AZORult: Now, as A Signed “Google Update”

blog.minerva-labs.com/azorult-now-as-a-signed-google-update

- Tweet
-

AZORult attackers continue to adjust tactics to increase the chances that they'll evade detection. This malware is a common information stealer, capable of exfiltrating a wide range of sensitive artifacts from an endpoint, including files, cached passwords, and even cryptocurrency wallet keys.

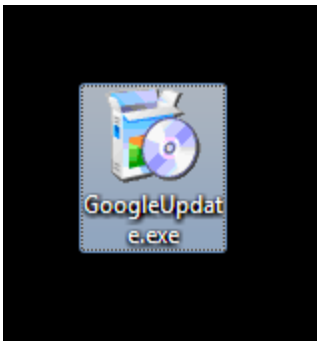
Since Minerva's last post about a highly evasive AZORult campaign, there were many other reports, describing AZORult attacks successfully infecting hundreds of individual victims in a single wave.

Most recently, we observed AZORult using additional tricks to extend its ability to survive in the wild Last month we protected one of our clients from an unusual AZORult attack that involved a signed malicious executable, which the adversary used to increase the chances of successfully bypassing security tools. Below are the details of this AZORult campaign, to assist others with detecting infected endpoints and clarify how such attacks can be identified in the future.

A Suspicious Signed Google Update

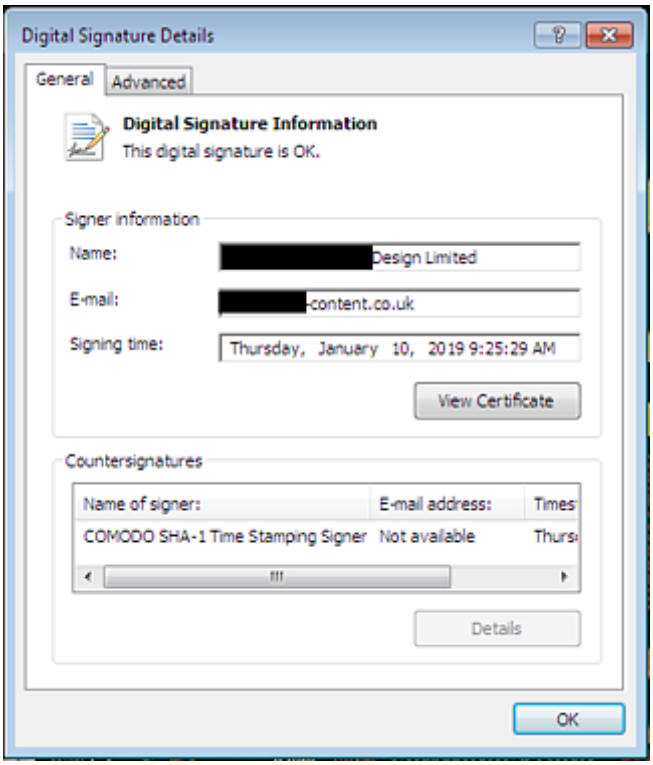
Our investigation began when a Minerva customer contacted us about a suspicious executable that Minerva's Anti-Evasion Platform prevented on their endpoint. The customer was surprised to see that the suspect file, named GoogleUpdate.exe, was digitally signed by a valid, non-revoked certificate.

The icon of this malicious file matched the legitimate updater:



The icon of the malicious Google Updater looked just like the legitimate one.

However, the certificate with which the malicious file was signed did not belong to Google:



Fake GoogleUpdate.exe, valid signature – but not by Google

If we're to take the meaning of this certificate attached to the malicious GoogleUpdate.exe file at its face value, we'd assume that the signer vouched for the legitimacy of this file. This does not mean that the file is benign, although some users (and even security products) assume that it might be. The certificate authority only verifies that the details of the signer are legitimate, regardless of the safety of the signed files.

The certificate used to sign the malicious GoogleUpdate.exe file either stolen from its legitimate owner or obtained for malicious purposes. Since this certificate was issued on November 19th, 2018, it was used for signing more than a hundred different binaries, all disguised as GoogleUpdate.exe (see the IOC section for hashes). We were unable to determine whether the signer was aware of the malicious use of their certificate.

AZORult in the Skin of the Signed Binary

After concluding that the GoogleUpdate.exe was malicious, we faced the task of determining the file's malware family. We identified it as a likely an AZORult variant by analyzing the specimen's network communications, which included the following AZORult patterns:

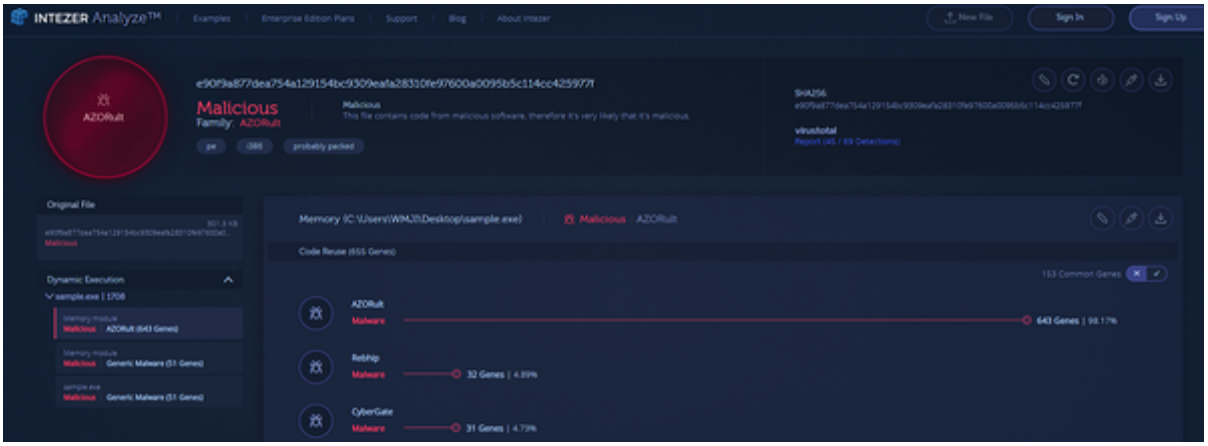
- HTTP POST request to a /index.php
- Using a .bit domain (for DNS over blockchain)
- Typical User-Agent Mozilla/4.0…

```
POST /index.php HTTP/1.1
Host: s63.bit
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Content-Length: 111
Cache-Control: no-cache

...Bp.0p.:p.6p.4[redacted].4..0c.&f.
```

AZORult's typical HTTP POST request

We were able to corroborate our initial identification using the publicly available Intezer Analyze platform, which confirmed that the sample, once unpacked, has an over 98% match to AZORult.



Intezer's Analyze report of the unpacked GoogleUpdate.exe file

A Sneaky Persistence Mechanism

One of the capabilities of this AZORult sample is that it not only uses the file name GoogleUpdate.exe, but also replaces the legitimate Google Updater in *C:\Program Files\Google\Update\GoogleUpdate.exe*. This helps the malicious program run with administrative privileges and allows it to establish a stealthy persistence mechanism.

Google typically defines two scheduled tasks to update its products:

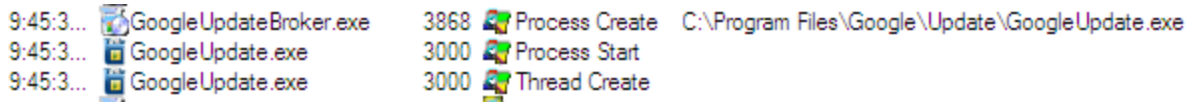
- *GoogleUpdateTaskMachineCore* – runs at login and once a day
- *GoogleUpdateTaskMachineUA* – runs once a day

In addition, there are two Google update services running this binary as well, as defined in the registry values:

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\gupdatem\ImagePath*
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\gupdate\ImagePath*

This AZORult variant does not modify either the tasks or the registry. However, as the result of replacing the original GoogleUpdate.exe file, the malware will run with administrative privileges whenever an update is started. This also allows the malware to gain persistence

that can be difficult to notice, since the tasks and services are not suspicious–only the contents of the file they run.



Google's update routine, GoogleUpdateBroker, starts the malicious GoogleUpdate.exe on the AZORult-infected system

This is not a new technique and was used in the past by APT groups like MuddyWater, but so far, there was no evidence linking AZORult samples to this method .

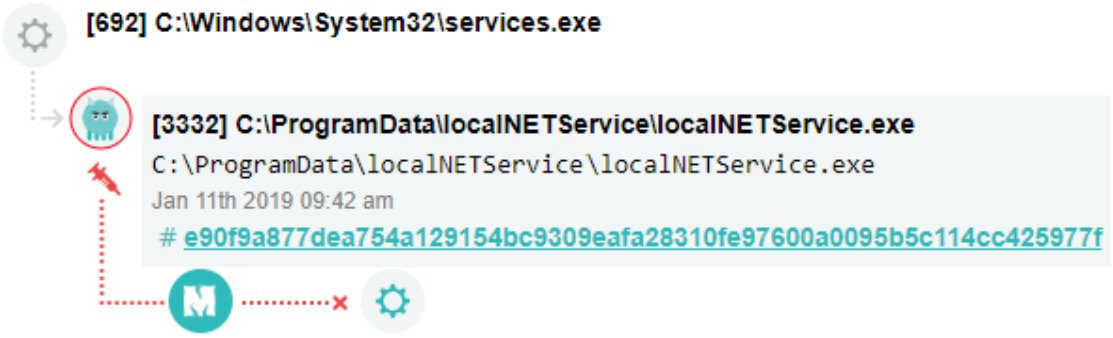
In addition to replacing GoogleUpdate.exe, this AZORult variant also drops a copy of itself to *C:\ProgramData\localNETService\localNETService.exe* and adds an entry to the registry to start it as a service as well.

Autorun Entry	Description	Publisher	Image Path
Task Scheduler			
\GoogleUpdateTaskMachineCore	Установщик Google	Google Inc.	c:\program files\google\update\googleupdate.exe
\GoogleUpdateTaskMachineUA	Установщик Google	Google Inc.	c:\program files\google\update\googleupdate.exe
HKLM\System\CurrentControlSet\Services			
gupdate	Keeps your Google softwar...	Google Inc.	c:\program files\google\update\googleupdate.exe
gupdatem	Keeps your Google softwar...	Google Inc.	c:\program files\google\update\googleupdate.exe
localNETService	Установщик Google	Google Inc.	c:\programdata\localnetservice\localnetservice.exe

Five different persistency mechanisms, four of those are achieved by replacing the original updater

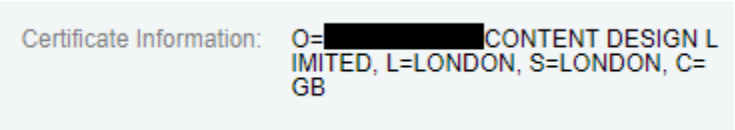
Preventing the AZORult Infection

Minerva's Anti-Evasion Platform prevents this infection by interfering with the attempt of AZORult to decrypt and run its malicious payload in memory. This allowed us to protect customers from this variant without any AZORult-specific countermeasures, days before other vendors did.



Minerva's Management Console, reporting it prevented the AZORult variant from injecting code into itself

After preventing the infection, Minerva's Management Console also displays details for the suspicious certificate, allowing incident responders and SOC teams to detect a mismatch between the alleged identity of the file and its actual signer.



The suspicious signer, as displayed in the Minerva prevention original event.

Interested to learn more about what we're doing here at Minerva to protect endpoints?

Come meet us at CyberTech Israel 2019, booth #C11

IOC

File Paths

C:\ProgramData\localNETService\localNETService.exe

URL

hxxp://s63[.]bit/index[.]php

Hashes

0120a9f8bbcc000a392f2c1c790d89b1786654f5b40afe2e2534b3d31111f99d

022c49854e180993f60f921fe203f624efcc0c9907d5af95cc183cd7f646c3bb

02376d17b1c3d5d82dfeeec3816fd15d0693c19b04b973f137a2bad6e0af2665

03cb174a5b69cf617c229600a6a56d7d73c71f41440d6d34891ef9f94d91d60c

0452783e893db661ffe3523d166ab2ea392df3c8cfad1ab33496dd5e6a0042ba

045360ff23f49642c5da4dd36b356cf54ed3c086c665fd1dfa727cab6d53cb25

0bc974389b2282feb812e12453f215f83da7e121d42566318463dfa6eefd5854

0bf313d7a4552a283dfff76b01e89acb98010c4bb9c12b6308739aa69b71d1e0

0ce7f1e2922b271938e92f2cd48590b45bb8499bb0b4041a704461f01f2a9c14

0da32f365a3e7edc3942383ba3e483a785d3100a2339a32095f436d66cd326ce

0e47f425d9306da35d828cde48011c97e6d0575625b3e823d22ae12ee2e4441e

0fb185b0b5f2394879f868b15bbbec81d8844e0e232d3e66a2ed142af12cbd5c

1086271ba095c5409c8c571cb0f8bcb6e936687d86f750c335c8dd7c23743357

128ba838c87c89d544703b63940f55dd9dc59bababa74faa9c2484f3196743ab

14dace048b51c4b6a8235a9887bde2fc45d02a64a50db9c40f3e9b1b98ed869f

16ca70a07296a058a143d574edb9f9a287ad6e7d4df6a51a00e62552f403e7cf

17bb8315aeb215c1f0f4d4373e9e1cc4483d09138410a346cf6c59db41ce8a6c

1e1db001c70e61ccdc54afa7d5a871947a0e452f9d28c7986262a2986bb079f2

20ce98e9091393da696092190825261aa9bdf5fd8287f1224a76f7318cb95776

277a078c8037976cc84461458b0f1bee8c991921f197806761f38ab9fd97f8bf

285b267d3b75047ef5ad52f380506473196deb557830ac02e7170d0d2a451b53

2afcf0debab6b45622c768080f6b076c1e34ed52c17a24ee673821acee8e029f

2caf51b28ac751488ec7442aea3295bc1c3d683e3ced8a8254d786bf2cae1bda

2d34076dee9d4439252509cbfe4da776954977657710acd88ad21c24eed4543f

316ad99eefcf0ec22da5fc3c0c42b53a28f15e451478995ebf4ee13594a4e580

32bbde1c10479f9130602d320c68e6fbd57954a01b89b86be3a1a9d1409faf95

34e0a3a8802468192d455bf462c1702e97e37211d680583bcd311561fc8b6bc9

374712ff911f69a02655e74ecff5f32922c941267671e5cc8ccfec297ffcf756

39aef8164662ba88d24abb1d5a85caf52891ba05a7da8c30891e5498e3b1102a

3ad4215327cceba68f540ba47fdf16c682a0241023dd676ce74ba2c1aff8d3a1

40fa02cbb5d50fd2964fa34316e7c090cc04cc5a55b8b7d8b047aefc371a1606

42ce72d29d635225acaf326d34909b2017737da5cef29ed90302ecdc2c8c61de

498727da1daae0368101b00d0673ddb420102711edc56e732f935e20fc3f27d9

49e1bc5e069bcc5e5710cd4f3b6ae0d1c937cd31e7b32e04a645977565d724b6

4a33787c56ade53e14c4a1d32d815ab47bda6e1ecfc97bbf5d6a7a9e4d0cdd0e

4c6ed9e8bcbaddf1406c8d774ea5edfa6eab1f66b87fc545013ff13b7f48aa48

4c7e8aa51bebf8b93c7c13ffd0965a9e97239cd9134457702c8d37924588b2ce

4ecb43e7e9cbaecc4a6c23d58c0e4f81277ceaceb991507d3078934cc8af04c8

4f27de33166a1e2134e047783d7f37684b47b34d07f95ca4abdd7362b6842f90

4f3a220543d1de1e00f37aa392b5b3ea57e670f629c45d1a0350e2aa943ab209

53408be699c75fc238c6d3a2fa8f71dd00823e85811f8cd061a553925c2dfb2a

542c266dc633cf849ed3662004784093dba20aaa86f10ad168e78d2c1670be1e

5496ea08d295d709e53e719b6907917bdf3d1857ad56c6ba0f819e1fc05c866b

590997178c691cb710fa8ab1cd29bcb0ce7d1000192a4ccb6211fb40b14162d4

5d494d83fbbb5cb54ace880e0a55ccb2d1c68e4572f9731d678ad597d1f5e3ae

619b146ca20c1f7e48a730c74b5495d0320a215f47a03aa5eef2658ec7a258f5

621e73d9000de5381d43569826e0f12a826776ae5bb66baeb320e27ad5034f6e

623825eb57410802b1f962e06b1019b9f925ec765392d07fe63850e44b9dec53

623ef7a97fceadad49973957ca60744a478efadab98800c92230f41d2b7578c6

6470780f62fec2f1f83dc9603590744fe164aa87af9b327a259055db7c8f8512

65889209b843850e898f91e448909c3966bd8d1a7d09eb3bea62b986acae5529

661d4c76f7e7e2d462955261510997764dc49ea6cf3fd18490cc7c6912397f33

6ae3932accedfb1146f1b9adf4e9747af0631ce8f32eb61debfad55243d86fd1

6b53afc53e02498237b4b63a905e25fddf09f1185977babc358e1d33829f556d

6d1aa1391e53680859342325a185160e9d44e68093d45c01c98f979498f4f79a

6e98c88abf5b2afed15ec241aa677e05e3a86c3d60adb9b4d15e1f4a7586ff21

6ecce12f0a1537804b8d832b646c39b1ba6b0b28e9395d3f53d7e3df66e7e643

6f111973df2ba254d7d9199b7c4dda01d5b90bb8405e67b8ed86b3e2a23b72f1

7462ef992764c96c2c3552886a0876fd354f558b9d44d61150236da67d3af370

749dcc0ffa6ab626db7fc2d6f9c74b92861708da73f9a422c90ad2af96724dcc

7936aab0b0dcd341f3ba168a267df093c1342fbc28015177db029cbd8c7f3fb3

796e6d59f5cbc3eba40c08c9a4c1002677bbf2be75a7dc3fd779a7f133a49e83

7c61add2fa581880a29aa1f4c57c7dc8363091ccfbdab5b56409db7800d155f2

7dc4667db0fa29871ad5519d0794b18f9b2bae279cf725e8673ba6948902e89d

7ece58274588bd45a1bf6c1c6ece9119d9982e0cbd668dbe82e8d8f674b30ef5

7efedfe5093d4743dc61332287ac79a2612b1dfedd3748fc37007bc5f84bd54d

815fef8e66cb9e437e0180e1a7df4de52ed893c4a702ce2959fbdc408fd9140b

8434186cc81c509adf373f676235cb33d819f06922b7d55da4c1ac6c58a1254a

8494845a22c826667e5fd666906cc93c116021f120e2fce98bdec30ddf6e7660

85c0209e535de0c7784f741762f92619502d8c72ee9494e6800dff398669a592

87c934ebcada9c63b197914faee225c99b90ea5e6e6ccd8a68aabecd068d69a8

88d6c77aa42cf820bf30ff424977134e7275cb9c279f82bba37e806b93c88711

8b61d64e82b15f28ba3636ee0372efac9103630eaca753dcad938a9003ef60fb

8cf61e83d1437da97ac90294ea9f936afba9dd3bb4e0c97e324e430dd503e222

8d76ecf2d26f25fe54cd71c724fba81a40c05a9a326c43dc22f0fa9e0acf0508

8e7b420b09dd6beeb83c81967b4951929964d4cbbdce963d26f09465614eab1d

8f571c57013f8dce29fc578e8342780ddf923b2df4193d2c1619e6acfb552d5b

8f79289e99047e6adc601085153924ccb3e0ba559dd422d985c74335d4e6fddd

92d6aaeef413ffda366128e2029c23f0bda38468ea3c5451a15a31e207f26538

954a37ab51ff28da4af7fd7f650a47c9d8e0613b97e7ce4e563254669d88709c

969aedd37401c7e720fb02ac84902b0c04bc1af8553e2b1d299b5d7ab0f72cd9

983f7e7c3604767211a8c5e2dc51c168e6577bdcec559f7e1206d9708c7eac65

9aaff103e2e460a9d99e2da9fc9413fca8182459141439487fb064b18377f006

9cad605e52f2f5752016ef317323712a69525415cf13c3c93215048d5c2c7147

9fe8e8e66680cdcd5e5d4c3b84ca764c7128c1f02223f21f5db9465249474016

a0f1ca933fb71c80d76e398baa573cc62fc73688b239e13c99c30b70861de25c

a79da5edaf4149183c7a10b167f8f4711e437e229e0dea87251447e52dfbc1af

a9181c2756fd7d2d3ff6e6830699ebf8f75aedb1e8ff6b61419815379637550b

ad48c5c7bfc485c075b2279d7c7e6e620db8c90a4e7934f529e36df5f211b010

b03e40eb9143ff8cc46cf50c5a67b12cda2523e22ff60dd43d8ffa4047f89e53

b0f51fbf63b3f1b223cc74b330edad8e174a08d37c61faa15ee8d18495abbfcb

b29ace5866157d3eb77105b185c07d2d99006756592f609d0242b264db05102b

b4b52e530cd71b21c08db6c3e45f338c175be9d10525aeeacb0a33886a0e9cbf

b4b7e5af784e663c38e09f0421d30b9fbd6743738f31e2832048ee283c91ef24

b98196e85334698723c7b006643d28a9efe54ab46496459354aa179d3b8a31bf

b9bc5839231bd00b293a5d11ae2479347f8858a12a522a6d48b6f9763afec69c

babfa300b0e487d73b7c51123571aad3b137b7208408e82f55ca5c5460c6a80b

bc61f7a60e2af89d20e910c672458b03ccfd2c3b4ecb5662a826342f9725795d

bcffbf7fb17d60e7c4362faa911c0efde7dad16b6d66fc8a7eef07d1ef1332f5

beb801f2362616272d92d6d074b6f188a751ea7d8006d68550469b169c92423e

bf8c6edeb15de02443fddb7ea0e1b8969fd4d17e48541ed8d552e62739dd7780

c6234945c0eb0e93895bf4a4925dd033d051dfe43b8c5e9da2525c1f0a61d828

c6e7e602580278c2017640bbf0bf92ad579c5bc98667ffa2bb369e1fc3a2b14a

c78e870076fc57b4a6a02a41acb3b213452ae9aa9eb31be95f333f5aa1fd0d24

ca661ebd67d48b5c1d47d6b65552a92653b91e83a6df550c8d1d394b00ba8213

ce006a6c046bd44356f1f26e16f4438357dd7fadf430e2c361ed7142b8d1f7a6

d0c7f4ab97583f443d03cbb23ed3c67cebe927ec1a7c1837a42f3a13ba426800

d2f4bfa5b24ed6e6d0e62693d2e3b07b30a7d31a87f4deef5fecaaf44d3df301

d40c1d1439cb85da7edbd04e9d54154c9387c717627d08ac6d8f12d566b3f2fd

d5b47dbe70a1b4cacb326b27154ad84c8f731ae80523a74ca53f7028115ddc3e

d65c5884e8545b8a401ad6bd6a5af7f0737c183a5959b7ecb93f66b57b10f7fb

dbc24ed727f1f1f175c4f08180052e119a4f644a23a98828ab6b253164bb54d7

dcc3befd071d0e330ab3e354911eecab356518b47ec8aad26034feef1e129a3a

dde0f363f70c97f67e45f6dab98e3efbb564e8cb66a77670cd74c49626aa1170

e1a486aaaa95263917b19880b98ad389d9bbec1abe4f9cb4b9ddc41b49a40a58

e3ef02eeb2ca1948d64bc311aba0cb19be1ad429a126ca02db3f9ba484e10201

e60dfedf1205b8e644ec747785368d9da52fbb37ed5942b43fd7ff21ef208027

e83d51193d200867a7b82faad431264557f37fee655956cb58706fc43092ca23

e887adab47c292919d0a387bc1aabdd2c3d48ba3379e48ffe1dd130c15c5da78

e90f9a877dea754a129154bc9309eafa28310fe97600a0095b5c114cc425977f

eaa4391f64958b453c0262b59cd31319eb4c37d5c7db0804d84890357cf6693a

ed5fe34a54652106a202ebe50ae56a138aa631aad33b16821391ac26443e0b6c

f1db46a5d4b3c160c182078fbd78050d97c60edc6a1040669b7849d016bdaeee

f284c19033c959ed3d84b9c18adcd479d8153194073a7ba517e349f64b0f0bcb

f60cb6f34fc7c7f8e2ed75f1b492352936588ab7e4f200a512d43f843b8b9a1d

f70a6392229e6677988fd6bb023a4c235b0b1c37b02da7cf38f409518463f994

f75f91e2f81ce8f8935acbe89eb69aca4e130fa41a107f3d020c6528dc868827

f7c50a860bd73fb8c3f1002cfb71d024eb0d8328938648669f1d542c62dca935

f9ed04d95028c71ac959811fc006cd478a17eebd62a68798f4333570257d907f