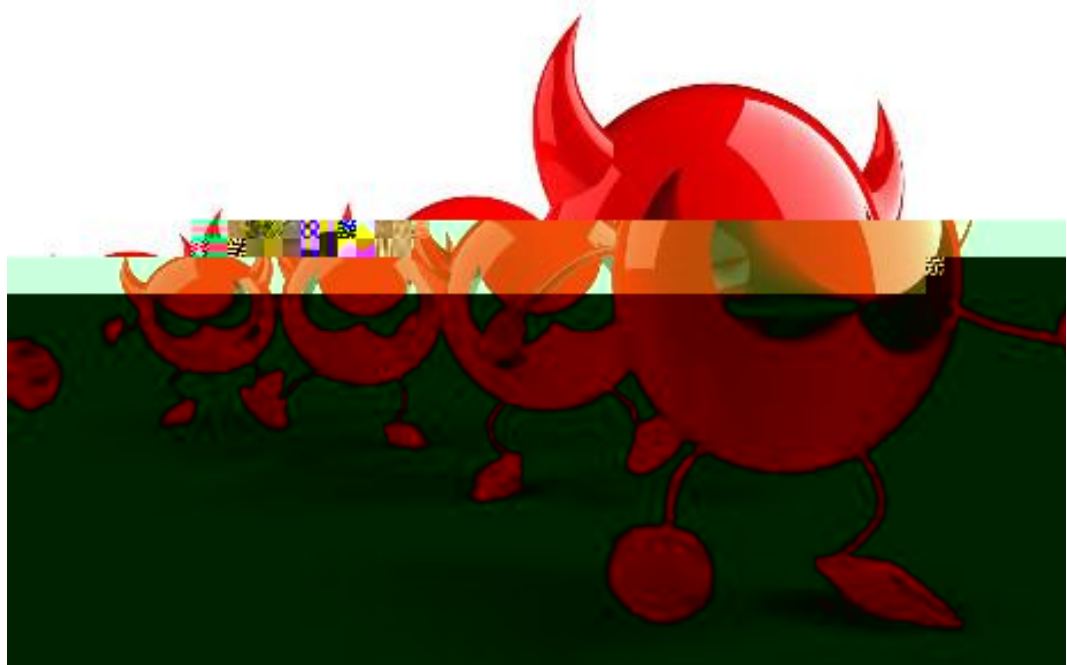




. “	4
.	4
.	4
3.1 0x01.	5
3.2 0x02. Shellcode	10
3.3 0x03. PE dump	12
3.4	14
.	16
4.1 APT	16
4.2	16
. APT	17
5.1 APT	17
5.2 VenusEye	18



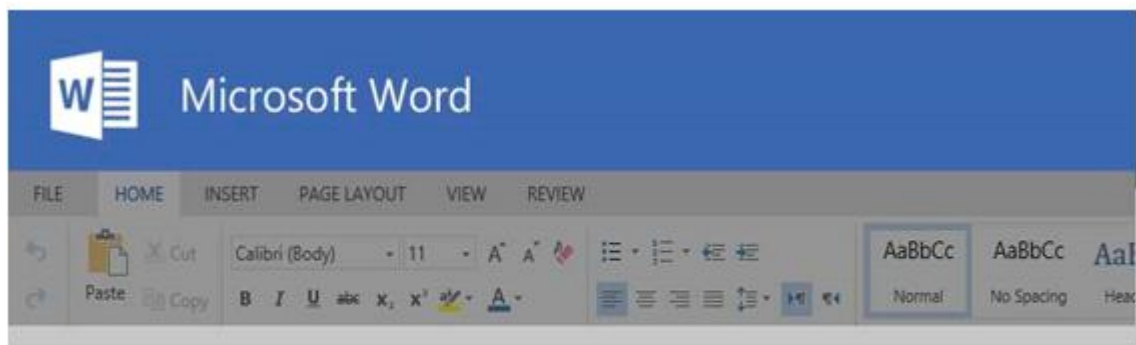
API

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

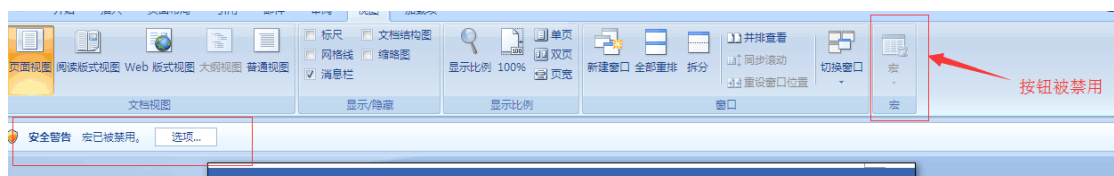
3.1

3.1 0x01.

1

Office

Word



3.2

2

```
Dim salvelinus As String
Dim cruststand
Dim otiosity
Dim hebetude
Dim burrock As String
Dim brassband

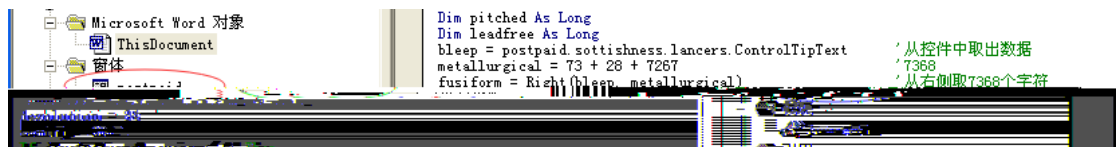
Sub bellwort()
Dim pitched As Long
Dim leadfree As Long
bleep = postpaid.sottishness.lancers.ControlTipText
metallurgical = 73 + 28 + 7267
fusiform = Right(bleep, metallurgical)
mandemus = luxation.truism(fusiform)
devolution = 64
scrip = 63
If devolution + scrip < 11 Then
devolution = UCase$("ca") & Mid("advancednosaurxenorhynchus", 9, 7)
otiosity = "aggsandirement"
nails = Right$("narrowmindedlac", 3) & Mid("archesporetobacillusalmondshaped", 11, 10)
Else
hebetude = brassband * 3
scrip = 68
End If

dicamptodontidae = Mid("megalomaniacalfagymkhana", 15, 2) & UCase$("St")
myeloblast = "malathion"
#If Win64 And Len("fortinet should create new signature") = 36 Then
Dim approachable As String
Dim communicating As acetous
Dim contractor As LongPtr
communicating.sheet = 0
Dim virginals As Byte
#Else
Dim inconceivableness As Byte
communicating = 0
Dim congridae As Long
Dim contractor As Long
#End If
sufficit = 42 - 110 + 68

autorgastic = 4 - 63 + 4135
mazer = 62
fannel = 58
If mazer + fannel < 12 Then
mazer = Mid("consumafiscuits", 7, 2) & Left("oremarking", 3)
brassband = brassband / 288
lovingkindness = Left("&#pittsburgh", 2) & Mid("edgingcesta", 7, 4) & "ry"
Else
hebetude = brassband And 398
fannel = 26
End If
shandrednan = "nessun"
```

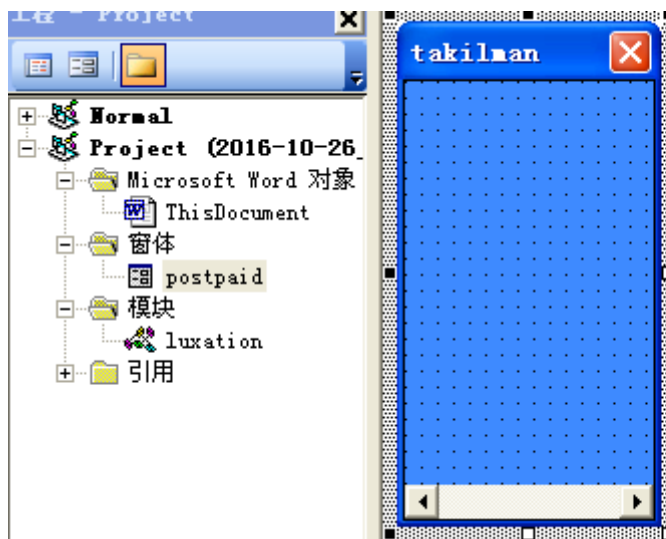
3.3

3 postpaid Toggle Button
ControlTipText 7368



3.4

4 postpaid Toggle Button



ToggleButton

ControlTipText

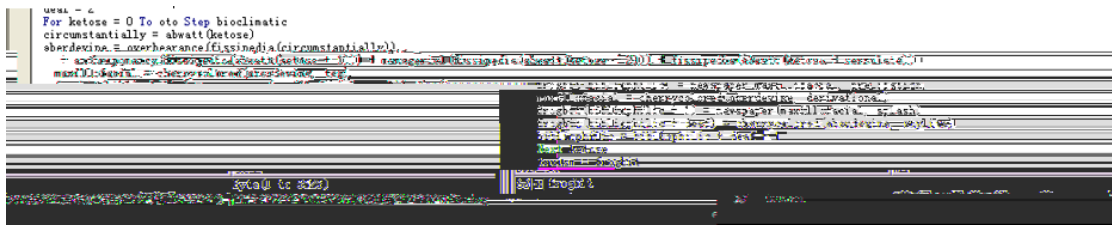


鼠标悬停在按钮上时可以看到ControlTipText提示信息

3.7 ControlTipText

6 ControlTipText

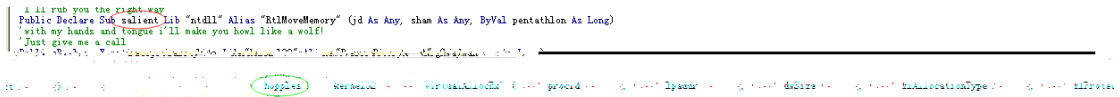
shellcode



3.8

shellcode

7 RtlMoveMemory VirtualAllocEx salient hopples



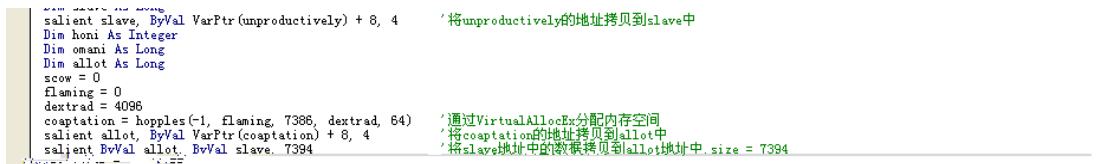
3.9

8 unproductively

shellcode

VirtualAllocEx

RtlMoveMemory shellcode

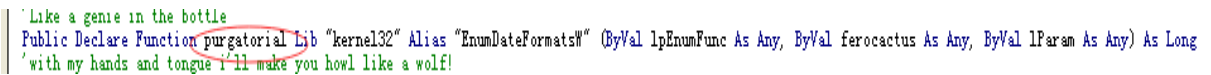


3.10

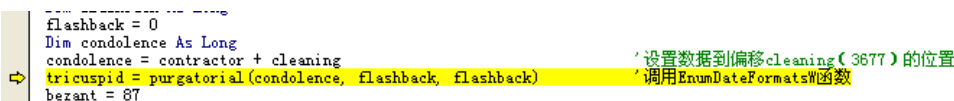
RtlMoveMemory

9 shellcode shellcode

EnumDateFormats



3.11 EnumDateFormats



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

Address	Disassembly	Comment	Hex
7C8387F9	8BFF	mov esi,edi	
7C8387FB	55	push ebp	
7C8387FC	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 kernel132.7C838819	
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 A853887C	mov eax,dword ptr ds:[0x7C8853A8]	
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 kernel132.7C8493CD	
7C838830	A1 5053887C	mov eax,dword ptr ds:[0x7C885350]	
7C838835	85C0	test eax,eax	
7C838837	0F84 8D000000	js kernel132.7C8388CA	
7C83883D	8B5D 08	mov ebx,dword ptr ss:[ebp+0x8]	
7C838840	85D8	test ebx,ebx	
7C838842	0F84 82000000	js kernel132.7C8388CA	
edi=0012EE68			
6504CDC7	RETURN to UBE6.6504CDC7		
0A520E5D	55	push ebp	
0A520E5E	8BEC	mov ebp,esp	
0A520E60	81EC CC070000	sub esp,0x7CC	
0A520E66	6A:A1 30000000	mov eax,dword ptr fs:[0x30]	
0A520E6C	8B40 0C	mov eax,dword ptr ds:[eax+0xC]	
0A520E6F	8B40 10	mov eax,dword ptr ds:[eax+0x10]	
0A520E72	8B40 14	mov eax,dword ptr ds:[eax+0x14]	
0A520E75	8B40 18	mov eax,dword ptr ds:[eax+0x18]	
0A520E78	8B40 1C	mov eax,dword ptr ds:[eax+0x1C]	
0A520E7B	8B40 20	mov eax,dword ptr ds:[eax+0x20]	
0A520E7E	8B40 24	mov eax,dword ptr ds:[eax+0x24]	
0A520E81	8B40 28	mov eax,dword ptr ds:[eax+0x28]	
0A520E84	8B40 2C	mov eax,dword ptr ds:[eax+0x2C]	
0A520E87	8B40 30	mov eax,dword ptr ds:[eax+0x30]	
0A520E8A	8B40 34	mov eax,dword ptr ds:[eax+0x34]	
0A520E8D	8B40 38	mov eax,dword ptr ds:[eax+0x38]	
0A520E90	8B40 3C	mov eax,dword ptr ds:[eax+0x3C]	
0A520E93	8B40 40	mov eax,dword ptr ds:[eax+0x40]	
0A520E96	8B40 44	mov eax,dword ptr ds:[eax+0x44]	
0A520E99	8B40 48	mov eax,dword ptr ds:[eax+0x48]	
0A520E9C	8B40 4C	mov eax,dword ptr ds:[eax+0x4C]	
0A520E9F	8B40 50	mov eax,dword ptr ds:[eax+0x50]	
0A520EA2	8B40 54	mov eax,dword ptr ds:[eax+0x54]	
0A520EA5	8B40 58	mov eax,dword ptr ds:[eax+0x58]	
0A520EA8	8B40 5C	mov eax,dword ptr ds:[eax+0x5C]	
0A520EAB	8B40 60	mov eax,dword ptr ds:[eax+0x60]	
0A520EAE	8B40 64	mov eax,dword ptr ds:[eax+0x64]	
0A520EAD	8B40 68	mov eax,dword ptr ds:[eax+0x68]	
0A520EAC	8B40 6C	mov eax,dword ptr ds:[eax+0x6C]	
0A520EAF	8B40 70	mov eax,dword ptr ds:[eax+0x70]	
0A520EB2	8B40 74	mov eax,dword ptr ds:[eax+0x74]	
0A520EB5	8B40 78	mov eax,dword ptr ds:[eax+0x78]	
0A520EB8	8B40 7C	mov eax,dword ptr ds:[eax+0x7C]	
0A520EBB	8B40 80	mov eax,dword ptr ds:[eax+0x80]	
0A520EBE	8B40 84	mov eax,dword ptr ds:[eax+0x84]	
0A520EB9	8B40 88	mov eax,dword ptr ds:[eax+0x88]	
0A520EBC	8B40 8C	mov eax,dword ptr ds:[eax+0x8C]	
0A520EBF	8B40 90	mov eax,dword ptr ds:[eax+0x90]	
0A520EC2	8B40 94	mov eax,dword ptr ds:[eax+0x94]	
0A520EC5	8B40 98	mov eax,dword ptr ds:[eax+0x98]	
0A520EC8	8B40 9C	mov eax,dword ptr ds:[eax+0x9C]	
0A520ECB	8B40 A0	mov eax,dword ptr ds:[eax+0xA0]	
0A520ECE	8B40 A4	mov eax,dword ptr ds:[eax+0xA4]	

3.14 EnumDateFormats

7C8389DC	E8 4F 97 0F	CALL kernel132.7C831210	
7C8389D1	33DB	XOR EBX,EBX	
7C8389D3	85C0	TEST EAX,EAX	
7C8389D5	74 3A	JC SHORT kernel132.7C838A11	
7C8389D7	395D 38	CMP DWORD PTR SS:[EBP+0x38],EBX	
7C8389DA	8D85 5CFFFFFF	LEA EAX,DWORD PTR SS:[EBP-0xA4]	
7C8389E0	8985 4CFFFFFF	MOV DWORD PTR SS:[EBP-0xB4],EAX	
7C8389E6	0F84 BE070100	JC kernel132.7C8491A0	
7C8389EC	3975 3C	CMP DWORD PTR SS:[EBP+0x3C],ESI	
7C8389EF	0F84 A3070100	JC kernel132.7C849198	
7C8389F5	50	PUSH EAX	
7C8389F6	FF95 58FFFFFF	CALL DWORD PTR SS:[EBP-0xA8]	call shellcode
7C8389FC	3BC6	CMP EAX,ESI	
7C8389FF	74 11	JC SHORT kernel132.7C838A11	

3.15 EnumDateFormats

shellcode

base64

PE

ADD XOR

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	je 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	881401	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	

3.18 shellcode PE

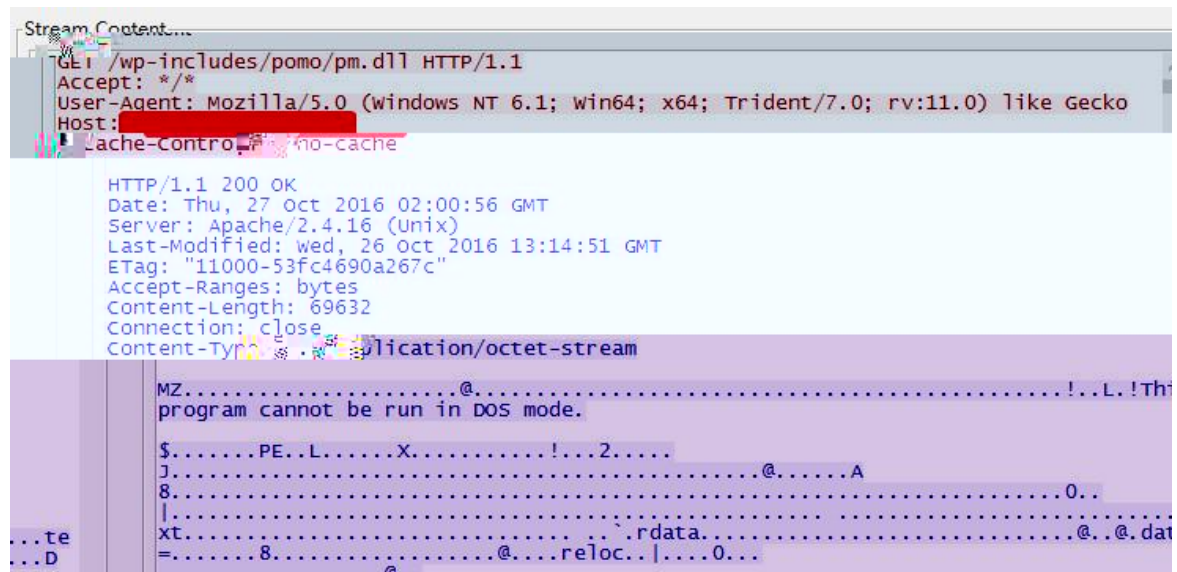
4 explorer.exe

0012DE68	01C714B8	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

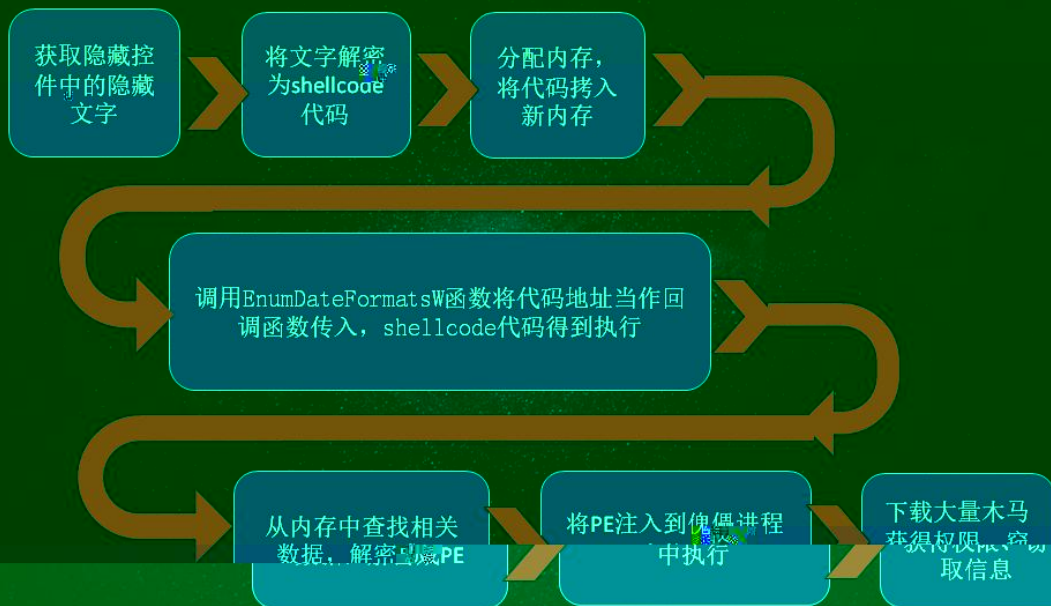
5 explorer.exe unmap
PE

0B2714C6	50	push eax	
0B2714C7	FFB5 68FEFFFF	push dword ptr ss:[ebp-0x198]	
0B2714CD	FF95 B0FEFFFF	call dword ptr ss:[ebp-0x150]	kernel32.GetThreadContext
0B2714D3	85C0	test eax, eax	
0B2714D5	0F84 B2000000	jg 0B27158D	
0B2714DB	BF 00004000	mov edi, 0x400000	
0B2714E0	57	push edi	
0B2714E1	FFB5 64FEFFFF	push dword ptr ss:[ebp-0x19C]	
0B2714E7	FF95 50FEFFFF	call dword ptr ss:[ebp-0x180]	ntdll.ZwUnmapViewOfSection
0B2714ED	8B45 F4	mov eax, dword ptr ss:[ebp-0xC]	
0B2714F0	E8 6FF7FFFF	call 0B270C64	
0B2714F5	6A 40	push 0x40	
0B2714F7	68 00300000	push 0x3000	
0B2714FC	8BF0	mov esi, eax	
0B2714FE	FF76 50	push dword ptr ds:[esi+0x50]	
0B271501	57	push edi	
0B271502	FFB5 64FEFFFF	push dword ptr ss:[ebp-0x19C]	
0B271508	FF95 60FEFFFF	call dword ptr ss:[ebp-0x1A0]	kernel32.VirtualAllocEx
0B27150E	8945 FC	mov dword ptr ss:[ebp-0x4], eax	
0B271511	3BC3	cmp eax, ebx	
0B271513	74 78	jg short 0B27158D	
0B271515	53	push ebx	
0B271516	FF76 54	push dword ptr ds:[esi+0x54]	
0B27151A	FF76 58	push dword ptr ds:[esi+0x58]	
0B27151D	FF76 5C	push dword ptr ds:[esi+0x5C]	
0B271520	FF76 60	push dword ptr ds:[esi+0x60]	
0B271523	FF76 64	push dword ptr ds:[esi+0x64]	
0B271526	FF76 68	push dword ptr ds:[esi+0x68]	
0B271529	FF76 6C	push dword ptr ds:[esi+0x6C]	
0B27152C	FF76 70	push dword ptr ds:[esi+0x70]	
0B27152F	FF76 74	push dword ptr ds:[esi+0x74]	
0B271532	FF76 78	push dword ptr ds:[esi+0x78]	
0B271535	FF76 7C	push dword ptr ds:[esi+0x7C]	
0B271538	FF76 80	push dword ptr ds:[esi+0x80]	
0B27153B	FF76 84	push dword ptr ds:[esi+0x84]	
0B27153E	FF76 88	push dword ptr ds:[esi+0x88]	
0B271541	FF76 8C	push dword ptr ds:[esi+0x8C]	
0B271544	FF76 90	push dword ptr ds:[esi+0x90]	
0B271547	FF76 94	push dword ptr ds:[esi+0x94]	
0B27154A	FF76 98	push dword ptr ds:[esi+0x98]	
0B27154D	FF76 9C	push dword ptr ds:[esi+0x9C]	
0B271550	FF76 A0	push dword ptr ds:[esi+0xA0]	
0B271553	FF76 A4	push dword ptr ds:[esi+0xA4]	
0B271556	FF76 A8	push dword ptr ds:[esi+0xA8]	
0B271559	FF76 AC	push dword ptr ds:[esi+0xAC]	
0B27155C	FF76 B0	push dword ptr ds:[esi+0xB0]	
0B27155F	FF76 B4	push dword ptr ds:[esi+0xB4]	
0B271562	FF76 B8	push dword ptr ds:[esi+0xB8]	
0B271565	FF76 BC	push dword ptr ds:[esi+0xBC]	
0B271568	FF76 C0	push dword ptr ds:[esi+0xC0]	
0B27156B	FF76 C4	push dword ptr ds:[esi+0xC4]	
0B27156E	FF76 C8	push dword ptr ds:[esi+0xC8]	
0B271571	FF76 CC	push dword ptr ds:[esi+0xCC]	
0B271574	FF76 D0	push dword ptr ds:[esi+0xD0]	
0B271577	FF76 D4	push dword ptr ds:[esi+0xD4]	
0B27157A	FF76 D8	push dword ptr ds:[esi+0xD8]	
0B27157D	FF76 DC	push dword ptr ds:[esi+0xDC]	
0B271580	FF76 E0	push dword ptr ds:[esi+0xE0]	
0B271583	FF76 E4	push dword ptr ds:[esi+0xE4]	
0B271586	FF76 E8	push dword ptr ds:[esi+0xE8]	
0B271589	FF76 EC	push dword ptr ds:[esi+0xEC]	
0B27158C	FF76 F0	push dword ptr ds:[esi+0xF0]	
0B27158F	FF76 F4	push dword ptr ds:[esi+0xF4]	
0B271592	FF76 F8	push dword ptr ds:[esi+0xF8]	
0B271595	FF76 FC	push dword ptr ds:[esi+0xFC]	
0B271598	FF77 00	push dword ptr ds:[esi+0x00]	
0B27159B	FF77 04	push dword ptr ds:[esi+0x04]	
0B27159E	FF77 08	push dword ptr ds:[esi+0x08]	
0B2715A1	FF77 0C	push dword ptr ds:[esi+0x0C]	
0B2715A4	FF77 10	push dword ptr ds:[esi+0x10]	
0B2715A7	FF77 14	push dword ptr ds:[esi+0x14]	
0B2715AA	FF77 18	push dword ptr ds:[esi+0x18]	
0B2715AD	FF77 1C	push dword ptr ds:[esi+0x1C]	
0B2715B0	FF77 20	push dword ptr ds:[esi+0x20]	
0B2715B3	FF77 24	push dword ptr ds:[esi+0x24]	
0B2715B6	FF77 28	push dword ptr ds:[esi+0x28]	
0B2715B9	FF77 2C	push dword ptr ds:[esi+0x2C]	
0B2715BC	FF77 30	push dword ptr ds:[esi+0x30]	
0B2715BF	FF77 34	push dword ptr ds:[esi+0x34]	
0B2715C2	FF77 38	push dword ptr ds:[esi+0x38]	
0B2715C5	FF77 3C	push dword ptr ds:[esi+0x3C]	
0B2715C8	FF77 40	push dword ptr ds:[esi+0x40]	
0B2715CB	FF77 44	push dword ptr ds:[esi+0x44]	
0B2715CE	FF77 48	push dword ptr ds:[esi+0x48]	
0B2715D1	FF77 4C	push dword ptr ds:[esi+0x4C]	
0B2715D4	FF77 50	push dword ptr ds:[esi+0x50]	
0B2715D7	FF77 54	push dword ptr ds:[esi+0x54]	
0B2715DA	FF77 58	push dword ptr ds:[esi+0x58]	
0B2715DD	FF77 5C	push dword ptr ds:[esi+0x5C]	
0B2715E0	FF77 60	push dword ptr ds:[esi+0x60]	
0B2715E3	FF77 64	push dword ptr ds:[esi+0x64]	
0B2715E6	FF77 68	push dword ptr ds:[esi+0x68]	
0B2715E9	FF77 6C	push dword ptr ds:[esi+0x6C]	
0B2715EC	FF77 70	push dword ptr ds:[esi+0x70]	
0B2715EF	FF77 74	push dword ptr ds:[esi+0x74]	
0B2715F2	FF77 78	push dword ptr ds:[esi+0x78]	
0B2715F5	FF77 7C	push dword ptr ds:[esi+0x7C]	
0B2715F8	FF77 80	push dword ptr ds:[esi+0x80]	
0B2715FB	FF77 84	push dword ptr ds:[esi+0x84]	
0B2715FE	FF77 88	push dword ptr ds:[esi+0x88]	
0B271601	FF77 8C	push dword ptr ds:[esi+0x8C]	
0B271604	FF77 90	push dword ptr ds:[esi+0x90]	
0B271607	FF77 94	push dword ptr ds:[esi+0x94]	
0B27160A	FF77 98	push dword ptr ds:[esi+0x98]	
0B27160D	FF77 9C	push dword ptr ds:[esi+0x9C]	
0B271610	FF77 A0	push dword ptr ds:[esi+0xA0]	
0B271613	FF77 A4	push dword ptr ds:[esi+0xA4]	
0B271616	FF77 A8	push dword ptr ds:[esi+0xA8]	
0B271619	FF77 AC	push dword ptr ds:[esi+0xAC]	
0B27161C	FF77 B0	push dword ptr ds:[esi+0xB0]	
0B27161F	FF77 B4	push dword ptr ds:[esi+0xB4]	
0B271622	FF77 B8	push dword ptr ds:[esi+0xB8]	
0B271625	FF77 BC	push dword ptr ds:[esi+0xBC]	
0B271628	FF77 C0	push dword ptr ds:[esi+0xC0]	
0B27162B	FF77 C4	push dword ptr ds:[esi+0xC4]	
0B27162E	FF77 C8	push dword ptr ds:[esi+0xC8]	
0B271631	FF77 CC	push dword ptr ds:[esi+0xCC]	
0B271634	FF77 D0	push dword ptr ds:[esi+0xD0]	
0B271637	FF77 D4	push dword ptr ds:[esi+0xD4]	
0B27163A	FF77 D8	push dword ptr ds:[esi+0xD8]	
0B27163D	FF77 DC	push dword ptr ds:[esi+0xDC]	
0B271640	FF77 E0	push dword ptr ds:[esi+0xE0]	
0B271643	FF77 E4	push dword ptr ds:[esi+0xE4]	
0B271646	FF77 E8	push dword ptr ds:[esi+0xE8]	
0B271649	FF77 EC	push dword ptr ds:[esi+0xEC]	
0B27164C	FF77 F0	push dword ptr ds:[esi+0xF0]	
0B27164F	FF77 F4	push dword ptr ds:[esi+0xF4]	
0B271652	FF77 F8	push dword ptr ds:[esi+0xF8]	
0B271655	FF77 FC	push dword ptr ds:[esi+0xFC]	
0B271658	FF78 00	push dword ptr ds:[esi+0x00]	
0B27165B	FF78 04	push dword ptr ds:[esi+0x04]	
0B27165E	FF78 08	push dword ptr ds:[esi+0x08]	
0B271661	FF78 0C	push dword ptr ds:[esi+0x0C]	
0B271664	FF78 10	push dword ptr ds:[esi+0x10]	
0B271667	FF78 14	push dword ptr ds:[esi+0x14]	
0B27166A	FF78 18	push dword ptr ds:[esi+0x18]	
0B27166D	FF78 1C	push dword ptr ds:[esi+0x1C]	
0B271670	FF78 20	push dword ptr ds:[esi+0x20]	
0B271673	FF78 24	push dword ptr ds:[esi+0x24]	
0B271676	FF78 28	push dword ptr ds:[esi+0x28]	
0B271679	FF78 2C	push dword ptr ds:[esi+0x2C]	
0B27167C	FF78 30	push dword ptr ds:[esi+0x30]	
0B27167F	FF78 34	push dword ptr ds:[esi+0x34]	
0B271682	FF78 38	push dword ptr ds:[esi+0x38]	
0B271685	FF78 3C	push dword ptr ds:[esi+0x3C]	
0B271688	FF78 40	push dword ptr ds:[esi+0x40]	
0B27168B	FF78 44	push dword ptr ds:[esi+0x44]	
0B27168E	FF78 48	push dword ptr ds:[esi+0x48]	
0B271691	FF78 4C	push dword ptr ds:[esi+0x4C]	
0B271694	FF78 50	push dword ptr ds:[esi+0x50]	
0B271697	FF78 54	push dword ptr ds:[esi+0x54]	
0B27169A	FF78 58	push dword ptr ds:[esi+0x58]	
0B27169D	FF78 5C	push dword ptr ds:[esi+0x5C]	
0B2716A0	FF78 60	push dword ptr ds:[esi+0x60]	
0B2716A3	FF78 64	push dword ptr ds:[esi+0x64]	
0B2716A6	FF78 68	push dword ptr ds:[esi+0x68]	
0B2716A9	FF78 6C	push dword ptr ds:[esi+0x6C]	
0B2716AC	FF78 70	push dword ptr ds:[esi+0x70]	
0B2716AF	FF78 74	push dword ptr ds:[esi+0x74]	
0B2716B2	FF78 78	push dword ptr ds:[esi+0x78]	
0B2716B5	FF78 7C	push dword ptr ds:[esi+0x7C]	
0B2716B8	FF78 80	push dword ptr ds:[esi+0x80]	
0B2716BB	FF78 84	push dword ptr ds:[esi+0x84]	
0B2716BE	FF78 88	push dword ptr ds:[esi+0x88]	
0B2716C1	FF78 8C	push dword ptr ds:[esi+0x8C]	
0B2716C4	FF78 90	push dword ptr ds:[esi+0x90]	
0B2716C7	FF78 94	push dword ptr ds:[esi+0x94]	
0B2716CA	FF78 98	push dword ptr ds:[esi+0x98]	
0B2716CD	FF78 9C	push dword ptr ds:[esi+0x9C]	
0B2716D0	FF78 A0	push dword ptr ds:[esi+0xA0]	
0B2716D3	FF78 A4	push dword ptr ds:[esi+0xA4]	
0B2716D6	FF78 A8	push dword ptr ds:[esi+0xA8]	
0B2716D9	FF78 AC	push dword ptr ds:[esi+0xAC]	
0B2716DC	FF78 B0	push dword ptr ds:[esi+0xB0]	
0B2716DF	FF78 B4	push dword ptr ds:[esi+0xB4]	
0B2716E2	FF78 B8	push dword ptr ds:[esi+0xB8]	
0B2716E5	FF78 BC	push dword ptr ds:[esi+0xBC]	
0B2716E8	FF78 C0	push dword ptr ds:[esi+0xC0]	
0B2716EB	FF78 C4	push dword ptr ds:[esi+0xC4]	
0B2716EE	FF78 C8	push dword ptr ds:[esi+0xC8]	
0B2716F1	FF78 CC	push dword ptr ds:[esi+0xCC]	
0B2716F4	FF78 D0	push dword ptr ds:[esi+0xD0]	
0B2716F7	FF78 D4	push dword ptr ds:[esi+0xD4]	
0B2716FA	FF78 D8	push dword ptr ds:[esi+0xD8]	
0B2716FD	FF78 DC	push dword ptr ds:[esi+0xDC]	
0B271700	FF78 E0	push dword ptr ds:[esi+0xE0]	
0B271703	FF78 E4	push dword ptr ds:[esi+0xE4]	
0B271706	FF78 E8	push dword ptr ds:[esi+0xE8]	
0B271709	FF78 EC	push dword ptr ds:[esi+0xEC]	
0B27170C	FF78 F0	push dword ptr ds:[esi+0xF0]	
0B27170F	FF78 F4	push dword ptr ds:[esi+0xF4]	
0B271712	FF78 F8	push dword ptr ds:[esi+0xF8]	
0B271715	FF78 FC	push dword ptr ds:[esi+0xFC]	
0B271718	FF79 00	push dword ptr ds:[esi+0x00]	
0B27171B	FF79 04	push dword ptr ds:[esi+0x04]	
0B27171E	FF79 08	push dword ptr ds:[esi+0x08]	
0B271721	FF79 0C	push dword ptr ds:[esi+0x0C]	
0B271724	FF79 10	push dword ptr ds:[esi+0x10]	
0B271727	FF79 14	push dword ptr ds:[esi+0x14]	
0B27172A	FF79 18	push dword ptr ds:[esi+0x18]	
0B27172D	FF79 1C	push dword ptr ds:[esi+0x1C]	
0B271730	FF79 20	push dword ptr ds:[esi+0x20]	
0B271733	FF79 24	push dword ptr ds:[esi+0x24]	
0B271736	FF79 28	push dword ptr ds:[esi+0x28]	
0B271739	FF79 2C	push dword ptr ds:[esi+0x2C]	
0B27173C	FF79 30	push dword ptr ds:[esi+0x30]	
0B27173F	FF79 34	push dword ptr ds:[esi+0x34]	
0B271742	FF79 38	push dword ptr ds:[esi+0x38]	
0B271745	FF79 3C	push dword ptr ds:[esi+0x3C]	
0B271748	FF79 40	push dword ptr ds:[esi+0x40]	
0B27174B	FF79 44	push dword ptr ds:[esi+0x44]	
0B27174E	FF79 48	push dword ptr ds:[esi+0x48]	
0B271751	FF79 4C	push dword ptr ds:[esi+0x4C]	
0B271754	FF79 50	push dword ptr ds:[esi+0x50]	
0B271757	FF79 54	push dword ptr ds:[esi+0x54]	
0B27175A	FF79 58	push dword ptr ds:[esi+0x58]	
0B27175D	FF79 5C	push dword ptr ds:[esi+0x5C]	
0B271760	FF79 60	push dword ptr ds:[esi+0x60]	
0B271763	FF79 64	push dword ptr ds:[esi+0x64]	
0B271766	FF79 68	push dword ptr ds:[esi+0x68]	
0B271769	FF79 6C	push dword ptr ds:[esi+0x6C]	
0B27176C	FF79 70	push dword ptr ds:[esi+0x70]	
0B27176F	FF79 74	push dword ptr ds:[esi+0x74]	
0B271772	FF79 78	push dword ptr ds:[esi+0x78]	
0B271775	FF79 7C	push dword ptr ds:[esi+0x7C]	
0B271778	FF79 80	push dword ptr ds:[esi+0x80]	
0B27177B	FF79 84	push dword ptr ds:[esi+0x84]	
0B27177E	FF79 88	push dword ptr ds:[esi+0x88]	
0B271781	FF79 8C	push dword ptr ds:[esi+0x8C]	
0B271784	FF79 90	push dword ptr ds:[esi+0x90]	
0B271787	FF79 94	push dword ptr ds:[esi+0x94]	
0B27178A	FF79 98	push dword ptr ds:[esi+0x98]	
0B27178D	FF79 9C	push dword ptr ds:[esi+0x9C]	
0B271790	FF79 A0	push dword ptr ds:[esi+0xA0]	
0B271793	FF79 A4	push dword ptr ds:[esi+0xA4]	
0B271796	FF79 A8	push dword ptr ds:[esi+0xA8]	
0B271799	FF79 AC	push dword ptr ds:[esi+0xAC]	
0B27179C	FF79 B0	push dword ptr ds:[esi+0xB0]	
0B27179F	FF79 B4	push dword ptr ds:[esi+0xB4]	
0B2717A2	FF79 B8	push dword ptr ds:[esi+0xB8]	
0B2717A5	FF79 BC	push dword ptr ds:[esi+0xBC]	
0B2717A8	FF79 C0	push dword ptr ds:[esi+0xC0]	
0B2717AB	FF79 C4	push dword ptr ds:[esi+0xC4]	
0B2717AE	FF79 C8	push dword ptr ds:[esi+0xC8]	
0B2717B1	FF79 CC	push dword ptr ds:[esi+0xCC]	
0B2717B4	FF79 D0	push dword ptr ds:[esi+0xD0]	
0B2717B7	FF79 D4	push dword ptr ds:[esi+0xD4]	
0B2717BA	FF79 D8	push dword ptr ds:[esi+0xD8]	
0B2717BD	FF79 DC	push dword ptr ds:[esi+0xDC]	
0B2717C0	FF79 E0	push dword ptr ds:[esi+0xE0]	
0B2717C3	FF79 E4	push dword ptr ds:[esi+0xE4]	
0B2717C6	FF79 E8	push dword ptr ds:[esi+0xE8]	
0B2717C9	FF79 EC	push dword ptr ds:[esi+0xEC]	



3.4

宏恶意样本执行流程归纳

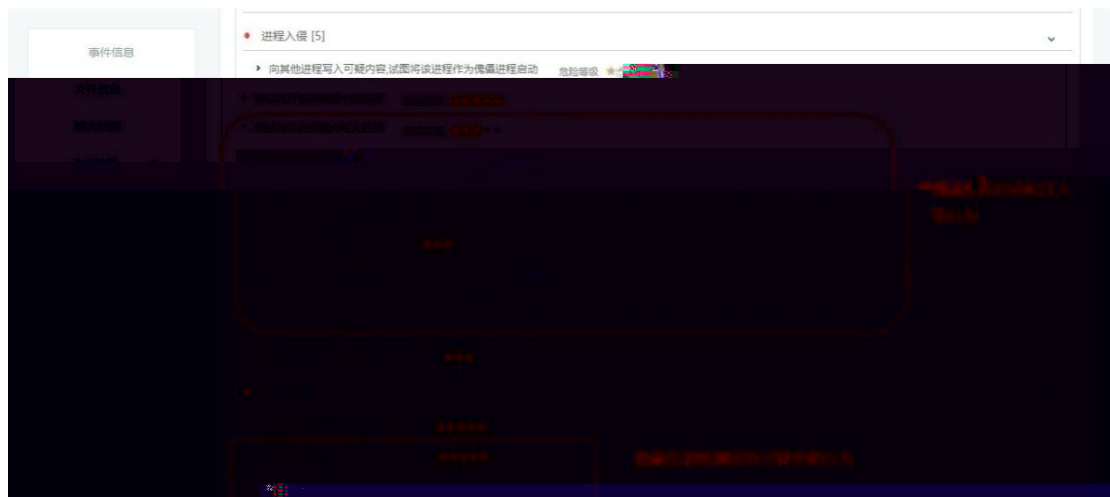


4.1 APT



4.1

4.2



4.2

▪

APT



APT

APT

APT

APT

0-day

APT

5.1

APT

APT

APT

APT

0-day

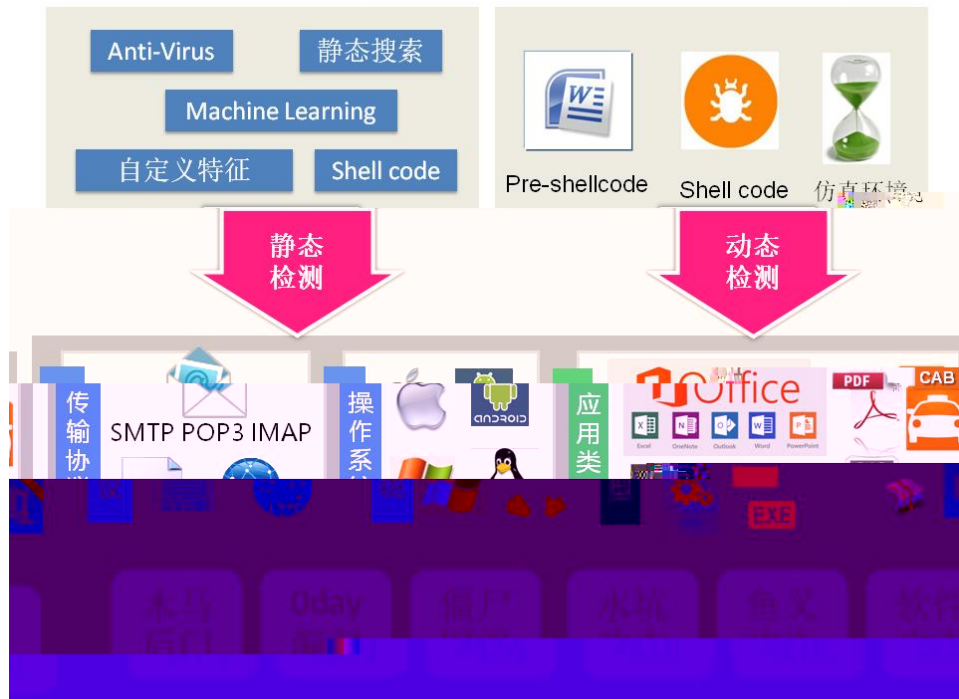
ROP

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

