Binary Options malvertising campaign drops ISFB banking Trojan

blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/

Jérôme Segura April 20, 2017

We have been witnessing a series of malvertising attacks that keep a low profile with decoy websites and strong IP address filtering. We are calling it the 'Binary Options' campaign because the threat actor is using the front of a trading company to hide the real nature of his business.

There have been similar uses of fake façades as a gateway to exploit kits. For instance, Magnitude EK is known to use gates that have to do with Bitcoin, investment websites and such, as detailed in this Proofpoint blog entry.

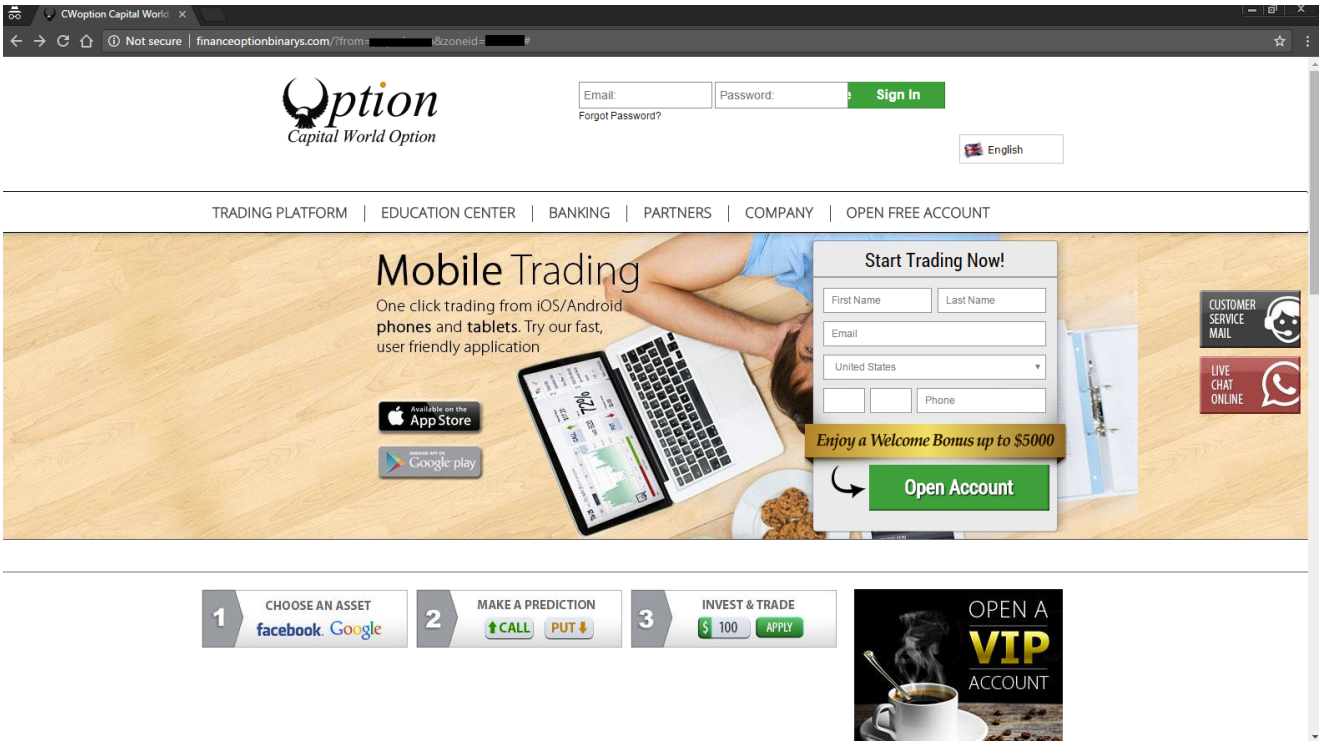
In this particular case, the threat actor stole the web template from "*Capital World Option*", a company that provides a platform for trading binary options. Participants must predict whether the price of an asset will rise or fall within a given time frame, which defines whether or not they will make money. Binary options have earned a bad reputation though and some countries have even banned them.

Fraudulent infrastructure

Below is a screenshot of the legitimate website that is being impersonated. There are some differences between the real one and the fakes; the former is using SSL and was registered a while ago. Also, some of the website functionality is not working properly with the decoy versions.

Legitimate site:

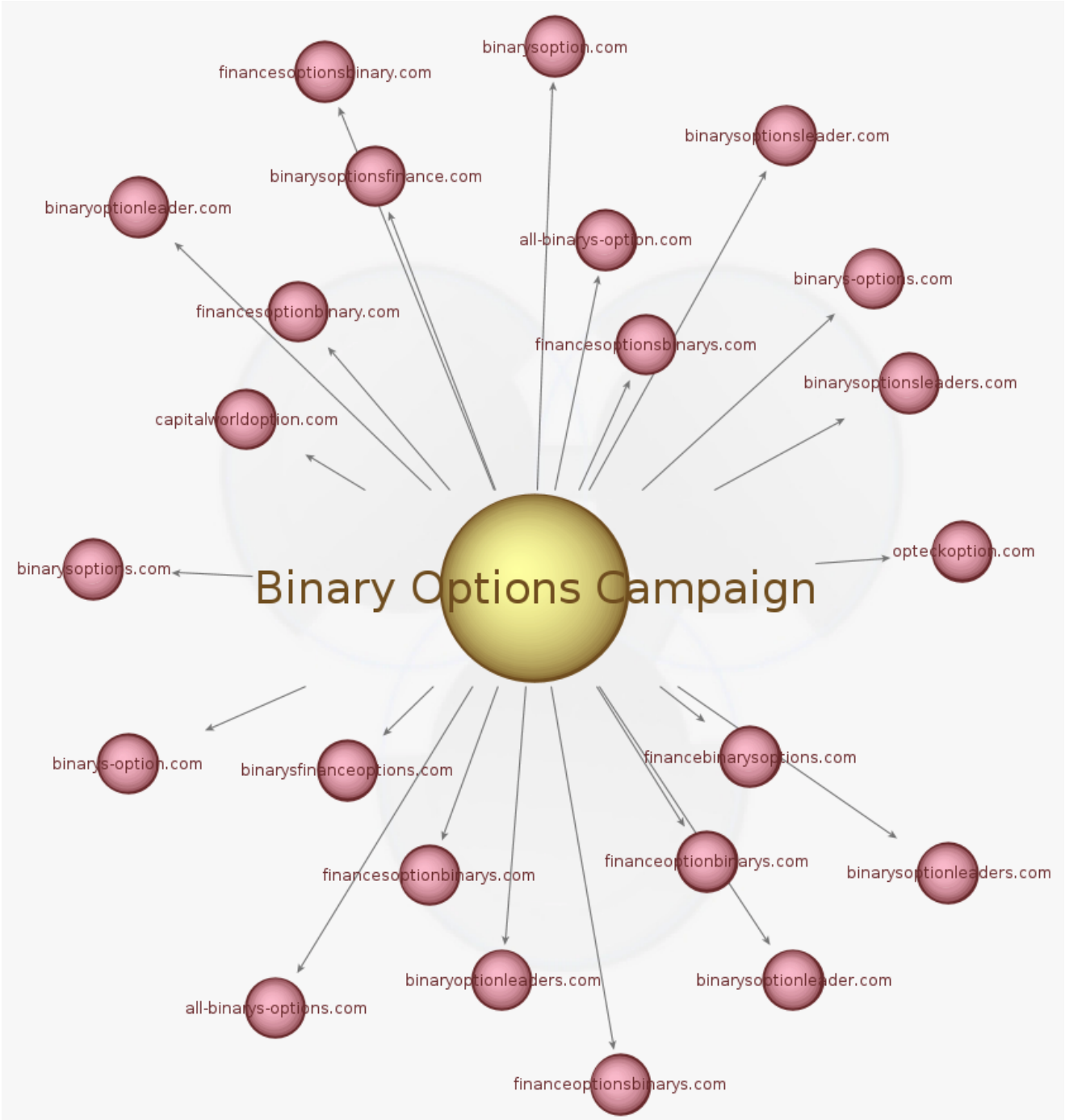
Decoy site that ripped all the branding:



Those fake sites are only meant to be viewed if you are not a target of this particular malware campaign. In other words, if you load the infection chain from the malvertising call and see the site, you will not be infected. Infections happen when the fraudulent server forwards victims directly to a second gate, without showing them any of the site's content.

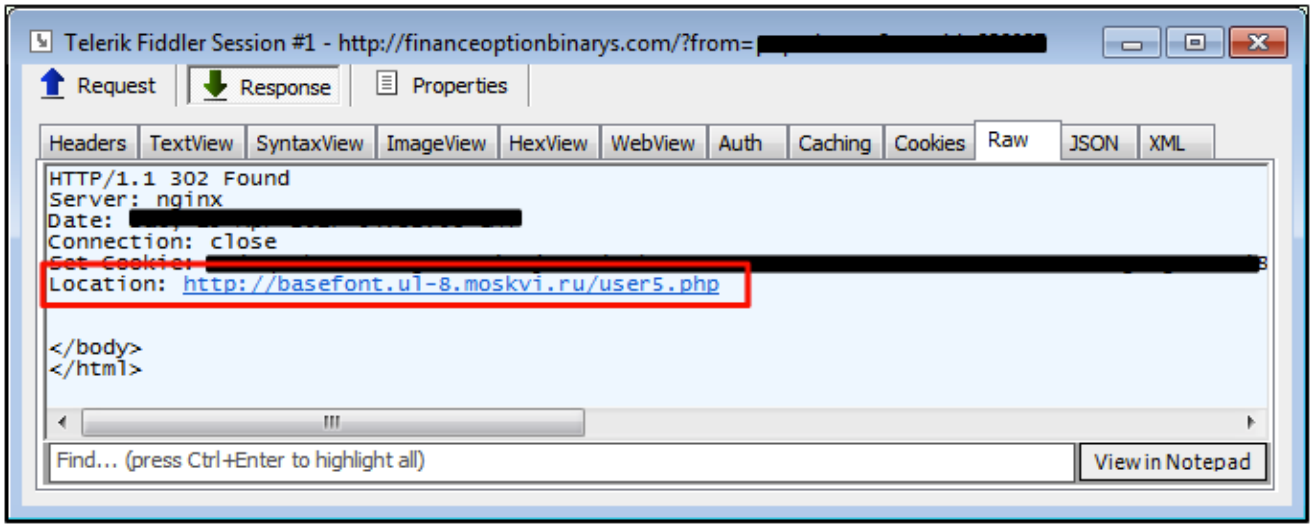
The same threat actor has registered many different domains all purporting to be lookalikes using a similar naming convention. The recent creation dates for these decoy sites is a hint that they are not likely to be legitimate:

```
Domain Name: CAPITALWORLDOPTION.COM
Creation Date: 2017-04-04T09:15:14Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrant Email: detes55@mail.ru
```

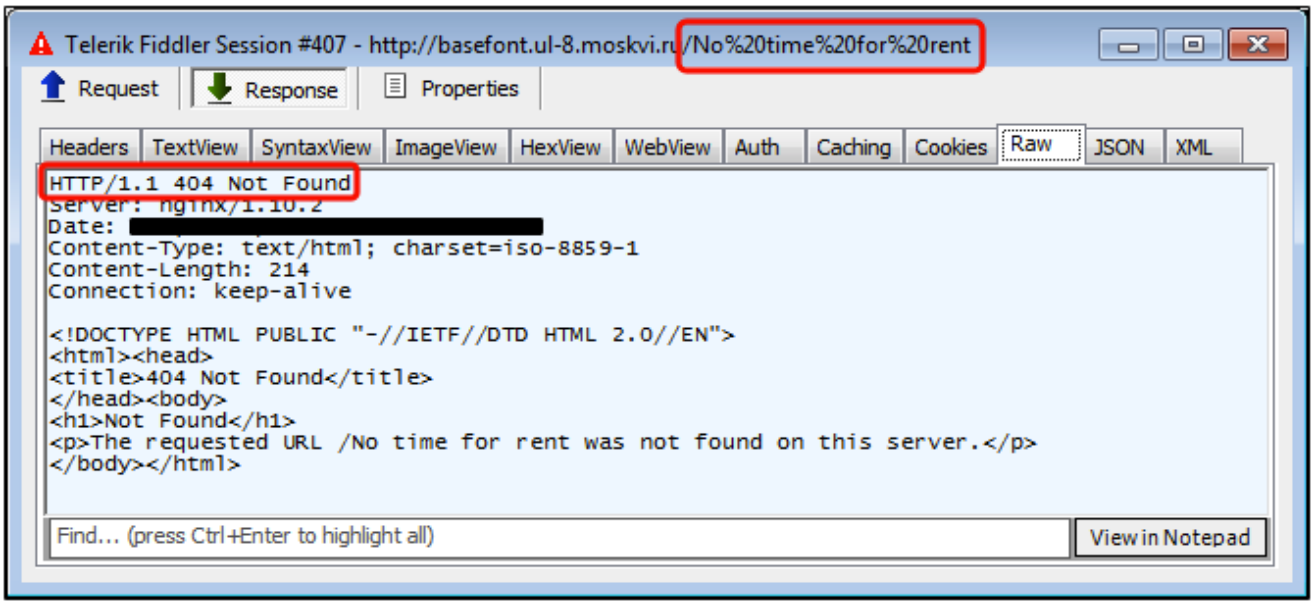


Malvertising chain

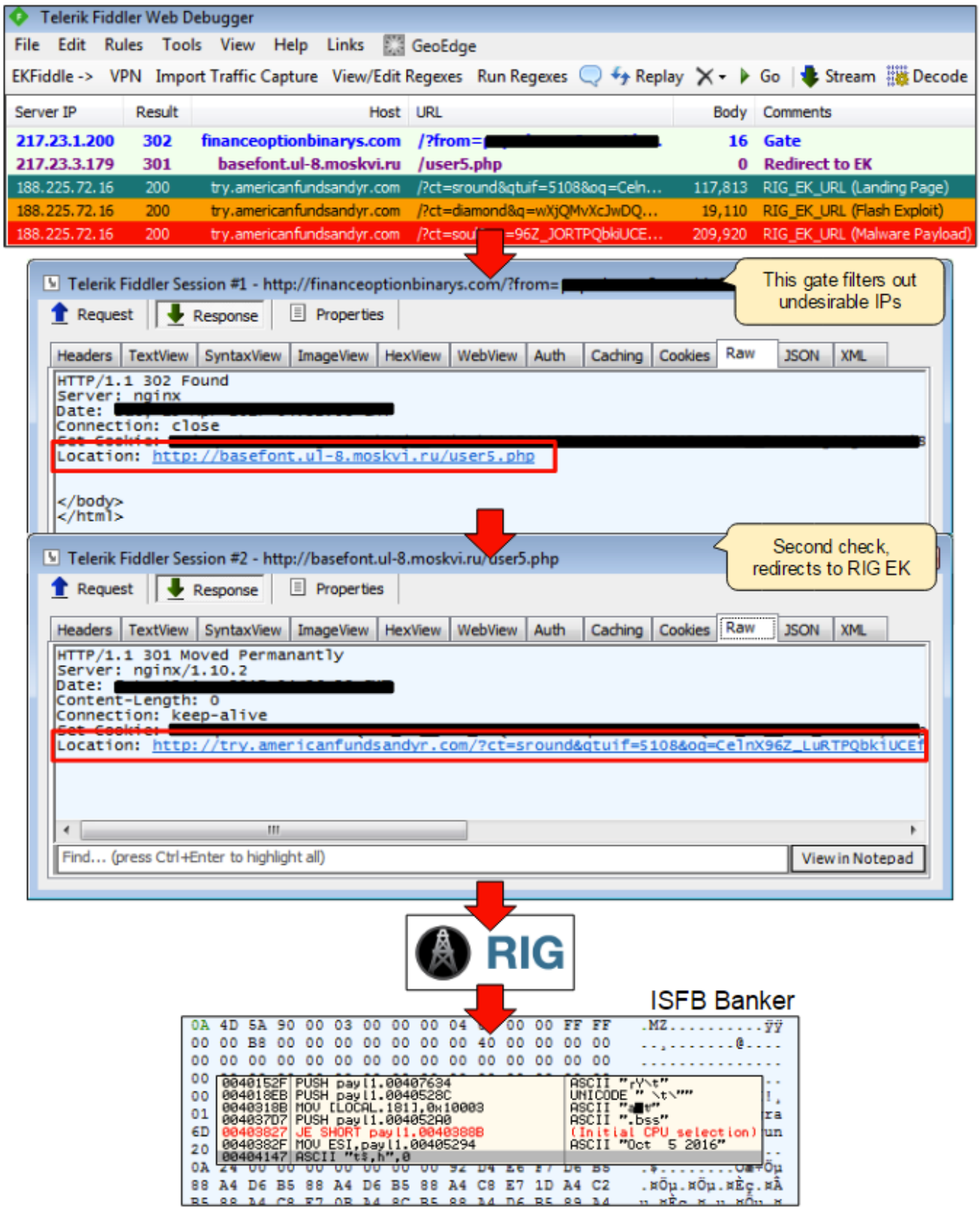
The attack starts off with an ad call from one of a few ad networks (Popads, PlugRush were detected in our telemetry) and redirects users to the decoy website where a quick IP check is performed.



Only legitimate users will be redirected to the second stage server, which also performs its own check. Once again, unwanted traffic will be dumped (and a message – perhaps from the threat actor? – "*No time for rent*" passed in the URL):



Otherwise, users that have made it past those two gates will be presented with the RIG exploit kit.

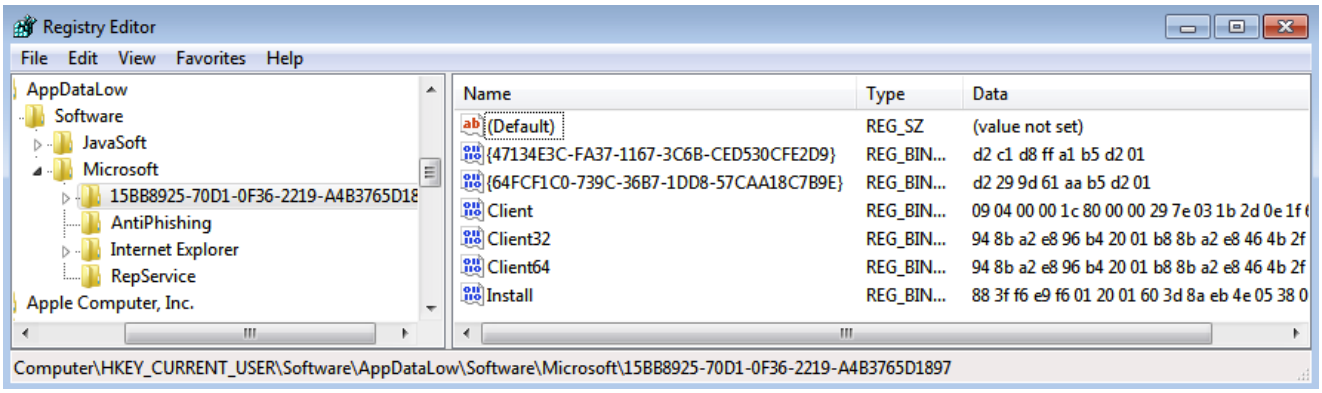


Binary Options malvertising campaign

Banking Trojan

The final payload consistently distributed via this campaign (across different geolocations) appears to be an ISFB variant (AKA Dreambot, Gozi, Usrnif), based off an old but resilient banking Trojan. Some of its features include web injects for the victims' browsers, screenshoting, video recording, transparent redirections, etc.

The artifacts left on the system were very similar to those described in a Proofpoint blog about Dreambot and the samples we collected also download a Tor client. The registry entry for the Tor client can be seen below:



Modular structure

The sample retrieves several modules once it sets hold onto a victim machine and below is an overview:

Original Dropper

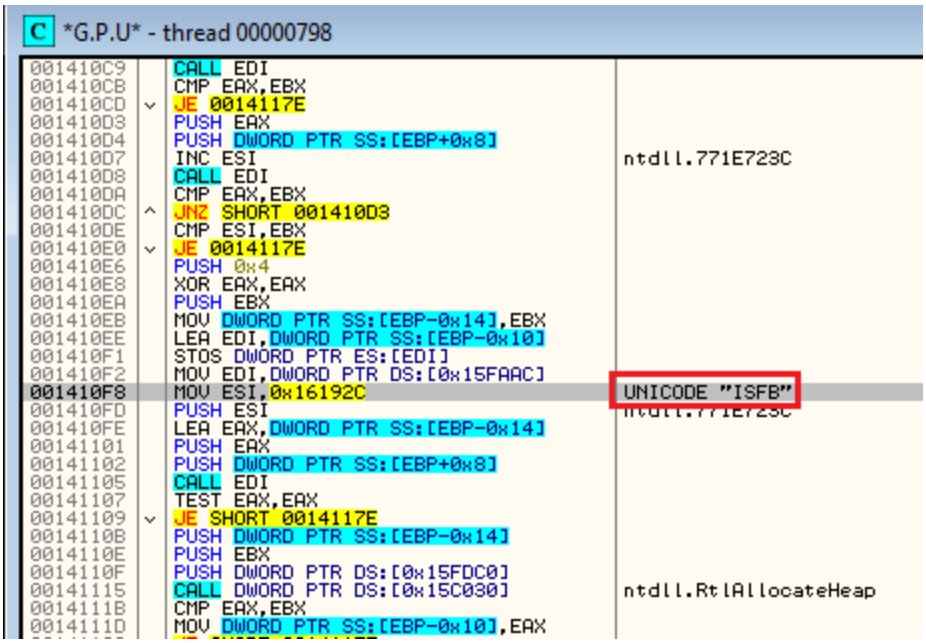
-> ***loader.dll*** injected into *svchost.exe*

-> ***client.dll*** and ***tordll.dll*** downloaded and injected into *explorer.exe* and into browsers

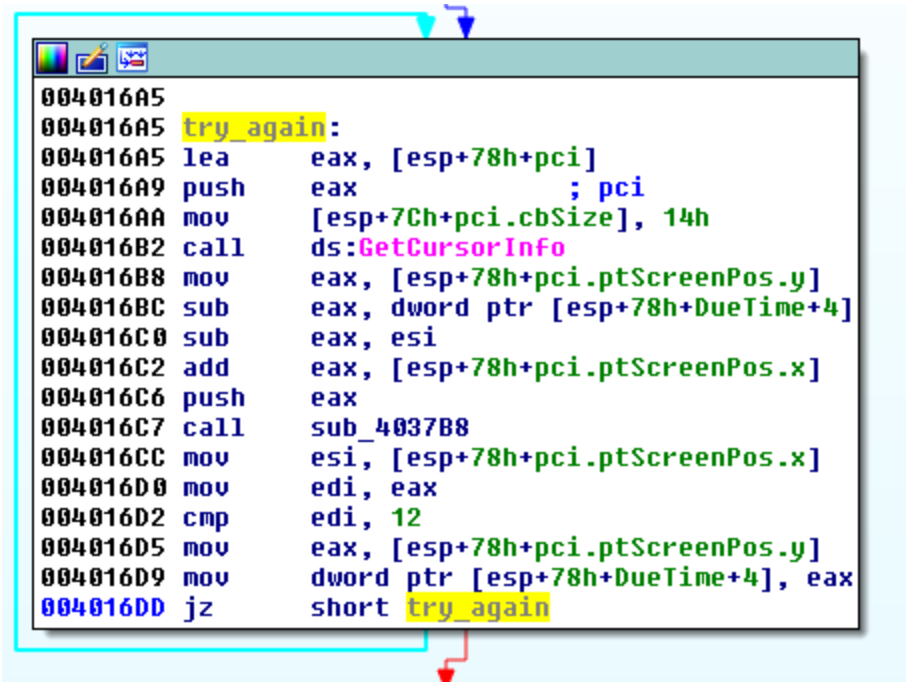
The main executable injects a file (*loader.dll*) into svchost.exe in order to download other modules which are encrypted during transport (*tor.dll* and *client.dll*) both available in 32 and 64 bits:

Host	URL	Body	Content-Type
89.45.67.99	/images/gzJ9FyErBLLLL/fo8G8MeD/QEk8GUa8CO4w...	136,770	application/octet-stream
89.45.67.99	/images/AD_2F4eOLq/W4HfWegIH7a8NmPPw/9MHh...	172,619	application/octet-stream
89.45.67.99	/images/_2BrizUG3nXwTphuZ1/VTdilaIM8/qFk9_2FXw...	136,770	application/octet-stream
89.45.67.99	/images/cw19piqMwyeY2mPRAlYK/drxg2iUUCjqJJVty...	172,619	application/octet-stream
89.45.67.99	/tor/t64.dll	3,162,183	application/octet-stream

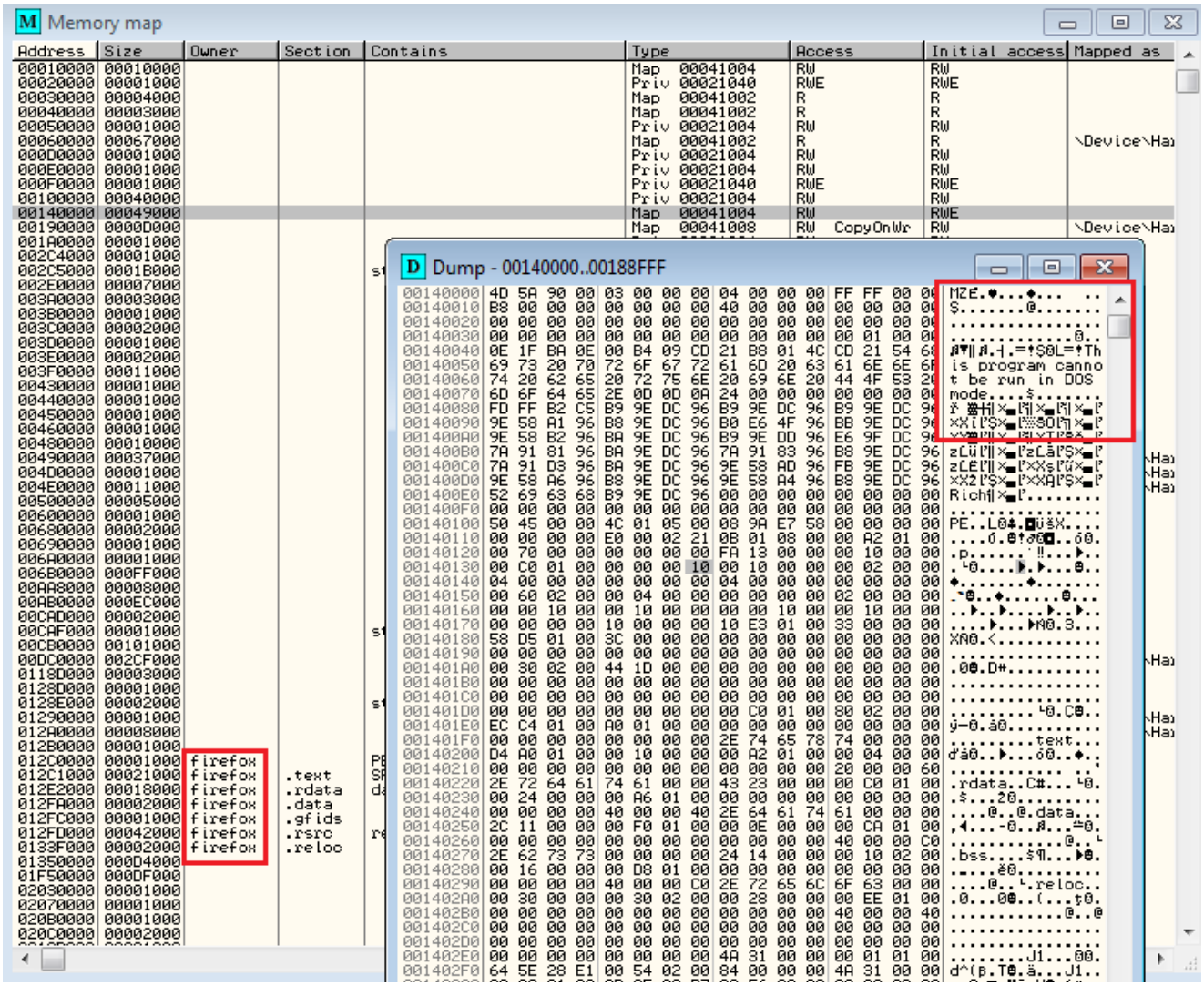
We can notice the "ISFB" signature within the malware code:



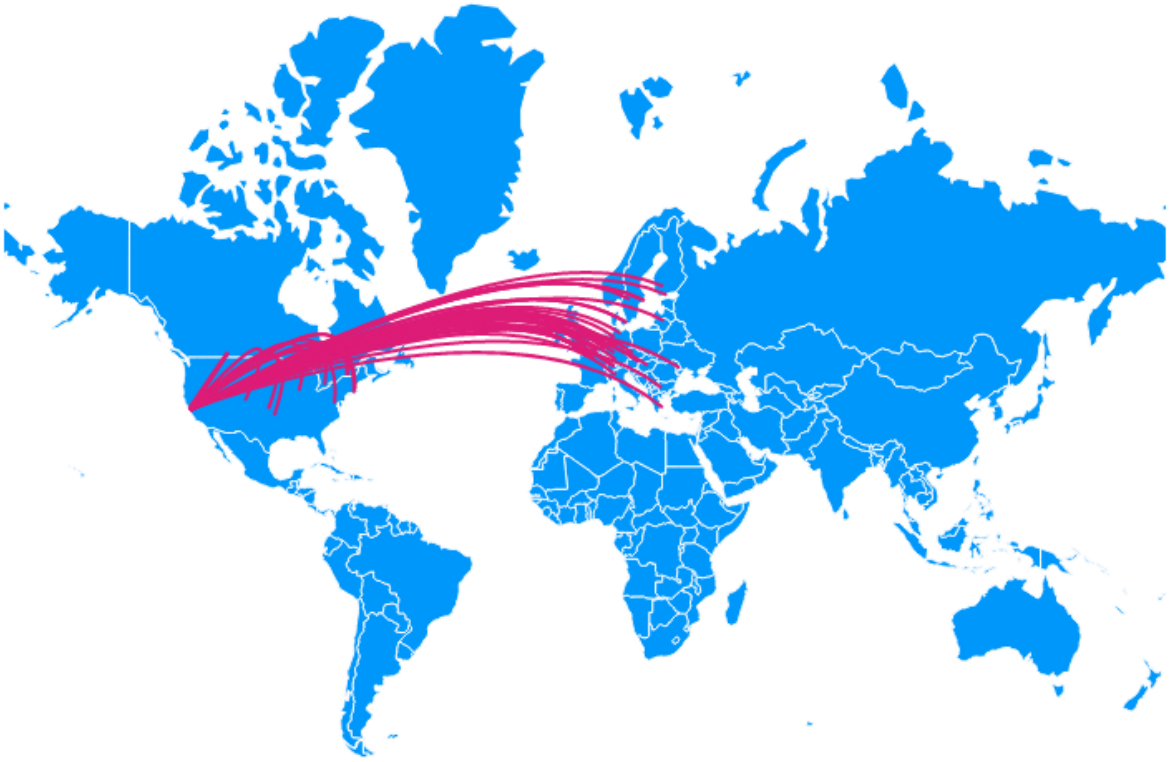
This piece of malware has some anti-VM features, for example, it checks on the mouse cursor:



Modules are injected into *explorer.exe* and try to establish a connection to an .onion address. Browsers are also injected, via *client.dll* as depicted below with Mozilla Firefox:



There are scores of hosts that are contacted post infection, as well as the Tor connections that trigger many ET rules as *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group*.



Conclusion

This particular campaign focused on a very specific malvertising chain leading to the RIG exploit kit and – as far as we could tell – dropping the same payload each time, no matter the geolocation of the victim.

Banking Trojans have been a little bit forgotten about these days as they are overshadowed by ransomware. However, they still represent a significant threat and actually do operate safely in the shadows, manipulating banking portals to perform wire transfers unbeknownst to their victims or even the banks they are targeting.

Malwarebytes users are protected against this threat at various levels: domain and IP blocks, exploit mitigation for RIG EK, and detection of the malware payloads.

Related material

- Proofpoint: *Nigthmare on Tor street: Ursnif variant Dreambot adds Tor functionality*
- Maciej Kotowicz, BotConf: *ISFB, Still Live and Kicking*

IOCs

'Binary Options' domains:

```
all-binarys-option.com
all-binarys-options.com
binaryoptionleader.com
binaryoptionleaders.com
binarysfinanceoptions.com
binarysoption.com
binarys-option.com
binarysoptionleader.com
binarysoptionleaders.com
binarysoptions.com
binarys-options.com
binarysoptionsfinance.com
binarysoptionsleader.com
binarysoptionsleaders.com
capitalworldoption.com
financebinarysoptions.com
financeoptionbinarys.com
financeoptionsbinarys.com
financesoptionbinary.com
financesoptionbinarys.com
financesoptionsbinary.com
financesoptionsbinarys.com
opteckoption.com
```

‘Binary options’ IP addresses:

```
217.23.1.65
217.23.1.66
217.23.1.67
217.23.1.104
217.23.1.130
217.23.1.187
217.23.1.200
```

Redirects:

```
basefont.ul-8.moskvi.ru/user5.php
p.figcaption-7.nfl.si/user5.php
command.bdo-3.mirifictour.ro/user5.php
menu.command-2.moskvi.ru/user5.php
code.a-10.moskvi.ru/user5.php
header.h5-2.mirifictour.ro/user5.php
input.noframes-8.narovlya.ru/user5.php
col.output-9.nfl.si/user5.php
meter.em-8.narovlya.ru/user5.php
applet.x-3.nomundodapaula.com.br/user5.php
```

Payloads from different geos (ISFB):

```
f2f8843673000b082ad08bd555c8cd023918a3c11af9d74e9fa98f3b1304b6be
f12bc471f040146318a6fbd2879a95d947d494bd0b869dc95c01cfc22af0ab13
61dd7aa2ca44371b7c8cd4dc9e5f3bd05a8c6213d8e6357dfdb9034b1c0fd590
aed39345668d24dced4b83c36321e98ec9f09af3044b94ceecf01662de0189ab
```

Post infection traffic:

```
158.69.176.173/images/zln7qsefZ961EfLVkD3/0FmzZhicPZalFMUtdp9E0C/JxRcPKmDA9QAA/dNCE_2B

158.69.176.173/images/KziuBbVMi/s2WSfAlAnamELXfRux7g/hq2LcDlwVjaxz0wE5od/9arE_2F5SMgQT

158.69.176.173/images/xeF9Qj1PPNbvhLGetscM/N_2FnVKgMXfiY05zWnD/WL5p5iqJTPu43MoqB_2FZ8/

158.69.176.173/images/smmqGoxf/caltlwZ4eJEFQRiF13_2FDr/jb3Lhoj5l3/3C3I8HbwUcIkIKNfL/GI

158.69.176.173/tor/t64.dll
ip-addr.es/
aeeeeeeeeeeeeeeeeeeeeeeeeeeeeva.onion/images/skmTPhNwp9NVU/_2F4G_2B/uO_2FVNwGzKHjF6XXm_

aeeeeeeeeeeeeeeeeeeeeeeeeeeeeva.onion/images/mUKxVkxTd4/jVGmdXz5wgukSnoqn/dHI0tQ0GMoHy/
```