WINDOWS PROJECTED FILE SYSTEM

THE REALITY STONE

CASEY SMITH
SHMOOCON 2025

AGENDA

Introduction – Canarytokens

What problems does this solve

Setting up ProjFS

Internals

Ideas/ Looking Ahead

Final tips & takeaways

THE POWER OF

CANARYTOKENS

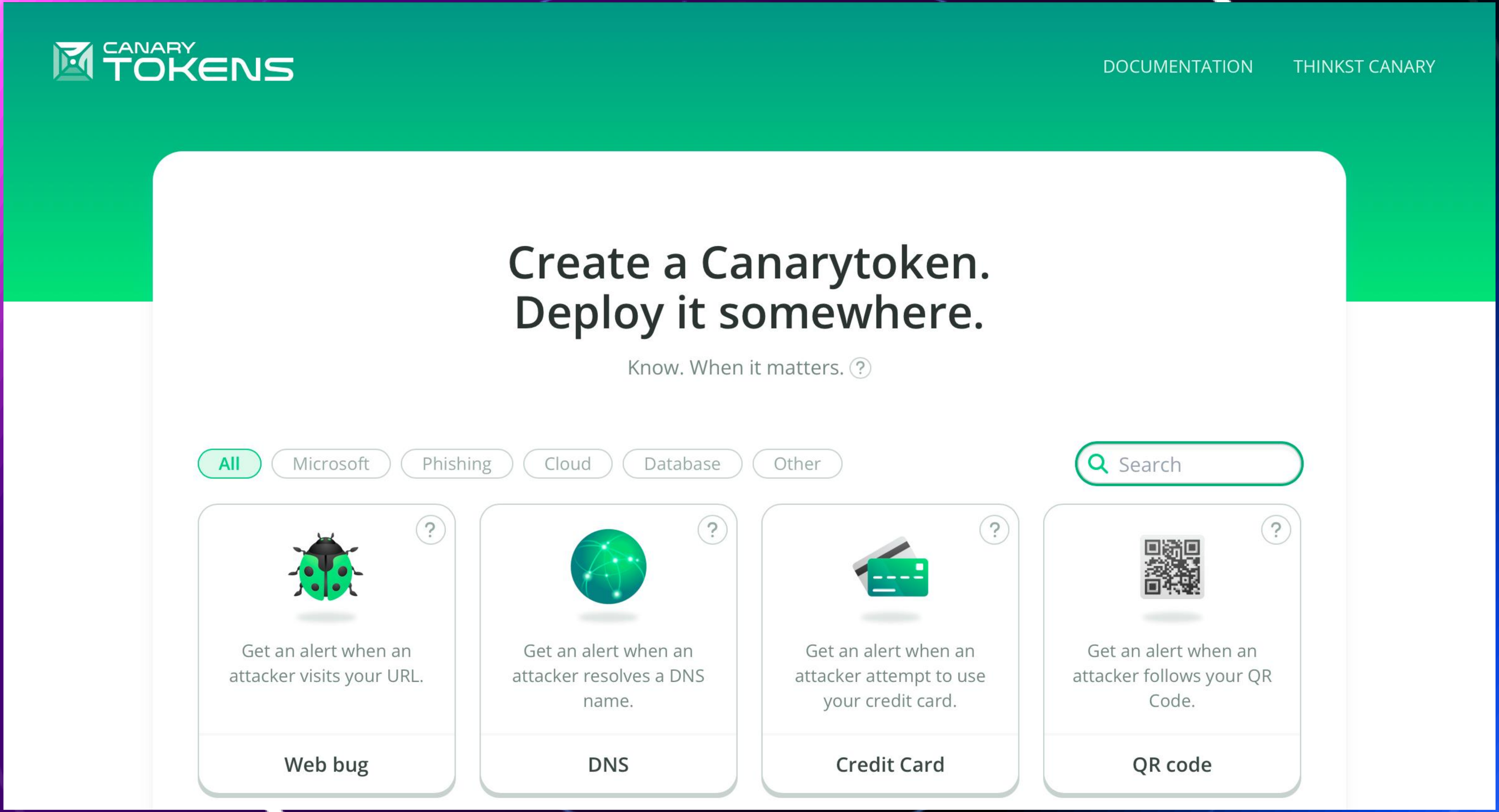
CANARY TOKENS

HTTPS://CANARYTOKENS.ORG

- Free Open Source

- Primitives –
  - HTTP
  - DNS

- Windows Tokens
  - Office Documents
  - Windows Folder
  - Signed EXE
  - Sensitive Command
  - Entra ID



CANARY TOKENS

DOCUMENTATION THINKST CANARY

Create a Canarytoken. Deploy it somewhere.

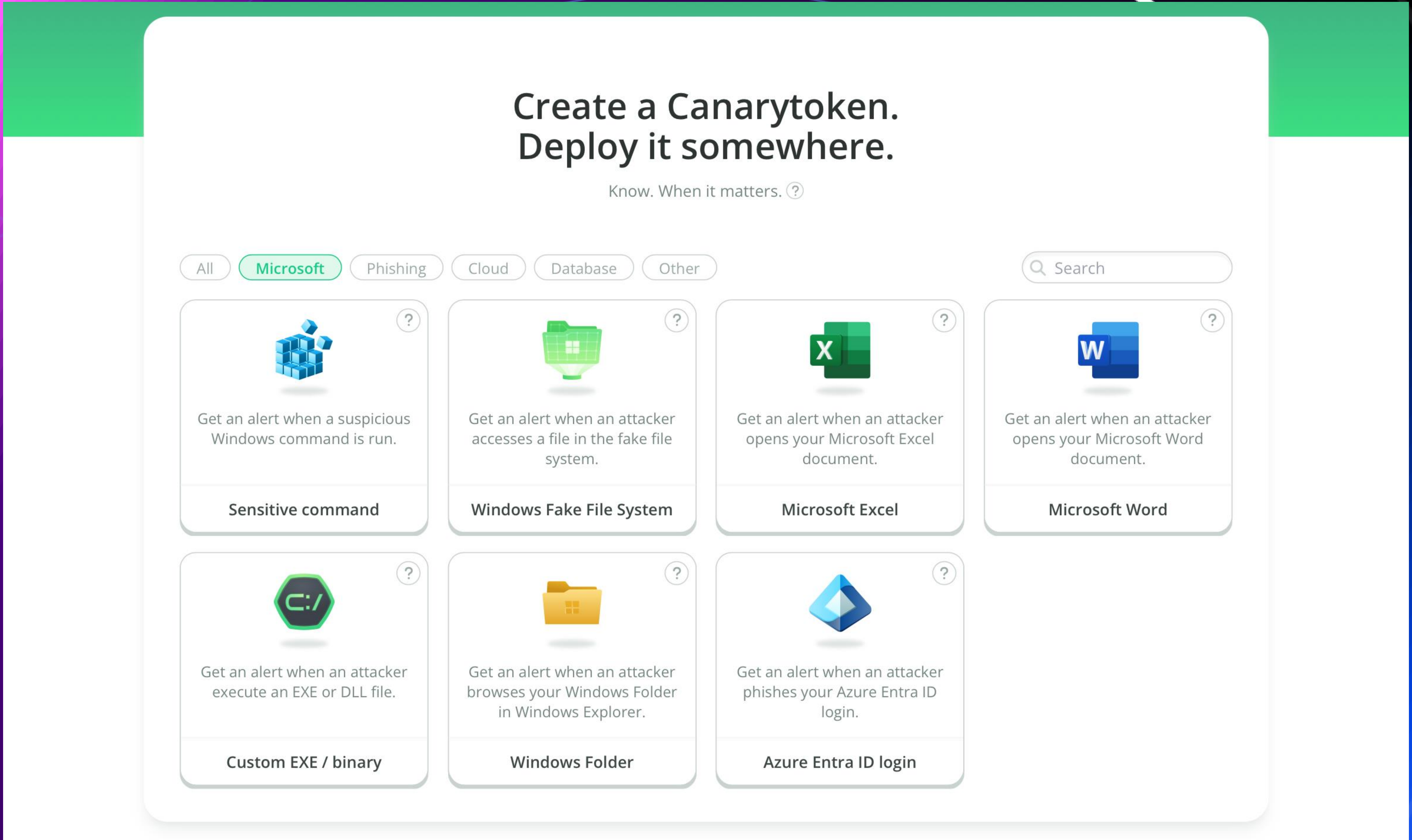
Know. When it matters. ?

?
Get an alert when an attacker visits your URL.
Web bug

?
Get an alert when an attacker resolves a DNS name.
DNS

?
Get an alert when an attacker attempt to use your credit card.
Credit Card

?
Get an alert when an attacker follows your QR Code.
QR code



Create a Canarytoken.
Deploy it somewhere.

Know. When it matters. ?

All | **Microsoft** | Phishing | Cloud | Database | Other

Search

Get an alert when a suspicious Windows command is run.

Sensitive command

Get an alert when an attacker accesses a file in the fake file system.

Windows Fake File System

Get an alert when an attacker opens your Microsoft Excel document.

Microsoft Excel

Get an alert when an attacker opens your Microsoft Word document.

Microsoft Word

Get an alert when an attacker execute an EXE or DLL file.

Custom EXE / binary

Get an alert when an attacker browses your Windows Folder in Windows Explorer.

Windows Folder

Get an alert when an attacker phishes your Azure Entra ID login.

Azure Entra ID login

THE POWER OF

CANARYTOKENS + PROJFS

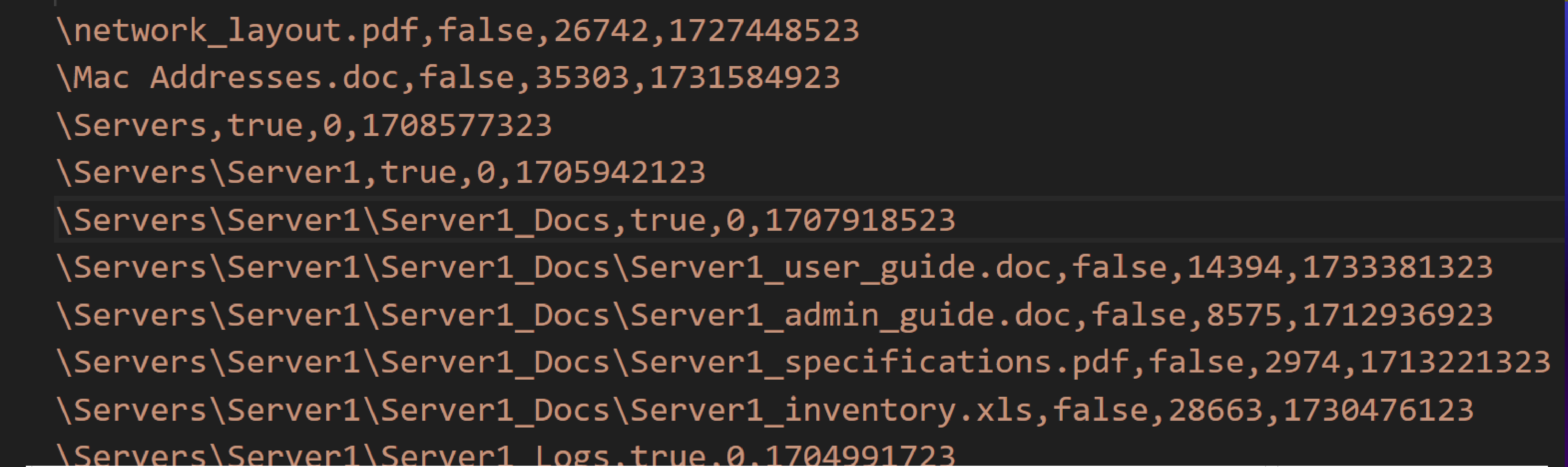
Why ProjFS ?

Its available ☺

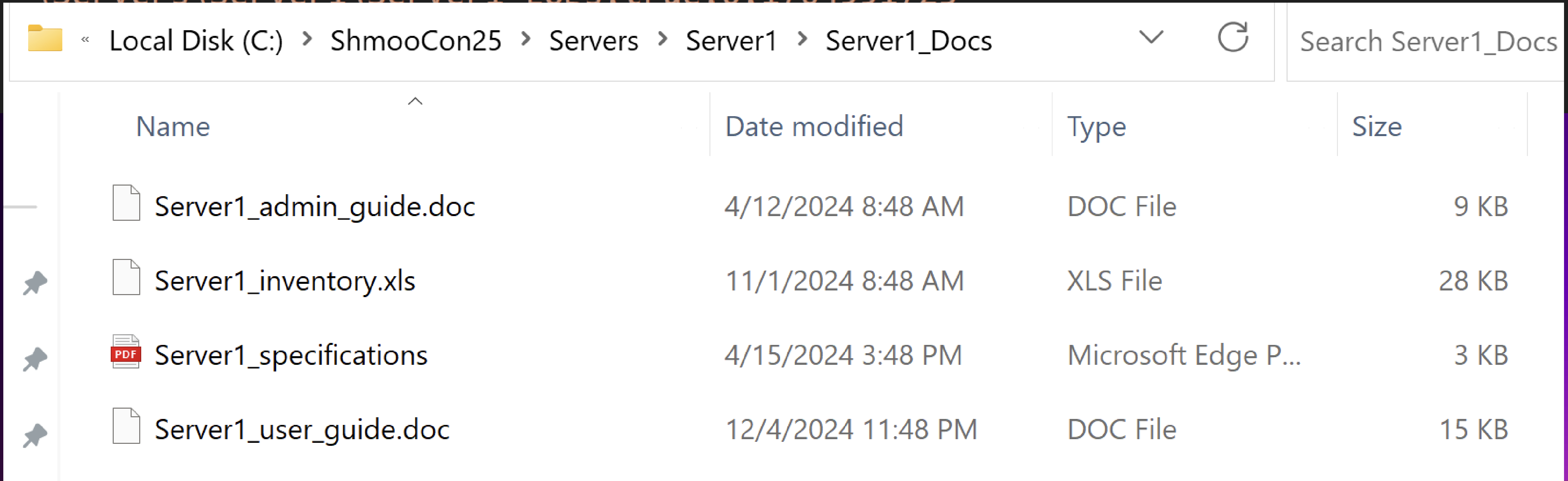
What problem are you trying to solve?

Tokens Efficacy Age Out / Systems Change

Example : Opening a Word Token, in Google Drive



```
\network_layout.pdf,false,26742,1727448523
\Mac Addresses.doc,false,35303,1731584923
\Servers,true,0,1708577323
\Servers\Server1,true,0,1705942123
\Servers\Server1\Server1_Docs,true,0,1707918523
\Servers\Server1\Server1_Docs\Server1_user_guide.doc,false,14394,1733381323
\Servers\Server1\Server1_Docs\Server1_admin_guide.doc,false,8575,1712936923
\Servers\Server1\Server1_Docs\Server1_specifications.pdf,false,2974,1713221323
\Servers\Server1\Server1_Docs\Server1_inventory.xls,false,28663,1730476123
\Servers\Server1\Server1_Logs,true,0,1704991723
```

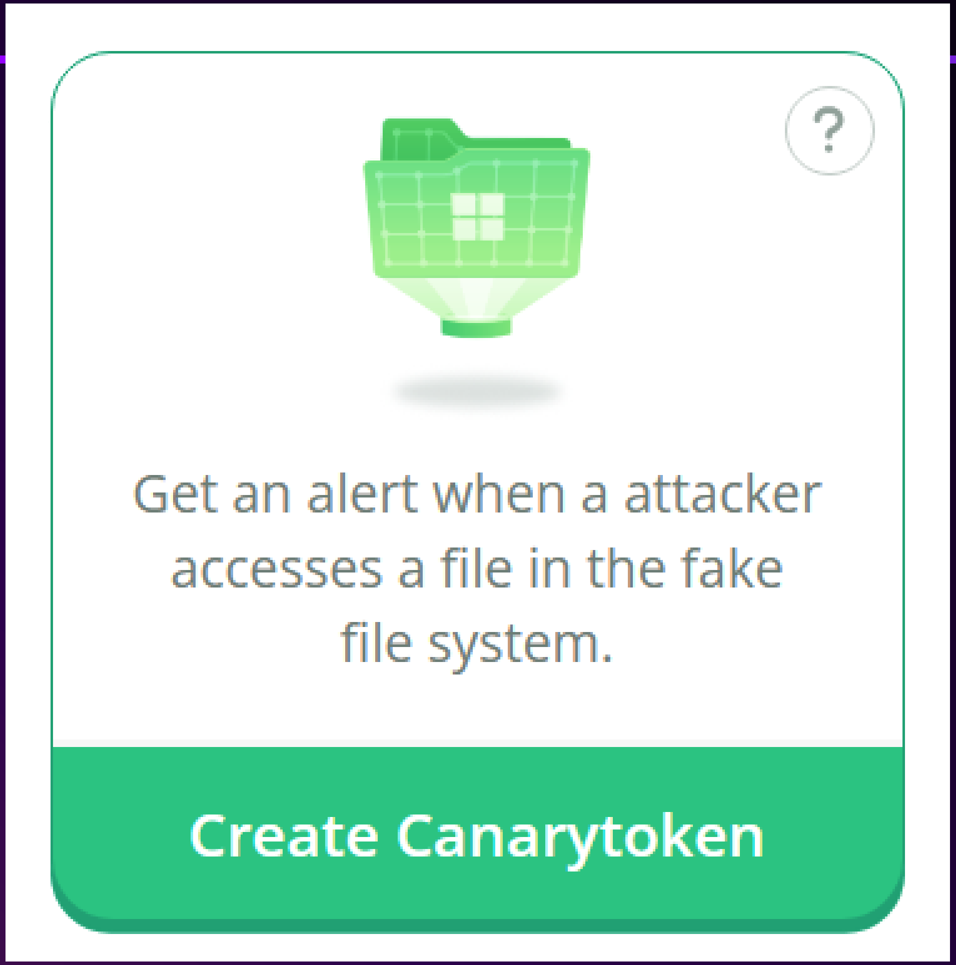


Local Disk (C:) › ShmooCon25 › Servers › Server1 › Server1_Docs
Search Server1_Docs

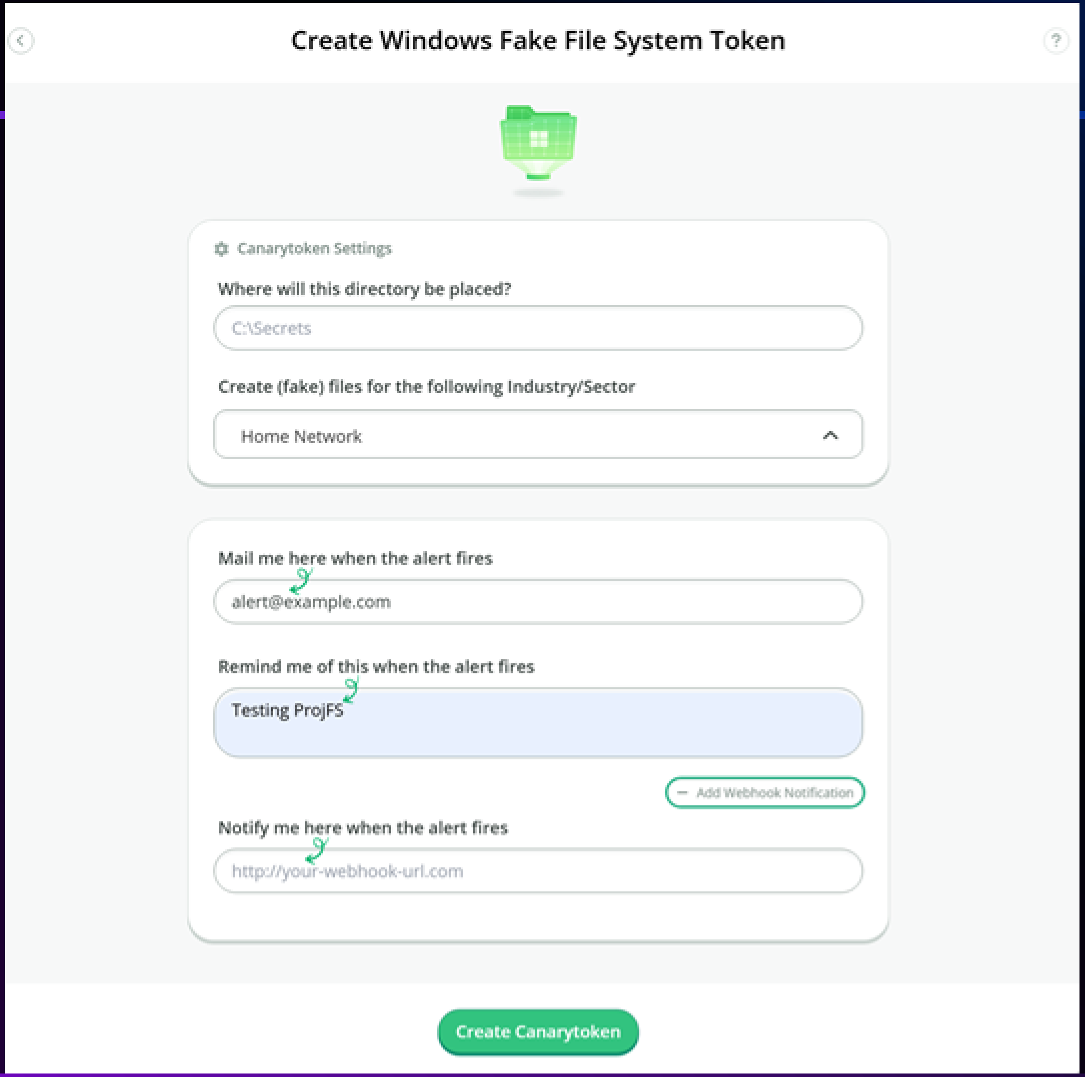
Name	Date modified	Type	Size
Server1_admin_guide.doc	4/12/2024 8:48 AM	DOC File	9 KB
Server1_inventory.xls	11/1/2024 8:48 AM	XLS File	28 KB
Server1_specifications	4/15/2024 3:48 PM	Microsoft Edge P...	3 KB
Server1_user_guide.doc	12/4/2024 11:48 PM	DOC File	15 KB

CANARY TOKENS

WE'VE MADE THIS EASY TO USE AND EFFECTIVE



Get an alert when a attacker accesses a file in the fake file system.



Create Windows Fake File System Token

Canarytoken Settings

Where will this directory be placed?

C:\Secrets

Create (fake) files for the following Industry/Sector

Home Network

Mail me here when the alert fires

alert@example.com

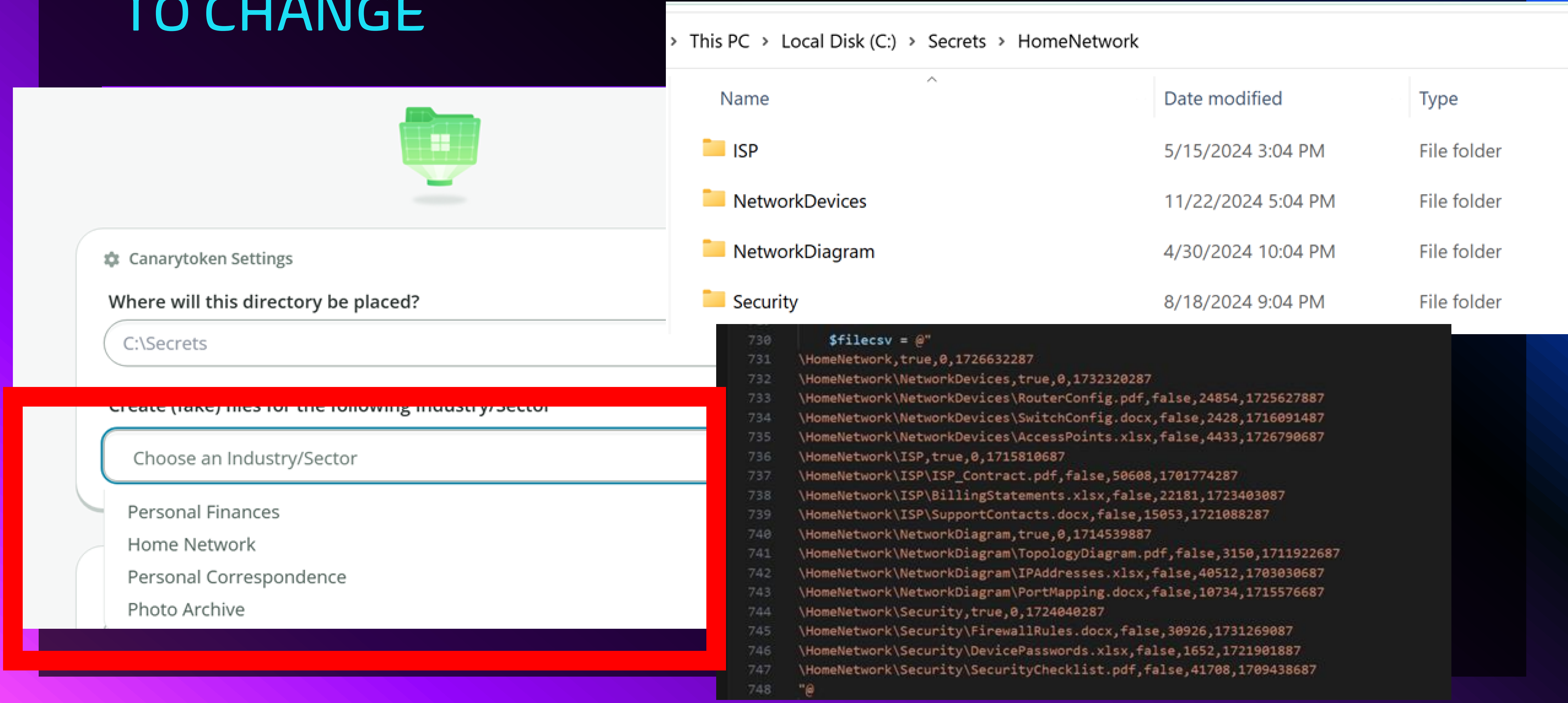
Remind me of this when the alert fires

Testing ProjFS

Notify me here when the alert fires

http://your-webhook-url.com

WE PROVIDE SOME FILES TO START YOU OFF, EASY TO CHANGE



Canarytoken Settings

Where will this directory be placed?

C:\Secrets

Create (fake) files for the following industry/sector

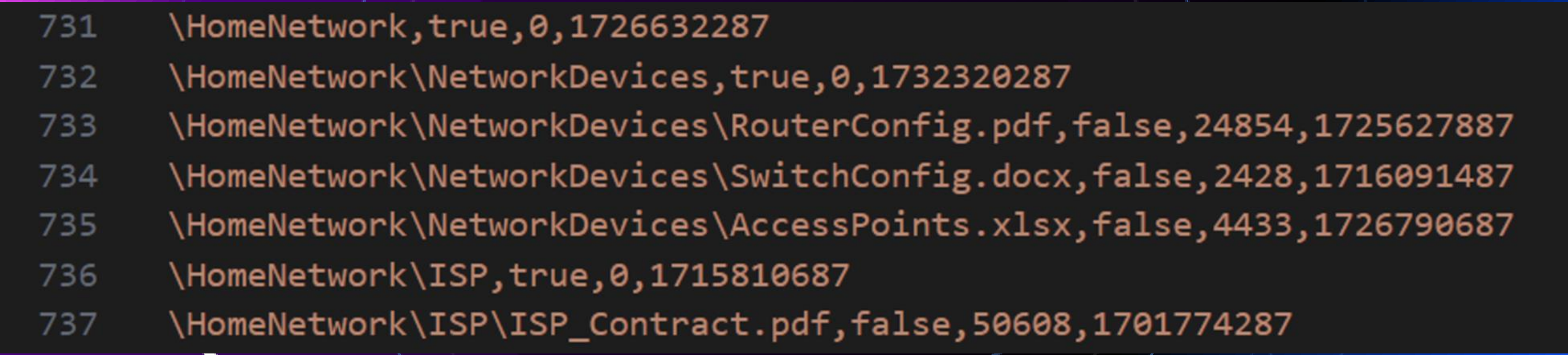
Choose an Industry/Sector

- Personal Finances
- Home Network
- Personal Correspondence
- Photo Archive

Name	Date modified	Type
ISP	5/15/2024 3:04 PM	File folder
NetworkDevices	11/22/2024 5:04 PM	File folder
NetworkDiagram	4/30/2024 10:04 PM	File folder
Security	8/18/2024 9:04 PM	File folder

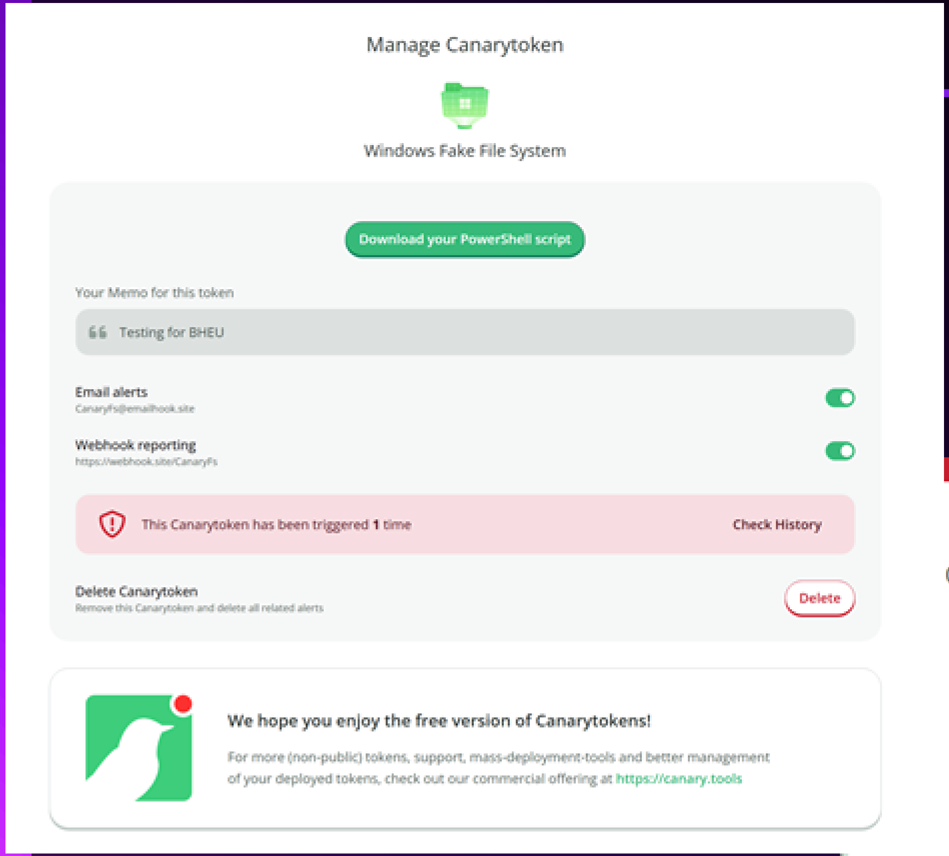
```
    $filecsv = @"
\HomeNetwork,true,0,1726632287
\HomeNetwork\NetworkDevices,true,0,1732320287
\HomeNetwork\NetworkDevices\RouterConfig.pdf,false,24854,1725627887
\HomeNetwork\NetworkDevices\SwitchConfig.docx,false,2428,1716091487
\HomeNetwork\NetworkDevices\AccessPoints.xlsx,false,4433,1726790687
\HomeNetwork\ISP,true,0,1715810687
\HomeNetwork\ISP\ISP_Contract.pdf,false,50608,1701774287
\HomeNetwork\ISP\BillingStatements.xlsx,false,22181,1723403087
\HomeNetwork\ISP\SupportContacts.docx,false,15053,1721088287
\HomeNetwork\NetworkDiagram,true,0,1714539887
\HomeNetwork\NetworkDiagram\TopologyDiagram.pdf,false,3150,1711922687
\HomeNetwork\NetworkDiagram\IPAddresses.xlsx,false,40512,1703030687
\HomeNetwork\NetworkDiagram\PortMapping.docx,false,10734,1715576687
\HomeNetwork\Security,true,0,1724040287
\HomeNetwork\Security\FirewallRules.docx,false,30926,1731269087
\HomeNetwork\Security\DevicePasswords.xlsx,false,1652,1721901887
\HomeNetwork\Security\SecurityChecklist.pdf,false,41708,1709438687
"@
```

PATH, ISDIRECTORY , SIZE, TIME



```
\HomeNetwork,true,0,1726632287
\HomeNetwork\NetworkDevices,true,0,1732320287
\HomeNetwork\NetworkDevices\RouterConfig.pdf,false,24854,1725627887
\HomeNetwork\NetworkDevices\SwitchConfig.docx,false,2428,1716091487
\HomeNetwork\NetworkDevices\AccessPoints.xlsx,false,4433,1726790687
\HomeNetwork\ISP,true,0,1715810687
\HomeNetwork\ISP\ISP_Contract.pdf,false,50608,1701774287
```

ALERT ON FILE OPEN OR COPY



Manage Canarytoken

Windows Fake File System

Your Memo for this token

Testing for BHEU

Email alerts
CanaryFs@emailhook.site

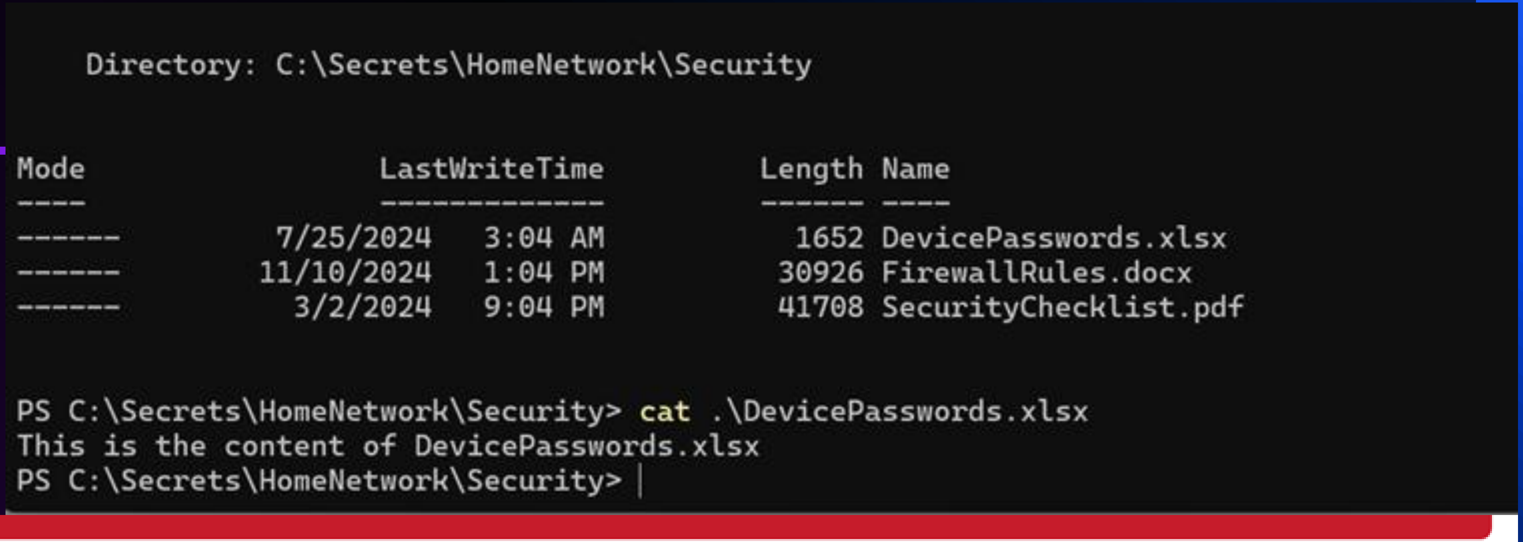
Webhook reporting
https://webhook.site/CanaryFs

This Canarytoken has been triggered **1** time

Delete Canarytoken
Remove this Canarytoken and delete all related alerts

We hope you enjoy the free version of Canarytokens!

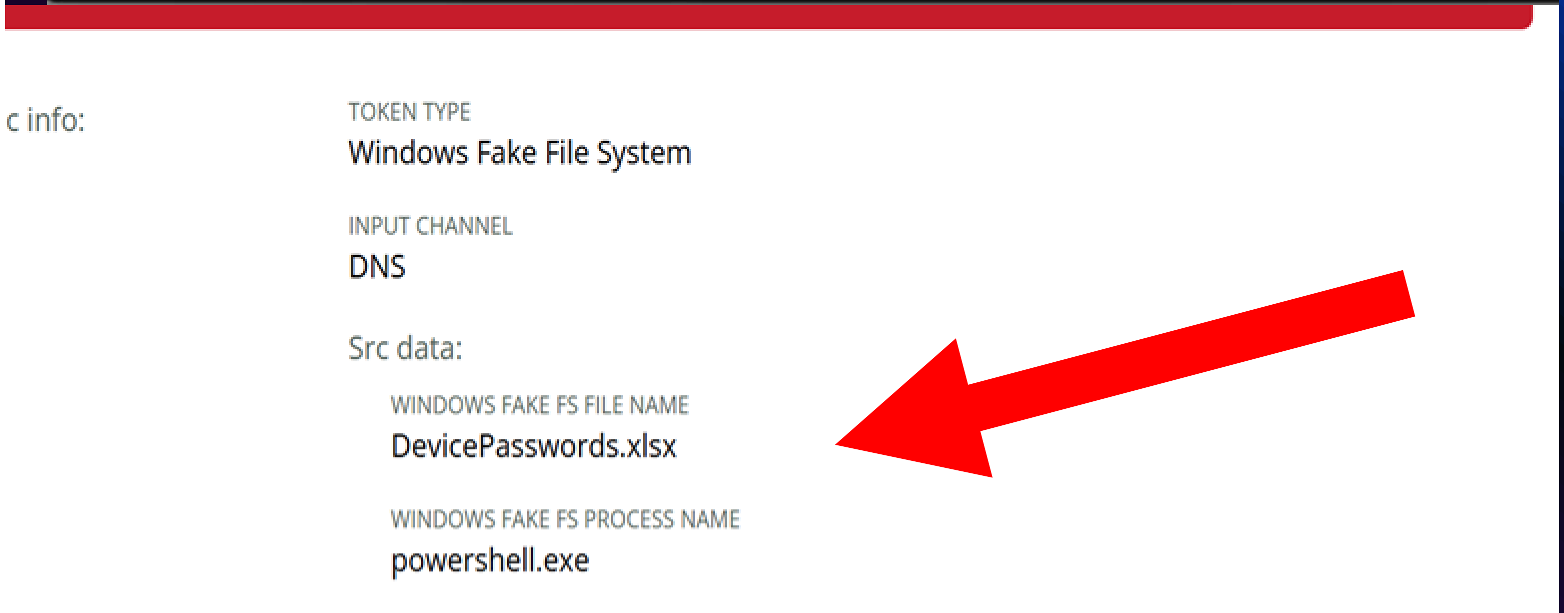
For more (non-public) tokens, support, mass-deployment-tools and better management of your deployed tokens, check out our commercial offering at https://canary.tools



```
    Directory: C:\Secrets\HomeNetwork\Security


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------         7/25/2024   3:04 AM           1652 DevicePasswords.xlsx
------        11/10/2024   1:04 PM          30926 FirewallRules.docx
------          3/2/2024   9:04 PM          41708 SecurityChecklist.pdf


PS C:\Secrets\HomeNetwork\Security> cat .\DevicePasswords.xlsx
This is the content of DevicePasswords.xlsx
PS C:\Secrets\HomeNetwork\Security> |
```



c info:

TOKEN TYPE
Windows Fake File System

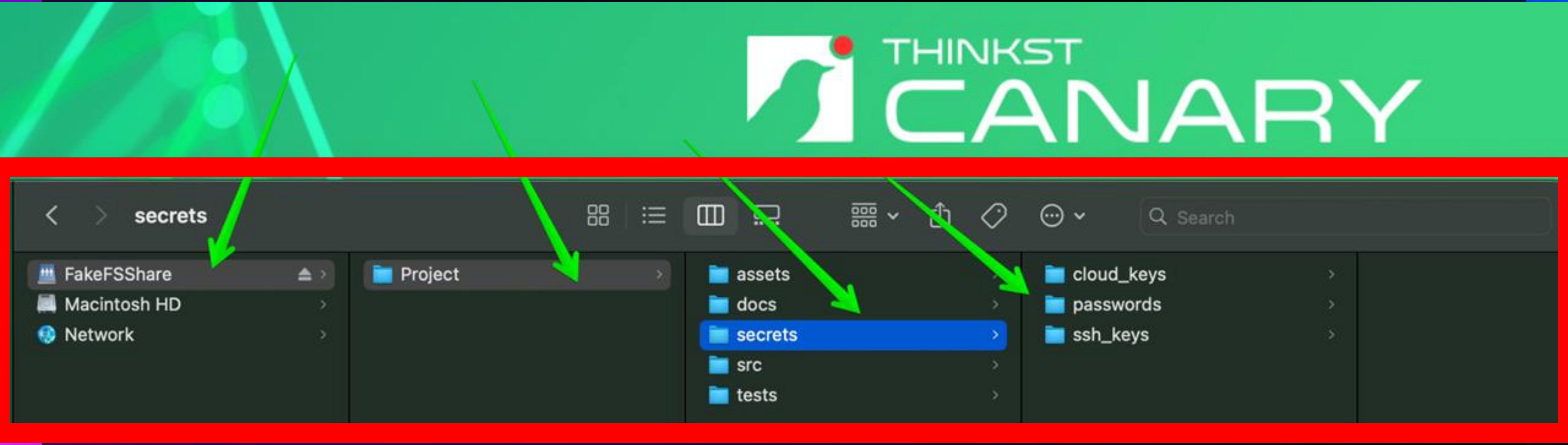
INPUT CHANNEL
DNS

Src data:

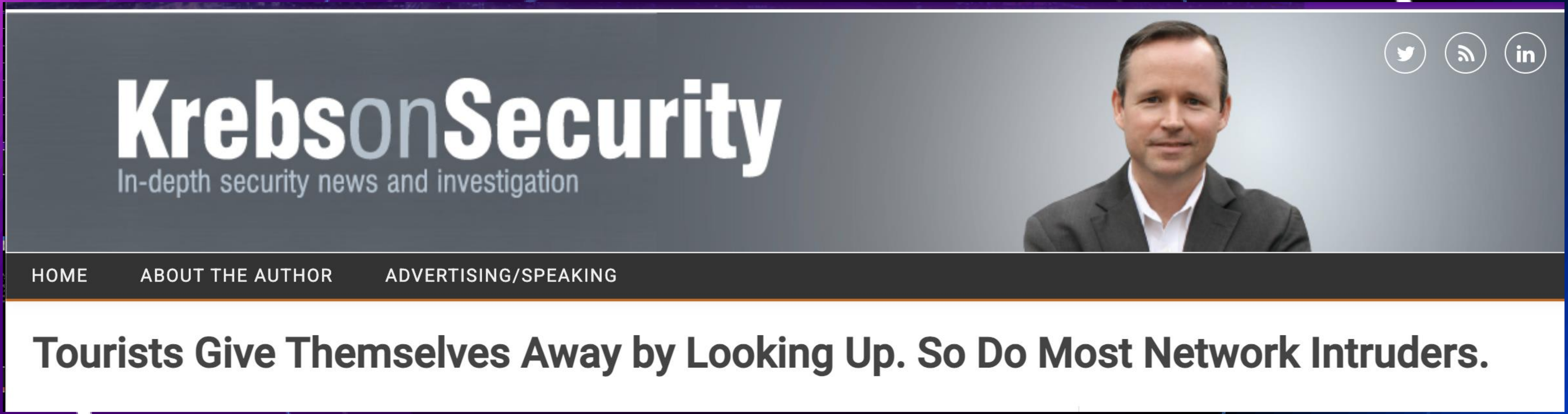
WINDOWS FAKE FS FILE NAME
DevicePasswords.xlsx

WINDOWS FAKE FS PROCESS NAME
powershell.exe

SMB REMOTE SESSIONS - ON REMOTE OPEN | COPY



Tool Name	Allows Enumeration	Detects on File Open/Copy
ShareFinder	✅	✅
FRansom	✅	✅
Snaffler	✅	✅
Full AV scan	✅ / Needs more testing	✅
Windows Search indexer	✅	✅



KrebsonSecurity

In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Tourists Give Themselves Away by Looking Up. So Do Most Network Intruders.

ATTACKERS BUMP AROUND – WE KNOW THIS

Dynamic File creation – context specific

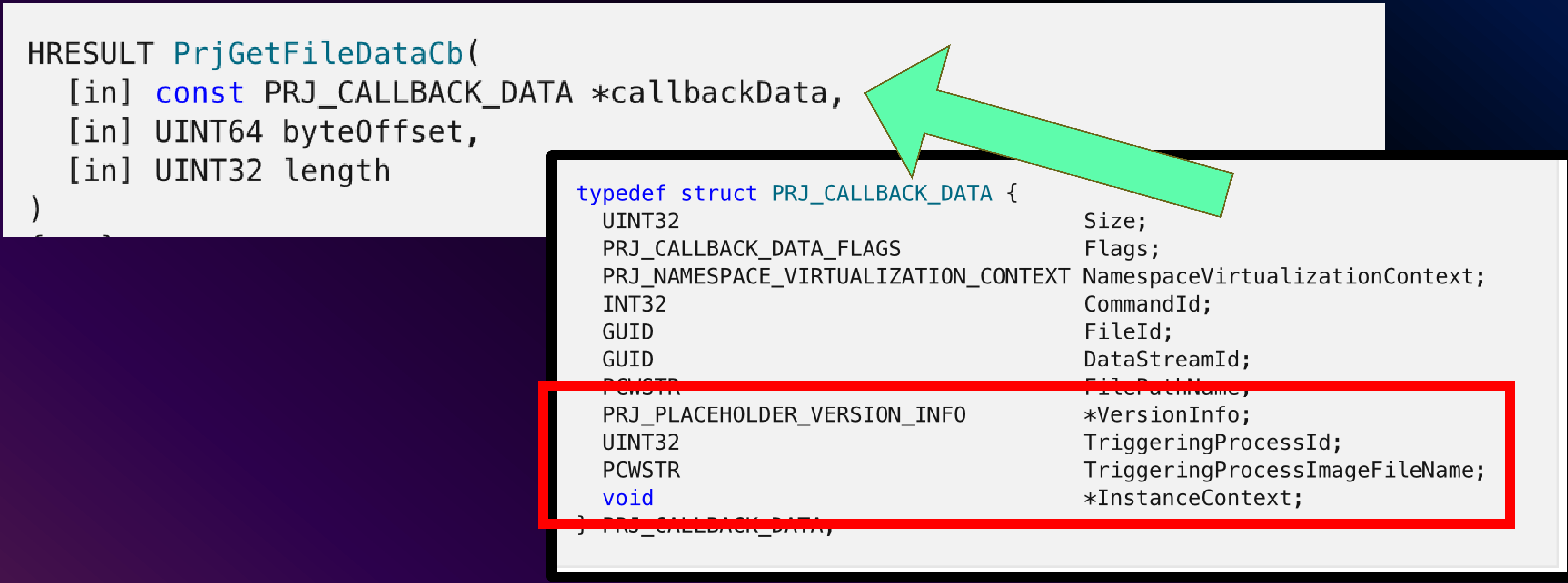
Defender Asymmetry

Alerts only on File OPEN | COPY

USE CASES – DYNAMIC FILE LISTING AND CONTENT

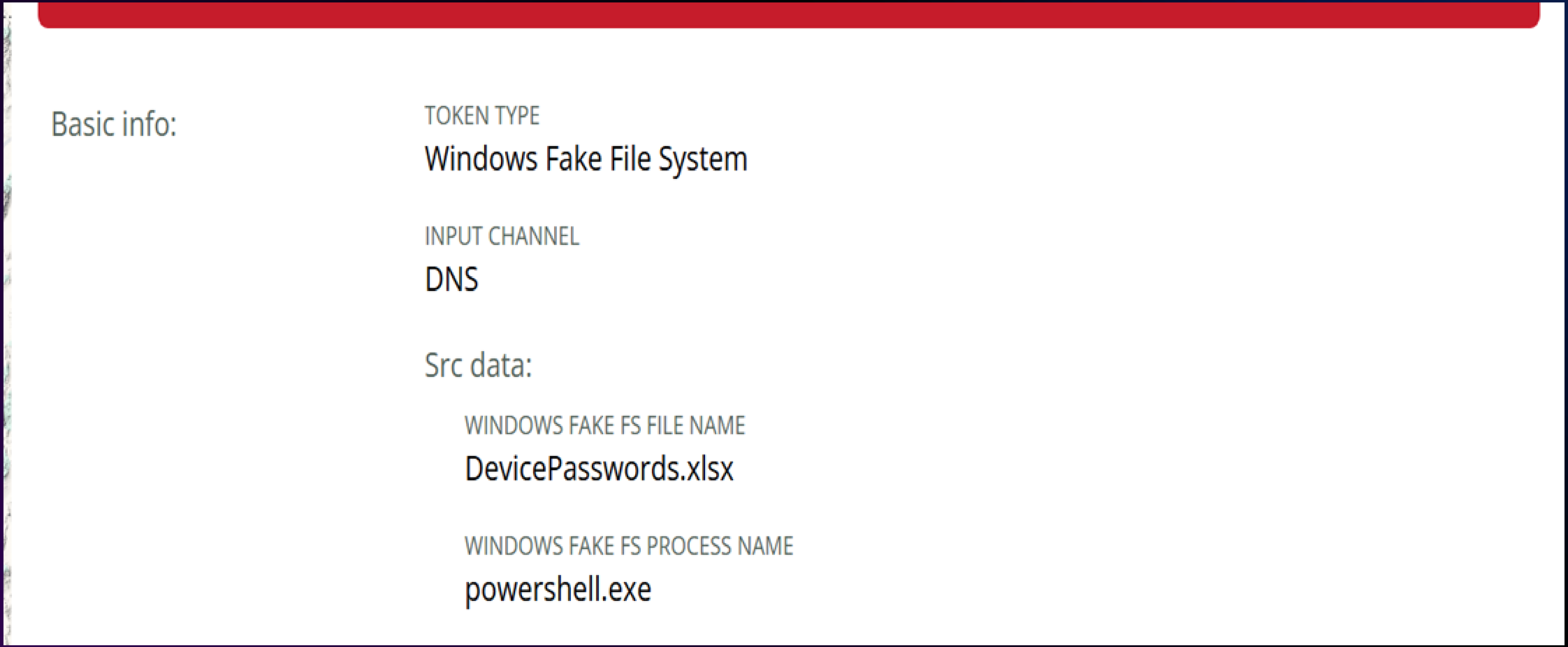
We intercept and inspect calling details, BEFORE we provide file content safely From User Mode

USE CASES – DYNAMIC FILE LISTING AND CONTENT



```
HRESULT PrjGetFileDataCb(
  [in] const PRJ_CALLBACK_DATA *callbackData,
  [in] UINT64 byteOffset,
  [in] UINT32 length
)
```

```
typedef struct PRJ_CALLBACK_DATA {
  UINT32                              Size;
  PRJ_CALLBACK_DATA_FLAGS             Flags;
  PRJ_NAMESPACE_VIRTUALIZATION_CONTEXT NamespaceVirtualizationContext;
  INT32                               CommandId;
  GUID                                FileId;
  GUID                                DataStreamId;
  PCWSTR                              FilePathName;
  PRJ_PLACEHOLDER_VERSION_INFO        *VersionInfo;
  UINT32                              TriggeringProcessId;
  PCWSTR                              TriggeringProcessImageFileName;
  void                                *InstanceContext;
} PRJ_CALLBACK_DATA;
```



Basic info:

TOKEN TYPE

Windows Fake File System

INPUT CHANNEL

DNS

Src data:

WINDOWS FAKE FS FILE NAME

DevicePasswords.xlsx

WINDOWS FAKE FS PROCESS NAME

powershell.exe

We base32 , Encode the Process Name and File and send a DNS query which is the Alert

LETS GO DEEPER

- ❑ How this works
- ❑ Provider – Reparse Points
- ❑ Fltmc
- ❑ Loaded Dlls
- ❑ Reference Architectures
- ❑ Other Ideas

SOME RESOURCES -

C# - PowerShell Implementation – for research , prototyping and production.

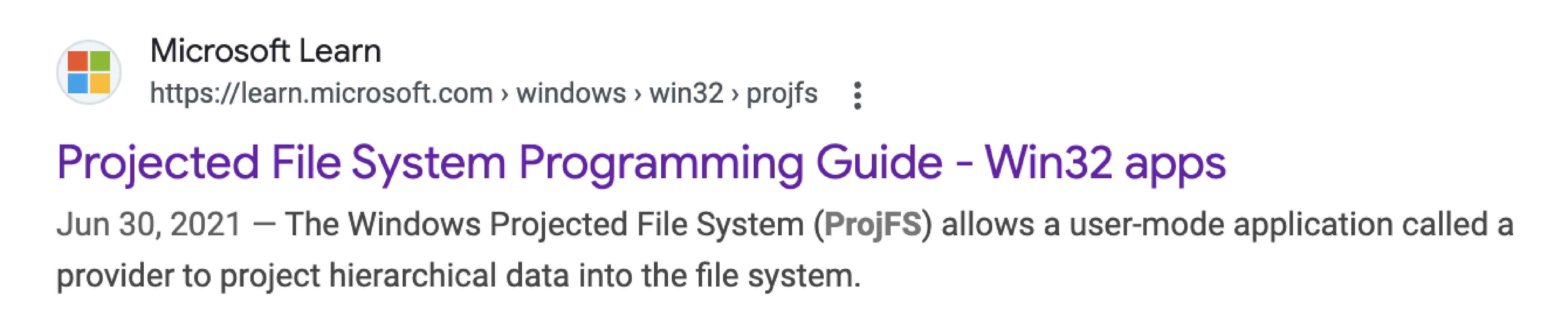
Provider – User Mode Projection Engine

Callbacks – Handle enumeration , file open, etc…

Virtualization Root – Empty

For complete details see:

Projected File System (ProjFS) Programming Guide



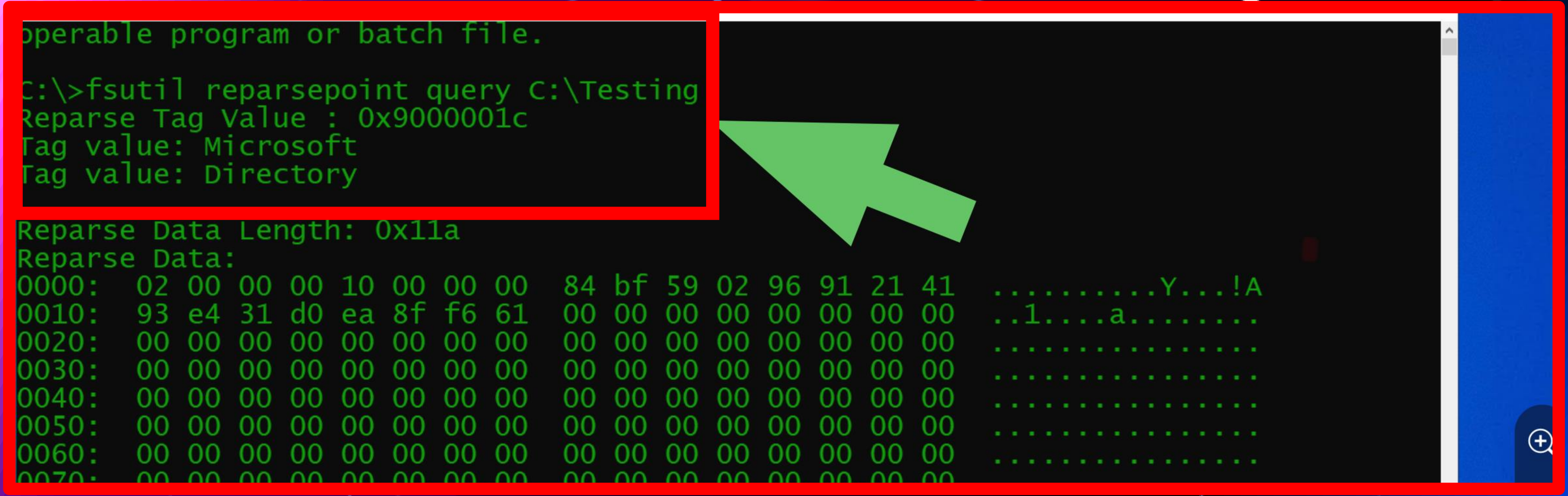
Microsoft Learn

https://learn.microsoft.com › windows › win32 › projfs

Projected File System Programming Guide - Win32 apps

Jun 30, 2021 — The Windows Projected File System (**ProjFS**) allows a user-mode application called a provider to project hierarchical data into the file system.

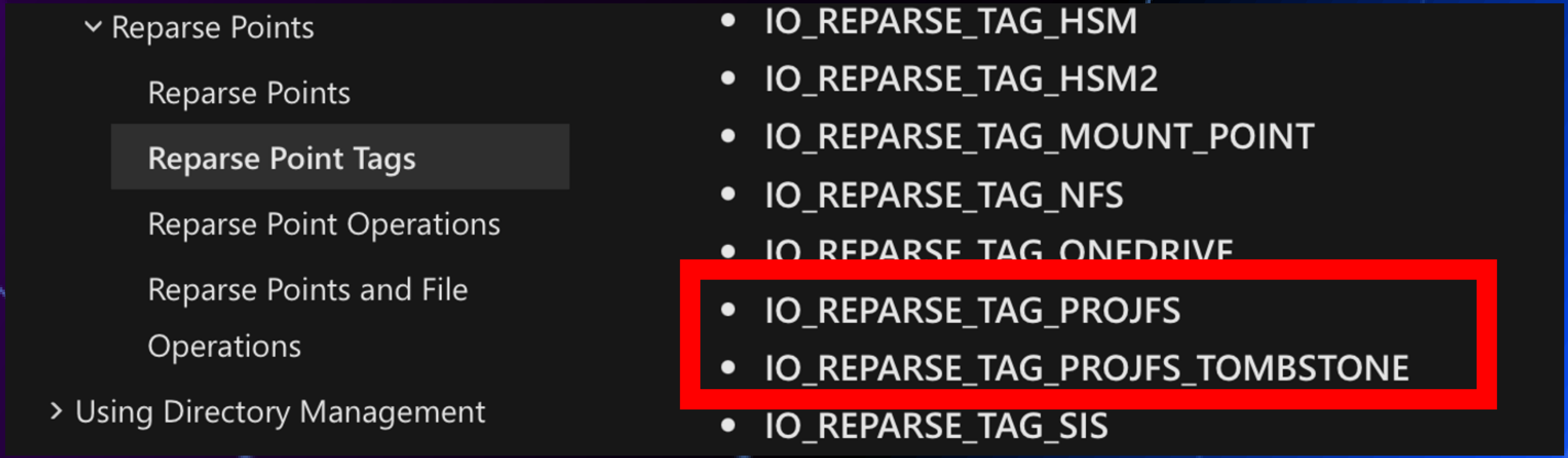
https://learn.microsoft.com/en-us/windows/win32/projfs/projfs-programming-guide



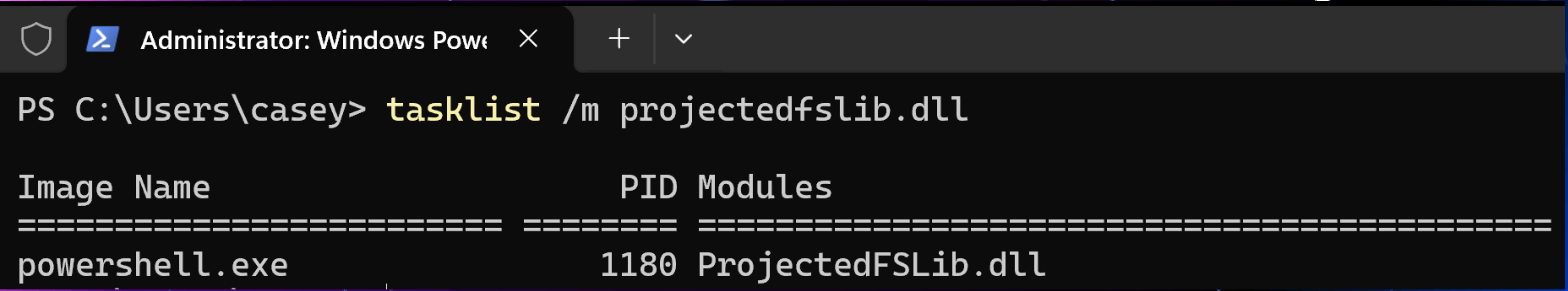
```
operable program or batch file.

C:\>fsutil reparsepoint query C:\Testing
Reparse Tag Value : 0x9000001c
Tag value: Microsoft
Tag value: Directory

Reparse Data Length: 0x11a
Reparse Data:
0000:  02 00 00 00 10 00 00 00  84 bf 59 02 96 91 21 41  ..........Y...!A
0010:  93 e4 31 d0 ea 8f f6 61  00 00 00 00 00 00 00 00  ..1....a........
0020:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0030:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0040:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0050:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0060:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0070:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```



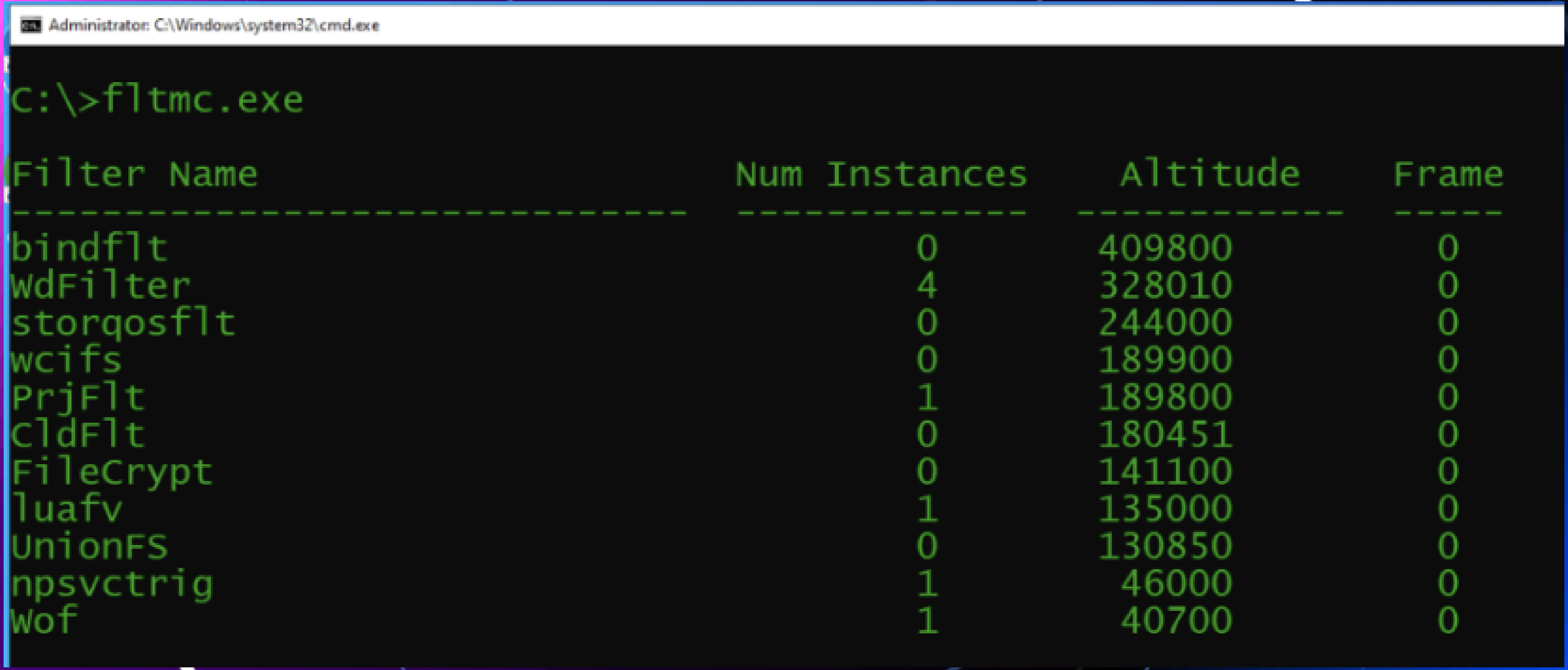
- IO_REPARSE_TAG_HSM
- IO_REPARSE_TAG_HSM2
- IO_REPARSE_TAG_MOUNT_POINT
- IO_REPARSE_TAG_NFS
- IO_REPARSE_TAG_ONEDRIVE
- IO_REPARSE_TAG_PROJFS
- IO_REPARSE_TAG_PROJFS_TOMBSTONE
- IO_REPARSE_TAG_SIS



```
PS C:\Users\casey> tasklist /m projectedfslib.dll

Image Name                     PID Modules
========================= ======== ============================================
powershell.exe                1180 ProjectedFSLib.dll
```

We need a good way to go from process to virtual root.



```
C:\>fltmc.exe

Filter Name                     Num Instances    Altitude    Frame
------------------------------  -------------  ------------  -----
bindflt                                 0       409800         0
WdFilter                                4       328010         0
storqosflt                              0       244000         0
wcifs                                   0       189900         0
PrjFlt                                  1       189800         0
CldFlt                                  0       180451         0
FileCrypt                               0       141100         0
luafv                                   1       135000         0
UnionFS                                 0       130850         0
npsvctrig                               1        46000         0
Wof                                     1        40700         0
```

OS Feature	Implementation	Perf Impact	File content monitoring	Scalability
ProjFS	User mode & MS driver	Low	Yes	High
File System Watcher	User mode	Moderate	No	Limited
Object Auditing / SACLs	OS subsystem	High	Yes	Fair
Controlled Folder Access	OS-$$ / MSFT Defender	Low	Low	High

REFERENCE ARCHITECTURES

1. https://github.com/thinkst/defending-off-the-land
   a. C# | PowerShell
2. https://github.com/danielhodson/pyprojfs
   a. Python
3. https://scorpiosoftware.net/2024/02/20/projected-file-system/
   a. Object Manager
4. https://github.com/adamplonka/RegFs-csharp
   a. Registry – C# patterns

IN SUMMARY

Canarytokens – free open source project

New Canary Token – Windows Fake File System

Monitors any Root Path you setup and alerts on File Open | Copy

You can do more – fake content, per process etc.

Casey Smith
Thinkst Canary
research@thinkst.com
canary.tools

CANARY TOKENS

https://canarytokens.org/