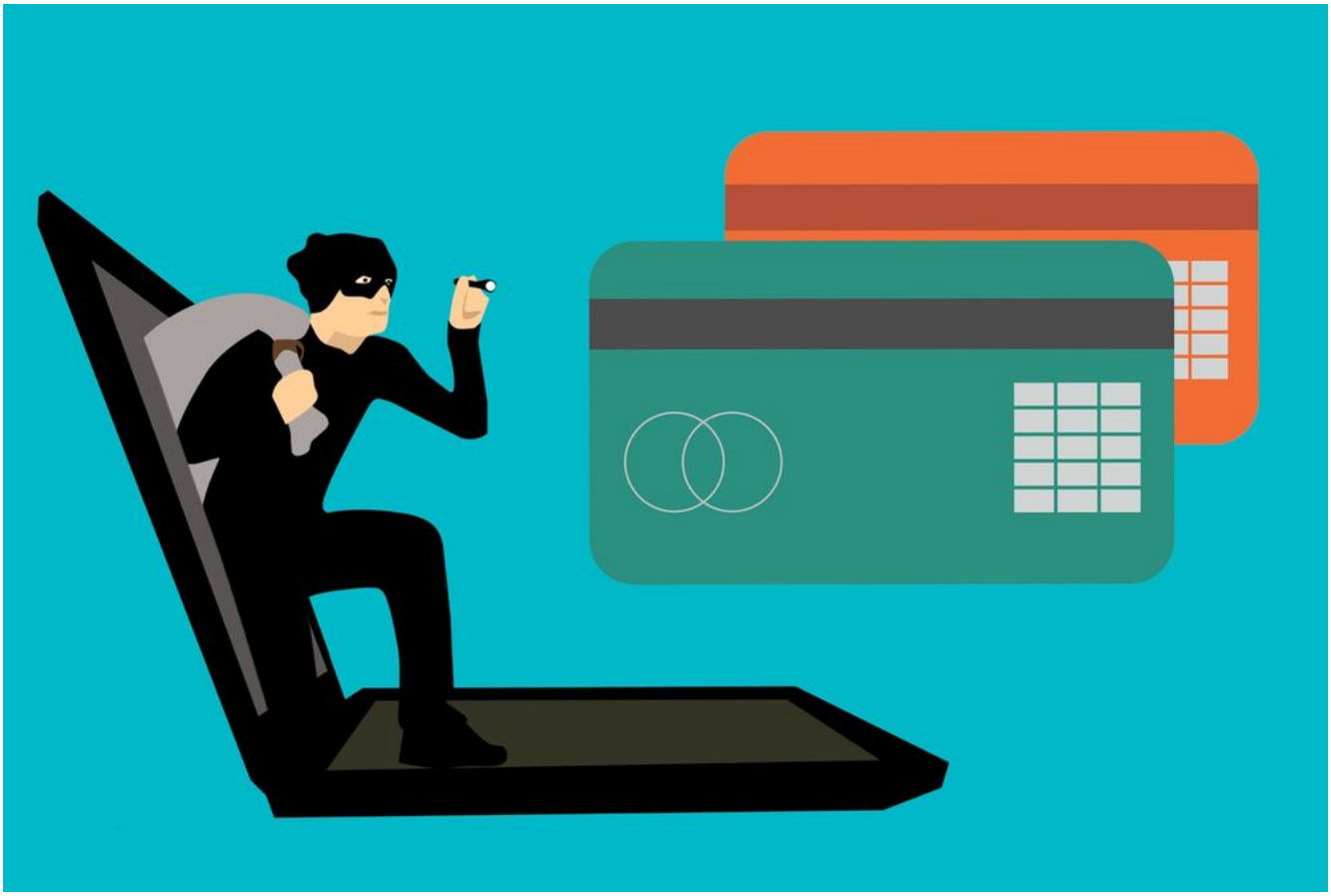
Apps on Google Play Tainted with Cerberus Banker Malware

labs.bitdefender.com/2020/09/apps-on-google-play-tainted-with-cerberus-banker-malware/

Anti-Malware Research
6 min read

Alexandra BOCEREG
September 24, 2020

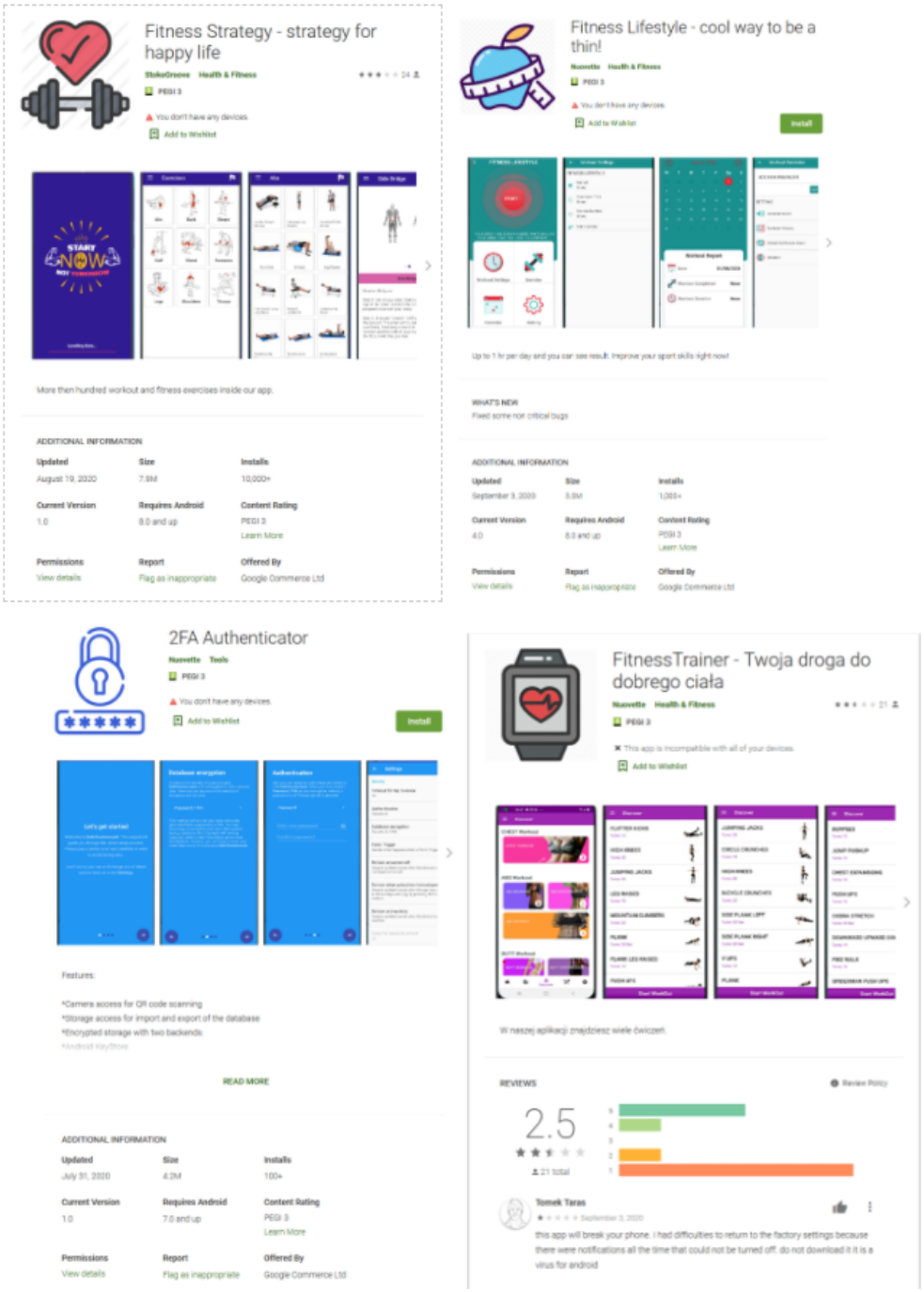


The official Android app market has traditionally been regarded as a safe place to install applications from. Every once in a while, remarkably malicious apps slip right through and start wreaking havoc before they're spotted and retired.

Today's blog post focuses on several utility apps that look innocent at a glance, but whose real purpose is to download and enable various banker Trojans on the device and lend hackers a hand into emptying victims' accounts.

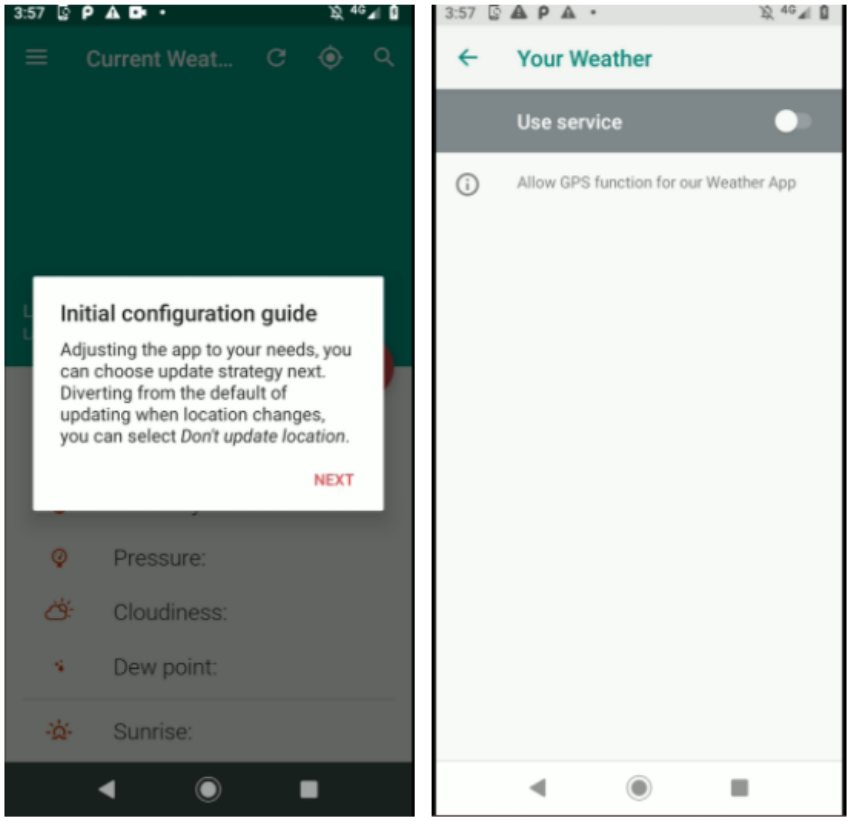
The apps in question were spotted on Google Play by some of our machine learning algorithms. The apps belong to different categories, but most of them are marketed as health and sports companions. Their presence on Google Play dates back to February this year, but the most recent ones were published just days ago. At the moment of writing this report, several samples are still available on **third-party stores**. The apps vary in popularity, with the more popular ones having been downloaded more than 10,000 times.

Bitdefender detects this threat as *Android.Trojan.Downloader.UT*.



Behavior

To some extent, these applications ship with the advertised functionality. However, under the hood, they communicate with a server and, if some prerequisites are met, the server decides whether to allow the app to download a malicious APK or not. If the APK is made available, the application will try to lure the user into granting it Accessibility rights. If the service is enabled, the app will install the payload and attempt to enable the payload's accessibility service through it.

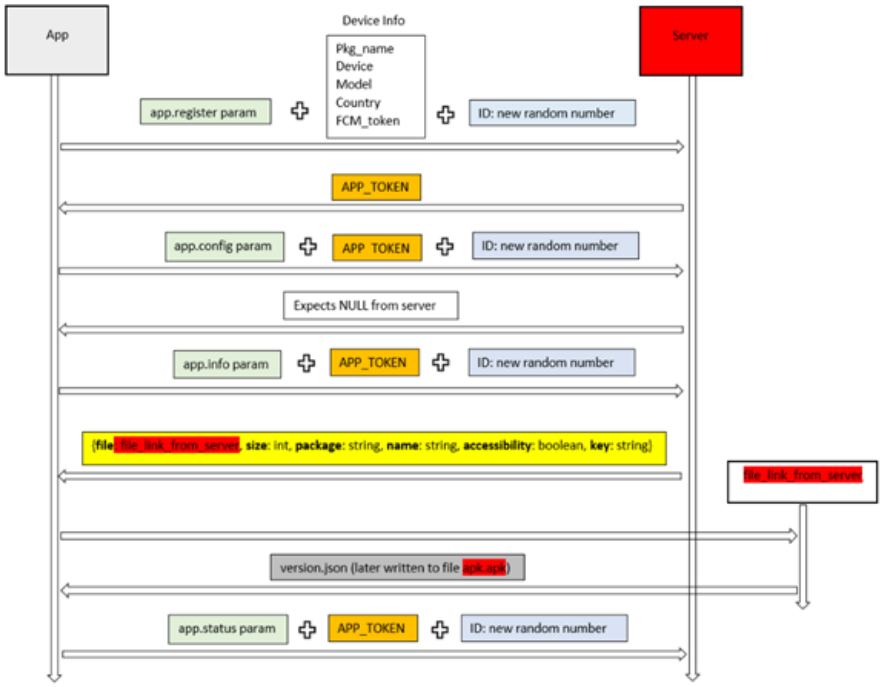


The apps have a specific way of communicating with the server. Information about the device (such as the country, the package name, the build version release, and the build model) is sent to the server as an app registration request, and an app token is sent back. This token will be used in all subsequent requests to the server. Depending on this, the app will receive from the server a link to the APK file to be downloaded later.

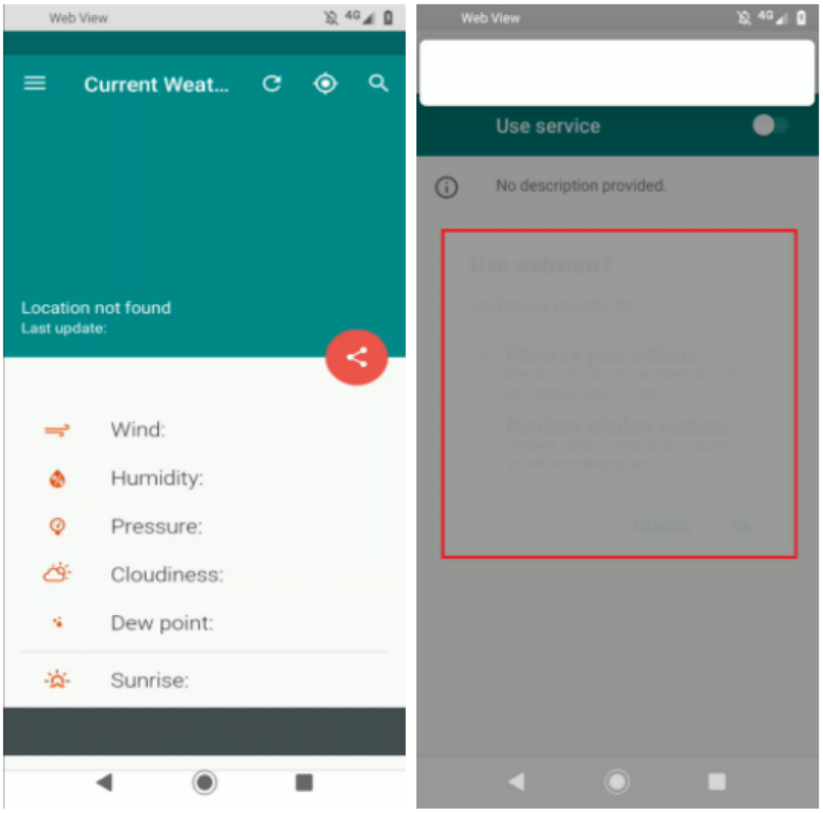
```
{"id": 1234567, "method": "app.register", "params": {"package": "com.yourweather.app", "device": "Android",
"model": "Samsung Galaxy Nexus", "country": "en-US"}, "jsonrpc": "2.0"}
```

Initial request mock example

The same CnC provides different APKs at different times, possibly due to different configurations being sent to the server. We conclude that the malware authors might have a selection process to determine what users should get the banker or when they should get it, making the downloaded APKs harder to trace and even possibly target it toward specific profiles.



The initial apps have the sole purpose of trying to download the payload app. After the payload app has been installed, the original one will enable accessibility services for the second app. Interestingly, once the downloaded APK has been installed and its accessibility service is enabled through the original app's accessibility control, the latter will disable its own accessibility abilities to avoid raising any suspicions and will continue to work as described in the application's description on Play Store.



A new app can be seen in the background of the initially installed app. It is named Web View, a generic name set not to raise suspicions. This happens for a split second while the downloader uses the accessibility service to enable the payload.

At this point, the first app is no longer of interest, and the second app takes charge of the device's infestation instead. The droppers continue to offer the neither good nor terrible features advertised on Google Play. It will keep listening for certain intents (e.g., BOOT_COMPLETED) and can even hide their launcher if all the prerequisites are met.

The downloaded apps that we interacted with are various banking malware applications in the Cerberus family. Since they had already received accessibility permissions, they proceed to give themselves all the needed permissions, set themselves as device admins, and even as default SMS apps. From there on, the payload application has full control over the device.

Versions

The apps can be divided into two categories, despite the main dropper functionality being very similar.

V1: com.radiofun.app and me.maxdev.popularmoviesapp

The first version of the malware, which is less obfuscated and mainly uses Base64 for encryption. The early versions of these apps offered a simpler communication interface and even lacked the second version's registration process. It dates back to February 2020.

V2: the others

The second version of the malware. It uses a different obfuscation technique and has made its first appearance in the wild in June 2020. It is stripped of most debugging information present in version 1. Communication with the server is more advanced, allowing for better control of the payload installation.

Origin

Presumably, in order to hinder investigations, the malware authors publish the malicious apps through several different developer accounts.

Developername	EmailAddress	Last Update
Nouvette	mcmillianschmid80@gmail.com	3 September 2020
Piastos	pennishavondaphamyo51@gmail.com	23 June 2020
Progster	nellafajardolysl85@gmail.com	3 July 2020
imirova91	annavladimirova91@gmail.com	4 July 2020
StokeGroove	hammonslarge3@gmail.com	19 August 2020
VolkavStune	jessicapeter70@gmail.com	27 February 2020

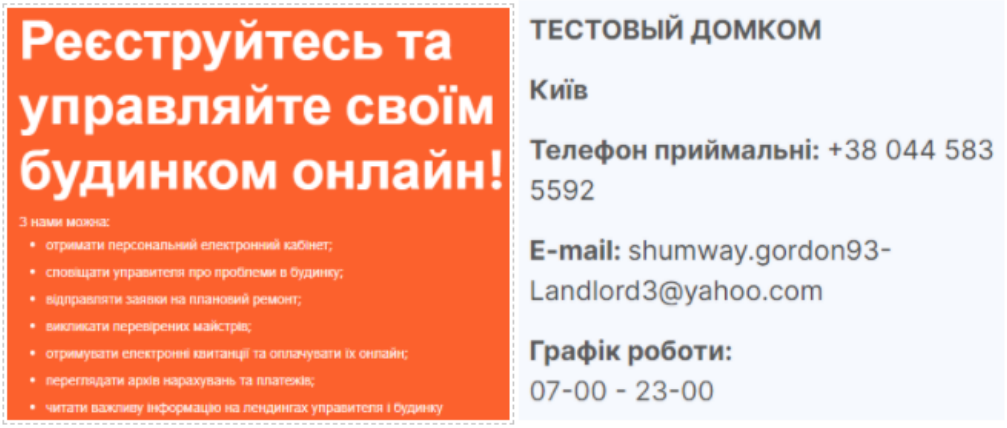
A vague pattern can be noted among the email addresses, which consist of a name, a surname and a number registered on Gmail.

C&C	IP Resolved	Status
vipyoga[.]today	95.142.40.68	UP
weatherclub[.]club	185.177.93.242	UP
downdating[.]club	185.177.93.32	UP
positivefitness[.]club	185.177.93.72	UP
loversfinder[.]xyz	198.54.125.121	UP
yoga4u[.]xyz	185.177.93.120	TIMEOUT
groovefitness[.]xyz	185.177.92.213	UP

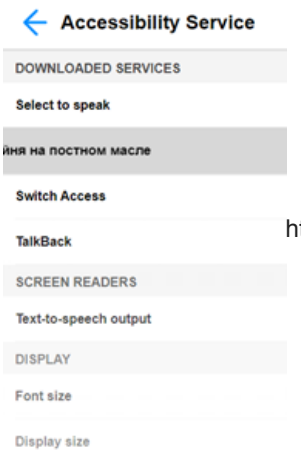
fitnessstrategy[.]xyz	185.177.93.44	UP
safeyourdata[.]xyz	185.177.93.145	UP
sport4ever[.]club	185.177.93.105	UP
2fapass[.]club	185.177.93.111	UP
androidradio[.]life	45.142.212.216	UP

While most of the command and control servers don't have any meaningful webpages available, one of them hosts a work-in-progress site for a home management provider from Kiev, Ukraine.

`https://positivefitness[.]club/landing/news/5f2463e1bbc5c5e5d`



The official site of the provider can be found at https://djek.org/.
Another server, loversfinder[.]xyz, hosts a page with the infamous Cerberus mobile user interface, tweaked a bit for Russian speakers.



https://loversfinder[.]xyz/accessibility.html

Given these pages, as well as some Russian language strings found in the oldest versions of the malware family and the fact that the only developer whose name matches the email address is clearly Slavic (Vladimirova), we can make an educated guess that the authors are probably of Eastern Slavic origin.

Telemetry

The droppers are most popular in Europe, particularly in Spain, but our telemetry shows that they are also spread across the US and Australia as well.

Appendix – Indicators of Compromise

MD5	SHA256
95df249db6c7b745aa42ab362d44bab7	91ac84bfa47d2ee5addb2eb7047f2f21fd7712c4d99fd224c6c1cb4f6e6a2ffa
477b37aa15058e1ac8167de3260a2400	446d44b2e2bdd063aed7c142da54d0bf1e1f145ddc5cb4f64b1de8dbb9b5a117
de0383f0c7a422f5ab24a1ec1ec65aa1	52f5c117e3fff7be71afa0a4c5e53b24c05434599aaad885fbc2d7d7658e69fa
53b5f39fb9e885767cf05270f6ed4286	6243ed1d4f2712be2e02edfb6411e8dc86ebe2c683e9f64462f7d23354a0e1ba
1f1458bf12f2f983a1517c06def840ac	446348a93ad38420f75bbd3ef4fff89ac55593ba8e9015e18df82645ad6fe424
c4e05d945aee3817f23ef52b9de065a7	9c81fc435bdeadb43e0085f2a49ffd648dfd4e0a29295e07adfd72810c326b4c
fa7f5825691eec7f9537fe91f3cba895	d1fb03695028dcccc23ea0d7562fb1e412ba7f1682f1288ccaa8c3a44ac44bce
cbf908c23201161e25dc93361cd59688	561b0057cbd91dec480999733b12b0d8bf7b173997384147fa7c6f2e830d3b8f
b06379eeb52758ba79bc5a2d643291af	79611be7f48e1c6c0f22a02e9dcd4f95851bb46be61c7c433b3ba645707f2cc3
b75bef4edf4d77d23a785457d3e01699	8d1a2a475f64ec074be71af600b1352bcd0705cb38dea2c84adeaaa39fd6f4c8
1eed680fc539c315278c87b2203442a4	6561f27e20affd1267e3993cc34424517d1704e7a89524c38755e8161674ff5b
38ccb576775c31f969be18fa211c2751	40b6f76b371d69ed4da4493525265f8d005d39bdfc6920e266ed659cac3239e4
d77de174654991a6d2db490206ea4dce	e1793a72cd8653dab70c2a12de2cd4bca6e01c394a6359fc1cd1d67f2302cfcb
51093ded1b425f46669f51a84e0664c1	6366d374a7a189908cb22ce7ab53f7a4d795334ddb7aaf20c45aa64889782e98
a6129e463e85d0ac0ef7764d7f8ec887	121b3779a0bd540eeae5897eac4dd94b0d8fa63cb8cc3023d5a8e914ac827b51
3c5b3611cba54e8898f974ccdda08924	0b04223581f96316df150bff2de7f428964f9050c6ffc731763d6aec78519f2d
3b28c538592bdf493391d85c81ef9757	0769ae906c0cbc5721000cbf7c1307c9007533baa786c70acd2ac1895758681e
96188f92d59863aaad3a680071268ae9	7d22c63ad869de425d353e25c6a24205ff3674c3fc86fb92ad22037a171b0213
17520f6e37ff64fc7d71015e8aeed6a4	d750ca521fe6d12a263e1e5114c7c9c54941501cb070f6e30656e7811692817a
dc234d845bcb5bdaf3a7d7b73d5ea5ad	4ed4edaa979fa129a6c739e492fa58be2cdb9399c8452d1faf10537a9f03aa25
a39304c60bacdf3ac7dd67d371a8d20c	aba7feb1240d4af3fae753d380eebf2ed169cb8c499b11d65f414a374d69c77a
cfb3be26ca038bc78057d001fb0e7d46	ddeada708a939df8bc3fd8bf23ef0d8b7364404e66ba9db4f1c4260f74b610da

ee6d3b2bda155e7d2a2efc284d8a8bc2	306cf08097ec1dfdfdd7c97fd3df3ce43c6c2dd15e383b3658682f41f6d7c53d
ef1e393b2deb59745780b83fbb44dc34	218fc17f0e9d9abb287f07dece10d073a521692c673aa2a24ebbbda49c4df624
fe7a15b4cd8a472c9b146fa9797dd4ec	9a71b14abfbc6ff4d8768dbdfcc3a573cfd107151d3d42f6d6cf11b7d7c699ef
8d6254c0a59ef1c6dae5403d92a0f9b9	196cca4c237fe013a273955c29f712ad07e61f2f5e44242fb336323fe7444371
0f4733a3a188ca0ddf3f730b17b23e20	301bacdc7163c5494bcbd165c3571659175b355c5ef640277d3929ea280e937f
5e355270a4b984bd12e62f1681809169	a830620a6942a916a7cd93409445dc857d239d9803bffd5a489e0d1057c1f52f

Payloads

nohiv.bzi.jrp
pliqlqpfihoul.joyqtbisgqdaclndxsu.igrl

Certificates

0b10b6815d41a238f1738c236c861cdb9f51adf3
422f61466215e0c6a5e4b3b80596d278652923cf
57f6acc0419af4434c3cf165605b40398581d0ae
83b03b43d86af65743a1a39cf20e7df86d056e40
86567aba9031c15a7064df6f7659dd234c7b609a
8bd3096cf26aab9d3d4122988bba3afaa095cf08
8da0b853891edf01df07689d53b281ded88f9db9
9890f3840906bb107ad7b210407964d1b7a7c13e
9972bc408a0756bb03bb494447599e2bc934d69f
9ca53fb35a5ddf3e2a4c14c7c636e81db8d6ccc1
cdb7cf5f21f2387f3c6ebac6c201cdeb2ccf6f59
d6eb62aef03a6f99213db4c859572c28475dfa32
eaec062e6af9e5282fc6f2bc8fb8f55f946a921d
eeb16846c4bbc9ba57f238aeb3b22694694bd1e0

TAGS

anti-malware research

AUTHOR

Alexandra BOCEREG

tware Engineering. When I'm not