What the DLL is happening?

A practical approach to identifying SOH.

red canary

Presenter

Frank McClain

Senior Detection Engineer

RED CANARY

@littlemac042

- Detection Engineering training lead within the Red Canary CIRT
- Ran the Security Operations team at a national financial services provider for several years
- Recently got a Mavic Mini drone, and I swear it's been windy ever since…

red canary

What is Dynamic Link Library (DLL) search order?

- A means by which DLLs are found and loaded into process memory
- Multiple factors or variables exist, but basically follows this order
  - DLL of the same name already loaded in memory (by another process)
  - DLL is listed in the ‘KnownDLLs’ registry key
  - DLL of the same name exists in the same directory as the loading process
  - System directory (e.g., ‘%SystemRoot%\System32’)

What is search order hijacking (SOH)?

- Form of DLL hijacking (on Windows)
- Commonly used by adversaries (commodity and advanced)
- Primarily leverages the same directory as the loading process

Why is SOH important?

TECHNIQUE T1038

DLL Search Order Hijacking

Dridex infections are the main reason that we observe high levels of DLL Search Order Hijacking in the environments we monitor. However, we've also observed Emotet and PlugX leveraging the technique.

#8

OVERALL RANK

16%

ORGANIZATIONS AFFECTED

788

CONFIRMED THREATS

red canary

Why is SOH important?

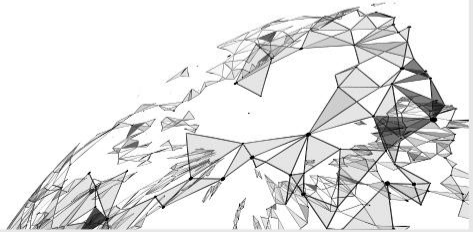
- Common adversary technique
- Persistence mechanism
- Privilege escalation
- Bypass security controls

red canary

Covering SOH

SEARCH ORDER HIJACKING

- Identification or detection methods
- Detector concepts (ideas to try)
- Detection examples (SOH in action)
- Mitigation strategies



red canary

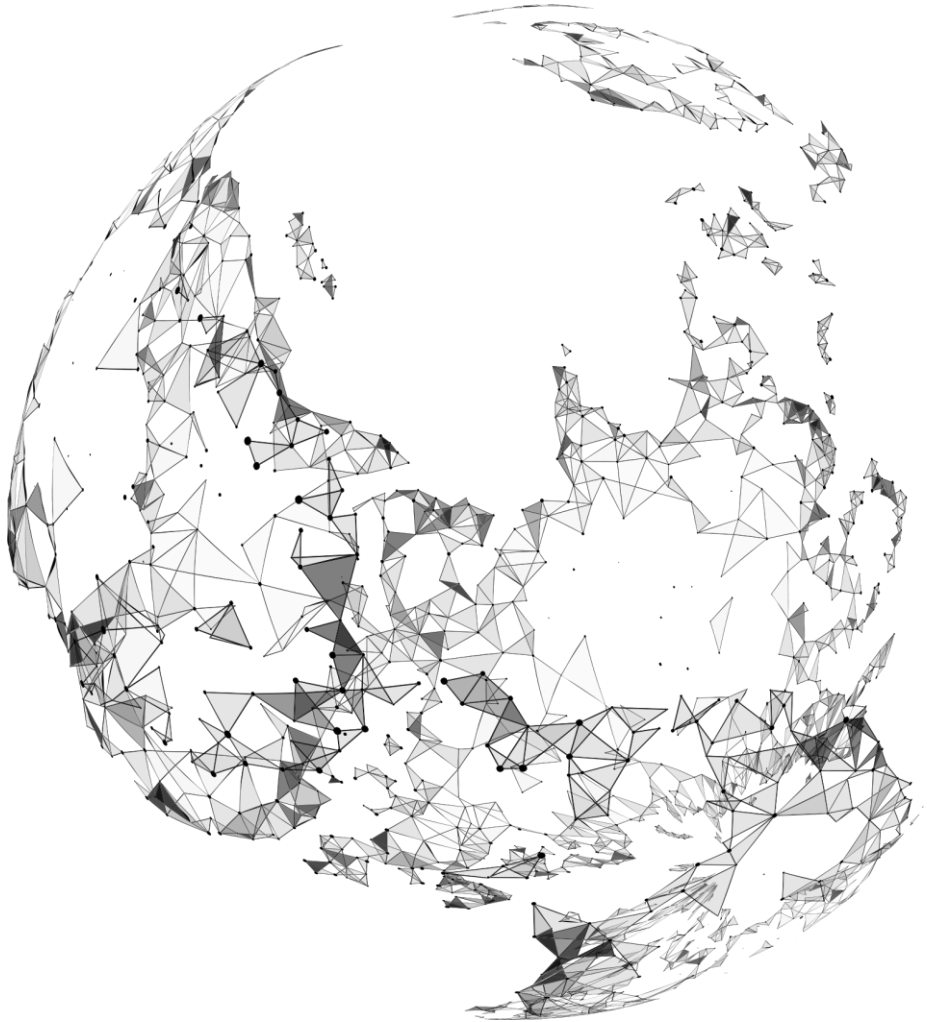
Identification methods

- Creation of a scheduled task in a suspect path (user path, ProgramData, etc.)
- Script processes (wscript.exe, cscript.exe, etc.) spawning an unsigned binary
- Service Host (svchost.exe) spawned by a suspect parent process
- Legitimate system binaries copied to/executing from suspect paths
- Unsigned, unknown DLLs written to/loaded from suspect paths
- And more…

Post-identification validation

- Check to see if binaries are legitimate, signed, or operating system
- Identify if any DLL files are written to the same (suspect) path
- Check DLLs to see if they are legit, or have the same name as legit DLLs
- If the binary was executed from the suspect path, see whether it loaded DLLs from that path

Detector concepts

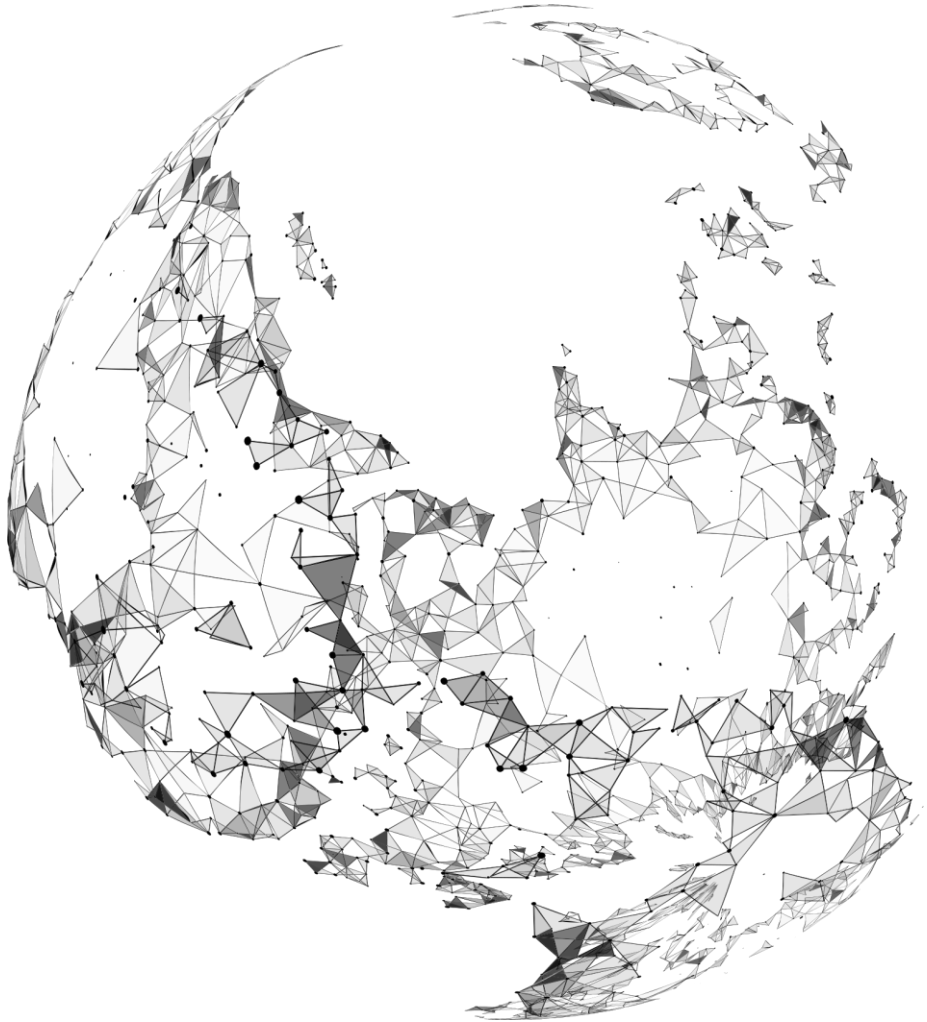


Sample query logic (getting started)

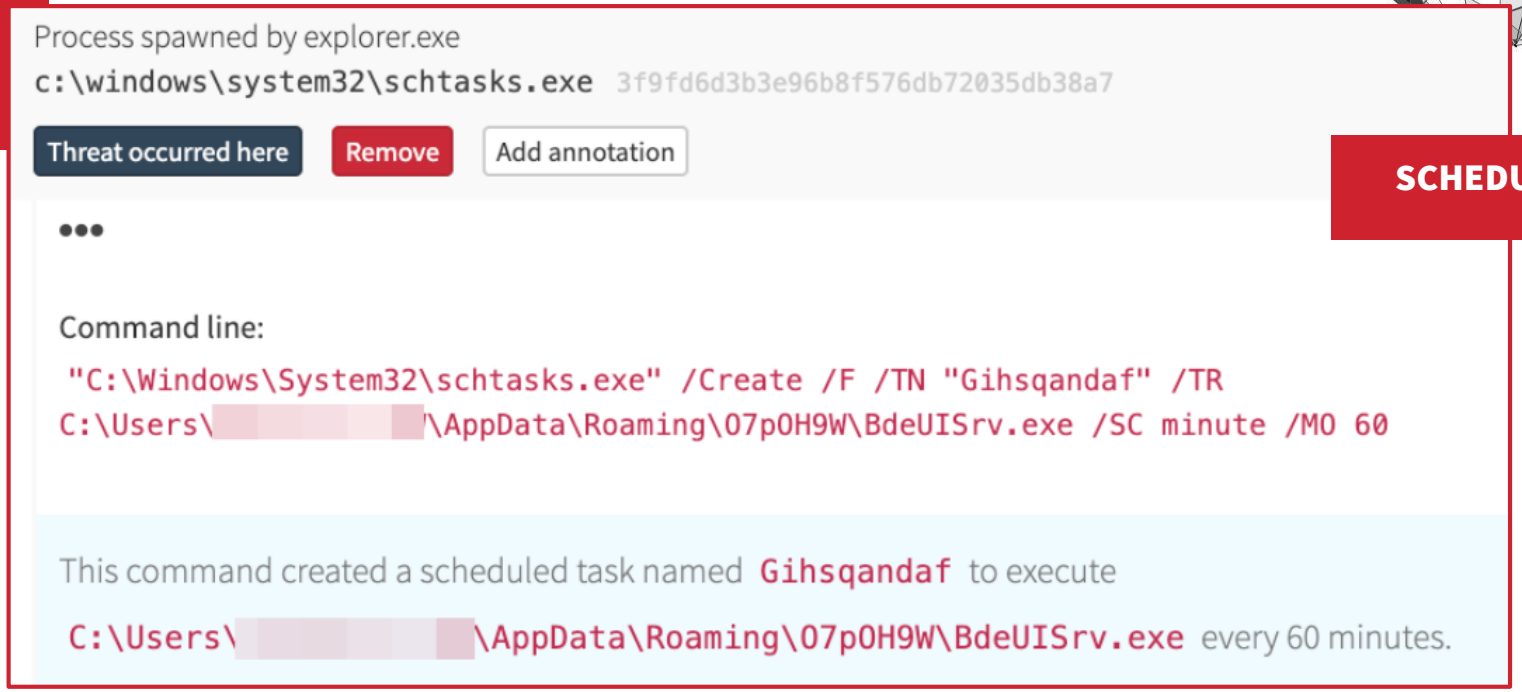
- *Process_Is* 'schtasks.exe' AND *Command_Line_Contains* 'appdata\roaming' AND *Command_Line_Contains* '*.exe'
- *Parent_Process_Is* 'taskeng.exe' OR *Parent_Process_Is* 'svchost.exe' AND *Binary_Publisher_Is* 'Microsoft Windows' AND *Process_Path_Is* 'appdata\roaming'
- *Binary_Publisher_Is* 'Microsoft Windows' AND *Process_Path_Is_Not* 'windows\system32' OR *Process_Path_Is_Not* 'windows\syswow64' OR *Process_Path_Is_Not* 'windows\winsxs'

red canary

Detection examples



DETECTION #1



SCHEDULED TASK

Setting up to execute a binary within the user profile. This legit binary is part of BitLocker.

red canary

DETECTION #1

FILE COPY

Here is where the binary is written to disk under the profile. It is expected to reside in System32.

red canary

DETECTION #1

FILE COPY

Here is where the malicious DLL is written to disk in the same path under the user profile; when the EXE is launched, this DLL will be loaded into memory.

red canary

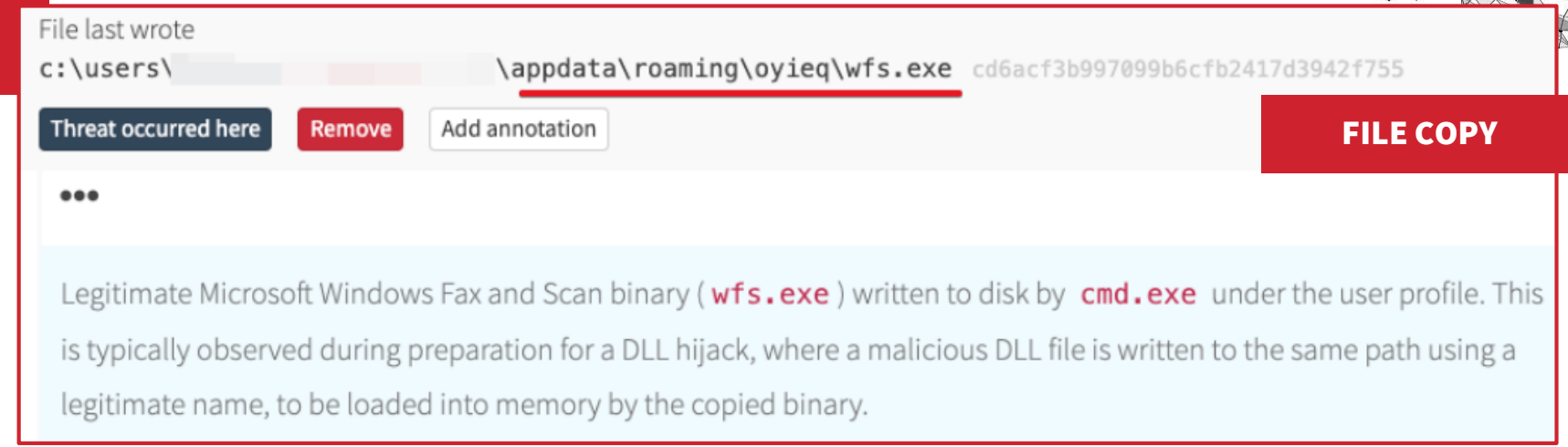
DETECTION #2

MASQUERADING

Malicious binary written to disk, leveraging metadata (or perhaps a compromised binary) to masquerade as GNU DiffUtils.

red canary

DETECTION #2

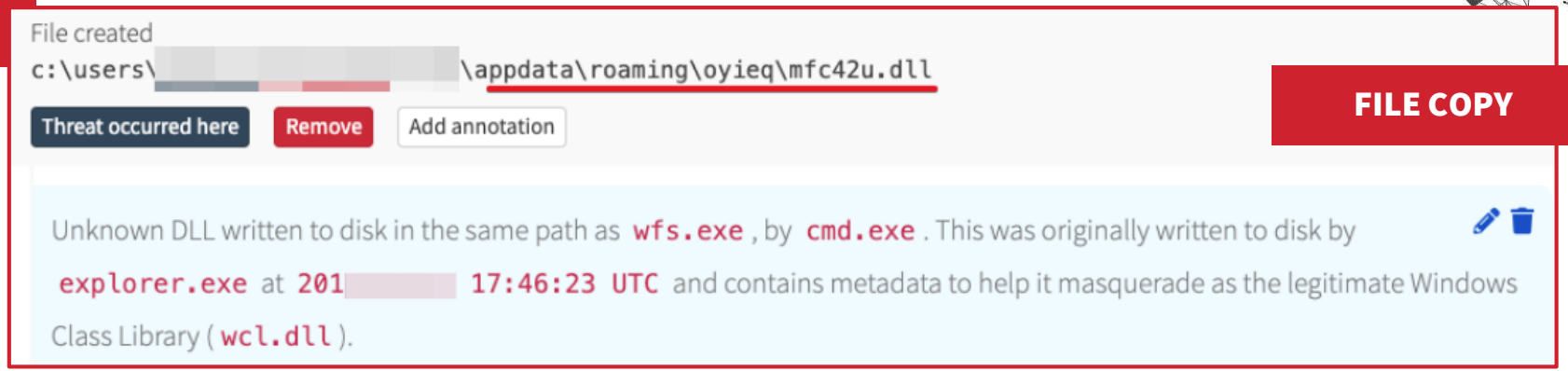


FILE COPY

Legitimate system binary written to disk under the user profile; SOH, here we come!

red canary

DETECTION #2



FILE COPY

Here is where the malicious DLL is written to disk in the same path under the user profile; when the EXE is launched, this DLL will be loaded into memory.

red canary

DETECTION #2

SCHEDULED TASK

Process spawned by explorer.exe

`c:\windows\system32\schtasks.exe` 838d346d1d28f00783b7a6c6bd03a0d

Threat occurred here | Remove | Add annotation

•••

Command line:

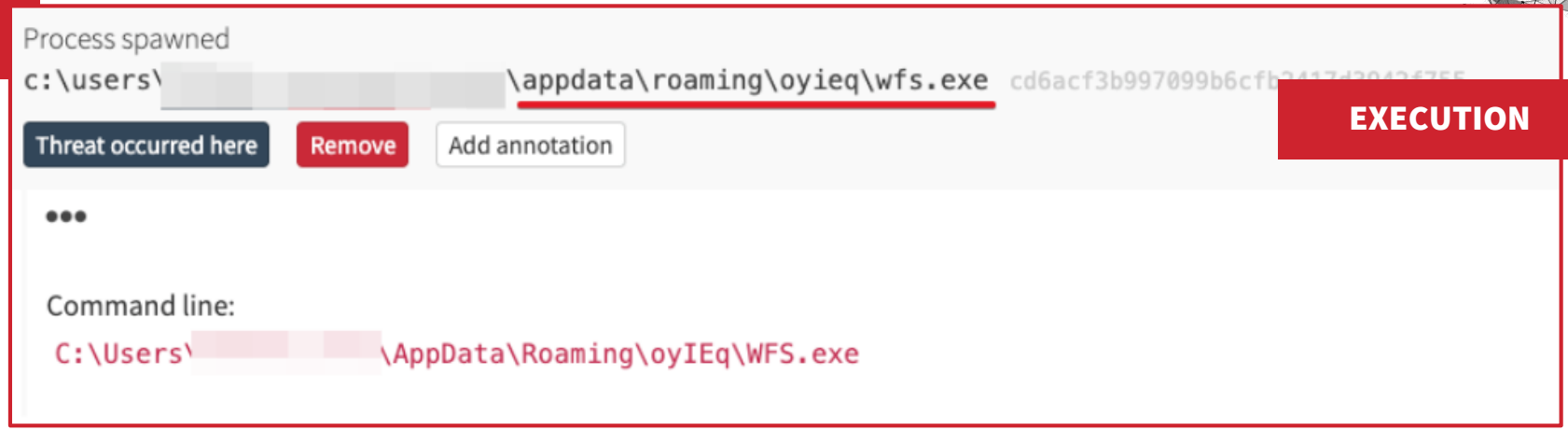
```
"C:\Windows\System32\schtasks.exe" /Create /F /TN "Lsbqpnq" /TR
C:\Users [redacted]\AppData\Roaming\oyIEq\WFS.exe /SC minute /MO 60
```

Setting up to execute a binary within the user profile.

This is the legitimate Windows Fax & Scan binary.

red canary

DETECTION #2

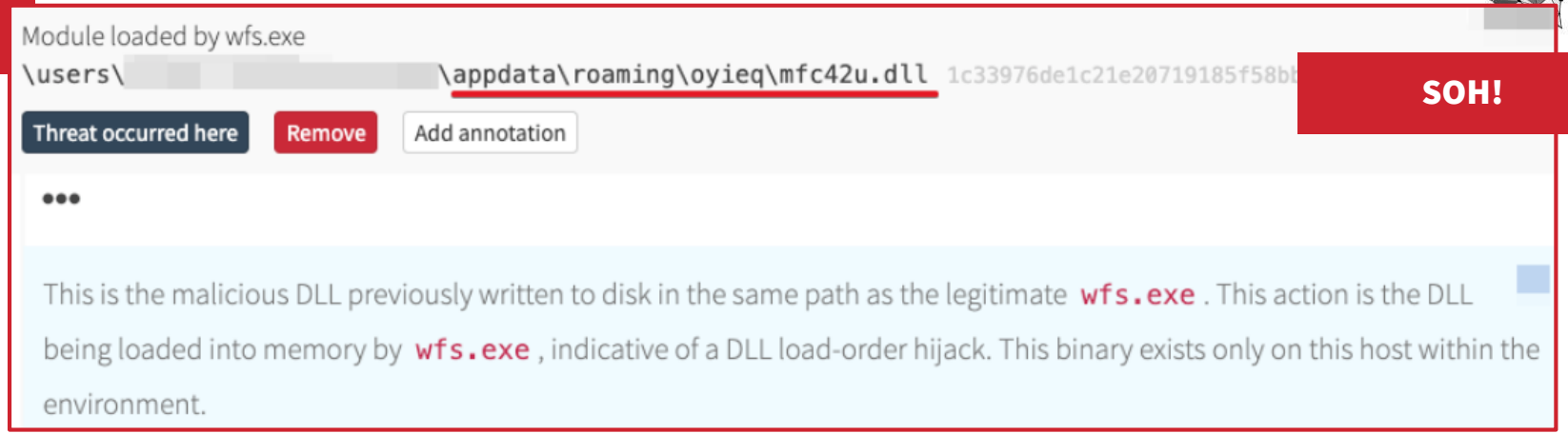


EXECUTION

Execution of the legitimate Windows Fax & Scan binary, from within the user path (1 hour after the scheduled task creation).

red canary

DETECTION #2



SOH!

And now the malicious DLL gets loaded into memory by the legitimate WFS process. Whatever code it contains is now active and being used by wfs.exe.

red canary

Can you prevent or mitigate the risk of SOH?

- If you're compiling binaries, make all DLLs explicit, including fully qualified path
- Maintain security hygiene and an active patching program
- Leverage Microsoft provisions
  - SafeDLLSearchMode
  - CWDIllegalInDllSearch
- Good detection methodologies

red canary

Reference links

- Red Canary on MITRE ATT&CK®
  - https://redcanary.com/mitre-attack/
- Red Canary (2020 Threat Detection Report)
  - https://redcanary.com/threat-detection-report/techniques/dll-search-order-hijacking/
- MITRE ATT&CK - Hijack Execution Flow: DLL Search Order Hijacking
  - https://attack.mitre.org/techniques/T1574/001/
- Microsoft on Dynamic-Link Library Search Order
  - https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order

red canary

FEEDBACK

Q & A

red canary