

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

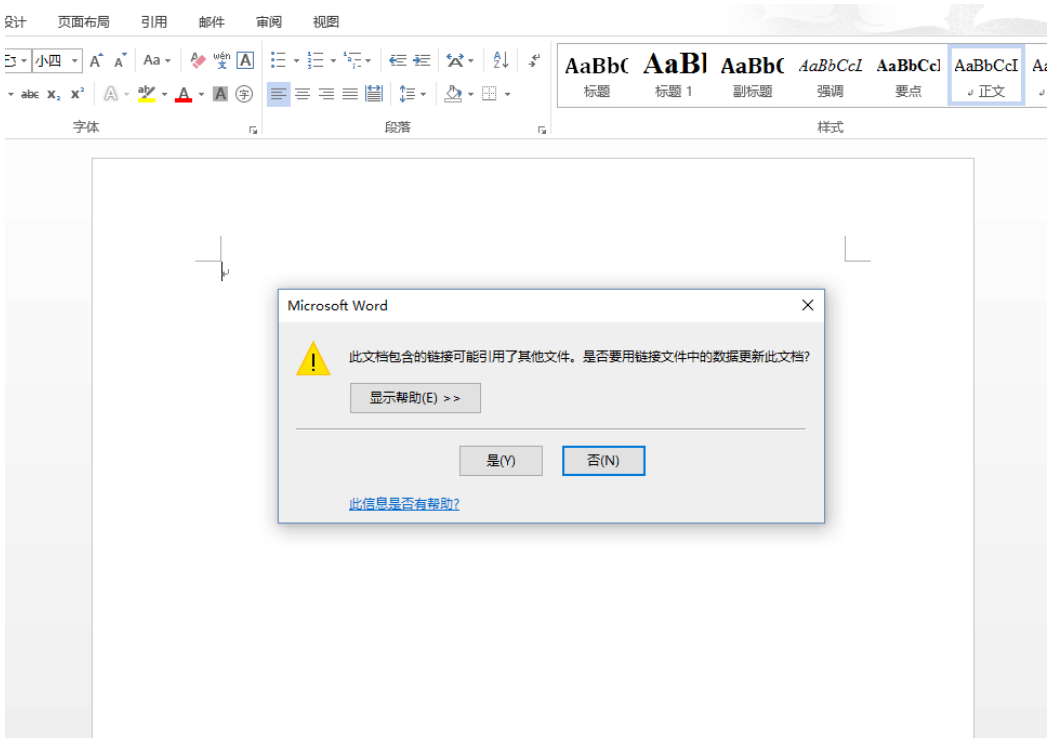
	5ebfd13		e9e01.rtf	2017/4/12 11:54	RTF 格式
	6e9483e		f7b.rtf	2017/4/12 11:54	RTF 格式
	20b15c4		d7dd9.rtf	2017/4/12 11:54	RTF 格式
	5f0550e		f d00d00ce		rtf-ent
	4b0270e		d70590da;		x65.rtf
	580270e		d70494390		aed3.rtf
	200670e		d706d366		af10e.rtf

MD5 65a558e9fe907dc5790e8a592364f64e

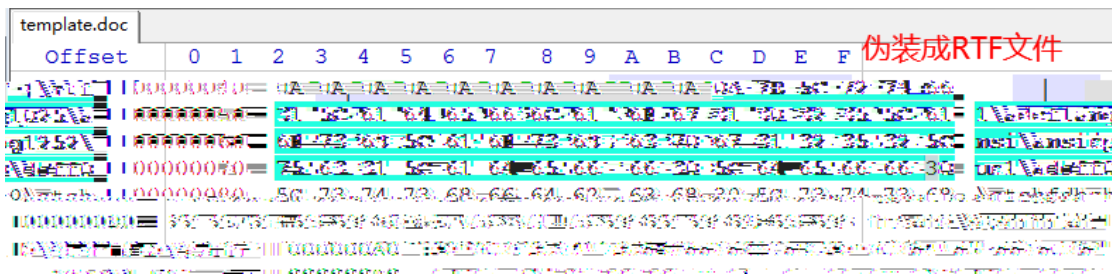
office2013

1. Office

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

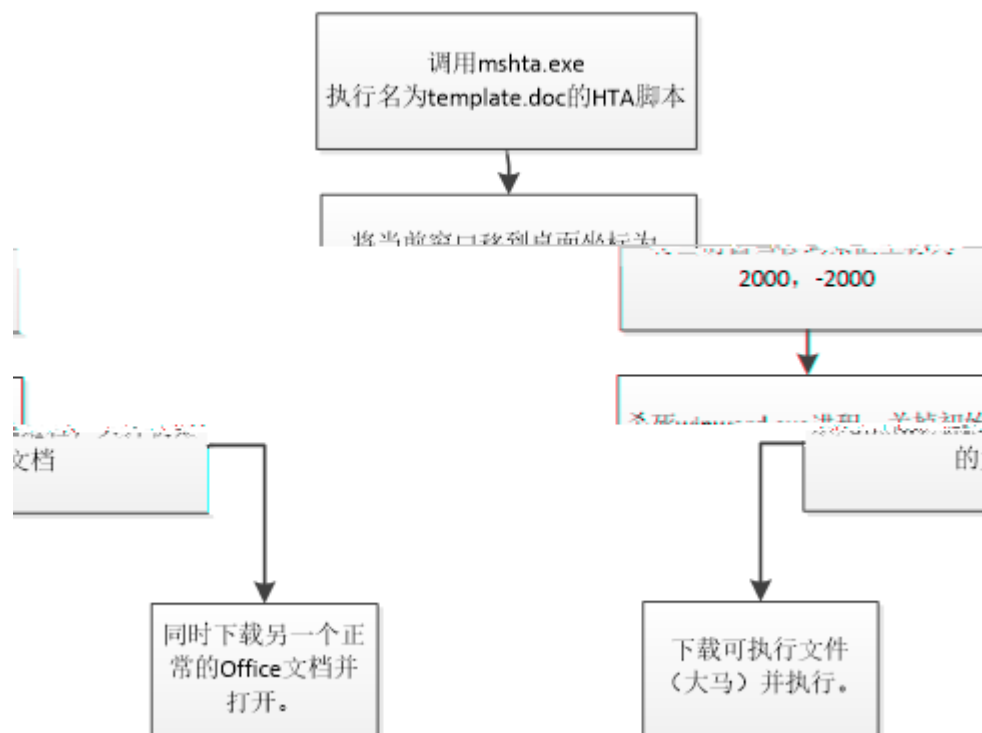


2. template.doc rtf hta



rtf

- [illegible]



1. APT Oday 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

05a558e9fe907dc5790e8a592304f04e.rtf

rtf

36.6 KB

2017-04-12 11:54:01

MD5

SHA1

SHA256

05a558e9fe907dc5790e8a592304f04e

f800e1d5949b54cec9b35edb7c7caf88fda8182b

3c0a93405b3d0a9904df03e3d178d544407203adb0e

3a79a9083a43a7e4a9cca5

软件版本：Microsoft Office 2010

结束时间：2017-04-12 11:57:39

危险等级 ★★★★★

80

求 危险等级 ★★★★★

15: 71/template.doc

动态检测

操作系统：Windows 7

开始时间：2017-04-12 11:54:02

隐藏信道 [2]

尝试连接某个服务器

可疑地址：195.17.129.103

检测到可疑HTTP请求

可疑URL：http://212.06.1

动态检测

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

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 ★★★★★

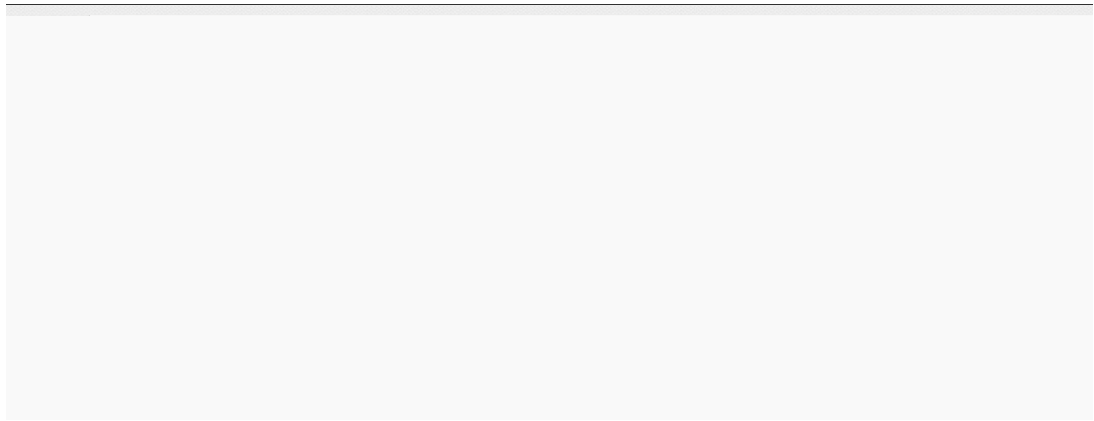
通过注册表判断VMware沙箱环境 危险等级 ★★★★★

反调试 [1]

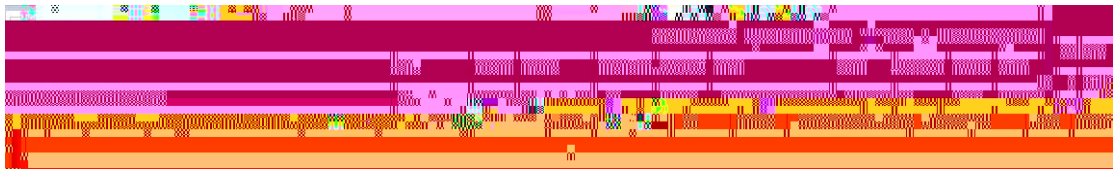
威胁行为 [6]

下载的大马拥有多种反沙箱反虚拟机功能。

2. IDS RTF hta



3. NGIPS RTF hta



4. 0day RTF



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

病毒查杀

风险类型

风险信息

AutoRun.Y1.zav

C:\文件夹\template.doc_

CVE-2017-0199.Y1.zav

C:\文件夹\sage50.exe_

建议清除

建议删除

实时防护

常用工具

防护日志

信任与隔离

☒ 下载者木马

☒ 恶意木马

VBS.Trojan-DI

C:\vir\新建文

Win32.Trojan.

C:\vir\新建文