

分



VenusEye

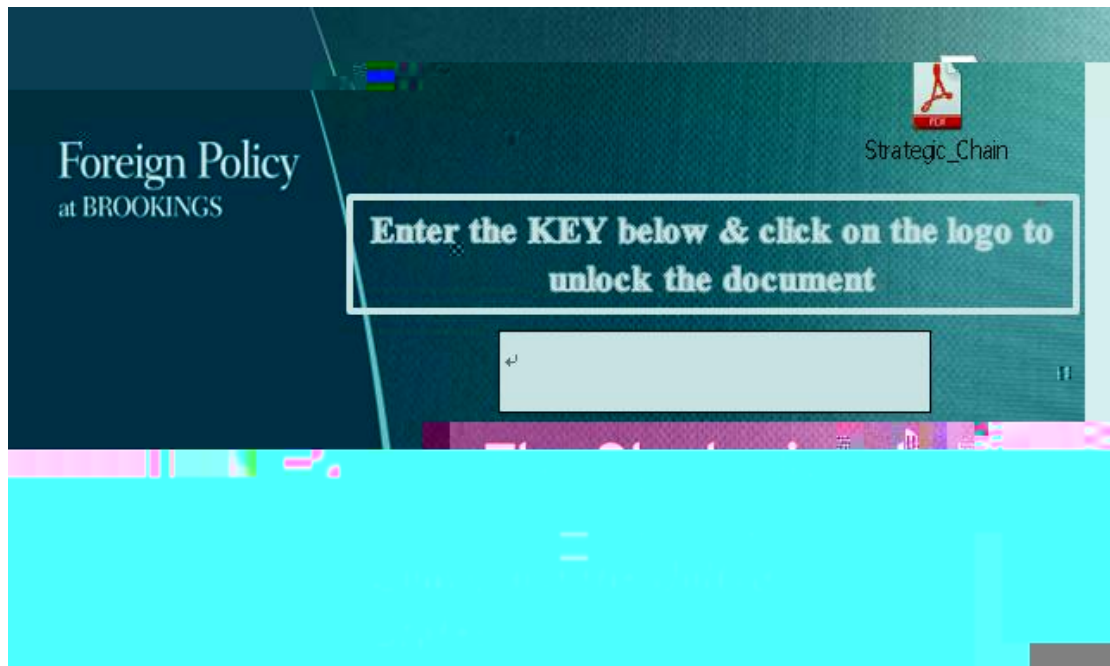


分

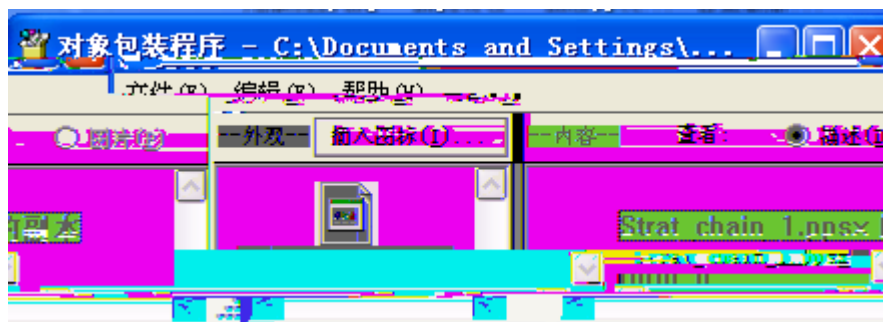


分





3. 文件 OLE 对象 Start_chain_1.pptx ppt 对象 ppt



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



5. sct 7 +X Powershell putty.exe - Strategic_Chain.pdf

6. LFI 01
01X

Entanglement 01 ppsx
CVE-2017-0199 %01X 01X

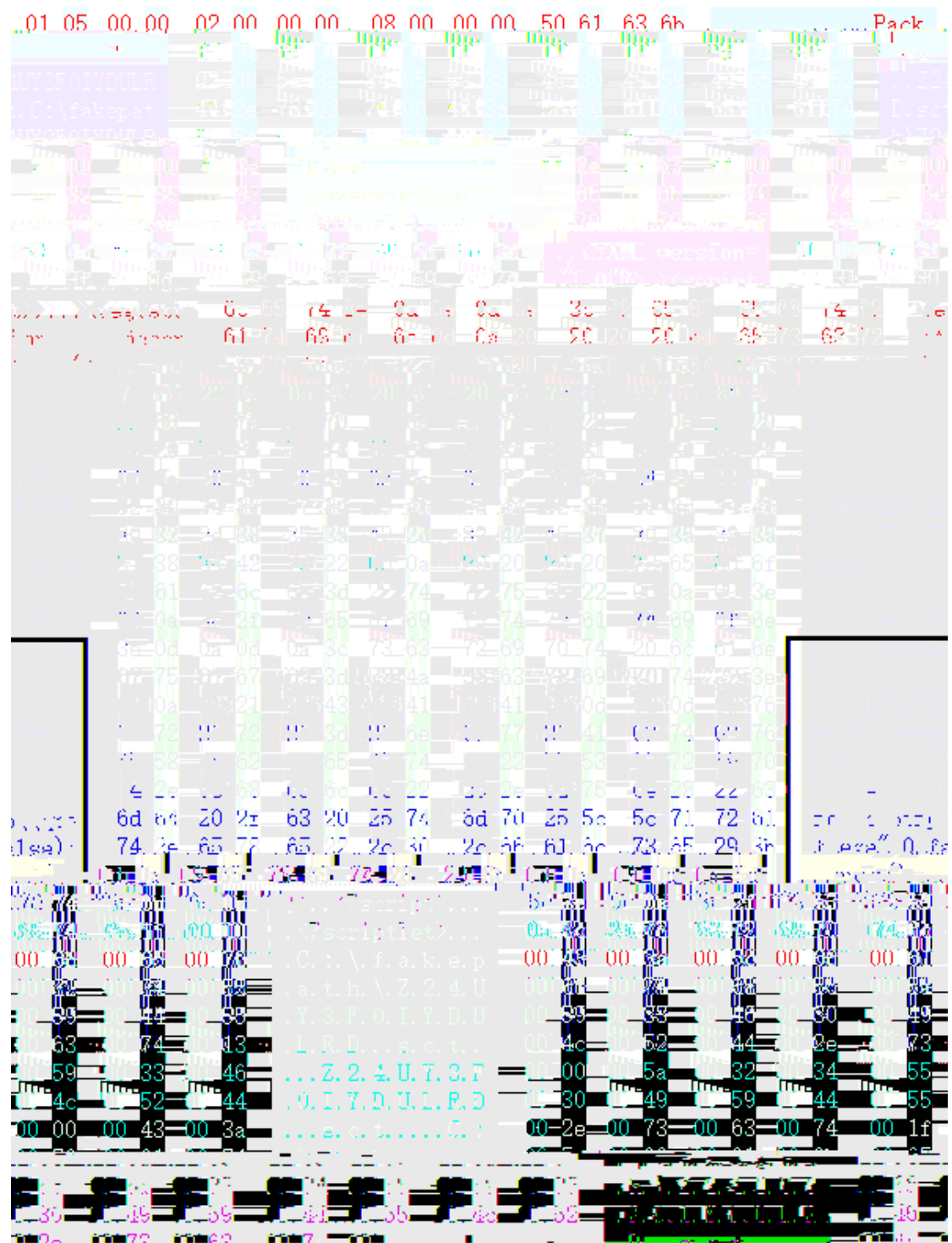


2018 3 30 17:00:00

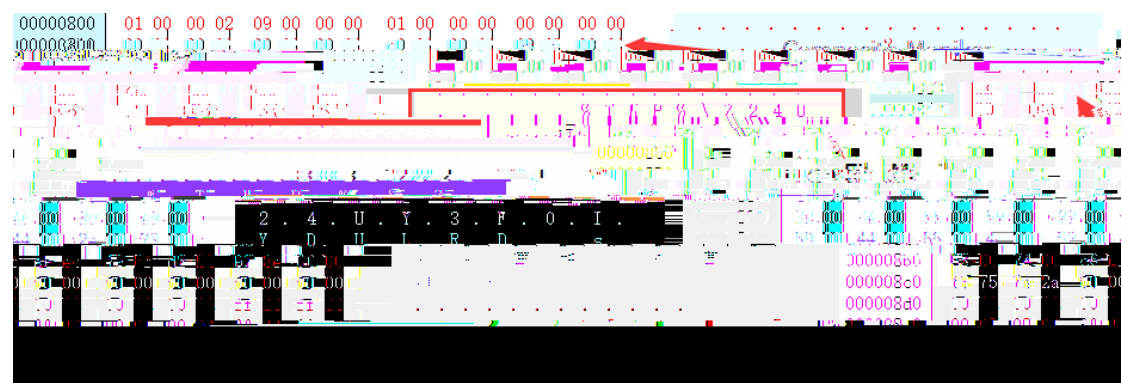
CVE-2017-8570 %INFILE#k-0

分





OLE CVE-2017-8570 % Scriptlet Moniker sct



%N040-0000

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 %N000000000000

&/000000000000

7-00y0

-000000000000

BADNEWS 3+0

XP0 0



QuasarRAT BADNEWS

1/2 0

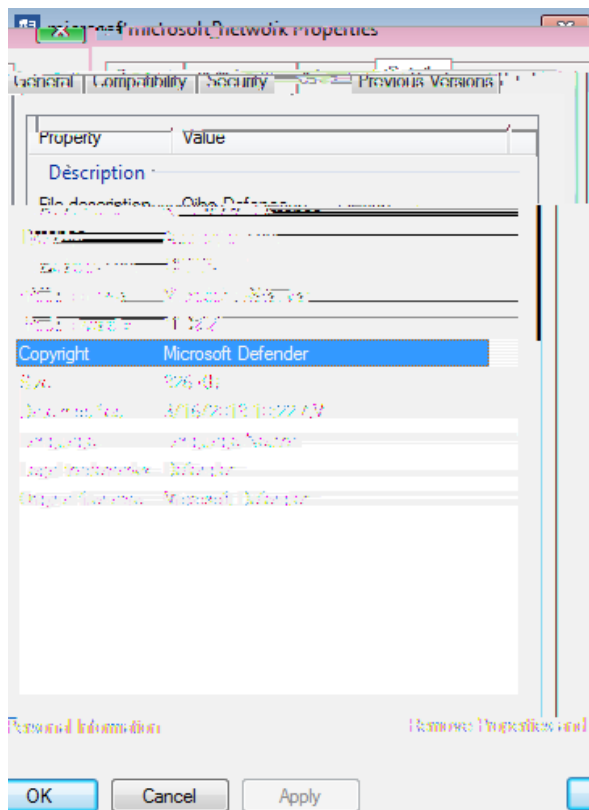
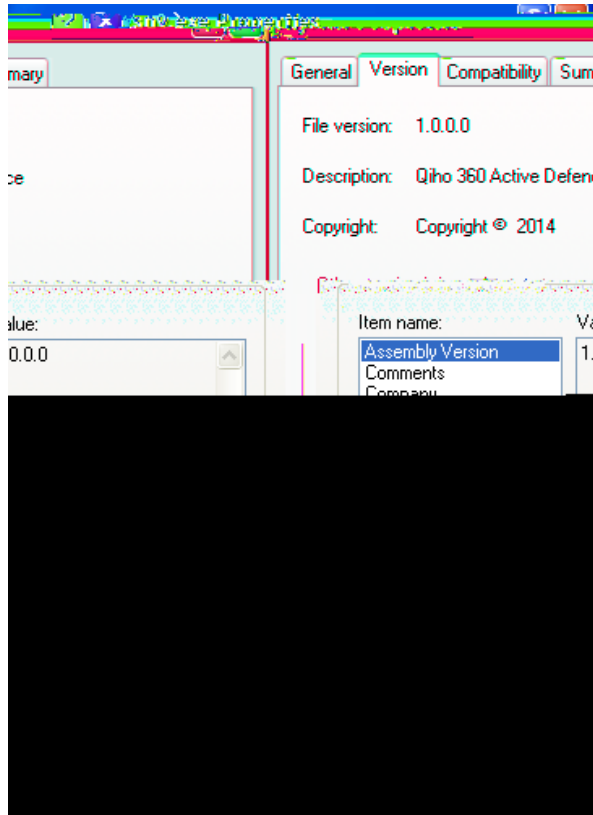
A 0000

B 0000P0

QuasarRAT0

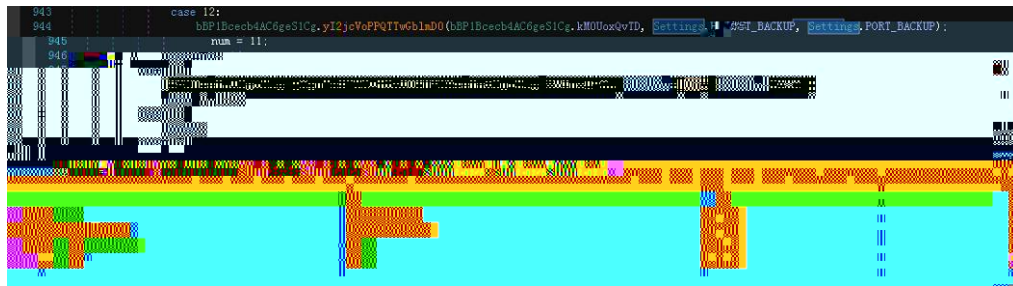
1. 0000

Qiho 360 1y0

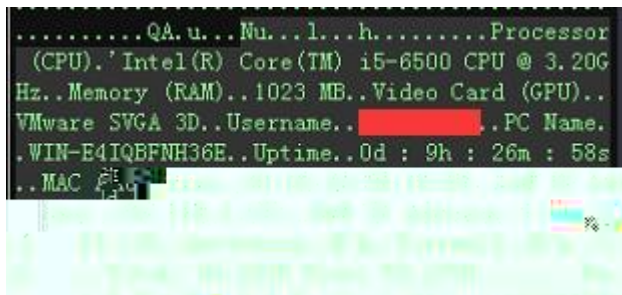


分





6. 0> 6fLÖ 5634yY E` C&C 图



C:\P\ BADNEWS \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


```
7. 0xTPX498.dat
8. f dat 0x0000 AES 0x0000 +base64 5F.1P1P
   ? v ? ? F 1 ? ? . ? 5 F . 1 ?
   \e3e7e71a0b28b5e96cc492e636722f73\4sVKA0vu3D\UYEfGepXAOE.php
```

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 H1LOEà Lö 6À °
LO 6À °
C ; 6À HLOJ 6À ° Š \$
; D > 6À 6À C 6À
HLO 6À °
Hedwig 6À Locky 6À °
@ 6À 18 6À ° Sage 2.0
kg 6À 18 Office 6À °

