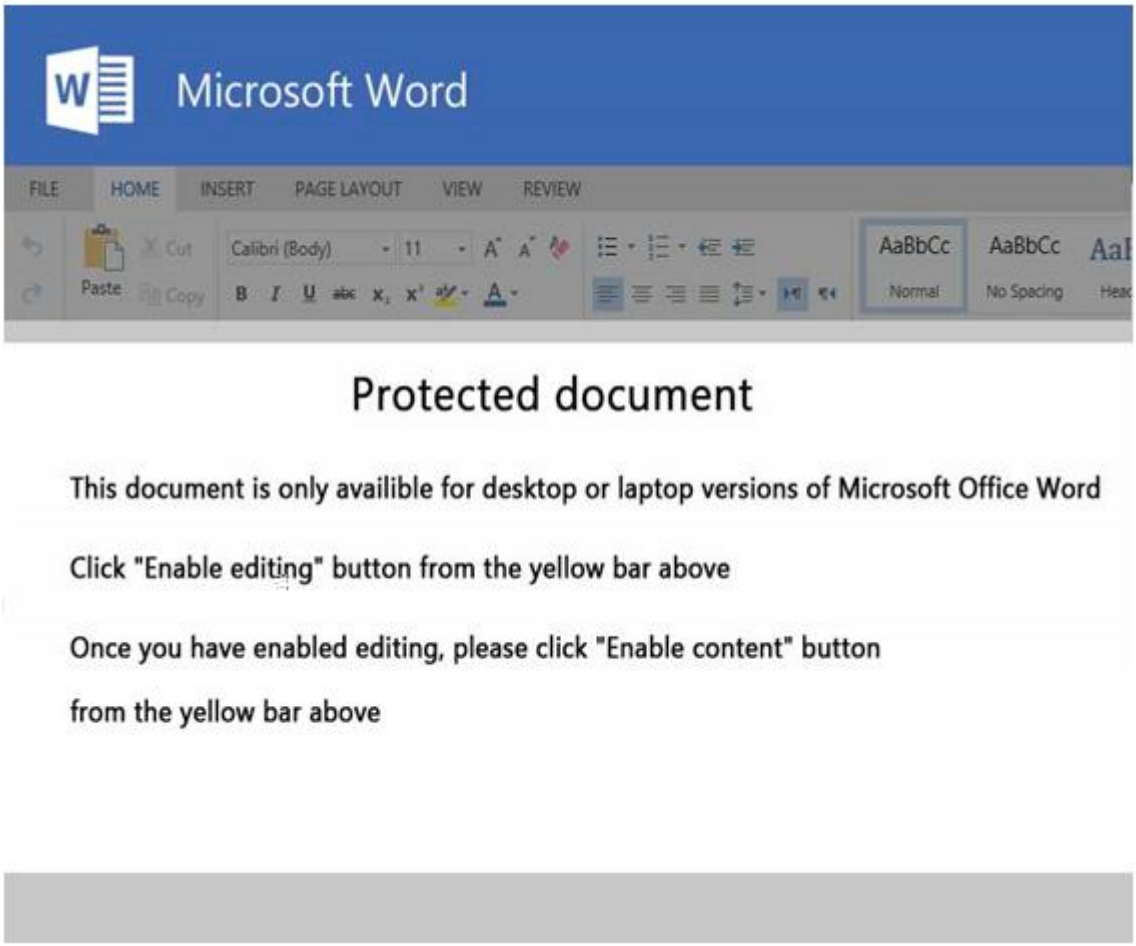
API shellcode

shellcode

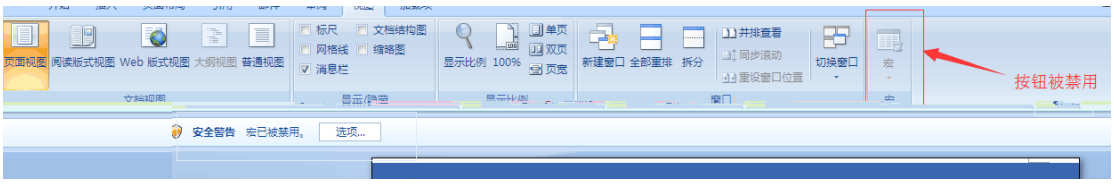
shellcode



3.1

3.1 0x01.

1 Office Word



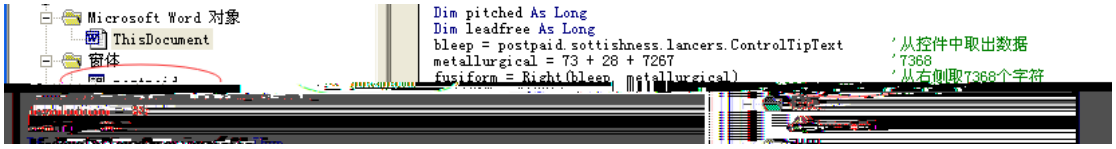
3.2

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
suffuit = 42 - 110 + 68
```

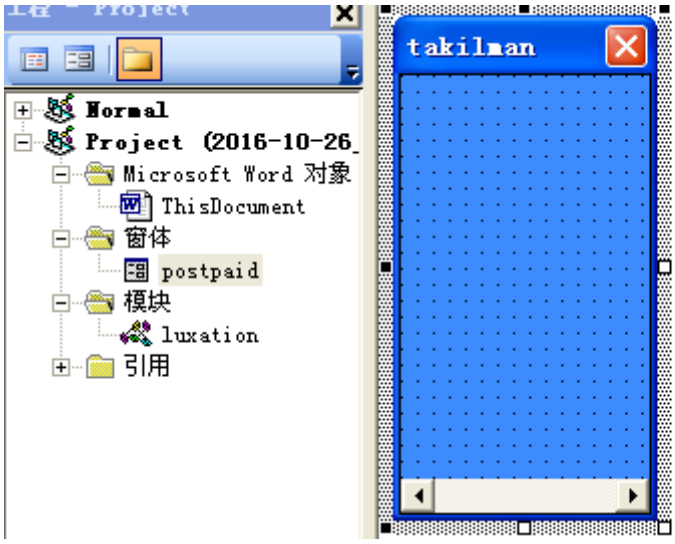
3.3

3 postpaid Toggle Button ControlTipText 7368



3.4

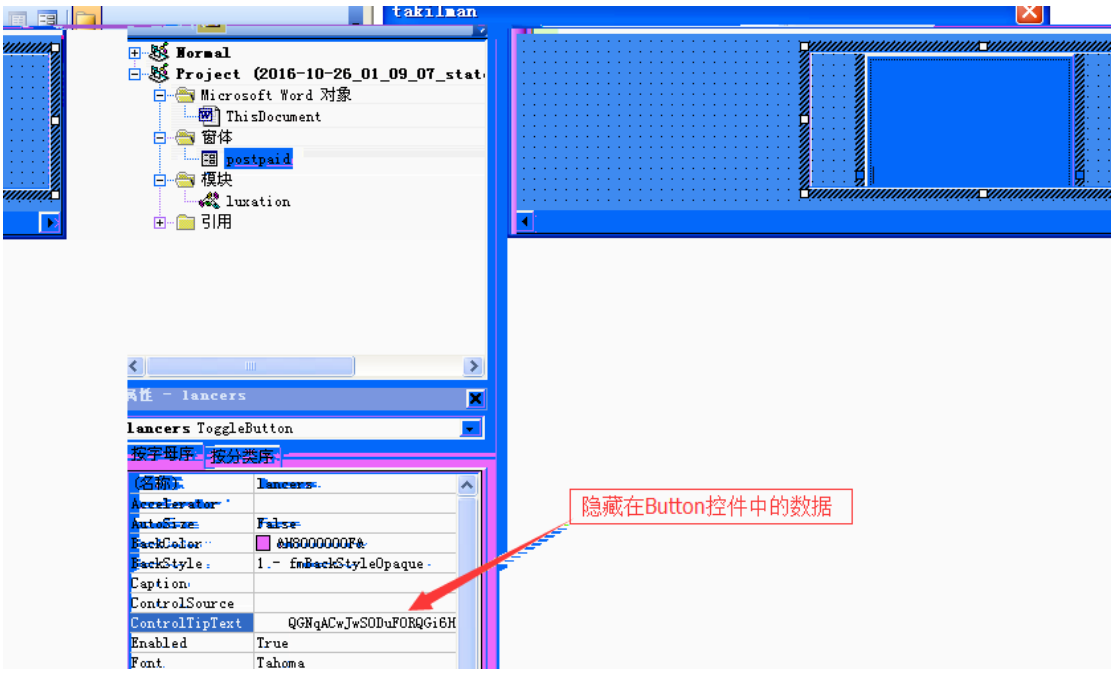
4 postpaid Toggle Button



3.5 Toggle Button

5 ToggleButton ToggleButton
Button

Button ToggleButton ControlTipText
ControlTipText

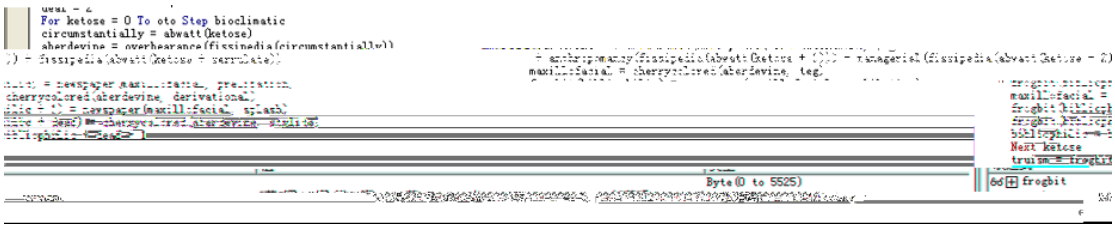


3.6 ControlTipText

3.7 ControlTipText

6 ControlTipText

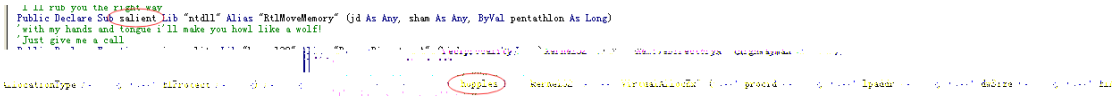
shellcode



3.8 shellcode

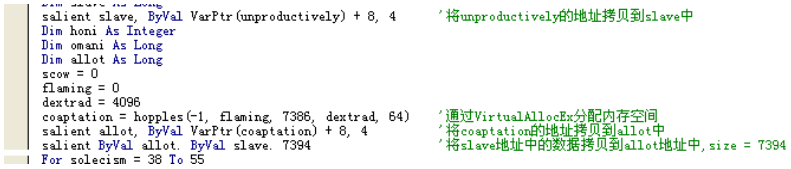
7 RtlMoveMemory VirtualAllocEx

salient hopples



3.9

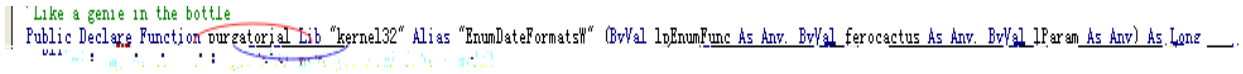
8 unproductively shellcode VirtuallocEx RtlMoveMemory shellcode



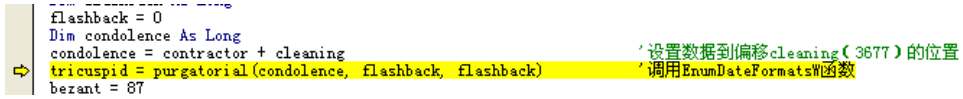
3.10 RtlMoveMemory

9 shellcode EnumDateFormats

shellcode



3.11 EnumDateFormats

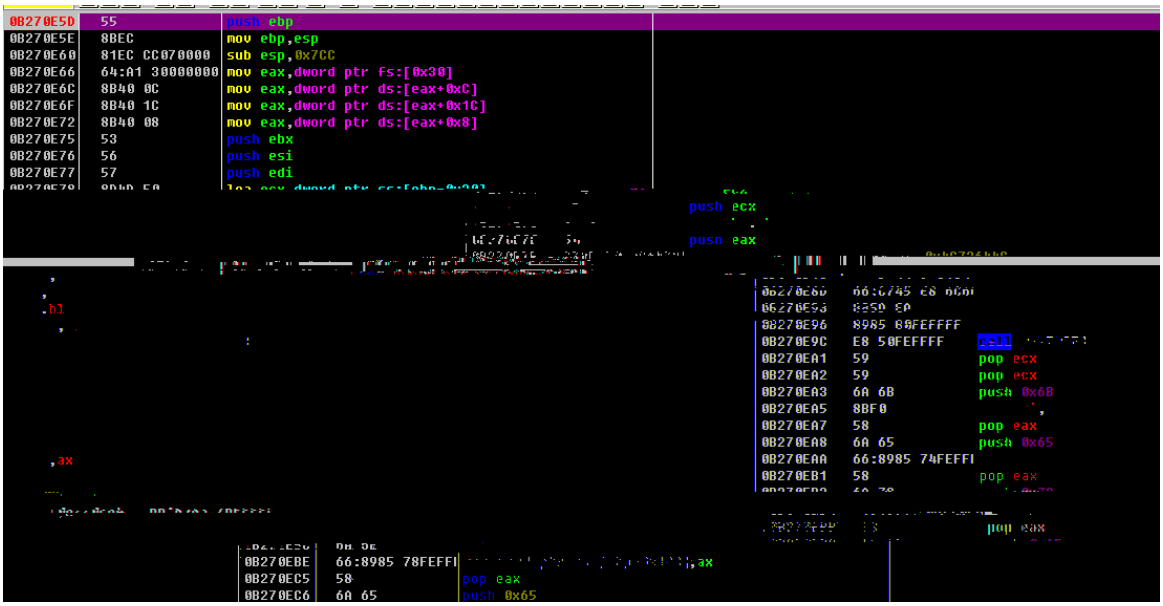


3.12 EnumDateFormats shellcode

3.13 EnumDateFormats

3.2 0x02. Shellcode

1 Shellcode

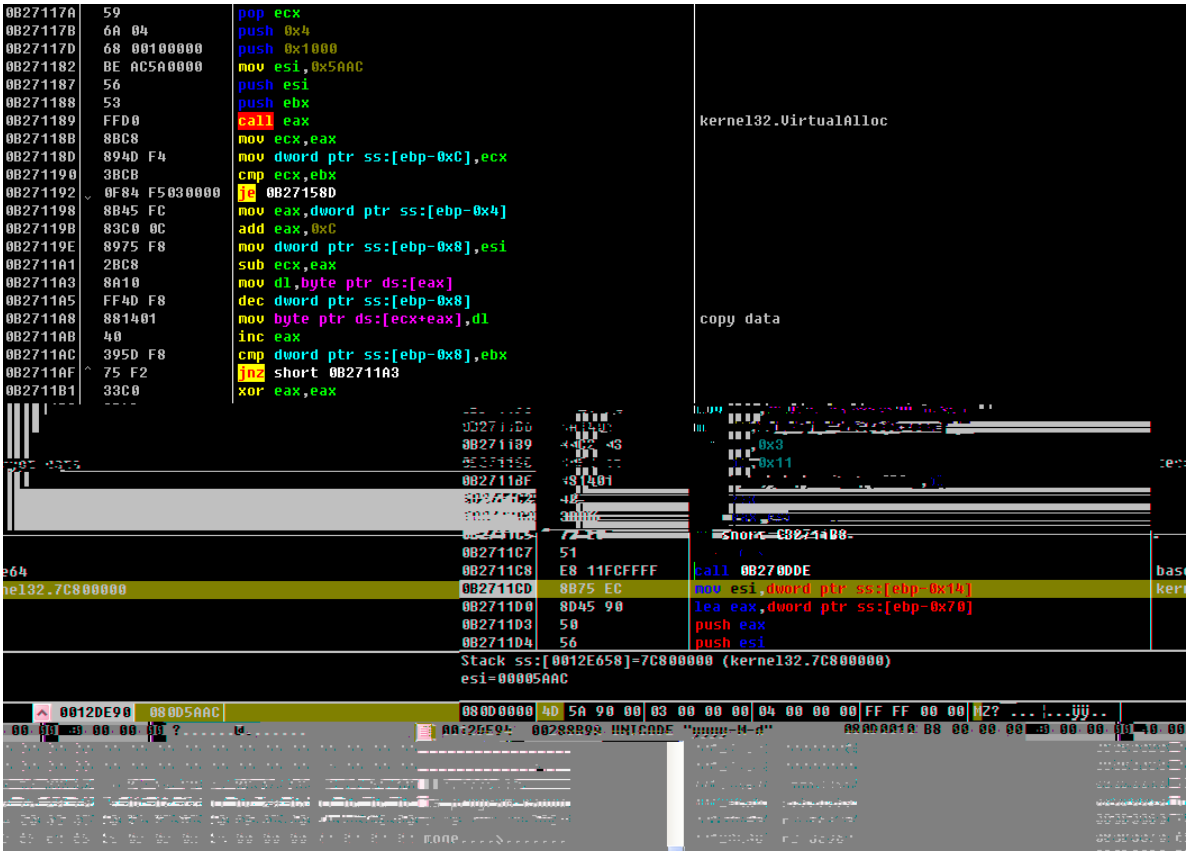


3.16 Shellcode

2 0x1000 magic 0x52415453 0x4C4C4146 GetMappedFileNameA

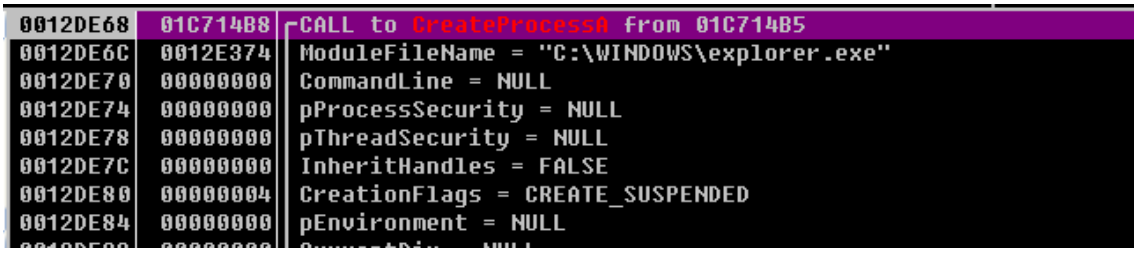
3.17 Shellcode

3 ADD XOR base64 PE



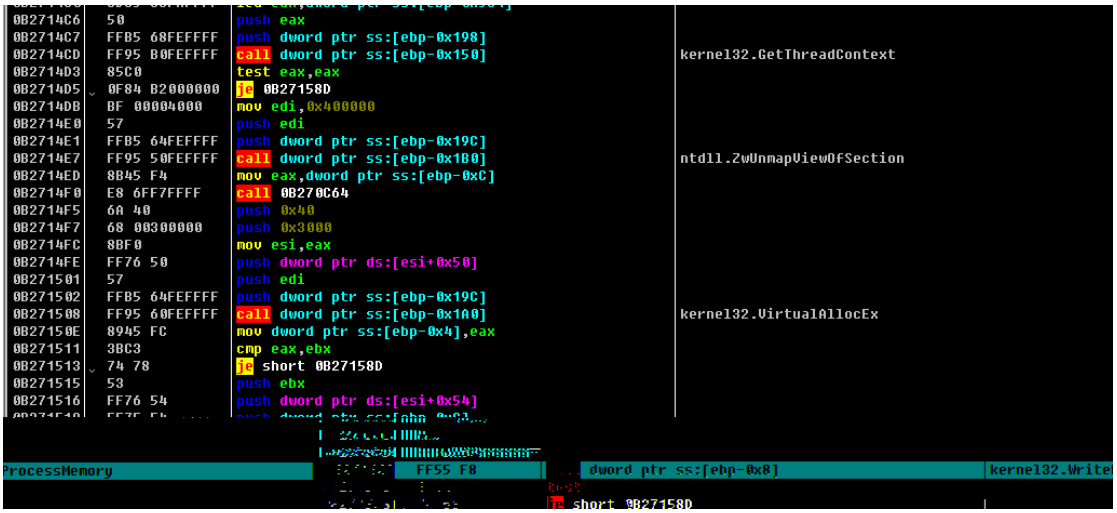
3.18 shellcode PE

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

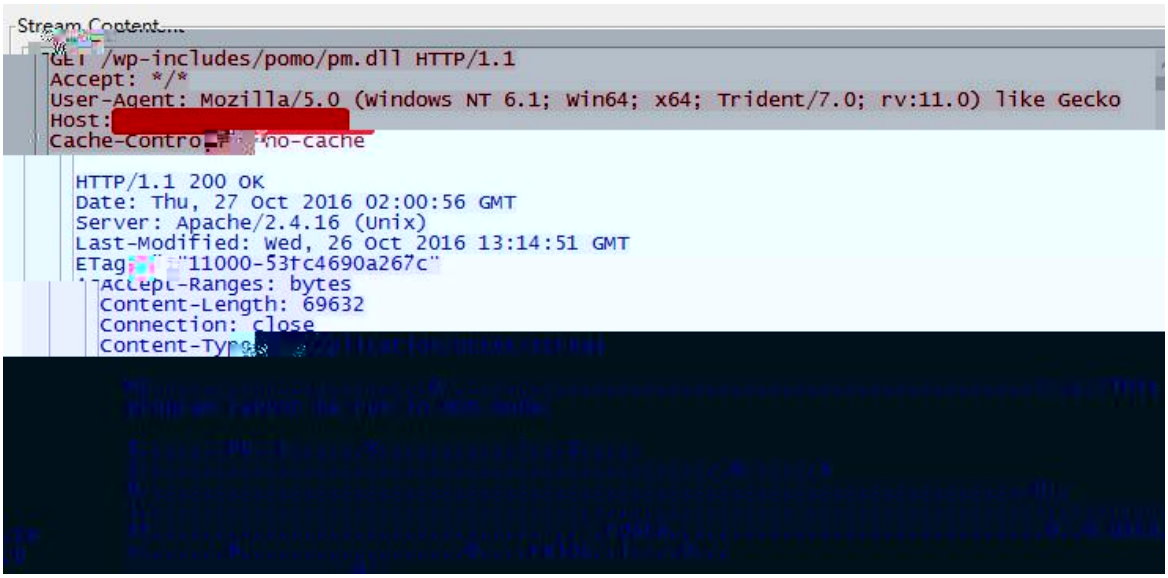
```
{
  int v3; // eax@9

  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' )
  {
```

a1 'r'

v3 sub_40157B(a1

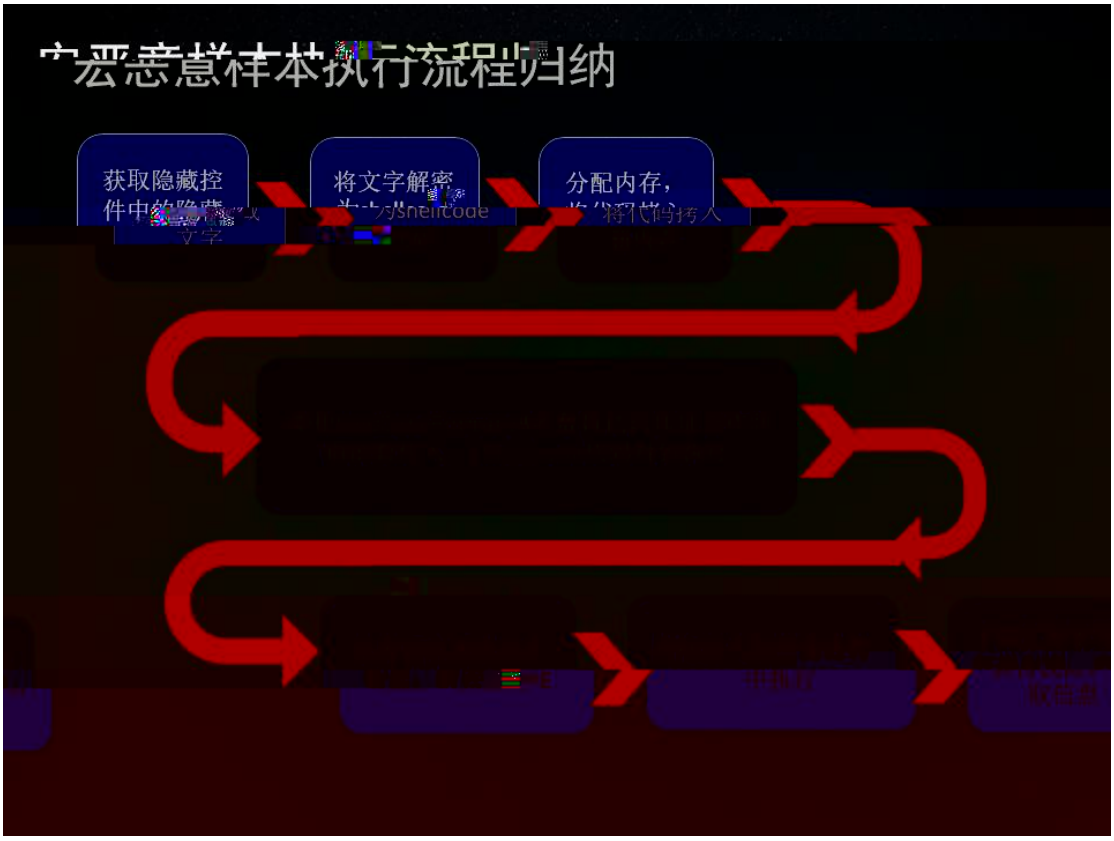
a2

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
分配内存，

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

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