

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.

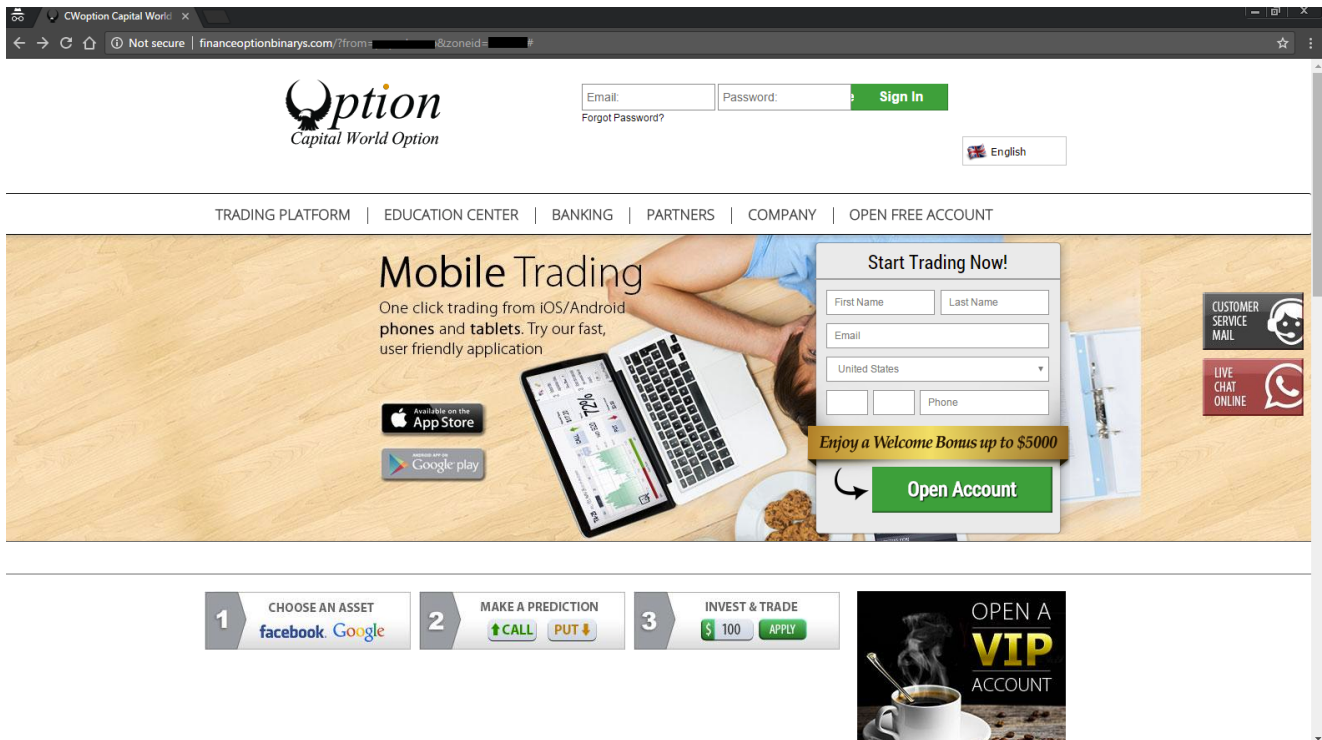
Fraudulent infrastructure

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:



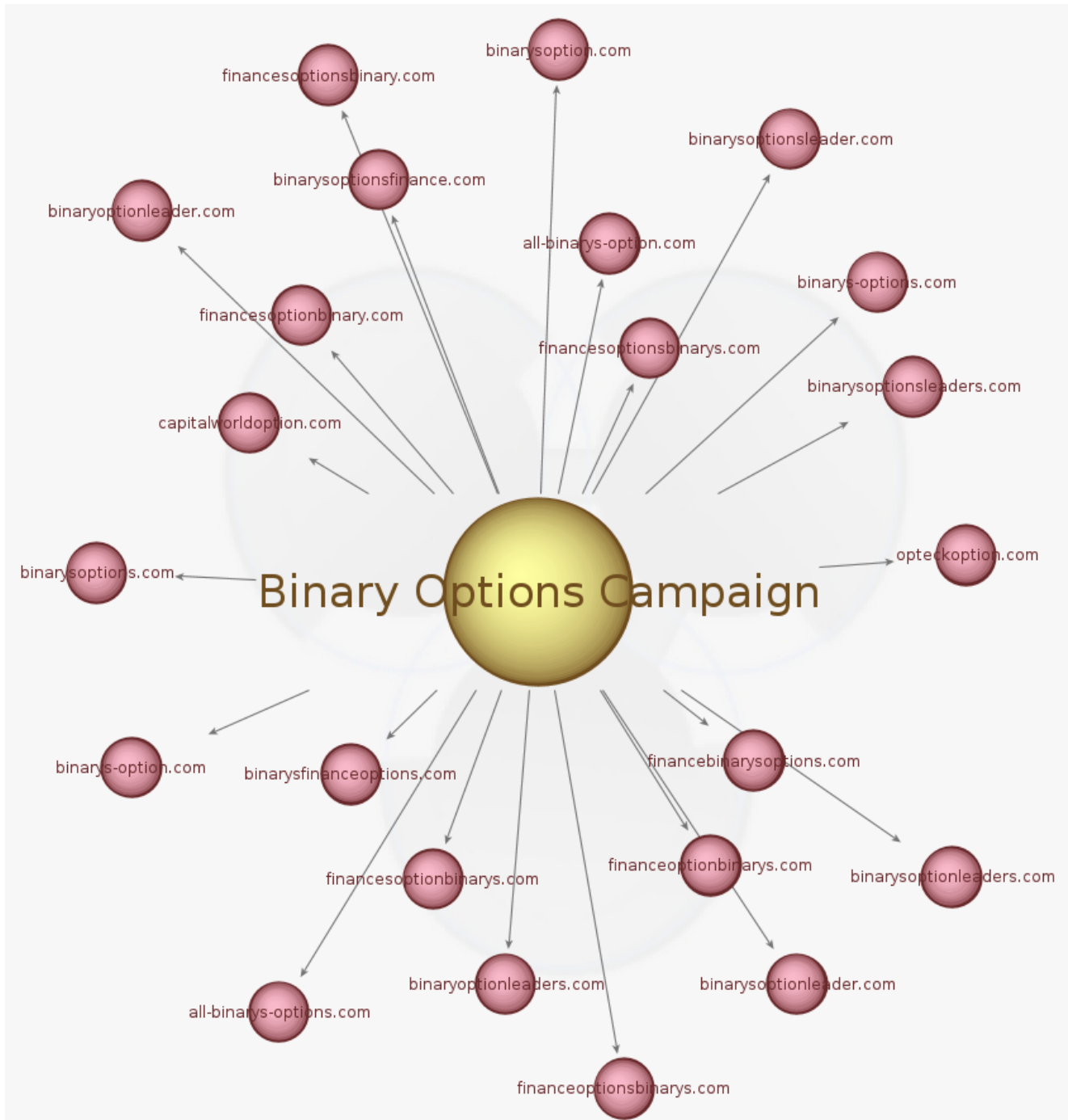
Decoy site that ripped all the branding:



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.

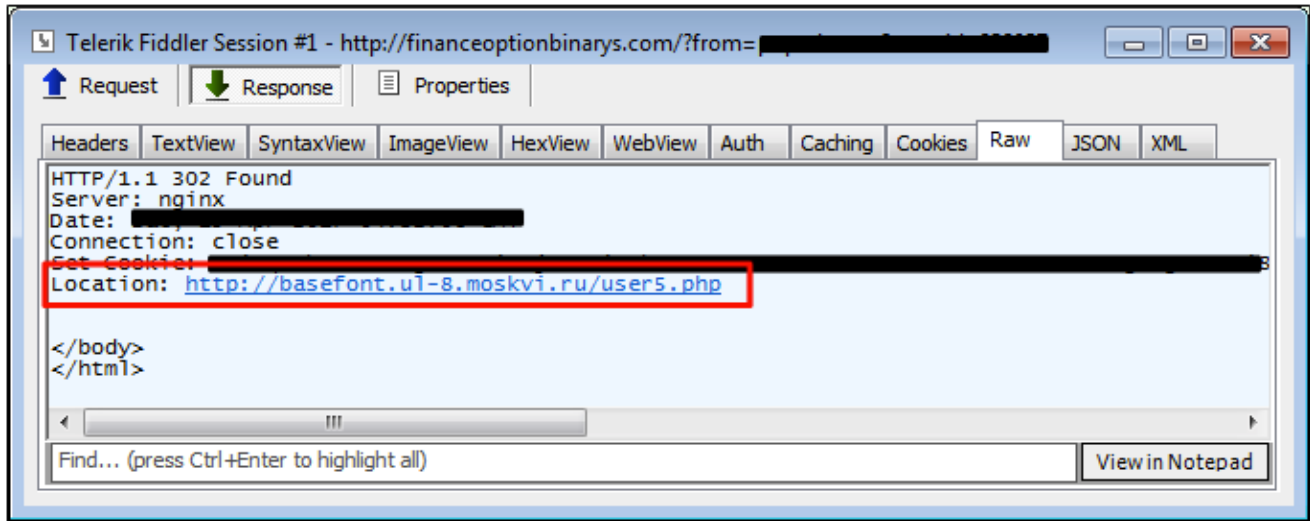
The same threat actor has registered many different domains all purporting to be lookalikes using a similar naming convention. The recent creation dates for these decoy sites is a hint that they are not likely to be legitimate:

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

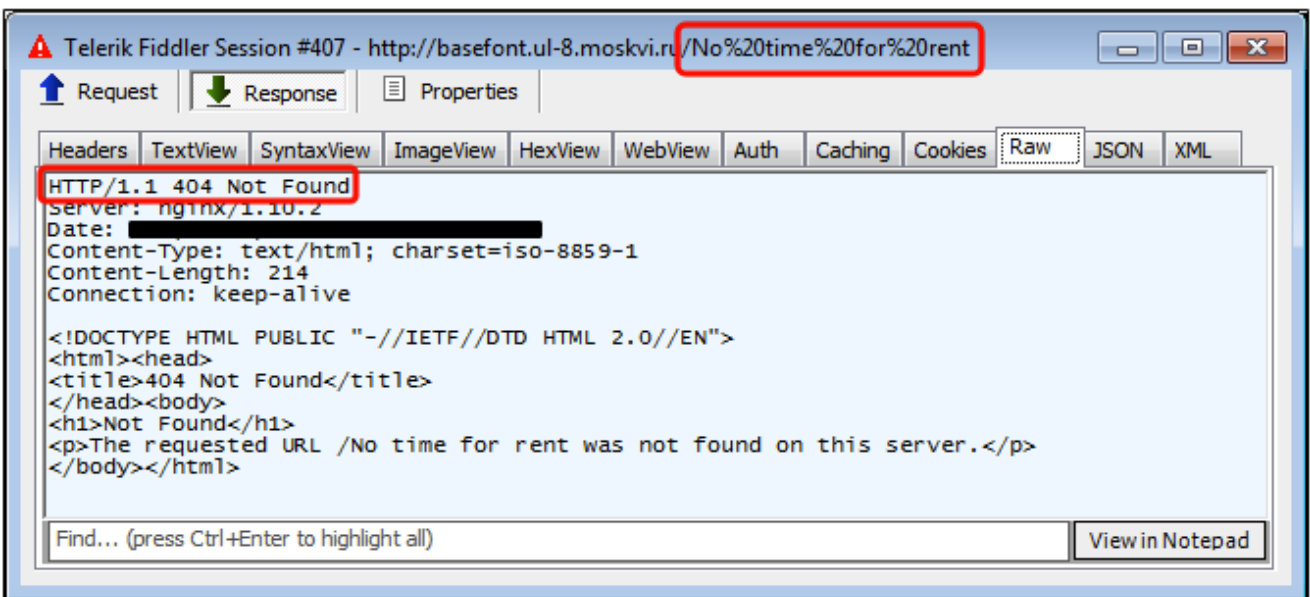


Malvertising chain

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.

Server IP	Result	Host	URL	Body	Comments
217.23.1.200	302	financeoptionbinarys.com	/?from=	16	Gate
217.23.3.179	301	basefont.ul-8.moskvi.ru	/user5.php	0	Redirect to EK
188.225.72.16	200	try.americanfundsandr.com	/?ct=sround&qtuif=5108&og=Ceh...	117,813	RIG_EK_URL (Landing Page)
188.225.72.16	200	try.americanfundsandr.com	/?ct=diamond&q=wXjQMvXcJwDQ...	19,110	RIG_EK_URL (Flash Exploit)
188.225.72.16	200	try.americanfundsandr.com	/?ct=sou...=96Z_JORTPQbkiUCE...	209,920	RIG_EK_URL (Malware Payload)

Telerik Fiddler Session #1 - http://financeoptionbinarys.com/?from=

Request | Response | Properties

Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML

```

HTTP/1.1 302 Found
Server: nginx
Date:
Connection: close
Set-Cookie:
Location: http://basefont.ul-8.moskvi.ru/user5.php
</body>
</html>

```

This gate filters out undesirable IPs

Telerik Fiddler Session #2 - http://basefont.ul-8.moskvi.ru/user5.php

Request | Response | Properties

Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML

```

HTTP/1.1 301 Moved Permanently
Server: nginx/1.10.2
Date:
Content-Length: 0
Connection: keep-alive
Set-Cookie:
Location: http://try.americanfundsandr.com/?ct=sround&qtuif=5108&og=Ce1nX96Z_LuRTPQbkiUCE

```

Second check, redirects to RIG EK



ISFB Banker

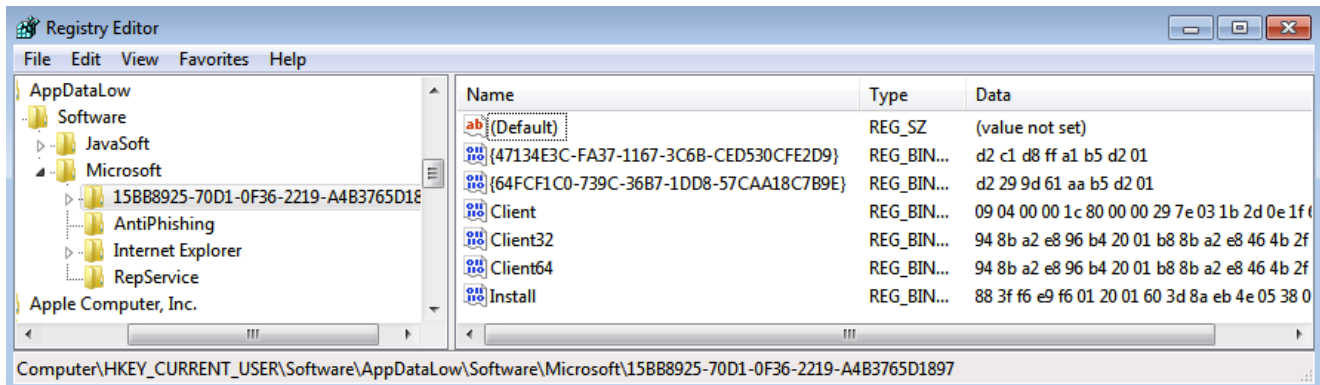
0A 4D 5A 90 00 03 00 00 00 04 00 00 FF FF	.MZ.....ÿÿ
00 00 B8 00 00 00 00 00 00 40 00 00 00 00@...
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 0040152F PUSH payl1.00407634	ASCII "\n\t"
01 004018EB PUSH payl1.0040528C	UNICODE "\t\''"
00 0040318B MOV [LOCAL.181],0x10003	ASCII "t"
00 004037D7 PUSH payl1.004052A0	ASCII ".bss"
6D 00403827 JE SHORT payl1.0040380B	(Initial CPU selection)
20 0040382F MOV ESI,payl1.00405294	ASCII "Oct 5 2016"
00 00404147 ASCII "t,h",0	
0A 24 00 00 00 00 00 00 92 D4 26 27 D6 B5ÿÿ
88 A4 D6 B5 88 A4 D6 B5 88 A4 C8 E7 1D A4 C2ÿÿ
B5 88 34 C8 E7 0B 34 9C B5 88 34 D6 B5 88 34ÿÿ

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, screenshots, 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:

```

C *G.P.U* - thread 00000798
001410C9 CALL EDI
001410CB CMP EAX,EBX
001410CD JE 0014117E
001410D3 PUSH EAX
001410D4 PUSH DWORD PTR SS:[EBP+0x8]
001410D7 INC ESI
001410D8 CALL EDI
001410DA CMP EAX,EBX
001410DC JNZ SHORT 001410D3
001410DE CMP ESI,EBX
001410E0 JE 0014117E
001410E6 PUSH 0x4
001410E8 XOR EAX,EAX
001410EA PUSH EBX
001410EB MOV DWORD PTR SS:[EBP-0x14],EBX
001410EE LEA EDI,DWORD PTR SS:[EBP-0x10]
001410F1 STOS DWORD PTR ES:[EDI]
001410F2 MOV EDI,DWORD PTR DS:[0x15FAAC]
001410F8 MOV ESI,0x16192C
001410FD PUSH ESI
001410FE LEA EAX,DWORD PTR SS:[EBP-0x14]
00141101 PUSH EAX
00141102 PUSH DWORD PTR SS:[EBP+0x8]
00141105 CALL EDI
00141107 TEST EAX,EAX
00141109 JE SHORT 0014117E
0014110B PUSH DWORD PTR SS:[EBP-0x14]
0014110E PUSH EBX
0014110F PUSH DWORD PTR DS:[0x15FDC0]
00141115 CALL DWORD PTR DS:[0x15C030]
0014111B CMP EAX,EBX
0014111D MOV DWORD PTR SS:[EBP-0x10],EAX
ntdll.771E723C
ntdll.771E723C
UNICODE "ISFB"
ntdll.771E723C
ntdll.RtlAllocateHeap

```

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

```

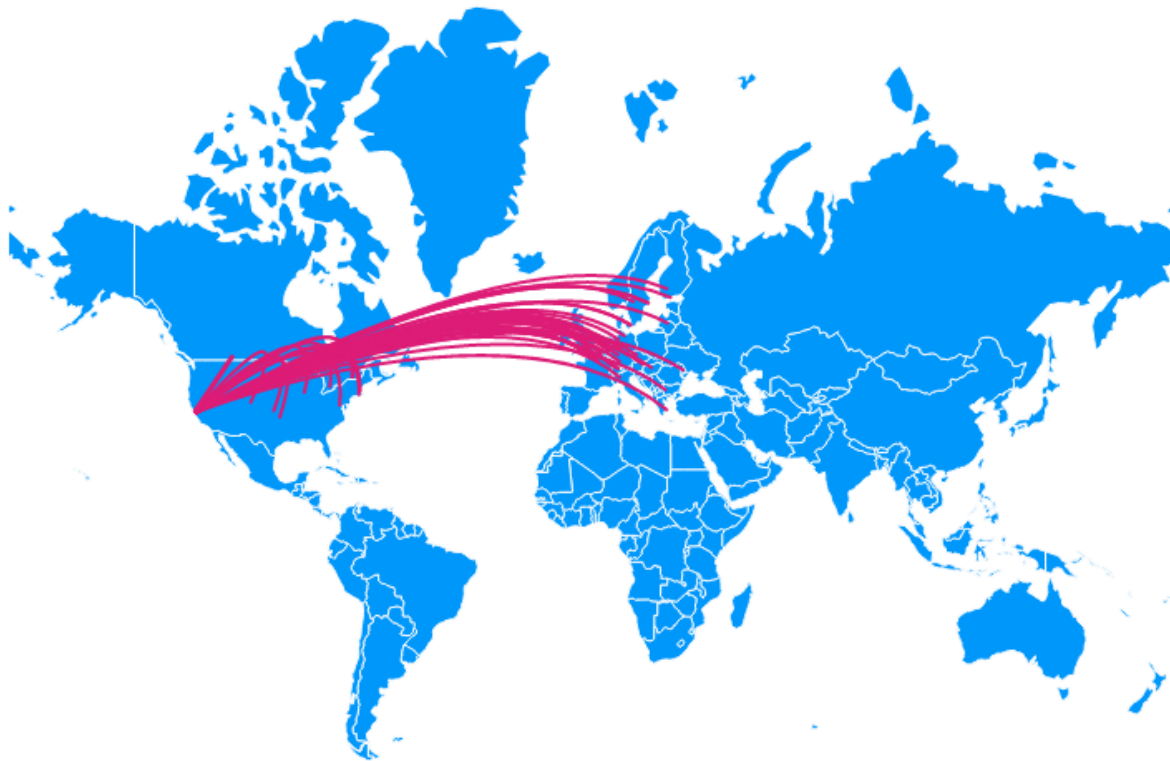
004016A5
004016A5 try_again:
004016A5 lea    eax, [esp+78h+pci]
004016A9 push   eax          ; pci
004016AA mov    [esp+7Ch+pci.cbSize], 14h
004016B2 call   ds:GetCursorInfo
004016B8 mov    eax, [esp+78h+pci.ptScreenPos.y]
004016BC sub    eax, dword ptr [esp+78h+DueTime+4]
004016C0 sub    eax, esi
004016C2 add    eax, [esp+78h+pci.ptScreenPos.x]
004016C6 push   eax
004016C7 call   sub_4037B8
004016CC mov    esi, [esp+78h+pci.ptScreenPos.x]
004016D0 mov    edi, eax
004016D2 cmp    edi, 12
004016D5 mov    eax, [esp+78h+pci.ptScreenPos.y]
004016D9 mov    dword ptr [esp+78h+DueTime+4], eax
004016DD jz     short try_again

```

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:

The screenshot shows a memory map application with a table of memory addresses, sizes, owners, sections, and types. A dump window titled "Dump - 00140000..00188FFF" is overlaid on the memory map. The dump shows hex and ASCII data. A red box highlights a portion of the dump containing a shell prompt and a command.

Address	Size	Owner	Section	Contains	Type	Access	Initial access	Mapped as
00010000	00010000				Map	00041004	RW	\Device\Harddisk...
00020000	00010000				Priv	00021040	RWE	
00030000	00040000				Map	00041002	R	
00040000	00003000				Map	00041002	R	
00050000	00001000				Priv	00021004	RW	
00060000	00067000				Map	00041002	R	
000D0000	00001000				Priv	00021004	RW	
000E0000	00001000				Priv	00021004	RW	
000F0000	00001000				Priv	00021040	RWE	
00100000	00040000				Priv	00021004	RW	
00140000	00049000				Map	00041004	RW	
00190000	0000D000				Map	00041008	RW	\Device\Harddisk...
001A0000	00001000				Map	00041008	RW	
002C4000	00001000				Map	00041008	RW	
002C5000	0001B000				Map	00041008	RW	
002E0000	00007000				Map	00041008	RW	
003A0000	00003000				Map	00041008	RW	
003B0000	00001000				Map	00041008	RW	
003C0000	00002000				Map	00041008	RW	
003D0000	00001000				Map	00041008	RW	
003E0000	00002000				Map	00041008	RW	
003F0000	00011000				Map	00041008	RW	
00430000	00001000				Map	00041008	RW	
00440000	00001000				Map	00041008	RW	
00450000	00001000				Map	00041008	RW	
00460000	00001000				Map	00041008	RW	
00480000	00010000				Map	00041008	RW	
00490000	00037000				Map	00041008	RW	
004D0000	00001000				Map	00041008	RW	
004E0000	00011000				Map	00041008	RW	
00500000	00005000				Map	00041008	RW	
00600000	00001000				Map	00041008	RW	
00630000	00002000				Map	00041008	RW	
00690000	00001000				Map	00041008	RW	
006B0000	0000F000				Map	00041008	RW	
006C0000	00008000				Map	00041008	RW	
006D0000	0000C000				Map	00041008	RW	
006E0000	00002000				Map	00041008	RW	
006F0000	00001000				Map	00041008	RW	
00700000	00001000				Map	00041008	RW	
00710000	00001000				Map	00041008	RW	
00720000	00001000				Map	00041008	RW	
00730000	00001000				Map	00041008	RW	
00740000	00001000				Map	00041008	RW	
00750000	00001000				Map	00041008	RW	
00760000	00001000				Map	00041008	RW	
00770000	00001000				Map	00041008	RW	
00780000	00001000				Map	00041008	RW	
00790000	00001000				Map	00041008	RW	
007A0000	00001000				Map	00041008	RW	
007B0000	00001000				Map	00041008	RW	
007C0000	00001000				Map	00041008	RW	
007D0000	00001000				Map	00041008	RW	
007E0000	00001000				Map	00041008	RW	
007F0000	00001000				Map	00041008	RW	
00800000	00001000				Map	00041008	RW	
00810000	00001000				Map	00041008	RW	
00820000	00001000				Map	00041008	RW	
00830000	00001000				Map	00041008	RW	
00840000	00001000				Map	00041008	RW	
00850000	00001000				Map	00041008	RW	
00860000	00001000				Map	00041008	RW	
00870000	00001000				Map	00041008	RW	
00880000	00001000				Map	00041008	RW	
00890000	00001000				Map	00041008	RW	
008A0000	00001000				Map	00041008	RW	
008B0000	00001000				Map	00041008	RW	
008C0000	00001000				Map	00041008	RW	
008D0000	00001000				Map	00041008	RW	
008E0000	00001000				Map	00041008	RW	
008F0000	00001000				Map	00041008	RW	
00900000	00001000				Map	00041008	RW	
00910000	00001000				Map	00041008	RW	
00920000	00001000				Map	00041008	RW	
00930000	00001000				Map	00041008	RW	
00940000	00001000				Map	00041008	RW	
00950000	00001000				Map	00041008	RW	
00960000	00001000				Map	00041008	RW	
00970000	00001000				Map	00041008	RW	
00980000	00001000				Map	00041008	RW	
00990000	00001000				Map	00041008	RW	
009A0000	00001000				Map	00041008	RW	
009B0000	00001000				Map	00041008	RW	
009C0000	00001000				Map	00041008	RW	
009D0000	00001000				Map	00041008	RW	
009E0000	00001000				Map	00041008	RW	
009F0000	00001000				Map	00041008	RW	
00A00000	00001000				Map	00041008	RW	
00A10000	00001000				Map	00041008	RW	
00A20000	00001000				Map	00041008	RW	
00A30000	00001000				Map	00041008	RW	
00A40000	00001000				Map	00041008	RW	
00A50000	00001000				Map	00041008	RW	
00A60000	00001000				Map	00041008	RW	
00A70000	00001000				Map	00041008	RW	
00A80000	00001000				Map	00041008	RW	
00A90000	00001000				Map	00041008	RW	
00AA0000	00001000				Map	00041008	RW	
00AB0000	00001000				Map	00041008	RW	
00AC0000	00001000				Map	00041008	RW	
00AD0000	00001000				Map	00041008	RW	
00AE0000	00001000				Map	00041008	RW	
00AF0000	00001000				Map	00041008	RW	
00B00000	00001000				Map	00041008	RW	
00B10000	00001000				Map	00041008	RW	
00B20000	00001000				Map	00041008	RW	
00B30000	00001000				Map	00041008	RW	
00B40000	00001000				Map	00041008	RW	
00B50000	00001000				Map	00041008	RW	
00B60000	00001000				Map	00041008	RW	
00B70000	00001000				Map	00041008	RW	
00B80000	00001000				Map	00041008	RW	
00B90000	00001000				Map	00041008	RW	
00BA0000	00001000				Map	00041008	RW	
00BB0000	00001000				Map	00041008	RW	
00BC0000	00001000				Map	00041008	RW	
00BD0000	00001000				Map	00041008	RW	
00BE0000	00001000				Map	00041008	RW	
00BF0000	00001000				Map	00041008	RW	
00C00000	00002000				Map	00041008	RW	
00C10000	00002000				Map	00041008	RW	
00C20000	00002000				Map	00041008	RW	
00C30000	00002000				Map	00041008	RW	
00C40000	00002000				Map	00041008	RW	
00C50000	00002000				Map	00041008	RW	
00C60000	00002000				Map	00041008	RW	
00C70000	00002000				Map	00041008	RW	
00C80000	00002000				Map	00041008	RW	
00C90000	00002000				Map	00041008	RW	
00CA0000	00002000				Map	00041008	RW	
00CB0000	00002000				Map	00041008	RW	
00CC0000	00002000				Map	00041008	RW	
00CD0000	00002000				Map	00041008	RW	
00CE0000	00002000				Map	00041008	RW	
00CF0000	00002000				Map	00041008	RW	
00D00000	00002000				Map	00041008	RW	
00D10000	00002000				Map	00041008	RW	
00D20000	00002000				Map	00041008	RW	
00D30000	00002000				Map	00041008	RW	
00D40000	00002000				Map	00041008	RW	
00D50000	00002000				Map	00041008	RW	
00D60000	00002000				Map	00041008	RW	
00D70000	00002000				Map	00041008	RW	
00D80000	00002000				Map	00041008	RW	
00D90000	00002000				Map	00041008	RW	
00DA0000	00002000				Map	00041008	RW	
00DB0000	00002000				Map	00041008	RW	
00DC0000	00002000				Map	00041008	RW	
00DD0000	00002000				Map	00041008	RW	
00DE0000	00002000				Map	00041008	RW	
00DF0000	00002000				Map	00041008	RW	
00E00000	00002000				Map	00041008	RW	
00E10000	00002000				Map	00041008	RW	
00E20000	00002000				Map	00041008	RW	
00E30000	00002000				Map	00041008	RW	
00E40000	00002000				Map	00041008	RW	
00E50000	00002000				Map	00041008	RW	
00E60000	00002000				Map	00041008	RW	
00E70000	00002000				Map	00041008	RW	
00E80000	00002000				Map	00041008	RW	
00E90000	00002000				Map	00041008	RW	
00EA0000	00002000				Map	00041008	RW	
00EB0000	00002000				Map	00041008	RW	
00EC0000	00002000				Map	00041008	RW	
00ED0000	00002000				Map	00041008	RW	
00EE0000	00002000				Map	00041008	RW	
00EF0000	00002000				Map	00041008	RW	
00F00000	00002000				Map	00041008	RW	
00F10000	00002000				Map			



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: *[Nighthmare 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.nomundopaula.com.br/user5.php

Payloads from different geos (ISFB):

f2f8843673000b082ad08bd555c8cd023918a3c11af9d74e9fa98f3b1304b6be
f12bc471f040146318a6fbd2879a95d947d494bd0b869dc95c01cfc22af0ab13
61dd7aa2ca44371b7c8cd4dc9e5f3bd05a8c6213d8e6357dfdb9034b1c0fd590
aed39345668d24dced4b83c36321e98ec9f09af3044b94ceecf01662de0189ab

