

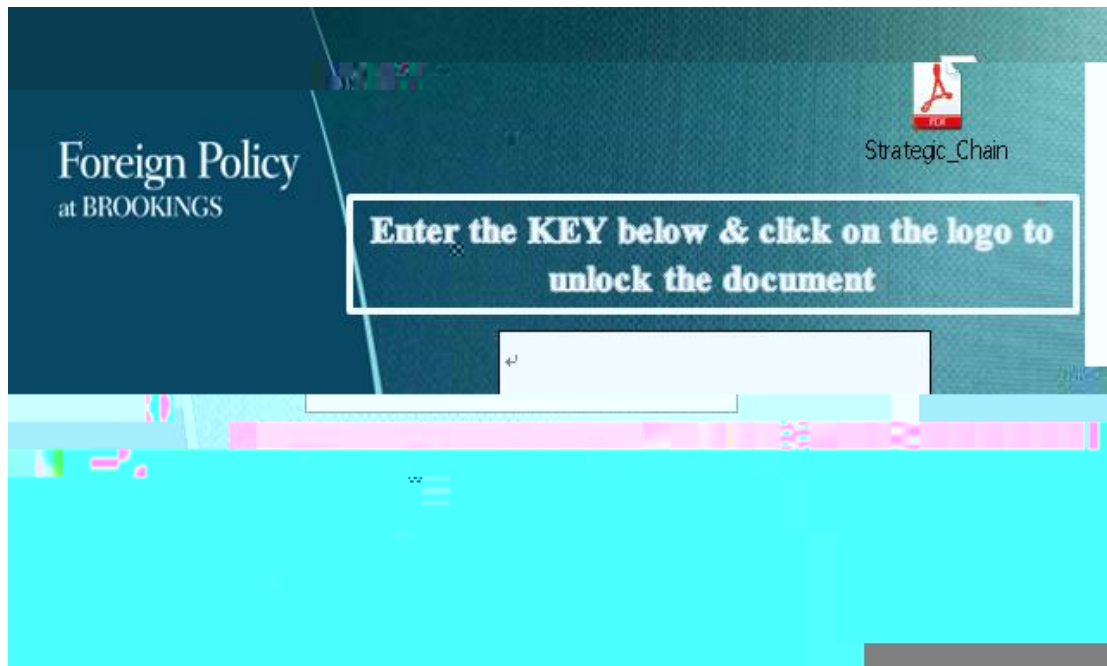
---

VenusEye

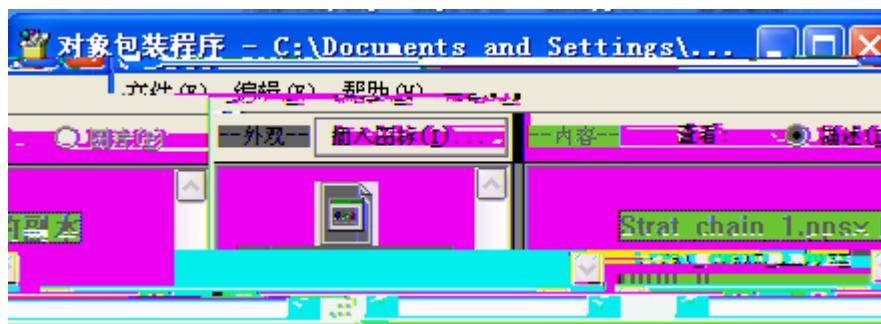




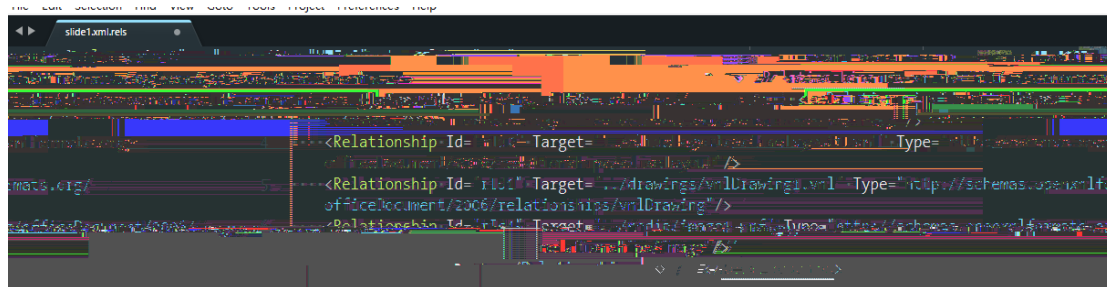




3. 文件 OLE 对象 Start\_chain\_1.pptx  
ppt 对象 ppt



4. B ppsx +X CVE-2017-0199  
PDF sct 7 ppt



5. sct 7 B3+X Powershell putty.exe  
Strategic\_Chain.pdf X@B

6. L~~1~~501j  
X

Entanglement ppsx  
CVE-2017-0199 %~~1~~X~~1~~\~~1~~C~~1~~



CVE-2017-8570 %NFKK

2018 3 800  
V#O#k-

Y+X

2







%N4G-0000

000

qratt 00

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00h:	AD	AE	10	00	02	00	71	72	61	74	2E	65	78	65	00	43	-@....qratt.exe.C																
10h:	3A	5C	66	61	6B	65	70	61	74	68	5C	71	72	61	74	2E	:\fakepath\qratt.																
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\qratt.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	.yy.....@..																
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 %N0000R000N

&/000000000000

0-00y

-00000000

BADNEWS 3+6

XP



QuasarRAT BADNEWS

1/2

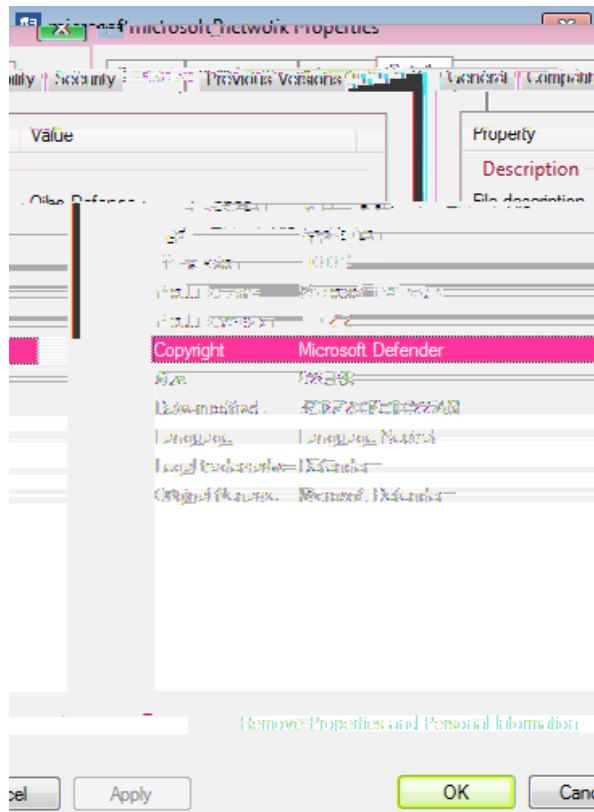
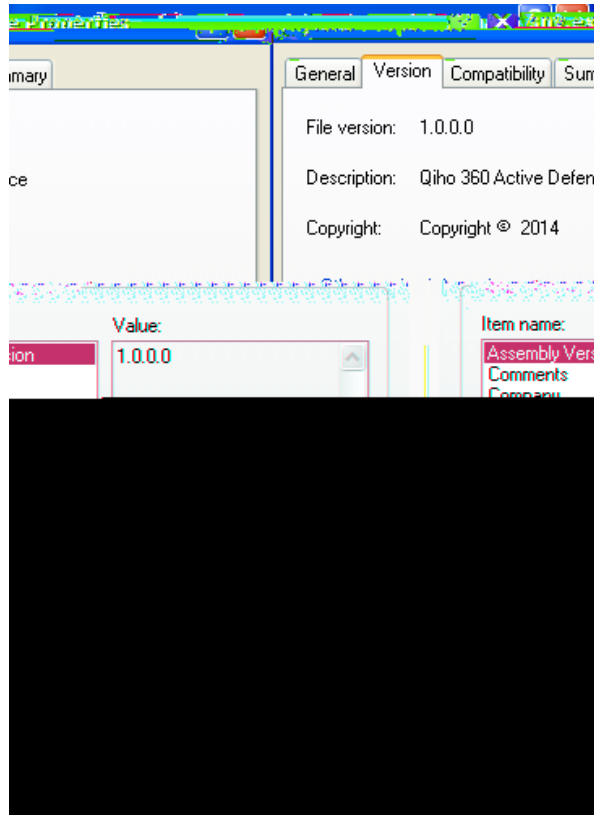
A 0000

B 0000P0

QuasarRAT0

1. 0000

Qiho 360 1y0





















```

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:00B690FF
-----
text:00B69100
-----
4
5
-----
text:00B6910C
text:00B69117
text:00B6911F
text:00B69125
-----
text:00B6912D
text:00B69130
text:00B69130 loc_B69130:
text:00B69130
text:00B69131
-----
push esi ; CODE XREF: findsensefile+61jj
call edi ; lpRootPathName ; GetDriveTypeW
-----
text:00B69138
text:00B69139 collectfile
text:00B6913E
text:00B69141
ifj text:00B69141 loc_B69141: ; CODE XREF: findsensefile+46
text:00B69141 ; findsensefile+58jj
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
ifj text:00B69153 loc_B69153: ; CODE XREF: findsensefile+35
text:00B69153 mov ecx, [ebp+var_4]
text:00B69156 pop edi
text:00B69157 xor ecx, ebp
text:00B69159 pop esi

```

7.   d&. TPX498.dat
  8.  dat  AES  +base64 5F.1E1
-  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 H...  
L...  
...  
...  
...  
Hedwig ... Locky ...  
... Sage 2.0  
... Office ...

