Office 0-day (CVE-2017-0199)

Office

Office 0-Day Windows

Office Windows 10 Office 2016

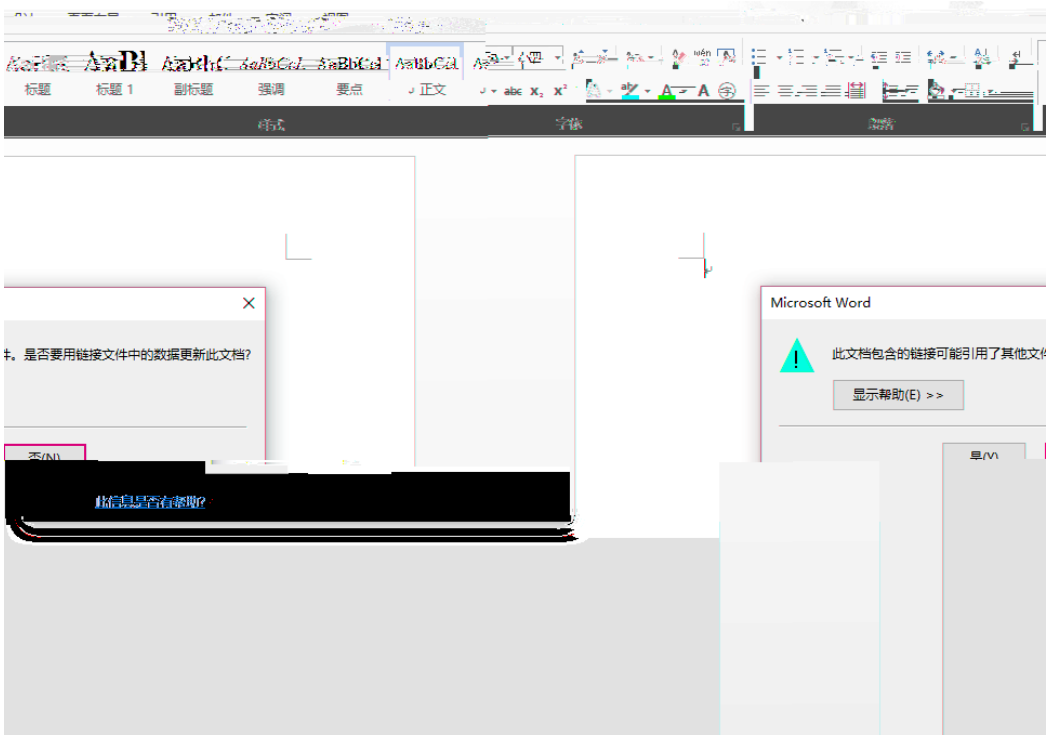
4 12

MD5 65a558e9fe907dc5790e8a592364f64e

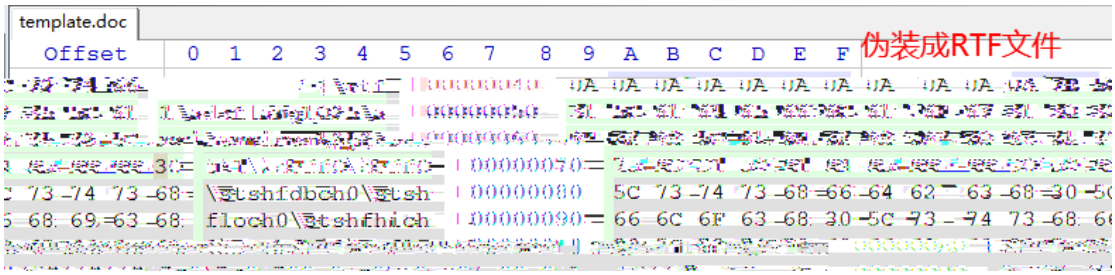
office2013

1. Office “ ”

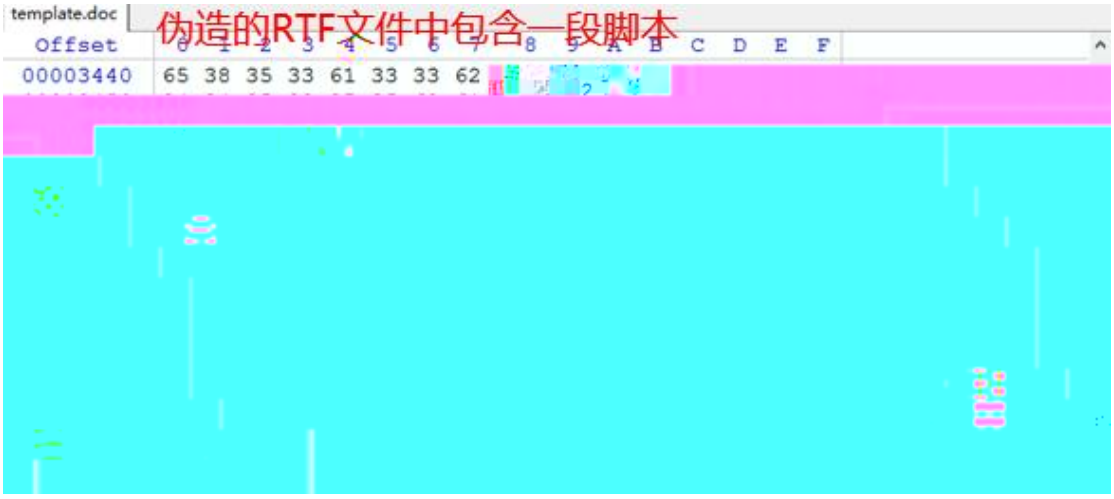
http://212.*.*.71/template.doc



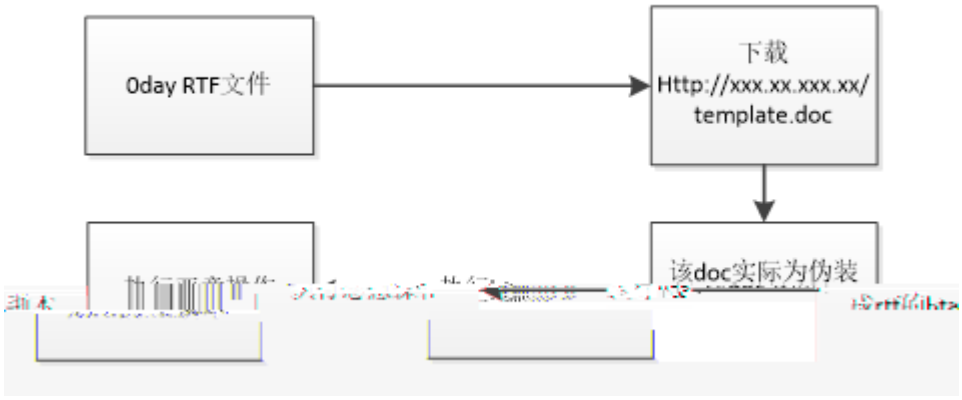
2. template.doc rtf hta



rtf



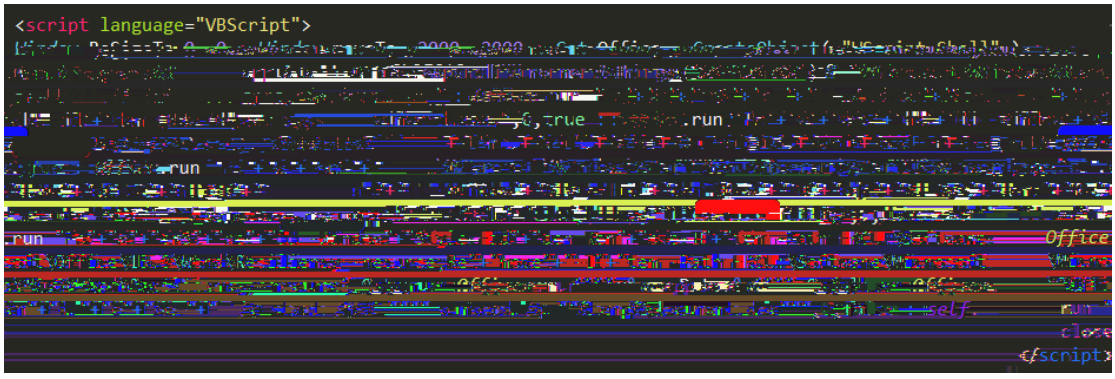
3.



4. template.doc Winword.exe Microsoft HTA mshta.exe

hta

5. Mshta.exe template.doc <script> </ script>



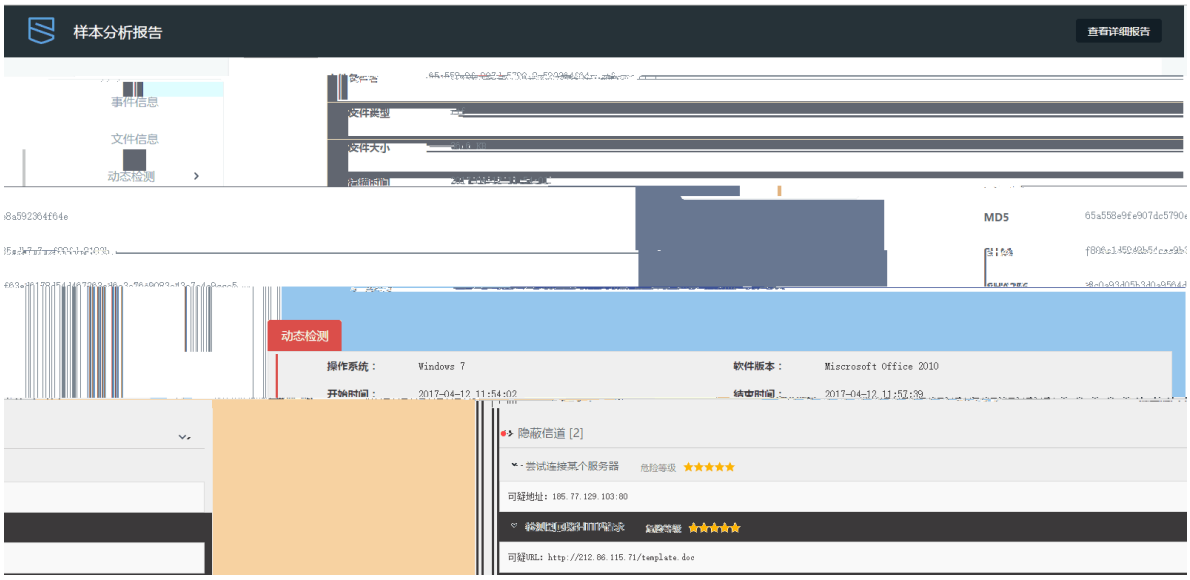
6.

(1) -2000 -2000

(2) taskkill.exe winword.exe word

(3)

1. APT 0day RTF





2. IDS RTF hta

3. NGIPS RTF hta



4. 0day RTF




景云杀毒
发现 2 个威胁
病毒查杀
风险类型
处理建议
VBS.Trojan-DL.AutoRun.Y1.zav
C:\vir\新建文件夹\template.doc_
建议清除
Win32.Trojan.CVE-2017-0199.Y1.zav
C:\vir\新建文件夹\sage50.exe_
建议删除
实时防护
常用工具
防护日志
信任与隔离