimedia module
    svn                Run php module
    sysadmin           Run svn module
    windows            Run sysadmin module
    wifi               Run windows module
    unused             Run wifi module

optional arguments:
-h, --help            show this help message and exit
-version              Lazagne version
```

Lazagne help menu

Examining the code for Lazagne and HackBrowserData, it is clear that both tools extract data from predefined file locations in the operating system. Both tools read the following known file paths.



```
Windows > lazagne > softwares > browsers > chromium_browsers.py
1 from lazagne.config.soft_import_module import soft_import
2
3
4 chromium_based_module_location = "lazagne.softwares.browsers.chromium_based", "ChromiumBased"
5
6 ChromiumBased = soft_import(*chromium_based_module_location)
7
8 # Name, path or a list of paths
9 chromium_browsers = []
10 (u'7Star', u'{LOCALAPPDATA}\\7Star\\7Star\\User Data'),
11 (u'amigo', u'{LOCALAPPDATA}\\Amigo\\User Data'),
12 (u'brave', u'{LOCALAPPDATA}\\BraveSoftware\\Brave-Browser\\User Data'),
13 (u'centbrowser', u'{LOCALAPPDATA}\\CentBrowser\\User Data'),
14 (u'chedot', u'{LOCALAPPDATA}\\Chedot\\User Data'),
15 (u'chrome canary', u'{LOCALAPPDATA}\\Google\\Chrome SxS\\User Data'),
16 (u'chromium', u'{LOCALAPPDATA}\\Chromium\\User Data'),
17 (u'chromium edge', u'{LOCALAPPDATA}\\Microsoft\\Edge\\User Data'),
18 (u'coccoc', u'{LOCALAPPDATA}\\CocCoc\\Browser\\User Data'),
19 (u'comodo dragon', u'{LOCALAPPDATA}\\Comodo\\Dragon\\User Data'), # Comodo IceDragon is Firefox-based
20 (u'elements browser', u'{LOCALAPPDATA}\\Elements Browser\\User Data'),
21 (u'epic privacy browser', u'{LOCALAPPDATA}\\Epic Privacy Browser\\User Data'),
22 (u'google chrome', u'{LOCALAPPDATA}\\Google\\Chrome\\User Data'),
23 (u'kometa', u'{LOCALAPPDATA}\\Kometa\\User Data'),
24 (u'opera', u'{APPDATA}\\Opera Software\\Opera Stable'),
25 (u'orbitum', u'{LOCALAPPDATA}\\Orbitum\\User Data'),
26 (u'sputnik', u'{LOCALAPPDATA}\\Sputnik\\Sputnik\\User Data'),
27 (u'torch', u'{LOCALAPPDATA}\\Torch\\User Data'),
28 (u'uran', u'{LOCALAPPDATA}\\uCozMedia\\Uran\\User Data'),
29 (u'vivaldi', u'{LOCALAPPDATA}\\Vivaldi\\User Data'),
30 (u'yandexBrowser', u'{LOCALAPPDATA}\\Yandex\\YandexBrowser\\User Data')
31
32
33 chromium_browsers = [ChromiumBased(browser_name=name, paths=paths) for name, paths in chromium_browsers]
34
```

Lazagne source code

```
fileFoxList = map[string]struct {
    name string
    storage string
    profilePath string
    items []Item.Item
}{
    "firefox": {
        name: firefoxName,
        profilePath: firefoxProfilePath,
        items: item.DefaultFirefox,
    },
}

var (
    chromeUserDataPath = homeDir + "/AppData/Local/Google/Chrome/User Data/Default/"
    chromeBetaUserDataPath = homeDir + "/AppData/Local/Google/Chrome Beta/User Data/Default/"
    chromiumUserDataPath = homeDir + "/AppData/Local/Chromium/User Data/Default/"
    edgeProfilePath = homeDir + "/AppData/Local/Microsoft/Edge/User Data/Default/"
    braveProfilePath = homeDir + "/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/"
    speed360ProfilePath = homeDir + "/AppData/Local/360Chrome/Chrome/User Data/Default/"
    qqBrowserProfilePath = homeDir + "/AppData/Local/Tencent/QQBrowser/User Data/Default/"
    operaProfilePath = homeDir + "/AppData/Roaming/Opera Software/Opera Stable/"
    operaGXProfilePath = homeDir + "/AppData/Roaming/Opera Software/Opera GX Stable/"
    vivavdiProfilePath = homeDir + "/AppData/Local/Vivaldi/User Data/Default/"
    cocccocProfilePath = homeDir + "/AppData/Local/CocCoc/Browser/User Data/Default/"
    yandexProfilePath = homeDir + "/AppData/Local/Yandex/YandexBrowser/User Data/Default/"
    dcBrowserProfilePath = homeDir + "/AppData/Local/DC/Browser/User Data/Default/"
    sogouProfilePath = homeDir + "/AppData/Roaming/SogouExplorer/WebKit/Default/"

    firefoxProfilePath = homeDir + "/AppData/Roaming/Mozilla/Firefox/Profiles/"
)
```

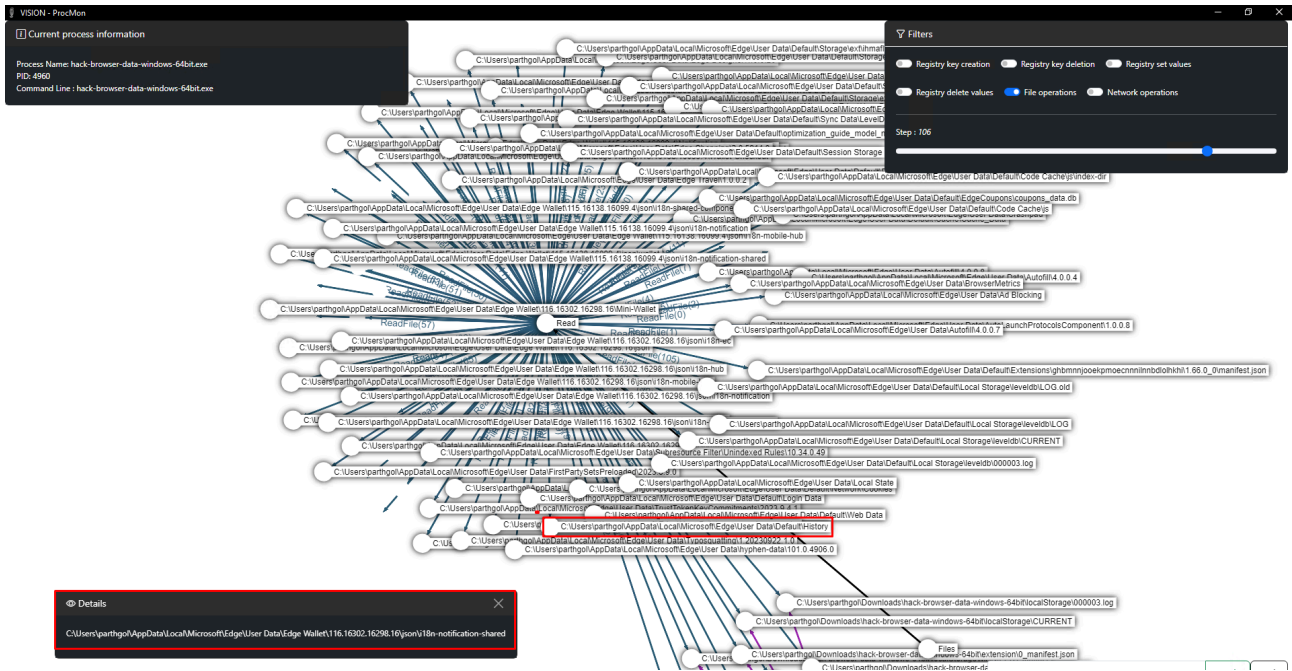
HackBrowserData source code

We can also execute both tools and observe them in [Procmon](#) to further corroborate our findings. Procmon will show us any process creation, registry/file access and other events to help us narrow down key behaviours among browser credential extraction tools.

Time of Day	Process Name	PID	Operation	Path	Result	Detail	Event Class	Seque...	Image Path	Command Line
4:11:00.423870 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 0, Length: ...	File System	20382	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.424242 AM	LaZagne.exe	11112	QueryDirectory	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	FileInformationCla...	File System	20383	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.424297 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 20,480, Le...	File System	20384	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.424350 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 28,672, Le...	File System	20385	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.425132 AM	LaZagne.exe	11112	QueryDirectory	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	FileInformationCla...	File System	20386	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.425153 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 4,096, Len...	File System	20387	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4254905 AM	LaZagne.exe	11112	QueryDirectory	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	FileInformationCla...	File System	20388	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4255019 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 12,288, Le...	File System	20389	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4255777 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Offset: 16,384, Le...	File System	20390	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4257797 AM	LaZagne.exe	11112	QueryDirectory	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	FileInformationCla...	File System	20391	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4258117 AM	LaZagne.exe	11112	QueryDirectory	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	NO MORE FILES	FileInformationCla...	File System	20392	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4258306 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS		File System	20393	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4261553 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	NAME NOT FOUND	Desired Access: R...	File System	20394	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4262830 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: R...	File System	20395	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4263261 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	VolumeCreationTi...	File System	20396	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4263489 AM	LaZagne.exe	11112	QueryAllInfor...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	CreationTime: 8/31...	File System	20397	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4263584 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	NAME NOT FOUND	Desired Access: R...	File System	20398	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4264439 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	NAME NOT FOUND	Desired Access: R...	File System	20399	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4265271 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: R...	File System	20400	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4265459 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	VolumeCreationTi...	File System	20401	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4265485 AM	LaZagne.exe	11112	QueryAllInfor...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	CreationTime: 8/31...	File System	20402	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4265647 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS		File System	20403	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4266371 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	NAME NOT FOUND	Desired Access: R...	File System	20404	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4267474 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: G...	File System	20405	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4268020 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	VolumeCreationTi...	File System	20406	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4268235 AM	LaZagne.exe	11112	QueryAllInfor...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	CreationTime: 8/31...	File System	20407	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4269072 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Desired Access: G...	File System	20408	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4270474 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Temp\iddobmto	BUFFER OVERFL...	VolumeCreationTi...	File System	20409	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4270588 AM	LaZagne.exe	11112	QueryAllInfor...	C:\Users\partngol\AppData\Local\Temp\iddobmto	BUFFER OVERFL...	CreationTime: 10/2...	File System	20410	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4270783 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Offset: 0, Length: ...	File System	20411	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4271159 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Offset: 0, Length: ...	File System	20412	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4273577 AM	LaZagne.exe	11112	WriteFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Offset: 0, Length: ...	File System	20413	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4272749 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Offset: 16,384, Le...	File System	20414	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4272785 AM	LaZagne.exe	11112	WriteFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Offset: 16,384, Le...	File System	20415	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4273495 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Offset: 32,768, Le...	File System	20416	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4273873 AM	LaZagne.exe	11112	WriteFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Offset: 32,768, Le...	File System	20417	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4273865 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Offset: 49,152, Le...	File System	20418	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4280353 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	END OF FILE	Offset: 57,344, Le...	File System	20419	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4280307 AM	LaZagne.exe	11112	ReadFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	END OF FILE	Offset: 57,344, Le...	File System	20420	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4280556 AM	LaZagne.exe	11112	WriteFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Offset: 49,152, Le...	File System	20421	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4280648 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS		File System	20422	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4282251 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: R...	File System	20423	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4283558 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: R...	File System	20424	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4283738 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	VolumeCreationTi...	File System	20425	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4283868 AM	LaZagne.exe	11112	QueryAllInfor...	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	BUFFER OVERFL...	CreationTime: 8/31...	File System	20426	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4283999 AM	LaZagne.exe	11112	CloseFile	C:\Users\partngol\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	SUCCESS	Desired Access: R...	File System	20427	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4285377 AM	LaZagne.exe	11112	CreateFile	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	Desired Access: R...	File System	20428	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers
4:11:00.4285517 AM	LaZagne.exe	11112	QueryInforma...	C:\Users\partngol\AppData\Local\Temp\iddobmto	SUCCESS	CreationTime: 10/2...	File System	20429	C:\Users\partngol\Downloads\LaZagne.exe	LaZagne.exe browsers

LaZagne process view in Procmon

We can also visualise the Procmon logs using [Vision-ProcMon](#), which allows for a graphical view of operations such as file access and modification of registry keys. Utilising the Step Option in Vision-Procmon, we can trace the events and identify multiple paths used to dump browser credentials.



hackbrowserdata procmon log graph view in Vision-procmon

Analysing the procmon logs of various open and closed source tools, we can confirm that all tools access fixed paths where the browsers store their data(such as cookies, credentials, history) and then process these files to extract credentials.

Detecting Unauthorized Access to Browser Files

To set up correct monitoring and detection of browser credential extraction, we need to enable auditing features in Windows to receive logs. We need to get process creation logs to monitor for known malicious command lines and file access logs to monitor unauthorised access to browser files.

Enabling Process Creation Event Logs

Enabling Process Creation auditing will create [Event ID 4688](#) and other necessary details such as Process Path, Parent, Command line, etc, using which we can monitor for malicious command lines. We will use Group Policy Editor to set up Process Creation Auditing.

Configuring Process Auditing:

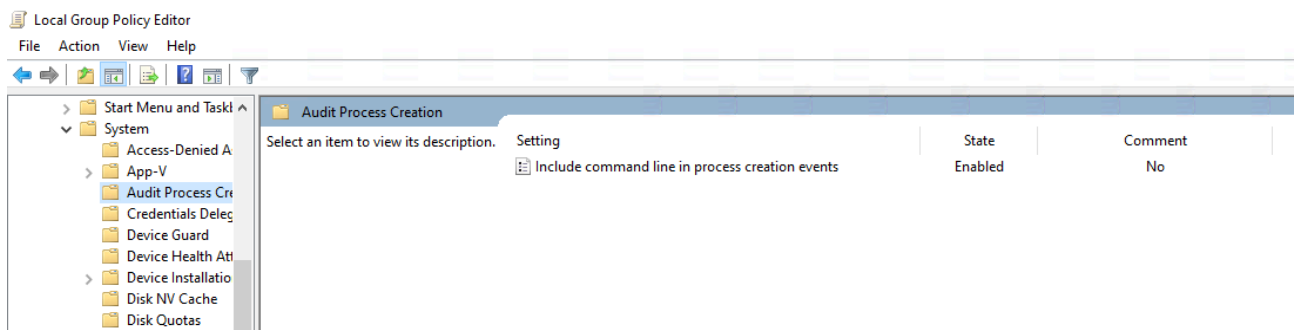
1. Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Detailed Tracking
2. Select: Audit Process Creation, Select: Success + Failure, Select: OK

Policy	Subcategory	Audit Events
Configuration	Audit DPAPI Activity	Not Configured
Settings	Audit PNP Activity	Not Configured
Settings	Audit Process Creation	Success and Failure
Resolution Policy (Startup/Shutdown)	Audit Process Termination	Success and Failure
Shared Printers	Audit RPC Events	Not Configured
Printer Settings	Audit Token Right Adjusted	Not Configured
Mount Policies		

Local Group Policy Editor

Configuring Command Line in Process Auditing:

1. Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation
2. Select: Include command line in process creation events, Select Enabled, and Press OK

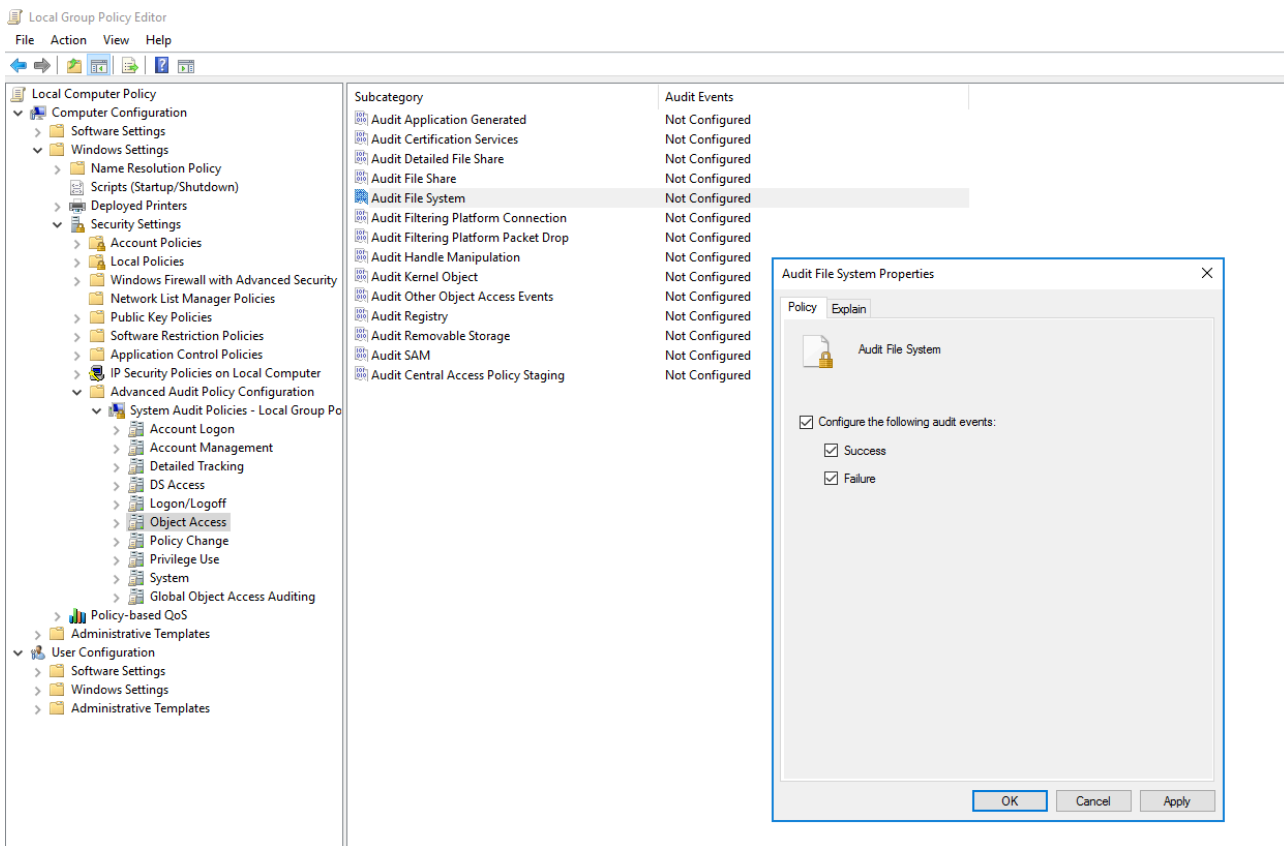


Local Group Policy Editor

Enabling File Access Audit Logs

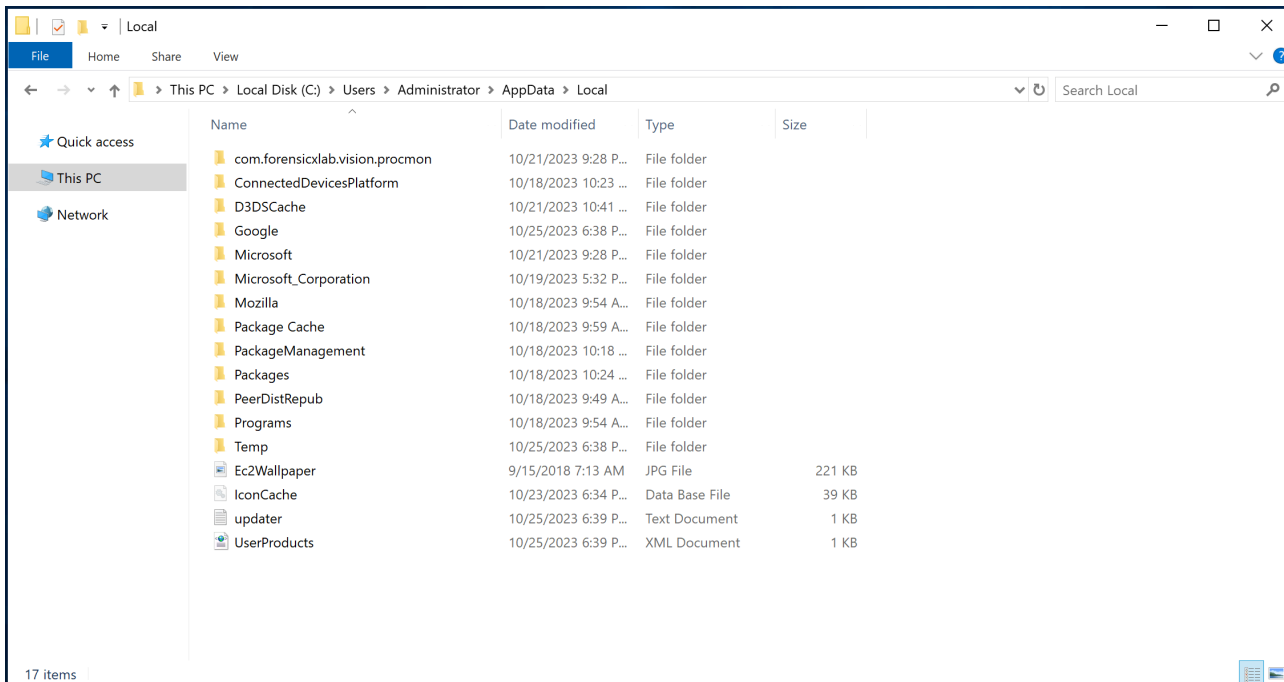
[Enabling File System auditing](#) is a two-step process where we first enable auditing in group policy and then configure individual files/folders we want to monitor. Configuring File Access auditing will create [Event ID 4663](#) along with other necessary details such as Object Path and which process is accessing the files. We will use Group Policy Editor to set up Process Creation Auditing.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Object Access -> Audit File System



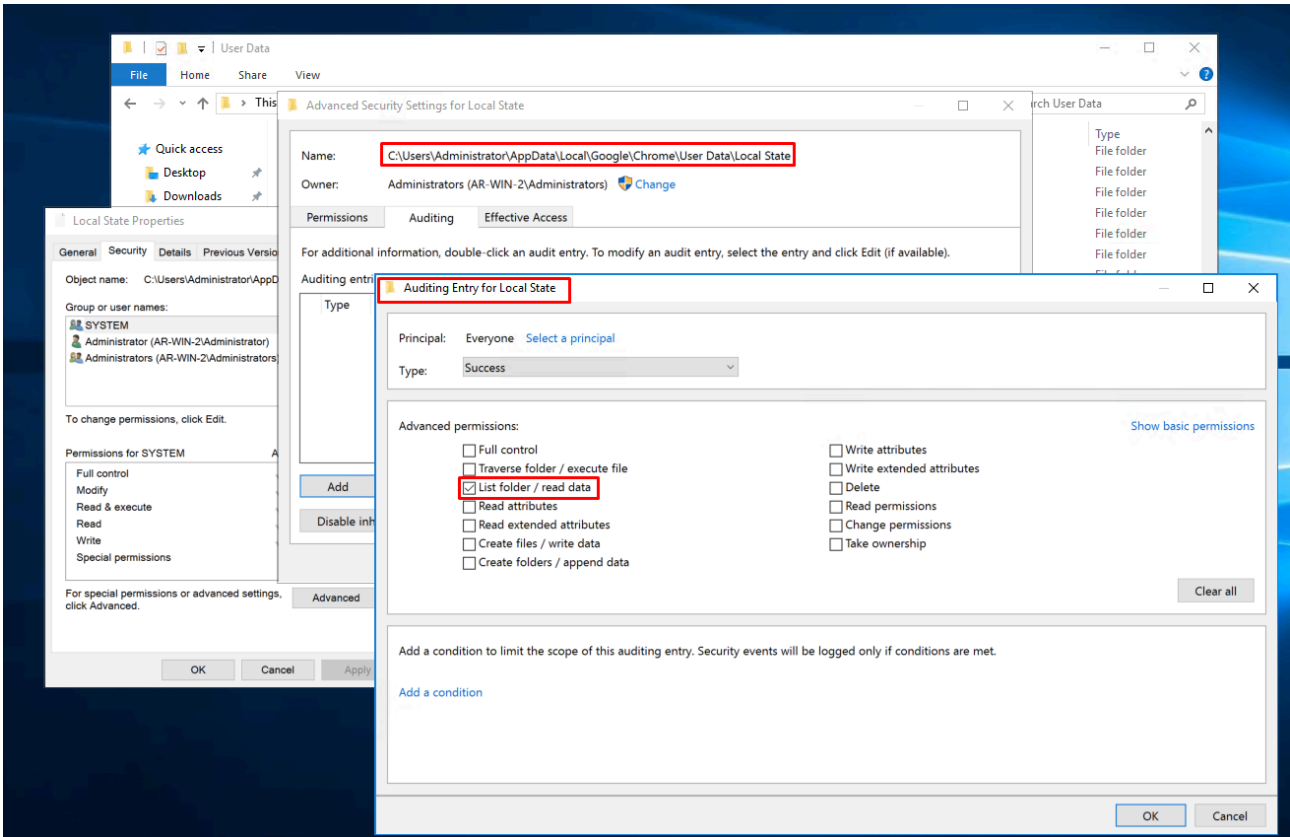
Local Group Policy Editor

1. Navigate to your Local Appdata folder at %LOCALAPPDATA% and configure auditing for each browser folder.



Browser important Files / Folder directory

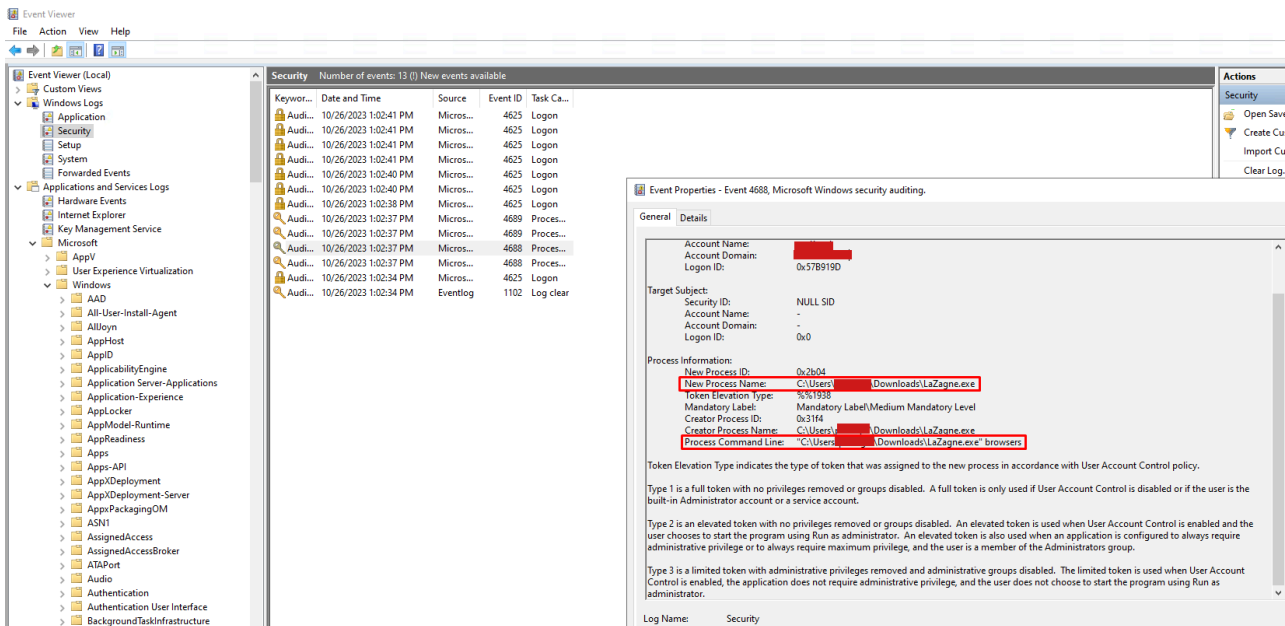
1. Right-click the target file/folder and select **"Properties"**
2. Select **"Security"** tab and click **"Advanced"**
3. Select **"Auditing"** tab and click **"Continue"**
4. Click **"Add"** to insert a new auditing entry
5. Click **"Select a principal"** and insert **"Everyone"**
6. Click **"Clear all"** in the permissions and click **"Show advanced permissions"**
7. Tick **"List folder / read data"**
8. Save all the changes



Enable Auditing for List folder / read data

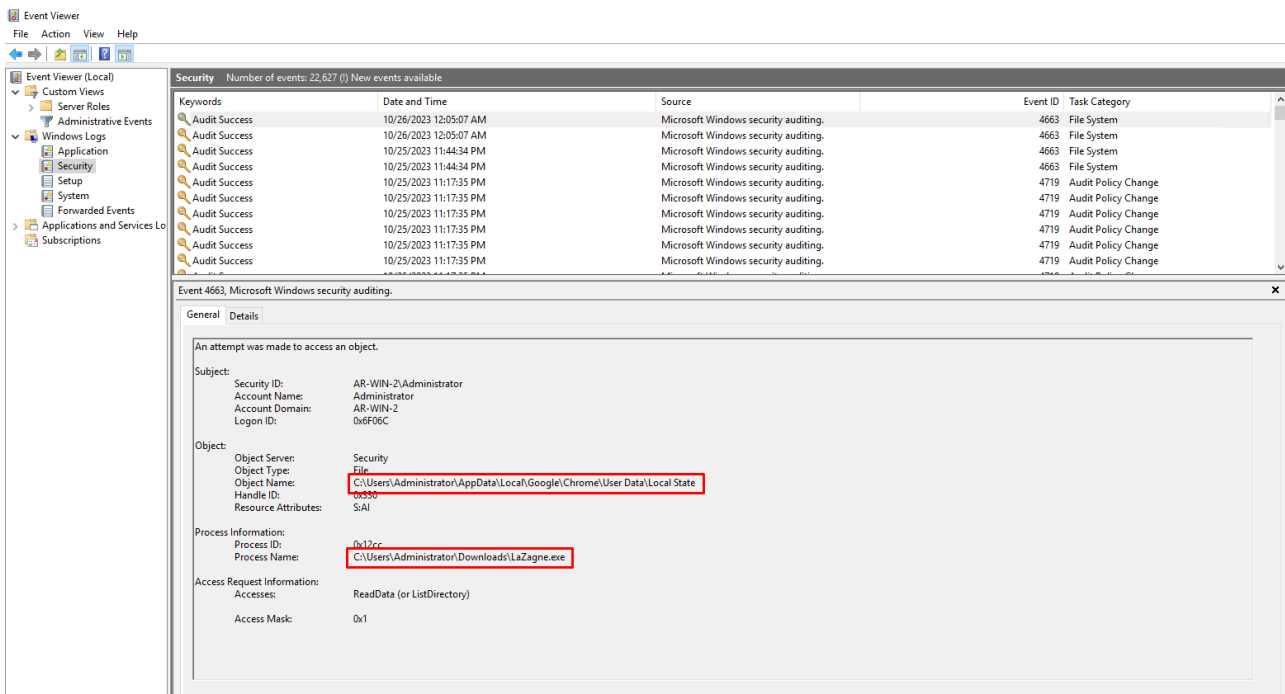
Ensuring Visibility

After enabling Windows event logs, if you execute Lazagne again, you can see the event logs that indicate the execution of Lazagne with the "browsers" parameter.



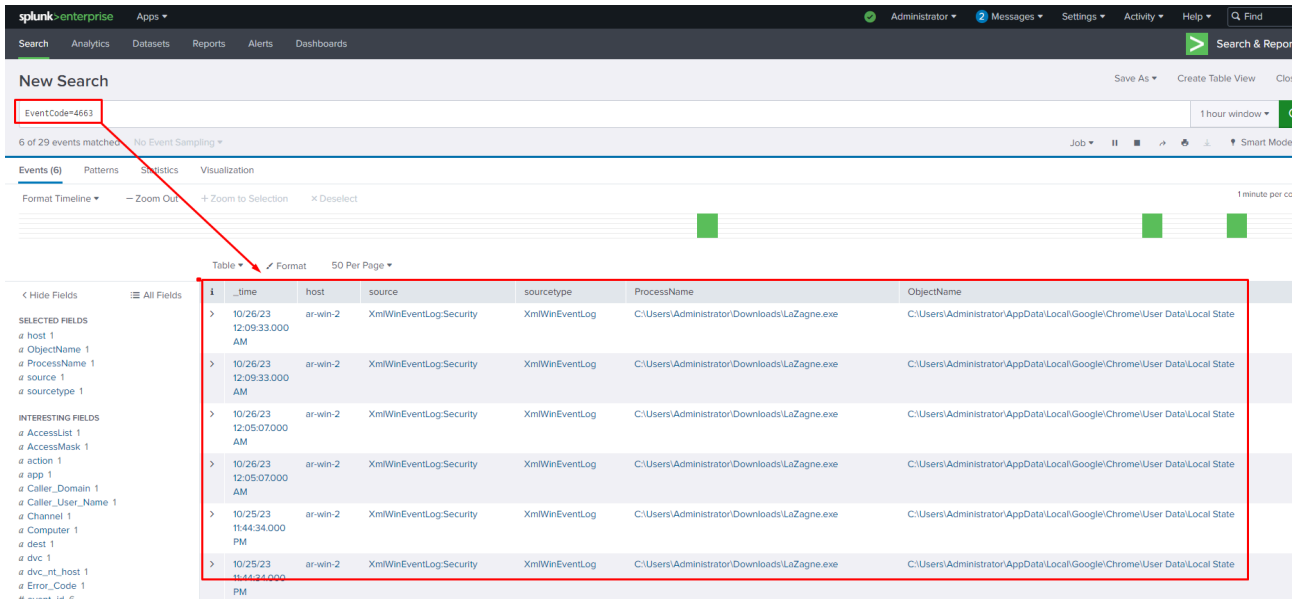
LaZagne Process Creation Event view in Event Viewer

We can also see the File Access Event Logs in Event Viewer → Windows Logs → Security logs by following Windows 4663 Events (**An attempt was made to access an object**)



File Access Event in Event Viewer

These events can also be forwarded to your SIEM dashboard so you can build appropriate alerts for these behaviours.



Splunk Dashboard filter for File Access Events

Detection Rules for the Win

By analyzing event logs, we can create a [Sigma rule](#) that can detect any unauthorized attempt to execute Lazagne for dumping browser credentials. We can use these rules to detect malicious or unauthorized access to browser credentials.

Command Line Detection

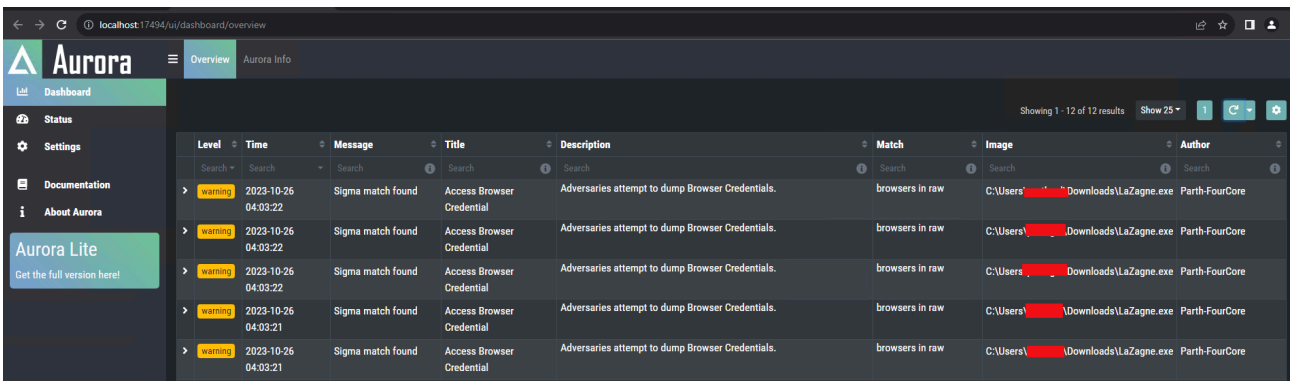
Command line detections are based on default and known command line patterns used by threat actors during the execution of the binary. For any unmodified tool, we can detect its presence either via its hash or by the known command line for this tool. The Sigma rule will detect the presence of the keyword "browser" in the command line along with other keywords commonly used by Lazagne to extract browser credentials.



```
1title: Access Browser Credential
2description: Adversaries may search for common password storage locations to obtain user credentials.
3id: 198c1a5c-72cc-11ee-b962-0242ac120002
4status: test
5author: Parth-FourCore
6date: 2023/10/21
7tags:
8  - attack.t1003
9  - attack.credential_access
10logsource:
11  product: windows
12detection:
13  keywords:
14    - 'browsers'
```

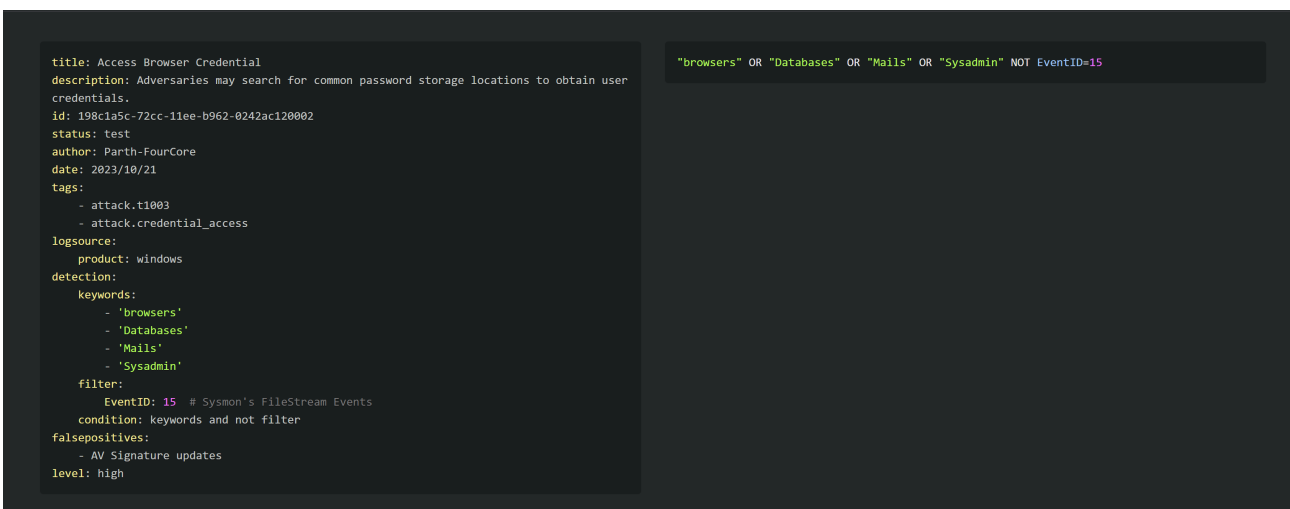
```
15 - 'Databases'  
16 - 'Mails'  
17 - 'Sysadmin'  
18 filter:  
19     EventID: 15 # Sysmon's FileStream Events  
20 condition: keywords and not filter  
21falsepositives:  
22 - AV Signature updates  
23 - Files with Browsers in their filename  
24level: high
```

In order to test the created Sigma rule, we can utilise [Aurora](#). Aurora is a lightweight and customisable EDR that is based on Sigma rules and can be [quickly set up](#) to test your rules.

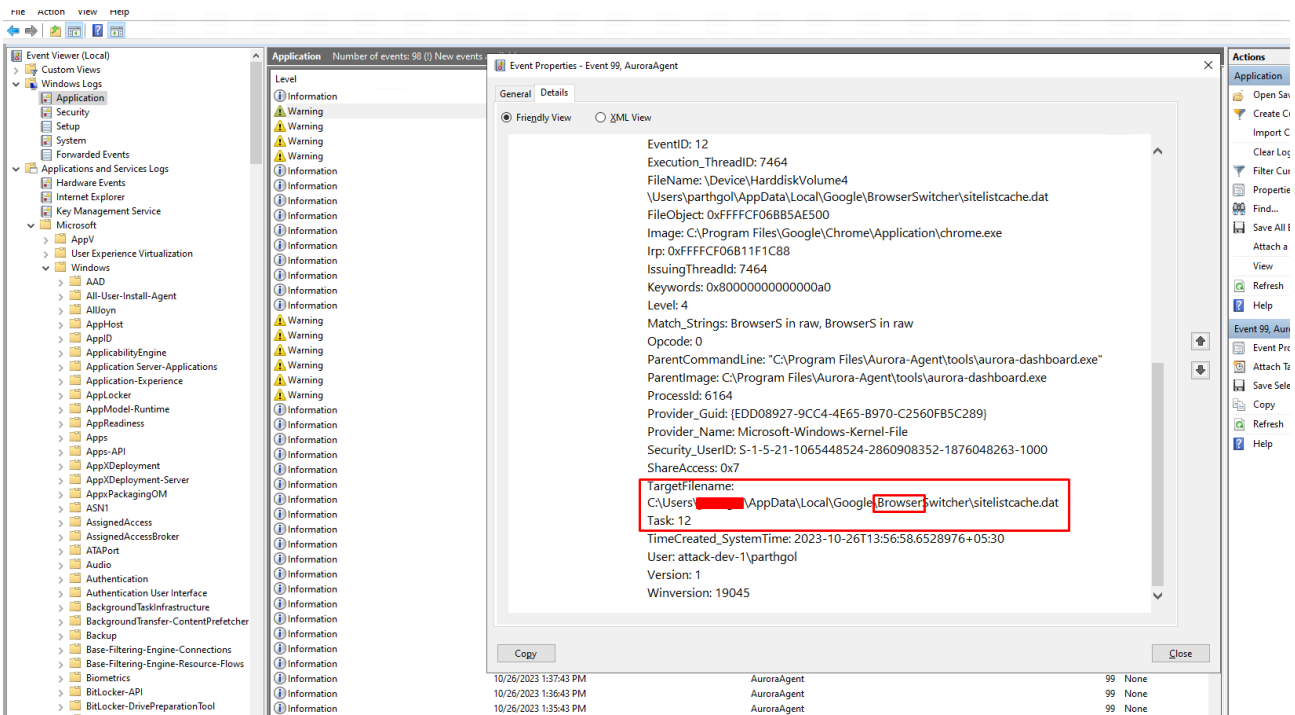


Aurora Dashboard

We can use the same Sigma rule to convert into SIEM, EDR, XDR, and data lake query formats to search related event logs and set alerts.



Let us use this search query in the [Splunk](#) dashboard



False Positive Event for Browser Credentials

Detect Behaviours not Tools

We can create a different sigma rule which, rather than focusing on command line parameters, focuses on the file access events by the unknown process to alert for malicious behaviours. It is essential to have all the browser paths mentioned in the Sigma rule so that we can monitor access events for all available browsers on the host machine.



- 1- '\cookies.sqlite'
- 2- 'release\key3.db' # Firefox
- 3- 'release\key4.db' # Firefox
- 4- 'release\logins.json' # Firefox
- 5- '\Appdata\Local\Chrome\User Data\Default>Login Data' # Chrome
- 6- '\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies' # google chrome
- 7- '\AppData\Local\Google\Chrome\User Data\Local State'
- 8- '\Appdata\Local\7Star\7Star\User Data' # 7Star
- 9- '\Appdata\Local\Amigo\User Data' # amigo
- 10- '\Appdata\Local\BraveSoftware\Brave-Browser\User Data' # brave
- 11- '\Appdata\Local\CentBrowser\User Data' # centbrowser
- 12- '\Appdata\Local\Chedot\User Data' # chedot
- 13- '\Appdata\Local\Google\Chrome SxS\User Data' # chrome canary
- 14- '\Appdata\Local\Chromium\User Data' # chromium
- 15- '\Appdata\Local\Microsoft\Edge\User Data' # chromium edge
- 16- '\Appdata\Local\CocCoc\Browser\User Data' # coccoc
- 17- '\Appdata\Local\Comodo\Dragon\User Data' # Comodo IceDragon is Firefox-based

```
18- '\\Appdata\\Local\\Elements Browser\\User Data' # elements browser
19- '\\Appdata\\Local\\Epic Privacy Browser\\User Data' # epic privacy browser
20- '\\Appdata\\Local\\Kometa\\User Data' # kometa
21- '\\Appdata\\Opera Software\\Opera Stable' # opera
22- '\\Appdata\\Local\\Orbitum\\User Data' # orbitum
23- '\\Appdata\\Local\\Sputnik\\Sputnik\\User Data' # sputnik
24- '\\Appdata\\Local\\Torch\\User Data' # torch
25- '\\Appdata\\Local\\uCozMedia\\Uran\\User Data' # uran
26- '\\Appdata\\Local\\Vivaldi\\User Data' # vivaldi
27- '\\Appdata\\Local\\Yandex\\YandexBrowser\\User Data' # yandexBrowser
28- '\\Appdata\\Local\\Mozilla\\Firefox' # firefox
29- '\\Appdata\\Local\\NETGATE Technologies\\BlackHawk' # blackHawk
30- '\\Appdata\\Local\\8pecxstudios\\Cyberfox' # cyberfox
31- '\\Appdata\\Local\\Comodo\\IceDragon' # comodo IceDragon
32- '\\Appdata\\Local\\K-Meleon' # k-Meleon
33- '\\Appdata\\Local\\Mozilla\\icecat' # icecat
34- '\\Appdata\\Local\\UCBrowser' # UCbrowser
```

Weeding out False Positives

Since these files and paths are not only accessed by unauthorized tools and processes but also used by antivirus software, legitimate binaries, 3rd party backup software, and other authorized tools in your environment, It is crucial to add appropriate filters to the Sigma rule to prevent false positives. The following list is what we observed in our test environment, which are false positives. Auditing the rules in your production environment is crucial to eliminate false positives.

Windows defender	C:\\ProgramData\\Microsoft\\Windows Defender\\MsMpEng.exe
Windows Installer	C:\\Windows\\System32\\msiexec.exe
Browser Files	chrome.exe, edge.exe

Here, adding all file and folder paths with a filter parameter will help avoid false positives.

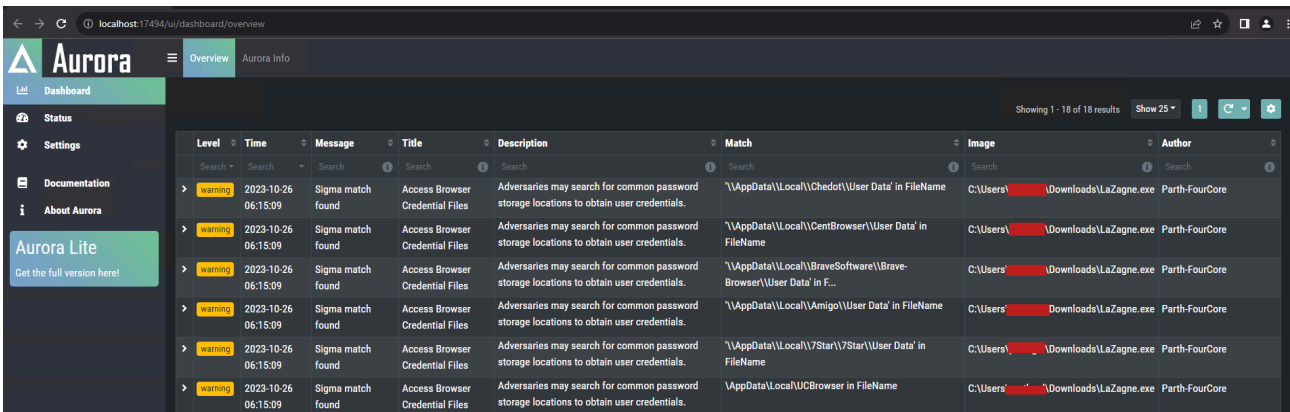


```
1title: Access Browser Credential Files
2description: Adversaries may search for common password storage locations to obtain user credentials.
3id: 198c1a5c-72cc-11ee-b962-0242ac120002
4status: experimental
5author: Parth-FourCore
6date: 2023/10/24
7tags:
8 - attack.t1003
9 - attack.credential_access
10logsource:
11 category: file_access
```

```
12 product: windows
13detection:
14 selection_all:
15   ObjectName|contains:
16     - 'cookies.sqlite'
17     - 'release\key3.db' # Firefox
18     - 'release\key4.db' # Firefox
19     - 'release\logins.json' # Firefox
20     - '\Appdata\Local\Chrome\User Data\Default>Login Data' # Crome
21     - '\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies' # googel crome
22     - '\AppData\Local\Google\Chrome\User Data\Local State'
23     - '\Appdata\Local\7Star\7Star\User Data' # 7Star
24     - '\Appdata\Local\Amigo\User Data' # amigo
25     - '\Appdata\Local\BraveSoftware\Brave-Browser\User Data' # brave
26     - '\Appdata\Local\CentBrowser\User Data' # centbrowser
27     - '\Appdata\Local\Chedot\User Data' # chedot
28     - '\Appdata\Local\Google\Chrome SxS\User Data' # chrome canary
29     - '\Appdata\Local\Chromium\User Data' # chromium
30     - '\Appdata\Local\Microsoft\Edge\User Data' # chromium edge
31     - '\Appdata\Local\CocCoc\Browser\User Data' # coccoc
32     - '\Appdata\Local\Comodo\Dragon\User Data' # Comodo IceDragon is Firefox-based
33     - '\Appdata\Local\Elements Browser\User Data' # elements browser
34     - '\Appdata\Local\Epic Privacy Browser\User Data' # epic privacy browser
35     - '\Appdata\Local\Kometa\User Data' # kometa
36     - '\Appdata\Opera Software\Opera Stable' # opera
37     - '\Appdata\Local\Orbitum\User Data' # orbitum
38     - '\Appdata\Local\Sputnik\Sputnik\User Data' # sputnik
39     - '\Appdata\Local\Torch\User Data' # torch
40     - '\Appdata\Local\CozMedia\Uran\User Data' # uran
41     - '\Appdata\Local\Vivaldi\User Data' # vivaldi
42     - '\Appdata\Local\Yandex\YandexBrowser\User Data' # yandexBrowser
43     - '\Appdata\Local\Mozilla\Firefox' # firefox
44     - '\Appdata\Local\NETGATE Technologies\BlackHawk' # blackHawk
45     - '\Appdata\Local\8pecxstudios\Cyberfox' # cyberfox
46     - '\Appdata\Local\Comodo\IceDragon' # comodo IceDragon
47     - '\Appdata\Local\K-Meleon' # k-Meleon
48     - '\Appdata\Local\Mozilla\icecat' # icecat
49     - '\Appdata\Local\UCBrowser' # UCbrowser
50 filter_main_system:
51   Image: System
52   ParentImage: Idle
53 filter_main_generic:
54   Image|startswith:
55     - 'C:\Program Files\'
56     - 'C:\Program Files (x86)\'
57     - 'C:\WINDOWS\system32\'
58     - 'C:\WINDOWS\SysWOW64\'
59 filter_optional_defender:
60   Image|startswith: 'C:\ProgramData\Microsoft\Windows Defender\'
61   Image|endswith:
62     - '\MpCopyAccelerator.exe'
63     - '\MsMpEng.exe'
```

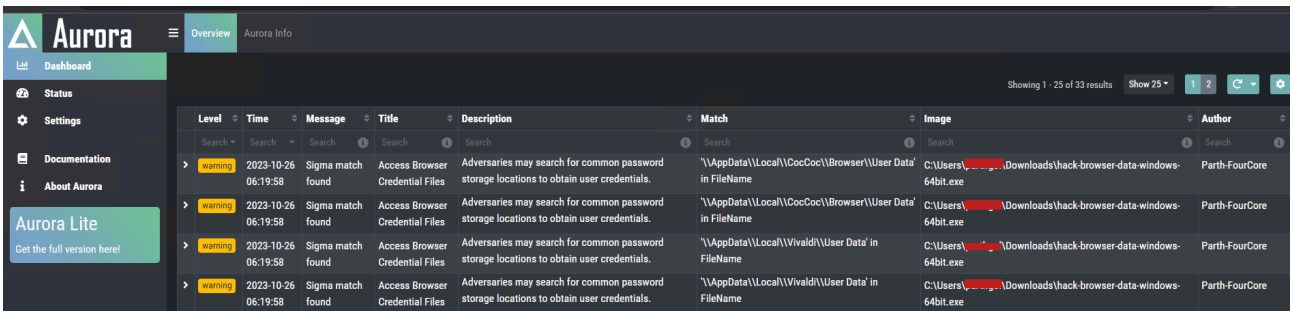
```
64 filter_optional_msieexec:
65   ParentImage: 'C:\Windows\System32\msieexec.exe'
66 condition: selection_all and not 1 of filter_main_* and not 1 of filter_optional_*
67falsepositives:
68 - Antivirus, Anti-Spyware, Anti-Malware Software
69 - Backup software
70 - Legitimate software
71level: high
```

Let's execute the lazagne and HackBrowserData tools with the Aurora agent to verify the new Sigma rule.



Aurora Dashboard

We will receive an alert when HackBrowserData attempts to access browser credential files as well.



Aurora Dashboard

These rules are now ready for use in our environment, albeit with a clause. This rule will not get triggered in case of a process injection attack; however, we will discuss that in a future blog. Identifying false positives and updating your rules accordingly is a continuous process.

Setting up alerts

Let's convert the Sigma rule to a Splunk query and use it to search in the Splunk dashboard.

Save As Alert ✕

Settings

Title:

Description:

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Expires: hour(s) ▾

Trigger Conditions

Trigger alert when:

Throttle?

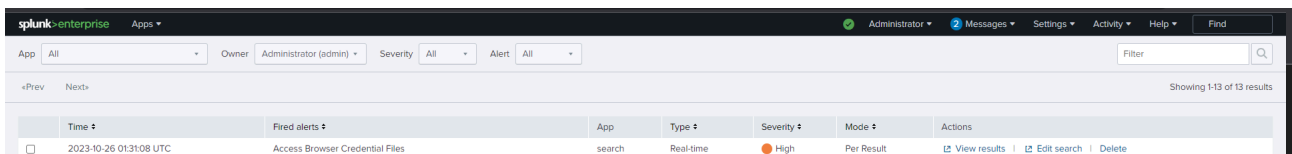
Trigger Actions

When triggered:

▾	Add to Triggered Alerts Remove
	Severity: <input type="text" value="High ▾"/>

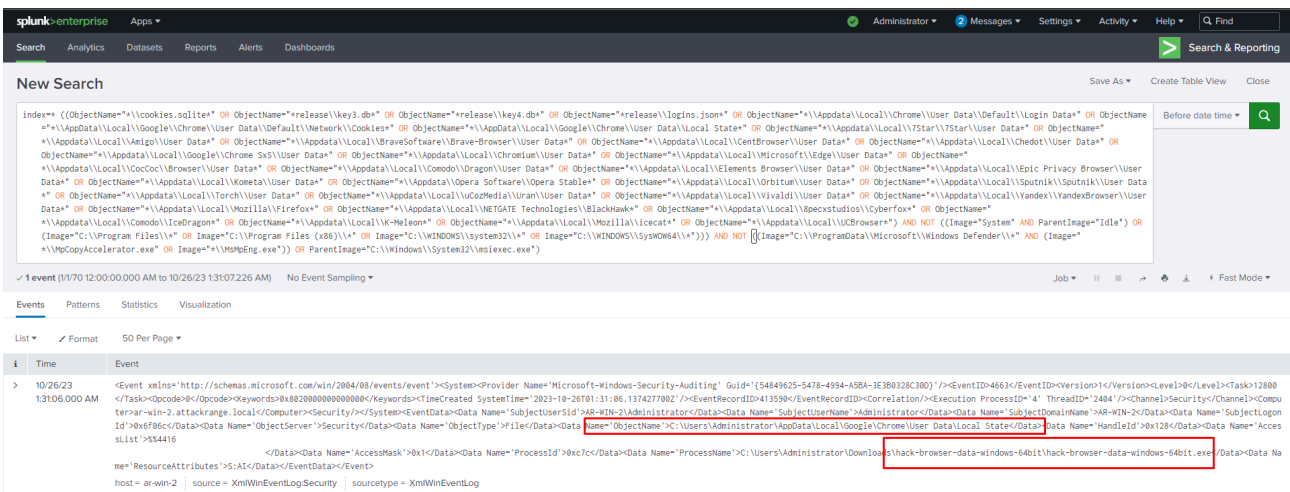
Alert Menu

Click on the Save button to save the alert. Now, let's try triggering the alert with different tools to ensure that the alert we created using a Sigma rule works with any browser credential extraction tool. Once configured, we can see that the alert is also triggered with different hacking tools.



Triggered Alert

When you click on "View Result", you will be able to locate the event that triggered this alert.

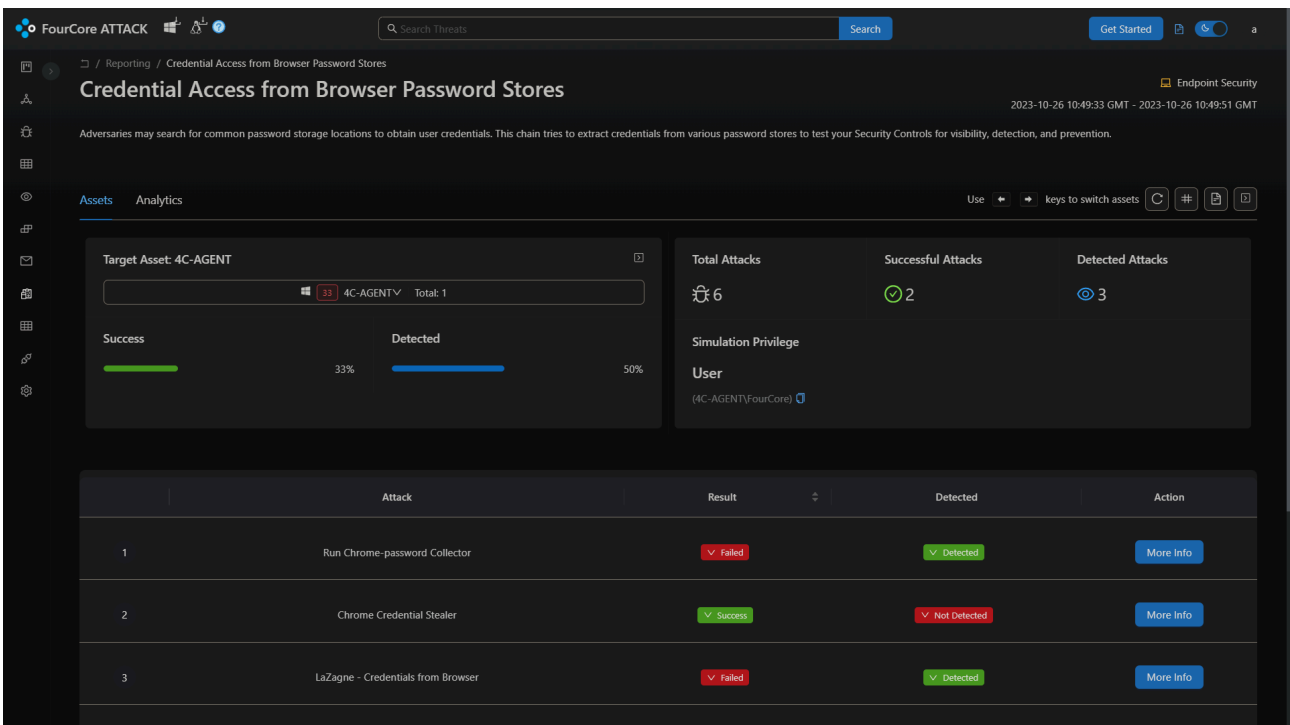


Event which Triggered Alert

By specifying file names and file paths in our Sigma rule, we can detect any unauthorised access to valuable files such as usernames and passwords stored in the browser. Additionally, we can identify any unauthorised execution of hacker tools which try to obtain browser credentials.

Browser Credential Access with FourCore ATTACK

The FourCore ATTACK platform can emulate the different types of browser-based credential access techniques, such as via LaZagne, via using Powershell or by accessing the files directly. These variants can be hunted using the Sigma rules shared in this post.



Learn about **writing your own Sigma rule** via this [deep dive into working with Sigma](#).

You can also read more about using **Windows Event Log IDs for threat-hunting** [here](#).

References

1. [Browser Password Managers](#)
2. [Redline Stealer](#)
3. [Browser Credential Harvesting MITRE](#)
4. [Nirsoft WebBrowserPassView](#)
5. [LaZagne open-source password stealer](#)
6. [Process Auditing Event ID 4663](#)
7. [Process Auditing Event ID 4688](#)
8. [Sigma Rules Github](#)
9. [Learn More about Splunk](#)

Source: <https://fourcore.io/blogs/threat-hunting-browser-credential-stealing>