

Very very very Hidden

Very very very Hidden



Hard Forensics picoCTF 2021

AUTHOR: SARA

Description

Finding a flag may take many steps, but if you look diligently it won't be long until you find the light at the end of the tunnel. Just remember, sometimes you find the hidden treasure, but sometimes you find only a hidden map to the treasure.

[try_me.pcap](#)

Hints



1 2

2,003 users solved



53% Liked



picoCTF{FLAG}

Submit Flag

1. Open the capture and focus on clear-text traffic

99 % of frames are TLS noise; the interesting bits are the handful of vanilla-HTTP requests. Load `try_me.pcap` in wireshark and apply

```
(http.request or ssl.handshake.type == 1) and !(udp.port == 1900)
```

Five HTTP requests remain; two of them fetch images from an AWS host:

```
GET /NothingSus/duck.png HTTP/1.1
GET /NothingSus/evil_duck.png HTTP/1.1
```

2. Export the objects

File ▶ Export Objects ▶ HTTP ▶ Save All
Now we have `duck.png` (\approx 45 kB) and `evil_duck.png` (**\approx 2.6 MB**) on disk.

3. Identify the hiding method

A sweep with `binwalk`, `zsteg`, `steghide`, etc. comes up blank.
So next, I look at the browsing history we captured. Among the HTTPS SNI fields there’s a `powershell.org`. That, plus a gigantic PNG, screams **PowerShell/Invoke-PSImage** steganography.

4. Extract the hidden PowerShell payload

Any Invoke-PSImage decoder works; the Windows-friendly binary in **PCsXcetra/Decode_PS_Stego** is the easiest drop-in tool, you can get it [here](#), after which you can run the following:

```
.\PowershellStegoDecode.exe
```

The decoder spits out a script

```
$out = "flag.txt"
$enc = [system.Text.Encoding]::UTF8

$string1 = "HEYWhere(IS_tNE)50uP?^DId_YOu(]E@t*mY_3RD()B2g3l?"
$string2 = "8,:8+14>Fx0l+$*KjVD>[o*.;+1|*[n&2G^201l&,Mv+_ 'T_B"

$data1 = $enc.GetBytes($string1)
$bytes = $enc.GetBytes($string2)
for($i=0; $i -lt $bytes.count ; $i++)
{
    $bytes[$i] = $bytes[$i] -bxor $data1[$i]
}
[System.IO.File]::WriteAllBytes("$out", $bytes)

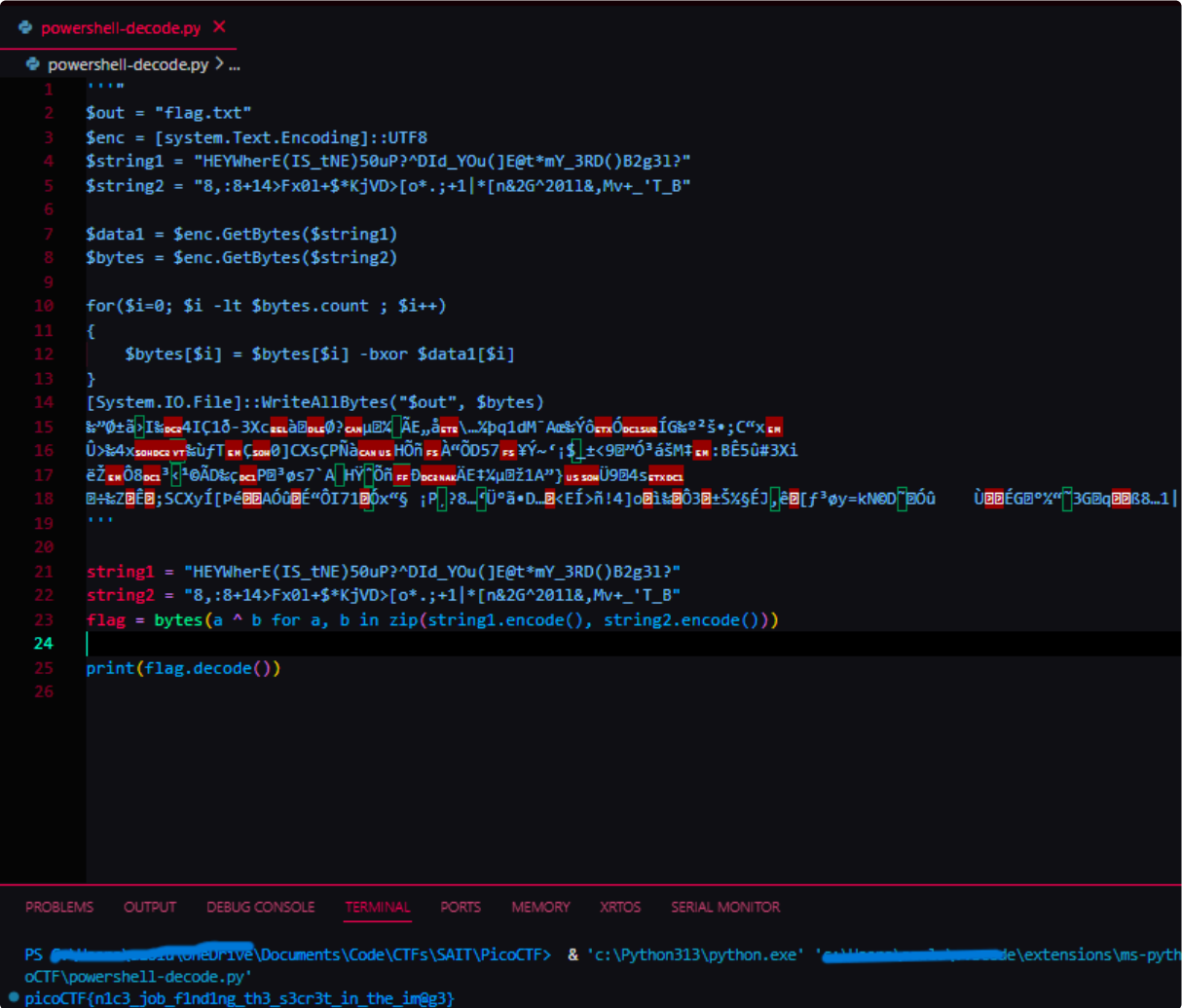
%”0±ă>I%04IÇ1ð-3Xc0à000?0μ0% ÆE,,â0\…žpq1dM~Aæ%Ýô0000íG%°²Š•;C“x0
Û>%4x000%ùfT0Ç00]CXsÇPÑà000HÕñ0À“ÕD570¥Ý~‘;$_±<90”Ó³ášM+0:BÊ5û#3Xi
ěŽ0080³<³@ÃD%Ç0P0³0s7`A HŸ^Õñ000ÄE*%μ0ž1A”}00Û9004s00
0÷%Z0É0;SCXyÍ[þé00A0ú0É“ôI7100x“$ iP,?8…‘Û°ă•D…0<EÍ>ñ!4]o0i%0030±Š%ŠÉJ,ê0[f³øy=kN0D~0Óû
Û00ÉG0°½“~3G0q00ð8…1|
```

5. Recover the flag

I run this python script to get the flag

```
s1 = b"HEYWhere(IS_tNE)50uP?^DId_YOu(]E@t*mY_3RD())B2g3l?"
s2 = b"8,:8+14>Fx0l+$*KjVD>[o*.;+1|*[n&2G^201l&,Mv+_ 'T_B"
flag = bytes(a ^ b for a, b in zip(s1, s2))
print(flag.decode())
```

Output:



picoCTF{n1c3_job_f1nd1ng_th3_s3cr3t_in_the_im@g3}

Very very very Hidden

Hard Forensics picoCTF 2021

AUTHOR: SARA

Description

Finding a flag may take many steps, but if you look diligently it won't be long until you find the light at the end of the tunnel. Just remember, sometimes you find the hidden treasure, but sometimes you find only a hidden map to the treasure.

try_me.pcap

Hints

1 2

2,005 users solved

53% Liked

picoCTF{FLAG}

Submit Flag