

Office 0-day (CVE-2017-0199)

Office
Office 0-Day
Windows
Office
Windows 10
Office 2016
4 12
CVE-2017-0199

Office

VenusEye

Office

<https://support.microsoft.com/en-us/help/4014793/title>

VenusEye

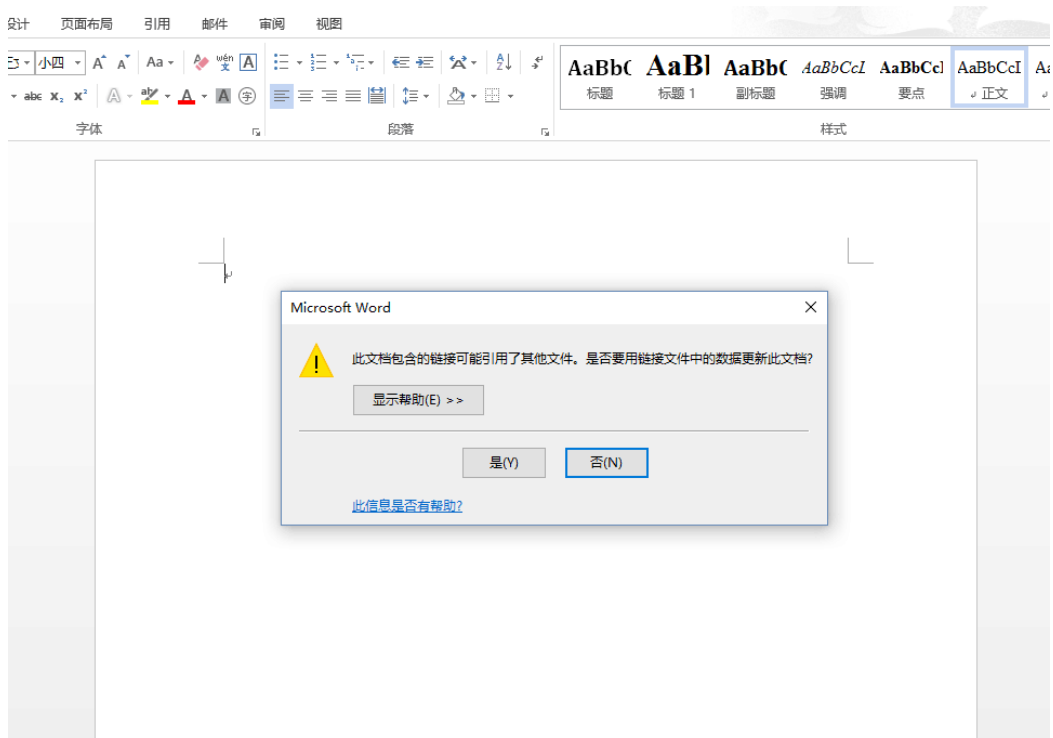
5ebfd13	[REDACTED]	9e01.rtf	2017/4/12 11:54	RTF 格式
6e9483e	[REDACTED]	77b.rtf	2017/4/12 11:54	RTF 格式
20b15c4	[REDACTED]	7dd9.rtf	2017/4/12 11:54	RTF 格式
6538530e	[REDACTED]	04e.rtf	2017/4/12 11:54	RTF 格式
33059f43	[REDACTED]	665.rtf	2017/4/12 11:54	RTF 格式
0404390	[REDACTED]	ae4d.rtf	2017/4/12 11:54	RTF 格式
10dabb	[REDACTED]	af10e.rtf	2017/4/12 11:54	RTF 格式

MD5 65a558e9fe907dc5790e8a592364f64e

office2013

1. Office

http://212.*.*.71/template.doc



2. template.doc rtf hta

template.doc	伪装成RTF文件																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
5C 72 74 66					{\rtf	00000040				0A 0A 0A 0A 0A 0A 0A 0A							0A 0A 0A 7B
32 35 5C 61	1\	a	deflang1025\	a		00000050				31 5C 61 64 65 66 6C 61						6E 67 31 30	
32 35 32 5C	nsi\	ansicpg1252\				00000060				6E 73 69 5C 61 6E 73 69						63 70 67 31	
65 66 66 30	uc1\	adef0\	deff0			00000070				75 63 31 5C 61 64 65 66						66 30 5C 64	
22 74 43 69	\	rich5ch0\	stch			00000080				5C 73 74 73 68 66 6A 62						62 6E 20 5C	
6E 74 43 69	\	rich5ch0\	stch			00000090				5C 73 74 73 68 66 6A 62						62 6E 20 5C	

rtf

1. AP T Oday RTF

Sample Analysis Report (样本分析报告) interface showing file details and dynamic detection results.

File Information:

- 文件名: 65a598e9fe907de5790e8a592304f04e.rtf
- 文件类型: rtf
- 文件大小: 36.6 KB
- 扫描时间: 2017-04-12 11:54:01

Hashes:

- MDS: 65a598e9fe907de5790e8a592304f04e
- SHA1: f806e1d5949b54cee9b35ed87c7caf88f4a8182b
- SHA256: 3c0a934d05b3d0a5f04ff63e8f178d5446f7203a80e3a76a9083a43a7e4df

Dynamic Detection (动态检测) Summary:

- 操作系统: Windows 7
- 开始时间: 2017-04-12 11:54:02

Hidden Channels (隐藏信道 [2]):

- 尝试连接某个服务器 (危险等级 ★★★★★)
可疑地址: 105.17.129.103:90
- 检测到可疑HTTP请求 (危险等级 ★★★★★)
可疑URL: http://212.86.115.71/template.doc

Dynamic Detection (动态检测) results for a virtual machine environment.

System Information:

- 操作系统: Windows XP SP3
- 软件版本: Adobe Reader 11
- 开始时间: 2017-04-12 14:07:06
- 结束时间: 2017-04-12 14:08:10

Virtual Machine (反虚拟机 [7]):

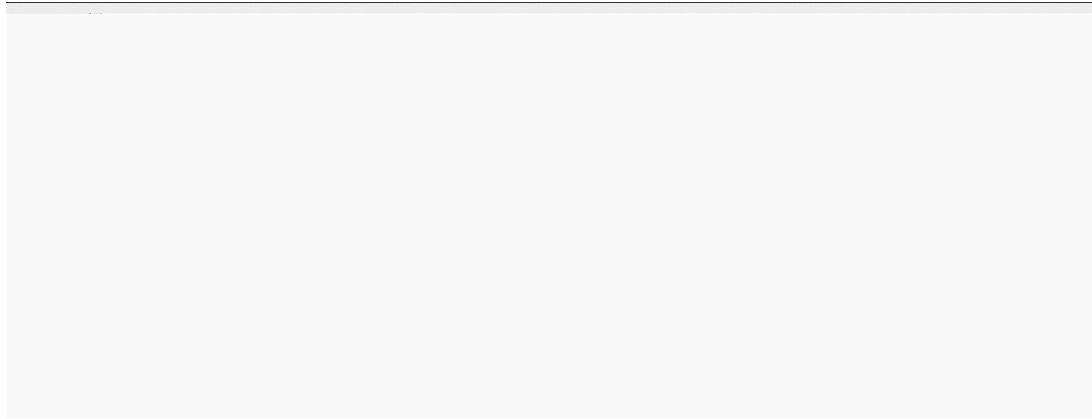
- 通过动态库判断Sunbelt沙箱环境 (危险等级 ★★★★★)
- 尝试通过动态库判断沙箱环境 (危险等级 ★★★★★)
- 通过动态库判断VirtualBox沙箱环境 (危险等级 ★★★★★)
- 通过特定文件判断ThreatTrack沙箱环境 (危险等级 ★★★★★)
- 尝试检测磁盘驱动器 (危险等级 ★★★★★)
- 通过特定文件检测VirtualBox沙箱环境 (危险等级 ★★★★★)
- 通过注册表判断VMware沙箱环境 (危险等级 ★★★★★)

Reverse Engineering (反调试 [1])

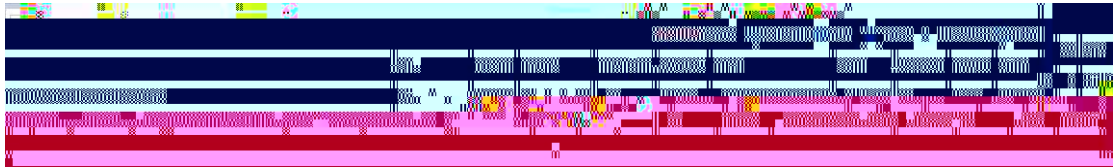
Threat Behavior (威胁行为 [6])

Downloaded file: 下载的大马拥有多种反沙箱反虚拟机功能

2. IDS RTF hta



3. NGIPS RTF hta



4. 0day RTF

景云杀毒

发现 4 个威胁

自定义查杀已完成, 耗时 00:00, 扫描项目 4 个

暂不处理 立刻处理

风险类型	风险信息	处理建议
<input checked="" type="checkbox"/> 下载者木马	RTF.Trojan-DL.CVE-2017-0199.Y1.zav C:\vir\新建文件夹 (2)\sample1.rtf	建议清除
<input checked="" type="checkbox"/> 下载者木马	RTF.Trojan-DL.CVE-2017-0199.Y1.zav C:\vir\新建文件夹 (2)\sample2.rtf	建议清除
<input checked="" type="checkbox"/> 下载者木马	RTF.Trojan-DL.CVE-2017-0199.Y1.zav C:\vir\新建文件夹 (2)\sample3.rtf	建议清除
<input checked="" type="checkbox"/> 下载者木马	RTF.Trojan-DL.CVE-2017-0199.Y1.zav C:\vir\新建文件夹 (2)\sample4.rtf	建议清除

防护日志

信任与隔离

景云杀毒

发现 2 个威胁

自定义杀毒已完成 耗时: 00:06 扫描项目: 2 个

暂不处理 立刻处理

处理建议	病毒名称	风险类别	风险信息
下载者木马	VBS.Trojan-DL.AutoRun.Y1.zav C:\vir\新建文件夹\template.doc_	建议清除	<input checked="" type="checkbox"/> 实时防护 <input checked="" type="checkbox"/>
恶意木马	Win32.Trojan.CVE-2017-0199.Y1.zav C:\vir\新建文件夹\sage50.exe_	建议删除	<input checked="" type="checkbox"/> 常用工具 <input checked="" type="checkbox"/>

防护日志

信任与隔离