Приложение 2

Перечни идентификаторов компрометации

Приложение 1, пункт № 2.

Сетевые индикаторы компрометации
185[.]17[.]3[.]215
185[.]186[.]244[.]57
208[.]92[.]227[.]183
evon-ch[.]github[.]io
filebulldogs[.]com
hxxps[:]//github[.]com/s1r1ban/
hxxps[:]//evon-ch[.]github[.]io/ob/conf[.]txt
hxxps[:]//raw[.]githubusercontent[.]com/s1r1ban/
hxxps[:]//raw[.]githubusercontent[.]com/evon-ch/
hxxps[:]//github[.]com/evon-ch/ob/raw/refs/heads/main/REA[.]md
hxxps[:]//files[.]catbox[.]moe/4nnmhq[.]dll
hxxps[:]//drive[.]google[.]com/file/d/1DjDui8hEf6GXTJeeETXCo1r3NBizj1WR/view?usp=drive_link
hxxps[:]//raw[.]githubusercontent[.]com/s1r1ban/pagesService[.]github[.]io/refs/heads/main/config[.]txt
hxxp[:]//185[.]17[.]3[.]215[:]11317/content/pt/SVODU[.]docx
hxxps[:]//github[.]com/evon-ch/
hxxps[:]//files[.]catbox[.]moe/gh9z6o[.]dll

Файловые индикаторы компрометации (sha256)
c3350c110ccb6feaf976b1e12adfeeda46ab11c175cd71064bbb4d9511a17c04
80fc01673524fbbe46f61bf232ab2497e21ad160c89657103a7f1fc48561056d
46b540454ddf4dbab3a85e6bcf96e5d492e89f847b9cac61398a70936fccfe2b
69ae746a6c774dbc05ed93df5bc1cef7389878a09dd7ad3481ce43b1c5c6d00c
6106f955b57cef9a978d65533534d36d80a01a35fe94de2a2e6f992d68a9b80f
13ed768e0f4b900ed3f67d418b5cce4363d675ffc5cb05a55b6a63283923aa3d
23ce6a743658a42b0e52289a05f254cf36de5d08e3464393778969c5681fbb6e
3f346b97bf2476d2815cf8ad84dcd6d890fb717de9cc4e7276f1cc477ca39dc3
addf650d7da70065a780a0f66562da8d9f9868b074411686bb485bf3ed6419ae
5ca095e6f4b2f9724374ce849c2f12360178eabbe5b419096d851972ba5fd415
7797ea96c8b6b9b5d1539957f3d2dabfee0783f69f1c71b9553018f926db047e

6779e1243c98b8ffcb53b63f5c968cf6308b4e0705d3056f7a44ccdc58ae783e
06603e1d494258acd09c4795fddf489c6965f8793eb4e19712be301e94893165
73271caa36dacbad62c9703399c917731376197c42d8572a5d7380348d5a94f1
d9bbb7d1f5c31f54f4b4dd58f00c88691b5a1a9143f7d7b338baa423d8b9bc76
307744fa1eb95b2163f260915c1725d8b3f58bfcc4a0fec8decfe3b0edd4783e
857e764cea3f322e6b24f2a7442a71ebb87234d475b3ca91fdfcb9cd39251354
b725ab999208c4c2f80182a2ba24b4da8b0c437e4c35920e62c9a118cb0ba8cf
a4aeb85ce09118a3c9af5307116c4fe95e94333bfbf6d268abbdb19bdfd043ba
84a131b452d30aef686f37f665fc80e4bd2af3d82247fb3abff51f5c4f0a2724
9f7e2c11d5701c54ed626b9771f7b71b794745ae62dc354034095f77c0315205
6d87993596bbb577a2f7e87654dbc5d03b8db659b14223c09fa0e40cbf2595f0
c5e01c3d82597730d6eedae8a827737060c64a4f175a46fd17d1a984036cef2a
b5a320c2fe5efd19d326d5c28b76650de901b95d497599427e8e48400ab7b762
c19e88f1f90bbbc1d7332a9340891ad49d4c3fb48cd2163be0ee0e0f4e4b0e27
3edae7a3502c4c6101911be485f865dbec0072d6af329534bf475f44429fe415
4eea38595ce1f45dbff61bea15df390595647718d8039376afe53f384c59ce75
4a0e2649f89e11121ffe55546ee081ac07472db650d094314414ebf26fcb7a8e
31f1a97c72f596162f0946df74838d3bef89289ce630adba8791c0f3220980ee
27d7a398a58c12093bc49f7144dac2f079232768096d0558c226ea5c53782e29
51af876b0f7fde362c69219f7dec39f7fb667fb53dc5fe2cbdf841d6c5951460
2902cdee050a60c3129b4bb84e74ddda7b129c3473556f689d83609d9a5981a7
92962bfa6df48ec0f13713c437af021f4138dc5a419bc92bc8a376d625a6519a
2671e1f43b2e5911310c5b3f124c076055eec5dee4e596854332ffcf791fd740
1d0ea66d347325902e20a12e1f2f084be45d3d6045264e513dcc420b9928013c
928be5447856555035e984d657b85c35f607161f96be6b3ff55a37e6958f20fc
90499b4ea50433946ab1b182145c7f86237409e51677131ced3935301abed43a
dabe22d794a19ff71c5212c391ffe19caf0542cfd68b951a66d87aca55a300bc
6e66e33a6f37866af589abe6d8b1d7259b371929fe34fdcc3c79a8c5d0b7307d

Приложение 1, пункт № 4.

Сетевые индикаторы компрометации к группировке Watch Wolf	
e732a5ae[.]xyz	hxxp[:]//e9e92d9c[.]buzz/index[.]php
e05f61b7[.]xyz	hxxp[:]//e05f61b7[.]xyz/index[.]php
e732a5ae[.]buzz	hxxp[:]//e05f61b7[.]shop/index[.]php
e9e92d9c[.]buzz	hxxp[:]//9eee1d0a[.]xyz/index[.]php

7956300d[.]shop	hxxp[:]//7e3bf414[.]shop/index[.]php
093cc482[.]shop	hxxp[:]//e9e92d9c[.]xyz/index[.]php
e9e92d9c[.]xyz	hxxp[:]//e732a5ae[.]xyz/index[.]php
e9e92d9c[.]shop	hxxp[:]//093cc482[.]buzz/index[.]php
97585121[.]xyz	hxxp[:]//7956300d[.]xyz/index[.]php
0e51009b[.]buzz	hxxp[:]//9eee1d0a[.]buzz/index[.]php
97585121[.]shop	hxxp[:]//7e3bf414[.]xyz/index[.]php
90359538[.]xyz	hxxp[:]//e9e92d9c[.]shop/index[.]php
7e3bf414[.]xyz	hxxp[:]//7e3bf414[.]buzz/index[.]php
0e51009b[.]shop	hxxp[:]//7956300d[.]buzz/index[.]php
e05f61b7[.]buzz	hxxp[:]//90359538[.]xyz/index[.]php
90359538[.]shop	hxxp[:]//97585121[.]shop/index[.]php
7e3bf414[.]shop	hxxp[:]//093cc482[.]xyz/index[.]php
e732a5ae[.]shop	hxxp[:]//0e51009b[.]xyz/index[.]php
093cc482[.]xyz	hxxp[:]//0e51009b[.]shop/index[.]php
093cc482[.]buzz	hxxp[:]//e732a5ae[.]shop/index[.]php
9eee1d0a[.]shop	hxxp[:]//97585121[.]xyz/index[.]php
9eee1d0a[.]buzz	hxxp[:]//0e51009b[.]buzz/index[.]php
97585121[.]buzz	hxxp[:]//093cc482[.]shop/index[.]php
0e51009b[.]xyz	hxxp[:]//90359538[.]buzz/index[.]php
e05f61b7[.]shop	hxxp[:]//e05f61b7[.]buzz/index[.]php
90359538[.]buzz	hxxp[:]//7956300d[.]shop/index[.]php
7956300d[.]xyz	hxxp[:]//e732a5ae[.]buzz/index[.]php
7e3bf414[.]buzz	hxxp[:]//9eee1d0a[.]shop/index[.]php
9eee1d0a[.]xyz	hxxp[:]//90359538[.]shop/index[.]php
7956300d[.]buzz	hxxp[:]//97585121[.]buzz/index[.]php

Файловые индикаторы компрометации к группировке Watch Wolf (sha256)
0330819d7a41405df52284c7c7cac1a6b70211916643dedfec26f9c03de9b979
3ffadad3cb64a5077a196f828ed8da78781d31fdf2131d9fceaf70c745048510
19c4a777c40ec4bbe8838b0322a75f0eda284ab458047d8146fefe5fb2e39a50
2dac6e71703662cc62f60dea1c10bad909e9cc75920079f74e1ffd4d816124c2
c97d5c7966bc19aa26c257d2177753f7f49596f952087b45f7b383f563387379
e1775c07b56137332890a3745e7b24f959807f62b46454e7ae90051e4efff5d9
ff6b67d059ed6db244ba13e64e6001078b17aba1119f03ae04c94d899487b139
49036c107c764582b8f0aeb91c1e837b7917dbe66b31b55d23ec67d3336d7899

1c470c241daf00576eb725aea04a99162afe57b20d517ff354b3ce7f3312b6b2
0241de58e01d0c0e7d97caaf3b0789e8080ee4fc837922887ce1a3dd699b6d68
b6ff8eff15206e5d05dde7ef0692c548e8cc94fb7471406ad30c240fb14423f5
e492e550d8288f3143580ab4150f5c95e5454ad9410b119081a7a8c4412701e5
68f0a186bd39aa8bc7e59b49c2d4251b0825878bb56c5b2fde3c153e738bdaca
db83403e6967ffe0512469693d081e9059db673c90e8186772dae1e69e3b0ae9
608009a8f572a9e15b318aa0225e191f814e2c105d35812b0dae350b443553c3
ec867d854c9ef6e95827579d9cdceb85fba36964c2b5a29b2ffc8b106c82803e
49036c107c764582b8f0aeb91c1e837b7917dbe66b31b55d23ec67d3336d7899
7734dee6eb2f642325a4b9171a4abda771a9edb8ab30728743d6fe7c75b35659
6a35dbc411e0688bb3c2101a271a324f7172cc9a2205640668bfe62d0ddc154a
c95c65411c7b400eac2645babea94f93f72a9efb56f9f98f8b9bc629ed2433e0
c6b4ee38e86b8338692066e13962df4371eacd6fd7ed62d14f92bd6be66200bf
eec2ec7985bf8ebe59dce1ef6d89240acc33e77eb795ba5899603c0dcf89e038
948d51832456d93cced64bb0449e18ac44c8f522094611aa5e6fa4c470e2608b

Приложение 1, пункт № 8.

Файловые индикаторы компрометации к группировке Rare Werewolf (sha256)
b19cfc6ca0510f9e79a847c9b2cbf83244bb5d75764f8c6dbe5f110c769dba3b
0321a70cff72d83ae68bd4d563ae089f98432c948ecb362da84d7330b1334db3
06081c49a284edef35883313bb4087546e315dff52e0703748ee591c2847401a
06192b470249e3c7a60cef6d3b21a06aff814307686ba3c3d2828f82d6f252de
06e8b0f2fc8296e078113874d8ed9dfda3ba79804e59191df75c1f17ebea6f06
08f2fa8d6fe9ff5c47ee312a490775b59dc6b77e7d52bf0f3c8a69a01ff487bc
0a258ca10028a8694a25c695c117deae6fd87ba9c5aa8cd1118f0c40b1db2b59
0a42f07132c0151f3fea713d68602c2382dd52fc64ce45e61f8f0b65fd708906
0a51ac9603dcea36c31b570682f734903716c94e924e5145d2c38bd21f34b7cb
0c5b6a0b4fe9f33eafe77dd3a30affa7612038f86b1577e6b5c2c02583d5ccc3
0cd4fa585b6d9e9ccf4651888c61f599040a502f315bb41155474c557cbe16b0
0ee38e38cd988f0a827bd31579d7aa3511baa50ad9d93aa6d5fa65f82dde2e2f
0eec89a592274cd5c6289b9ddbb20a359ed47d7f9f804dd414cfb534a6e7ffd5
179eea948829a3f0f69556af88ad189a82bafcec3d3060b1a8abb34456fb3699
1895c97537f73edf7d57fc3464d83fb0cd77bec55d17a0d803917df01f126608
18a5b922ab04ab343e1a473ef32d1f836d1ea79adbc4a3771be654beb86a19b5
18d0458a550028452d9b01516638c72feb174be961e1762c6c6c1416aad0ac81

1a58ff3a89b8802396cd1e668cbd0b3bc24bc3a0d3ac2946f947839a001d00e8
1aece74ccd8a1b08c79ffbbc25905b9e57a719abe4b3905b8561e9cb4f9c0460
1df3d2f3982babeeee2a7e523ffcf9aef60b7241dc21fdf97a42ab34586f69fa
1fea09de5fe4ecabc7a2c4caf3bfbf9cc05e96506adc8abc326ed9b6fc50483e
2184fcfd1b0064a3ec83dbbd62444c5e6a0459234ce61b2c4d0d04819f6def72
2273f86f21ebb4b5a20eebae63d310e3138842a84bebfe2d81a15dbbbaec82cd
26724214bae6decce21218ebdd0d0cbbbc0b9d50f6d3a2f9485cfb7de690459c
282852cc193d08906a89ee3ad3ccefa04a14929b4272298210aa66694dbb101b
28b3482f51bd81ad2238660e506de00929f1758fd7ebfdddfc34b780a6b319ea
2d9c9eb1ca09a8c857a41dce43f9b03785b88c5deb63c79ffda8a0be816aadd5
2f2bdb26725e0320196cdb36fdeb0cc991a82b93d4bd9d05216469211488dc4f
2f4349107822e2aef92e98afe7d261041a5b5db49023d4e91e2943fd71aada3c
31b7b844658869958ec7a0a85e0efd7b197489c696a34973449077804c0266dc
3248e0f352eea478bc4523482b768518f0ab933ca38a606f7560086c70eb7edb
337ec7e3a4791668172e3cb2156fea9c8f875b90f7814e89dc341108db4f9907
368e0c40ac8276a56f827a14be063a44fd97d38245d7402e8894bee5b2c32be6
3715765e6a44ea927e2e2791cd7f6f06ac55f0382f0507c1af19c433596a0ca1
3f1df6e8c6f87776b37dea328d161e9a162cd5f31ee1c6c894209e15c27b3b59
40849935d7eecf3c73445c2980fcc9101dd165b63090d411f5a18c33d66de72d
4094d65ac51b2406fa7dde9745d499c1e7a572abf89e516309cb34c42bceb1e2
43d8e334425fec6d48527db2e2f6ffe752fd28c12587844b440f7ac7c0c7d05f
4508c9eaa74bcdafe68e77842348df01554bdc713031e4726ed9e84382322198
45540346c5f1492f3d599dd5673e8f0d8646e4e3b0b8bfff4c041cd00e3b0b9d
4708320b05d74a1dcc4680c4e35467708376eacb110c7534b6e30e846a341134
48c93c07c77bbc45123820861aea85b38cebd56cb23b80f27799f63965304077
491f09dd1a66c2f2ed155ae6ee35370f4af699de045cd0233908697e1403ee9b
4975039a136db55ee55f96032796c7d5667fead712a3ad3a46e6b03ad8c81bec
4e0b027d89a72ae1f8635fe7a94f160588982db087d9b4d0bdef6280ccf70454
5178547ec59d52d588ade5cc36881a134d0c44b253a7f734d04e7c9fa79ac79a
53010f70828025d0e78f899336a04a05ce9b0d6594ac9b891906d1be0ebcdeed
54ad4dc92471697a80dc68e20321edc8dba30f646965711808cb4443390e356f
55e4a511e087339f77c1ff19229ed80d29c071345b6464eb21c9a1f00818463d
5613c60321f5c213492dcb08367315f2cb3559b346c505573d5d0c286f8d22d0
582e6ece505463d0786a61c46b46ac543e8173bd4fcae894fd8eebb4f41c968f
586336c823fa0147a54e497204224261a525e8352d3f328af1631c0eec37dcc4
5a6e0e76a5d5c6ea80762259c92fa61f2cde5d5f4862d30821384158ec4eab78

5aeee3bc751c5974d6732aa9b824a4fadb5ea30179a4d12fb26aec0efd193333
5fd370bafb2786e5ba6e5df080591358c0280bd7d43520fa86b7279dd7213935
5fe146ac8c4c2f6a71553c0945991fa6532c2fb9ded4ff1f924c1acb696b785e
626d3b6c76c922edf2d987fd44c577da664967f30e3d5a41478e4c5f00f61d03
635d1afee99787bf53644a700b423ca7c21198552a96b414b55a4f95c63e33e9
644f7de01f05c82f7987641c3bed73f6bfbc715705c8f67a5d38167ab4b4f587
6566abec7a202c5c75217a4ec2acc554dae698c7d53562d5f2df21b0056136fb
679bdc8c20313d8d14162fb0cef82f97e537c60e5ba3022b9aedef3f8dc8d74c
6c604a6e55de4bbb94a3e7d2c19890d139daaebcceefa25ba11f09e2a333e382
753eeefc2061c16a29ce6dd61b98888925e540cde73870a8c69e06f7d830779d
77695ee3b73fd362bea97a84f86f17058c78eeab310b0dc9e9c9a4967ba5dc2f
7b61c1121e491ceec9ea8558e323078a5d7852fc56253ada3c561e5441e64e9a
7bbb07ad30ed1b1c85379f8ccdcd2e4651ae878160ccb0a5115a967aa6c8f6c8
7f85d6828bbf16e2e7301e5848f246fe18be8d28ee355a04c3e386ef24be121b
80fc515d176444e4f35eaa78242414409c3c155e87763ec09aa52c1e504bdb95
818200bc8ba8ffedc94e86dfac8b99d743c328c939ad54de112044ab4ac3a9df
84e4c090f96ea5338bb6ced39ee2cabdb95e9d452d72a31abad41de63ea93202
84e94ce421eb47bab3b9cfd00f2eff73586818cc378a3bbf3759458b9e515ed9
85a00e2257e2703471e96e451b5446f0d8aaab86752b5a7e1842f6e578c9a8bf
86fceb74a3e3c3add298e00511a73103de48f3031a7d574d9bc112b4d134d75e
889f85d990dd2121b57d99b449302954012ad4fa7d5d157a7e266b97e78e4779
8911b30f1b6d5f4eccb677adeaa022652a002dd1a1c95a6dfc9f47bcb9b36a8e
8a7a365939ba1445f94d61e96f00a1a95e6f8e1fec99250f10c1e85f876b5425
92eb0cb39732affb31637bdb9a4f76bd2f1274ceea89b0d0bdbc587092cd7c6a
93213be1822c9baf5608eddb47a79f565502b4370e98068f578fcd97d074a538
93cf770ca08d82aa888d6ade54ec0c480ab09b61bab80385b33b2151f867e2a0
9736740259de52ebbfd2347480a84bac9a5623eda286bf6b00184b2dd3837de4
99702191593d486405c7dc6c15e8178086f7b0dcf20081e6a76adc9e297211c0
9c24b601643c919d7b5e1f7684ca4faccd93e095c2c21c31b464b08891ee6f26
9cc062e08e48422cadc3cf2d934abb11c261de1a3f67096567077a71ec16efe9
9f618a9d91b791d5e577689287a500490046f62b710e13b167e6ba2c92ad3ba0
a1725eb2bc32ae8e69dd6772621dcd51b6c7be17d1217a1c1f9e99a1ab9c6dd7
a388e84f7eceed4ca57cd08820f3c7122340110da5dc0ac613568977f54de8bb
a458cfead00466e0889ac0f1c4646ba883463ac3cccb1be8a6dd9b6a3342d904
a4936218f3fb4c237bfe2debd48cfe7a3b8d3ab45b1712ef144f20c8d7391749
a6ff418f0db461536cff41e9c7e5dba3ee3b405541519820db8a52b6d818a01e

a8e3071d50c61a6466b349c88b3f7630910ea52eb9f7c80f66f571fb260bb08d
aee709cd52c4a58e759a1a26a74d68bfb593c9fb56ccf70baf05d8eb452f5e2f
b14b4ea3a69f2e3b727229b28343aef540929dac0e8df739337841a11fe95a40
b2894a34816de89edb6f7233615b004a19d151e63bb774889973888ce264ee7c
b7ad4c32ba976ee90924da85e1f5bf8d9ba2b07f52e6fa89a573dc0e9881f404
b918dd9d1307ff17427f1e1f72dc05e8afb571a5fcd8b68da044502d446cb107
bc549b7dcbc323aaa34e4c2f6a264e664931a70f930513ded3a38d7b605ec629
c182255413aab4b3058850b352c9ee93ba643d09cc874cac97b7645353fc15d5
c254e2edcd35e761a0380aff66069f78ea30ec7b2695dc2071f25736843b5924
c47ef5db00f9b5c85ecbda85661baab121f6b7fcb98dbcb9810ab1cb737ed0dd
c7e368737f10f187d5a83c02553c3300e775a3dc7cfde289bfb6fc5b59faa040
c85f292f29533a082dbbd531e14b8ac3afded0c1bba9eb9c3358a94b26f7f3f3
c880856f622bddd266fede6cac140246c65e8c2fcae14916cd8999b1561cf18a
cab1db4a3e2c9a4f9dbe364b6de05cd7b57a8e26fc5e1e88f4eda374a4371028
cbd2b4af962cc357ee2771240f72a69aa9955fd8b8a47f0e6ae0632805ea79c6
cdf1a85e669ff0d20f45625351f0eb29ac08eda36cff4d92f68613b8cda94b4b
cfae137dd1bb235c18aa37a4669a93ceb7a540a2e0980aef207c8d9490cd1aa9
d036f3e6a5b51e9585908b5167ad94549170ae43fc488e318b2f90c87e226263
d43049d509b9553e43002a5d1287bae95737df9e5b1c95927153f3bca99790a9
d64035f46ad9dcebef03d313ba0133cad63017104abf7be5a87e7dbc1792d746
d8ce553e90f5f80c3d6da6aab2e7dc5b59697156152d8ba815dddd60600b3223
da795093048d41ed955c1e7ec8c408add2cfc05f12d70e9deefbfea98b19b9ea
da85fa8d062c66fee6cf4828facd9da527bb1c126945c64b692ff1cb37065916
daa0da4a46283b10e177641c0bdb8fc89f89c5ba36d82441d1589b94e755c0f8
db7f675145ab8be0d040215af8edafca581a296d182bb1720457b4666344e9a2
deb317699216af45e10b464c67ffa89ced02c2a312122359c16e9466aeee7dc5
e097bee52827e25c97495616ea788e6a30961fca1fc1cb03463764f5aeefd4b9
e25b1aee0d9f65310b10558a9ec8af80176c876864d5170b57e911e7ed508f6a
e32b5f487514180385ff2a16a170689ad91c22c94fb94498d7dfe3d6b566fd9f
e46387f1607dbadc0e877ae1b7fc1a27bb8fecf9a274ce0d8199d285de03bcfd
e5745ae30247814686a60f55c04d83bd8df8f6cdea2f6bb8bf0c1bafedb8e1d3
ea5543c5248d18e9d6a0113022642bd9d9f804f43d5f2bbb88433c2e41205114
ea6f1aa6734fc57da74bd64520936809205955172296e593663fccabefcdf59b
ec421fcffebd641df10acdb535368c8b534a58b8976b5dc13d6b787eab31e8d4
ec91a6a191f5ad4b519b6755778802257133a0ff6ab723688c5a1475aeb44253
f31bf7a2050eb722e85934e8571191a7864f638d4b7a30116853ada4aac3b94f

f5600c6eb5aa1a943d9b90fe857b1f261371e1346541d897b8e0dfb3a4d6f318
f67a8653ceb69ec078aa1733080e5bf9e0cd5ff55c2711daabd38da2ad94e88b
f8539b92f9a391ee7b38279d2bd7e32cad5d6d21ed98265743a8620ccaf55624
fbe2ac472f89ff99a94de444321fb4e515a66a647fab4e2730706c6ac531b417
feec7be17471ed8661b499863e3d38e4db6c8ca28f8f34cb2f1adbbc7ced4e52
ff8eca5a05e9285e3b85b9668aa788243e87b66ef53a1bc54197045415dca57d
c82c059f29e1b505d0c5b887338b178d329c8baba3df871d890bc7d2dd667e40
a8d97bd915b043ec5555992b2eb5e05a12179d46affda1659d62b82032e15422
41de025ad3628a3f3d56625ac58954d4daf278e4628477c3ea716164ceb49c0f
be8805651a0cae1aaa346ad1be96eda83ad827c322cb196af6ef292c2a25203d
12d5967f7a04047011c9dea44ca319e4dfd9284371a18217a4340dfbd2d53419
255251fee8680d341b9a214e8c7a25f82f1c4f9b93dc443ed240333b13bce428
019b97ddbc81f0dbd2c452008764b02837dd6c11054a88025a61777018031392
269723b5da1676299850fc8aed664e505d9668dee88e8fff1ea327ff670b0441
aceb77f28d3994c7582a83050a7d8cebe4878d71539e0be3a23c97ed88ff557a
2d00848ec6a4ebfd34521c99086dbee4c15cc17aa83beb6ed13fedc124d2c59e
33088c6cb8a4297ba02213567d3d503fb73ca5b1b6996d36e4eaf82bffab0826

Приложение 1, пункт № 11.

Файловые индикаторы компрометации к группировке Toy Ghouls (sha256)
57d0517157adc70f9d7f94c4686b44ba9d58b22719ebf914303cf9fd73a6c8a5
e593aae24a3fa83df6b043c9c454430e5b0b253c3d524db492cb1efa30d5cbf3
a21870d260f1b1805f6284d4d32114cdb6680b178849de526974927c15288afd
24ac8b8ea99e1fc7056d29f6b21e8a6927f308c34b004ec63766872153da4f83
fc9482ae04976930b56e76de7128ea88812619c4fe467d0331b51bd5f729e946
aafeaf53936b8a40e0e91ab930a764b0a18072bbe3ffdc19e85cf6c365e72c20
6bc7d279a7dc69d42de91a29f1e5aeafa4c0eca08ce61505cae40f25121c7d5f
77906d5c8e8ba7dadcd66b8b468eac12c25ee625c7f995284bdfdd6938c5368c
45aa395354c88e49e73bf3ef904bfdaa004b25a0b72c0c8cca87852571d9b539
a14faa026cfb6d01b743725509fd3f823ebe9d56221700607c9571e44e58369b
8806bed035c9bdebe0a1e67cf23efde68ac3b1587df287aef318dcee91256276
bd503c81ef9fe0bc03d70e60bab29e0eef829bed26916adbc1cb778182f3dffa
4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5
26d5748ffe6bd95e3fee6ce184d388a1a681006dc23a0f08d53c083c593c193b
77cc2bb8b8d0a9b90ae730eec105a3d26fffd8eb2194099701e222d81f9211e5

fde643fe1299a83740d7ab5b19263fe1adb24a76698dca4f30f03fff7d35cad3
92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
7b9efc7ef8957411cdd22582ce4bfb3a5f76d9c91cdb7e36bf85c9785a2480e9
d8ebb7aeb7c9aa2d082673b14ec598f2bdbd48046a7fbdc923a137ce3b6011f3
62b3325432d03f5c9d8b65eee1ff4cd2f6d13a0a28ff4eb7ba6bd4f47557cfe1

Приложение 1, пункт № 15.

Файловые индикаторы компрометации (sha256)
1e8965b4d9ff13d9a71f702f1290f1caec9a3569870b9cb4dd39182fd33b758a
06d9d92b51d6801a4c359c7800644899583d4a5c93a842a072204d74f3fbd424
168a8f539999c5aa8be06a620fdc7d0f9dc44ea28fc436218a1bb9fd04d273be
3b77ad9aca70f8d722320218c8e6d6422409cda9f51e2b222e351d0125504260
412551d0d179d53bfa83258e19a2ade71af70a372dc2235ed10490f9217dd496
5501dec4aed51de2c33ca105f5897cbb73f4d65e32b239877a30db918c7c2fea
6747a5acac297724c4f6cb2332c7b84d8f3776f190bddf469c625f052cf1de59
6a14b39ae8ac4a30b6345ff84e2afa19ec33e0e29178d803e723e783f1db3cff
70f3f1092e5df170c6522ea35ed1c1caa0b44b5914c332e04f4136f5d9d0513b
7558458b8c87d45007299a8a1e1af9c31627f20a7cc6b5d49e083c42249b1cc2
818ce6d4783106f464ea36b948c76de53631164b37e2189f5a689deab76f4494
8b7f751fb4f0382b2ccf8382b9467e854abae80c2516f61d2e5e045e64789b3b
8c6f181fa2742049a1c34ffbd78426d7ffb42f32abfbbc7e6c343980bd500b6c
8f62742a2a529a12295be70321622a85d62411d064882ca18e9f871c43dbd5bf
a16727907b3f116a257311fb8436dbd3c6e15f39cf45e422aa525c0bff5d5533
aeaf7f32d40f0ef11e314e595734b28e15aea039e193a6b760164e7e8404aeeb
aee1d14e32cfe09436141a605cdb3f7b9216e11a9e7a094198a4b871a6d9a6a6
bd2c00f361efde942fd1c15856071a6f146423f314fffd2884073c501e34eed8
c43ed482b76f03e7e0939af3d009aedee98ef7f93f4f05cb3e2f60b5952ef2e9
d5b81b9b94b92499a8bc6bedff84109a04772e56dbfc263b2395c48b6f1ab0d4

Приложение 1, пункт № 16.

Файловые индикаторы компрометации к группировке Watch Wolf (sha256)
0a4ac8f45a51ed772a35a667c8dd318c2da8f47ea0c92bf814f183de459ddd3f
6b580f37f876b398a647d0f89edf7a61684aae3cfc3337089a6f44adc6129c2d

029f739d4d8ce8447b6d59f4fa4ad4c3b1451e156fab5d46c3018a8710385255
6336da0810e7a6b9aaeda9b9411a916cbae377fa90bb8847fe23b39304637c2f
618deacbca9ff6354a414c79443a64ca271a5726809be4ae7defb6dc404d65e0
703c59a2e81bf5b0904c7a4fa5004c7ddef98b826a1b399d2b624e62d4b61999
1e3d4646587c33406990448f742435cd2aee00bfa55ad05e51090144ae9187ac
6e0af63ddd50e1bf08797650143d14fcf48e3105906c09ef3caa33857bc6cf69
3804e9abb51a92acce5e6f123f89df4ae30b23bdb6a8e0ecad3fbc845d65dcb5
11fe824ec299fff3a68d179942d1a69bcab713f08f3b8285708a3a870cb10a31
42601c54ce777327ec0696763777b2e1e14a8c78b34e567d47001c0edaf46b1c
46d6f566f53193fa69cf938fcd3a4979d9b4d604ffa78fda913aaec228272d8d
e96291b5a8614c64174edf8f8a661caddfa776003581971301e55a94c0eb4a13
20b56f71776ac9ce6cf8daea24dc3794c0209ac738821a7a9b107fb4c1eff597
d380f283adb3901a6134798f58acdd94dd7522fc8ca5f01695f78712dd524102
9809439b1761c3ead0e7faf7fd093fc841c15244bb62999539a173bad138f91d
33ec006c120769ad24adc027a2ac36ed480b29f8a9cb4ef0bb8847d17171c0ea
6ef059fc912103f9392e26fcb007af9b891c061dc49c98b47f9f36f427b55992
5f08d0eb789418e69573d984bd4b5ac60e413327cd2a3fd078d826669276d48a
96433ba9d91ef87e18cf429a99d0f4f308fc6454cfc3145d7c4e26b57e5b1103
c96578564e3f4d949d97ce7f55c6a9d407da8e0de06cc5994917ef24aa5d38b0
ba0bc48892d6d9b18fd8d672b5ead41caa5e85306a07c1c20cbae4c135ae3566
a125b357a3eaf73586ff29053e92bb9bffeb4bb257640e4be28bf53ba327d78f
46c15e9e8a0388cd151ceb80182cdb1c92a9fb79e1e2a055f245f0cf7efda2df
4698f188cb4cf0c3b1bd8da28247f6dd61dcc5cc9e0f0e3a58aaa092607c31ba
428f5bcad2db6b049e8b995fc7dd771ad62bf4671016bc9b64420c7d5c891531
bdc050d36b0eab3353dd93aad6096477872dcb070a205f51bfae28652fa9adbf

Приложение 1, пункт № 17.

Файловые индикаторы компрометации к группировке Rare Werewolf (sha256)
518db376330d8b5ba5eb60c50b9ebca3bc270de94810df21391a832e2eab1e26
de93a0a68a7be47fc8670dc5b7e82ff47db9562adab41af67aa128a2ef19b0f7
214715d956079f150906bf60bd62cc6f6cc0d8ba32ea1952b7c8192dadbe6eac
8d78d1cd054ff3ec9e4e52260137d16f366c19b5c71629a1e6f7a32f653ad4f7
e3739a1aa66ee85834e0c7d833c25589008108d661351eef7293f8746f77a64f
d524fff9c8fec16aece394fd6783cac432dd80fe5091ed3646b0fd9a5d99a2ea
837f40f29e58eefbace561f630c201ec9c6315505982f0daa46ba9a3a470535f

9cf15856827580521d0e73c2246164a415d70f598f2a513a7e799f99fcebf093
5b5fecc3a269c5af4c10633480f0f081833ec738dd3e1a6abeec69a90b6ea0e3
a5c8dfd310df5b63d32763157143dff45559008a0e7e0b3144b01c2a79f595c8
a7f8d034dff004ff52c272aa5bc12aa5b2bc6ac1d8e14634b30ecf37813381c4
d4fd4b10ff0138d6b14b6cac6850e6533fa89a65286ea9751fa2def212727270
df5240efa0511efbca6f86727e1db5780bb3d5ec8db23f2730fc534410a0c34b
b945150bf3330bcc67aed6d779e6c1239f21702fda540368823b9944f2ba590c
0359064c01a7a5e95666912c6e9009d1c782c01631c9fdede7321fd743521258
5f46982bcb737da5cc2cefbd59d3cab75c8d7ac4fad535c50447c1b4653e1260
6d593b8569dcc11b06ce8b850fab879b16dd5fa2075ed970d316932dd3d560db
440cfbb90a8894cae0418081d45acc593944d56e3e1cdc5de257007a7c521a1f
8de53ef7a7fc12c2568ce561c13efbd24740a6e3b1d388a7f7506b63fbad5161
077bfb93b8ce9df4ac33835ab8e723994bf6f788a53bf42bc2ec564be08ebf88
b969f5e8c75c8c408c33541c7418436ea8da536cbfea31704566c89d2dcef3c7
15126c0decd6a4cb9033cae53d9ae9543ccf8575b683b77d37aa45e03234bcab
03378309b7398b87c483b93de862724e3258d14b313274ee54130d5c9dbdffd8
93265ae9e43179d04f9cfc98f1355f4dbf74dc0df74a051e2838cf55efc614ae
993b38e4824b44b776bb8787e2e4a54e2337fdd9c9100f1db3ea5f24e71dbfbc
6fd1aac9f4f3f4f2d2257d898251bd9bcee1fe9a8fa8df1bad5a3539947a84b6
bcbeefc0218101a2fb74d209c5c8ed234fcff8ebedfe1104f5bf1f37b79df8c1
26d66ebc64277fd40ab26714f3f0b96356f7fa7998e003e6f318d40f819e965c
ac287dc3e25031a68f662bad657fa4d14bca2747c14cf7e4b00d56f170a0c82f
0ff8de94147e5edb4388d162284b91b0b60f654c9e62dc3c816e138ff624956b
c435cf727ba64b2b3ea4645f5f97121c97cb1a112a21223214890b031dcd5efe
7dd1ecd725f230c34ae32b1efb3f843230a2e8000e9c14c21786ed66b5f0b5d7
f6a5d216a7a91b84cb8bd922ce88d9ae3e86ae0e6d4ac6264b4e373085e17e19
4e7b46b70ed93faf0eef9723de9b2f477b35e9f73635b7c16035a700c93e0ee1
1700c1120fbd4db82a288de27cc98adb470748dcfe71e6ca80124e444fd08c3d
ca9eb95f1c624c52a1c1ca9d294f7c3402531517c7e1be497463705f67e80e8b
cdfb84060bd1d8e84c8a46ac86793801fd671487483fbe4e8928190466c1269e
3f77ed5b6b694942644b69f25ff8d1fd2436c70b92f7f6a5ffdb6479ad192e01
d5cb3c67e7fd11c01eee3f3a35b078a0636b17b2b2212724a13294a05151f0f7

Приложение 1, пункт № 18.

Файловые индикаторы компрометации к группировке Rainbow Hyena (sha256)
c7d86b46afd546e6ba231789859be55d83ad74225671a02fbc43bd8bee5d9214
4095be0a139a6f53f1cc361fc1f34464cbc6e3b60db9cd974505a37976f5df38
3535c5a2a4c845c325c4db3d0d34255d8e6fa0c9ee2d03f5711e0ff89525000c
9e73c4afc31cae3a0a668004ac6c266a88517f7ae036bbd1a5bfeb9ec6b2dae3
99bf6ca0fd356f853ca8165e4cad28850d191470d17573814875c1019e43152a
8c6c3baf4cd8a7c42dd878a2a8d427a8388a0044297c7491c84e386b25f47916
0ec270041428c14016559325013feea06bcf3ac483e3dbfe7b0a222c3b35871e
d37bb958c50975b59a8cb4c16ee07d4999040ffdeb2271cff71f4908603c0e7f
e5c4395e7f111b04fd7edb821e0037598823f71c6ea217605349922139f0b4f0
2d5dbaad4590720b6117871ff0ecd7300d51f80aee8df7a11ec9e984a30d598a
76fdae0c129f158707d96aec15893862b82351f91ed03731e3077938f9f37e7b
c237c5ee8baa9625e9d9115d52223656ba4a840a3124d1dab397c46a2277b541
42ba749a7b51f55bcf19bb425999c0848ad100c37e2494fb7ce44a18642ebf72
eaf8a29eb096e22c48f2f39954e4e852bb80f3b50f5aad1d2518efaa5b066b39
0730181d132d40f742bd9f06e1e2d4065445320f0133e1cc00b91f8d161cc9e4
af4ca0e90548672b7a180ca24c581420af8ef4aa5f60c2d99b76ca31a376769e
754f7f3d2f7e10d95487eda0b89b594dfcf7e57f1a2391ec86b555585bb14827
d9cb5b69b162646ce119923e98c301a9f3012c4e5f7395e1eb06d3b5f4fb0990

Приложение 1, пункт № 21.

Файловые индикаторы компрометации к группировке Toy Ghouls (sha256)
511d32b8ffcaca77f86601ae758adec70949b46441f383cd6ab3dc02cc898723
6ddb2eb0a6db394f6fc70fa823869531b6d11c0029939e53349d4e5ddc393317
380ffc4cf15d6052e59942f1725b29a46e3bb8d69f82d31d195fee5302221d8e
62b933d91cde72980c8f5a996094a806abe8f71a66b5f3149a0dcb3217520f28
a6b0561531300d571221d31c5b893904ca01bf58c7a92b85502a017e6d2201bf
c744f7084e70f7fa2c76f519b32db66aefcac78ca246747e0c20133b03b85acb
ac10ca1170bb7f336d8a6c077e3acd2fdfc724eab2d44780cc3f13625b2daa21
9fe4936dbb1b7f42f1ac73d38deb231092a8c640e96ea8d3c14c8d811b56ada8
e8c934be01db631df1e82058ce9ac06b9a64e7c50d1196a889e074f972c78d1e
5021c2ea1b33dded0987d85768cefde586ef050a1c860c26b6a039d94e86e364
87cc1feb11ff3c1d4941ebdc2e03514a8eb9d466a7d485c9bf4c3471ffacf8bc
fd81d59de37e86c87f65c91a8e630a60a212fd655ffdb27ccb0bffc8d0b6c4b1

f70c8dfd406389cf8cfd27d3a9c9f0ebd25eb0ce39529cb3ad7a3206783786f4
655a85b9925beb2453ade8abea4d3f3f9ef541624736cb8f5e35c5b75834c26d
30c66b50553234c3c036a87eef101b4a4287e5658f9e35ed5202950cd2c61e50
4833472a2361ab60347ef2ba3b0b1d4957502f00e284bdddc5047b6feb820a01
5d6da2a79f549143432b9704812e4736b10fbd3c4f9c6da66a24d3b6f6400ef9
725070925f35990b68f01cf0a50a82963ed2bc987f3ddac8b02ee96e1a3cfcad
acc25182c8b36a80a9304fd3d8111fa7e4189a90cd7d6869def852d51f92a3d7
930bac37b9f1c8eead4f6b74bdd64c26d885f304beb2b45f8c2c79d179eb15c9
0c139c3c41093ac65e680f93dd90a94e42e922e54942445358ed2c78199fc9e4
343c3ee81d75622fe45186fc9e64420d35eba1cdd9e3d69f74d1acc7be01379d
125d3e51b015880f00abb146d63748a2418ec596f66a261bc5d4136fc025764f
b1f46184dfd79578233103f2da0a758b02f6eb0ab4449578028963635fea90c4
afeefbdbf3efd3411d154a2d9ef54abe5395fb21c23c891674bb37f9c9dee26f
3cf0891ba2d0646994df31899247c93d153755729ae0966f71e6a4f8c2cc7646
17f8ccde658b4fc356ef318002389a44488473300c7f2a09999e9beec5867316
bcbe12c718964a12896023ce21b2558efcecdd6474e6a8d23037ad800f901631
04b8d022fbbf39230a7599c892fbc16623ef6048c1357812b6a6919a9fa1a682
12a006b91ac3ab554c9b06f529ca82d12873c21e3612ea7f0831f23cc8f8a64a
02cb8fac2876403f030fd6cd32779f23162e9d2a193c9b371c5a43061464fb8e
5ceda242ad30a9bca8e86bf7eac66fd026e1afbd8b20e982d30c157458859669
0b0573ed0656f19502d079a9353b058e235e70c0086010509722f4c64bc273e4
02d0903db0538a70b790acd1c785f35c3fbf1867350b868b71caa544c0d808c3
e9ed6a8f4da145b19d9935bbe3afdfa9d06b6ec46a2f6876e817a5d7b7ec1b72
901b46aba2a8aa089b2e6a84bb07f296fdb013355ae559149c302aa790fb1811
b9f5c41720928ca2c363e485517e40d8fe499e202d0801d81fd253573d9c62c7
1fe81ccd9147802144b04e0ae161b6fa3edf4c3fe5df8bc7090d92f32bba62da
5842382b68625aec225d2f98b02b233879b80618ce92d7d27f786249eef4dfa0
a67e11d99a0f0fbf09c99879c3ce36b4aec6b3fab79ceb7adfcea1fee8ce4f1b
808bb18818e488551174fd1d550dc4b7fc54a7add98df8d54716347b902c6958
1d494d80ce3b68aab594985e87c1645b52aed4a3a7caaf091c3e259f9386a184
d0ed318e4703240ac43e9047a15f83e6ce0464c4487c1737483677c89f1140d3
7408c60cf6e547b38cdcd8d8f7811e1da457944819f1cc0d59d5c0560e626a32
95cff75ecee81ff64eeaeb0826aafaf109f10f2678ec7f740112e44afcf33c47
e9e52e2f607433e2d18be8a9ca7942628c5f304a8b72b6e559cfa0201e3ef959
e1555a0b2c92d43050dcb92703da50ea637cf523714c7034c641fff792f12fc7
4ea92c7bf337a83b13413ffc88e2f348f1cf81b3d9ec5ad9769536002b275254

5cb9d807524c77e3d2ec3dda55541bbf0e1bef4403f45c68ec24b349098462ed
99acdf11b74029d053ee7daf62575e50dd43a42b474efd44853b78e29b4fa7cd
c48a5ae1da1c5e1901e4da5a752c88a520de213bd2046d8d02fca2aa05594e9e
1a007936a43bf7672ac4c69367f4f9fc4aed263f7abd0555052f037d3c585529
dce818f0738af0dc9592627b7db5f4d3e02aadfe24c8de8d4f10161a7b5f75df
57d0517157adc70f9d7f94c4686b44ba9d58b22719ebf914303cf9fd73a6c8a5
e593aae24a3fa83df6b043c9c454430e5b0b253c3d524db492cb1efa30d5cbf3
a21870d260f1b1805f6284d4d32114cdb6680b178849de526974927c15288afd
24ac8b8ea99e1fc7056d29f6b21e8a6927f308c34b004ec63766872153da4f83
fc9482ae04976930b56e76de7128ea88812619c4fe467d0331b51bd5f729e946
aafeaf53936b8a40e0e91ab930a764b0a18072bbe3ffdc19e85cf6c365e72c20
6bc7d279a7dc69d42de91a29f1e5aeafa4c0eca08ce61505cae40f25121c7d5f
77906d5c8e8ba7dadcd66b8b468eac12c25ee625c7f995284bdfdd6938c5368c
45aa395354c88e49e73bf3ef904bfdaa004b25a0b72c0c8cca87852571d9b539
a14faa026cfb6d01b743725509fd3f823ebe9d56221700607c9571e44e58369b
8806bed035c9bdebe0a1e67cf23efde68ac3b1587df287aef318dcee91256276
bd503c81ef9fe0bc03d70e60bab29e0eef829bed26916adbc1cb778182f3dffa
4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5
26d5748ffe6bd95e3fee6ce184d388a1a681006dc23a0f08d53c083c593c193b
77cc2bb8b8d0a9b90ae730eec105a3d26fffd8eb2194099701e222d81f9211e5
fde643fe1299a83740d7ab5b19263fe1adb24a76698dca4f30f03fff7d35cad3
92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
7b9efc7ef8957411cdd22582ce4bfb3a5f76d9c91cdb7e36bf85c9785a2480e9
d8ebb7aeb7c9aa2d082673b14ec598f2bdbd48046a7fbdc923a137ce3b6011f3
62b3325432d03f5c9d8b65eee1ff4cd2f6d13a0a28ff4eb7ba6bd4f47557cfe1

Приложение 1, пункт № 22.

Сетевые индикаторы компрометации	
205[.]185[.]115[.]242	34[.]58[.]66[.]17
67[.]159[.]18[.]115	46[.]246[.]86[.]20
23[.]132[.]28[.]196	trannynet[.]adgods[.]uk
103[.]181[.]182[.]245	seriosbot[.]geek
139[.]59[.]53[.]195	erfffxz[.]bounceme[.]net
41[.]216[.]189[.]108	rzchi[.]duckdns[.]org

66[.]85[.]26[.]200	netwoasysn[.]ddnsgeek[.]com
41[.]250[.]136[.]90	negro07d8090[.]duckdns[.]org
172[.]111[.]162[.]252	pipeiro[.]ddns[.]net
177[.]157[.]188[.]182	bmtxf0usc[.]localto[.]net
38[.]165[.]82[.]8	ddos[.]8ucddos[.]com
104[.]155[.]138[.]21	amushuvfikjas[.]b2047[.]com
104[.]131[.]68[.]190	a[.]gandzy[.]shop
104[.]131[.]68[.]180	shet0ldmeshewas12[.]uno
173[.]208[.]162[.]39	reald27[.]duckdns[.]org
yu5bca55387d2a9ba0d7[.]ddnsfree[.]com	