cybereason

TrickBot-Anchor: Indicators of Compromise

December 11, 2019

AnchorInstaller_x86
4bba60ff11f8b150b004960c658ad74a707ebcea
9efd42856bd596eb3246e7dc85288098e5289874

anchorInstaller_x64
3ed09498214d93c9ec14a15286546d242ad58943
49f6d0beca33af85e8a5ba64aa9e848ce250188b
Dd3421cf241ec2058167122ce6af0184fb1666ce
Fa98074dc18ad7e2d357b5d168c00a91256d87d1
9efd42856bd596eb3246e7dc85288098e5289874

Anchor_x86
F3683a0c12154e8bf44d9d942db3eac9e930e7a5
Bd26238fb7d7e16ea79073d882bba00d34dd859c
9ebb541dcb24d564448a6f5e00c613b73eba7148

Anchor_x64
E5dc7c8bfa285b61dda1618f0ade9c256be75d1a
46c595e580719a4c54f55b4041f81d6e50ab4062
4dff20e4a24d161e288bd8692c668d3cf0b057ee
bd4bada49725daff995e4d7d3554aaee7d737bab

Anchor_dns (new variant):
5f1ad1787106de9725005d8da33d815d0994ee83
B34B201F727CA2C0907850A427FE220ED9CDB2BD

Anchor_dns (older variants):
8b185b88519206b883554613a8660cd73dc8fff5
e26d5ed1aa0c38a64f0f9c2f85fc144b320c0147
c759203d19d86540b6c1efa6eec6aab9ed25470d
bb52acd9f09c190dc9a4a61aeb1971a4907d1b79
33c9a73ec1150f0b55903537e79e11413954e58f
24d4bbc982a6a561f0426a683b9617de1a96a74a
fc0efd612ad528795472e99cae5944b68b8e26dc
8beef55eee4608afe013741033f060c8f47804b5
dacd5b49ac628157fcb9cf8d6e537e851ef29a64
b388243bf5899c99091ac2df13339f141659bbd4

Trickbot Downloader:
f654a4dca9faf8795ef29ac1bdbf0c8bf669ef87
83bd3bc3f0d4b69fc58beeb7660b90da568b2bb6
6e9dd519b910c4ae53ab1721a5707ad7fc1ab3f3
11d7bf29f1fcbacfae77f1d724813e1a333d88fc
65ba257dbc25eed3bfff6e93e74073ee8b724e28
b0d4ef710e879b6b8d769a7bd96063af20b8a1ce
02d431f7159c504269fe63472f1c1466412f7d1b
e72270bbdab7a85a5c5721f3f3cd298608dff04a

TrickBot:
778b8b23266d1e4ba757c4cf1132aef5df8fd759
598f7f64ebd368dcdc97b0185b4dc1b402e81947
545f77c1bc384b77e8f588a4e95e5b38ffbf517b
02993e94cb86d258c649a9a47bf0951b5ac845bf
e72270bbdab7a85a5c5721f3f3cd298608dff04a
42a5e06c6feb7e3087f206066f37a96763c54122
21979320b046cd54f9e6c34fa2b2094536f9ce20
594397cacb56a47e026563a99dacaadeead3d304
545f77c1bc384b77e8f588a4e95e5b38ffbf517b

Malware signed by BRO-BURGER, LLC
f654a4dca9faf8795ef29ac1bdbf0c8bf669ef87
83bd3bc3f0d4b69fc58beeb7660b90da568b2bb6
6e9dd519b910c4ae53ab1721a5707ad7fc1ab3f3
11d7bf29f1fcbacfae77f1d724813e1a333d88fc
65ba257dbc25eed3bfff6e93e74073ee8b724e28
b0d4ef710e879b6b8d769a7bd96063af20b8a1ce
02d431f7159c504269fe63472f1c1466412f7d1b
E72270bbdab7a85a5c5721f3f3cd298608dff04a

Malware signed by NIRMAL 0013 LIMITED
8b185b88519206b883554613a8660cd73dc8fff5
effda16b763f8d6fd4f2baf7779367eabf9678ec
b718e3103be3076ea0c53ca703c073fa08eb1e6c
be0aeea7b7742541b199f7ff8bacc0c0cabb35b2
ff0a4d7cecc6bc9c06f8d4bb1da9991e45cd1966
a00e355e1b1328e7198530a533a3db12a55cf384
1137e0ad0b75942d36c62639cbc688b645966df2
641bb4901222ec0cf7f2f1d518ffa7cace810394
aa38113d8b9fd5bfc7b2075d1b63c167cf687b9f
b718e3103be3076ea0c53ca703c073fa08eb1e6c
91270cb84c2a40ed488b4ca363f1db06b7edc589
fc97628dfa3ae7feb78906f8f1170b901a138bae
23e5e8d180d8d7bfaf9cf469aa104ab0ce6a5ee6
e196560eecb90050e97cd45b45922a356c3647a3

5d523c83094194b86da06320b6b3019e3adcad8a

Malware signed by Biller FIN Oy Signer

d0d761b5a1745838c558ee17c547eb3fdfd25f71
44e346ed991e1f7aa967116a225d2e9a539181eb
26b0d47d5fadea36f909fd5576e51e5f3227735d
acf6ab5b9a983c70864f0c95790d85d257ceb528
c06325c906690e1ddc3cfd89d7769290dcb0cafc
6938102082e77a8142816ebe5a0989392ad5eafd
8b55e3eb84d157f6ac2d0fe707bac3ee89a3fc2b
295a0d5be269c83ecc4e72f1519dc4278f08dbec
8afd75b83357fdfe09d4d86704a74c6ac13f0573
4daf210250cf44766c3ec5441fcb143235f4ee6d
322be936e633eb792879034d276b042fcdbf9965
e7a26ef19640e1856438d73c2fd5814b90036fe4
69e5d564340600083d8a088d66497691d0074792
e38f1d32f2cc13c93841b4b812cb78a575300fad
d89480a4b11438499e962d525f9b9f8f940b217c
934b074521117c2e59214d4e163164d7006c7f14
e63abcd741809c81ad40fa6005f0fea7b9c045ea
156b9b6e1bec69f19fbf999b870042fb8934d7c9
e133981f3a5c1c9341218a93dcf1cd0ac7374c34
5c2a0c531ccba09281d824b79fb706c9d6d8e7a2
2e5ab9b6826a78672f22911653b5098272815d46
e2e21411d286ffe7e2515f9ad917e3d0d43d6caa
a51dd270c543e1e69c1fbfe8411ad7f57b611377
0c8031fdff7fc620705d2b9bfc6a4390711e89db
6019be44f581a90c3f98cd93edf70f9a4c6fc39b
5bc9b2bd56401d05b6429c32791cfe96e7976842
219a8496fd2be9419b9368271e2a4bc3c37b279c
ada4e1205849adc804a1187cfd35561b884e0905
ec808ed2b078c773c561aa319999006e4281250b
185df1bd6804ae508fb3e18e1120222fbcf44598
fe782824c8a51a0410b765867f99424bc6c74fee
8d58679bc1d221bad55ad793715e378ccc96e734
59347a37d550d8cd530ac2fb3b77310a7088bf16
aae85a8e8a106002e8e35e695140fab2924dee48
7472dcb193c700180857a33144c5d635770d4978
6699960d91b1dfdbe12d8b99d2380ee3c159cdb1
eea8449c46eb6e3cd22009b90b84e0498147bd3e
b7953c1d994ed31814212f9351ea73c752e6ca44
640a1a6dcef9e6ec0c5c19edb7cc4e1acb77c3a7
e3895abdcf851598206f49b20f8c1b585f439e8c
720f44e8d31729005483ca4e650309f88aa3d751
8b91ac1b369d31afb60056922a552bb6bd9dc913
bcd217b6f9667690bc2470d95dd05440c0bbeafa
42d2f35d2f3164de2e1b2980cde19555f52a7a72

44510c33c823c7c57f8d8224e8335187a723418d
f840bdaa91e9cce452ab5c2cc0a016b9eff3bb13
2e61331b8d971d9af19b87c738edff6c65b4f8c3
32f00707bed681d9bb1abaac81df4efc4ccb5d61
1db526e00f3e7b50d4dd58688229f6eb48be887b
3ca12ce264a9aae7a752b1b062de229c58337acb
59299c754e825081a36c5deae20bfd7baf772de3
ce82546501d0399f0d15ac0f99784033eac14c43
fdb92c349397ef25f5a674f57c66a9d03d4eb149
e66aa75268fea36ad8c5bfac413f948c7f508c0a
586211678fd565e6ca5b4f65fa3acbec11e6a5d2
98a0c1121fc3007b79c10316eb48ade345f80382
30df65d5ca527910c6dd8c485fd82c9c028e8de7
6b71389f2a2fa9767fe45d85fd5953f3e9949845
94c2d854b2008e4ec0c7b069ca7e1f514e4657da
64bfa88fdc68db4c1f7c6b81da35d35e7db0f1ab

Malware signed with Serial number: 06 27 E6 3C FA 11 17 45 84 28 D3 92 DF AA 8D AE

295a0d5be269c83ecc4e72f1519dc4278f08dbec
22e9f403e62ffd3334ec15f12b7d530546dbe1ef
c5d6a4fea017a9e59099e6e94603b9cece433bc9
8beef55eee4608afe013741033f060c8f47804b5
c5e23aa3517029bb0fece0095d1bf5f0a44946d7
fbe87d969d67fa5406f06bce16ca81571ecf8e6b
d2e49e805a84374b478595a487e2bfeec7e27932
c7371ce37c57a8725ddf4d551ecdbae8b097e638
8cfe7e8e3c747fcfb2e2657e557d07baa3d4c4f4
b6081f8217d44c68fba046acbb502d8002a40b50
8d5a99e9f7f2076637fceee41356a614585848a7
ad2213c170dbc2af6766ee82a1180a731cafd78b
5e10e00763394ab2b52f3c1f18f9dbd965948e4d

Trickbot domains:

wuniuqhi5byfc5qh[.]onion
carambaneed[.]club
cics.secureforge[.]info
northracing[.]net
sodonnews[.]com
qfcallc[.]com
sulushash[.]com
codificarte[.]org
fmjstorage[.]com

Anchor Domains

excelestimation[.]com
nuthetazeta[.]org
Deckmastershousesavers[.]com
Toexample[.]bazar

foreducation[.]bazar

Anchor_dns domains
kostunivo[.]com
chishir[.]com
mangoclone[.]com
onixcellent[.]com

Anchor IPs:
51.254.25[.]115
193.183.98[.]66
91.217.137[.]37
87.98.175[.]85
23.95.97[.]59

Interactive hacking:
45.11.19[.]91
45.147.228[.]91
91.121.89[.]129
170.238.117[.]187
185.158.248[.]251
186.10.243[.]70
199.188.200[.]17
199.217.115[.]53

Trickbot IPs:
23.94.3[.]13
31.214.138[.]207
36.89.85[.]103
37.230.114[.]53
45.138.157[.]23
45.141.100[.]6
46.174.235[.]36
51.89.115[.]100
66.55.71[.]141
81.177.181[.]222
81.190.160[.]139
89.32.41[.]104
91.92.136[.]82
94.156.35[.]235
103.196.211[.]212
103.219.213[.]102
103.255.10[.]24
107.172.39[.]48
107.173.160[.]18
108.170.52[.]149
117.196.233[.]79
117.255.221[.]135

131.161.253[.]190
164.68.96[.]155
170.84.78[.]224
177.105.242[.]229
178.183.150[.]169
181.112.157[.]42
181.113.28[.]146
181.129.104[.]139
181.129.134[.]18
181.140.173[.]186
181.196.207[.]202
185.99.2[.]169
185.99.2[.]242
186.71.150].]23
189.28.185[.]50
190.13.160[.]19
190.72.235[.]47
190.142.200[.]108
190.214.13[.]2
192.3.73[.]164
192.3.104[.]48
192.3.247[.]106
194.5.250[.]109
194.5.250[.]162
194.5.250[.]169
195.123.220[.]184
195.123.220[.]193
200.21.51[.]38
200.127.121[.]99
212.73.150[.]233

Public IP identification resources
ipecho[.]net
api[.]ipify[.]org
checkip[.]amazonaws[.]com
ip[.]anysrc[.]net
wtfismyip[.]com