

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

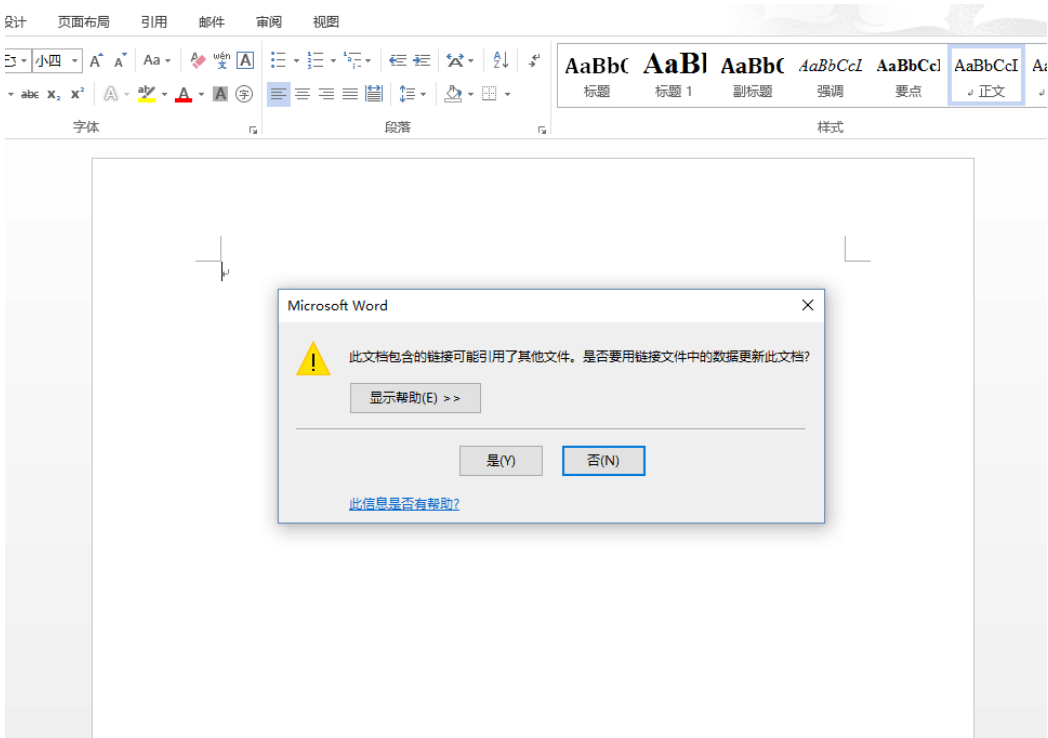
5ebfd13	9e01.rtf	2017/4/12 11:54	RTF 格式
6e9483e	77b.rtf	2017/4/12 11:54	RTF 格式
20b15c4	7dd9.rtf	2017/4/12 11:54	RTF 格式
65d539e	0ae.rtf	2017/4/12 11:54	RTF 格式
3059f43	665.rtf	2017/4/12 11:54	RTF 格式
20404390	ae4d.rtf	2017/4/12 11:54	RTF 格式
10dabb	af10e.rtf	2017/4/12 11:54	RTF 格式

MD5 65a558e9fe907dc5790e8a592364f64e

office2013

1. Office “ ”

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

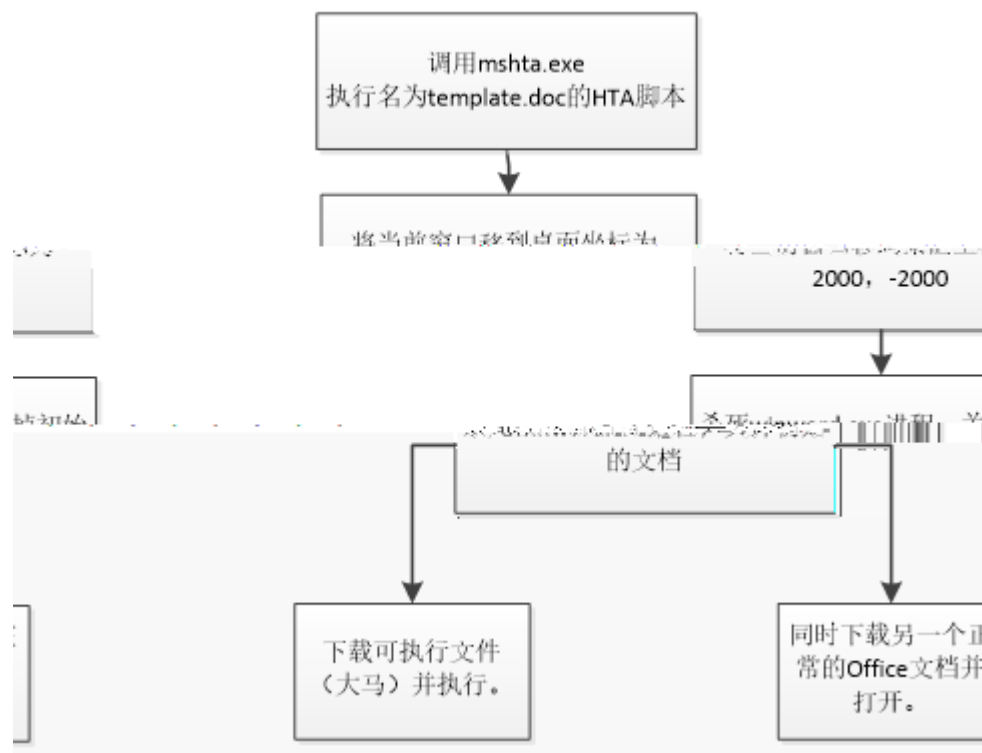


2. template.doc rtf hta

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 0A 0A 0A 0A 0A		0A 0A 0A 0A 7B																				
32 35 5C 61	1\ade	flang1025\	a	00000050		31 5C 61 64 65 66 6C 61		6E 67 31 30																								
32 35 32 5C	nsi\ansi	cp1252\	00000060		6E 73 69 5C 61 6E 73 69		63 70 67 31																									
65 66 66 30	uc1\ade	ff0\deff0	00000070		75 63 31 5C 61 64 65 66		66 30 5C 64																									
22 74 73 69	\rich5	chch0\stch	00000080		5C 73 74 73 6E 6A 6A 6A		6A 6A 6A 6A 6A 6A 6A 6A																									
0E 0E 0E 0E 0E 0E 0E 0E	00000090		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000A0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000B0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000C0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000D0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000E0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	
0E 0E 0E 0E 0E 0E 0E 0E	000000F0		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E		8E 8E 8E 8E 8E 8E 8E 8E																	

rtf

-

[illegible]

1. APT 0day RTF

样本分析报告

查看详细报告

事件信息

文件信息

动态检测

文件名

文件类型

文件大小

扫描时间

05a558e9fe907dc5790e8a592304f64e.rtf

rtf

36.6 KB

2017-04-12 11:54:01

MD5

SHA1

SHA256

05a558e9fe907dc5790e8a592304f64e

f806e1d5949b54cee9b35ed67c7caf88fda8182b

3c0a93d05b3d0a9064df63e8f178d54467203a8e3a76a9083a43a7e4d

样本

时间

Microsoft Office 2010

2017-04-12 11:52:39

动态检测

操作系统

软件

开始时间

Windows 7

Windows 7

2017-04-12 11:54:02

隐藏信道 [2]

尝试连接某个服务器

可疑地址

检测到可疑HTTP请求

可疑URL

危险等级

危险等级

危险等级

危险等级

危险等级

可疑地址

可疑URL

105.77.129.103:80

http://212.86.115.71/template.doc

动态检测

操作系统

软件版本

开始时间

结束时间

Windows XP SP3

Adobe Reader 11

2017-04-12 14:07:06

2017-04-12 14:08:10

反虚拟机 [7]

通过动态库判断Sunbelt沙箱环境

尝试通过动态库判断沙箱环境

通过动态库判断VirtualBox沙箱环境

通过特定文件判断ThreatTrack沙箱环境

尝试检测磁盘驱动器

通过特定文件检测VirtualBox沙箱环境

通过注册表判断VMware沙箱环境

危险等级

危险等级

危险等级

危险等级

危险等级

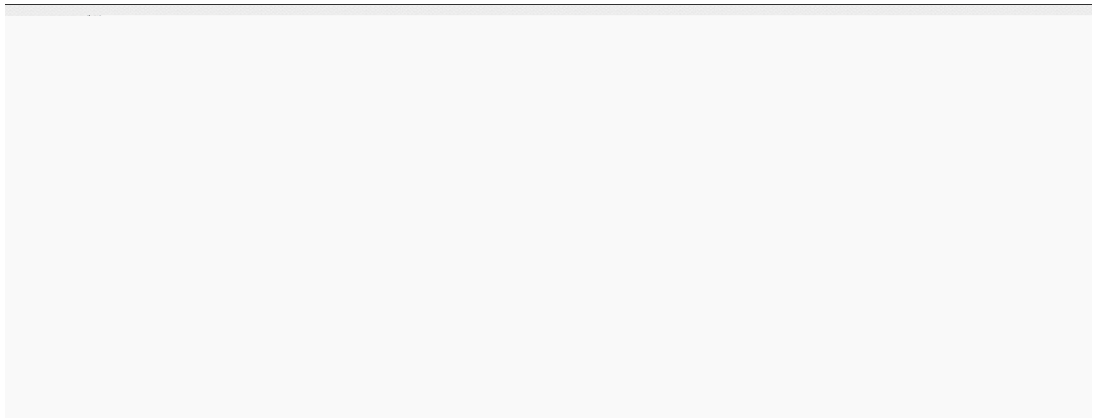
危险等级

危险等级

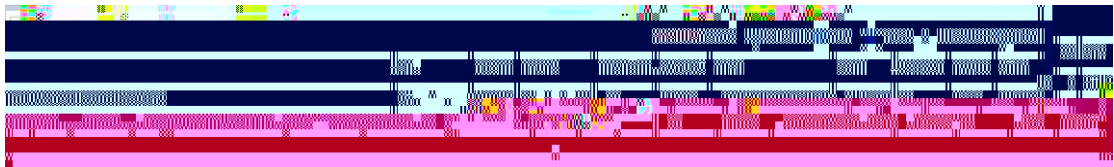
反调试 [1]

威胁行为 [6]

下载的大马拥有多种反沙箱反虚拟机功能



3. NGIPS RTF hta



4. 0day RTF



