Hive ransomware uses new 'IPfuscation' trick to hide payload

bleepingcomputer.com/news/security/hive-ransomware-uses-new-ipfuscation-trick-to-hide-payload/

Bill Toulas

By
Bill Toulas

- March 30, 2022
- 10:12 AM
- 0

Threat analysts have discovered a new obfuscation technique used by the Hive ransomware gang, which involves IPv4 addresses and a series of conversions that eventually lead to downloading a Cobalt Strike beacon.

Code obfuscation is what helps threat actors hide the malicious nature of their code from human reviewers or security software so that they can evade detection.

There are numerous ways to achieve obfuscation, each with its own set of pros and cons, but a novel one discovered in a an incident response involving Hive ransomware shows that adversaries are finding new, stealthier ways to achieve their goal.

Sentinel Labs analysts report on the new obfuscation technique, that they call “IPfuscation”, and which is yet another example of how effective simple but smart methods can be in real-world malware deployment.

From IP to shellcode

The analysts discovered the new technique while analyzing 64-bit Windows executables, each containing a payload that delivers Cobalt Strike.

The payload itself is obfuscated by taking the form of an array of ASCII IPv4 addresses, so it looks like an innocuous list of IP addresses.

In the context of malware analysis, the list may even be mistaken for hard-coded C2 communication information.

```
[0x140002298]> x 500
- offset -    0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x140002298  3235 322e 3732 2e31 3331 2e32 3238 0000  252.72.131.228..
0x1400022a8  3234 302e 3233 322e 3230 302e 3000 0000  240.232.200.0...
0x1400022b8  302e 302e 3635 2e38 3100 0000 0000 0000  0.0.65.81.......
0x1400022c8  3635 2e38 302e 3832 2e38 3100 0000 0000  65.80.82.81.....
0x1400022d8  3836 2e37 322e 3439 2e32 3130 0000 0000  86.72.49.210....
0x1400022e8  3130 312e 3732 2e31 3339 2e38 3200 0000  101.72.139.82...
0x1400022f8  3936 2e37 322e 3133 392e 3832 0000 0000  96.72.139.82....
0x140002308  3234 2e37 322e 3133 392e 3832 0000 0000  24.72.139.82....
0x140002318  3332 2e37 322e 3133 392e 3131 3400 0000  32.72.139.114...
0x140002328  3830 2e37 322e 3135 2e31 3833 0000 0000  80.72.15.183....
0x140002338  3734 2e37 342e 3737 2e34 3900 0000 0000  74.74.77.49.....
0x140002348  3230 312e 3732 2e34 392e 3139 3200 0000  201.72.49.192...
0x140002358  3137 322e 3630 2e39 372e 3132 3400 0000  172.60.97.124...
0x140002368  322e 3434 2e33 322e 3635 0000 0000 0000  2.44.32.65......
0x140002378  3139 332e 3230 312e 3133 2e36 3500 0000  193.201.13.65...
0x140002388  312e 3139 332e 3232 362e 3233 3700 0000  1.193.226.237...
0x140002398  3832 2e36 352e 3831 2e37 3200 0000 0000  82.65.81.72.....
0x1400023a8  3133 392e 3832 2e33 322e 3133 3900 0000  139.82.32.139...
0x1400023b8  3636 2e36 302e 3732 2e31 0000 0000 0000  66.60.72.1......
0x1400023c8  3230 382e 3130 322e 3132 392e 3132 3000  208.102.129.120.
0x1400023d8  3234 2e31 312e 322e 3131 3700 0000 0000  24.11.2.117.....
0x1400023e8  3131 342e 3133 392e 3132 382e 3133 3600  114.139.128.136.
0x1400023f8  302e 302e 302e 3732 0000 0000 0000 0000  0.0.0.72........
0x140002408  3133 332e 3139 322e 3131 362e 3130 3300  133.192.116.103.
0x140002418  3732 2e31 2e32 3038 2e38 3000 0000 0000  72.1.208.80.....
0x140002428  3133 392e 3732 2e32 342e 3638 0000 0000  139.72.24.68....
0x140002438  3133 392e 3634 2e33 322e 3733 0000 0000  139.64.32.73....
0x140002448  312e 3230 382e 3232 372e 3836 0000 0000  1.208.227.86....
0x140002458  3732 2e32 3535 2e32 3031 2e36 3500 0000  72.255.201.65...
0x140002468  3133 392e 3532 2e31 3336 2e37 3200 0000  139.52.136.72...
0x140002478  312e 3231 342e 3737 2e34 3900 0000 0000  1.214.77.49.....
0x140002488  3137 322e                                172.
```

The list of IPv4 addresses that will assemble the payload

(Sentinel Labs)

When the file is passed to a converting function (ip2string.h) that translates the string to binary, a blob of shellcode appears.

Once this step has been completed, the malware executes the shellcode either via direct SYSCALLs or by proxying execution via callback on the user interface language enumerator (winnls.h), resulting in a standard Cobalt Strike stager.

Here's an example from the Sentinel Labs report:

The first hardcoded IP-formatted string is the ASCII string "252.72.131.228", which has a binary representation of 0xE48348FC (big endian), and the next "IP" to be translated is "240.232.200.0", which has a binary representation of 0xC8E8F0.

Disassembling these "binary representations" shows the start of shellcode generated by common penetration testing frameworks.

```
FC                  | cld
48 83 E4 F0         | and rsp,FFFFFFFFFFFFFFF0
E8 C8 00 00 00      | call 22BECABA112
```

The resulting shellcode from two IP addresses

(Sentinel Labs)

The analysts have discovered additional IPfuscation variants that instead of IPv4 addresses use IPv6, UUIDs, and MAC addresses, all operating in an almost identical manner as what we described above.

Before translation into binary:

Address	Hex																ASCII
000000C000080000	66	63	34	38	38	33	65	34	66	30	65	38	63	38	30	30	fc4883e4f0e8c800
000000C000080010	30	30	30	30	34	31	35	31	34	31	35	30	35	32	35	31	0000415141505251
000000C000080020	35	36	34	38	33	31	64	32	36	35	34	38	38	62	35	32	564831d265488b52
000000C000080030	36	30	34	38	38	62	35	32	31	38	34	38	38	62	35	32	60488b5218488b52
000000C000080040	32	30	34	38	38	62	37	32	35	30	34	38	30	66	62	37	20488b7250480fb7
000000C000080050	34	61	34	61	34	64	33	31	63	39	34	38	33	31	63	30	4a4a4d31c94831c0
000000C000080060	61	63	33	63	36	31	37	63	30	32	32	63	32	30	34	31	ac3c617c022c2041
000000C000080070	63	31	63	39	30	64	34	31	30	31	63	31	65	32	65	64	c1c90d4101c1e2ed
000000C000080080	35	32	34	31	35	31	34	38	38	62	35	32	32	30	38	62	524151488b52208b
000000C000080090	34	32	33	63	34	38	30	31	64	30	36	36	38	31	37	38	423c4801d0668178
000000C0000800A0	31	38	30	62	30	32	37	35	37	32	38	62	38	30	38	38	180b0275728b8088
000000C0000800B0	30	30	30	30	30	30	34	38	38	35	63	30	37	34	36	37	0000004885c07467
000000C0000800C0	34	38	30	31	64	30	35	30	38	62	34	38	31	38	34	34	4801d0508b481844
000000C0000800D0	38	62	34	30	32	30	34	39	30	31	64	30	65	33	35	36	8b40204901d0e356
000000C0000800E0	34	38	66	66	63	39	34	31	38	62	33	34	38	38	34	38	48ffc9418b348848
000000C0000800F0	30	31	64	36	34	64	33	31	63	39	34	38	33	31	63	30	01d64d31c94831c0
000000C000080100	61	63	34	31	63	31	63	39	30	64	34	31	30	31	63	31	ac41c1c90d4101c1

After translation into binary:

Address	Hex																ASCII
000000C000080000	FC	48	83	E4	F0	E8	C8	00	00	00	41	51	41	50	52	51	üH.äðèÈ...AQAPRQ
000000C000080010	56	48	31	D2	65	48	8B	52	60	48	8B	52	18	48	8B	52	VH1ÒeH.R`H.R.H.R
000000C000080020	20	48	8B	72	50	48	0F	B7	4A	4A	4D	31	C9	48	31	C0	H.rPH.·JJM1ÉH1À
000000C000080030	AC	3C	61	7C	02	2C	20	41	C1	C9	0D	41	01	C1	E2	ED	¬<a|., AÁÉ.A.ÁâÍ
000000C000080040	52	41	51	48	8B	52	20	8B	42	3C	48	01	D0	66	81	78	RAQH.R .B<H.Ðf.x
000000C000080050	18	0B	02	75	72	8B	80	88	00	00	00	48	85	C0	74	67	...ur......H.Àtg
000000C000080060	48	01	D0	50	8B	48	18	44	8B	40	20	49	01	D0	E3	56	H.ÐP.H.D.@ I.ÐãV
000000C000080070	48	FF	C9	41	8B	34	88	48	01	D6	4D	31	C9	48	31	C0	HÿÉA.4.H.ÖM1ÉH1À
000000C000080080	AC	41	C1	C9	0D	41	01	C1	38	E0	75	F1	4C	03	4C	24	¬AÁÉ.A.Á8àuñL.L$
000000C000080090	08	45	39	D1	75	D8	58	44	8B	40	24	49	01	D0	66	41	.E9ÑuØXD.@$I.ÐfA
000000C0000800A0	8B	0C	48	44	8B	40	1C	49	01	D0	41	8B	04	88	48	01	..HD.@.I.ÐA...H.
000000C0000800B0	D0	41	58	41	58	5E	59	5A	41	58	41	59	41	5A	48	83	ÐAXAX^YZAXAYAZH.
000000C0000800C0	EC	20	41	52	FF	E0	58	41	59	5A	48	8B	12	E9	4F	FF	ì ARÿàXAYZH..éOÿ
000000C0000800D0	FF	FF	5D	6A	00	49	BE	77	69	6E	69	6E	65	74	00	41	ÿÿ]j.I¾wininet.A
000000C0000800E0	56	49	89	E6	4C	89	F1	41	BA	4C	77	26	07	FF	D5	48	VI.æL.ñAºLw&.ÿÕH
000000C0000800F0	31	C9	48	31	D2	4D	31	C0	4D	31	C9	41	50	41	50	41	1ÉH1ÒM1ÀM1ÉAPAPA
000000C000080100	BA	3A	56	79	A7	FF	D5	EB	73	5A	48	89	C1	41	B8	26	º:Vy§ÿÕësZH.ÁA¸&

Deobfuscated strings forming a Cobalt Strike stager

(Sentinel Labs)

The takeaway from this is that relying solely on static signatures for malicious payload detection is not enough these days.

Behavioral detection, AI-assisted analysis, and holistic endpoint security that aggregates suspicious elements from multiple points would have a better chance at lifting the lid of IPfuscation, the researchers say.

Related Articles:

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

Microsoft: Credit card stealers are getting much stealthier

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Quantum ransomware seen deployed in rapid network attacks

Microsoft Exchange servers hacked to deploy Hive ransomware

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.