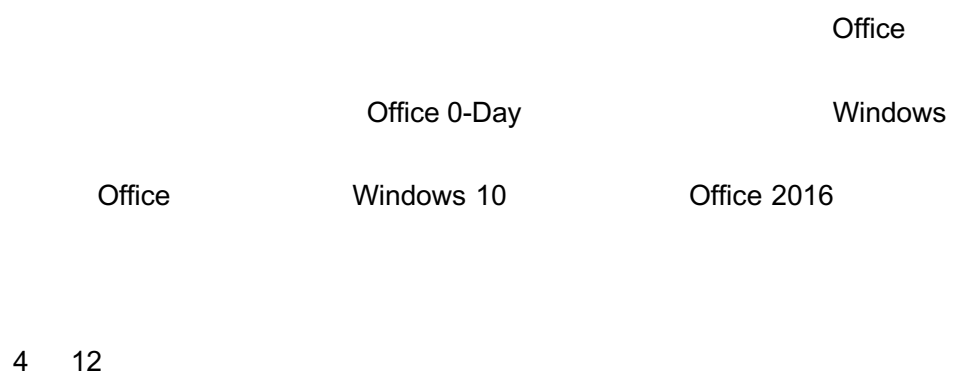


Office 0-day (CVE-2017-0199)

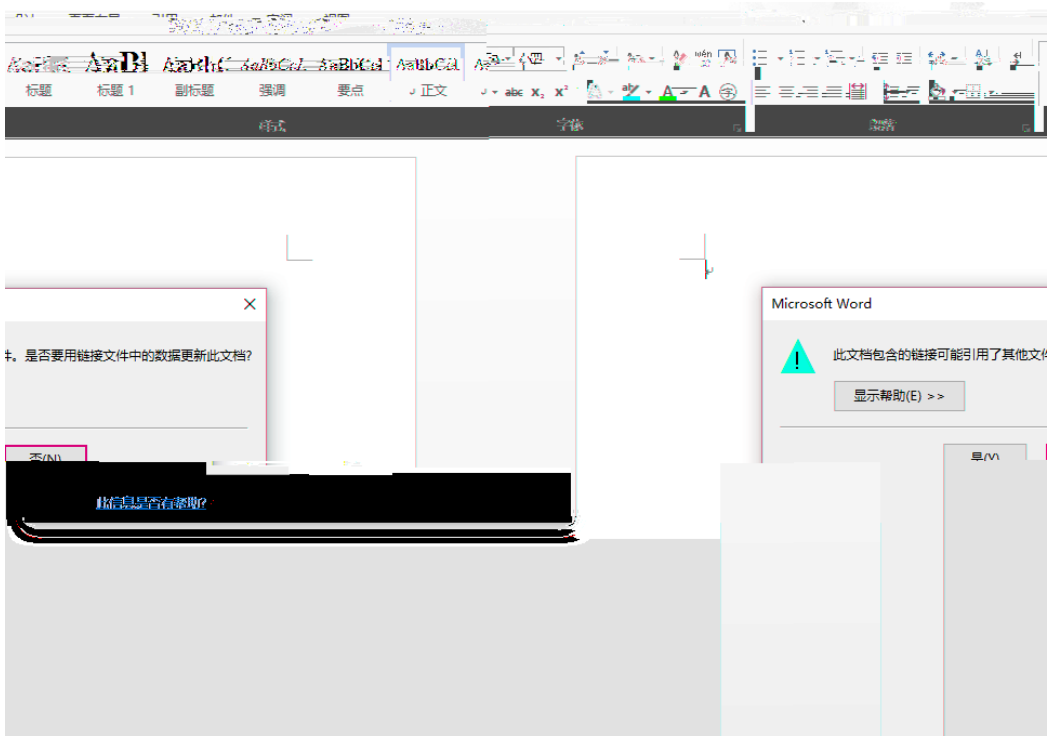


MD5 65a558e9fe907dc5790e8a592364f64e

office2013

1. Office “ ”

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



2. template.doc rtf hta



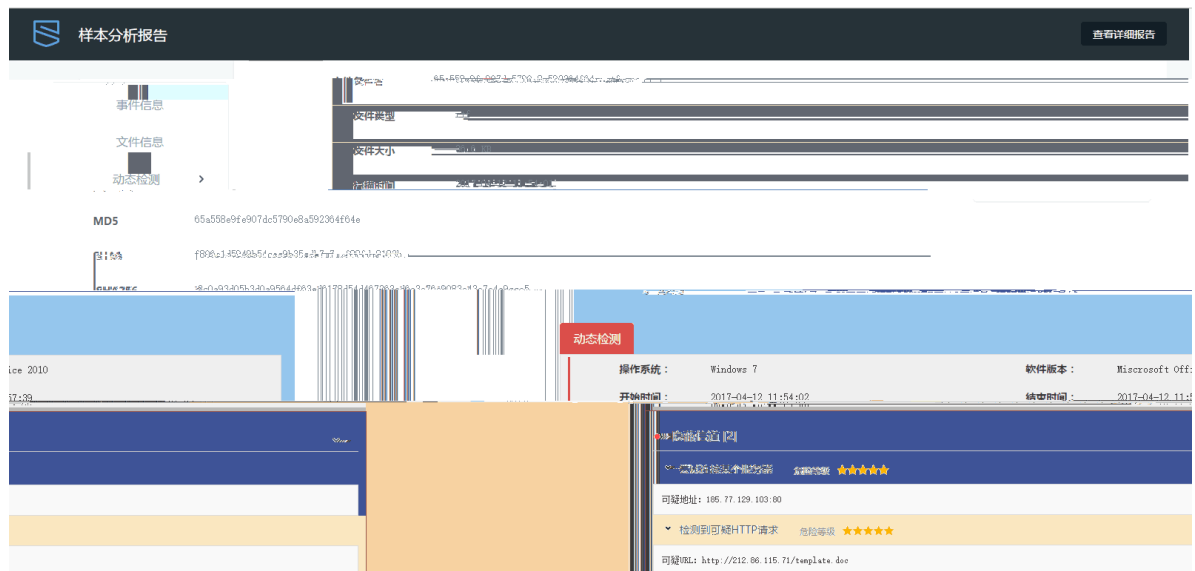
rtf

(1) -2000 -2000

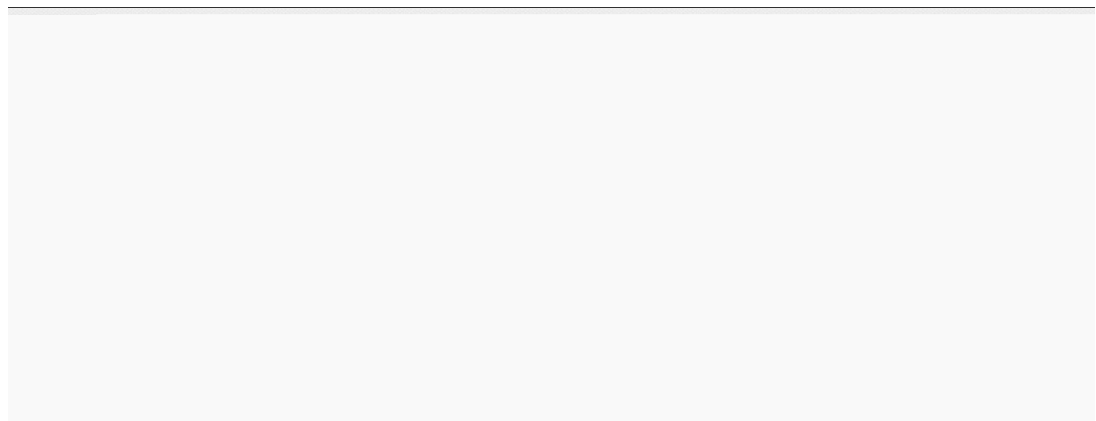
(2) taskkill.exe winword.exe word

(3)

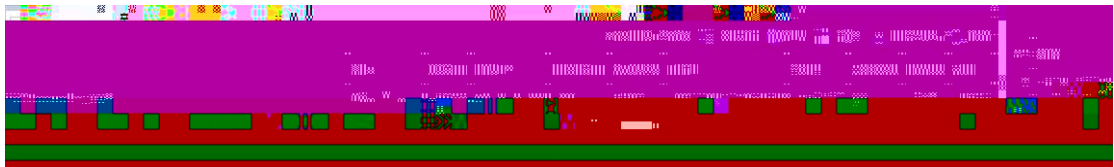
1. APT 0day RTF



2. IDS RTF hta



3. NGIPS RTF hta



4. 0day RTF



