

Перечни идентификаторов компрометации

Приложение 1, пункт № 7.

Файловые индикаторы компрометации группировки Core Werewolf
179831492da2ed8d9771e5a1fce4615deb0618d6977bd2a5953ebe67352df890
3bb64031a9f2be48b427fa143e0b3f7f12f032470f0d3a8e433692c43642e966
560404f3b5ffc52db8260b29dc3716e510261191f0a68152729c0387c376919b
0c57fd5cf0496f8b5f480202cc9f4c2b1eed1f787cba93035d1773d100737039
d14128508ec90b1a0f5c973a403b7b62cd4122ab92dfdcf74b893fffe1ddc1c6
081c65e07fe4958078ba7b09050fdb3fb8cbd1d59c91bd5d8147057c4c21c1b5
c34fc3a3020d9f7528b5fc48a676eed02e43792b666f3d3f71f22238042dc84e
c868049d2cce5a00a0e7a72620d9e77e289a394fc7e8def67508273f1c614240
6af1ff57b4034f6bc2c9015dfb6a43d9a709a4f61d6d337f53b4ac8ced1054b2
be14454c2d4982f72bf8b2944083186efeb848a6ff1eb4abda33e76edde48795
f39f0bcd24f90ac0db8e4cdc82c789ec4c65b0fee4133d1e6fbdee60451b8505
b494a48427ed3f410c485fa68aa8aa4df86276718bf062cdc16976c945207e3e
1ae5b8e4ba349292edf062d4173d8ebf25701b7b540eb2509b165fd219a0d4e7
e89edcddff86c204817124c865cf1f37b6bc5ab6a6a3b4ed2431e92d917fa141
a023753f743666d9e88d0a9135825ba4dd2f517e71adf81ec737eb51854d148c
49405126b9734d1784a0f4a49f3ddc28b5945c53e1079f83cc026de6f107c8b1
864f3bc5fc80ebb58c69f7715875742a0d7746ff4cef79d4031f061262e46fd1
2b5da54a8a94dd15dd7a5d53bf17d8df7856154fc9b20160867efe29a7c0501a
b49e9759e529158aff7d81081f0f5242bc741873fb0fe414b475c4b6c83360ee
5f225c7f9f81d78b2ee45ec1eeb305d009631748bb2537b3376d7cd3390ad811
b05e25dc7da1139d8731ca282572799168666708f8eb7201edd38999ea3db0b2
7a83edb3e23511910aff571be07e013d67ede6da439ff5907946fc2b455bc132
a704d37bd6c45d5cda547d1702dbc34235c59a33c4038e8b4cfa8e13da058ce7
c07f1bdbfb12f5e9f5f3a748f75b93a0a0a617d0289da80ee428ce1edf5c8d16

Приложение 1, пункт № 16.

Файловые индикаторы компрометации группировки PhantomCore
204544fc8a8cac64bb07825a7bd58c54cb3e605707e2d72206ac23a1657bfe1e
be14fc604c840c3aff9542106c73ed247417de5a56b1e9b2843e7947f0722d9
b701272e20db5e485fe8b4f480ed05bcdba88c386d44dc4a17fe9a7b6b9c026b

2611121e4100b60e8644211bdc831144ba8b772d4d40e616864e7a723a9d7bf8
a2be4d9fdb560a4706ff8c4b32f092ef476f203c96e1b4afaf391cfe82aa533
9f9acdd833f3fd7b8bf987a8cc17e9456546fdbcbfe80c3b0dfc57c6f62d3e4b
c3d05d7d6e1c50c6bd493fd5613c3204e6beadf8b6e4915cdf2f899fabf86a4e
ad0e3a42120602534512ac4a4415a9fb867f0ecc71b6d341c2ebded7a52e0afe
2d79ea29838f1c35648658bbb6e48573630c15a113cd16f045fcf5a310411cab
b350beb7f069da939aec1eef6fd428fcbc0e17edac983dc87e67716d83a04822
d7d6894c2fbce3d91af8de50e7cd649f12627d94a1a9b430f6e583714d48be29
06ae2986402f0cb9ca03e4b1d9d09430d32aacdda8b016d3e6801bef3fb1f8b4

Сетевые индикаторы компрометации группировки PhantomCore	
193[.]187[.]174[.]3	softline-solutions[.]cloud
194[.]116[.]215[.]166	mgfoms[.]org
193[.]187[.]174[.]251	195[.]133[.]32[.]213
194[.]87[.]253[.]233	185[.]130[.]251[.]227
213[.]232[.]204[.]110	185[.]130[.]251[.]219
194[.]116[.]215[.]36	88[.]66[.]89[.]231
46[.]8[.]71[.]104	91[.]219[.]151[.]103
217[.]19[.]4[.]206	91[.]219[.]151[.]59
91[.]239[.]148[.]211	45[.]8[.]228[.]253
austolns[.]pw	185[.]130[.]249[.]224
nextcloud[.]1cbit[.]dev	188[.]127[.]254[.]234
nextcloud[.]trust-sec[.]it[.]com	famesborka[.]ru
meet[.]jibs[.]events	aezis[.]ru
browser[.]anaiytics[.]org	aventrix[.]ru
91[.]239[.]148[.]213	hostmc[.]ru
voen-pravoru[.]online	examplehost[.]ru
voen-pravo[.]online	loot-craft[.]ru
bi-zone[.]com	ркнс[.]рф
дискусс[.]рф	кино-музыка[.]рф
fame-nodes[.]ru	

Приложение 1, пункт № 17.

Файловые индикаторы компрометации группировки Vengeful Wolf
e7dfada954ec732cf88344423e36bceccce308973468ce906da1125758575559

1c55b62e82660c8fad236d6e6b6bcbcbce951ab424de7d9520a1180410d6d44d1
820f00b535de46f740c19ce9277dce1a27f294ea21e38d5c6c9c369ea51b0a8d
3afad44323a9069914ee1afc2e2fd96e8998f0b4a4e19f5076fb9ed5875cf5fa
164434831e0348c4fce1f3f27773efa95a249761eff02601224e683df89b2fc7
e3c9e82aa3dcc3d7e1c25531b3277460b2a9af5532e1fd2708a0e56f43139f66
abfa7aa4cb5e85a8275f2849c9baafc9c380eb00faf411301424b5807abb36f6
523b41549932d25a131f440863449c6d2256ca868c870c377becb1296e17533a
73d1006cd55a96396a41d8ccc8926cd27fc1ce140c29ef9036ceb44cdfb2f4c3
6c43a47bdfd70ee42943cf572b2b0cb953f3948b9f6a5fb8cac55d3daa76bb1e
f13ddf02ca28ed39172bd0047aaf641a379e20d5f40669b05be535f2ebbaab2
7b9a54d7856621de7f1c550ff5675d454bed713a79719ea929e3dc8ff0b96658
bef398e2903fa45dd6721d1b016c1456c75b3729c0275b2294efc4eb81026821
b2dfe15daa65106af2e3e7b7eaa9b1babf1b095c1745bd8ac42fb31d2bd2ccaa
95958e209e0328fdc090fa65b8490f10adb9b44adb3fa08c4f67d7d726cd03cb
c83f97e3b327506505379c80fa3b3621c2e3a61d8a24aeaeb4808b7da324f34a
d32a410f784daaeed1d50c5d4c40a40e12cdb6383223d3e060391d6f73d7cd3c
cae01f57ed2155e68fbe5af932c8982cfaf693c7e4c4f421d5e061fb37018944
a1247fae33a32ffe3ec82cc4b6e2a8d07cdf21c02b7ac50f5d6487f4c5fcf5bd
7dd33e93c3f4d7cfad237c011377acd09a1167b1dc07149247a2fb44f3b9505e
cb7d92f712b39d1ff585c93d261a81e4f1a72b193c4fd73c7125ff5768ee2a26
eddd8965ff9765ad47e9b53d9cc12b9131eb78d12a95207c253d0d37f47fe2fa
2c4477ed78f3948a3a7f3bc11a799229b69af40837d2208f0262707f8a5ad458
58040680d1f78d12f5e3bc9c506895d03e5334a3b34299e9cad519f2e17ce84c
75ece8dd79354984ec6f57b446909636f40749d9cad2c140728e8c2689de8bf2
a1268842f616a2dbaf4afde5117c4bd8a0a13a98edbf1cc22b7f47f247f8aea0
e4ecc60934ddb82610e3e0148b0141406429b38a748c46ce7b4602329e44fdf1
a8e9c2fff2a9d3bea97da76e21263b52e4ea9ed4376735149a8cb2c31ed39d53
02703a8b263b7ba4dfb406536292240156d7f21df3f3f74f21cc7b841a9ca7e4
c6b1e9418b5c09a218d58abea2e94aadf94b65160553b8b771cd5472aade348d

Приложение 1, пункт № 19.

Файловые индикаторы компрометации группировки Fairy Wolf
1a229333815b46379fd859d26859e553d01057d8e3667ee5eb3b05ec9af29c69
ad49d30d5532e59e9256a08c68dcc4f74544d58e2a921094c8fb22aaf696c691
d74cd14654577857c71d501bc5281bc2e76b18e618c6ec6d01586db2d5ac802e

127c63ebc156b996b121314eefec162d640a31a68cc5078500db4cad5b7eae9f
f4ba7569314ccc25068861f485c2b2f0401bba8621a487548c963b6aa975a360
bbb792bd39a2ba1de110c47f226e9260a8272521f8b26d1cefb38bc5297698a1
10f686ed2993b1881474f8416183b0bc8c5f066100a64448f6457300123c4373
6a824920a39c1e4d8dc4be4270ab5541709c103b2cd72d7b1e87bfea9279a368
e696c6944325110566057848d3c4f5d9056f8c25527ef2659eb3cd840a456401
467c4c63e4459c760b65186a32fec68411b1260934b6aa99016d680efd7bd68f
1aac1cf911d448ceb544b2355ffa55418e2956bd3710eafb6d68faec0f65ce4c
50a7b67e0c8dd5b4500f7e67c9dfd90e77e59560db2ed1d8ab20473c0884921d
827135782280900cc8ab07ac39789b3c3eff340af298a67bc5ba951fb2e49cfe
d9d192aa40a7db3dee0c064704543c801a4b9d0e17223fbe340d6528153a8e84
3a6304c5a55ef36fbcca3ab3b0a940cc4b3736cf172d2ce142382478f4d9cccf
e5be7ead80197c011c22730a985493a919a973f18fb12fe6c1bf9132facdf31c
116e8d46dbf3f021ce429f897e16e5cfc1686603b0a2095eba74be3398a66baf
ef81f7a7f4deba2b078a3d5cf4a08dae552d8227bda498ac86bd6617993fc32a
16af3167253dd9bbc9754d56004cf17b345f9181a444b7232db38f5171215561
5babf7a1e33ac06be481aff03491841cdef62538c5e3a497fadf8d61088d9306
c557d92fc2d3d3ec47e480cc2aba8ba7932cdcf1f4f1644c018f77a7dd375cb5
f98ddec5a0fd86c9a9f33c50a0fe07eec1030446ec15ef2d6dcf5be0135cd8a5
238a1bbf67bd797c21a0402cd740b3bf88a3aa70aaf3ff8179ee2d3dc9ee02c0
fa7e5004cb7d7b9d255044780a1bf655ccc52878f07d98cfe56b454aa25c4078
03c2d8441e999ec298990d9375dc0ab48f082033accb44b18d0739f14d01ba9e
5381e7787bec221bf35ba5f4c95e8841ac0f129d6eef36c1edc7969e918cb3dd
7c0c1edf27d02651dfd762875c20050c0069a8d4530e8d8dcdf55bad93d1dff
9e1b920d1b1feaf91ef7a116204560b1f5acea1e40dc72efaca82caaf61d6dda
1acf58d1507f1802deab65a06e4e05019c06c2d70b637c67b7b624cb3a527ba0
689e947ac0d54aae159253ac184693acd9f3cae5fe5f5c59c57e744b964d155e
407c02e7b83fd9d9bf9a35dcef415ddca670136d658a56348509a744930cf88c

Приложение 1, пункт № 21.

Файловые индикаторы компрометации группировки Scaly Wolf
b463f775a28e134615984d58f774c80575f002af
26df8e86faa6ee9c19a22b9ac35dd08983e794af
d7bfa3b87e6458c8e3a901779ac76adaca0cc0ce
602751b9f1cd94813163fcfe3cab64c7d2a3a64c

2eeb94fd24b66284f5e2f19ec6b284255d1a4c0d
a9d356b851ca2942925d937e02f6a7b09881b6c9
bb9d5c2d31ca7711a5e1c87d429dc495f9fc45db
e517577a8e2166335fa1b640578fd8a1cb353c6d
08e2edeea11515c5c83a9d14d723d29939549978
856225319df6fbb1ff3ea2b9e418a83fbec300d9
65ffe173a0f48711531c1cc8155d32c55569facb
e324c7490dc287168c2de66021f02e7d999d8538
98f90f98efa163f2d79877284d30947d7c079b43
27daaa589d76c8e6a7190d63cfc6daea4281ee4b
f49fa6e6bef00cd00bc31fcf4f019fdf82c28fd3
64ee90631ecf47d5d0f1916007f96069083292cc
b385e11c70b81ddcd594ac0929fb7882a8354af3
9e1486417007f84cb76999ec95231362a7daf840
7e4add7c7135fc091a4ae2452e5683ad4f883e86
e0800e803c00db69a06caa68d5889fccc8080772
5e9934c1ed5da62dc7d05e5c2a9d364dbb06d3a6
1041f2df7770456e3759a86f7db3cd9b29fb6a39
23873bf2670cf64c2440058130548d4e4da412dd
903283f46df39c46d3be506fd99fdf61b6f0edeb
535374b9391410798ee9490eade689996809bc12
26df8e86faa6ee9c19a22b9ac35dd08983e794af
dc6ba17b27e6611489c5c52f8956bc5a45001ecd
d58d987989d1f44effb4bb29d06efb1c51f66718
7902b08fb184cfb9580d0ad950baf048a795f7c1
462653d8b96c6ee9cca5c09b2955588e5af40256

Приложение 1, пункт № 22.

Файловые индикаторы компрометации группировки Kinsing
e8c818d9e76e5512ba49cbf79a0e2c7f752d589000eac13bfd32e1bd5eaf48d9
90c52a8ef785980bf062cd2be0c47839d12c7e5e3318a49ca4dc5e13d0f88846
21c20cf2f55e0f7010bc0e051889aee75cf94ae69f1e6a206104a213500f4b5c
a5af590ef864daaf11433acfde9be087104d6237fbd0295858ccc1a3d5f18de0
63c5ff40ead3b6df9e484c938c9b950aa1a3851f7f0b906c9b4d4ec17446b04e
b01cc74a00761368bc3a2eec09d2671bd4e02b00bb561e50db042fa566ee7422

fa8a54ad772c873ebcf76991dde17a82f15dae0f3b65ab08076d254905244c2d
a89c0d506ecf6fabee7d54c09ae1060c0e6aacd3ec6a2fd91f36b783153d81d3
022c0880c46be81727cc416d28bccaa0f84779ec5369d4dfaf4c326e819a1a70
440723f366a04802a937c49dcfbdc6f5bc969fb23484472acb708b2a8f25d064
1fd5654dbf2edd837784fc9e7b0f16164aaab53d865f23385be8e9b67d9a8cf1
b19e8c9e342903dac2cd8dbf455f9fe3c63cf5ce1489e7be42c6e18987186810
71414a7620a8dab16303c5ba6f1a36e58044fd685ca0c61662e1103f72a89667
e463089b25fe4363aa46175f38b75138581965375f4f20286c6af07f271e2688
8ed7c2ccd28262c167af60d45c5449b2bc0eee8be07e4b108eddf3f9f17f396f
d02143bda84c0123a04d2233dece27d9d471fc5ee30c8d4d462ccf8a48113161
51e8e098f4a6cc0a096df3b866a864cc69a569ed038baa52268e7383b4339c53
7c7d085218de6852ed24cff9866b28e26aef2b13ec25efade84637162df27366
da26d18dcd30bee1612f054bcb98efeecfd6f955351c31e84872b2df0de98d16
f03ee1963cbe167e44759ecd86efc744faf850eaec8a14d67548f7874d51ef63
37922be1425b5cebf920960dfe3652a2b7abb222672f1069106278299aea36b7
7d31843ce5231c95ce07a609cb4473fe53b95a8d0685df9d666de348d17c69ff
0bc4c52d010076f71e1a6eae8b8731952167a00cedc88e3e1da369181df80c88
267c844d1ec54c8ff892596277681bed888de9edf815d3b070ce7d46c173d652
4c3a074d0729aee87bb9141598402e8690ec35db40c90134570e016edb16a90
3a67df40721703c455c6364ff6da6af4a6df95d0b7bff1a7cebd45cc3f5d1f0
882b29ce61b9b17830a40a079fc569eee6e1bc5061c7f013e618f9aae6da41bb
38058a01b9a8c9b077465fed1bb2c38c33624996ed6a1b6121e31ed3a88b5d20
4208ff01c5b0da8e4b392853fa048841625404e7f331c9e1e0d2bdd578b6b1ec
e150e490c1bd6a6a6b2a9c82388962d8af25e9923d98eb4cd049de2d0c168bcd
4ec925abc87c45e54dca0a1e7edc7b233046be70620de58d93fe964a1357cc8c
9d2761bf8f7d4305b3af26d319d73ef35d1147fdfd025d1954e35ef386738d46
54db0ca2882fb8767b4ebdf404d423ccb14a2c369e890151a556ab53711dec2
9c1cb1513cd7cb50490763d9f92bd94e6d924df2a8b1248beb9726888f105465
37616e57c1c7a1f8c3703f7be0d2cb4a18bc96cdb32e50ba968ca036fbd8960f
16149a469432f90f78552affc874f832f3ad2fd9c59c17a63f3cf8cac745fd95
5a2a5e79bd0f86fa63114686547c2319f691827e5f05efb477a953d9c94e771a
3c30b31be9db6ce3fd4bd8bf342163943ca6b3dbbb03e4db18cc1011762ad5ca
28fd24867741710caae692f5faa388d503552783f07311ee8e7c2b42a0192ab3
787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c
322bc93e3209b4977141b501243c8437ae16a012d92e25e21d1eae8fda50d93e
4b95ecbf4a30930d89cb99c68e4e39f4e81b0b391223320bc4931b83e41069d1

27e07e76c18ee92a126abb22ea3c84a2f07ce184225221316ade8ce8ac4ed208
c831727f5efb73f530aaf0464d4a2e9dd3caa410097bc4fec91da2adc270b8d3
0959139a7a2ee4f024f8007ffbb60f9e35144cc266f462187c4bcd62d2339f9e
64f896d772f370692beeac2cb23ddb7c0c11ce1643f6f1d9f17eaea87f1ebaa9
5d4613a22c0e1c6d10de75e0a97c49487c0fd97a11ae46cfd514b60f0e612456
e68b44764638b2e7266f383c5f3541623778cda75418f6efd57f563fc850062e
b64a947b1eb22cec61a17ce16fae8fc27566df058bcf4e8453bb2cd47eabe75f
5e5b5171a95955ecb0fa8f9f1ba66f313165044cc1978a447673c0ac17859170
3be11178aeb8b6da8a53da8a9cf02f8866f97771fea4871e1a2fa8d06b482f08
868c7743ec1666c4386da439406dd1f5c54323bde57690659de3f44735df1988
c0acade112fbda25dbbc1d3b2acf5fd64fededb9672feb9013ab5664c00c7081
8fb3f050841ae082f0d120c45f677181c4a8841e5c85e64a34cf11ec97cefdb6
1d6356a43d59e2e557fdca7054235c17c4f5fadedf9c8998c9d5e7002fa22076d
c339b89b57cb8f74cc34053f984bcc5a14f46dff6a5df4f78459d841f6ec7d9e
3263612fad0b6d943b23970109a8ed60e38ba3163f870049cd53ff21936336e4
a62408b8595d5f96286588c3aab65aba8dff47e8f5a71f520d1af1f1a8645e07
787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c
f913e0c9afa4f840dcec88b81dda5f613b154cefd027036bbe9c10f2266c30aa
65f3faf634654ea8dc3e0c473608e8430a629d8d033820662b43888254ded79b
fc5370dafe589e64d45fa8da975e000ee1df5163a0b1804e24c97197c9b3351f
0d78e14411ac375c511dbeddba6b97c4d6c72d46d7d99087348747826be5b5bf
42ea3a6c73b96e3b284488b6dfb46ea07ede2f5aecdd5da48f5288b027cb7b1f
2559246194b9d5092e9c2e3e8f21b4ac355b78038e68c86f3ca156f702ba3def
95152724c66710bc28dc907f74dd84c17c9fd259696714c88427b7442db10eb1
e3d66d633cfa384a50c234f197c82f3bcdabd22c1a3c5cfb755e025fe0f8007ba
5104d5e2aad414874cdc20767302a8267b5bcd93b071dcf3e0f05dea7d4c8abc
c38c21120d8c17688f9aeb2af5bdafeb6b75e1d2673b025b720e50232f888808a
7d349b7f39c93d181969f3cf91fb6a2097a51949489272225851d8f01dac7e12
b1d79b505f5410acf6f439adc3a98c6ba6bfc3a6b1423f6b0785399bb4355b54
887f53a95bb2b545d056921bfda7aeb0779373e54b73c1e2639f6ace8f1855a8
84fe109fca8ae9b363d18871465c161a2c19412728ef7ad488c85dc6cfff12d2
f1af867269130c3e2325f8bb03afd68b516b605f4172fbf58fa69e904f98b56a
db107e4c590fd0e2e1377b0e245687c14cca0032d6e561841bf3f5978d5d541d
1fd7144a5acffd234271c4c26d365c8460f3c028cab5cdf66ce3810eaf72f567
3c331f25f3ed7661501ea2ba906edcef8de9d7a7ba0b4007b3ed3a92763f85a2
645ceab4d47fcc64a388127327a9afefd36087a3e3037dc5d29c651f212c1d51

4c0514858b9a464aa2f95482269b7006f7b0cc7f9ff058d80db19c234595ff55
20c37f6829c8863f69d430d39b359470b5b90051f67decf98136da59233623f2
394754a0befed11d229df72cbbb310f3a343ac17e08b7983753832378095c95b
a6e41cc8f7238b02699c823c4364355573fdefadc1e734102c9346b5d9b5ef65
fec30cd7802f8ac4137a2d0659b3052411a99d809a5aefb48f8b821905100f3
5a168e046df1b068f9e1d88d3d98ba00a465801f40a544c67f7464e6cabd4a96
30f020bc7ce456f4d8b798f33375c9c2e8fd4ec9611c04699e2333bdc376eaea
1033629253cc27a1d00f9cbb995e0deeee316ff20e14489c7b38db97eb4880f2
9dab7540a8cbfc786d5321e6c23d5f17edfd4f6c738cfaac1c08439dab3a4efd
72ac9bbf0aa818e2894730d3d3659aaf08489b607a7308192382cc9d382f4dd4
6d28e919edc5a2dd69984d14c42d823efaf3113e6d7295926780474d0a152e26
d8947f46271d1340a1a45ad762031eefce5fce6d2136fbdcd7085db49de1c671

Приложение 1, пункт № 30.

Файловые индикаторы компрометации группировки Rare Werewolf
5eb18f34aae8b30636354ccd918cd9a46d0f3892a5789bfb0e9f59194c89c871
eeb6b7f8c7261fd9af6800e73cefa7e899e30f3c0032404fb491532c10fe23d2
90f306a7cd4c7592e8cc166f8d000626521596809202fd59c6676c4077b2f337
cae68a67643e0bd6071801da20ac0a6829809c2280ecd4d857a7f955c495860a
45c2943257af1c0405e7cd20e89d8a3ef229245ad09590f0399b04e5bf9be0ea
a52d98af7750acf1a39d53ca4cafca86fb07b21fb742fbee2631b722f414bea3
b9dad201d2968a2caab63d61a05a27aebea5f95bbcd6f3150c14cbf36ebb50b0
45ae020d691e5ba5ce298585de50244265c639f015d5bccb487b9d29256976b
669ac00e67084f942dabff393a7eff09d802c72b30d971ab425c6ddf342783ac
5a45cf3531d629909a743701e7e2ce8315a18be42ddf0b79ec2882bc890782b6
89a6726b31656e3802195559a8762543a8e1cebf58eba0ca18a8fd869e597f94
104c3c8e21e2a69d9033733b0ee4f6fc152a743e3d5de3e51f1d79b44f75e763
90f36fb496261f56834391cd80eb083cd33fa670bd03dfd5b6b6404254936ef2
11fb60f7a8ba3fd1912472f8a19cc31b34b308fe8a9ebcc48275b0be936e66ca
f02ee80ac7ba76abb105c848134a13e9b5ce91a7779e4d3e77670d0b3b54dfcb
06ae798542f9abb6220ab8fe1c17b7fd5a76d23fc38ba01b0045e7b70ef09c74
45540346c5f1492f3d599dd5673e8f0d8646e4e3b0b8bfff4c041cd00e3b0b9d
5afdedbf0341806eab7d99a5187a35279f6edf5503835512b0f82607b5b79dd6
c2c8e4e10e1440840068027baa346db0bc47c055b89aac9806d04280a60fc360
27d354920763483794629000581e12a6ade3a6f682ec4a31295adde0f507df2b

b3cdec85b122e5ef7cb39a50203b822ebb28d1d6a7e1545f492e33c5e6ebf440
84974cda62f4c1823d08aace5675459fa974007cc273fcef8c90d50dc0f46f11
c65faa010cde93e484e8d61ed2046d8203cb4150909a198d6d6d163884faa5ef

Приложение 1, пункт № 31.

Сетевые индикаторы компрометации группировки Rainbow Hyena	
185[.]130[.]251[.]116	91[.]239[.]148[.]21
185[.]225[.]17[.]104	95[.]182[.]115[.]170
185[.]255[.]133[.]195	hxxp[:]//217[.]19[.]4[.]195/poll
217[.]19[.]4[.]195	hxxp[:]//31[.]56[.]206[.]116/poll
31[.]56[.]206[.]116	hxxp[:]//31[.]57[.]62[.]30/poll
31[.]57[.]61[.]137	hxxp[:]//31[.]58[.]171[.]246/poll
31[.]57[.]62[.]30	hxxp[:]//31[.]59[.]41[.]149/poll
31[.]58[.]171[.]246	hxxp[:]//5[.]178[.]96[.]82/poll
31[.]59[.]41[.]149	hxxp[:]//91[.]108[.]189[.]139/poll
5[.]178[.]96[.]82	hxxp[:]//95[.]182[.]115[.]170/poll
91[.]108[.]189[.]139	

Файловые индикаторы компрометации группировки Rainbow Hyena
f7451e6b2d95d0fb325a3fc25e1b23a71dc7b35617ed64ea554df18fba023aa6
2c2b1bb9f65e1a75b70f2ea007573813e45e903b94b02bf4d0a18c1b8f465aca
58d49f8e12b9281206e0aed32808243cd728e860dc8f3e730abf287d2cdeab9f
b9579e65e5499be393cf182496103941a006479ff8b41c0ad3b57b1d678d9794
d585aa73d28af621abcef44ae024fde62366c29f5730a3cb31ff3c8bb5eb84a8
66dd68177a5b31159579cfcab558771097d753a17b63c1cbf4dad2f5c4f0e2e
1aa6076dd5ec53acc130b1a55e05b811c533ef7e0e14228ab651d2820296c1c8
bd6fd49e87823122a55821238cf183c98894134e4329d3ac772f9729a27d72ae
8aad3e5f41d0c62c36abcc28532bdd23c709e324c10716672fdda848ff01f0ff
7726288c836dd39037e6424c0f0d7e5170bc9f7d46afbca10e67b1e66f09e5c2
068d8e7a5d2eaa94b4142b7a65f32d2e1cb168a6a8a574428a35880980940e15
3d9d1376f2d2b4a284697eba5eccb9f1537af15621a7fc8cb439fc0c69a61971
774cc8c02425bb6c59b9a18120ae1819530cbda684e4662a176eacd6e8bd2401
eafb92088a266014dfdec3eb58519aa24c18ff445b868bea0e17ddec05dfefef
60207e83e8065962764441bdfedf62150b7cf8fc6434965ac22d3aaad8fee67b
c68d1b3dca1e5b1b04d7b5bae63238606fe81bddae8ee6ff8fb04381fe3c5a83

6f8e5a239ff3b7eafee1354ab7d43b65d2d72c1fb2ad95666ee0ff1dac4d3f3e
9d10b1e7ef6bfa76da5959f1ad750b3fa765cff645bb3e72d29ef711313699a8
75e95bfec6d38b80315d32116a4c157b408464e73e4df66125f69ed1381ccf30
3fb7f5b2504386eab868c6c4001e08787f13f3d915d1f25876c9192266a67549
d9eadcbab4703094481ef388f4f639223d66ffa42ebd4da1037aa79b5bf87c4a
fbde1d8fdb5f66fc6e61e2fe6896bcffffeaf6ae68b8c7d19f1078c76ba41af
5736b3f21666968e388c1e49da42a1fcbbd6a3b5c8f0cbfe5be486208b396957
ea54123d430337271f7b6e03aea653af817cea20a64faaa082f44ca2b01c2db
ebef31df330554290f519db3f16bb4efb326f2c9d6b93601ea3c67d2374f3a7a
8f4a3e22d0c988ee8574392533da8b9256f79c87770820e1ec530d3b9dbd9fcd
d6b3645c750d1dde284c1b88011f4b89f4987dc2a248c2ccd54a8516f75616c3
4619cef20c15d0fdee44fabaccf93916f53a02971d5c87cfd30faabfff57309e
5540f27f12db5a9e954727079665a282f905a0be787b76d798ca79a318d197f5
d42d16e11947a1ed548fd2f23b4d9226d3282badecf8f254e4da747a8659a60d
c97f7a2f09b5f17d1c1ced5eed68946dc8d4a7a2b3116a806ab29e29717c16b9
9b2866063b0f5e2e72cbc60fb5b0b267f03b1e0f47ef71a10c2df63b1b5c67da
7da87f51e939400c473b77945f0f1e8950847aeabf2becc76b0fbe26e46ed7a4
2d886a2f0f5e96346a560af06654b9b04d1755e683ce6397ee5b46f183fb4996
ccaee012d7dded1e58f8d8c20e0a26f7cd16d337539e131e238fc2b2e77a2d04
a5b7af0b5faafecf3b9ed135d728c726c652deed5dd8ac72148536c488378a1
b478664d0bb1dd1bea7b30136be4cb4e7ca1da6c1eca55817b557b9e4c5097ec
2a0d5c3a17e5c7fee3d7a798dcc2d3d81688a05092d709b177afddcdf0096db5
fb2c943ba8babb5ec0c210093acebbbe642fb83a4a09fa0fe427acb599ef13d
e21c4b8a7fd4673410f395acc0963a80064ee9831a600dbed469a7e02123ffad
9880988bfff19825504313eca505b0a4192bfb757a4a4dbe33ab40543cfed8b64
c504d1a6ce6b08488f2f8d07f6f397d8ee14df00982be7c6e2d6e28111018630
c3985a240abd9a0a59ba51aab48f6263ba92c2450cba2537513c55f2fb942523
e5406942ce12debae0f6720e5dc4dcb2c80b032fb8ed260d313af3c695336318
5265332860d0c81a5687f75d836441e5e1f45eb98e6dea6e3d8830d70c97783a

Приложение 1, пункт № 32.

Сетевые индикаторы компрометации группировки Paper Werewolf (Goffee)	
impact-dns[.]ru	it-enterprise[.]cloud
minpromtorg[.]msk[.]ru	sajjooapnindazoa[.]com
minprontorg-gov[.]ru	sopranosolutions[.]com

auntastic[.]com	kranzlerbar[.]com
winetwist[.]org	81[.]30[.]105[.]154
studiomisery[.]org	109[.]107[.]189[.]187
forbidfashion[.]org	109[.]107[.]189[.]187
crystalarticles[.]org	193[.]124[.]44[.]63
get[.]astrarepository[.]com	195[.]19[.]93[.]162
vks[.]bft-holding[.]com	mtls[:]/167[.]235[.]239[.]144
possessionpower[.]org	hxxps[:]/possessionpower[.]org/photographing /insinuating/predisposing/insolent/envious
regrety[.]com	hxxps[:]/regrety[.]com/perplexed/blanket/cary atids/enthused/microlight
votexrp[.]com	hxxps[:]/votexrp[.]com/glossed/complainingly /blank/looks/adjudge
brothiz[.]com	hxxps[:]/brothiz[.]com/counties/indicating/foo tball/compress/bards
axenixservices[.]com	mtls[:]/188[.]246[.]166[.]157
archive-linux[.]com	mtls[:]/194[.]28[.]29[.]122
pestctlsvc[.]host	hxxps[:]/cloud[.]mvd[.]spb[.]ru/8u43sj/

Файловые индикаторы компрометации группировки Paper Werewolf (Goffee)
b9ebe61825b8e93e55ac792a0947551692b4e5008f9a5b7cc3378b2892bfd836
e7dfa9f6835bf1695e8e2e1879e8c4026d0bce1102462265d5acc0cbf8476e94
b7bbeba45137ab6c136c3b268d3addc1dda4009b207f8d922c65c4b136058083
1a06af232aea96634ad1437bd9ce4ea8a17e2f7f9f570e1aab7134024e407871
34874abe99d6e47084615c4f012a467920312b2353e338722f771110a9c1a5f8
c848ab632ede81b53e681a4bf466b31fb3ac509e754d72a18fe373d2476d71ca
ee128761eb65438a786981b141d7751a17ab88bf2fa4c4fa7158944a906f57e7
4c1e81840685e1fd5cf8b3efd576858d376cb83db6e49332b8785bd8483b6a89
b729686b11fb32055492312b32eb968bc4c231a4bbbd51abc7dc6a5f45f63b41
2c5da865cddf35a0143ddf77b0679e7e234a2a7eba2abeaa24a41ab6cafc60b2
700bfc68c40c3ed1cf43527efc32a0f08ccc759cf94fb292b23c2d2e9b542f77
55aa6fb21c9a93222e028bf4171b303fdd1af371d1dd33c0521bf1f1c9db49d8
18f21acc9d891de3718b4dbac3728874006dba67ba2f28f5ea2c0cb4c13c7fe5
4360db4463a676daa46dcc6e2b6608ee6ddea32f46c13699fe71ec647bf2c74a
613462c4258a0060e9d77da49d6b4e8fe6dc8c0f62adef03ed9a26cedb4931a8
aca62103ed44fba69bc5b375b28d372dbcadd07d86ed544d4863ba05259f5a66
d30d5bc6cf2a1473ea388612516ec12511629400012a1c7651206b408612dd00

ed89db8e83b050d9785974c3515032365033e3e26e6180d000e26f2831c98e35
453c4a7abb661ee95280ac7679b9debfaa2008d8d5a1a61e310437825d605b1f
b3bf5689f6c5be704de977fe07e8257255afcf8f4ddaf3cd27cc371fbe1b6446
8bb3a199130de8f860c3d1f8867c2af59e22bbd40ad2c016db5152f77c741c46
d3f4eb1083df767e80f44ab964e1f7f30f622c0965f73480ffa52741bb9a9b9a
43e22f52633963c3e31d943c9393237beca61b9aea06175d09051d655515a812
ebfd91ebb462b68080c4c578ff47f6e9df8dda5931208513d47bf0df2616482b
28a2b98ae214376ccd549a8b0dccaafad31c8b234d0b81a0e8817579566615567
fe2587dd8d9755b7b3a106b6e46519a1ce0a8191eb20821d2f957326dbf912e9
bf74820d40d281c28d5928b01e5b68d6caf85b5b9188bf4efb627765d708bcff
2446f97c1884f70f97d68c2f22e8fc1b9b00e1559cd3ca540e8254749a693106
a6f3afccd28eb04f626cb9f34bd83f8dca77e8435b315a83b290f124d46da4b9
289e73c9d1da41fc9c5b428ea12c745f83ac7187431c0cdb98d566ee25afba9b
202645d53e040eddb41dfeb1ed0560d3500a15c09717d8853928ee9a17208e22
e27af28d19791d18c0cb65929a530fe5aeb5db25a35fe26e2993c444dcd58352
3f151143fc4747f0f99aeba58a3d83d9ae655da3b5721a0900320bc25992656f
fd54cda0111f9746a3caa64a1117b94a56f59711a83ec368206105d5c8d757b0
b8cf62b529b17f5c8cf3cfa51d47f5dcf263c8ee5fffc427ea02359d4597865a
4888c94e8a943d02f5fcc92f78a0cd19b957fb0c8709d4de484cd36c97448226
c89ab2c5648be4f4e459422fe90be09402824e8555484f1cc51a22ad96edf19b
6262e99b7020b8e510ae9e6d8119affb239b42f4a5966af362f58292aa0af700
66be8e919a890231e9b53718225fda5ccb0c564798900181814952c79104df73