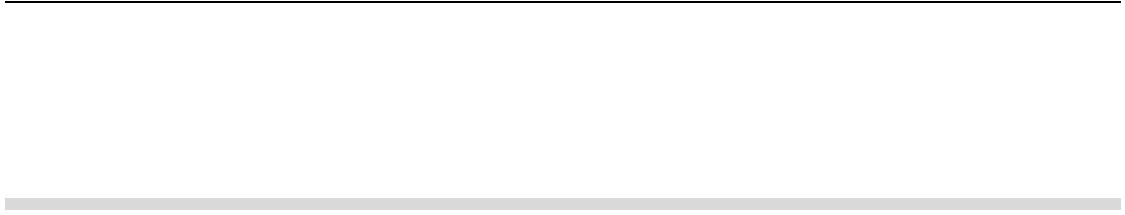
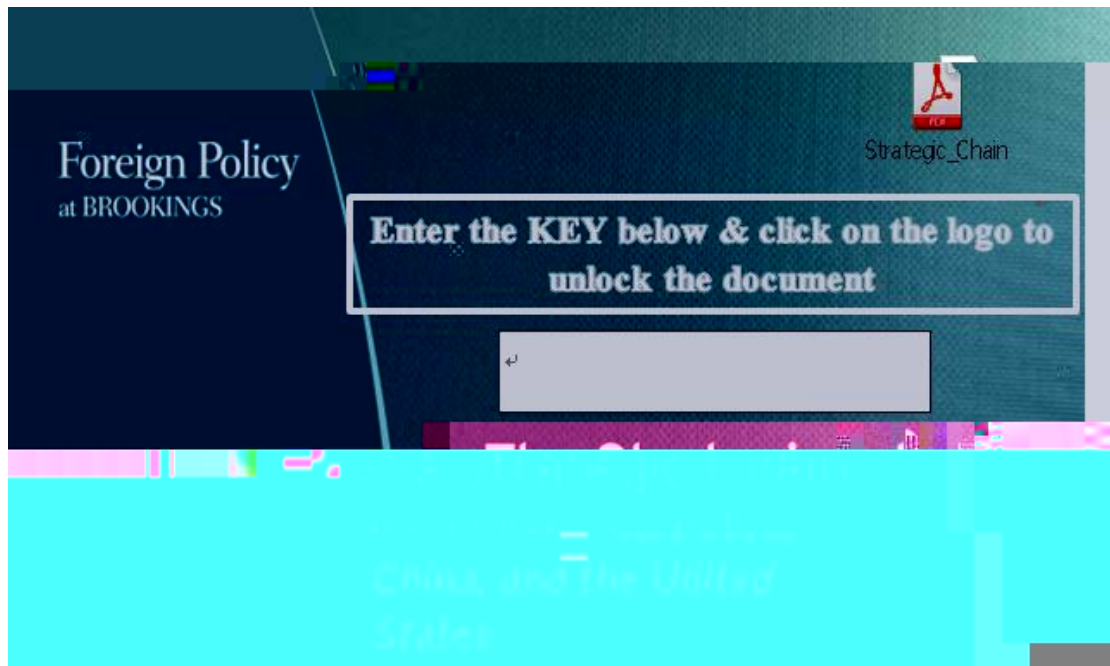
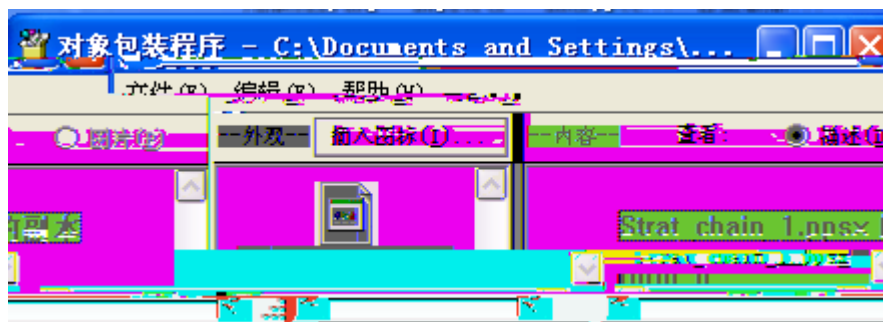

VenusEye



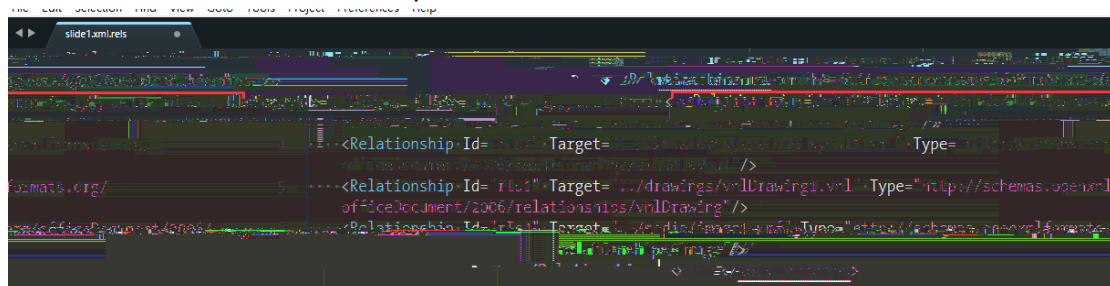




3. 在 对象包装程序 - C:\Documents and Settings\... ppt OLE 32022 Start_chain_1.pptx ppt



4. B pptx 7+X CVE-2017-0199 7F02 ppt sct 7



5. sct 7 3+X Powershell putty.exe Strategic_Chain.pdf 7F02

6. LFI 漏洞利用

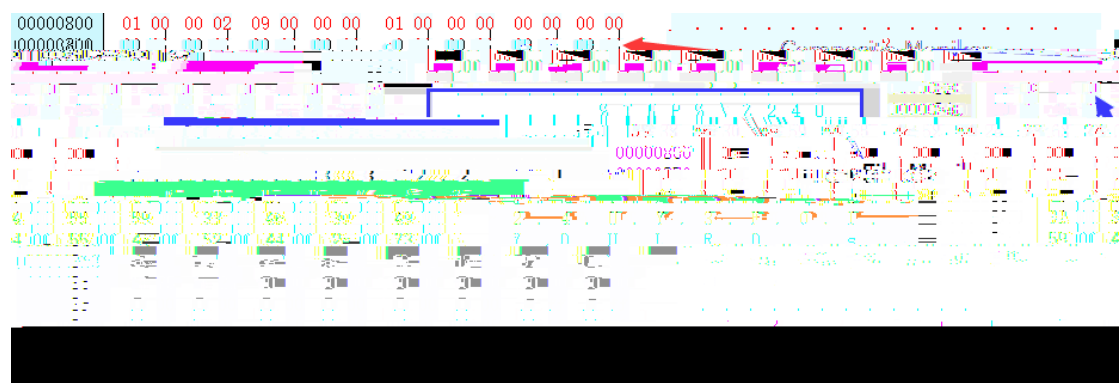
Entanglement 2 ppsx

CVE-2017-0199 %00XND\000



CVE-2017-8570 %NFR? 2018 ? 3 80? ? ? ?+X
 0/0#k-? ?

OLE DB+X CVE-2017-8570 %#&# Scriptlet Moniker &#



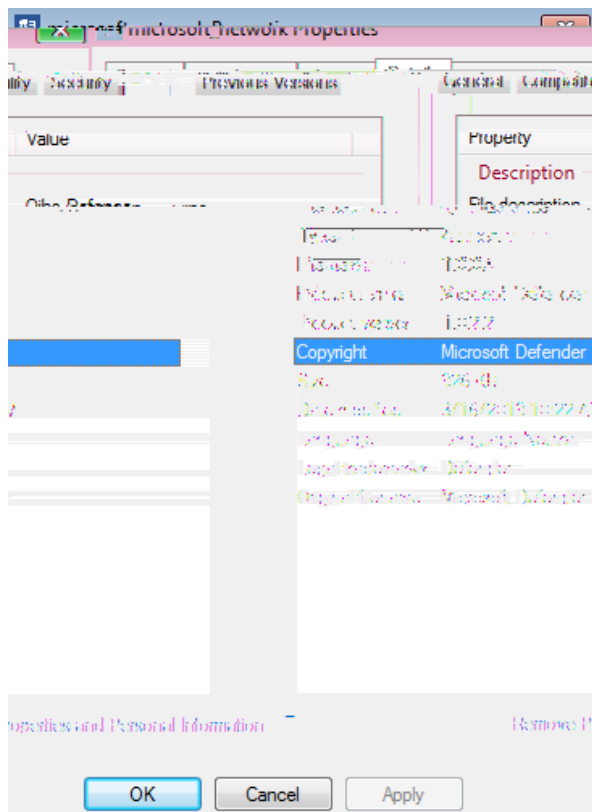
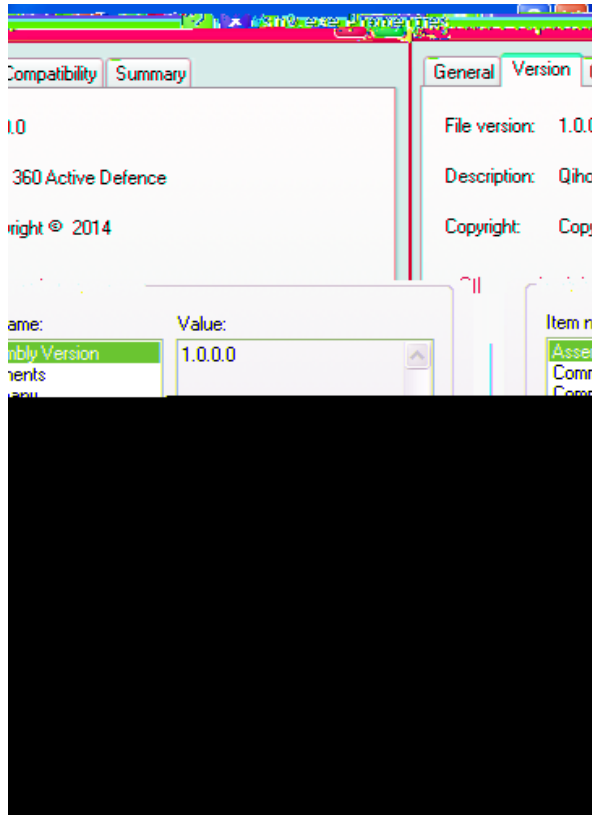
A 瑞星

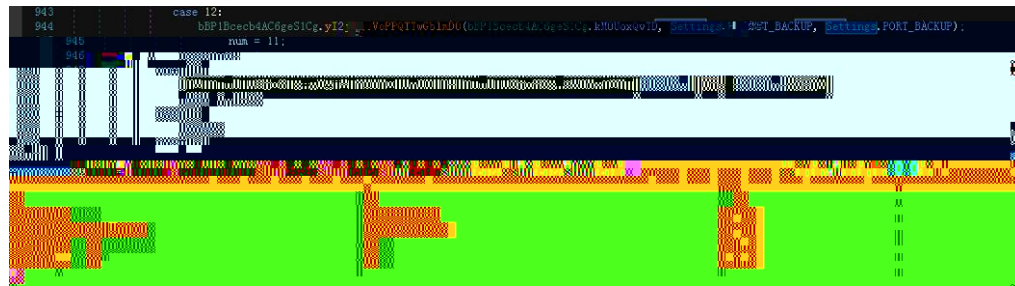
B 金山毒霸

QuasarRAT

1. 瑞星

Qihoo 360 1y





6. 0> 6fLÖ  yY  C&C 



```

00 .....Q.....1.0.0.r3..W
57 indows 7 ..... 32 Bit..User".China*.CN2.
07 Beijing:.Beijing@.I@EF087A3E748E4C8ED35F1E051
30 843D49A0740D5F24C6853821DF8E13213D75114.....
30 .....
  
```

```

.....QA.u...Nu...1...h.....Processor
(CPU).Intel(R) Core(TM) i5-6500 CPU @ 3.20G
Hz..Memory (RAM)..1023 MB..Video Card (GPU)..
VMware SVGA 3D..Username..PC Name.
.WIN-E4IQBFNH36E..Uptime..0d : 9h : 26m : 58s
..MAC ..
  
```

C   P  BADNEWS  

1. 

%PROGRAMDATA%\Microsoft\DeviceSync\VMwareCplLauncher.exe

%PROGRAMDATA%\Microsoft\DeviceSync\vmtools.dll

%PROGRAMDATA%\Microsoft\DeviceSync\MSBuild.exe

 VMwareCplLauncher.exe  # 

vmtools.dll 

rannd.org

brokings.org
crazywomen-dating.com
ifenngnews.com
209.58.185.37
mail.ifenngnews.com
chinapolicyanalysis.org

C&C 中国
94.242.249.203
209.58.183.33

VenusEye H100Ea
LÖ
p c 1 6A °
LO
c ; 6A HLOJ 010
; D > 6A 6A c 5
HLO
Hedwig Locky 6A
@ A 18 18
kg 18 Office

