Threat updates – A new IcedID GZipLoader variant

threatray.com/blog/a-new-icedid-gziploader-variant/

February 25, 2022

Author: Markel Picado and Carlos Rubio from Threatray Labs

Published on: 25.02.2022

Summary

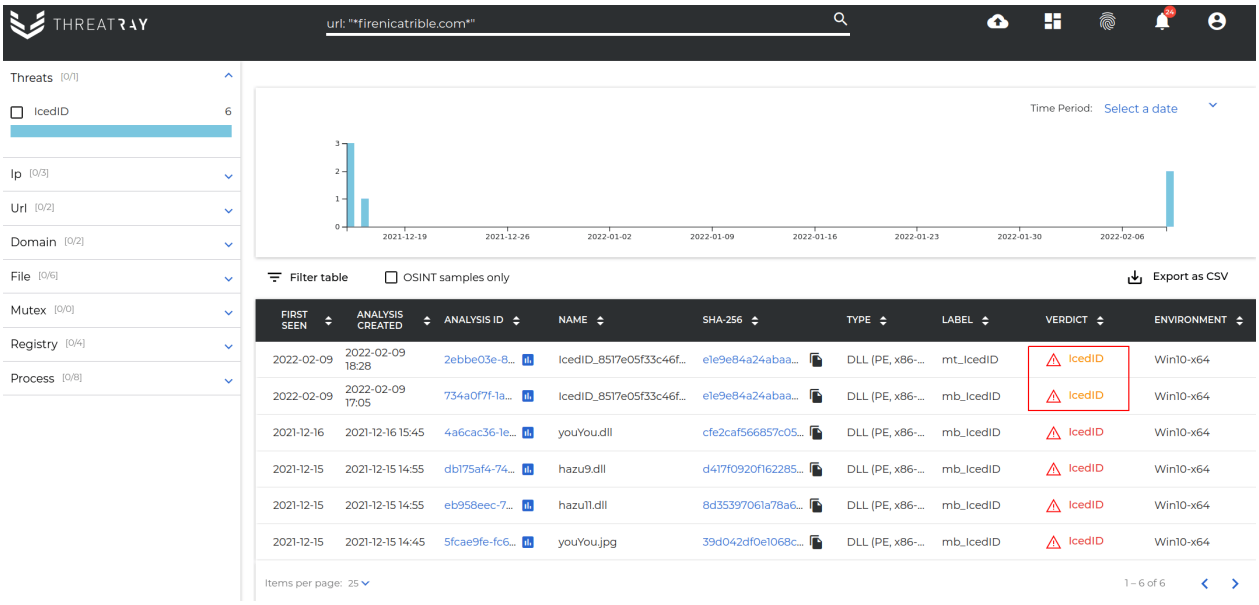
IcedId is a modular banking Trojan discovered in 2017. It is one of the most prevalent malware families in recent years, targeting financial information and acting as a dropper for other malware families, such as Vatet, Egregor, REvil.

GZipLoader is the loader component of the IcedID infection chain. Its purpose is to download and execute the final encrypted payload from the control panel. The encrypted payload mimics a GZIP file, which is why it is called GZipLoader.

While monitoring our incoming malware feeds, we have detected a new version of the IcedID GzipLoader component which is distributed since the beginning of February. This version introduces new anti-analysis techniques, whereas it is functionally equivalent to previous versions, except for the removal of the SSL-pinning feature. The anti-analysis techniques that have been introduced are the dynamic resolution of Windows API functions and string encryption.

Discovery and timeline

The new loader version came to our attention while monitoring our incoming malware feeds. Threatray classifies malware families using search algorithms that are based on code reuse analysis. We have seen (see image below) that the confidence of our classification algorithms for IcedID has dropped from high confidence (“red”) to medium confidence (“orange”). This was the trigger for further investigations.

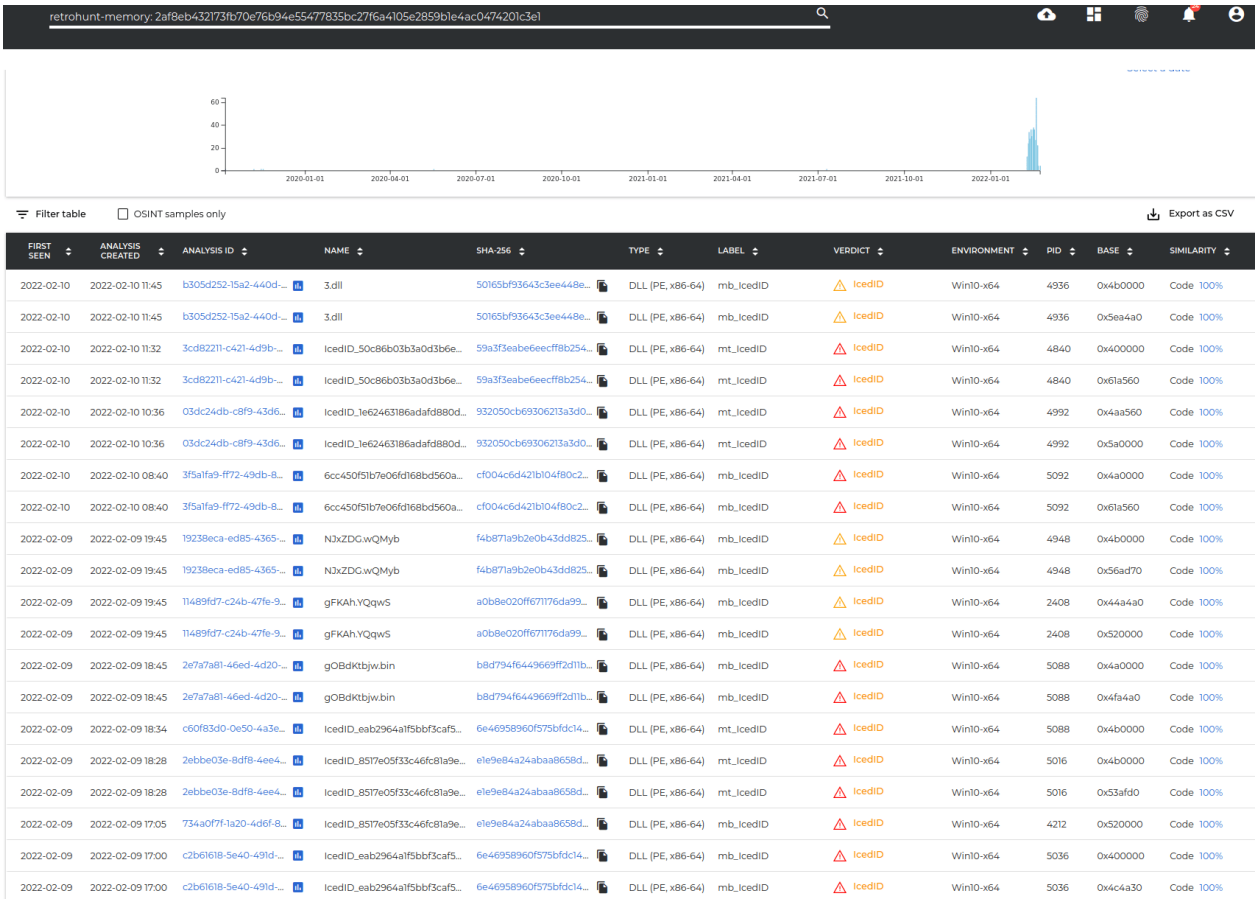


Looking for samples contacting a known IcedID URL.

Looking for instance at the analysis of the sample **e1e9e84e84a24abaa8658d871515d32e21ed51f1c54812315155f4c88bbc8722eecbfbd** we see that the virtual memory region 0x4b0000 of the regsvr32 process contains 9 functions that are related to IcedID GZipLoader component.

IcedID detection based on code reuse.

Using our retrohunting capabilities, we have searched through our platform for samples that contain a similar loader (see image below).



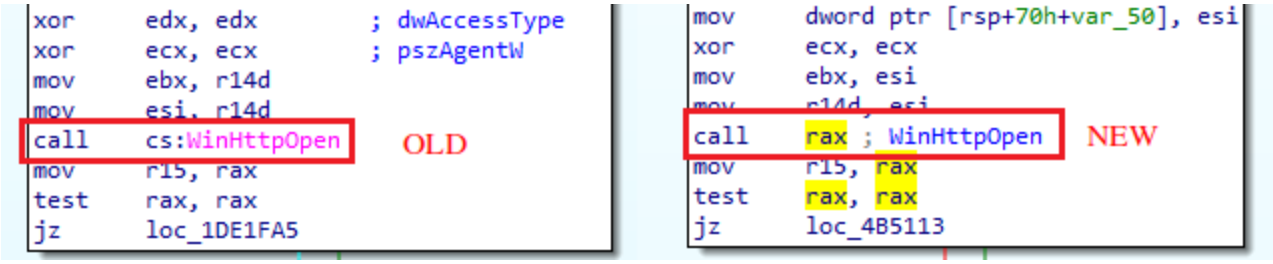
FIRST SEEN	ANALYSIS CREATED	ANALYSIS ID	NAME	SHA-256	TYPE	LABEL	VERDICT	ENVIRONMENT	PID	BASE	SIMILARITY
2022-02-10	2022-02-10 11:45	b305d252-15a2-440d-...	3.dll	50165bf93643c3ee448e...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	4936	0x4b0000	Code 100%
2022-02-10	2022-02-10 11:45	b305d252-15a2-440d-...	3.dll	50165bf93643c3ee448e...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	4936	0x5ea4a0	Code 100%
2022-02-10	2022-02-10 11:32	3cd82211-c421-4d9b-...	IcedID_50c86b03b3a0d3b6e...	59a3f3eabe6eecff8b254...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	4840	0x400000	Code 100%
2022-02-10	2022-02-10 11:32	3cd82211-c421-4d9b-...	IcedID_50c86b03b3a0d3b6e...	59a3f3eabe6eecff8b254...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	4840	0x61a560	Code 100%
2022-02-10	2022-02-10 10:36	03dc24db-c8f9-43d6...	IcedID_1e62463186adafd880d...	932050cb69306213a3d0...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	4992	0x4aa560	Code 100%
2022-02-10	2022-02-10 10:36	03dc24db-c8f9-43d6...	IcedID_1e62463186adafd880d...	932050cb69306213a3d0...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	4992	0x5a0000	Code 100%
2022-02-10	2022-02-10 08:40	3f5a1fa9-ff72-49db-8...	6cc450f51b7e06fd168bd560a...	cf004c6d421b104f80c2...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5092	0x4a0000	Code 100%
2022-02-10	2022-02-10 08:40	3f5a1fa9-ff72-49db-8...	6cc450f51b7e06fd168bd560a...	cf004c6d421b104f80c2...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5092	0x61a560	Code 100%
2022-02-09	2022-02-09 19:45	19238eca-ed85-4365-...	NJxZDG.wQMyb	f4b871a9b2e0b43dd825...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	4948	0x4b0000	Code 100%
2022-02-09	2022-02-09 19:45	19238eca-ed85-4365-...	NJxZDG.wQMyb	f4b871a9b2e0b43dd825...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	4948	0x56ad70	Code 100%
2022-02-09	2022-02-09 19:45	11489fd7-c24b-47fe-9...	gFKAh.YQqwS	a0b8e020ff671176da99...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	2408	0x44a4a0	Code 100%
2022-02-09	2022-02-09 19:45	11489fd7-c24b-47fe-9...	gFKAh.YQqwS	a0b8e020ff671176da99...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	2408	0x520000	Code 100%
2022-02-09	2022-02-09 18:45	2e7a7a81-46ed-4d20-...	gOBdKtbjw.bin	b8d794f6449669ff2d11b...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5088	0x4a0000	Code 100%
2022-02-09	2022-02-09 18:45	2e7a7a81-46ed-4d20-...	gOBdKtbjw.bin	b8d794f6449669ff2d11b...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5088	0x4fa4a0	Code 100%
2022-02-09	2022-02-09 18:34	c60f83d0-0e50-4a3e...	IcedID_eab2964a1f5bbf3caf5...	6e46958960f575bfdc14...	mt_IcedID		IcedID	Win10-x64	5088	0x4b0000	Code 100%
2022-02-09	2022-02-09 18:28	2ebbe03e-8df8-4ee4...	IcedID_8517e05f33c46fc81a9e...	e1e9e84a24abaa8658d...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	5016	0x4b0000	Code 100%
2022-02-09	2022-02-09 18:28	2ebbe03e-8df8-4ee4...	IcedID_8517e05f33c46fc81a9e...	e1e9e84a24abaa8658d...	DLL (PE, x86-64)	mt_IcedID	IcedID	Win10-x64	5016	0x53afd0	Code 100%
2022-02-09	2022-02-09 17:05	734a0f7f-1a20-4d6f-8...	IcedID_8517e05f33c46fc81a9e...	e1e9e84a24abaa8658d...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	4212	0x520000	Code 100%
2022-02-09	2022-02-09 17:00	c2b61618-5e40-491d-...	IcedID_eab2964a1f5bbf3caf5...	6e46958960f575bfdc14...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5036	0x400000	Code 100%
2022-02-09	2022-02-09 17:00	c2b61618-5e40-491d-...	IcedID_eab2964a1f5bbf3caf5...	6e46958960f575bfdc14...	DLL (PE, x86-64)	mb_IcedID	IcedID	Win10-x64	5036	0x4c4a30	Code 100%

Retrohunting for similar GZipLoader samples.

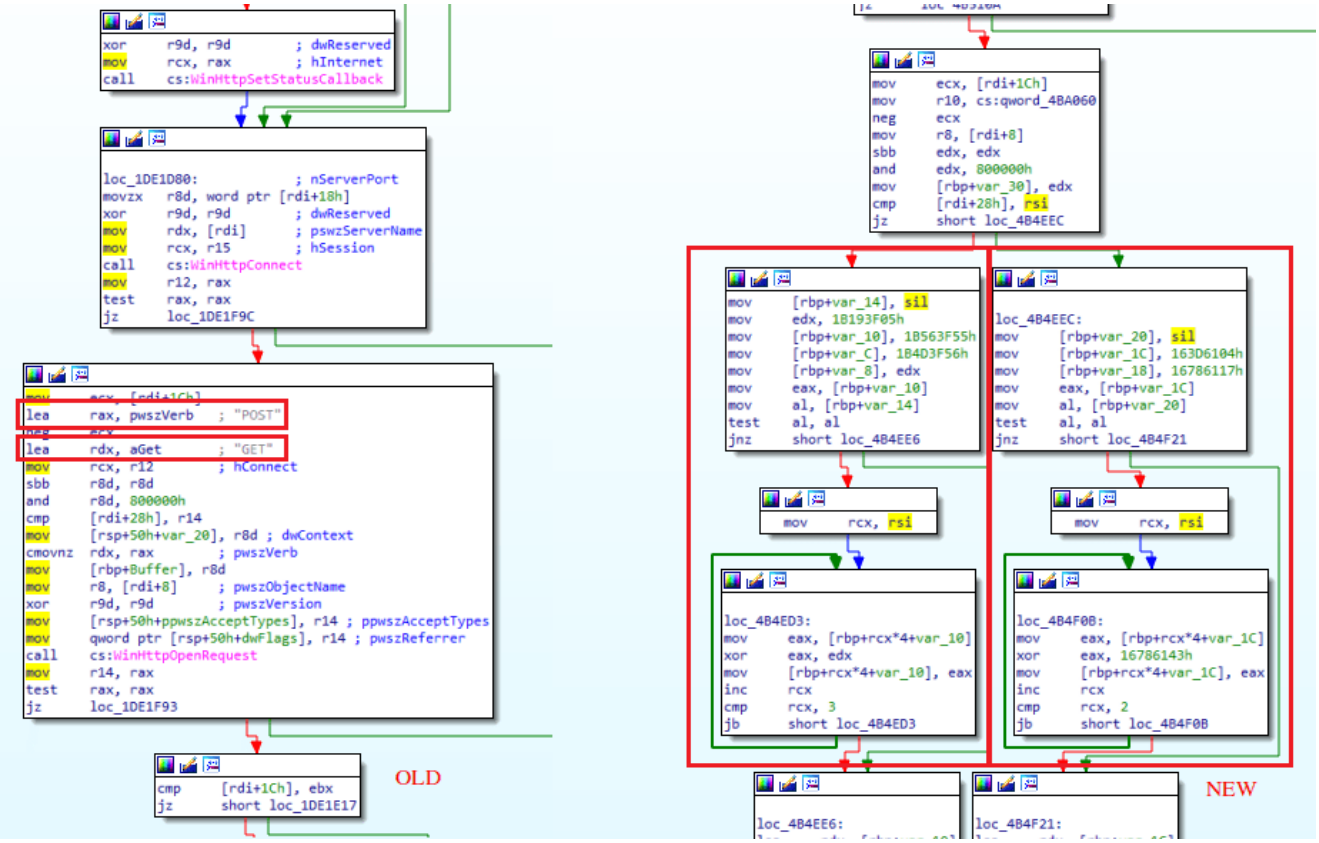
The earliest sample in our feeds with this new loader is from February 9th, 2022.

Detailed analysis

The new version of the loader resolves imports dynamically, whereas the old version does not:

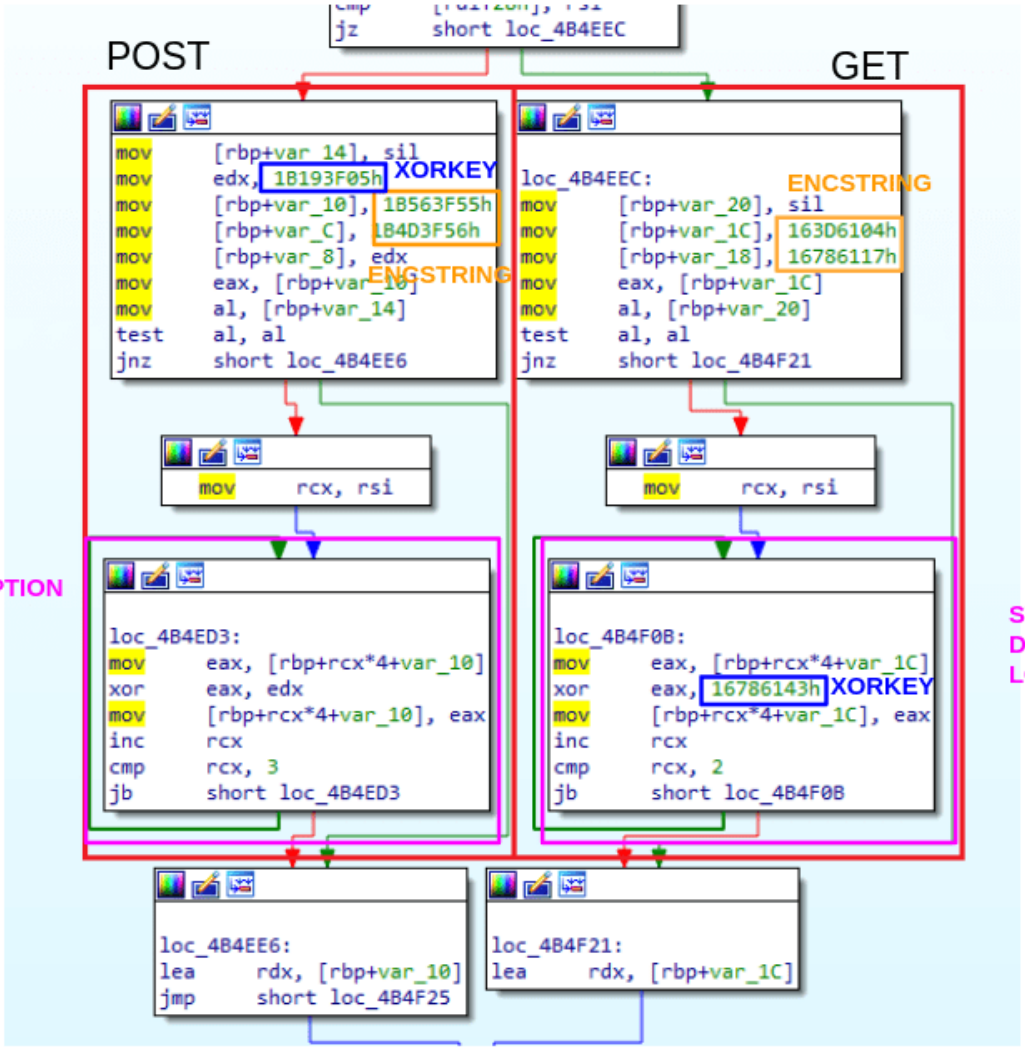


The second functionality that has been added to the new loader is string encryption:



Strings are hidden using a technique commonly known as stacked strings, which is combined with simple XOR encryption.

The following code is in charge of decrypting the strings using XOR operations:



A Python version of the decryption function for POST requests is as follows:

```
In [1]: enc_string = b"\x55\x3F\x56\x1B\x56\x3F\x4D\x1B"

In [2]: key = b"\x05\x3F\x19\x1B"

In [3]: dec_string = ''

In [4]: for i in range(len(enc_string)):
   ...:     dec_string += chr(key[i % len(key)] ^ enc_string[i])
   ...:

In [5]: dec_string
Out[5]: 'P\x00O\x00S\x00T\x00'

In [6]: dec_string.replace('\x00', '')
Out[6]: 'POST'
```

The same string decryption method is used throughout the binary.

The string encryption code is in-lined (as opposed to take place in a dedicated function). This new code changes the control flow graph of all functions which are referencing strings. This could break some detections rules based on patterns recognition such as YARA rules. We thus recommend to double-check your detections rules for IcedID.

Retired features

We have also realized that in this new version, the SSL-pinning feature has been removed. For more details about this feature, we highly recommend reading the report from Group-IB on the old version (https://blog.group-ib.com/icedid). To summarize, IcedID sets a callback when it sends data to a legit server (mostly to aws.amazon.com) and it verifies the checksum of the public key from the server's certificate.

As you can see in the image below, in the old variant when the set_bot_information() function is called, the result of SSL_pinning_feature() is passed as argument. However, in this new variant (since the feature has been removed) the value passed to set_bot_information() is hardcoded to 1.

Old variant

```
decrypt_cnc((__int64)&v12);
SSL_Pinning = SSL_pinning_feature();
botinfo = set_bot_information(v13, SSL_Pinning, (__int64)&v11);
if ( botinfo && cnc_comm1(&v14, botinfo, &lpMem, &v16) && v16 >= 0x400 )
{
  v5 = create_directory(lpMem);
```

New variant

```
botinfo = set_bot_information(v12, 1u, (__int64)&v11);
if ( botinfo && cnc_comm1(&v13, botinfo, &lpMem, &v15) && v15 >= 0x400 )
{
  v5 = create_directory(lpMem);
```

Searching in our telemetry for IcedID samples , we see that the most prevalent URL among all IcedID samples was aws.amazon.com, due to the SLL pinning feature.

However, if we limit the search scope to the last 2 weeks, we can confirm that the aws.amazon.com URL is no longer used:

```
threatray-lab> python3 check_url_prevalence.py
TOP 3 contacted URLS by IcedID samples last year:
    http://aws.amazon.com: 8070
    http://calldivorce.fun: 3163
    http://tvorartificialnature.xyz: 1127
TOP 3 contacted URLS by IcedID samples last 14 days:
    http://keepfootbal.com: 111
    http://reseptors.com: 57
    http://hdtrenity.com: 5
```

Another less important change that occurs in this version is that the function responsible of decrypting the command and control has disappeared. In this new version the code of this function is in-lined in the main function.

IOCs

02e58a9e73e314497356a4d420f83584ccb85d49edce98a36f9e738b85ca637f
03a41a586c17dd1bd79aa20dfa9a0b1e11d8b0acc21d687bfc3953baf8907a86
03c12545f5dd6cb2a36fcc6da5184cda9259d71f2d12f537cb916a7029654330
05e15f807b0e89e6af4c42a38ca8100ce0064f63530abad455334b31a2a69c88
05e4a3ef8a29fd09f10e500acf62d628b77b2719b5664a011e66811af6509a69
0990cb15328b1784aa0338e5f21eaf771b2ec1a6b0ac16d30d94c30e33741312
09edd4cda6f4dc5bb313570bf5c206b3691f4453d15bf742460cec8c0d4aff7d
0d8041601a71723fd9a41e1350cb8baabd9a690a26f12723bccc8a91b461245a
0f5fbad82dae02e2a48775762f8ff0eb067eb4f81ce637607ac893d4e0c613b3
10a841e167daefdba33ce9fd8e5f3b0c2a30c1e3c37f034c0bffdbaf97a5db5f
134774292f7745f4b91b833735e03c6b8e21197606511b5b1bde965e9cb3f515
15f8da5acf0b2b3e7334ef9d15e290758fcc918930ca8be801acc7682868b91b
18cc18377e2fef33c4ac8f700a15889def8d7965149033c9cf80d7499e966942
18f8c27d91db287a18034e39a2df2e4e3ec9755d4067809b37580859c6a8acd6
1c5467229ec9eadb6c9cdd09d4f69cdbb31906605af609e44505383660ba2f31
1c86607f8145c0c20c4b6345223a8ba0a8f7c31f0e6f952d5baa80ff776b676d
1d371ef854dac871c335d8ad1ba2f3d7916fc449e6383eec9196c117930c4d98
1fa43e3a239c517b2af4fbf9cd176b7ef8282d82f6f555917fefc64e4c9cde30
204bcb9f2278761c541c5be310382f02e21a7b83d6944fb619abec110063dc66
205e180196d948fe19ba8ca04d244f505b667af92e8e85ee05caf61c39e38510
23bd947bcd5946b8b7c985562b6c866b3f573f26929726ec2b24a793d9245639
24a6327b7913db912a1c22fdacc0c7148a03c1aa04ee8e67c5c2f63f894d9fef
255fedca93d25a470f2b59ac374249bf3f8f5325815a7e82a5c2a63cc08f76d4
2c4ebb47841760e94ae3f6f26e9ffe4cc7e933d618b0721e6dce5da6f4595122
2d48d620321ed65bca7f16330d30d8658d8046cedc89c9135c2dfee88316267f
2d7c3f733948bd01e428e517b84eacd96e816ad3d181db27c13246a22dcc03b4
2dc18df6aa58c8646823c532debd0522e0cda5bb113b02caebadb4489ba48ce4
2ebeebe48a1bc8541fa769187fef1214b5855e8979cd902b21b792c57cbd808b
31597d65343eb5ca523fa81dbe4331d577d5d819f60f3aec071b2fb7eb9d01e4
31a5ee81cc3206f30e6bc62e84ec89e9aa35e44b52baacc8955aa68baa0a093e
3215a0502c123bd08d9374e2508d79adabcb36e3a3f5d7cd87a97d616ff9c601
33270eab7adb83b72240a9546d6d310cbc692d4ef102b7136042165b1d95a91a
3388b2781e84a2fdb1d37e5ee1371af605fee7b70e16bd7b57ed8025db2447b4
358679a5aa1ce479cc20c624d3fefe26170b3ad052ed9aa8111bf3047c755ee2
368be300f148a956b017cedac10721e64f8030499ea3411db6519a8eeb68d43c
374c7619257b545ac83cf1870f50f38066c5ded225c780af28cb8bd8c8c80070
39b49f2c3d6cfe9c1064086116abe323d1eb59ab852099dbf9efaca81f662c5b
3adc2160c304c344f6c1efcba1b759af3cc87b85376535b088adb15562aa0254
3c4b375de8b20a9036c3ac9139855f312bbcbe8b3e869b36ebfbf2533422a06e
3d1ec1f66ba4a30aac55590ff3d120ae22e345685caa916f9d1c74592c98f0c3
3e3c5d318ed1a4dd83cf0dc9279d82b5dffa7181f2b650d24c61b1a008d6d0f2
3ee0dd7a2c2d122790e560a535c4a3cc8a11da78df15cd5d4da461797d1e48bf
407baf0c60024ff01e4d2128264064eea5099c33efa6688362ff38e0ee97fbe2
40aa95077ab694181272d48457920b6ca587c9b0752d8752940840e620039793
4528ee62b7c2b479c32b2b401dc875bca1d7125f2206b083d7c3595fd827f839
4aaf857e59a25f98e133aa59bac419b22a60ecc4dcade883bf217ce76c25bf84
4c40fa74b961f90a67d2780412891c49f0a2919b3e90a216daa5f5b12187e219
4d0aaf50b254b52e403a2d613d1aa8ab4b1406f7658db03710cc75752e9c6e01
4f6cea3ce429ccdccee1a4e014cebcfa971e8a2ca8332a68239a7940d7224818
50165bf93643c3ee448eb480217442f19567918b7ea98722bb404e7fea558a2b
515ac55d2575077dfc2f50273fd5e52652d17ab6fcd7bb7b23ce2dfbb3685414
53ea999f28add82bb8d70aa9e030893521bf57a08a9564ee7380562142734fd5
54d334b0b1a89677c22dc5490780f3c3724f9b4d6113eca073a241c8921b5977
55a33e1bb55138d85d229f434fcea0b0b147a98e4beb3ce1860b00e8137467d6
5753cb2ece6bc64d950641a48a3c38335c8dd738e7a30f50ae8fad4e09d55914

59a3f3eabe6eecff8b254cea75dcdd898d7bd6886da929f85ffcddaa287f13e4
5a07bc16a6c1039b8f45bee3738abae9b22a109efdfc4dc64366a4c1f7367a2d
5bb3dba425e01da86ccda2e90f343a52690fb687e18ada32624179557498228e
5ce84f9baa96f6b2e854221f8ca9eb3e1b4c00ebec90935b0cbd2640140974c0
5d17794aeae5d5352a7579454419909d2339c51d57b9e4a4e1b77e034d291f22
5d83037ac01f286e920f6a16bf8e158945fda752d6b841031af85e8e778dd5b3
5e9b1bf9407a2baa402451ae8d9a7ffb1fa3ea990bd5d0674756982bf9393b65
5fd948425254ca242b37cdbd9d6d4782683fe31ba08a65053e9b273ffea343c3
60626638547c49bb876c132d0aae3d728c47952ad0da46da64a785e3862d05cb
65519e29f8bd88a50558126c0c2a38c7fdf3809e76624a2efc9d8e2d48aa0937
66a90194dd80475dc2c18ce5884bc94979747aa8cd5f24a4b971d8efaaf59426
66e3893430e6f89b5f0d7d14f113fe60bbe2e3da15b42ec8295fc52579f7a453
686e36a4e3f6dcb113f0b6b54bdeb7574a7e47bb4b6a8341629d8251e022e197
69b59c6263ec89edf585edca4e4c1af204d8b92603cfa6e7c8a02d2361aba147
6b6195fa5809045ed7d27cc851832bb6272941549b69c22d09228531a0ded2db
6c1fdedbd252fec4e35422d639a2bc2256701d4e2569122e3d0940c898adfcb4
6c46ea476eea3b54d7149947cb99424ddfbdc869b527f6a69815c5f9d42b43c3
6e46958960f575bfdc14a3da83de4249ab3f23f834aec3d2b5ca8891f9c91bc8
6eacebaa6b9457c95cde935110876fde8bf1e6f7f43a9276fb9a8a7e09603ba2
715c11a153cbed9ace1618a36142bb7ae2cdcd7bcae3a69161f796ace5d857a0
7215735224ae5437685e0465c36eb8a3a87a3d86e4be0763cfdc06820a62a184
721aa0a8007454b99c90306180c89ef7fc61d85f53e17fa8e3197508064d8d9f
724c4d872ad8a538edfbc55520d27e4639474cdaede5e6f67ccbe5e3477a8912
731c19a06f31328d7336bb50c00851cfc7ecad87159f3277a9729bec4f9d4a53
73c3395e7ad9787595df98570420d3cef4585d02489b1d30f22685e9c1760ab2
76c1e9298873358e28f93977eb97350801937187519ea63fbbb8f8dfe1ba52fc
7c614ec8c5341386f2c98dbeb0aeecdff35a9438c9c80b5942e81b22fc0641b4
8037a59ce1465fa74b2f440eb8eda65a55cab317afab76af725ffa6d6d142ad4
8236ead722c2bc40ad14cf3ac8ecd6d647c415cbaed4b48cbfc4f8ffbe19d761
82a7fca34437668d26a6b1f815986ca4068d63fa3264e8d8f6ab623fb2ffd13c
8368b23494628423416a81f57eae7349edf38128caf92c873143b75e8bad1eb3
841c94ef717b5fd39ee1bfe6cd80700080174b598376a6a393d0d36cac777f13
84629a575a4f2eafd30e86d07663cabd247572c09d7c6cc251bb5b5a641875a6
854dd9d16fd46bec4a6b03a51752275df79906fea15c5cd8475da1814f0bc37e
85f8aaa9aecaa7ddbb2dd10e3fa620108d26573af0aaed888ad51aec0763f8e9
861cad69153a30f93456e51801d933385f0e67b09f0aa55977990fd38102276c
87e2d2769c11ca86553d1a83483b33071cee53a2097530677bf0c56c74d9e19f
87f4e3af806ac0ec376b1ab0235a15b203d19489b27049144f2697da6df29a7d
88234568ba22d7676e0f57e2b910e4a84360849aa660ffada104186a41dabe71
88c376b943a1855b006605b1ebf826eceb5334ccea81bf18a53f4fc70c1645fd
8d4462edf5b928a5817dc59d583ac925200b3621d060a66cc237ad972bdde8ce
8ec2058763207a52bf912bbf9108ad5c134f7991d54267a144d66c10adbfa261
919c627af8b1d832aee1ad25de3d1d99c0a04221bb5bfc8a7c8f095b1346bfc6
92243763637516274579f2b9b5f37661b9805ef6be95b56e5e91b619f9b2ba8c
931c900905566bab01a27a9b7722a3dcc0cc5fa9e0ed513486ef6e964ba57a7e
932050cb69306213a3d0c1893a6df1fc23ac41a7890678d24021f3f2297a8855
95e0888ca69ae02606b68b6fc684bcdd6c9e0e74a53394bb3f80560507b599c8
964bb12c1e9687ab7408dc02e953c27a419187c4310ade1b3a0b35431519f142
9717fe080058d75aee1cb2406204052e5ac5eb0b30bc988a34e7c817cc24bb65
984531c88100ca2ab139fc11d6988d596e9e1c511b06335baa9a0c40abdeeb53
994d028748ec7e65004548526394de9df0e5ce0a0c22232d9fdf844b85194616
9a3d9a2da5d2386936063651536881577ff58e0dea8d509ddfe36074096d715c9
9cde570788d1430d0545b727963a85c0da7f492e838e43b3cf8b6a1fc984d798
9ea309f425c3cd53ce0302eb33543d5f9a0c7956f3ed58845ded88deca2084ca
9eea1a5a74e2c7d41871222410d9d337dc76cd973dd3fb0dcde89514ff83c219

a0b8e020ff671176da99897f3cfa35be9206e46e3d7215603aa09b091ef4db57
a3d512f6451ce214e6207edd59d37ad7dfead333094a04ddab9c181472f25742
a3e0a9973a4abeed587070b3c052a1ad1809b0db7de2754339dea4616d87d2a9
a42e2b5a0b758b189d51dcb2b5093d4b9354e88209255022cd1119afe559aec8
a45c573fce0d03856894530561c1370615fa4daddd13da76147bc7ce447c3c3d
a5e2e629255556f9324623e86f42a87ff429cd4497269b2abd214dd39702bc33
aa7d12fe99100805b6970a01b5abf8e450d719245e0dc5da370bd1e624a7120f
ab8ba737e560a257fccb3dbba1fc341d0002d877436720846270be0fc0f2b68c
abe63be5854813b62f29876a2480cb2ed1eae4d9dcd51596390b62c2befc0988
acede4e871ff7ebeda48cd568f8761e7129ed6f596cccbbdce7634e58ecbd7e8
ae3038147f454d8099fe12c5bbdf224f98574fa11f65f932380e039bb16ec1db
af35fd57fa3d82b26f3e99136089f010be9ae75259a50c3cb8b354a18cd55d17
b0788325664cd57b0b83cfe756db012120c91506643c26f0e3b2982fe7a3ebad
b11e5dc72111b371e57b8afee104020194517e53263a9f2c2d9bdc8f9bc1dbfa
b1fa4853125c6fbfc38553076e31a3dea62ab066f8cc1f609803a8b26e931a8a
b274567f9238e94357355cfd4e95acc0f9290c0c88c43438e985c299308adebd
b38c9a3fd842f23694bddd6c3d31a99edeb09a8e46f38415962fbfd364694b39
b4aff3da5e0e59bfe2f1df0f966860b4f0e31ba202b6d8e1dbd7eaae4327ae7e
b6772a7ec2ea28d71f5ee696e6d671d47a4ea9ad1b9dee191b476a905d7f54e5
b7b2cfde39268af729c507ff82fd9b20e5dc2abf0d0506c129053d7cc262dfb3
b7f346ba20c63c83ba8a593e2a64e957cfc1e4104c5ba62630ecab330ae14ed2
b8d794f6449669ff2d11bc635490d9efdd1f4e92fcb3be5cdb4b40e4470c0982
b99b856b0401ce5cc085e2c5b766662ae77f9b8e37a4b191b8280fef1e6c27f3
bc6a441a3036c1310886b671943e487d47f2c7d1b4bd125d7b0cf0f3090b8281
bf285da82b9ddcb61db82e40163832eaa0f77657a5fccabb46e6a2b89b06f854
bfde769562ba97b4e1fde1eb26eb5c670a13154f8a5b6b479b710ca239aff559
c164fc6d2c20cb05925a4d50e56af6ce3d2c4c9fe95d8cac52e8f8728e82395a
c1b3b057acfd3ff79d59523d30affc3d4269f7856e8bf45c7289a5e095d100a1
c2561a8ce8729d8d6f8066946b215f07c83bdb542a3b55009d69a57220e3339f
c2969a902dc2c2eab063dfdf50c7bcd56f9ce989045dbe41e0d9cd546eae6b30
c3fbbb5fc9699a1e48dcc8e9ff6be63a35936f9f3f203925978cb822e0435a63
c5bdcc6a758d9810226e1012a8aa8979fa7fc6205e162d136ae5399065a9a075
c662f5b2ddfb067058c5e4bfc726fb86f3543c6ae4fe160b26915498dea6f9aa
c6765b0c795af907637ebc5e0703a285b44041e96d43e81922f8601a2346cafa
c8d02f7bf46941dbd67761d30c12585033bca9ca34bf4bd02d8d3fe13b313fec
c9ca29ceb1a3a2e5e10b8eba5723222b119c9e51dc7ab7b195d16b505a29d896
cb2c71f81a2592f38bb78ee7d6c62d399575de75f51ecdaad6b33003615aaba6
cb3cdb8eb96570da4c544533189a73dcde533e23380ca8a51d0133eab9f0bc16
ccf86807e7b572efee1d4c631744fcee4a44699a236927e46a5011188e9cb10c
cecae728ae8fc29506d18ee4ba8f7ef68ed45d1fbff5273ea3e6c1f636173c1a
cef57bfcad0a3fb5a756d0dcf329f3135ec52d1eac2ec33d8ec94d81b5e92877
cf004c6d421b104f80c2076b2ae28f27c065da7e61317364c0daef85d4ac7136
cf961cb072619763a6f2594495b7941d11c634147324b267e958edaddd77936e
d5cbf1579a017a587c69df1c0ec1bc5a29d0e252244998f91701c776d63f796d
d6dc8d8296b85b1b802e430f48e4e8580261849591980fee8cd534c622942de5
d70865663ae6ce65571200cf5e3148ca65ec06ffb3802453b78d3e112b10b386
d757eb59003c4a7df43e64d5aadaed7a2d5fde15570511ec691cc92378253c44
d9e26a194a1ff7d1f2b2659b3b8e6793e1f185633d4c6e17c81171e1d8f7c067
da965e128b7810b230cec8880cb38416287f8676e88cacf7d86847865258a6d6
db5378044d9ba78de9668c5e6320b6fed0ab7efe61191b8c749a351ebea7c48c
db55ce99250c1cd4c07bba00172845d8f46b3246a2d63debb02b058e526ff14b
db7a59b74dc1b3734723488d9b6d67be932c19d5e8da155f634f221e18d74524
dc259fd862a143d4817de17d30f16ed2687929e73f387e9397415fcc74007821
dd1a831e9da418794a92c7061de920eeb741edb4774334d8c8362f6c334c884c
debc8996917f9ea29356644ecd8945aceece8c44120730acf657afd64b02dde6

```
e1e9e84a24abaa8658d8715d32e21ed51f1c548123155f4c88bbc8722eecbfbd
e311aaaa543d6c2f87bda69ac2d15a657a6fe8dfbc01e0571a8038c4a54373ef
e48e313a540cb86ed557b3041fdf4b5a95327d00e1ae1210cf10255c97720b11
e5a5d52aa887812801789ec36413abb9ab204c79d2b9030a6f1605730133db3d
e761c5d96f779f5167df24f0cc72e33e5e849f83f1ff1572b9b11301c78346fa
eae80962a4e2dce1a1cd5104dc244b04ff4a852b5c3232c5dee7749500de87f1
ec34fa7adacd8f11fc8efe29f4d7115fd2e7688e06b72f66043f9c2c4a1e5d64
ec7af4291bcd47e2f7776a4332fd557f2ec54b631988ae3355d216334b43cd69
ec9be4c081747bc436f9214d7af6693b43ef7c7af9cf6074c973b00efd34425e
ee8b2a0c8774b2ecca257da63053a9bc84ea4aac39026c53e6efcc56e99a22c3
eece4848cd49ca360335e44c7f8febb42349649885fc6a945f97ed09e79081f5
f1a6ed4877497aee8f121b7cb20768859bb785393d5dc91d1b2470408e7d3ae8
f2e08df6880d599f89c5b4d5497164ab4489e79c233555c53031a90b02d11f51
f4b871a9b2e0b43dd82576d80d178048c95d62876bc8c832f5d874f74e830336
f4f4d7a9d1fd337b7a6d298d7d7271ab8b489c5304b871b1e8d8f1f1719198c2
f6d6f68c4d97dd4270d909c97712cc4ce1098aecc9821ef8356e38cdc7f12b43
f874e0c5e423b8dcf3ec9bc74de93af2cd4be092a7ea73859c777685e411f37c
fd61dbe6be6c33deb3f372cdf279641d97eb6836ca1d55827b649a1268d3f3b7
fda95dfc80c40b06dd680dd4bc8c57e989e1ba9cf36ea1d55ac172bdb0367fb0
fdae004e66cf3dee59380f06e27f286fc5772ce658c9e1765867c07a6fdd131b
fef2172e461fe90ab99dcb0825d7de72ae6bdfb9b2be0838f13fb7f0b4566cd0
```

About Threatray

Threatray is a novel malware analysis and intelligence platform. We support all key malware defense use cases, including identification / detection, hunting, response, and analysis. Threatray helps security teams of all skill levels to effectively identify and analyze ongoing and past compromises.

At the core of Threatray are highly scalable code similarity search algorithms that find code reuse between a new and millions of known samples in seconds. Our core search algorithms do not make use of traditional byte pattern matches and are thus highly resilient to code mutations.

Our user facing features are based on the core search technology. They include best of class threat family identification and detection, easy to use real-time retro-hunting and retro-detection, cluster analysis to quickly find relevant IOCs, and low-level multi-binary analysis capabilities. Some of our binary analysis capabilities have been used for the research presented in this report.

Contact us at https://threatray.com/contact-us or https://twitter.com/threatray

Freddy Dezeure

Freddy Dezeure graduated from the KUL University in Belgium in 1982, with a master of science in engineering. He was CIO of a private company from 1982 until 1987. He joined the European Commission in 1987 where he held a variety of management positions in administrative, financial and operational areas, in particular in information technology.

He founded CERT-EU, the Computer Emergency and Response Team of the EU institutions, agencies and bodies in 2011. Until May 2017 he held the position of the Head of CERT-EU.

Presently, he is an Independent Advisor in cybersecurity and cyber-risk management and he acts as Board Member and Advisory Board Member in several high-tech companies. He is a highly respected keynote speaker and is very active in the cybersecurity community. He is leading the EU MITRE ATT&CK Community.

@FDezeure

https://www.FreddyDezeure.eu/

Mathias Wegmüller

Matthias is a highly accomplished entrepreneur, board member and investor. He has multi-year expertise in digital transformation, facilitating the effective execution of digital engagement initiatives. A passionate, action-oriented and motivational team leader, Mathias Co-founded Qumram in 2011 and led it in different roles until the successful exit and trade-sale in November 2017 to Dynatrace.

Pierre Noel

Pierre has over 30 years of international experience in Information Security, Data Privacy, and Enterprise Risk Management. He is in charge of the nation-wide Swiss Finance Service cybersecurity information sharing program. Previously, Pierre was the Chief Security Officer for Microsoft, covering the wide Asian region and the Chief Security & Privacy Officer (CSPO) for Huawei Worldwide He designed, built, and operated complete Security and

Enterprise Risk Management environments for Governments, Finance, Transport, and large conglomerate industries over the World. Pierre was the advisor to three large nations in Australasia, working directly with their ministers or presidential offices in building nationwide cybersecurity & privacy programs. He is a member of the board of advisors of Airbus Industries and also sits on the board of several established and start-up organizations in the field of CyberSecurity and Privacy.

Thomas Dübendorfer

Thomas Dübendorfer holds a Ph.D. in computer science from ETH Zurich and is the president of the Swiss ICT Investor Club (SICTIC). He has worked at HP Research Labs in Silicon Valley and seven years at Google on security engineering projects. He is an angel investor in more than twenty tech startups in Switzerland. UBS, Nasdaq, Lufthansa, Adobe, Swiss Re and many other highly ranked companies are customers of tech startups that he co-founded. He was honoured as “Top 100 Digital Shapers of Switzerland” in 2016 and 2018 and as “Top 200 most prominent persons of Zurich, Switzerland” in Who Is Who in Zürich 2019. He has published a paper on Web browser security that got downloaded more than 100’000 times and that proved Web browsers with silent security update mechanisms to protect their users significantly better from vulnerabilities than others.

Peter Stalder

After studying Computer Science at the ETH in Zurich, Peter worked as a software developer, system technician, consultant and project lead in multiple industry projects. He was the CTO of Finnova, a leading banking software in Switzerland, for 20 years. At Finnova, he was responsible for the System- and Software Architecture, as well as the development of its core technologies. In 2015, Peter transitioned to independent consulting and now supports startups with his experience.

Ariel F. Lüdi

As the CEO of Hybris Software, Ariel was instrumental to make Hybris become the global leader in omnichannel commerce and the sale to SAP in 2013 for around 1.5 B USD. Since then, Ariel is investing in and coaching innovative IT start-ups. Prior to joining Hybris, he held senior positions at Salesforce.com, BroadVision and Oracle. Ariel studied Physics at ETH in Zurich.

Jonas Wagner

CTO and Co-Founder

Jonas is founder and CTO of Threatray

Jonas has over 10 years of professional experience in software engineering, with a focus on machine learning and cyber security data analysis. He holds a M.Sc. in Computer Science from the Bern University of Applied Sciences, where he spent years researching and developing the core algorithms that now power Threatray.

Endre Bangerter

CEO and Co-Founder

Endre Bangerter is founder and CEO of Threatray.

Endre has over 20 years of experience in Information Security and Cyber Defense. He has been serving as a malware analyst for the government and as a technical consultant for Accenture and IBM. Endre has rich experience in developing novel IT security technologies gained while working at IBM Research in Zurich and as a professor and lab director at Bern University of Applied Sciences. He has a Ph.D. in IT security from the Horst Görtz Institute For IT-security at the University of Bochum in Germany.