APT

2016中国高级持续性威胁研究报告

SkyEye 天眼实验室

HeliosTeam 追日团队

摘要

APT 攻击的基本研究

- 2016 年，全球各地安全机构展开了大量关于 APT 的专业研究。截至 2016 年 12 月，360 追日团队共监测到全球 41 个安全机构发布的各类 APT 研究报告 100 份，涉及相关 APT 组织 43 个，被攻击目标国家 38 个。
- 美国在 APT 研究方面处于全球领先的地位，至少有 19 个研究机构发布了各类 APT 研究报告 50 篇。俄罗斯目前主要的 APT 研究机构，虽然仅有 Kaspersky 一家，但其研究质量，深度和总体水平显著高于绝大多数其他研究机构。国内研究机构目前仍处于全球 APT 研究的第二梯队。
- 中国 APT 研究水平明显落后于美俄等国的主要原因有以下两个方面：首先是国内能力型厂商的缺乏，目前国内仅 360、安天等少数机构能够对 APT 进行深入与专业的研究；其次是美俄两国，特别是美国，非常善于通过公开威胁事件及情报共享等方式，提高国内机构与企业的整体安全防护水平，同时借此对其他国家施加政治压力。
- 截至 2016 年底，360 威胁情报中心已累计监测到针对中国境内目标发动攻击的境内外 APT 组织 36 个，最近三个月内仍处于活跃状态的 APT 组织至少有 13 个。在过去的 12 个月中，这些 APT 组织发动的攻击行动至少影响了境内超过万台电脑，攻击范围遍布国内 31 个省级行政区。
- 统计显示，疑似 APT 攻击目标的境内组织机构近 200 个。其中，大学占比最高，为 40.0%；其次是企业占比 25.0%；再次是政府及事业单位占比 18.3%；还有科研机构占比 11.1%，其他机构或个人占比 5.6%。

针对特定领域的攻击与影响

- 2015 末-2016 年，APT 攻击在三个领域中产生的重要影响最值得关注：针对工业系统的破坏，针对金融系统的犯罪，以及针对地缘政治的影响，
- 2015 年 12 月 23 日，也就是圣诞节前夕，乌克兰遭遇了大规模停电事件，数万“灾民”不得不在严寒中煎熬；在 2016 年 11 月 17 日晚，即伊斯兰教的大赦之夜，沙特阿拉伯又遭遇了 Shamoon2.0 的攻击，包括沙特国家民航总局在内的 6 个重要机构的计算机系统遭到严重破坏。
- 2016 年堪称全球银行机构的网络灾害年。先是上半年接连发生了以孟加拉国央行为代表的一系列发展中国家的央行或大型国有银行被盗事件，受害者损失高达数千万美元。下半年又接连发生了以台湾第一银行

ATM 机吐钞事件为代表的一系列 ATM 机攻击事件。而一个以合法软件开发企业为伪装的，以不当盈利为目的的，长期从事敏感金融交易信息窃取活动的境内 APT 组织黄金眼，也在 2015 年 12 月被截获。

- 网络攻击事件对地缘政治的影响也在 2016 年也异常突出。特别是对美国大选产生了直接影响的 DNC 邮件泄露事件，其实质影响可能是世界性的。此外，方程式组织工具的泄漏事件也显示，中国很可能是这个超高级组织攻击的主要目标。

APT 攻击的组织与事件

- 网络军火商是 APT 活动中一群特殊的利益团体和组织，他们会出售计算机程序、软件或设备给其他组织机构。全球比较著名的网络军火商包括意大利的 Hacking Team、英国的 Gamma 和以色列的 NSO Group 等。
- 2016 年 8 月，iOS 三叉戟漏洞被曝出。这是苹果史上第一次公开披露的针对 iOS 的 APT0day 攻击。
- 索伦之眼是 2016 年度被全球所有机构披露的 APT 组织中技术实力最强的，与之前的方程式（Equation）组织相比也毫不逊色，其幕后组织的综合能力不亚于震网（Stuxnet）、火焰（Flame）等知名 APT 组织。索伦之眼组合使用了一系列复杂高难度的技术对目标实施了隐蔽性极强的攻击，譬如：高度模块化的平台、加密虚拟文件系统、无文件实体等。
- 2016 年最受全球关注的 APT 组织非 APT28 莫属。该组织在 2015 年第一季度大量攻击了北约成员国和欧洲、亚洲、中东等地区国家的政府。2016 年 12 月披露的的证据表明，该组织可能帮助亲俄武装分裂分子追踪乌克兰部队的动向，曾使乌克兰炮兵部队损失一半以上的武器。此外，2016 年 4 月 DNC 邮件系统被入侵，2016 年底被披露的德国政府官员、国会议员等遭到的网络攻击也都被认为与该组织有关。
- 摩诃草组织（APT-C-09），是一个来自于南亚地区的境外 APT 组织。摩诃草组织最早由 Norman 安全公司于 2013 年曝光。该组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到 2009 年 11 月，至今还非常活跃。

APT 攻击的趋势特点与监测防御

- 综合 2015-2016 年 APT 攻击的情况分析，未来几年内，APT 攻击将主要呈现以下四个趋势特点：网络空间成为大国博弈的新战场，针对基础设施的破坏性攻击日益活跃，针对特定个人的移动端攻击显著增加，一带一路与军民融合仍将是攻击焦点。

- 从目前 APT 监测与防御技术体系的发展来看，企业在网络安全建设方面仍存在诸多盲区，同时，国内的能力型安全厂商仍然严重缺位。而数据驱动的，协同联动的纵深防御体系将成为未来 APT 检测与防御的主要方法。

关键词：APT、工业系统、孟加拉央行、ATM、黄金眼、DNC 邮件泄漏、索伦之眼、APT28、 摩诃草

目　　录

第一章　全球 APT 研究前沿概览

一、　APT 研究机构与研究报告

APT 攻击（Advanced Persistent Threat，高级持续性威胁）堪称是在网络空间里进行的军事对抗。攻击者会长期持续的对特定目标进行精准的打击。

为了能够更加全面的掌握全球 APT 攻击态势，了解全球 APT 研究的前沿成果，2016 年以来，360 威胁情报中心下属的 360 追日团队，展开了对全球主要安全机构及安全专家发布的各类 APT 研究报告和研究成果的监测与追踪工作。截至 2016 年 12 月，360 追日团队共监测到全球 41 个安全机构及安全专家发布的各类 APT 研究报告 100 份，涉及相关 APT 组织 43 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 38 个。下表给出了 360 威胁情报中心监测到的全球各国关于 APT 研究情况的对比。监测可能有所遗漏，敬请谅解。

研究机构或专家所属国家	APT 报告数量	发布 APT 报告机构数量	涉及 APT 组织数量
美国	50	19	29
中国	14	5	14
俄罗斯	10	1	14
加拿大	4	1	4
英国	3	1	3
以色列	2	2	2
罗马尼亚	1	1	1
荷兰	1	1	1
科威特	1	1	1
西班牙	1	1	0
未知（秘密黑客组织）	1	1	1
跨国公司或联合机构	12	7	10

表 1　全球各国 APT 研究情况对比

从上表中可以清楚看出，无论是从研究报告的数量、研究机构的数量，还是涉及 APT 组织的数量来看，美国在全世界都处于遥遥领先的地位，有 19 个美国的研究机构（其实，在上表中的“跨国公司或联合机构”中，也至少有两家与美国相关）展开了 APT 的相关研究，发布相关研究报告多达 50 篇。

从报告数量和参与研究机构的数量来看，中国排名全球第二。共有 4 个组织机构和 1 位安全专家发布了 14 篇关于 APT 的研究报告及成果。

而俄罗斯目前主要的 APT 研究机构，则仅有 Kaspersky 这一家安全厂商。报告数量在各国中排名第三。但客观的说，Kaspersky 属于以一当十的高水平研究机构，其发布的 APT 研究报告的质量，深度和总体水平，不仅明显高于国内的绝大多数研究机构，甚至也较美国的绝大多数研究机构略胜一筹。

例如：2016 年 8 月，美国安全公司 Symantec 发布了一份比较简略的研究报告，披露了一个新的、年度最强大的 APT 组织 Strider；但该报告公开不到 24 小时，俄罗斯安全公司 Kaspersky 就发布了两份合计长达 60 页的，关于 Project Sauron（索伦之眼，与 Strider 为同一组织）的详细分析报告，由此也使索伦之眼闻名天下。此事足见 Kaspersky 在 APT 研究领域拥有深厚的积累和丰富的日常储备。

总体而言，从全球范围来看，在 APT 研究领域，美国和俄罗斯目前还是处于绝对领先的地位。并且这两个超级大国都拥有数目庞大的安全初创团队和初创公司在关注、狙击以及深入研究 APT 攻击。国内研究机构关于 APT 的研究水平，目前最多只能算是全球第二梯队的排头兵。

造成中国 APT 研究水平明显落后于美俄等国的主要原因有以下两个方面：

首先是国内能力型厂商的缺乏。APT 攻击针对性强，隐蔽性高，普通的民用安全技术往往很难有效防御，甚至根本无法发现。目前在国内，除了 360、安天等少数机构外，其他真正有能力发现和研究 APT 攻击的厂商、机构非常有限。

其次是美俄两国，特别是美国，非常善于通过公开威胁事件及情报共享等方式，提高国内机构与企业的整体安全防护水平，同时借此对其他国家施加政治压力。APT 攻击的研究与披露，已经成为大国政治与战略博弈的重要棋子。

关于 2016 年全球各国研究机构针对 APT 研究的具体情况，详见附录 1。

二、 APT 攻击目标的全球研究

尽管目前仍有大量的关于 APT 攻击的研究成果处于各安全研究机构的保密之中。但目前已经披露出来的研究报告，也能在一定程度上反应全球 APT 研究的关注点和发展趋势。

在 2016 年 360 威胁情报中心监测到的 APT 报告中，被提及次数最多的被攻击国家依次是：中国、美国、印度、俄罗斯、乌克兰、巴基斯坦、伊朗、韩国、日本、以色列、土耳其、埃及和沙特阿拉伯这 13 国家。

被攻击目标国家	所属地区	相关报告数量	攻击组织数量	主要被攻击领域
中国	亚洲	26	9	政府、基础设施、教育、科研、大型企业
美国	北美	15	9	政府、金融、基础设施、大型企业
印度	亚洲	15	7	政府、军事、商业组织
俄罗斯	欧洲	15	6	政府、能源、军事、外交、金融
乌克兰	欧洲	14	5	政府、军事、电力、金融
巴基斯坦	亚洲	13	3	政府、军事、外交、能源、教育、科研
伊朗	亚洲	12	3	政府、外交、能源
韩国	亚洲	8	4	政府、大型企业
日本	亚洲	3	3	基础设施、组织机构、大型企业
以色列	亚洲	3	3	政府、军事、金融
土耳其	亚洲	3	2	政府、军事
沙特阿拉伯	亚洲	2	2	军事、金融
埃及	非洲	2	2	政府、军事、金融

表 2　全球 APT 研究关注被攻击国家排行

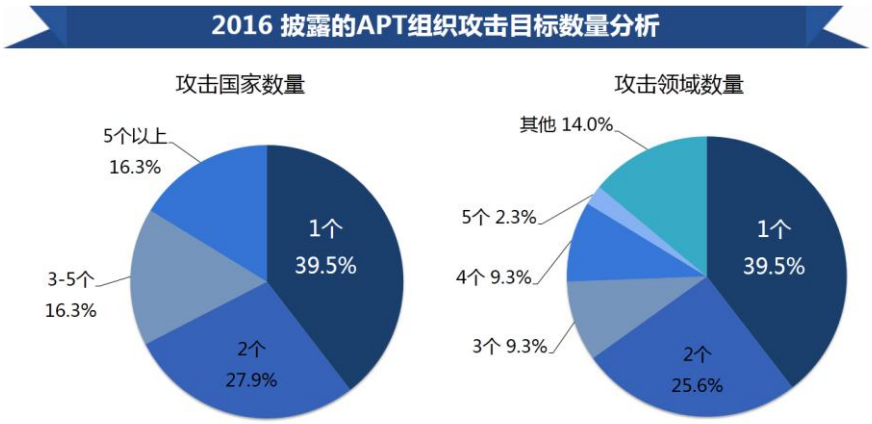
从上表中可以看出，无论是从相关研究报告的数量来看，还是从攻击组织的数量来看，中国都是全球 APT 攻击的第一目标国。各家报告披露的攻击美国的 APT 组织数量与中国相同，也是 9 个。同时，盯上印度、俄罗斯和乌克兰的 APT 组织也都超过了 5 个。

另外，在 2016 年 360 威胁情报中心监测到的 APT 报告中，我们还能看到：攻击政府和外交领域的 APT 组织最多，达 21 个；其次是金融领域，15 个；接下来以商业和技术机密为目的，攻击大型企业、商业组织和技术组织的 APT 组织，共 14 个；攻击军事、部队或其他国防机构的 APT 组织 13 个；攻击能源、交通、电力、医疗等基础设施的 APT 组织也有 12 个。有趣的是，还有 3 个 APT 组织会专门针对特定的个人发起攻击，这些被攻击的个人大多为政治异见者或媒体从业人员。最后是攻击教育、科研领域的组织共 2 个。

排行	APT 攻击领域	攻击组织数量
1	政府、外交	21
2	金融	15
3	大型企业、商业组织、技术组织	14
4	军事、部队、国防	13
5	能源、交通、电力、医疗等基础设施	12
6	特殊个人	3
7	教育、科研	2

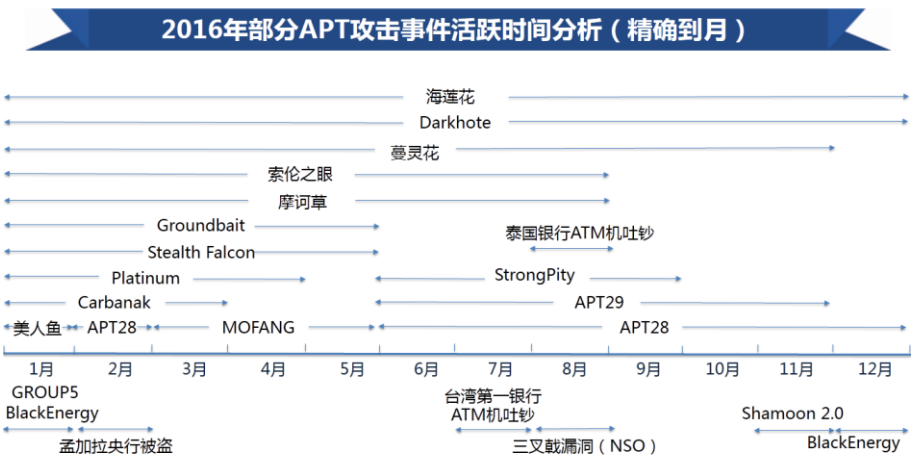
表 3　全球 APT 研究关注的 APT 组织攻击领域

还有一点值得注意：APT 组织的攻击虽然具有很强的针对性，但其攻击目标也并不一定是单一的。有的 APT 组织只攻击特定国家特定领域的目标（仅从目前已经披露的情况看），但也有很多 APT 组织会对多个国家的不同领域目标展开攻击。下图给出了 2016 年全球各国研究机构发布的 APT 研究报告中，披露 APT 组织攻击目标的所属国家、领域数量分析。



三、 主要 APT 组织的活跃时间

结合 360 威胁情报中心的大数据监测分析，以及 2016 年以来全球各研究机构与安全专家发布的 APT 研究报告，我们给出了 2016 年部分 APT 组织主要活跃时间的分析（精确到月），详见下图。



第二章　针对中国的 APT 攻击

一、　攻击中国的 APT 组织

截至 2016 年 12 月底，360 威胁情报中心已累计监测到的针对中国境内目标发动攻击的境内外 APT 组织 36 个。

在这 36 个 APT 组织中，针对中国境内目标的攻击最早可以追溯到 2007 年。而最近三个月（2016 年 9 月-11 月）内仍然处于活跃状态的 APT 组织至少有 13 个。

统计显示，仅仅在过去的 12 个月中，这些 APT 组织发动的攻击行动，至少影响了中国境内超过万台电脑，攻击范围遍布国内 31 个省级行政区。

下表给出了部分针对中国境内目标发动攻击的 APT 组织互动情况。

APT 组织	APT 行动	首先披露报告厂商	最早活动时间	最近活动时间
APT28	APT28	Fireeye	2007 年	2016 年 11 月
APT-C-12	APT-C-12	360	2011 年	2016 年 10 月
OceanLotus（APT-C-00）	OceanLotus	360	2011 年	2016 年 11 月
蔓灵花	蔓灵花	Forcepoint	2013 年	2016 年 11 月
索伦之眼	索伦之眼	Symantec	2010 年	2016 年 8 月
摩诃草	摩诃草	Norman	2009 年	2016 年 11 月

表 4　针对中国境内目标攻击的部分 APT 组织活动情况

二、　疑似 APT 攻击的目标

本报告定义以下组织机构为疑似 APT 攻击目标：若某个恶意程序样本或 C&C 服务器已经被确定为特定 APT 组织专用，且某组织机构的内部系统中出现了该恶意程序或与该 C&C 服务器有异常通信等状况发生时，则称该组织机构为疑似 APT 攻击目标。

通过对 360 威胁情报中心截获的 36 个 APT 组织专用木马的全网检测分析发现，截至 2016 年 12 月，国内疑似 APT 攻击目标的组织机构近 200 个。

若按照机构的数量统计，大学占比最高，为 40.0%；其次是企业，占比 25.0%；再次是政府及事业单位，占比 18.3%；还有科研机构占比 11.1%，其他机构或个人，占比 5.6%。

若按照机构内设备感染专用木马的数量统计，则企业是第一大疑似攻击

目标，占比为 35.2%；其次是大学，占比 30.3%；政府及事业单位占比 22.2%，科研机构占比 7.7%；其他机构或个人占比 4.6%。

APT 组织攻击不同类型的境内机构，其攻击领域和目的也有所不同。

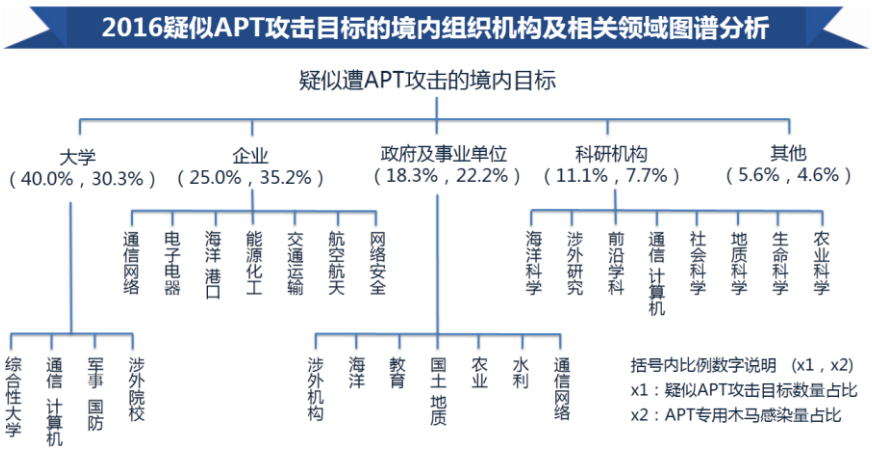
例如，在针对大学的攻击中，攻击者除了会攻击大量的综合性大学外，还会专门攻击通信与计算机、军事与国防、涉外学科等专业领域的院校。

在针对企业的攻击中，攻击者重点关注的领域依次是：通信网络、电子电器、海洋与港口、能源化工、交通运输、航空航天和网络安全，且疑似 APT 攻击目标的企业以网络运维、工程建设和制造业企业居多。

在针对政府机构和事业单位的攻击中，攻击者重点关注的领域依次是：涉外机构、海洋、教育、国土与地质、农业、水利和通信网络。

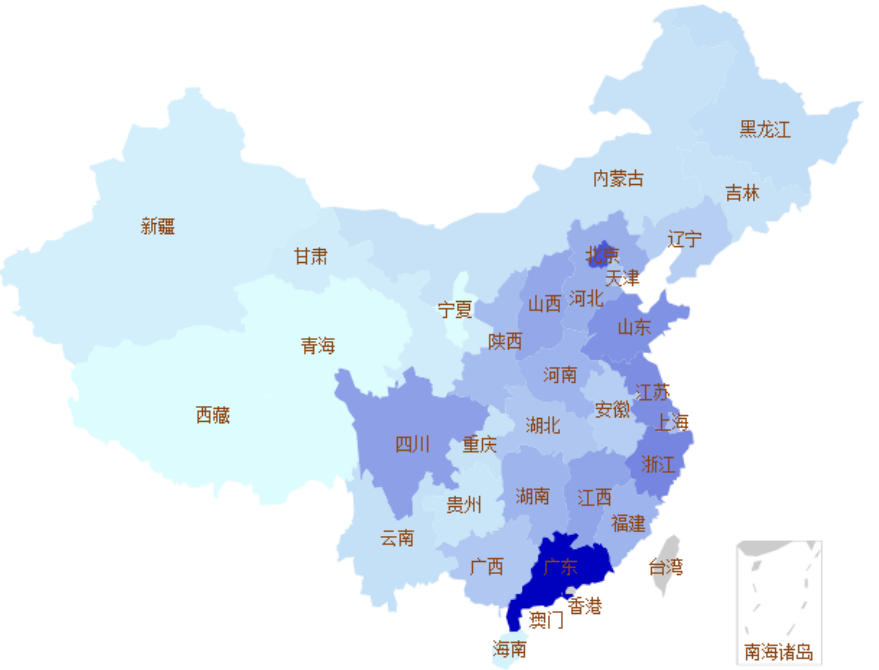
在针对科研机构的攻击中，攻击者重点关注的领域依次是：海洋科学、涉外研究、前沿学科、通信与计算机、社会科学、地质科学、生命科学和农业科学。

下图给出了 2016 年，疑似 APT 攻击目标的境内组织机构占比情况及被攻击领域的图谱分析。

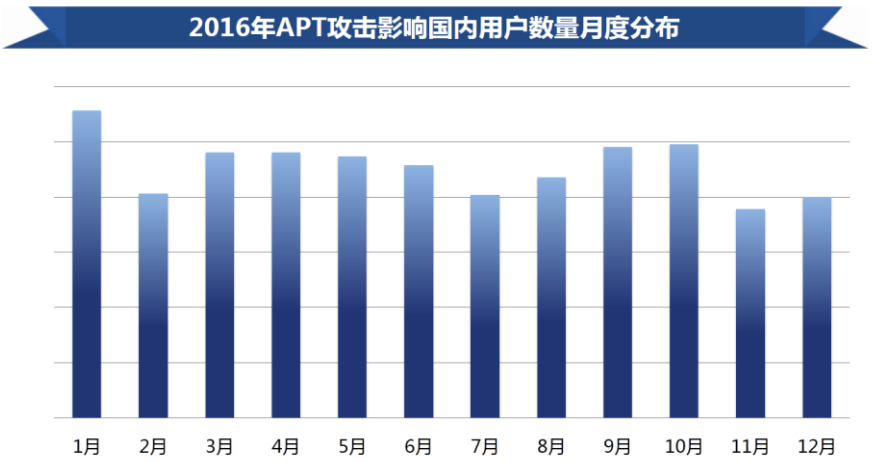


三、 APT 攻击的时空分布

根据 360 威胁情报中心的统计显示（不含港澳台地区）：国内受 APT 攻击影响最大，感染专用木马用户最多的省级行政区依次是：广东、北京、浙江、江苏、山东。而受影响最小，专用木马感染量最小的五个省级行政区依次是：新疆、海南、宁夏、青海、西藏。关于 APT 攻击在中国境内的分布情况，详见下图（不含港澳台地区）。



下图给出了 2016 年以来，APT 攻击影响中国境内用户数量的月度分布情况。



第三章　针对工业系统的破坏

从全球范围内的 APT 攻击事件监控与研究情况来看，绝大多数的 APT 攻击是以窃取机密信息为主要目的的，而具有显著破坏性的 APT 攻击并不多见。但 2015 年末至 2016 年以来，在世界范围内却先后发生了数起引起全球关注的，具有显著破坏性的 APT 攻击事件。其中尤以针对工业系统的破坏性攻击最为引人关注。

2015 年 12 月 23 日，也就是在圣诞节的前夕，乌克兰遭遇了大规模停电事件，数万“灾民”不得不在严寒中煎熬；而在 2016 年 11 月 17 日晚，也就是伊斯兰教的大赦之夜，沙特阿拉伯又遭遇了 Shamoon2.0 的攻击，包括沙特国家民航总局在内的 6 个重要机构的计算机系统遭到严重破坏。似乎每到年末的时候，针对工业系统的网络攻击就会悄然来袭，使那些可怜的受害者们无法“安心过年”。

一、　乌克兰圣诞大停电事件

2015 年 12 月 23 日，也就是 2015 年的圣诞节前夕，乌克兰一家电力公司的办公电脑和 SCADA 系统（Supervisory Control And Data Acquisition 系统，即数据采集与监视控制系统，一般用来代指工业控制系统）遭受到第三方非法入侵。事故导致伊万诺-弗兰科夫斯克地区将近一半的家庭经历了数小时的电力中断。起初，电力公司估计约 8 万名左右的用户受灾，后发现共有三种不同配电站的能源公司遭受攻击，造成各领域约 22.5 万名用户的电力中断。

攻击事件发生后不久，乌克兰政府官员声称电力中断是由网络攻击引起的，并指责俄罗斯国家安全部门应为此事负责。美国政府，以及许多的当地私营企业均对乌克兰的政府调查人员施以援手，协助乌克兰政府对攻击事件进行分析，以确定故障的根本原因。

2016 年 1 月 3 日，安全公司 ESET 最早披露了本次事件中的相关恶意代码，并发表文章称：乌克兰电力部门感染的恶意代码为 BlackEnergy。BlackEnergy 是一种后门程序，攻击者能够利用它来远程访问并操控电力控制系统；此外，在乌克兰境内的多家配电公司设备中还检测出了恶意程序 KillDisk，其主要作用是破坏系统数据以延缓系统的恢复过程。再者，研究人员还在电力系统的其他服务器上发现了一个被添加后门的 SSH 服务端程序，攻击者可以根据内置密码随时连入受感染的主机。

事实上，恶意程序 BlackEnergy 对乌克兰以及电力控制系统的攻击并不是第一次了。自 2007 年被首次披露以来，BlackEnergy 已经经历了多次的变种和升级，并且对乌克兰电力系统进行多轮次的“狂轰滥炸”。国外安全机构发布的研究资料还显示，2016 年，BlackEnergy 还在继续对乌克兰境内的多个工业系统发动攻击，并且在 2016 年的 12 月，又再次造成了乌克兰某电

力企业的一次小规模停电事故。下表给出了 BlackEnergy 发展的简要历程。

年份	事件概要
2007	Arbor 公司首次披露一个在 DDoS 攻击中被用来创建僵尸网络的工具 BlackEnergy，该版本一般被称之为“BlackEnergy 1”
2008	俄格冲突期间，一些身份不明的黑客针对格鲁吉亚的网络系统发动了 DDoS 攻击，BlackEnergy 被用于创建僵尸网络
2009	有黑客利用 BlackEnergy 盗取美国 Citibank 数千万美元
2010	戴尔旗下安全公司 SecureWorks 发布配备 Rootkit 的 BlackEnergy 变种，该版本一般称之为“BlackEnergy 2”
2011 年 7 月	ESET virusradar 研究显示，BlackEnergy 在全球活动达到高峰
2013 年 10 月	BlackEnergy 支持 64 位操作系统
2014 年 9 月	F-Secure 发现了为乌克兰政府量身打造的 BlackEnergy 新变种，该版本一般被称之为“BlackEnergy 3”
2014 年 10 月	有报道称，BlackEnergy 开发团队，疑似沙虫组织，针对北约、乌克兰和波兰政府、欧洲各重要工业系统进行了攻击
2014 年 10 月	ICS-CERT 警告 ICS 和 SCADA 中存在高危漏洞，并发现攻击者使用 BlackEnergy 2 攻击 SCADA HMI（人机接口）系统
2014 年 11 月	卡巴斯基称，BlackEnergy2 已经可以对路由器、Linux 系统、Windows 系统发起攻击，且能够攻击 Cisco 思科设备和 ARM 及 MIPS 平台
2015 年 11 月	乌克兰一家矿业公司和一家大型铁路公司的系统中发现感染了 BlackEnergy 和 KillDisk
2015 年 11 月	CERT-UA 首次将 BlackEnergy 和 KillDisk 关联在一起。当时正值 2015 乌克兰大选，多家新闻媒体公司被攻击，许多视频和文档资料被毁
2015 年 12 月	乌克兰电网被攻击，引发大规模停电事件，引发关注
2016 年 1 月	CERT-UA 通报称乌克兰最大机场基辅鲍里斯波尔机场遭受 BlackEnergy 攻击
2016 年 1 月	卡巴斯基研究人员发现新型针对乌克兰的 BlackEnergy 文档类攻击，使用 Word 攻击乌克兰电视台 STB
2016 年 12 月	乌克兰的国家电力部门疑似被网络攻击，导致其发生了又一次的大规模的停电事件，本次停电持续了大约 30 分钟。此次停电事件疑似由“外部干扰”所导致的，恶意攻击者通过网络对公司电力系统进行了非法操作。

表 5　BlackEnergy 的发展历程

乌克兰电力系统遭到的持续攻击，引起了世界各国安全行业和政府的高度重视。实际上，全球几乎所有的电力公司所使用的工业控制系统都十分类似，操作系统也都以 Windows 居多，底层的硬件更是垄断在为数不多的几个大公司手中，因此，我们预期类似的攻击很有可能会在其他国家和地区重现。

二、 沙特大赦之夜攻击事件

根据境外媒体报道，2016 年 11 月 17 日晚，也就是伊斯兰教的大赦之夜（Lailat al Qadr），包括 GACA（沙特国家民航总局）在内的至少 6 家沙特重要机构遭到了严重的网络攻击。受害者的电脑系统中大量文件和数据被损毁，代之以一张 2015 年 9 月 2 号溺水的叙利亚难民男孩 Alan Kurdi 的照片。

研究者们将此次攻击行动调查中截获的恶意程序样本命名为 Shamoon2.0，同时也将此次攻击行动命名为 Shamoon2.0，因为研究人员们发现，被截获的攻击样本实际上是 2012 年被发现的 Shamoon 程序的一个变种。

2012 年 8 月 15 号，在针对沙特石油巨头 Saudi Ameraco 的网络攻击中，Shamoon 恶意程序首次现身。攻击发动的时候，正值该公司员工休假期间，该公司大约 3 万多台电脑上的文件都遭到损毁。事后，有一个自称 Cutting Sword of Justice 的组织宣布为此次事件负责，但是根据当时多家安全机构的分析，此次攻击应该是一个来自伊朗的有国家背景的黑客组织所为。

所以，尽管媒体在报道 2016 年 11 月发生的这次网络攻击事件中，并未详细报道更多受害者的具体信息，也未对受害者遭受的具体损失情况做详细的说明，但参考 2012 年的 Shamoon 攻击事件以及 Shamoon2.0 与 Shamoon 的相似性，我们大致可以猜测出：此次攻击事件中的主要受害者应该是沙特的工业系统或工业部门，而受害者的主要损失就是大量系统文件与系统数据被恶意删除，致使工业系统无法正常运行。

Shamoon，又称 Disttrack，是一款模块化恶意程序，具有很强的毁坏性，能够导致目标网络完全瘫痪。此前共发生了两次由 Shamoon 引起的网络攻击事件（其中一次为疑似案例），而攻击目标都是沙特。

Shamoon 使用的模块程序分为三类：分别是投放器（Dropper）、通讯组件（Communications）和擦除组件（Wiper components）。Shamoon 不仅仅会对目标进行数据的收集，还具有很强的破坏性——即程序内部存在定时器，当系统时间超过设定的时间，Shamoon 就会用无用的数据，例如特定的 JPEG 图片，来覆盖磁盘（包括 MBR、分区表和分区），导致磁盘数据的损毁和被攻击系统的瘫痪。

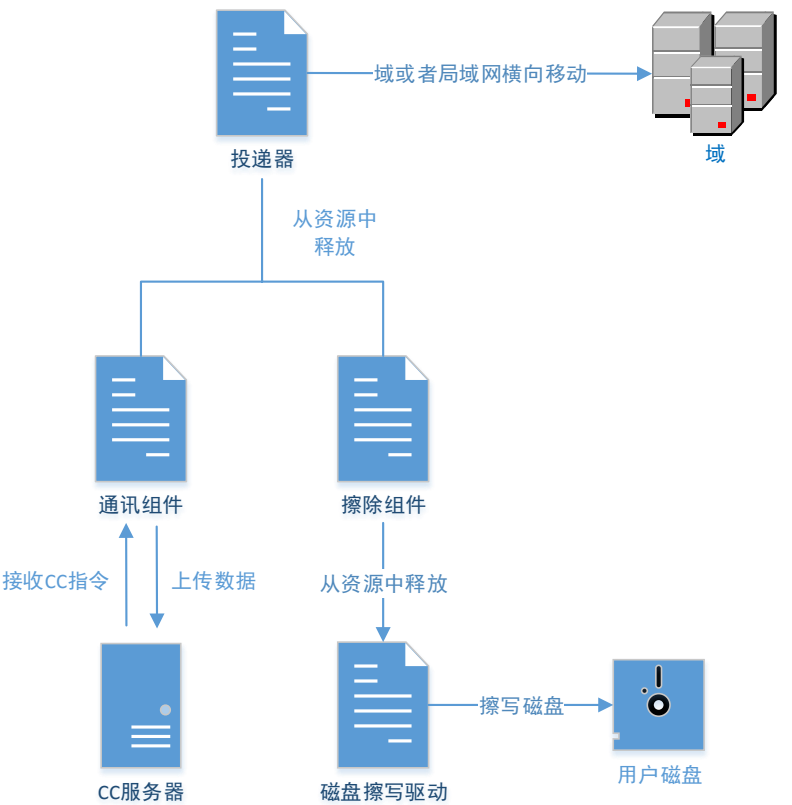
实际上，Shamoon 在 2012 年和 Shamoon2.0 在 2016 年的攻击中都用了 JPEG 方法：2012 年的攻击中使用的是燃烧着的美国国旗，而 2016 年的攻击中出现的图片是 2015 年 9 月 2 号溺水的叙利亚难民男孩 Alan Kurdi。

两次攻击的恶意程序编写方式也十分相似，使用了同一个 RawDisk 设备驱动（临时的证书密钥都一样），投递器在释放恶意程序组件时，会从资源中的特定位置读取字节数并且用 Base64 编码的密钥来解密，在与从资源中获取的 Byte 串进行异或操作，拼接后获取完整的程序。

Shamoon 本身还会尝试通过当前的权限来访问当前系统的活动目录，相同域及局域网上的其他主机，进行横向移动。Shamoon 的横向移动可能导致的最严重情况是整个目标网络的大规模瘫痪。

特别值得一提的是，Shamoon2.0 的恶意破坏性要比 Shamoon 更加明显。在先前的 Shamoon 攻击中，恶意样本会首先窃取用户数据并上传到 C&C 服务器上之后，才会执行文件删除或覆盖操作，这就使我们在理论上有可能通过阻断网络或限制 IP 访问等方法来阻止 Shamoon 的破坏行为。但 Shamoon2.0 的攻击者却在程序中填写了一个完全不可达的 C&C 服务器地址，并在程序中编码了定时器时间为 2016 年 11 月 17 日晚 8:45。这就使得 Shamoon2.0 俨然成为了一颗“定时炸弹”，一旦成功投放，就几乎一定会“爆炸”。

下图给出了 Shamoon 的基本攻击原理。可以看到，投递器投递成功后，通讯组件被释放并且执行后开始与 C&C 服务器进行通讯，其通信过程使用的是 HTTP 协议。但 Shamoon2.0 与之前的版本存在区别，之前的 Shamoon 是将用户的数据上传到 C&C 服务器当中；但是 Shamoon2.0 中，C&C 服务器的地址却被填写成一个不可达的地址：1.1.1.1:8080。



总体而言，Shamoon 与 Shamoon2.0 具有很强的相似性，不仅是攻击的目标国家相似，选取的攻击时间点存在共性（休假期间），而且具体实现技术和攻击原理也都十分相似。因此，多数研究者认为，Shamoon 与 Shamoon2.0 的攻击应为同一黑客攻击组织。

第四章　针对金融系统的犯罪

2016 年可以称得上是一个全球银行机构的网络灾害年。先是上半年接连发生了以孟加拉国央行为代表的一系列发展中国家的央行或大型国有银行被盗事件，受害者损失高达数千万美元。随后，下半年又接连发生了以台湾第一银行 ATM 吐钞事件为代表的一系列 ATM 机攻击事件。而一个以合法软件开发企业为伪装的，以不当盈利为目的的，长期从事敏感金融交易信息窃取活动的境内 APT 组织“黄金眼”，也在 2015 年底至 2016 年初被截获。在这些攻击中，我们可以看到，即便是在理论上隔离的，防护级别极高的金融系统中，网络攻击依然可以无孔不入，而且危害巨大。

一、　多国银行被盗事件

2016 年初，媒体陆续曝出了孟加拉、厄瓜多尔、越南、菲律宾等多个国家的银行系统曾经遭遇黑客攻击的消息。尽管这些攻击事件的发生时间不尽相同，但它们都有一个共同特点，就是攻击者都瞄准了 SWIFT 银行间转账系统，并利用这一系统存在的某些“特点”来发动攻击并销毁证据。下表给出了部分攻击事件的发生时间和损失情况。

攻击时间	被攻击银行	计划窃取	实际损失
2013 年	索纳莉银行（Sonali Bank）	未知	25 万美元
2015 年 1 月	厄瓜多尔银行（Banco del Austro）	未知	1200 万美元
2015 年 10 月	疑似菲律宾某银行	未知	未知
2015 年 12 月	越南先锋银行（Tien Phong Bank）	120 万欧元	无
2016 年 2 月	孟加拉国央行（Bangladesh Central Bank）	9.51 亿美元	8100 万美元
未知	疑似香港某银行	未知	未知
未知	疑似菲律宾、新西兰某银行和其他 10 多家金融机构	未知	未知

表 6　BlackEnergy 的发展历程

（一） 孟加拉国央行（Bangladesh Central Bank）

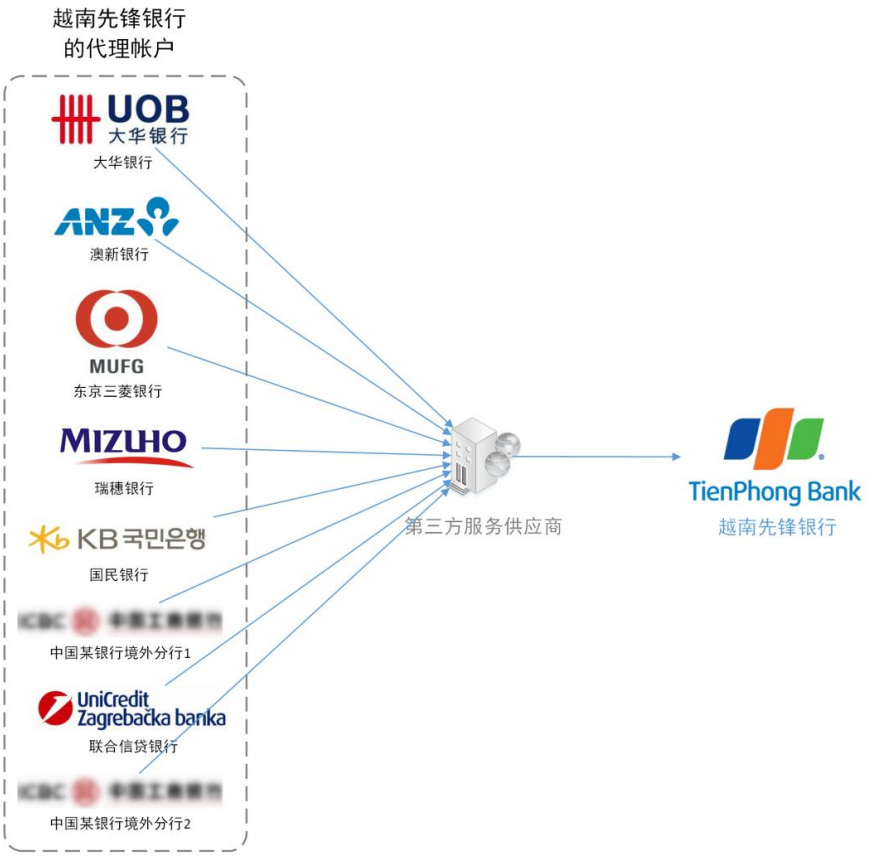
2016 年 2 月 5 日，孟加拉国央行被黑客攻击导致 8100 万美元被窃取。攻击者通过网络攻击或者其他方式获得了孟加拉国央行 SWIFT 系统操作权限，随后，攻击者向纽约联邦储备银行（Federal Reserve Bank of New York）发送虚假的 SWIFT 转账指令，而孟加拉国央行在纽约联邦储备银行上设有代理帐户。纽约联邦储备银行总共收到 35 笔，总价值 9.51 亿美元的转账要

求，其中 30 笔被拒绝，另外 5 笔总价值 1.01 亿美元的交易被通过。而这其中又有 2000 万美元因为拼写错误被中间行发觉而被找回，而另外 8100 万美元则被成功转走盗取。

而我们捕获到的这次网络攻击所使用的恶意代码，其功能是篡改 SWIFT 报文和删除相关数据信息以掩饰其非法转账的痕迹。其中攻击者通过修改 SWIFT 的 Alliance Access 客户端软件的数据有效性验证指令，绕过相关验证。

（二） 越南先锋银行（Tien Phong Bank）

2015 年 12 月 8 日，越南先锋银行遭黑客攻击，其攻击手法与孟加拉央行遭到的攻击类似。攻击者最终从越南先锋银行盗走了约 120 万欧元。



360 追日团队也捕获了攻击越南先锋银行的恶意程序样本。相关恶意代码内置了 8 家银行的 SWIFT CODE（参见上图），越南银行均在这些银行中设有代理帐户。目前看到的 Fake PDF Reader 样本的目的并不是攻击列表中的这些银行，而是用来删除越南先锋银行与其他家银行间的转帐确认消息（篡改 MT950 对帐单）。这样银行的监测系统就不会发现这种不当交易了。

关于针对越南先锋银行攻击的详细分析，可以参见 360 追日团队此前发布的报告：《SWIFT 之殇——针对越南先锋银行的黑客攻击技术初探》。

（三） 厄瓜多尔银行（Banco del Austro）

据路透社报道，2015 年 1 月 12 日，在一条来自厄瓜多尔银行系统信息的指引下，位于旧金山的 Wells Forga 美国银行向某个香港的银行账户进行了转账。并且在接连 10 天内，至少有 12 笔厄瓜多尔银行资金通过 SWIFT 系统被转走，总金额高达 1200 万美金。厄瓜多尔银行已就该事件将 Wells Frago 告上了纽约法庭，理由是 Wells Forgo 美国银行本应该将这些交易标记为可疑交易。然而从诉讼资料看，双方银行都相信这些资金是被匿名黑客盗走的。

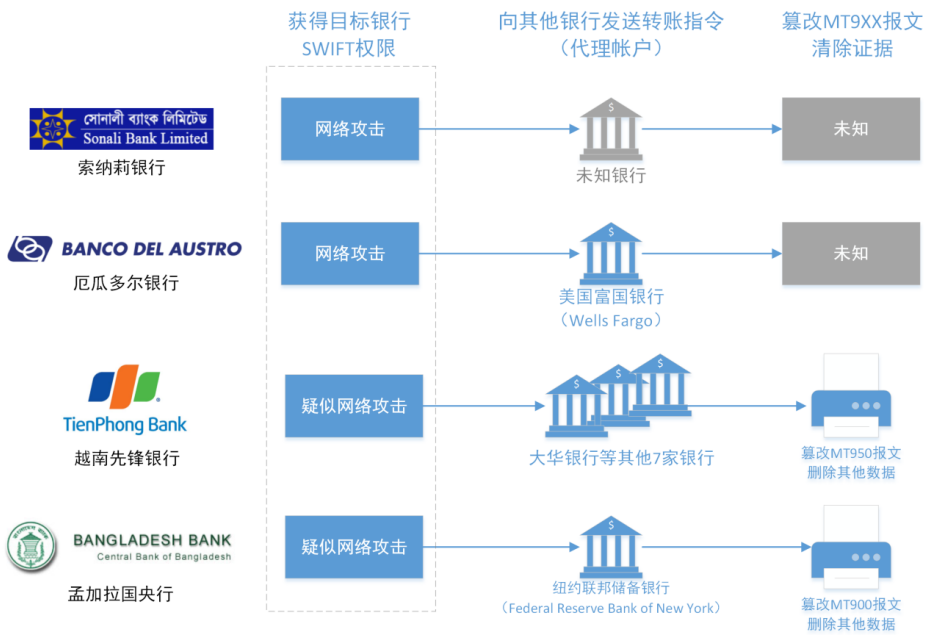
另外，SWIFT 方面的负责人在案件被报道之前却对此毫不知情。相关人士称，SWIFT 确实会核验系统发送信息中的密码来确保信息来自银行用户的终端设备。但是一旦网络盗窃者获取了密码和证书，SWIFT 就无法判断操作者是不是真正的账户持有人了。而黑客正是钻了这个空子，盗取了一名银行雇员的 SWIFT 证书，进而盗走了巨额资金。

（四） 索纳莉银行（Sonali Bank）

据路透社报道，2013 年孟加拉国的索纳莉银行（Sonali Bank）也发生了类似孟加拉央行的攻击事件。在索纳莉事件中，攻击者共盗取了 25 万美金的银行资金。银行 IT 运营部的高级官员称，在索纳莉银行劫案中，黑客们在一台电脑上安装 keylogger 来窃取其他系统的密码，然后使用 SWIFT 系统发送伪造的转账申请。

（五） 攻击事件的相似性分析

通过分析从 2013 年的索纳莉银行到 2016 年的孟加拉国央行这 4 起攻击银行的事件，结合下图，不难看出相关攻击事件之间有很多的相似性。



从攻击战术或攻击流程来看，攻击者的攻击过程主要由三个环节组成：获得 SWIFT 权限，利用 SWIFT 发送转账指令，最终清除证据掩盖事实。下面就来分别展开分析一下。

1） 获得目标银行 SWIFT 权限

攻击者首先需要获得目标银行的 SWIFT 系统操作权限。从相关报道来看，在索纳莉银行和厄瓜多尔银行攻击事件中，攻击者均是通过网络黑客技术来获得相关权限。特别是索纳莉银行攻击事件中，可以确定 SWIFT 相关登录帐号和密码是被植入的恶意程序所监控窃取。

由此我们可以得到一个信息，就是攻击者要获得 SWIFT 操作权限，并不一定需要与银行内部系统进行物理接触，完全可以通过网络攻击来完成。而目前尚未有报道明确指出孟加拉国央行的 SWIFT 系统权限是如何被盗取的，但调查孟加拉央行事件的研究人员则表示，应该是黑客利用网络攻击获得了相关登录凭证。而越南先锋银行的情况略有不同。该银行系统本身并没有被攻击，问题出在其第三方服务商（提供 SWIFT 服务）身上，但目前尚不清楚攻击者是否是通过网络攻击的方式获得了相关 SWIFT 操作权限的。越南先锋银行表示之后要改为直接连接 SWIFT 系统。

2） 向其他银行（代理帐户）发送转账指令

攻击者在获得 SWIFT 权限之后，最核心的目的就是要利用 SWIFT 发送转账指令。我们推测攻击者发送的应该是 SWIFT MT 报文中的第一类报文，如 MT103（单笔客户汇款）。除索纳莉银行以外，我们发现攻击者均向存在目标银行代理帐户的银行发送了转账指令，如美国 Wells Forga 银行设有厄瓜多尔银行的代理帐户；大华银行等其他 7 家银行设有越南先锋银行的代理帐户；纽约联邦储备银行设有孟加拉国央行的代理帐户。通俗来讲也就是孟加拉国央行等这几个目标银行存在其他银行上的钱被冒名转走了。

3） 篡改 MT9XX 报文清除证据

由于我们暂未捕获到针对索纳莉和厄瓜多尔银行进行攻击的恶意样本，所以我们无法知道是否有该环节。本段分析主要来自于对越南先锋银行和孟加拉国央行攻击事件的追踪。

首先攻击者都是对 MT9XX 报文进行了劫持：对越南先锋银行的攻击是劫持 MT950 对帐单，对孟加拉国央行的攻击则是劫持了 MT900 借记证实。

其次，两次攻击事件中，攻击者都对相关报文进行了篡改，目的是删除相关转帐记录，进行平帐。而两次攻击事件有一点点区别的地方是：孟加拉国央行事件中是对相关报文篡改后直接发送给打印机打印出来；而越南先锋银行事件中则是对 MT950 的电子版 PDF 文件进行篡改，然后再把 PDF 文件发给打印机打印。但不论怎样，攻击者最终目的就是篡改报告，另外删除其他一些数据信息，从而抹去相关证据线索。

另外，我们还发现，在越南先锋银行事件和孟加拉国央行事件中，攻击者所使用的恶意代码，都存在一个特殊的安全删除函数，这也更进一步证明了这两次攻击事件的同源性，它们并不是孤立的，两者之间必然有一定联系。

二、 ATM 机盗窃事件

与前述的利用 SWIFT 机制进行跨国银行盗窃的攻击手法相比，针对 ATM 机的攻击，风险则要大了很多。因为攻击者最终必须现身于 ATM 机前提取现金款。这也就给警方侦破案件，抓捕犯罪分子留下了更多的机会。

（一） 台湾第一银行（First Bank）

2016 年 7 月 12 日，台湾第一银行发布公告《第一银行 ATM 遭异常盗领客户权益不受影响》表示“第一银行部分分行 ATM 提款机遭异常盗领，作案过程约 5~10 分钟，交易集中在 7 月 9 日和 7 月 10 日，目前本案共计遭盗取的金额约 7000 多万新台币，20 家分行共 34 台 ATM 发生异常，目前已紧急报警处理。初步了解可能遭植入恶意软件驱动吐钞模块执行吐钞”。

后经第一银行清算核实，全台共有 41 台 ATM 遭到盗领，被盗金额 8327 余万元。这是台湾首宗银行遭跨境黑客盗领案。后经台湾警方侦破追捕，抓获罗马尼亚籍和摩尔多瓦籍共犯各一人，追回赃款 6050 万元。后续调查还显示，此次攻击中，攻击者是通过攻击补丁更新服务器，向 ATM 机下发恶意程序的，这些恶意程序会开启 ATM 远程控制服务(Telnet Service)，使藏身在海外的幕后操控者可以操控 ATM 机“吐钞”。

此次事件中遭攻击的 ATM 机，全部是来自德利多富（Wincor）公司的同一款机型（pro cash1500 机型），目前该款机型已全面暂停服务。据了解，德利多富（Wincor）的产品涉及银行业及零售业，提供包括现金类自助设备和非现金类自助服务终端及其解决方案，代表硬件产品包括自动取款机、存取款一体机、多媒体服务终端、存折打印机等，业务遍及 130 多个国家。

在对相关攻击事件的分析中，我们发现攻击者并没有使用银行卡和对 ATM 机操作等，即攻击者无需物理接触 ATM 机，就能实现 ATM 机自动吐钞目的。这点攻击现象引起了我们的注意，以往攻击 ATM 的事件并不少见，但能达到不进行物理接触而使 ATM 吐钞的攻击，还是比较少见的。

（二） Anunak 组织（即 Carbanak）

不过，在台湾第一银行 ATM 机吐钞事件之前，也有其他攻击组织曾经实施过这种针对 ATM 机的非接触式攻击。其中最为最著名的 APT 组织就是 Anunak（即 Carbanak）。

Anunak 组织的攻击活动始于 2013 年，该犯罪团伙总计向全球约 30 个国家和地区的 100 家银行、电子支付系统和其他金融机构发动了攻击，相关

攻击活动还很活跃。在《2015 年中国高级持续性威胁（APT）研究报告》中我们也提到了 Anunak。通过研究分析该组织相关攻击手法和意图，我们将该组织视为针对金融行业的 APT 组织。

Anunak 组织攻击的一般过程是：首先，通过极具针对性的攻击手法，入侵金融机构员工的计算机或银行网络；随后，通过内部网络，对计算机进行视频监控，从而查看和记录负责资金转账系统的银行员工的屏幕；最后，当攻击者了解到银行相关员工工作的全部详情后，就会模仿银行员工的行为进行恶意操作，盗取银行资金。

另外该组织还可以控制银行的 ATM 机，命令这些机器在指定的时间吐出现金。当到支付时间时，该组织会派人在 ATM 机旁边等待，以取走机器“主动”吐出的现金。

通过将 Anunak 的攻击手法与台湾第一银行吐钞事件进行对比，我们发现，二者之间有很多相似的地方，具体如下表所示：

	台湾第一银行	Anunak（即 Carbanak）
幕后组织	攻击者来自俄罗斯	攻击者来自俄罗斯
攻击方式	利用恶意程序	利用恶意程序
植入方式	攻击补丁更新服务器	攻陷银行内网，到获得 ATM 权限
ATM 品牌	Wincor	Wincor
吐钞方式	突破取款上限，连续吐钞	突破取款上限，连续吐钞
取现方式	指定时间，无需物理接触	指定时间，无需物理接触
攻击规模	40 台 ATM	52 台 ATM
窃取金额	8000 万新台币	5000 万卢布

表 7　台湾第一银行吐钞事件与 Anunak 攻击特点的对比

（三） 泰国邮政储蓄银行

2016 年 8 月，泰国政府储蓄银行发现，从当月的 1 日至 8 日，全国共有 21 台 ATM 机中的现金被盗。这些被盗的 ATM 机分别分布在曼谷、普吉岛、春蓬、 巴蜀、 碧武里和素叻他尼等地。获悉此事后，泰国中央银行（Central Bank of Thailand ， BoT）向全国的商业银行发出安全警告，关闭了全国约 3300 台 ATM 提款机。

通过对 ATM 机内部摄像头捕获信息的分析，泰国警方确认此次事件中的犯罪团伙属于外籍人士。随后，泰国警方逮捕了三名犯罪嫌疑人，据这些犯罪嫌疑人交代，他们组织大约有三十名东欧人，其中大部分人都在 ATM 机领域有多年的工作经验，同时，组织内部还有三名俄罗斯人。

该犯罪团伙的主要攻击手法是：通过插入特别制造的 ATM 卡（带有 EMV 芯片），将恶意程序 Ripper 植入到 ATM 机中。恶意程序一方面会让 ATM 机每次吐钞 4000 泰铢，另一方面会使 ATM 机与银行网络断开，从而使 ATM

机在吐钞时不会被发现。

据调查，该犯罪组织通常是在深夜集体出动，相互配合作案。在 8 月的 1 日-8 日期间，该组织累计从泰国各地的 ATM 机上取走了大约 1229 万泰铢（约合 346,000 美元）。

有意思的是，就在曼谷邮报正式对外报道“泰国银行 ATM 机被攻击，一千两百万泰铢被盗” 这一事件的几分钟之前，该恶意软件样本就被一位身份不明的人上传到了 VirusTotal 平台上，而 IP 显示上传设备位于泰国境内。

（四） 针对 ATM 机的各种攻击

由于 ATM 机通常是处于一个相对隔离的网络环境中，因此，在对 ATM 机发动攻击时，如何植入恶意代码就成为了一个关键问题。目前已知的主要攻击手法有以下两类：

1） 入侵银行内部网络，获得 ATM 机控制权限

2） 通过光驱、USB 接口等直接对 ATM 机进行操作

另外，攻击 APT 机器的恶意程序也不一定只是让机器吐钞，也有一些恶意程序会通过 ATM 机暗中收集银行卡持卡人的数据信息。

下表给出了部分专门攻击 ATM 机的恶意程序的攻击方式对比。

出现时间	恶意程序名称	植入需要的媒介	ATM 机接口	攻击目标	目的	物理接触
2009	Skimer	特制的银行卡	读卡器	银行持卡人	盗取现金、银行卡数据	是
2013	Ploutus	手机	USB	银行持卡人	盗取现金、银行卡数据	是
2013	Anunak Carbanak	攻陷银行网络		银行	盗取现金	否
2014	Tyupkin Padpin	可引导光盘	光驱	银行	盗取现金	是
2015	Green Dispenser	内部人员植入		银行	盗取现金	是
2015	SUCEFUL	未知		持卡人	盗取现金、银行卡数据	未知
2016	Ripper	攻陷银行网络		银行	盗取现金	是

表 8　部分 ATM 机的恶意程序的攻击方式对比

三、 黄金眼行动事件

2015 年 12 月，360 安全服务团队基于日常的应急响应记录结合云端大数据，发现一系列针对金融机构的定向攻击事件，360 安全服务团队联合 360 追日团队对此事件展开了深入调查。

调查结果显示，攻击者是一个以合法软件开发企业为伪装的，以不当盈利为目的的，长期从事敏感金融交易信息窃取活动的境内 APT 组织。其攻击水平和反侦察能力均达到了国家级水平，甚至超出了很多境外的 APT 组织。该组织的活动时间至少长达 12 年以上，遭到该组织长期攻击的金融机构涉及多家。

鉴于该组织是一个专门针对金融系统发动攻击的 APT 组织，我们将该组织及其发动的攻击行动命名为“黄金眼”，组织及行动编号 APT-C-19。

调查显示，黄金眼行动最早可以追溯到 2004 年，相关攻击活动分别在 2012 年和 2014 年呈现两次高峰，且 2014 年的攻击强度远远超过 2012 年。其主要攻击对象为：基金、证券、保险、理财和资产管理等多种类型的境内金融机构，还包括一部分的个人股民。

黄金眼行动使用了一整套恶意代码对目标系统实施入侵和控制，并可跨越所有 Windows 平台发动攻击。特别的，该组织的相关攻击工具经过了长期不断的版本升级和功能演化。我们甚至发现在某些特定时期，攻击者会不分昼夜地对工具进行开发改进。

此外，黄金眼行动还具有极强的反侦察能力，相关攻击代码在被释放出来之前也做了必要的清理，基本不包含任何可能泄露作者或攻击者所处环境的信息。

黄金眼行动的恶意代码，其架构之复杂，功能之完善，反侦察能力之强大，以及持续改进的繁多版本，显示出该组织开发运维的高度专业性。

此外，我们也发现，即便仅仅从对金融业务的熟悉程度来看，黄金眼行动也具有高度的专业性。我们有理由认为，该 APT 组织实际上是由一群计算机专家和熟悉金融业务的人员共同组成。

从攻击目的来看，黄金眼行动主要是通过恶意程序窃取其他金融机构的敏感交易信息，进而将这些交易信息作为投资情报，用于不当的投资活动并赚取非法超额利润。

第五章　针对地缘政治的影响

网络攻击究竟会在多大的程度上影响一个国家的安全与发展？美国的 DNC 邮件泄露事件真的可以说让我们所有人都大开眼界。很多人都相信，是俄罗斯的 APT 组织，通过巧妙的攻击与运作，成功改写了美国大选的竞选结果，进而也可能因此改变了整个人类的历史发展进程。此外，方程式组织工具的泄漏事件也引发了人们对于网络攻击影响地缘政治的深度担忧。

一、 DNC 邮件泄露与美国大选

（一） 希拉里邮件门

首先需要说明的是，希拉里邮件门并不等同于 DNC（民主党全国委员会，Democratic National Committee）邮件泄露事件，DNC 邮件泄露事件只不过是希拉里邮件门的一个关键组成部分。只不过，这个关键的组成部分确实对希拉里邮件门的最终走向起到了决定性的作用，并最终帮助特朗普战胜希拉里，成功当选美国总统。

分析希拉里邮件门事件，还要从 2009 年至 2013 年说起。根据 FBI 的调查显示，希拉里担任美国国务卿的这段时间里，使用私人电子邮箱和位于家中的私人服务器收发公务邮件，其中包括一些涉及国家机密的绝密邮件。这批邮件一共约 6 万封。此事于 2015 年 3 月被曝出。2015 年 7 月，美国联邦调查局 FBI 启动了对此事调查程序。

但是，在 FBI 的调查工作开启之前，即将被调查的 6 万封邮件中，就有 3 万多封已经被希拉里团队以涉及私人生活为由删除了，只剩下另外约 3 万封邮件可供调查。此事被媒体披露后，引发了公众对希拉里更多的质疑。不过，当时还远未到美国大选的关键时刻，此事件对希拉里即将参加的美国总统大选的影响甚微。

然而，事态在 2016 年 7 月，也就是美国总统大选最为热闹、最为激烈的关键时刻，却发生了急剧的变化。自 2016 年 7 月 23 日起，维基解密逐步公开了与 DNC 有关的 19252 封电子邮件及 8034 份邮件附件，这些邮件主要是 2015 年 1 月至 2016 年 5 月间，DNC 高级职员间往来的电子邮件，涉及的账户主要包括民主党的一些高层官员，如通信主管、国家财务主管、财务负责人、数据与战略行动部的财务主管等。事件发酵后，有多名希拉里团队的高级官员引咎辞职。

2016 年 8 月 12 日，此前声称对 DNC 遭黑客攻击事件负责的黑客组织 Guccifer 2.0 也再次放出大量机密文件，涉及美国民主党国会竞选委员会（DCCC）的大量数据，并声称自己放出这些资料是因为公众有权力知道竞选过程中被主流媒体、政治家们隐藏的事实真相。

实际上，这些 DNC 泄漏出来的邮件主要揭示了这样一个问题：早在 2016 年 2 月民主党内初选开始前，DNC 就已经开始暗中支持希拉里争夺党内提名，同时排挤希拉里在党内的最大竞争对手伯尼·桑德斯。此外，邮件内容还显示了希拉里竞选团队操纵媒体，涉嫌洗钱，有意抹黑特朗普等党内丑闻，此事引起美国政坛的巨大震动，也进一步引发了公众对于那被删除的 3 万封邮件内容的负面猜测。

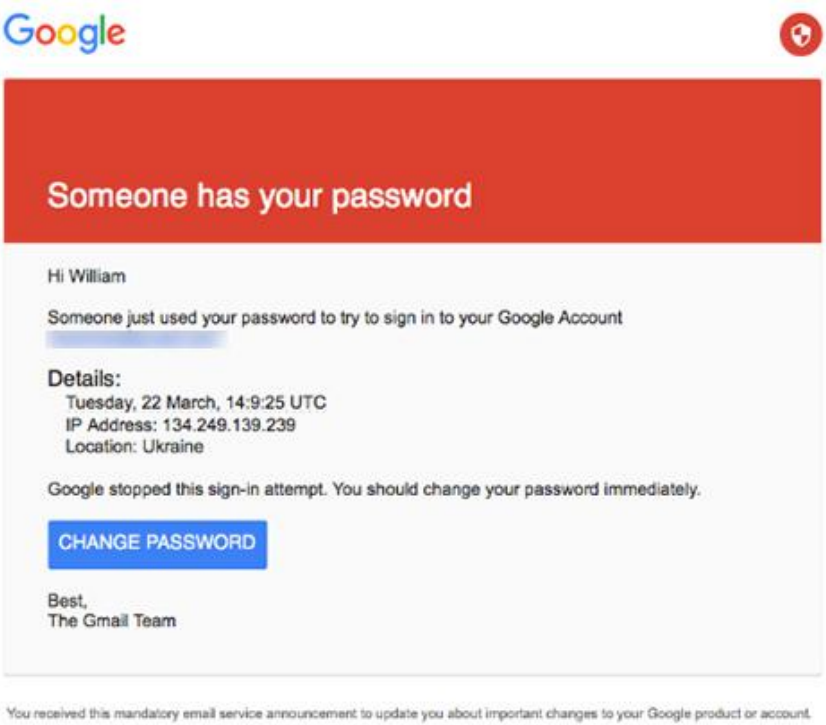
DNC 邮件泄露事件把希拉里邮件门推向了高潮。事件持续发酵并对美国社会和大选舆情产生了微妙的影响，最终使本来民调一直相对领先的希拉里在最后关头败下阵来。特朗普成功当选美国总统。

（二） DNC 邮件泄露过程

下面就来说说 DNC 的邮件是怎么泄漏出去的。

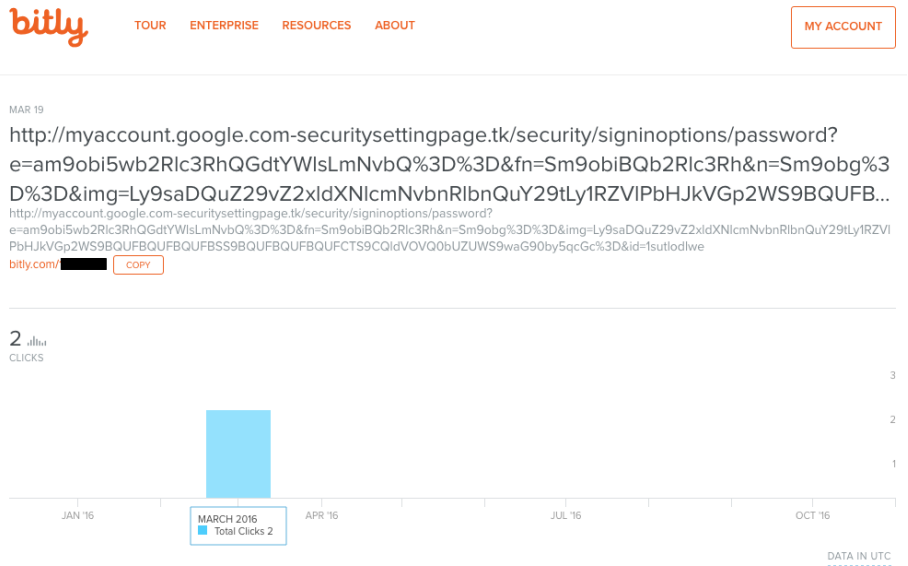
安全人员的事后调查发现，DNC 邮件泄漏事件可能最早始于 2016 年 3 月。2016 年 3 月 19 日，希拉里竞选团队主席约翰·波德斯塔（John Podesta）收到了一封伪装成 Google 的警告邮件的钓鱼邮件，Podesta 无意点击了邮件中的恶意链接，进而泄露了自己的邮箱密码，从而使得攻击者获取了他邮箱里的所有邮件。

相同的攻击手法还被用于攻击科林·鲍威尔（Colin Powell）和希拉里另一竞选团队成员威廉·莱因哈特（William Rinehart）。下图为威廉·莱因哈特收到的伪装成 Google 安全团队的钓鱼邮件。



特别值得一提的是，在上述攻击过程中，攻击者还使用了一些独特的伪装手法。例如，利用 Bitly 将钓鱼邮件中恶意网址伪装成 Bitly 短网址。而 Bitly 则是世界上最流行的短链接服务之一，可以让用户自定义自己的短链接域名，把正常的网址缩短成短链接。

下图就是攻击约翰•波德斯塔的 Bitly 短网址链接。



实际上，DNC 的工作人员也早就意识到了其组织内部的电脑或邮箱可能遭到了黑客攻击，并于 2016 年 5 月聘请了网络安全公司 CrowdStrike 进行检查，该公司与 7 月宣称，已经将这两组黑客清出 DNC 的系统。

（三） DNC 攻击者背景分析

1） Guccifer 2.0

那么，究竟是谁攻击了 DNC 并泄漏了 DNC 的机密邮件呢？

首先站出来宣称对此事件负责的是一个名为 Guccifer 2.0 的黑客。

2016 年 6 月 15 日，在 CrowdStrike 发表对 DNC 被攻击事件调查报告的第二天，一名自称来自罗马尼亚的黑客 Guccifer 2.0 承认为 DNC 攻击事件负责，并宣称自己已经掌握了大量 DNC 的机密资料。为证明自己身份的真实性，他还披露了十几份机密文件，其中包括捐助人信息和党内财务记录等。2016 年 8 月 12 日，Guccifer 2.0 再次放出大量机密文件，涉及美国民主党国会竞选委员会（DCCC）的大量数据。

Guccifer 2.0 还否定了 CrowdStrike 的调查报告，认为 DNC 试图让俄罗斯为此事负责是非常可笑的。他否认自己与俄罗斯有关，并说明自己之所以取这个名字是为了向一位名为 Guccifer 的黑客致敬。

第一代 Guccifer 是一名 44 岁的罗马尼亚出租车司机，他在 2013 年破解了美国前总统布什的私密文件，随后因攻击政府网站，2014 年被罗马尼亚政府起诉获刑 7 年，后被引渡到美国。

从 Guccifer 2.0 公开的资料来看，该黑客或黑客组织应当与 DNC 被黑有关。但其是否是维基解密披露信息的全部来源，其掌握的相关信息是否为自己窃得，其真实身份是否就是来自罗马尼亚的的黑客，目前都还不得而知。

2） Fancy Bear 与 Cozy Bear

尽管已经有 Guccifer 2.0 主动站出来宣称对 DNC 被黑及邮件泄密事件负责，但美国的安全厂商则并不认可这一说法。包括 CrowdStrike、FireEye 在内的多个美国安全厂商陆续发表报告，公开指责是俄罗斯黑客组织 Fancy Bear 和 Cozy Bear 攻击了美国民主党全国委员会，同时还窃取了有关共和党总统候选人特朗普的资料，意图干扰美国大选。

Fancy Bear 又名 Sofacy、APT28、Sednit、Pawn Storm、Strontium，Cozy Bear 又名 Cozy Duke、APT29，这两个黑客组织的相关攻击活动已持续数年，至今仍然非常活跃，并被公认为是由俄罗斯国家支持的黑客组织。

安全厂商的观点也有一定的依据。例如，研究人员通过大量关联分析发现：用于注册 Bitly 短网址服务账号的域名实际上是一个被 Fancy Bear 控制的域名。

尽管目前美国的情报机构、安全厂商大多都将 DNC 邮件泄密事件的攻击者背景指向了俄罗斯，但俄罗斯方面对此一直予以坚决的否认。也有很多安全专家和国际问题专家认为，这有可能是美俄之间打的一场口水仗，真相仍然不得而知。

有趣的是，宣称掌握了大量与美国总统大选有关机密材料的维基解密创始人朱利安 阿桑奇在谈到情报来源时，既没有认定俄罗斯就是幕后黑手，也没有正面否决。而更有趣的是，美国新任总统特朗普也不认为俄罗斯应该为此负责。

而事实上，我们也相信国与国之间的网络战争从未停歇。正如 2016 年 6 月北约国家缔结的联合协议一样，网络空间已升级为第五空间，网络攻击将被视为战争。

（四） 美国情报机构的最新调查

本小节中主要内容引述或摘编自网络媒体。敬请参考。

1） 1 月 6 日的解密报告

根据 CNN 网站报道，2017 年 1 月 6 日，美国情报机构（US Intelligence Community）解密了一份受奥巴马委托制作报告。报告称，俄罗斯总统普京

曾经下令发起“影响攻势”，损害希拉里的选情，助选特朗普。

这份报告指出，俄罗斯的干涉手段包括：侵入民主党团体和个人的电脑，比如希拉里的竞选主席波德斯塔（John Podesta）；通过第三方平台发布信息，比如维基解密。报告称，这是俄罗斯长期破坏“美国领导的自由民主秩序”的“明显升级”。其主要目标是破坏公众对美国民主程序的信任，诋毁国务卿克林顿（希拉里），损坏她的候选资格，降低其当选概率。报告同时认为，普京和俄罗斯政府明显偏爱当选总统特朗普。

报告还称，俄罗斯干涉 2016 年美国大选的努力，是莫斯科长期试图破坏美国领导的自由民主秩序的最新证明，但相比以前的行动相比，这次更直接、活跃度更高、范围更广。

美国情报部门官员还“高度相信”，俄罗斯情报部门格勒乌（GRU）在公开的黑客行动中盗取了美国受害人的信息，然后通过 Guccifer 2.0 persona、DCLeaks.com 和维基解密来公布这些数据。

报告指出，俄罗斯的干涉手段不限于黑客行为以及在大选期间公布劲爆的私人信息。俄罗斯的国家媒体以及被收买的社交媒体用户也在推波助澜。

比如，今日俄罗斯和卫星新闻网等俄罗斯国家媒体，把特朗普描绘成“美国传统媒体不公平报道的打击目标”，此外，俄罗斯的宣传官员也把特朗普称为“美国政治利益集团的受害者”。与此同时，今日俄罗斯对国务卿希拉里发布了持续的负面报道，集中在她被泄露的邮件上，并指责她贪腐、身心健康都有问题，还和伊斯兰极端分子有关联。

针对这份报告，当地时间 1 月 6 日，特朗普在纽约与美国政府情报机构领导人会晤，他在会晤后发表的声明中表示，网络攻击对美国大选结果没有造成影响。

特朗普在声明中说，他与情报机构领导人进行了建设性会晤和对话，他对情报机构的工作抱有极大的敬意。虽然俄罗斯等国持续试图侵入包括民主党全国委员会在内的美国政府机构、企业和组织的网络基础设施，但网络攻击对美国大选结果没有造成影响，美国的投票机没有遭到破坏。特朗普说，黑客也试图侵入美国共和党全国委员会，但该委员会拥有强大的网络防御，黑客未能取得成功。

特朗普强调，美国需要积极应对和阻止网络攻击，他将任命一支网络安全团队，责成该团队在其就职后 90 天内提交具体的网络安全计划，保护美国的安全将是他作为总统的首要任务。

2） 关于报告的补充报告

不过，事情并未就此结束。据 CNN1 月 10 日报道，在上一周，四名美国情报机构高官向现任总统奥巴马和候任总统特朗普提交了秘密报告。这份

由 3 名 CNN 资深记者以及水门案资深调查记者卡尔·伯恩斯坦联名的报告中，引述了多名不具名美国官员的说法，主要情报来源则是前英国情报人员。

这份两页的秘密报告实际上是美国关于“俄干涉美大选”调查报告的补充，由美国国家情报局局长克拉珀、联邦调查局局长科米、中央情报局局长布伦南、国家安全局局长罗杰斯联名提交。目前只递交给了奥巴马、特朗普和一些高层立法者。

这两页文件其实只是一份 35 页报告的摘要。文件指出，俄方已培养、帮助、支持特朗普至少五年时间。CNN 还称，目前联邦调查局正在核查情报的真实性、准确性和一些关于特朗普的具体细节。

爆炸性消息一出，美国各家媒体纷纷跟进，网络媒体 BuzzFeed 更是直接公开了这份 35 页的秘密报告。

文件认为，在起码从五年前开始，俄罗斯就留意到特朗普，并试图对他施加影响。俄罗斯的办法是，利用特朗普自己的商业和环球小姐选举事务到俄罗斯出访时，刻意为他提供好的商业协议条件，并用各种手段招待他。

例如，俄罗斯向特朗普提供了许多利润丰厚的房地产生意，以便继续培养特朗普，不过到目前为止都被特朗普拒绝了。但是，特朗普和他的核心团队已经接受了克里姆林宫定期提供的情报，包括民主党以及他的其他政敌。

特朗普为何要接受普京的“培养”呢？文件显示，这可能是因为特朗普受到了“威胁”。根据这份情报提供的信息：俄罗斯手中持有特朗普 2013 年到莫斯科出差时，在酒店召妓的录像。

目前，这份文件的真实性还未经核实。除了特朗普对报告的内容极力否认外，俄罗斯方面也出面辟谣。俄罗斯总统新闻秘书佩斯科夫表示，有关俄方掌握特朗普不利信息的消息纯属捏造。

也有分析指出，这份文件的其中一些指控似乎已经被证明站不住脚。例如，特朗普被指曾在布拉格与俄罗斯特工见面。但特朗普的律师迈克尔•科恩在推特上写道，特朗普从来没有去过布拉格。

二、 方程式组织工具泄漏事件

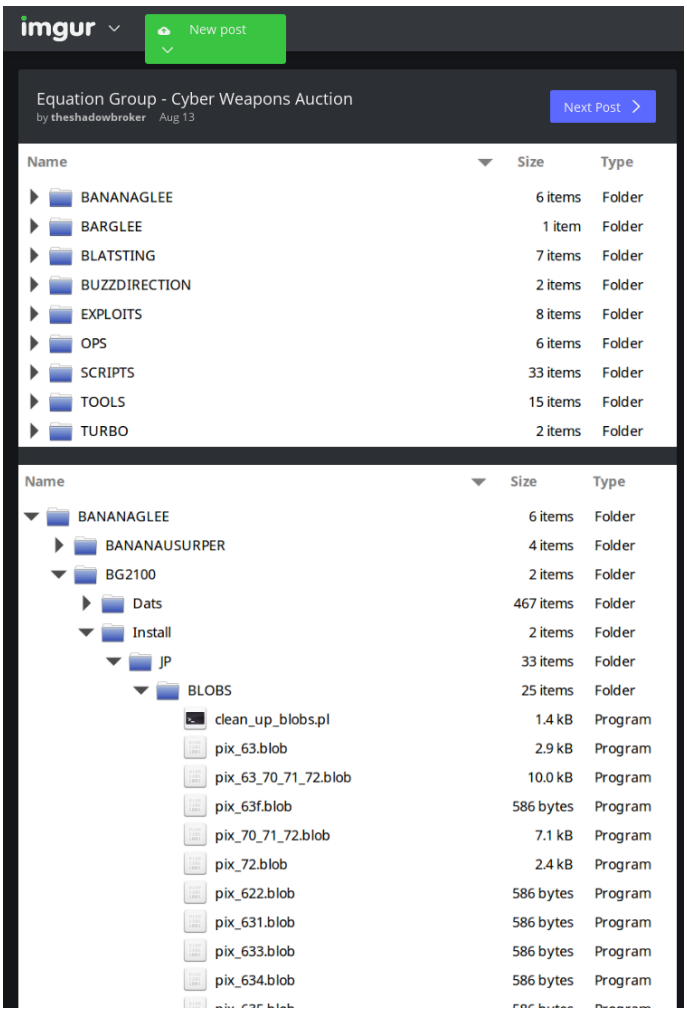
Equation Group（方程式组织）是由卡巴斯基实验室于 2015 年披露的网络攻击幕后组织。该组织在攻击复杂性和攻击技巧方面超越了历史上所有已知的网络攻击组织，并且掌握大量 0day 漏洞，是一个十分先进而隐秘的计算机间谍活动团体。该团体的恶意软件至少已感染 42 个国家的 500 台电脑，受害者涉及各国政府、军工、能源以及重要基础设施建设领域等。幕后组织与此前发现的火焰病毒（Flame）及震网病毒（Stuxnet）的幕后组织存在联系，很可能与美国国安局 NSA（NationalSecurityAgency）的间谍活动有关。

然而，2016 年，一个自称是“theshadowbrokers”（影子经纪人）的黑客组织宣称获得了方程式组织的网络武器，并公开在网上进行拍卖。根据影子经纪人泄漏的相关信息分析，中国很有可能是方程式组织的首要攻击目标。

1） 方程式组织拍卖邀请函

2016 年 8 月 13 日，一个自称为“theshadowbrokers”（影子经纪人）的黑客组织在 github 网站发布了名为“theshadowbrokers/EQGRP-AUCTION”（影子经纪人，方程式组织拍卖邀请函）的消息，并同时在 tumblr，imgur 网站发布了截图认证。而该 github 页面在 15 日被官方删除。

在邀请函中，影子经纪人声称自己攻破了方程式组织的网络系统并获得了 Equation Group 的网络武器。为了证明自己的说法，影子经纪人还同时在声明中公开了一份证明文件，该文件大部分的代码由 python 编写，后被证明包含针对思科、Juniper、Fortinet 和天融信等的多个厂商的防火墙产品的漏洞利用程序。同时影子经纪人声称拍卖的文件 eqgrp_auction_file 比 stuxnet（震网病毒）更好，比免费提供的文件更好，并且给出了拍卖的规则。



根据拍卖规则，有意购买者需要向指定的比特币地址转入比特币，转入比特币最多的人或组织就可以获得拍卖的文件。而如果该地址收集到了 100 万个比特币（约合 10 亿美元），影子经纪人将会向所有人公开拍卖文件的内容。上图就是影子经纪人泄漏的 eqgrp 部分网络军火工具截图。

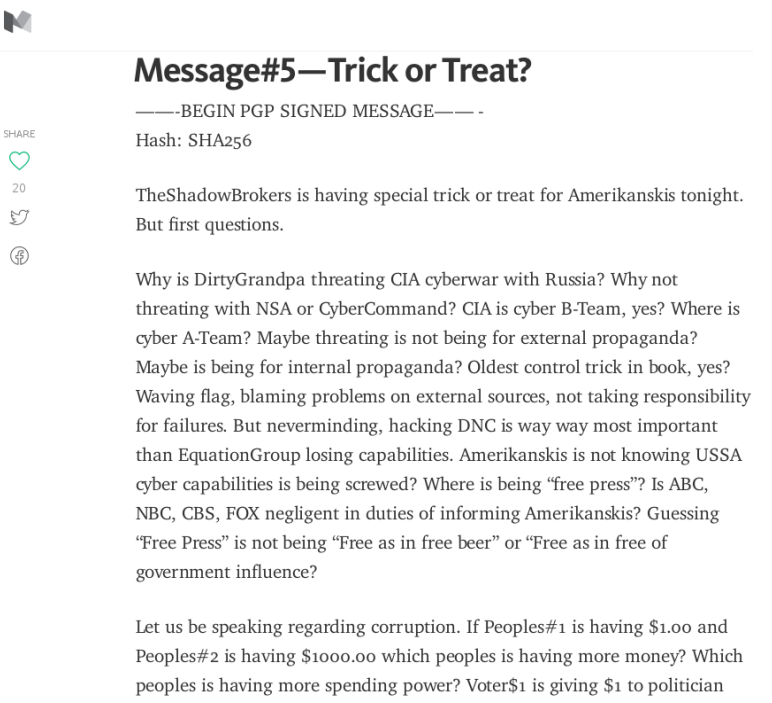
经过安全研究人员确认，影子经纪人泄露的文件，包含多个针对防火墙的 0day 漏洞，影响非常大。Kaspersky 通过对泄露代码中加密算法的对比，认为影子经纪人泄露的代码和方程式组织使用的恶意程序高度一致。

8 月 19 日，前 NSA 员工爱德华·斯诺登公开了六份 NSA 文档，证明了影子经纪人公开的文件与 NSA 的关系。

影子经纪人泄露 NSA 网络武器事件发生后，FBI 逮捕了一名美国政府承包商哈罗德·托马斯·马丁三世（Harold Thomas Martin III）。此人在被逮捕时，被发现其存储了约 50TB 的机密文件。而另有知情人士向路透社表示，当局认为可能是该公司的某位操作员不小心将代码留在了远程电脑上，因此才会被俄罗斯黑客发现。

2） 万圣节前再次发声

正当部分媒体认为马丁就是泄露 NSA 机密文件的影子经纪人时，万圣节之前，影子经纪人再次在网站 medium.com 发声（见下图），并且再次泄露一批机密文件。该文件包含众多的域名和 IP 信息，据称是方程式组织黑掉并且控制的服务器信息，其中包含代号为 “intonation” 和“pitchimpair”的两个文件夹，里面包含有域名和 IP 信息，并且还有配置单的 key 信息。



SHARE
20

Message#5—Trick or Treat?

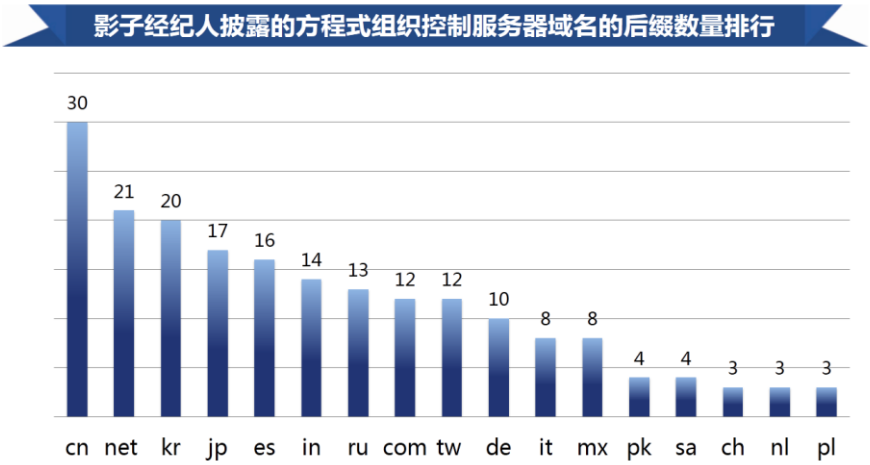
——-BEGIN PGP SIGNED MESSAGE—— -
Hash: SHA256

TheShadowBrokers is having special trick or treat for Amerikanskis tonight. But first questions.

Why is DirtyGrandpa threating CIA cyberwar with Russia? Why not threating with NSA or CyberCommand? CIA is cyber B-Team, yes? Where is cyber A-Team? Maybe threating is not being for external propaganda? Maybe is being for internal propaganda? Oldest control trick in book, yes? Waving flag, blaming problems on external sources, not taking responsibility for failures. But neverminding, hacking DNC is way way most important than EquationGroup losing capabilities. Amerikanskis is not knowing USSA cyber capabilities is being screwed? Where is being “free press”? Is ABC, NBC, CBS, FOX negligent in duties of informing Amerikanskis? Guessing “Free Press” is not being “Free as in free beer” or “Free as in free of government influence?

Let us be speaking regarding corruption. If Peoples#1 is having $1.00 and Peoples#2 is having $1000.00 which peoples is having more money? Which peoples is having more spending power? Voter$1 is giving $1 to politician

影子经纪人披露的这份文件还向我们传递了一个重要的信息，即：从被攻击的服务器域名后缀统计来看，“.cn”出现的次数最多，这表明中国可能是方程式组织攻击的首要目标。



而从具体的域名信息来看，国内的顶尖的大学是方程式组织主要的攻击目标，清华大学，国防科技大学，北京邮电大学，北京工商大学，西安电子科技大学，郑州大学，兰州大学等都有上榜。

此外，如中国原子能科学研究院，西北核技术研究所，杭州市经济与信息化委员会，中国科学院紫金山天文台等科研机构，如华为等商业企业也在其中。

影子经纪人称，这些被黑的服务器实际上只是跳板机，方程式组织通过这些机器作为跳板大量入侵其它机器和窃取数据。

3） Zeronet 上的直接销售

可能是由于前期的拍卖方式叫价过高没有成功，12 月 15 日，影子经纪人又在 Zeronet 上发布了新的消息。ZeroNet 是一个以 P2P 用户为基础而构成的类互联网的分布式网络。影子经纪人声称要以直销模式出售 NSA 的工具，并公开了 auction_file（拍卖文件）的目录和标价。

下图为影子经纪人发布的各文件包拆分零售的价格情况。其中，标价 1BTC （比特币）的是 Linux 下的工具，标价 10BTC 的是 exploit 分类和部分的 implant 分类，标价 100BTC 的主要是 Linux 下的植入体 implant 分类和 RAT 分类，而完整的 auction_file 包标价 1000 BTC。按照目前的比特币市价约和 100 万美元。

从影子经纪人本次泄露的文件列表来看，相关文件应该还是属于 Firewall（防火墙）的目录，而 Firewall 目录对于庞大的 NSA 网络军火库来说，还只是冰山一角。

THESHADOWBROKERS ON ZERONET

YOU LIKE. YOU EMAIL. YOU BUY.

Message#6

Download Screenshots (sig)

Name	Type	BTC
auction_file	everything	1,000.0
bs	unknown	10.0
catflap	unknown	10.0
charms	implant	100.0
common	unknown	10.0
curses	implant	100.0
dampcrowd	unknown	10.0
dewdrop	implant	100.0
dubmoat	trojan	10.0
earlyshovel	exploit	10.0
ebb	exploit	10.0
eggbasket	exploit	10.0
eh	unknown	10.0
elatedmonkey	exploit	10.0
eldestmyriad	exploit	10.0
electricslide	exploit	10.0
eleganteagle	exploit	10.0
elgingamble	exploit	10.0
endlessdonut	exploit	10.0
enemyrun	implant	100.0
englandboggy	exploit	10.0
envisioncollision	unknown	10.0
envoytomato	unknown	10.0
epichero	exploit	10.0
es	exploit	10.0
esna	exploit	10.0
estopmoonlit	exploit	10.0
evolvingstrategy	unknown	10.0
ewok	unknown	10.0
exactchange	exploit	10.0
expoxyresin	unknown	10.0
exze	unknown	10.0
forkpty	tool	1.0

影子经纪人的故事还并没有完结，该组织留下的比特币拍卖地址截至 12 月 8 日也仅仅收到约 2 个比特币的付款。整个事件中影子经纪人做了很多次尝试，从拍卖，众筹，再到直销模式的黑色星期五大减价。但是否真的会有人购买还不得而知。

影子经纪人泄漏方程式组织工具事件再次引发了人们对网络空间战争深刻影响全球地缘政治的担忧。类似于方程式组织这样的，有强大国家支持背景的，网络空间战争的顶级参与者，已经使全球各国政府、科研、军事和商业机构面临巨大的威胁。而中国则很可能是众多网络空间战争顶级参与者的主要攻击目标。

第六章　危险的网络军火交易

有战争的地方就会有人贩卖军火。APT 是网络空间中的战争，自然也有人在这里贩卖军火。网络战争中使用的军火主要分为两类：一类是专用木马程序及配套的控制工具，另一类是安全漏洞和漏洞的利用工具。

2016 年，在网络空间战争愈演愈烈的大环境下，一大批专业网络军火商和地下黑客军火商走上了历史舞台。但不论怎样说，军火的交易都是危险的，不论这个军火是现实生活中的，还是网络空间里的。特别是当这些网络军火商的电脑或系统遭到入侵时，其可能泄漏的大量攻击代码，往往会使某些军用技术民用化，从而造成普通网民的安全灾难。

本次报告为读者介绍三个全球知名的网络军火商，并通过“三叉戟漏洞”事件来介绍一个网络军火商参与 APT 攻击的典型事件。

一、　网络军火商

网络军火商是一群特殊的利益团体和组织，他们往往掌握着网络世界最前沿、最先进的技术，与本国政府或区域性政治团体之间有着紧密的联系。一般来说，网络军火商会出售计算机程序、软件或设备给政府，成为驰骋于网络战场上的“作战利器”；更多时候，他们会和政府签订协议，政府直接将情报搜集项目如监控监听外包给各网络军火商。

下面就来介绍三个全球知名的专业网络军火商。

（一）　Hacking Team

意大利的 Hacking Team 2003 年就已涉足网络军火市场，是一家以协助政府监视公民而“闻名于世”公司，2015 年 7 月 5 日，该公司的 Twitter 帐号遭到不明人士入侵，攻击者丑化了其 Logo、简介，并通过被害者的 Twitter 发布了一条关于 Hacking Team 数据泄露的通告，爆出了 400GB 的猛料，引起了安全界的轩然大波。下图即是 Hacking Team 的 Twitter 帐号被黑后，攻击者留言的截图。

（二）　Gamma

声名在外的网络军火商还包括英国的老牌网络军火商 Gamma 集团。该机构研发的恶意程序 FinFisher（或 FinSpy）曾经因为参与在巴林地区、埃及等国家和地区的监听事件而备受舆论指责。2013 年和 2014 年，Gamma 两度遭到黑客入侵，大量内部资料外泄，这家老牌公司再次被推到了舆论的风口浪尖，但这并不能阻止 Gamma 在这场没有硝烟的战争继续赚取巨额红利。

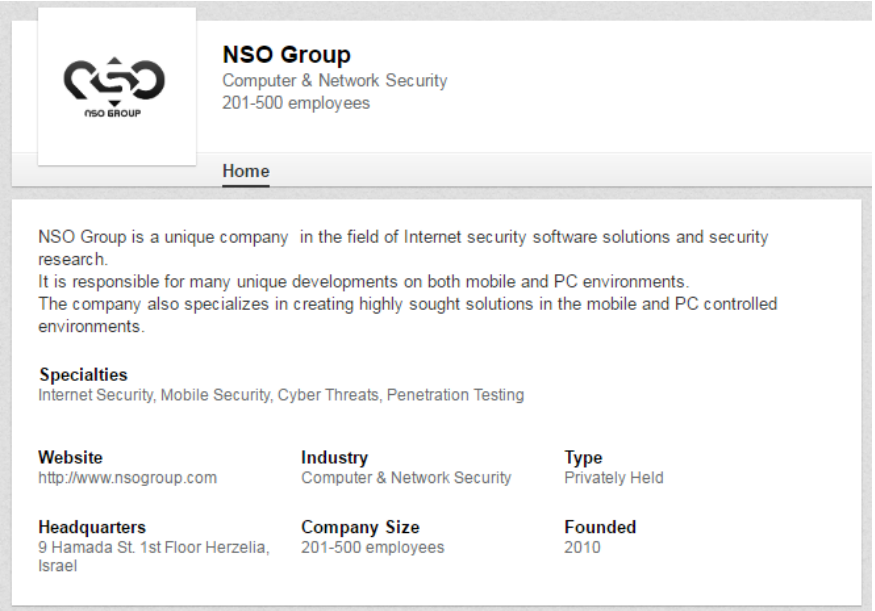
下图就是 Gamma 研发的一款黑客工具.

（三） NSO

说到商业化的网络武器，还不得不提以色列这个国家，以及以色列数字间谍工具开发公司之一的 NSO 公司。

以色列被公认拥有全世界最先进的监控技术。英国非政府组织隐私国际（Privacy International）曾发布报告称，总部设在以色列的监控公司总数多达 27 家，按人均计算，以色列每 10 万人就有 0.33 家监控公司。

NSO Group 是以色列数十家数字间谍工具开发公司之一，是网络战争领域的领导者，它们的产品可追踪智能手机上的任何活动。他们主要为世界各国政府和执法机构提供服务。自从 2010 年成立至今，NSO Group 始终保持着低调。有关 NSO Group 的资料很少，他们的创始人很少对媒体讲话，公司也没有网站。其主要产品是一款名为 Pegaus 的间谍软件。



二、 三叉戟漏洞事件

网络军火在实战中是如何被使用的？2016 年 8 月曝出的 iOS 三叉戟漏洞就为我们呈现了一场精彩的好戏。

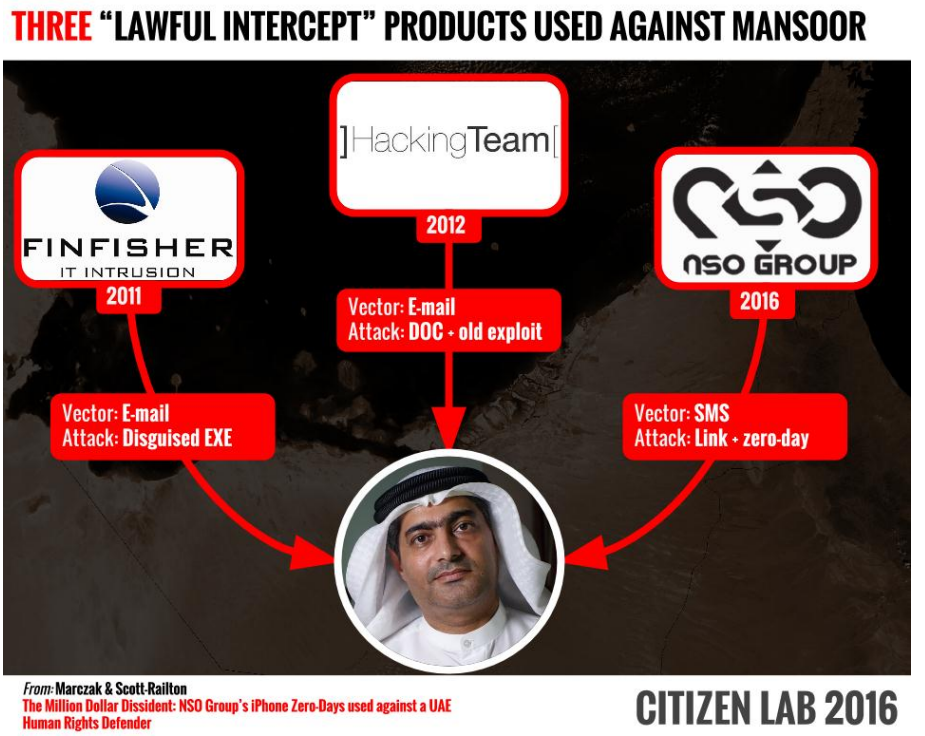
2016 年 8 月 25 日，阿联酋一位著名人权活动家 Ahmed Mansoor 的 iPhone 手机上收到 2 条含有链接的短信，信息显示，该链接将透露阿联酋监狱受虐囚犯的“秘密”。下图就是 Ahmed 收到的两条短信截图。

不过，这位斗争经验丰富的“战士”并没有立即点开短信中的连接。事实上，Ahmed 自己经常成为政府使用恶意软件针对的目标，每次他们得到新的间谍软件，都会在他身上进行尝试。Ahmed 担心这两条短信中也有可能“暗藏杀机”，于是在第一时间将这两条短信报告给了 Citizenlab 的安全研究人员。

Citizenlab 和 Lookout 的安全研究人员对这两条短信中的链接进行研究后也是大吃一惊。研究人员发现，一旦 Ahmed 点击了这两个链接，不需要任何具体操作，手机就会植入由以色列 NSO 公司研发的手机监控软件 Pegasus。攻击者可以通过 Pegasus 远程控制 Ahmed 的手机，并且可以在 Ahmed 完全不知情的情况下，窃取手机上的短信、邮件、通话记录、电话录音、存储的密码等隐私数据，还能监听并窃取 Whatsapp、微信等社交软件的聊天信息。

这两条神器的链接之所以会有如此强大能力，主要是由于 Pegasus 利用了苹果手机 iOS 操作系统中的 3 个 0-day 漏洞，这三个漏洞也就是在安全圈名声大噪的“三叉戟漏洞”。漏洞消息的公布迫使苹果公司紧急发布了安全更新。

这也是苹果史上第一次公开披露的针对 iOS 的 APT0day 攻击。0day 漏洞本就罕见，一次发现数个这样的漏洞更是罕见。正是鉴于这三个漏洞的危害特别严重，苹果才在短时间内火线修复漏洞。



由于 0day 漏洞罕见，能够发现并利用这种系统安全漏洞编写攻击软件，在网络间谍领域意味着“丰厚利润”。据美联社报道，2015 年 11 月，曾有人出价 100 万美元购买这类间谍软件。

而此次事件“三叉戟漏洞”也暴露出网络军火或网络武器使用的一个显著弊端，即如果武器投放失效，很有可能就会暴露武器的存在，并直接导致该武器永久失效。Ahmed 本人并非是一名网络安全专家，而仅仅是一名网络

安全意识很强的“普通用户”，但 Ahmed 还是很轻易的就让价值上百万美元的网络武器“三叉戟漏洞”永远报废。

下表给出“三叉戟漏洞”漏洞的漏洞编号和简介。

漏洞编号	漏洞简介
CVE-2016-4655	该漏洞将有可能导致应用程序泄漏系统内核内存中的数据
CVE-2016-4656	该漏洞将有可能导致应用程序以内核权限来执行任意代码
CVE-2016-4657	访问了精心设计的恶意网站之后，攻击者或可利用该漏洞实现任意代码执行

表 9　三叉戟漏洞简介

第七章　部分 APT 组织与行动

一、　索伦之眼（APT-C-16）

2016 年度的 APT 事件中，索伦之眼行动可谓独树一帜。其展现出的强大技术实力令人叹为观止——整个攻击过程高度隐蔽，目标针对性极强，且针对不同的目标定制开发不同的恶意程序，而整个过程却不重复使用相关资源。纵观当下的 APT 事件，索伦之眼行动恶意代码实现技术的复杂度，与之前的方程式（Equation）组织相比毫不逊色，其幕后组织的综合能力不亚于震网（Stuxnet）、火焰（Flame）等知名 APT 组织。

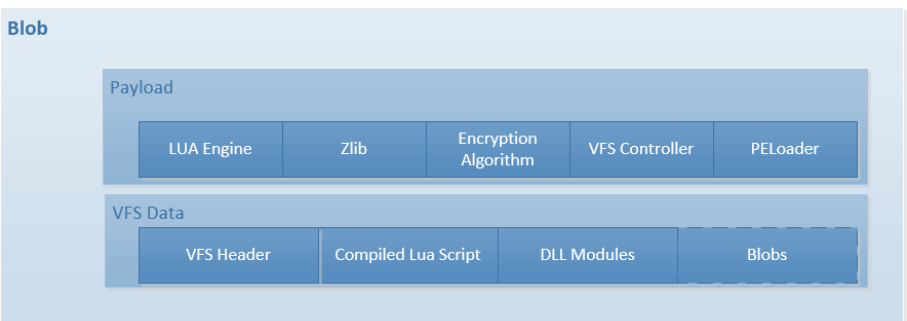
下面来逐项分析索伦之眼的技术特点。

1） 高度模块化的定制平台

索伦攻击行动中所采用的恶意程序适用于 Microsoft Windows x64 和 x86 平台。索伦攻击平台将各种功能都封装成为模块，使得功能高度组件化，并且能够利用多种方式进行传输，例如管道、各种通讯协议，或者以单独文件的方式将 Shellcode 写入注册表项中。所有的模块都使用了强加密算法并且进行压缩，减小了文件体积并提高了传输过程中的隐蔽性。模块化使索伦之眼的扩展性得到了空前的提高，攻击者可以根据目标的实际情况进行快速的功能定制。

2） 无文件实体技术

索伦攻击平台采用了 EVFS（加密虚拟文件系统）对攻击模块进行管理。EVFS 采用了高强度加密算法并使用 Zlib 进行压缩，每个 VFS 文件都拥有独立的密钥。这使得对应的攻击组件不存在可执行文件实体，只有当组件被调用时才会出现在内存中。这种攻击方式极大的增强了数据的安全和隐蔽性，同时，分析人员在获取完整载荷的过程中，需要获取全部的 EVFS 文件碎片，分析加密算法并且获取其中的解密密钥，使得分析难度大大增加。下图是索伦之眼的 VFS 结构示意图。

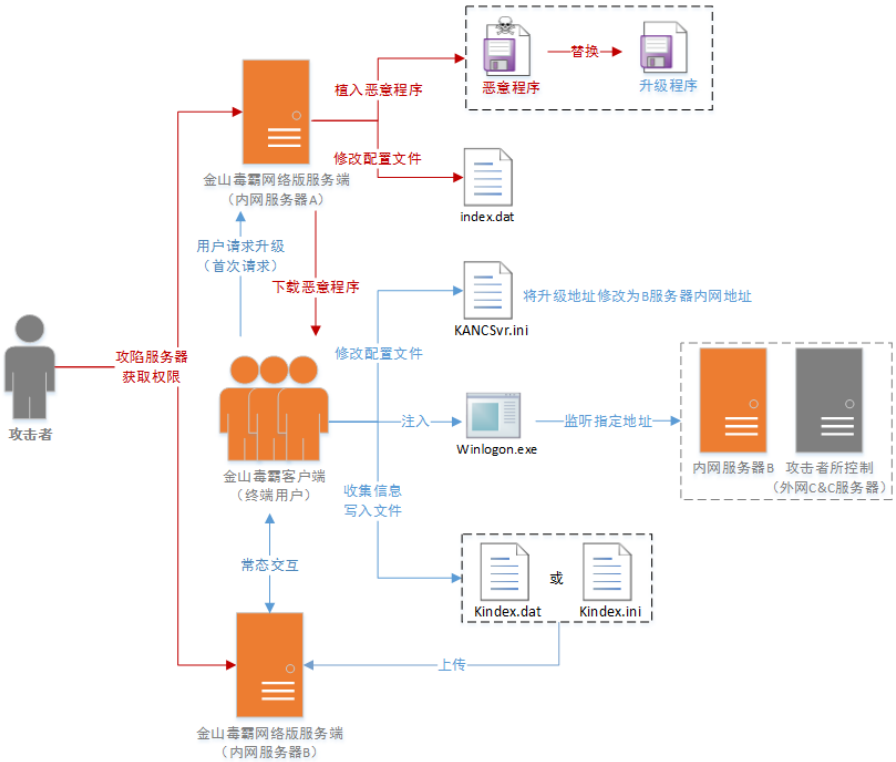


3） 定制化的 LUA 引擎

索伦之眼在其内部使用了自我定制的 LUA 引擎，平台的核心模块通过执行释放出的 Lua 预编译脚本来调用其他子模块实现具体功能，分析人员需要解析整个 Lua 预编译脚本，这无疑是雪上加霜。

4） 针对目标环境定制的内网横向移动

根据攻击目标的不同，实现了不同手段的横向移动方式——可以利用 Windows 域，也可以劫持金山毒霸升级程序，后者突出说明了索伦具有极强的针对性，对目标进行了长期的渗透和侦察活动。下图给出了索伦之眼通过劫持金山毒霸进行横向移动的过程



5） 隔离网络数据窃取

针对隔离网络，索伦之眼会通过特殊的格式化减小 USB 磁盘分区的大小从而在磁盘末端产生了系统无法识别的保留区域，进而通过 U 盘进行隔离网络的数据窃取。

6） 高强度加密的通讯方式

索伦之眼攻击行动中使用了一系列复杂的方式来隐藏数据窃取、指令接收和模块下载等行为。除了常见的通信方式和内部代理外，索伦之眼还用到了一些较为罕见的技术，例如 DNS 隧道协议或者邮件协议进行通讯。其对

高强度的加密方式情有独钟，模块和网络通信中大量使用了例如 RC6, RC5, RC4, AES, Salsa20 等算法。

总体来讲，索伦之眼的技术实力是 2016 年度被全球所有机构披露的 APT 组织中最强的（没有之一），其组合使用了一系列复杂高难度的技术对目标实施了隐蔽性极强的攻击，活跃时间横跨 2011 至 2016 年，整个过程展现出来的技术特性，譬如高度模块化平台、加密虚拟文件系统、无文件实体等技术等，在历次高水准的 APT 攻击中都有体现。

二、 APT28（APT-C-20）

APT28（APT-C-20），又称 Pawn Storm、Sofacy、Sednit、Fancy Bear 和 Strontium。APT28 组织被怀疑幕后和俄罗斯政府有关，该组织相关攻击时间最早可以追溯到 2007 年。其主要目标包括国防工业、军队、政府组织和媒体。期间使用了大量 0day 漏洞，相关恶意代码除了针对 Windows、Linux 等 PC 操作系统，还会针对苹果 iOS 等移动设备操作系统。

该组织早前也曾被怀疑与北大西洋公约组织网络攻击事件有关。APT28 组织在 2015 年第一季度有大量的活动，用于攻击北约成员国和欧洲、亚洲、中东等地区国家的政府。目前有许多安全厂商怀疑其与俄罗斯政府有关，而早前也曾被怀疑秘密调查 MH17 事件。从 2016 年开始该组织最新的目标瞄准了土耳其高级官员。

2016 年 12 月披露的数据取证的证据表明，该黑客组织可能帮助武装亲俄分裂分子追踪乌克兰部队的动向，曾使乌克兰炮兵部队损失一半以上的武器。2014 年底至 2016 年，该组织将 X-Agent 植入程序植入合法 Android 应用程序，并秘密在乌克兰军事论坛散布。亲俄分裂分子在该恶意软件的支持下，能获得乌克兰炮兵部队的位置信息。此事件表明，该组织在移动恶意软件开发能力方面，已经从 iOS 植入程序向 Android 设备扩展。

近期，在针对美国大选过程中民主党委员会（DNC）邮箱遭到网络攻击一事的调查中，众多迹象和证据都将矛头指向了 APT 28，该组织可能在 2016 年 4 月就入侵了 DNC 邮件系统。

无独有偶，2016 年 12 月，德国情报机构联邦宪法保卫局(BfV)发现了大量疑似俄罗斯黑客组织 APT 28 的网络攻击活动，攻击多是针对德国政府官员、国会议员和各民主党派人士。黑客通过鱼叉邮件传播恶意软件，相关样本与入侵美国民主党全国委员会系统的恶意软件相同，而攻击时间也正值德国大选前后。

三、 摩诃草（APT-C-09）

摩诃草组织（APT-C-09），又称 HangOver、VICEROY TIGER、The

Dropping Elephant、Patchwork，是一个来自于南亚地区的境外 APT 组织。该组织已持续活跃了 7 年。摩诃草组织最早由 Norman 安全公司于 2013 年曝光，随后又有其他安全厂商持续追踪并披露该组织的最新活动，但该组织并未由于相关攻击行动被曝光而停止对相关目标的攻击，相反从 2015 年开始更加活跃。

摩诃草组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到 2009 年 11 月，至今还非常活跃。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，其中以科研教育领域为主。

从 2009 年至今该组织针对不同国家和领域至少发动了 3 次攻击行动和 1 次疑似攻击行动，期间使用了大量漏洞，其中至少包括一次 0day 漏洞攻击。该组织使用的恶意代码非常繁杂，恶意代码数量超过了上千个。载荷投递的方式，主要是以鱼叉邮件进行恶意代码的传播，另外会涉及少量水坑攻击。在最近一次攻击行动中，即时通讯工具和社交网络也成为了主要的恶意代码投递途径。进一步还会使用钓鱼网站进行社会工程学攻击。

该组织主要针对 Windows 系统进行攻击，同时也会针对 Mac OS 系统进行攻击，从 2015 年开始还会针对 Android 系统的移动设备进行攻击。

第八章　APT 攻击的特点与趋势

结合境内网络安全监测与全球 APT 前沿研究成果，360 威胁情报中心对 APT 攻击的特点与趋势总结如下。

一、　网络空间已经成为大国博弈的新战场

如果说震网病毒事件、乌克兰停电事件表现出了“弱小国家”的基础设施在面临网络空间非常规打击时的脆弱性，那么 2016 年 DNC 邮件泄漏直接影响美国大选结果的事件，则充分说明：即便是当今世界唯一的超级大国，在网络攻击面前也同样脆弱，其政治、经济、社会心态等各个方面都有可能受到网络攻击的深远影响。

根据媒体披露的美国情报机构报告的说法，俄罗斯实际上是综合使用了网络攻击、媒体传播、政治渗透、商业影响等多种手法，系统性的干预了美国大选，而且其正真的目的还不仅仅是影响一次美国大选的结果，而是要影响人们对美国政治体制及自有民主的信心。尽管俄罗斯方面对此予以坚决的否认，但是这次 “干预”行动本身的成功，使我们有理由相信：未来几年内，类似的，将网络攻击手段与其他手段相结合，对目标国家的政治、经济、文化进行综合性影响 APT 行动一定会不断的增加。

从另外一个角度看，公开其他国家对本国的网络攻击事件，也可以成为本国政府对其他国家政府施加政治压力，以及进行政治、军事谈判的砝码。美俄两国，特别是美国，非常善于通过公开威胁事件及情报共享等方式，提高国内机构与企业的整体安全防护水平，同时借此对其他国家施加政治压力。

综合来看，无论是发动 APT 攻击，还是披露 APT 攻击，均已成为了现代国际关系中，大国政治与战略博弈的重要棋子。而整个网络空间就是大国战略博弈的新战场。

二、　针对基础设施的破坏性攻击日益活跃

自从震网病毒被发现至今，针对基础设施进行破坏的网络攻击活动就一直没有停止。但是，真正有较大影响力的基础设施网络攻击事件其实一直并不太常见。更多的 APT 组织还是把窃取机密信息作为首要攻击目标。

不过，2015 末-2016 年以来，一系列针对基础设施的破坏性攻击被曝光，而且尤以工业系统和金融系统遭受的攻击最为严重：乌克兰停电事件，沙特 Shamoon2.0 事件，孟加拉央行被窃事件，台湾第一银行及泰国邮政储蓄银行 ATM 被窃事件，都属于非常典型的破坏性攻击。也正是由于这些破坏性攻击的存在，才使 APT 攻击更加引人关注。

事实上，随着工业互联网及“互联网+”的快速发展，互联网技术的应用正在快速的从生活领域过渡到生产领域。这也就必然使更多联网的生产系统和基础设施面临巨大的网络安全威胁。而特别让人担忧的是，很多领域的基础设施和生产系统的网络安全体系建设目前还基本为 0，大量已知的安全漏洞长期得不到有效的修复，系统严重缺乏升级、更新等运维管理。这也就使得很多基础设施和生产系统的安全隐患要远比终端设备大得多。从某种角度看，很多联网的基础设施系统就是暴露在互联网上的活靶子。

预计在未来几年中，针对能源、交通、制造、金融、通信等领域的基础设的破坏性攻击仍将持续加剧，安全生产事故，甚至是安全生产灾难，随时都有可能大规模爆发。

三、 针对特定个人的移动端攻击显著增加

2015 年，我们已经截获了很多针对移动终端实施攻击的 APT 样本。而 2016 年，针对移动终端的 APT 攻击显得更加活跃：摩诃草、蔓灵花等针对中国发动攻击的 APT 组织都被发现使用了移动端专用木马程序，其中即有适配安卓系统的，也有适配苹果系统。

2016 年最具影响力的针对移动终端的 APT 攻击非三叉戟漏洞事件莫属。而攻击事件被揭露，主要原因就是被攻击的目标人具有极高的安全意识，收到陌生人发来的可疑短信后，没有点开短信链接，而是直接将短信转交给了安全公司进行审查。

客观而言，移动终端上存储敏感或机密文件的可能性要比 PC 终端小得多。因此，攻击 PC 端的 APT 专用木马也要比攻击移动端的专用木马多得多。但是，移动端也有其特殊的攻击价值，特别是攻击移动端客观上可以实现对设备持有者日常活动的贴身监测，并且能够获取目标人的关系网信息。

从一定意义上讲，针对移动终端设备发动的 APT 攻击，其真正的攻击目标往往即不是是移动设备本身，也不是单纯的几条敏感信息，而是移动设备背后的使用者——即被攻击的目标是人而不是物。三叉戟漏洞事件就是一个最典型的实例。

预计未来几年内，以特定高价值人群或个体为目标的 APT 攻击还会持续增加，而这些特定人群或个体被攻击的主要方式，可能就是他们所使用的智能移动终端设备。而在针对移动终端的 APT 攻击中，社工手法和系统漏洞都将成为攻击者的主要武器。

四、 一带一路与军民融合仍将是攻击焦点

2016 年的全年监测显示：“一带一路”、“军民融合”等战略方向，仍然是众多 APT 组织关注的焦点，相关组织主要包括海莲花、摩诃草、蔓灵花、APT-C-05、APT-C-12、APT-C-17 等。而这一趋势在 2017 年，乃至未来几年都仍将持续。

事实上，如“一带一路”等超大型国家系统工程，往往是多学科，多领域的合作工程，也是众多高新技术集中应用的工程，因此具有很高的攻击价值。同时，一旦这些国家级系统工程涉及到边疆地区建设，沿海工程建设，外交外贸等领域时，又必然会在政治、军事和经济层面引发周边相关国家的关注，从而进一步引发相关国家 APT 组织的攻击活动。

而“军民融合”项目，则是攻击组织窥探军事情报的重要突破口。因为一旦军事技术或项目转为民用，其安防级别往往就会大幅下降，这也就可能给攻击者的窃密活动留出了可乘之机。而反过来，当民用技术转为军用时，通过攻击民用机构，就有可能实现对军事系统的渗透。这就是为什么军民融合项目会特别受到境外 APT 组织关注。所以，军民融合项目，更需要特别注意网络安全建设。

从本质上讲，攻击者对“一带一路”、“军民融合”等大型国家系统工程的关注，事实上是对中国政治、军事以及高新技术情报的关注。而这些大型系统工程，也往往存在很多网络安全的薄弱环节，容易给攻击者以可乘之机。

第九章　APT 攻击的监测与防御

一、　国内能力型厂商严重缺位

2016 年，至少有 19 个美国机构以及多个美国参与的联合研究机构展开了与 APT 相关的安全研究，发布各类 APT 研究报告 50 余篇。而反观国内，能够进行相对独立的 APT 研究的企业及安全机构则屈指可数。在 APT 攻击已经广泛渗透到国内各个领域的今天，国内的能力型厂商依然严重缺位。

（一） 能力型厂商缺位的主要表现

能力型厂商的缺位主要表现在以下几个方面：

1） 普遍缺乏独立发现 APT 事件的能力

目前国内企业针对 APT 的研究绝大大多停留于对国外文件的翻译及对已披露 APT 事件的跟进追踪。从目前已经披露的研究资料来看，仅 360、安天等少数企业有能力发布相对独立的 APT 研究成果。

2） 普遍缺乏攻击溯源及背景研判能力

很多国内机构发布的 APT 相关的研究成果，实际上只是对特定恶意样本的分析报告，明显缺少对攻击过程及攻击者本身特征的分析，而能够研判攻击背景的就更少了。但实际上，如果没有攻击溯源及背景研判的过程，事实上就等于是没有最终确认该恶意程序样本是否真的属于 APT 攻击。

3） 大多只能参考国外报告做应急响应

由于普遍缺乏独立的 APT 发现能力，所以国内安全厂商给企业提供的 APT 防御服务，绝大多数是基于国外相关报告已经披露的信息进行报告和预警，并提交给有关单位或部门。至于后续的检测与防御，基本就是基于公开的 IOC 来进行。这实际上是把 APT 的检测与防御变成了一种纯粹的事件响应，很难做到防患于未然，或防患于初然。

4） 对已知 APT 攻击仍然不能积极响应

与上述几点相比，这一问题更加可怕。但根据 360 威胁情报中心的监测，2016 年，很多已经被披露的 APT 组织（有的甚至是一两年前被披露的），对某些重要机构的攻击仍然十分活跃，并且这些攻击者所使用的木马和 C&C 服务器绝大多数是其他安全机构已经披露的。这种情况表明，为这些受害企业提供安全服务的安全厂商不是严重缺乏责任心，就是严重缺乏基本能力。

（二） 能力型厂商缺位的主要原因

造成国内能力型厂商严重缺位的原因是多方面的，但最最主要的瓶颈是

大数据能力的严重不足，其具体表现在以下几个方面：

1） 历史安全大数据储备能力的不足

历史安全大数据是对 APT 组织进行全面溯源和背景研判的重要依据，但很多传统安全企业以往只关注产品的研发与推广，缺少对安全大数据的系统性收集与管理，储备明显不足，从而导致其在 APT 的发现与研究方面明显缺少基础资料。

2） 本地多维大数据的协同分析与处理能力不足

实践证明，任何静态的防御技术对于 APT 攻击来说都是基本无效的。必须通过对内网系统流量的动态监测，全系统日志的综合分析，联网设备的实时监控，以及不同品类安全产品运维数据的综合分析处理，才有可能在攻击初期对 APT 实现有效的识别与发现。同时，也必须通过多品类安全产品的协同处置，才有可能实现对 APT 攻击的快速响应和有效防御。

但是，目前国内绝大多数安全企业提供的安全产品普遍缺乏数据联动分析能力，同时也严重缺乏多维度数据综合收集与处理的计算能力。安全产品体系普遍缺少一个以大数据技术为核心的“安全大脑”。

3） 云端威胁情报技术的不足

APT 攻击的危害很大，但攻击面往往很小，所以单纯依靠本地数据监测，能够获得的情报仍然十分有限，很难复原攻击全貌。所以，将本地安全大数据与云端威胁情报相结合，就成为检测与发现 APT 的必然选择。

但是，目前国内威胁情报市场的整体发展仍然十分缓慢，能够实现稳定商业运营的威胁情报中心凤毛菱角。

二、 协同联动的纵深防御体系

APT 攻击一般具有针对性强、隐蔽性高、代码复杂度高等特点，这也是很多 APT 攻击能够持续数年而不被发现的主要原因。针对 APT 攻击，传统的安全手段往往应对乏力，我们需要革新传统的安全理念和防护手段，建立全新的技术体系以应对 APT 带来的挑战。

2015-2016 年以来，数据驱动的安全协同已经成为安全产业在应对 APT 攻击方面的技术共识。从技术角度看，针对高级威胁的发现，还需要将多维度检测技术、大数据分析技术和威胁情报技术结合起来。

这里要特别对多维度检测技术加以说明。多维度检测技术是 APT 检测与防御的基础，相关数据主要来自于各种品类的传统安全防护产品。也就是说，各种传统的安全防护技术与防护产品在 APT 攻击的检测与防御中仍将发挥基础性的重要作用，但其核心作用已经从单纯的系统防御，升级为探测

攻击信息的主要情报来源。将不同维度的安全检测结果汇聚到大数据中心进行综合关联分析，就可以实现一加一大于 2 的效果。

从实践角度看，数据驱动的，协同联动的纵深防御体系，大致可以概括如下：

1） 高级威胁的判定

安全厂商协助企业建立轻量级的大数据安全平台，之后汇集企业内部各类安全数据进行关联分析，结合多源头的可机读威胁情报应用，沙箱动态行为发现，以及关联引擎分析等多维度方法，进行高级威胁的判定。

2） 安全威胁的处置

高级威胁判定完成后，还需要进一步联动网关处的 NDR（Network Detection & Response，网络检测与响应）及终端处的 EDR（Endpoint Detection & Response，终端检测与响应）系统进行快速协同联动处置。

附录 1 2016 APT 组织境外研究机构列表

下表给出了 2016 年，境外研究机构发布 APT 研究报告及研究成果的组织机构名单（按所属国家名称拼音首字母及机构名称字母排序）。

所属国家	机构名称	机构性质	报告数量	涉及 APT 组织数
多个国家	Novetta 为首的产业联盟	网络安全厂商	1	1
美国/日本	Trend Micro	网络安全厂商	4	4
美国/以色列/法国	SentinelOne	网络安全厂商	1	1
欧洲	Group IB	网络安全厂商	1	1
俄罗斯	Kaspersky	网络安全厂商	10	14
荷兰	Fox-IT	网络安全厂商	1	1
加拿大	Citizen Lab	安全研究机构	4	2
科威特	Cyberkov	网络安全厂商	1	1
罗马尼亚	Bitdefender	网络安全厂商	1	1
美国	Arbor ASERT	网络安全厂商	1	1
	CrowdStrike	网络安全厂商	4	2
	CyberX	工业安全厂商	1	0
	Cylance	网络安全厂商	1	1
	FBI&DHC	政府机构	1	1
	FireEye	网络安全厂商	4	74
	Forcepoint（原名 Websense）	网络安全厂商	2	2
	Lookout	移动安全厂商	1	1
	Malwarebytes Lab	网络安全厂商	1	1
	McAfee	网络安全厂商	1	1
	Microsoft	网络安全厂商	4	4
	PaloAlto	网络安全厂商	15	11
	Proof point	网络安全厂商	2	2
	Recorded Future	威胁情报厂商	1	1
	Symantec	网络安全厂商	7	7
	ThreatConnect	网络安全厂商	1	1
	Vectra	网络安全厂商	1	1
	Volexity	网络安全厂商	1	1
	Zscaler	云安全平台	1	1
西班牙	ElevenPaths	网络安全厂商	1	0

以色列	ClearSky	网络安全厂商	1	1
	Skycure	网络安全厂商	1	1
英国	Mustafa Al-Bassam	安全专家	1	1
英国	Reuter(路透社)	媒体	3	2
总部设在斯洛伐克-布拉迪斯拉发	ESET	网络安全厂商	3	2
总部位于美国旧金山	Cymmetria	网络安全厂商	1	1
未知	ShadowBrokers（影子经纪人）	黑客组织	1	1

国内关于 APT 组织及 APT 攻击的研究比较有限，相关研究机构主要包括 360 和安天等。

附录 2 报告涉及相关组织机构情况说明

Arbor

网络安全厂商，2015 年被 NetScout 的收购，提供专为企业和电信运营商骨干网路设计的。DDoS 和 APT 威胁防护解决方案，并针对新兴威胁提供全球网路流量情报。

AVAST

捷克杀毒软件公司，全称 AVAST Software a.s. 于 1988 首次发行了杀毒软件 Anti-Virus-Advanced-Set，分成家用用途的免费版本以及企业和专业用户的付费版，在全球拥有数亿用户。

AVG

捷克杀毒软件公司，原名“Grisoft”，2008 年更名为“AVG Technologies CZ, s.r.o.”。同年，AVG 推出的 8.0 版本颠覆杀毒专长的 Anti-Virus 版，另辟网络安全的新途，这一举动也正赶上了 2008 年网络混合威胁浪潮。2016 年 9 月，捷克的另一知名杀毒软件公司 AVAST Software 并购了 AVG Technologies。

CERT-UA

全称 Computer Emergency Response Team of Ukraine，即乌克兰网络应急响应小组。

Cisco

Cisco Systems, Inc. ，美国互联网解决方案提供商，公司成立于 1984 年，其设备和软件产品主要用于连接计算机网络系统。

CItizenLab

加拿大多伦多大学蒙克国际研究中心的公民实验室，是一个跨学科的研究发展机构，由许多计算机专家及学者组成。专门从事扫描互联网以曝光政府资助的间谍软件和网络攻击工作，简单说来，实验室的研究核心是对互联网的开放与安全、对网民的基本人权造成侵害的信息控制——比如政府监控项目和信息过滤系统。

它是一个非营利研究小组，研究的财政支持来自福特基金会，开放社会研究所，加拿大社会科学和人文科学研究理事会，国际发展研究中

心，加拿大的全球安全中心的研究，赛风 Inc.，约翰 D.凯瑟琳 T.麦克阿瑟基金会，加拿大唐尼基金会，沃尔特和邓肯戈登基金会。

CrowdStrike

CrowdStrike, Inc.成立于 2012 年，是一家美国网络安全技术公司，客户遍布全球 170 多个国家，为客户提供终端防护、威胁情报和事件响应服务，曾参与过一系列高级网络攻击的应急响应工作，如索尼影视被黑事件和 DNC 邮件泄露事件等。

DHS

全称 United States Department of Homeland Security，美国国土安全部，为美国政府在 9.11 事件之后设立的一个联邦行政部门，负责国内安全及防止恐怖活动。2002 年，美国总统小布什于 11 月 25 日在白宫签署《2002 年国土安全法》，宣布正式成立。

ESET

世界知名的电脑安全软件公司，创立于 1992 年，由两家私有公司合并而成，总部位于斯洛伐克布拉迪斯拉发，最知名的产品为 NOD32 杀毒软件。

FireEye

成立于 2004 年，是一家公开上市的美国网络安全公司，也是第一家由美国国土安全部颁发认证的网络安全公司，提供用于应对高级网络威胁的自动威胁取证及动态恶意软件防护服务。

ForcePoint

成立于 1994 年，前身是 Websense，2000 年上市，2013 年又被私募股权公司 Vista Equity Partners 收购，2015 年成为 Vista Equity 和国防承包商 Raytheon 合资公司，后改名 ForcePoint，为企业和个人用户提供 PC 端安全软件。

F-Secure

原名 Data Fellows，是世界知名计算机及网络安全提供商。成立于 1988 年，总部设在芬兰的赫尔辛基。该公司发行的同名产品 F-Secure（芬安全）

为一款防毒软件，支持 22 种语言，在美国、法国、德国、瑞典、英国、日本有其分公司，与之相关的合作伙伴总数超过 170 家。

Gamma Group

成立于 1990 年，总部位于英国，主要政府机构提供监听技术、监控方案以及监控设备。旗舰产品是 FinFisher 系列软件（木马涵盖 PC 端和移动端），2013 年和 2014 年分别由于黑客入侵事件，导致大量内部资料。

Hacking Team

一家来自意大利米兰的信息技术公司，主要向政府部门及执法机构有偿提供电脑入侵及监视服务，允许政府监听网民的通信、解码加密文件、记录 Skype 等网络电话通信、远程开启麦克风和摄像头。也因提供这些服务给不重视人权的一些政府而遭到批评。

ICS-CERT

全称 Industrial Control Systems Cyber Emergency Response Team，即美国工控系统网络应急响应小组，是美国国土安全局（DHS）下属机构的国家网络安全集成中心 National Cybersecurity and Integration Center (NCCIC)的一部分，专注各个重要基础设施建设领域的工控安全。

Lookout

2009 年成立于美国加州，是一家专注于移动领域的网络安全公司，曾用 Flexilis 作为公司名。Lookout 的理念是在移动攻击造成伤害前进行预测和拦截，打击网络罪犯，为个人和企业提供保护。

NetScout

NetScout Systems, Inc. 是一家应用和网络效能管理解决方案公司，1984 年成立于美国，主要客户是企业、政府以及通信服务提供商。2015 年收购了包括 Arbor 在内的 4 家公司。

Norman

1984 年成立，总部位于挪威奥斯陆，公司全称 Norman Safeguard AS，开发和销售数据安全软件（杀毒软件、反垃圾邮件、反间谍软件、安全备份等），2014 年 11 月被安全公司 AVG 收购。

NSA

National Security Agency，即美国国家安全局，是美国政府机构中最大的情报部门，也是世界上单独雇佣最多数学博士和电脑专家的单位，专门负责收集和分析外国及本国通讯资料，隶属于美国国防部，又称国家保密局，是美国情报机构的中枢。2013 年，美国中情局前职员爱德华 斯诺登披露的“棱镜计划”即是 NSA 实施的一项大规模监控和情报搜集计划。

NSO Group

NSO Group 是以色列数十家数字间谍工具开发公司之一，是网络战争领域的领导者，它们的产品可追踪智能手机上的任何活动。他们主要为世界各国政府和执法机构提供服务。自从 2010 年成立至今，NSO Group 始终保持着低调。有关 NSO Group 的资料很少，他们的创始人很少对媒体讲话，公司也没有网站。其主要产品是一款名为 Pegaus 的间谍软件。

附录 3 360 关于 APT 组织的命名规则

（一） APT 组织命名的一般规则

APT 组织的发现与命名，是 APT 研究工作的重要组成部分。截至 2016 年 12 月，360 威胁情报中心已经监测并独立发现了 36 个针对中国境内目标实施攻击的 APT 组织，并已通过研究报告等形式，对外披露了包括海莲花、美人鱼、人面狮、摩诃草、蔓灵花、黄金眼等多个由 360 命名的 APT 组织。

那么，APT 组织是如何命名的呢？从世界范围内来看，APT 组织的命名虽然并没有统一的规则或规范，但相关机构在命名过程一般会参考以下原则：

1） 谁发现，谁命名；

2） APT 组织攻击方式或 C&C 服务器的特点；

3） APT 攻击组织可能的政治及地缘背景猜测。

特别的，“谁发现，谁命名”这条原则还需要进一步解释一下。发现，一般是指独立发现，即指特定的研究机构在没有获得任何其他相关研究机构披露的相关信息辅助的情况下，独立进行的研究发现。但独立发现与率先披露是不同的。受各种客观因素的影响，所有 APT 研究机构都不会把自己截获的全部 APT 组织对外披露。一个 APT 组织究竟是由哪个研究机构率先披露的，往往存在一定的偶然性。

如我们在前面的报告中就介绍过，率先披露索伦之眼的是美国安全公司 Symantec，但给出的命名是 Strider。而 Symantec 发布报告后不到 24 小时，俄罗斯安全公司 Kaspersky 就发布了两份合计长达 60 页的，关于同一组织的研究报告，只不过 Kaspersky 将其命名为 Project Sauron，并且 Kaspersky 给出的命名得到了更为广泛的认可和传播。显然，Kaspersky 对于索伦之眼的截获，是独立于 Symantec 的相关研究的，但首先披露该组织的却是 Symantec。

为了强调自己对相关 APT 组织研究的独立性，绝大多数的研究机构都会尽可能对一个新的 APT 组织给出自己的独立命名，即便可能已经有多家其他研究机构对该 APT 组织给出了不同的命名。不过，一旦某个机构给出的 APT 组织命名已经得到了绝大多数研究者的认可，则其他研究者也就不会再为其进行新的命名了。例如，360 追日团队也早就独立截获了索伦之眼行动，但鉴于“索伦之眼”这个名字已经在很短的时间里得到了全球研究者及媒体的认可，所以，360 就没有对这一组织再给出自己的独立命名。

当然，也有一些研究机构仅仅使用某些特殊编号对 APT 组织进行命名。

（二） 360 命名 APT 组织的特殊规则

360 在给 APT 组织进行命名时，也基本上会参考上述三个主要原则。不

过，已经有很多网友和研究者注意到，360 给出的 APT 组织命名似乎参考了其他特定的规则，并通过邮件、微博、论坛留言等方式向我们建议，希望我们能够对 360 的 APT 组织命名规则给出更加明确的解释和说明。

诚如网友发现，360 自从命名第一个 APT 组织海莲花开始，就为 APT 组织的命名设计了一套详细的命名规则，并且沿用至今。其具体内容如下：

1） 组织与目标配对原则

以中国的视角来看，APT 组织主要分为三类：攻击境外目标的境外组织，攻击境内目标的境外组织，以及攻击境内目标的境内组织。对于这三类不同的 APT 组织，我们会分别采用不同的方式进行命名。

2） 现实世界不存在原则

考虑到 APT 攻击实际上是发生在虚拟世界中的，所以，使用虚拟的，传说的，甚至是神话中的事物来命名 APT 组织，更能表现虚拟空间战争这一主题。所以，360 用来命名 APT 组织的事物通常是现实世界不存在的东西。

3） 地缘与领域兼顾原则

即在某些组织的命名过程中，我们即会考虑攻击者及攻击目标的地缘特征，也会考虑攻击者所攻击的特定领域特征。

例如，我们披露的第一个 APT 组织“海莲花”，“莲花”就是表现了该组织的地缘及文化特征，同时，“海”则主要表现了该组织以海洋领域为主要攻击目标的活动特征。再比如，APT 组织黄金眼，“黄金”代表的就是攻击者以金融机构为目标这一特征。

综合上三点，360 对 APT 组织及其行动的命名大致可分为三个系列：

1） 幻兽系

攻击境外目标的境外组织，主要使用各种传说中的，或者是虚拟的动物形象来命名，同时结合了地缘及领域特征。如美人鱼、人面狮等。

2） 魔株系

攻击境内目标的境外组织，主要使用各种传说中的，或者是虚拟的植物形象来命名，同时结合了地缘及领域特征。如海莲花、摩诃草、蔓灵花等。

3） 超人系

攻击境内目标的境内组织，主要使用各种虚拟的，具有超能力的人体器官来命名，同时结合了地缘及领域特征。如黄金眼。

（三） 能力型厂商研究成果互认

根据 360 威胁情报中心与安天实验室之间的达成的能力型厂商成果互

认约定，360 命名的部分 APT 组织与安天实验室命名的 APT 组织对应关系如下：

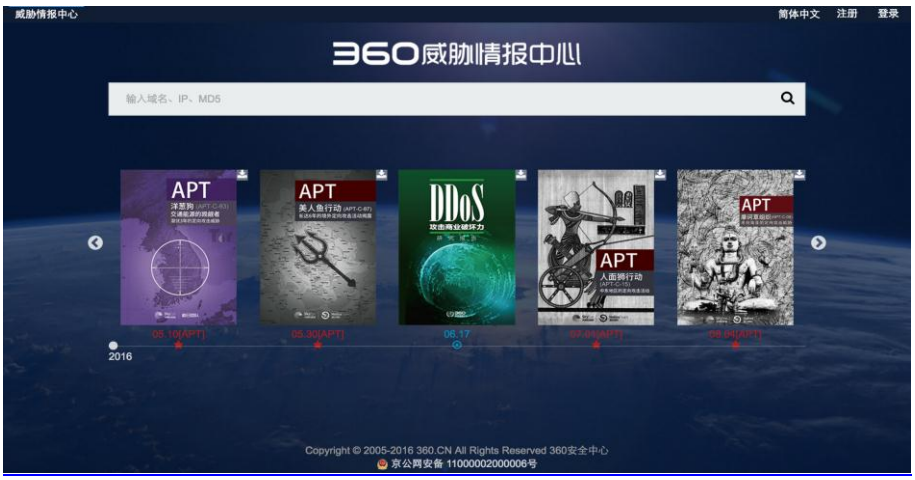
“摩诃草”对应安天实验室发布的《白象的舞步——来自南亚次大陆的网络攻击》报告中的“白象行动”。

“海莲花”对应安天实验室发布的《一例针对中方机构的准 APT 攻击中所使用的样本分析》报告中的“APT-TOCS”。

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 http://ti.360.com。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。



360 天眼实验室（SkyEye Labs）

360 天眼实验室（SkyEye Labs）正式成立于 2014 年 1 月，是 360 公司旗下专门利用大数据技术研究未知威胁的技术团队。该实验室依托 360 公司多年来积累的海量多维度安全大数据和数据挖掘技术，实现对全网未知威胁的发现、溯源、监测和预警，及时准确地为客户提供安全检测和防护设备所需要的威胁情报。

360 天眼实验室同时也是 360 各类大数据安全分析产品及解决方案的研发中心。实验室成立以来，以先后研发了包括 360 新一代威胁感知系统，360 态势感知与安全运营平台在内的多套国内领先的大数据安全分析系统。同时，360 天眼实验室研发的大数据分析产品还可与 360 推出的各类企业安全防护产品进行协同联动，从而实现数据驱动的协同防御。

360 天眼实验室研发的部分大数据安全分析产品简介

360 新一代威胁感知系统，是 360 天眼实验室研发的国内首套基于大数据的高级威胁定位与发现分析系统。该系统通过对本地流量的全量还原、存储与深度分析，将本地流量、文件及终端日志，与 360 云端威胁情报中心推送的专属威胁情报相结合，实现了对未知威胁与高级攻击的快速发现，精准定位和攻击溯源。该系统目前已广泛应用于政府、金融、能源、运营商等多个关键基础设施领域，并已在实践中捕获了多起重大 APT 攻击事件。

360 态势感知与安全运营平台，是 360 天眼实验室研发的，面向政府、金融、能源等大中型企事业单位的综合安全事件分析与全局安全态势感知系统，简称 NGSOC。该系统不仅具备传统 SOC 系统的内网信息综合监控与管理能力，同时还首次在 SOC 系统中引入了威胁情报技术与本地大数据分析引擎，从而使该系统能够实现各类安全数据的快速汇集、深度关联，以及自动化的高级智能分析，能够对企业内网系统实现持续的安全监测、快速响应、事件调查及安全态势感知，并能够联动 NDR，EDR，进行快速协同响应处置。同时，系统可通过图形化、可视化技术将威胁和异常的总体安全态势用最直观的方式展现给用户，有利于业务管理者迅速做出判断和决策。

了解 360 天眼实验室研发的更多产品，参见：https://skyeye.360safe.com

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。

已公开 APT 相关研究成果

发布时间	报告名称	组织编号	报告链接
2015.05.29	海莲花：数字海洋的游猎者 持续 3 年的网络空间威胁	APT-C-00	http://zhuiri.360.cn/report/index.php/2015/05/29/apt-c-00/
2015.12.10	007 黑客组织及地下黑产活动分析报告		https://ti.360.com/upload/report/file/Hook007.pdf
2016.01.18	2015 年中国高级持续性威胁 APT 研究报告		http://zhuiri.360.cn/report/index.php/2016/01/18/apt2015/
2016.05.10	洋葱狗：交通能源的觊觎者 潜伏 3 年的定向攻击威胁	APT-C-03	http://zhuiri.360.cn/report/index.php/2016/05/10/apt-c-03/
2016.05.13	DarkHotel 定向攻击样本分析	APT-C-06	http://bobao.360.cn/learning/detail/2869.html
2016.05.30	美人鱼行动：长达 6 年的境外定向攻击活动揭露	APT-C-07	http://zhuiri.360.cn/report/index.php/2016/05/30/apt-c-07/
2016.06.03	SWIFT 之殇：针对越南先锋银行的黑客攻击技术初探		http://bobao.360.cn/learning/detail/2890.html
2016.07.01	人面狮行动 中东地区的定向攻击活动	APT-C-15	http://zhuiri.360.cn/report/index.php/2016/07/01/apt-c-15/
2016.07.21	台湾第一银行 ATM 机“自动吐钱”事件分析		http://bobao.360.cn/news/detail/3374.html
2016.08.04	摩诃草组织 来自南亚的定向攻击威胁	APT-C-09	http://zhuiri.360.cn/report/index.php/2016/08/04/apt-c-09/
2016.08.09	关于近期曝光的针对银行 SWIFT 系统攻击事件综合分析		http://zhuiri.360.cn/report/index.php/2016/08/25/swift/
2016.11.15	蔓灵花攻击行动（简报）		http://zhuiri.360.cn/report/index.php/2016/11/04/bitter/

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

360 安服团队

360 安服团队汇集国内知名安全专家，在网络攻防以及攻击溯源方面有着丰富的经验。

360 安服团队创新性地提出基于数据驱动的安全服务运营理念：以安全数据为基础，使用安服专业分析工具，结合云端数据及专家诊断，为客户提供事前，事中，事后全周期的安全保障服务。

360 安服团队参与了多次知名 APT 事件的分析溯源工作，参与了国内重大活动安全保障工作超过 50 次，参与 APEC、G20、两会、纪念抗战胜利 70 周年阅兵、首届丝绸之路（敦煌）国际文化博览会等重大活动安全保障工作，并屡获客户认可及感谢信。

截至 2016 年 11 月底 360 安服团队共服务过人民银行、农业部、水利部、国土资源部、民政部、教育部、人社部、财政部等多家部委客户。