Breaking Down the Casbaneiro Infection Chain – Part II

By Sygnia

Published: 2023-07-25 · Archived: 2026-04-05 16:08:15 UTC

In previous Casbaneiro campaigns, the infection chain was initiated by a spear-phishing email containing a malicious PDF attachment that contained a download link to a zip file. In recent attacks observed by Sygnia, the infection chain was initiated by a spear-phishing email containing a malicious HTML attachment that redirects the target to download a RAR file, as illustrated in Figure 1:

Another major update in the threat actors' tactics, techniques, and procedures (TTPs) is the use of a UAC bypass technique to execute code without a UAC prompt, by employing *fodhelper.exe*
Fodhelper is an executable used by Windows to manage features in its settings, and is often used by attackers to achieve a UAC bypass.
This attack is usually initiated by creating the following registry keys:

Following the creation of the registry keys, the attacker populates a (default) sub-key with the command line. Once fodhelper.exe is executed, either manually or by navigating to "Manage Optional Features" in Windows, it executes the command line with high integrity execution, thus bypassing the UAC prompt.

Casbaneiro attackers were also observed creating a mock folder on C:\Windows[space]\system32, and copying fodhelper.exe to that folder; however, the use of this path was not detected during Sygnia's investigation. It is possible that the attacker deployed the mock folder to bypass antivirus detections, or to leverage the folder for side-loaded DLLs with Microsoft-signed binaries for the purposes of bypassing UAC.

The *contactofiscal[.]cfd* domain which is embedded in the HTML file (*adjuntos_0102_.html*) that was sent in the initial email was registered in mid-February 2023, and resolves to a Choopa ASN IP *45.32.90[.]170* which hosts hundreds of additional domains. Several additional domains were created and resolved to the same IP around that time, and are also embedded in HTML files with the same name; this led us to assume that those domains are also part of the current Casbaneiro campaign: *factudigital[.]cfd, factdigital[.]shop,* and *cgdf[.]shop.*

Furthermore, during our analysis, we discovered that over 40 files with the same unique HTML file name (*adjuntos_0102_.html*) were uploaded to VirusTotal since February 2023. All of the files were embedded with one of the four abovementioned domains, and two additional domains: *serviciofac[.]shop* and *fiscalcgdf[.]shop*.

The *adjunto[.]shop* domain also resolved to *45.32.90[.]170*; based on its name, we assumed that this domain is also part of the current campaign. The *tributaria[.]website* domain which was used in later stages of the infection chain, was registered in July 2022 through Tucows Inc. The first resolution of this domain was recorded in mid-August to the IP *172.104.193[.]212,* and at the end of November it resolved to the IP *139.177.193[.]74,* which hosted it until mid-March 2023.

The Canadian Akamai IP *139.177.193[.]74* also resolved to the *ckws[.]info* and *m9b4s2[.]site* domains earlier this year. These domains were part of the malicious infrastructure that was reported by Sygnia in our previous

Casbaneiro blog post – although they resolved to different IPs at the time. Additional domains hosted by the same IP which might also be part of recent campaigns include *wiqp[.]xyz* and *live.xtream-ui[.]info*.

Based on the information available in VirusTotal, over 20 malicious files communicating with the *tributaria[.]website* domain were uploaded since August 2022. Most of the files are obfuscated PowerShell scripts – like those described in Sygnia's previous blog post – and some are CMD files.

Based on the samples collected during recent Casbaneiro investigations, Sygnia's research team validated and updated three YARA rules that were published in the previous blog post (see Appendix for details). VirusTotal retro-hunt queries for these YARA rules one year back yielded the following results:

All samples retrieved from the retro-hunt analysis are listed in the IOCs section below.

If you are currently being impacted by a cyber incident, or are seeking guidance, please contact us or call our 24/7 hotline +1-877-686-86

Due to minor changes observed in recent Casbaneiro campaign, we have updated some of the YARA rules published in Sygnia's previous blog post:

Casbaneiro_Dropper_Script – detects Casbaneiro dropper script.
This rule was adjusted by excluding specific C2 domains that were changed in recent attacks.

Casbaneiro_Directory_Script – detects Casbaneiro directory script that creates a proprietary folder in the root directory of victim's station (no changes were made).

Casbaneiro_Trojan_DLL – detects decrypted Casbaneiro trojan DLL. This rule was adjusted by adding unique strings and exported function names.

11f01a5357a0b388c5b783af95cff460619a02a8e0089702d24752f0cb9b2585
b8d2cbeb41d449b43103c7da0a8221dd350462c5ec5eb48f51deb5721f5280b0
cb3cb149657d21f71f4476c35f9ac8480a61fe3a4d54cabd4b66797334a15ca0
ed6f357cfe91cf9d3d7895c5b286992e6cfa7e508cbe346cf71a30ff5bee1815
947f08178dd04e36f1c0ec7223a931cfeb671e665433ef1a1c34b396def8c993
00d5e0da3e57afbb2bc9812435519ae6a74f2c49b9eab4347855f68c4da005b1
b7d036439300be2b1a78ef1fba1df0c3495c62d81e85a09fd83611ce0a52c0e6
b8de390cc2e66eca6f37da05b39bf1e69de6e2c78f14e317929cac9201ac5b86
fd6085a4f0fc7b9cd613eda999bdd7cb63fc1e6e36a640a6a8bfb2f4718ca963
bbd916dddd0f8849e6a860b4f7e9e8a3f342508b6d36525b783c7ef6a29cbe60
a967e3181984aabd705828f540935451fe7487f84711031d467d92ae48a47b09

f4aa142a2d45c62966a319ccdb37b30621a4ad22b4be82c0c1e67dedf56442d9
692a498dc935c3965171fda920728bec25039201e2cd734a2be8d0110fada35c
3765b1a7901b40c84dc69bccf63641bddb6c2341ffc24caecf1dfec2aebe283b
d05dbd52d14718db186b592a352d38394e17b49b4e03fe0cf7481fd10367a131
67b12f31fab1a66a398e4655fcff90e278805ad85c1516d222849ce8ea815519
965b0de04dc0e7305da99c656fa4c3a7ecfc93dde1975e283f3645dc13394512
33fb18a1eea637777911bb7f51ee439b98c696ecc25ce38e371e46edd1cc4ff1
43e4378549664935dced7b60f7dddeb37774b363a952c4402b12b877957a44c7
db50dc942b87d49a505c25841b88e71ec99c9e26727fcf348b3c2844d2737477
ab7e105943218ef48c00f9ee04b4b3cff79054f9a6591e6ed5b40c47d77c34ee
5f76126a2acb908efbc950c12add52fe8ac9b872802176ff39551eec1a05fbe2
83d692c95335dd38486282c429b9744e1228ca7d24851ff9d601d494779c508b
914d4f30f170f64b1e61e421061454f058f73c79b5f720850f6eb7c18166bdbc
51a6225aa049b78c2ade7c7f94788fd3dfe115ccab962cd39936e01433d789a7
13e2c5b07b28bfea1a493dbdb755fc85b74064417b21c08526aa63c66aadcdca
d0923cb0c89c117554b3eefd8efcd8d368d82e1d74834059cef363cbd669d2ec
01422b80b6c3fd58caaed7fa03cf040a3836c1c5932b5bb23e95ff5aa7319667
0f5c356335909f05bfee17f75da47e9c0b2214b82d298bda0c4763ad2009a577
5edf716aab84a3434e79b67c829dc6ddffc19b9e5992f69be4b4150236fd4616
e53f15601c10ba98f8e667e4d97bd1eabbc8a1546e01f753255b6ef2b0df5428
30b43c9055a906957e0f986bce5509b4448006ef1ef873a8c4fc736c22244ffe
da965b8d71587bb820873f1594976477fd4bc6b980f981f05585bf84048e2b88
5dc1a5fd7af11e7a4595c1140c7414cfe90a27c12915bce042bbd277b33c6863
cf2eaee4489e0ddcaa8b0e7250c807838c4695655d1ce52bbb5b462e5a4f688b
ff440dfbbb8aeabd6d0c02a581299221ef038080f532d76cda3986af6ca1b97e
f348e1b36f9c0d679524cf13ee47aa12a98db2a7333ea95b94129455c0730df2
f62875a957abf962a097c3288ba6cd69d599dff2efea7a7a30be25cb1d4d19aa

5c770af12eb7d9909b949bcca56594734ac7afbce65471dae3f750b7f069a234
4a23b6b48afd468afaf633b3c16a9c4dffeffa2080e3e70decc6ff3490369c0a
6cfdcb9e370d9c5e24b3c442e3a6d10e143e546371aca6585c55b83626edf88c
80216218bf59331042d7ece32bda55cfb07b60885b5208e1f392842f486bbe19
a40e203cb9969cff95c007d4517b4f2c3323ee3717f6628af0110f2035bca1cd
182be5deaf5782e73e3f03624e14d4cc300a33eba45dede18cf79b7f7ce50fd9
f0e25b939069e195e3f38157bda524fbece239758e66be871284e9d300db985b
f6d3d7e59b0e860ca2448bbaa6d31d515b3ea7b9a492f851d425e9df75d52615
bb5a835f15f3b8d0064c4f9b222b40ace27b8a56730e718b45b0a5a7afbf7175
cc3dc627a3a9be0c90c0cc49c63cac554aa5beb4b4eb2af7f252bc023bd65eea
b0b7c57fa4eb66dcc30c5dd2b459155d69227bbe2e989d3fe99cd4ea15600d9b
94a03c12ff5e4427182e81d3f0596b75e974cd30a6b85a3ab86b09c08bc28240
a2320ea11cbac9e87651c4afec29e9df4f6d4c9b1f1c7aae1d7f244dd7d923aa
4723e36ab1dabf48f44898895848c86157f215bf6c21ce40373b09ec3c15d70a
04736c07b767bb780c01f2bae422c9174101b0c2e57948cd1c5ca744e5a3124f
7bb65622a41630d423382adf9cff706dccf23791be6235cff3fd5974de5ae831
92a9c8d3050a4c6020f651530e995fdabe2898f37a42d9612b1b4d720854a11d
bd030f863ab39de4bccb702778cbaabba8fd50c9cbf9261f3d7cc072cb48666c
761dc188fd9d761a01403c59434133d5a58a08c6a8ddfe6196edc08d4d00e9c1
3ba9a15929b3a0aa165352a068cbc4f0dd205a2d779e808ccfc72e7eede1f2a0
35bbb3a6c7510e6f518036f3ff0f09ef51c6a0add0ba14d9ae0925f5ea9337be
d2b422e2e177d6f33a684e18b3ec59c23173fd7fecbf7a0569df1efe20a8b3b6
b40032379af79ee32cfe7aeb8e239a864a7a8cc3d932db53de806858e57a860a
cf4f9f3e17aa74d3818977c2bd0a9d1f530b51f58e5389d49a32d66794a3924b
b6306f004af6a831ec5f878acb93d5167878e39e0a90b75d377bcdbed340d60f
236155ca53e8afda04e04181f57fc89cdc5a702ff44a2e22782c68503ccdc7b3
fe796047548af3aa72f7250354eb7d8f80dba768047f46dae8ee115404eb04c4

d3a2653f7d49178bc14a6d838af864501d9a6e9962c2210f810b03a5131bcdc8
fa82be4605c59dafb8fd7b006aa125b174ec46f6ace06bb6b25583e1aac20dd0
f68b47b80aa9b70f47a459d33d1a7745fe5b2c3658050aa5ba7d4dabf6ac42fe
7e21500d4d39b725cdf52013fd7d1efc873c41cbf36f4d55ee7d1ae804e3274a
de43853bfb670a457df4844936c0b984507723089a39c17d5bb5d66bfe24c6ca
6f89360690991707ae035eb30221ea1c319673a78125d0caf03b56641b543fcf
9be8fe0915f4e991560aaf14b3b809257e86a3554664a18812bcad3bff65bc17
9b96b4f0c25b7e80883d57e1245880a2fb63024ceedb36809292c840590206e0
7a2d37bd3fdc3e36cac939262435339e0a887a0dcdf49f78ae8a05d6d43a838b
c91aeb5024a150db97f2d83f0207e9a960c51bba615c0e82d71ec6b9b59c849c
5d9d89a7f224a7b5c18785f9b72969d8079f63cb7f4ee8137d3699632e39aa90
e819d1f87027069a920bb2373ac20b392ed47eeb1d4d55220147e8a7b4d40a90
9616137243c827a1cf2d73d9296033e2b504ee154d5204d102b08e08ade1b9de
e5948aa8c61cdc585f9b33654bb502f1fb991a23cce45169ddc0db76318c2923
c42afd24bec1873eb5c674cfb5791576032715cee642712f6ab2fb1bc4543a8e
5866fec6080ada776b1c17aa22c4525d678fc091ab21179ede79a0a994885f1c
30bd9b42d7357ff24dc64543d286441ca15f9869a2e2307124de0c49c6c2613a
e31a061e1e7a36d4a1cad4c8eb058ea469ba5163e00a10249259c0ad733cef17
21983983af5e1a3915fa1659dc1d3db2a1830e6c2e723c47365f8dd4c112277e
502e0b155e91c1a7b5580d9171ac02ec1ebc58e8b07979fa0b297996e5da210b
2b67769c29ef7d90fc16e3138aad99f1428027589e2c676e55c6024939830453
71caee789ccb097d71bc650b7ddc01df9399ee0fe528487b9a4604b538e17f2c
489a5d3fff408a7adba3bc689c7a69a240694e65c97756a450307244e8197db8
9cbc6c1415c1643e9dedefe2b99fcc5f5c5e626899b9b88f469fd7df9ffd1b49
2cf9b85fca1469f801033952ecc6082e4eb7a7e9944a9893b79e758c57214313
eee919352e49e165d6c281bc29a8f50fbefd1f4ddd6dc866648ac9f1f7193828
9fec5be2103ebcb7a2c0306a43fbece75ae1cf2c8074913606e13f64d8be59ce

f655a95ccdb0b8c9adcf1f2e1e0887ff506d4022b9cd7c2b3b3058ff38904c67
9d0551707c87a1079f962334a90a79fd747302bb4ff15aae9502d58540e07230
132e5442a2ddfc1439956c9f9c86bf201c180cefad59a003ad1709aa98d84fe6
9bd634dc3b7531e914aa36426d67b69b09d0a8a62c8dddd916d8503934d7f23f
ea3604a1e2dc34e87b4d3c338fa631f3ea8bb6d61ff2bb754985b6a399594661
cef0fa4ffd2a4750525abff9a5d3d77c343eaf20df39aa96a10246c77b968013
868f99f1bcd144afa8d302690c2a77dc280cc0aa2bc80bc5742a470328cc987d
0d9da2f3d007a4368ff82a166aac77264d85a9989ae93b644bf5d4535ef23d1e
44c1635b7f6573f7bce52a9fe0c430bf534a4b3ed344b7c7e5d749e92ca92cf1
3c14105a215a1f55489fb31505cb904aa6f6d0c153b58637a12f12df64fb4543
e597b4e40fb47f13fd004f9794b79d70d8a53a663a671ac5ef9dda9ee1b5ccdc
4ea64156be129a289087e392ef3bf561fc7d6aa1321c073e59efa7cbc57751da
cce27ecfb2e590322b098568ea846263696aa7eaa268c9f3e109ee202e0e8ff7
c28fe222150f1063a63c54b9ee642e448a2c7e7f4ab76bb770de1a9ee7082e40
4024824acb6751e345e5937fcad52a37952ce811efeeccbb5ca271fbdc029d95
137d12f7f8fd07b3bd2640417db8d57d787478e1d07696fe34420a33108c53a2
46a2d7e3d420966791b5f9f5323e27181d03a4b011dc2cf0f64b66fea6fcaf47
26975f0893c0ea65748b0a5c67c56ddef3c853190b10fd0fe0f173ed7e613fa8
34696299d98ca01c41f6e0158ec0620282877eae4ef39695baf20694d5f173b1
2ab7cbdf29058f0e0f30200c23b39989dc16144d778e843bc1e19b540b4e68a9
ac72d3831fabddc0c3e240ac4fa477823ed56fc63fedf1831a9a4cc6abfb062f
1c9ef52271c1e16cd65f06961fc0b603beacf0ad7d0167a530b348e67830a888
d0ddf3ec1dff97912976d5e1747c90c5567c47350eaee7009f2285cd33e9eee8
9840ed043fa897970899ea4de352ebd1581c23288f358a55d1d72d91fbb07f39
ecb1a0ff06a49394544f3018cdb66b4e170c4ae6fb288cb0559dfe2388106eeb
f8c30a42ea4ce894a8c3da414aa6eae01d559062504f087924e5bc810315d7d6
544068651e45d10785c9be8f1e4a18fdf5dcad6c3faba42a0956ccc5926057a0

349aed1d23d789587b38c66026f61966c48470cfa93724123b5cd101611a8b79
425180e3f04990f5f286a77f247f9c80b59d212b638a3a54c56de9565c608e82
4e1925f0ca68a56964235612b7940a64ed518b7532bcc28cc99c023e0425a0aa
16a955d7d7e246724e96b58ecde1515e8831fea290d1836b7aec8dc1b0d4fbde
4c42b69f9518f6fb523b35893e8da99337c11f0aab5d6b399f9675587aaf1ed2
68eb62f064112f4d72e93918a30c5ff86ad28dd95e52d498dc91a0a1dd5d4839
0775dc738e65fb6289175183099611a6de4e8334bbbfe8f4fd2835b87b632402
4ffd56151f34fa6a6817003b7b4d3758307449c965b45b277c723eb93bd01c39
4c6b9afba4deefe844ac49c73e29a2732488e654a0fc9255db480eb0eb28c590
ef8fb90a608370d41317cbff6a2fb2938f23d7952fdce7be6e36dc261dc82c7a
4b0a1952811894a67178db48e6617ec5528c236444884abf4f4f8b8fe2e014e9
38879044af231b5b38d508d177b2974381f87f120c14121166bcaf1aec092480
0610f151dfc45503f84363e443e211ad1187d8f42065cdb1bd7bb8a64fc44011
97a3e9c92f38f2d6114bd901f74307a0cc2e6708adbaaa6c8fa7adb61ee814d3
6b60b0f0ffc6a8983215ebfd575058bbdeeee8b364416e0f7e2de461af8bd3f7
442d28a4662139a7f396b96790200bdd6877d52536ab3a3014c4e7432ba89a39
84416f491e74c1e3167e8c7bc9b4cdd93c793652032ab1bad9a599b6d1e3e228
7c82ba1c68e2007a1b0d6ab1011c62261af9dabe03cc4c007602ce500b3fbbc2
7802f680b075bf9f111f227847f28dba882891a06bbdc601ef37b478823e9303
f57d1a313084f1b28d45f996fffb69eaaec7e3da425ed90ff00d485e09175675
775b4e0599241dc7698de6896c5088705e4d38ce7b037cb01703a5e52e286b44
6d821b08f5bea0ccaaedf48dd004376852be11d560d893fe33f7f5f8ce123146
eb690c83b700e68474ccb274a74701baed1acc8dc48e55f4abfe99753b28ea41
84311ab4e5c7fa27ea9567261a72c30d12a4100d4e6b2d9d6b95aae5bfd801d9
a95f0915f8ff5a7b3aac5539ffe916739e8f887ee4f50e16430a4c56c647dabf
1d2fa0eaf2b6a6fca89704df40a70e9767ffe6d2539e4cdc0612ba8e4a66d751
c2480b67bc4cffdfd597cf5f0257acc312607f1c338b5ced1c941dc816c73eb6

46fb4204b4c3b584e966a66fc053e06cc470ec4b67ff96b9b8127b81acc0c7f2
e136674e057e6c2f5e9ac3be515922946c3ab1326f4e7bf4cbc1fb5d1f8a11ab
434ff54507cd1285e17aa78fb1e7ef46963b66d71aee47835154aeadc74889f4
3925552b848f321e5c85d84cfe66ddd7a9eb3693a2704f1871f732f389a1fea9
30a9703b92a528c357a3e8f4144a93a9e8ddd246a82875283df8c9ba4d9fd349
ae6b3ac5cb27a068a28caf901401df64e24b411c47339a786418758a84f53069
4137e675014b0ef0975480c46879c9da5eed705d36a71f97664aac5bf383bef4
1d2746bda0892153c9cd5e3e8cf5ba3e911b3c6ca70f371486f6bd9262e74108
1adeb65277518275e049282c981faf5ed684877aa476baf07b5b82a806e29ed8
9152f1df74c2e2237f4b348cf83bd9f0c880140a0d18e0f3d270fd03f5dd7b0c
0ffbb9bcbda44122c64dad324b8f3823fd60a556a63a2a42f686787069756cda
d4eb079659b0b247424da03d9d0ad0eb670d84d9ddf360a1b866ca8564ae87fd
850cb53cb3ea0299cea757234265fc3adbf7c6e464e7995b66f27bd1218bf409
f9a5f5b3797b3bfdd27cbadf6e0f50327fc70b1cc47b75c55ccc1389b2610502
0dea1725a9b72a3214b946a8755d83f9256ddf1cec05a540255357259324a390
8288598c3caafc3ea95e2742209d03f6472ef71350e61891c17fe70d4c1c211e
a1de65ba82c6256b10858be700ea60d5334fd7f6647583f7c6dbef04a9d7489f
f3f75bb5c96c01436d66ca0d82092855b4ba9e7a4e24186475047c75a066b85a
42c11aa10873029f2e777350a5f965b984e277d99c3aa3e5779daccf4776ed9d
50b79051c2a94506255e598bd5db7a1ec1525c48ce243e61f84d8a8ea3f7b7b7
9274b4aaf62104026baa695e285b0883bb445dffe4a7cdb1f592f85fc2096183
0ec4d3d8ebd506b7fceb8e16f3910b545aff127db9ce6a230fa3b337173e020a
7355e00844e0cb7edc31933151873fee456521c5a16f0ab4644f99fbb4bb9a92
edbd849ccfc876dc4831718206ab14625debe07a27449fc20506dbf8b1d4f877
2c9c7c442fc314cf2215c2367b9407195dcb5d62c133cfcca66256ac8f9c779c
1de425cf303205b49b79189925ed4bd8a0cea94c9fdbeaf6698ab52c47461d35
0093cce0fa9a52d6ecde470a19f5d3f91d15a93013ed4179a3a39df5a024e45e

fd8b025b1e9e7a1ad38d74c15c7aeeab2445596ae7a47b12cdb3988dc43a1676
0d5ec1aa0f3989aabd8dee83b6290c6d570a98f7b124c3cb0d54488a9e70bf70
1d02017bfe23da76e2396d33a37ac28ad77b9cd357508777f6c28400505d7eaa
369a6ea6b33a8f2a6ace9a060ed8cad3e9abb935b31cf0fd0db7f1f31c55c909
24beb0f91992ed857b814bf466aa44bbea5354a1410b9750a243f1fd709c202d
8b47d734a82ad4a3742a81e7e68d5e8cf90a6f6d41fa87fc10609951957e6940
36e47266347336338ce36d653168485f6d06b8bbcf601d4fd8c05fcb6276eefb
a2f47cdac813535fc68f86d9a89f78d75e8d382dc30a0e73cd640fac27048dc0
884e597d265aedc58e2551e36b669835adb57ca1463e87a73c27742111b907b4
a53b87210d1439220442375569e527b6b0709481f2a0a0ba3509a6bf1aab625a
230b72cf8d87fbc84eb7cdf703033d1271703f35dc6ddd22d00211f996c35a75
069f49425c8705b27cf4dbc68d574461ab934e8cdaf0b3a7cd0aed38e6b01303
efe9d0bd30f865ac896bbb8174c679246afed339a81a787fbe3a2d6426667ce3
5661e7815e62ba78de6738c1b4b79b6edb9b07eddc64604ced96dae633258bd8
f7f6413d17c431ff97bd905be0465a91971f2fc1aa3a838939ac4b5b0df154dd
18cbf55d11b6bd092def3b82dcb2b767a16338204cdb8cfda284f65866ada347
36690591b58f66e1bb9f0694c708b70c2dad7a32e676768908f7e2a67e612aa8
db5e1fbd256786afa9ce03e98cacf137cff43f27b388ec0881928df1a97af050
e06e49aae02c014f1fb14aecf0d638a5c70c73a47a2109403cb8b7ce486526b1
11e7a8eb1e5e57a242f1c4a0950ad94fe356838a8c5b02567ddebdc2071b327d
7ade94921173352ebd89b9599d6c0c05eeb6205c40bf0d8c916a455f9c9c58f20
ad00798e0ad77199ce218de0b0f3a8c5c32bea8324341e02f607bdbaa24f9520
83d0c84b1ac57380bc6992f3a5687a9c688ef423b411b122e3561e026342d596
586434284288010 29d43e429ee1f9754066d275b14fa7e8144f2b52bc8db3c5a
4e8b8ab73d2ef4060146268b69e192a735b89f5a58d593ab00ebdfe656205384
3c446e5cdc68adc5b07d48b3f449ea44feb37490a68139c9d92aea4a1f33777c
816a100e89c3a948bdafcf2ea3b7b8d5e839d54a5adf06c594dbe803fa431f36

2f52b7450f0bb16607878e79758479273766b52db146a38e5f800d88a6157d2a
b7dc343b87dff3fc016811ff8be5156a3576b47b50247ffe5b3173f525543556
441992a0e3d0d0760fe9b0268c079d8bab84ae1310863e92e8983cb1861fb90c
858345b5ab03236a9e738d5a5dabd13a208927229aeb97879ab319f023e0d454
9e4290a850ab68b1036851556a7bd53f8e5855d2aea3dd47d6d28c6dc05d4adb
91b78766844f0771dfad52819e991065c1a248245df0b20c75cdf69ca9cf31be
e42f81262acfdb9a84505deb422a6a7aa799ac017a6619b64bb17a59cf031f85
b8c9a7353f463e93b30d3f5c55628c182580cd982a1901734d8e4ce3c5bcdfd3
89123cd09aa8f99b189da32e3a11268934b95686708a4f74447cb3aaec56892f
43693c3d9a5e83df26d4b4a2baffba5c3ca6c472d5dbc6545b7e299b0e103ff7
be6541dfa193bb7ce04c323da76d7bf52e3ecb3c8e099d3adb9bbeeee119534d
9245d75a27ca65985cdeb27a122ee4989e4e0c9a020bb41f865dfec512b9d81d
bdc0c2040212acde13429e2d329949abe4f2edea24ef9e765616f8b2821e2d76
090e3a1be2b3124e46b65d2593c08d0b45a6660c7f809b238f41aded734d335d
c77016e4f94ae81f5a3cc702b46e32f029d5ffe36a7a10eab7356868ec516085
d997db37507103e19aa2efc0d28c5bbb46ab825828ae756b15b5d39a9adae2f2
c663f0715d083a76d5a13a71e90d3e42a60981055bef4b97da84b1d041f334f5

If you are currently impacted by a cyber incident, or are seeking guidance, please [contact us](#) or call our 24/7 hotline +1-877-686-86

This blog post and any information or recommendation contained herein has been prepared for general informational purposes and is not intended to be used as a substitute for professional consultation on facts and circumstances specific to any entity. While we have made attempts to ensure the information contained herein has been obtained from reliable sources and to perform rigorous analysis, this advisory is based on initial rapid study, and needs to be treated accordingly. Sygnia is not responsible for any errors or omissions, or for the results obtained from the use of this blog post. This blog post is provided on an as-is basis, and without warranties of any kind.
