T1217 - Browser Bookmark Discovery

Description from ATT&CK

> Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.
> Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially Credentials In Files associated with logins cached by a browser.
>
> Specific storage locations vary based on platform and/or application, but browser bookmarks are typically stored in local files/databases.

Atomic Tests

- Atomic Test #1 - List Mozilla Firefox Bookmark Database Files on Linux
- Atomic Test #2 - List Mozilla Firefox Bookmark Database Files on macOS

- Atomic Test #3 - List Google Chrome Bookmark JSON Files on macOS
- Atomic Test #4 - List Google Chrome / Opera Bookmarks on Windows with powershell
- Atomic Test #5 - List Google Chrome / Edge Chromium Bookmarks on Windows with command prompt
- Atomic Test #6 - List Mozilla Firefox bookmarks on Windows with command prompt
- Atomic Test #7 - List Internet Explorer Bookmarks using the command prompt
- Atomic Test #8 - List Safari Bookmarks on MacOS

Atomic Test #1 - List Mozilla Firefox Bookmark Database Files on Linux

Searches for Mozilla Firefox's places.sqlite file (on Linux distributions) that contains bookmarks and lists any found instances to a text file.

Supported Platforms: Linux

auto_generated_guid: 3a41f169-a5ab-407f-9269-abafdb5da6c2

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed.	Path	/tmp/T1217-Firefox.txt

Attack Commands: Run with `sh`!

```
find / -path "*.mozilla/firefox/*/places.sqlite" 2>/dev/null -exec echo {} >> #{ou
cat #{output_file} 2>/dev/null
```

Cleanup Commands:

```
rm -f #{output_file} 2>/dev/null
```

Atomic Test #2 - List Mozilla Firefox Bookmark Database Files on macOS

Searches for Mozilla Firefox's places.sqlite file (on macOS) that contains bookmarks and lists any found instances to a text file.

Supported Platforms: macOS

auto_generated_guid: 1ca1f9c7-44bc-46bb-8c85-c50e2e94267b

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed.	Path	/tmp/T1217_Firefox.txt

Attack Commands: Run with `sh`!

```
find / -path "*/Firefox/Profiles/*/places.sqlite" -exec echo {} >> #{output_file} '
cat #{output_file} 2>/dev/null
```

Cleanup Commands:

```
rm -f #{output_file} 2>/dev/null
```

Atomic Test #3 - List Google Chrome Bookmark JSON Files on macOS

Searches for Google Chrome's Bookmark file (on macOS) that contains bookmarks in JSON format and lists any found instances to a text file.

Supported Platforms: macOS

auto_generated_guid: b789d341-154b-4a42-a071-9111588be9bc

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed.	Path	/tmp/T1217-Chrome.txt

Attack Commands: Run with `sh`!

```
find / -path "*/Google/Chrome/*/Bookmarks" -exec echo {} >> #{output_file} \;
cat #{output_file} 2>/dev/null
```

Cleanup Commands:

```
rm -f #{output_file} 2>/dev/null
```

Atomic Test #4 - List Google Chrome / Opera Bookmarks on Windows with powershell

Searches for Google Chrome's and Opera's Bookmarks file (on Windows distributions) that contains bookmarks. Upon execution, paths that contain bookmark files will be displayed.

Supported Platforms: Windows

auto_generated_guid: faab755e-4299-48ec-8202-fc7885eb6545

Attack Commands: Run with `powershell`!

```
Get-ChildItem -Path C:\Users\ -Filter Bookmarks -Recurse -ErrorAction SilentlyCont
```

Atomic Test #5 - List Google Chrome / Edge Chromium Bookmarks on Windows with command prompt

Searches for Google Chromes's and Edge Chromium's Bookmarks file (on Windows distributions) that contains bookmarks. Upon execution, paths that contain bookmark files will be displayed.

Supported Platforms: Windows

auto_generated_guid: 76f71e2f-480e-4bed-b61e-398fe17499d5

Attack Commands: Run with `command_prompt`!

```
where /R C:\Users\ Bookmarks
```

Atomic Test #6 - List Mozilla Firefox bookmarks on Windows with command prompt

Searches for Mozilla Firefox bookmarks file (on Windows distributions) that contains bookmarks in a SQLITE database. Upon execution, paths that contain bookmark files will be displayed.

Supported Platforms: Windows

auto_generated_guid: 4312cdbc-79fc-4a9c-becc-53d49c734bc5

Attack Commands: Run with `command_prompt`!

```
where /R C:\Users\ places.sqlite
```

Atomic Test #7 - List Internet Explorer Bookmarks using the command prompt

This test will list the bookmarks for Internet Explorer that are found in the Favorites folder

Supported Platforms: Windows

auto_generated_guid: 727dbcdb-e495-4ab1-a6c4-80c7f77aef85

Attack Commands: Run with `command_prompt`!

```
dir /s /b %USERPROFILE%\Favorites
```

Atomic Test #8 - List Safari Bookmarks on MacOS

This test searches for Safari's Bookmarks file (on macOS) and lists any found instances to a text file.

Supported Platforms: macOS

auto_generated_guid: 5fc528dd-79de-47f5-8188-25572b7fafe0

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed.	Path	/tmp/T1217-Safari.txt

Attack Commands: Run with `sh`!

```
find / -path "*/Safari/Bookmarks.plist" 2>/dev/null >> #{output_file}
cat #{output_file}
```

Cleanup Commands:

```
rm -f #{output_file} 2>/dev/null
```