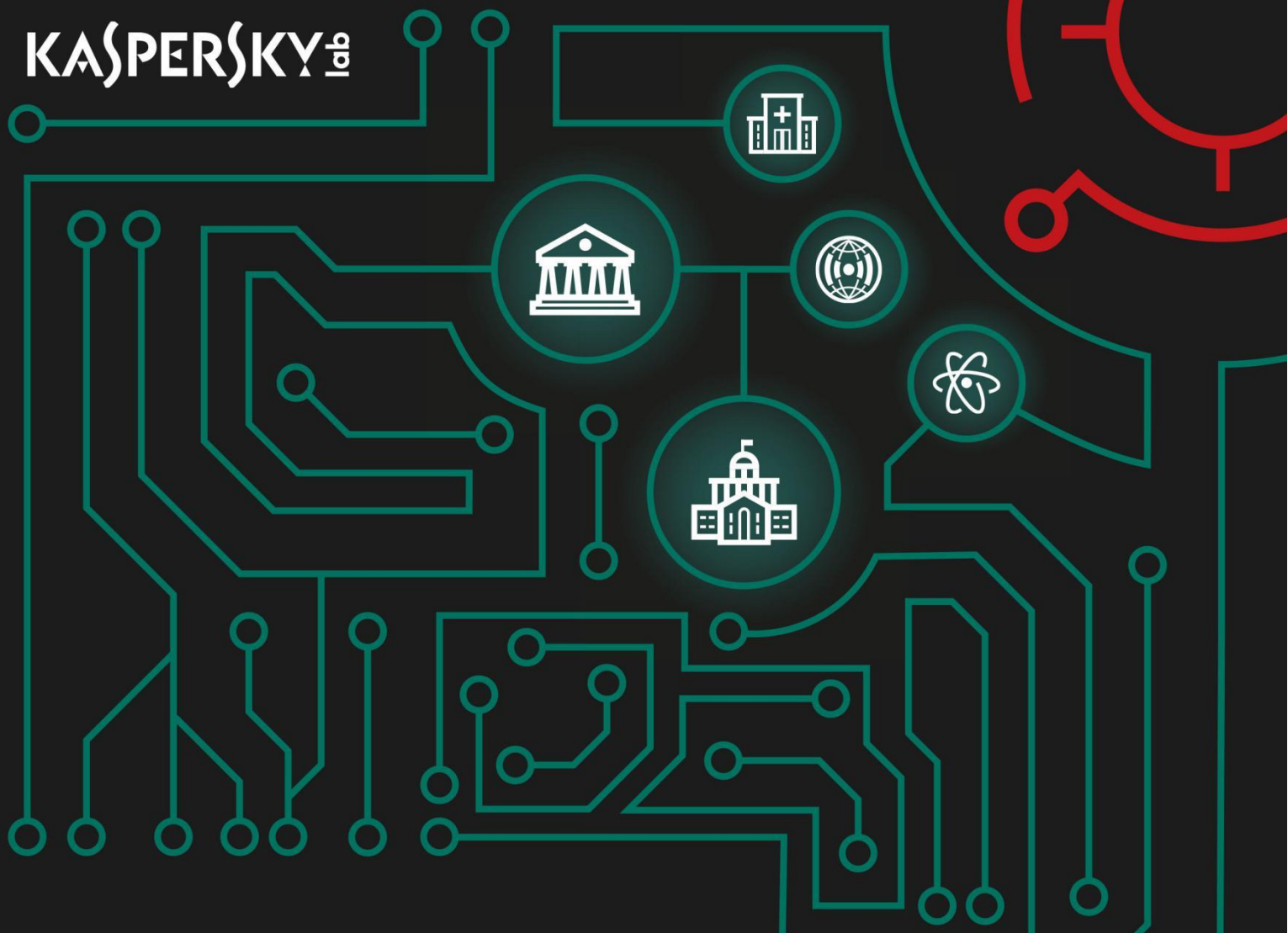
KASPERSKY lab



卡巴斯基安全公告

2017 年回顾

简译版

2017 年回顾

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Review of the Year 2017		
原文作者	卡巴斯基实验室	**原文发布日期**	2017 年 12 月
作者简介	卡巴斯基实验室是一家跨国网络安全和反病毒供应商，总部位于俄罗斯莫斯科。该公司开发和销售杀毒软件、互联网安全、密码管理、端点安全以及其他网络安全产品和服务。 https://en.wikipedia.org/wiki/Kaspersky_Lab		
原文发布单位	卡巴斯基实验室		
原文出处	https://cdn.securelist.com/files/2017/12/KSB_Review-of-2017_final_EN-1.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

译者小序

又到一年岁尾，全球网络安全公司开始盘点：总结过去、展望未来。2017 年，各种威胁源出于政治动机、经济动机和破坏目的继续发动针对性攻击和盗窃活动，他们采用新的、难以检测的工具和方法，为全球范围的组织和个人带来了严重的网络威胁，造成了重大的物理或声誉损害。诸如 Equifax 这样的大规模数据泄露事件，导致数百万客户的个人信息遭泄，面临被攻击者滥用的风险。今年，我们还看到了一些供应链攻击，即攻击者感染目标公司供应链中相对容易攻破的某家公司，以此作为跳板，6 月份的 ExPetr 攻击就是一个很好的例子。此外，各种金融攻击、物联网攻击和移动恶意软件层出不穷，花样不断翻新。

“Review of the Year 2017”（《2017 年回顾》）是卡巴斯基实验室在 2017 年 12 月发布的一份重要报告，该报告以其两位颇具代表性的高级分析师的视角，总结了 2017 年的重要威胁，包括全球大型网络间谍威胁源发动的针对性攻击、假借勒索软件而实为彻底删除数据的破坏性攻击、旨在窃取资金的金融攻击、以供应链作为垫脚石的“曲线救国”式攻击、针对大量物联网设备的攻击等。此外，为了突出移动设备的威胁，还特意单独分章节专门介绍了本年度的移动威胁，最后提出了应对威胁的建议。

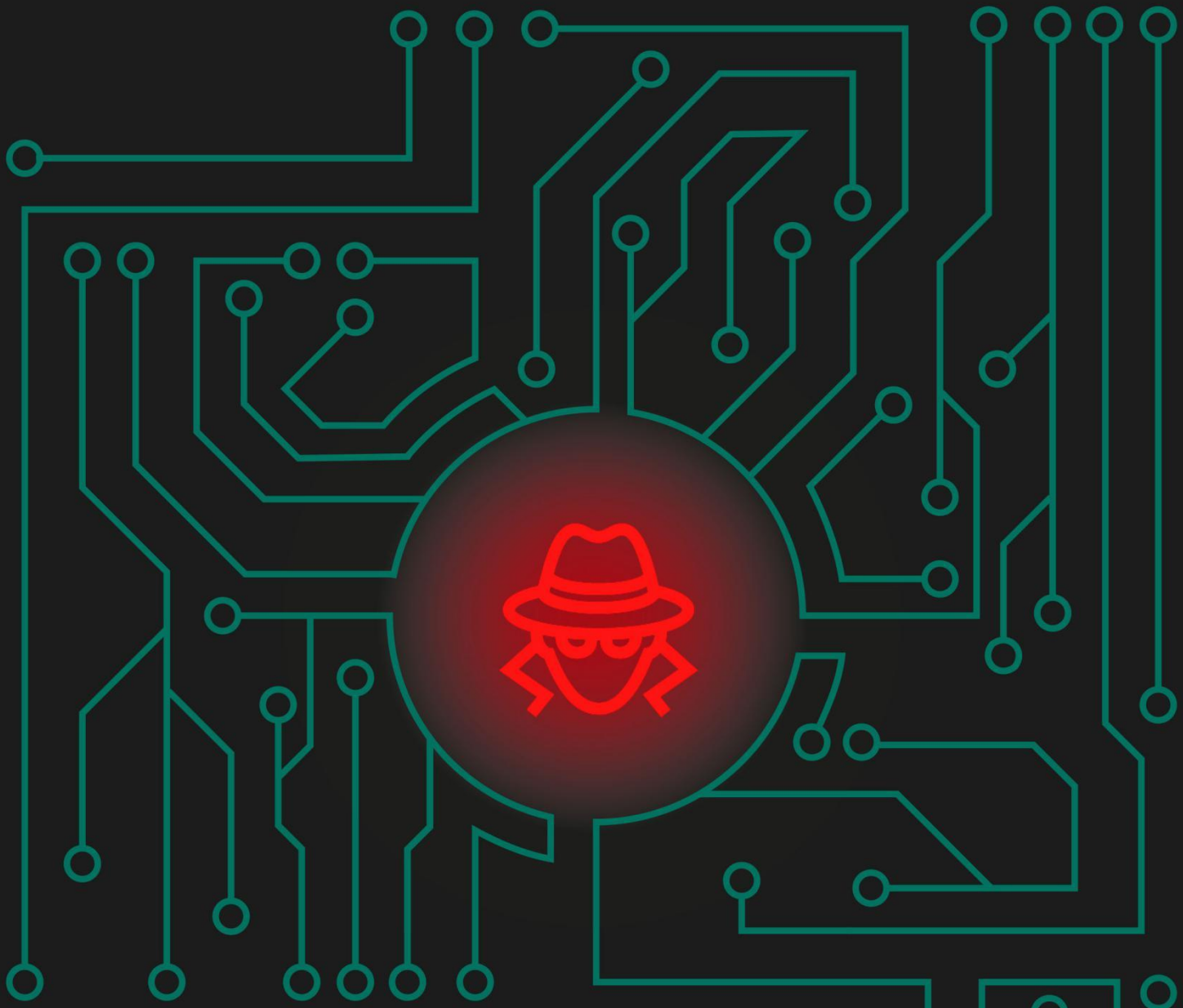
网络安全国家队安天同卡巴斯基实验室一样，是一家专注于威胁检测防御技术的领导厂商，以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命。在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，提供了先发预警、深度分析或系统的解决方案，其中多篇报告均为国内首发。为帮助用户应对 PC 终端的网络威胁，安天先后推出了自主研发的网络威胁检测设备“安天探海威胁检测系统”（PTD）、深度威胁鉴定设备“安天追影威胁分析系统”（PTA）、终端安全防护产品“安天智甲终端防御系统”（IEP）等产品，并针对移动终端推出了移动版追影系统。

作为一个保持着传统反病毒行业正直而严谨风格的团队，安天对卡巴斯基的技术能力与深度一直保持着良好印象，虽然其最近在美国市场上遇到一些障碍。“Review of the Year 2017”让我们看到，无论是技术深度还是直面威胁的勇气，他们依然是业内的榜样厂商。鉴于本报告对了解和对抗网络威胁和移动威胁具有重要的指导意义，安天实验室公益翻译小组对其进行了突击翻译，希望能为所有同网络威胁和移动威胁对抗的友商和团队提供一定的帮助。

安天技术公益翻译组

2017 年 12 月 12 日

目录



边界模糊之年

David Emm

全球研究和分析团队，首席安全研究员

边界模糊之年

简介

互联技术无处不在，是我们生活中不可分割的一部分，它们为网络犯罪分子提供了比以前更大的攻击面。在全球范围内，组织和个人面临越来越严重的网络威胁，犯罪分子旨在获取经济利益、数据，执行破坏，造成物理或声誉损害，或者仅仅为了“好玩”。多年来，网络威胁生态系统一直在建设和发展，我们对关键安全趋势和事件的年度评估也是该系统的一部分。

对于我们而言，2017 年最为重要的问题是边界——不同类型的威胁与不同类型的威胁源之间的传统界限——逐渐消失。在 2018 年这个问题会如何发展呢，我们拭目以待。

该趋势的一个例子是 6 月份的 ExPetr 攻击。乍看之下，它似乎是一个勒索软件，但实际上它是一个破坏性的数据擦除程序。另一个例子是影子经纪人（Shadow Brokers）黑客组织公布 NSA 开发的漏洞利用代码，这使得任何犯罪组织都能利用这些复杂的代码。还有一个例子是，旨在窃取钱财而非执行网络间谍活动的高级持续性威胁（APT）活动出现，其目的是为该 APT 组织的其他活动提供资金。

我们在《2017 年的勒索软件事件》（Story of the Year 2017）报告中详细讨论了 2017 年勒索软件的演变和低级犯罪组织利用 Shadow Broker 公布的漏洞利用代码。我们将在下文详细介绍其他趋势。

针对性攻击

在 2017 年，全球大型网络间谍威胁源继续运作，但是采用了新的、难以检测的工具和方法。我们报告了很多这样的活动。

俄语威胁源

在 4 月份的安全分析师峰会上，卡巴斯基实验室和伦敦国王学院的研究人员介绍了一项持续了 20 年的、以五角大楼和美国宇航局等为目标的“月光迷宫”（Moonlight Maze）网络间谍活动和一个非常现代化的 APT 组织 Turla 之间的可能关联。Moonlight Maze 攻击者劫持了一个服务器用作代理，利用其中存储的数据重建原始攻击者使用的操作、工具和技术。研究人员还对 Turla 进行了平行调查，发现这两个活动都使用了基于 LOKI2（1996 年发布的一个程序，允许通过隐蔽通道提取数据）。您可以通过本文了解研究细节。

8 月份，我们报告了另一个与 Turla 相关的 APT 组织 WhiteBear。在 2017 年年中，WhiteBear 将焦点从世界各地的使领馆扩大到包括国防相关机构在内。我们强烈怀疑该组织使用鱼叉式钓鱼邮件向其受害者发送恶意 PDF 文件。其主模块编排器（orchestrator）特别有趣。攻击者使用 RSA + 3DES + BZIP2 对资源部分进行加密/解密和压缩/解压缩，这是独一无二的做法。大多数 WhiteBear 样本使用在英国注册的组织“Solid Loop Ltd”签发的有效证书签名。这可能是一个傀儡组织或失效组织，攻击者冒充该组织，利用客户信任，创建假的数字证书。

英语威胁源

今年 4 月，我们还发现了 Lamberts 的最新工具包，它是一个高级威胁源，复杂程度可媲美毒曲（Duqu）、方程式（Equation）、Regin 或索伦之眼（ProjectSauron）。该组织在 2014 年首次引起安全社区的关注，我们发现它一直在开发一系列复杂的攻击工具，包括网络驱动的后门程序、几代模块化的后门程序、收集工具和擦除程序。目前已知的有 Windows 和 OS X 版本，包括白色、蓝色、绿色、黑色、粉红色和灰色变种，我们认为可能存在针对其他平台（如 Linux）的版本。

中文威胁源

我们还发现了关于春龙（Spring Dragon）黑客组织的更多技术细节，该组织的活动可以追溯到 2012 年，并且大量使用鱼叉式网络钓鱼和水坑攻击手段。其目标包括中国南海区域周边国家和地区（包括中国台湾、印度尼西亚、越南、菲律宾、中国香港、马来西亚和泰国）的政府机构，政党，教育机构和电信企业。特别是，我们调查了该组织用于窃取数据、执行其他恶意软件组件，并在受害者的计算机上运行系统命令的后门。这些后门使得攻击者能够在受害者的计算机上执行各种恶意活动。该组织维护着一个庞大的 C&C 基础设施，包括 200 多个独特的 IP 地址和 C&C 域。

其他语言的威胁源

在 10 月份，我们的高级漏洞防御系统发现了一个通过微软 Office 文档传播的新型 Adobe Flash 零日漏洞，其载荷是最新版本的 FinSpy 恶意软件。我们的客户群中只发现了一次攻击，所以我们认为攻击的数量很少，而且是高度针对性的。通过分析载荷，我们确信它与威胁源 BlackOasis 有关。我们非常确信，该威胁源与火眼公司 9 月份发现的另一个零日漏洞（CVE-2017-8759）有关。我们在 2016 年 5 月首次发现了 BlackOasis 活动，当时我们正在调查一个被广泛传播的 Adobe Flash 零日漏洞（CVE-2016-4117）。卡巴斯基安全网络（KSN）的数据也帮助我们确定了 BlackOasis 在 2015 年 6 月使用的另外两个类似的零日漏洞（CVE-2015-5119 和 CVE-2016-0984）：这些漏洞也通过 FinSpy 安装包传播。BlackOasis 组织的目标是参与中东政治的人士和与该地区有关的人士，包括联合国领导人、反对派博主和活动家以及地区新闻记者。

其他暗中运作的针对性威胁源包括黑色能量（Black Energy）——该组织可能是 ExPetr 和坏兔子（BadRabbit）勒索软件攻击的幕后黑手：研究人员认为，ExPetr 可能与 2015 年和 2016 年的 BlackEnergy KillDisk 勒索软件有关。

破坏性攻击

在 2017 年，我们发现旨在破坏数据（有时还会窃取数据）的针对性攻击再次活跃。

近年来出现了多起擦除攻击，2017 年我们又报告了两起这样的攻击：Shamoon 2.0 和 StoneDrill。研究人员认为，Shamoon 2.0 是 2012 年擦除了沙特阿拉伯超过 3 万台计算机数据的恶意软件的变种，该恶意软件在 2016 年 11 月和 2017 年初重出江湖，目标是沙特阿拉伯各种关键和经济部门的组织。新版本提供了新的工具和技术，其中包括使用被盗凭证在组织内横向运动的自定义擦除程序。该擦除程序一旦安装在网络中，就会在预定义的日期激活，导致受感染的计算机无法使用。Shamoon 2.0 还包含一个勒索软件组件，不过我们还没有发现该组件的传播和使用。

在调查 Shamoon 攻击事件的过程中，我们发现了一个以前未知的擦除程序，我们称之为 StoneDrill，该程序似乎也针对沙特阿拉伯的组织。StoneDrill 与 Shamoon 有相似的风格，还具有规避检测的功能。卡巴斯基安全网络的数据显示，其中一个 StoneDrill 受害者位于欧洲（属于石油化工行业），这说明攻击者可能将其擦除行动扩大到了中东以外。两者之间最显著的区别在于擦除过程。Shamoon 使用磁盘驱动程序直接访问磁盘，而 StoneDrill 则将擦除程序直接注入受害者的首选浏览器。StoneDrill 还包含一个后门，用来对一些目标执行间谍活动。

Shamoon 和 StoneDrill 背后的组织是同一个，还是说他们仅仅是有相同的兴趣和目标？貌似后者更有可能。

顺便说一下，ExPetr 也属于擦除程序，因为它纯粹用于破坏数据，只是伪装成了勒索软件。Shamoon 2.0 未使用的勒索软件组件是否也打算作为伪装手段呢，这个问题倒也挺有趣。

成功不必高大上

2017 年，我们发现威胁源能够利用简单的攻击活动获得成功，有的甚至持续多年。

成功的针对性攻击不一定多高级。2016 年 1 月，意大利警方逮捕了两名嫌疑人，由此曝光了一系列针对知名政治家、银行家、共济会和执法机构成员的网络攻击。EyePyramid 攻击中使用的恶意软件并不复杂，犯罪分子的运营安全（OPSEC）措施也很差。尽管如此，在被逮捕之前，攻击者还是成功地感染了多达 1600 名受害者（大部分在意大利）的计算机。尽管警方的报告中没有包含太多的技术信息，但是包含了 C&C 服务器、电子邮件地址和用于泄露被盗数据的 IP 地址的详细信息。

我们创建了一个 YARA 规则来搜索我们的系统，看能否找到任何匹配的样本。我们最初的 YARA 规则找到了两个样本，我们据此创建了一个更具体的 YARA 规则，又在数据库中找到了 42 个样本。由此，我们得以了解关于 EyePyramid 的更多信息。这些攻击严重依赖于社会工程手段 ,欺骗受害者打开和运行鱼叉式电子邮件的恶意附件。样本的时间戳显示它们是在 2014 至 2015 年编译的。因此，尽管技术上并不复杂，攻击者还是成功地运行了好几年，并从受害者那里窃取了数千兆字节的数据。

另一个例子是 Microcin 攻击，说明网络犯罪分子如何使用便宜的工具并小心选择目标来实现成功的攻击。攻击者利用微软 Office 漏洞执行水坑攻击，感染一个讨论俄罗斯军事人员及其家属有权获得国家补贴住房的论坛。攻击者在受害者的计算机上创建一个可执行文件 ,然后下载更多的模块 ,从而扩展了恶意软件的功能。攻击者使用 PowerShell 脚本和其他实用程序窃取受害者计算机上的文件和密码。犯罪分子使用的方法既不复杂也不昂贵，但是颇为有效。这个攻击有两个方面特别有趣。首先，攻击者选择利用人为失误，而不是花时间和资金开发漏洞利用代码直接攻击企业资源。其次，他们利用常用的系统工具在目标组织内横向运动。

为间谍活动执行窃取行为

2017 年，高级威胁源执行多样化的盗窃活动，从而为其他活动提供资金。

2016 年 2 月，一群黑客（当时不明身份）企图从孟加拉国中央银行窃取 8.51 亿美元，最终成功转走了 8100 万美元。他们被认为是有史以来规模最大、最成功的网络抢劫犯。卡巴斯基实验室等厂商调查发现，几乎可以肯定该攻击是由臭名昭著的网络间谍和破坏组织拉撒路（Lazarus）发起的，该组织在 2014 年攻击了索尼影视娱乐有限公司（Sony Pictures），自 2009 年开始至少对 18 个国家的制造企业、媒体和金融机构发动了攻击。该组织新增了对经济收益的兴趣，调查发现似乎是 Lazarus 内部的 Blurnoroff 团队负责获取非法收益。到目前为止，我们已经发现了四种主要的目标：金融机构、赌场、开发金融交易软件的公司和办理加密货币业务的公司。

Bluenoroff 其中一个最著名的活动是对波兰金融机构的攻击。攻击者感染了许多金融机构经常访问的一个政府网站——使其成为一个非常强大的攻击媒介。

Lazarus 不只是一个 APT 组织。其经营规模令人震惊：它似乎经营着一家恶意软件工厂，随着旧的工具“被毁”不断创建新工具。该组织使用各种代码混淆技术，重新编写自己的算法，应用商业软件保护器，并使用自己的和地下市场中的打包器。所有这一切都需要钱——这也许能够解释 Lazarus 多元化的盗窃行为。

Lazarus 组织似乎也是 2017 年 5 月魔窟（WannaCry）疫情的幕后黑手，更多的细节可参阅《2017 年的勒索软件事件》（Story of the Year 2017）。这样一个先进的攻击组织为何发布不完善和不受控制的破坏性恶意代码仍然是一个谜。

其他金融攻击

2017 年，ATM 攻击持续增加。攻击者使用先进的无文件恶意软件、遮挡闭路电视监控探头和钻孔手段攻击银行基础设施和支付系统。

在今年的安全分析师峰会上，我们的两位研究人员 Sergey Golovanov 和 Igor Soumenkov 讨论了网络犯罪分子从 ATM 机窃取资金的三起案例。

第一起案例是 ATMitch 攻击，涉及感染银行的基础设施并远程控制 ATM 的运作。攻击者利用未修复的漏洞渗透目标银行的服务器，使用开源的代码和公开的工具来感染银行的计算机。但是，他们创建的恶意软件仅驻留在内存中，而不是存储在硬盘上，并且在计算机重启后几乎所有恶意软件的痕迹都会被清除。感染之后，攻击者与 C&C 服务器建立连接，这允许他们远程在 ATM 上安装恶意软件。由于看起来像一个合法的更新，恶意软件安装并不会触发银行的任何警报。一旦安装，恶意软件就会查找控制 ATM 的指令。恶意软件首先发出一个指令，确定 ATM 机中有多少钱，然后发出进一步的指令来取钱——由等在 ATM 机旁的钱骡收钱。此后，恶意软件擦除所有的证据。

第二起银行攻击也是从发送命令开始的。钱不翼而飞，但是 ATM 机的日志是干净的，犯罪分子遮挡了闭路电视监控探头，所以没能录下攻击过程。银行将 ATM 机送到我们的办公室，拆卸之后，我们发现犯罪分子在 ATM 机上安装了蓝牙适配器，并等待了 3 个月的时间，直到日志被清理。然后，他们再次接触 ATM 机，遮盖监控探头，并使用蓝牙键盘在维修模式下重启 ATM 机，最终取走了 ATM 钞箱中的所有钱款。

在第三起案例中，涉事银行请我们帮忙调查 ATM 机盗窃事件。我们发现，这种方法更加恶劣：犯罪分子在密码键盘上钻了一个直径约 4 厘米的孔。不久之后，我们得知俄罗斯和欧洲也出现了类似的攻击。警方逮捕其中一名嫌犯时，发现了一台笔记本电脑，还有一根探进面板小孔的线缆。打开面板，可以看到可能是窃贼通过小洞连接的一个串行端口。该端口连接到串联起 ATM 机所有组件的内部总线上，从控制用户界面的计算机到吐钞器都连上了。研究人员发现，该机器唯一的加密机制，就是用个弱异或（XOR）密钥，而且机器各模块间根本没有真正的身份验证。我们花费了大约 15 美元创建了一个简单的电路板，一旦将它连接到 ATM 机的串行总线，就可以控制 ATM 机，让它乖乖吐钞。我们的研究人员指出，要想解决这个问题并不容易，需要进行硬件更新，而且不能远程完成：技术人员必须到现场安装。

最近，我们发现了一起针对金融机构（主要俄罗斯的银行，也有马来西亚和亚美尼亚的银行）的新型攻击。攻击者使用 Silence 木马和类似 Carbanak 的方法。他们持续进入内部银行网络，记录银行员工的日常活动，了解银行的工作流程和安装的软件，然后利用这些信息发送包含恶意附件的鱼叉式钓鱼邮件，从而窃取资金。然而，Silence 攻击的一个有趣之处是，网络犯罪分子破坏了银行基础设施，从真实银行员工的电子邮件地址发送他们的钓鱼邮件，因此看起来很可信。

供应链作为垫脚石

2017 年新兴的企业威胁将在 2018 年进一步增长。

在 2017 年，我们看到了一些“垫脚石”攻击：攻击者感染目标公司供应链中相对容易攻破的某家公司。这是 6 月份 ExPetr 攻击最显著的特征之一 攻击者专门针对一家向乌克兰公司提供会计软件的公司。大多数受害者都位于乌克兰，但攻击事件对在全球运营的公司都产生了影响，包括全球最大的集装箱船和供应船公司马士基。该公司在其收益报表中指出，ExPetr 攻击造成“重大业务中断”，预计损失在 2 亿至 3 亿美元之间。另一个受害者是联邦快递，它透露，TNT 快递部门在欧洲的业务受到这次攻击的“严重影响”，损失在 3 亿美元左右。

8 月份，ShadowPad 攻击者采用了类似的方法，进入了受欢迎的服务器管理软件供应商 NetSarang 的网络，从而感染了一些客户——包括金融服务、能源、零售、技术和媒体行业的公司。攻击者修改其中一个更新，植入一个后门，从而下载和执行任意代码，创建进程并在注册表中维护虚拟文件系统，所有这些都被加密并存储在每个受害机器的独有位置。

另一起供应链攻击发生在 9 月份，攻击者感染了 Avast 发布的 Windows 清理工具 CCleaner 的更新。他们修改了 CCleaner 5.3 的安装程序，向任何下载该程序的用户的计算机投放恶意软件。这个用有效证书签名的恶意软件活跃了一个月，感染了大约 70 万台电脑。攻击者使用了两阶段的感染过程：第一阶段是向攻击者的 C&C 服务器发送受害者信息，第二阶段为特定目标保留。

物联网攻击

Mirai 僵尸网络爆发一年之后，Hajime 僵尸网络来袭并感染了超过 30 万个联网设备——这只是联网设备和系统遭遇的众多攻击活动之一。

如今，我们的生活中充斥着智能设备。这包括电话、电视机、恒温器、冰箱、婴儿监视器、健身手环和儿童玩具等日常家用电器；也包括汽车、医疗设备、闭路电视监控摄像机和停车收费表。现在有些家庭内置了“智能”设计。作为物联网（IoT）的一部分，无处不在的 Wi-Fi 将所有这些设备连接到网络。这些设备是为了让我们的生活更轻松。然而，日常物品连网意味着网络犯罪分子拥有更大的攻击面。除非物联网设备是安全的，否则它们交换的个人数据可能会遭到泄露，它们会遭到攻击，也可能被用于攻击。

2016 年 10 月，Mirai 僵尸网络劫持了大量联网家庭设备（如 DVR，闭路电视监控摄像机和打印机）发动 DDoS 攻击，导致美国大范围网络瘫痪。今年 4 月，Hajime 僵尸网络背后的攻击者感染了超过 30 万台设备，不过迄今为止它还没有被用于恶意目的：攻击者可能只是想提醒人们注意某些联网设备严重缺乏安全性。研究人员已经展示了很多不安全的物联网设备的例子。德国联邦网络管理局（德国电信监管机构）担心攻击者利用“我的朋友 Cayla”（My Friend Cayla）洋娃娃，建议购买该娃娃的父母予以销毁。在安全分析师峰会上，安全专家乔纳森·安德森（Jonathan Andersson）展示了一个高明的攻击者如何在几秒钟内创建一个能够劫持无人机的设备。攻击无人机似乎离我们远了点，但是无人机的使用已不仅仅是小众活动了：去年 12 月，亚马逊测试了使用无人机传送包裹。

这种攻击并不局限于消费者使用的日常物品。以前不需要考虑网络安全的组织现在也面临网络攻击风险。其中一个例子就是医疗行业。以前以纸质形式存在的医疗信息现在可以在数据库、门户网站和医疗设备中找到。危险的是，对智能医疗的攻击不仅会导致患者数据被盗，而且还会导致诊断数据的修改——导致病人被错误地治疗或用药。今年早些时候，我们报告了医疗机构的潜在风险，并提供了相关建议。

数据泄漏

2017 年发生了大量数据泄露事件，包括 Equifax 事件，该事件导致数百万条记录被盗，其后遗症会持续数年之久。

个人信息是一种有价值的商品，因此网络犯罪分子瞄准在线提供商、寻找获取数据的途径并不奇怪，这些数据可以进行销售或用于将来对消费者或企业的攻击。2017 年发生了大量的数据泄露事件。其中包括雅虎事件（严格来说，泄露事件发生在 2013 年，只是在 2017 年被披露出来）、Avanti Markets、Election Systems & Software、Dow Jones、America's Job Link Alliance 和 Equifax。2016 年 10 月发生的 Uber 数据泄露事件暴露了 5700 万客户和司机的数据，但是直到 2017 年 11 月泄露事件才被披露。

一些攻击导致大量数据被盗，然而大部分泄漏事件是完全可以避免的。Election Systems & Software 和 Dow Jones 等泄露事件都是由于亚马逊网络服务的配置错误造成的。在 America’ s Job Link Alliance 泄露事件中，黑客利用了 web 应用程序中的已知漏洞。Equifax 泄露事件是由 Oracle 在攻击前几个月就已经修复的一个漏洞造成的，但是 Equifax 没有打补丁。

结论

2017 年，很多事情并不像表面看起来那样：勒索软件实际上是擦除程序；合法的商业软件是一种武器；高级威胁源利用简单的工具，而在食物链底层的攻击者则获得了高度复杂的工具。这一网络威胁全景说明安全防御者面临越来越严峻的挑战。

这不仅是企业的问题。随着供应链攻击日益增多，任何一家公司都可能成为受害者，尤其是当他们处于威胁源目标所在的供应链中时。世上不存在 100%的安全，但是组织和个人可以采取更多的措施来保证安全。

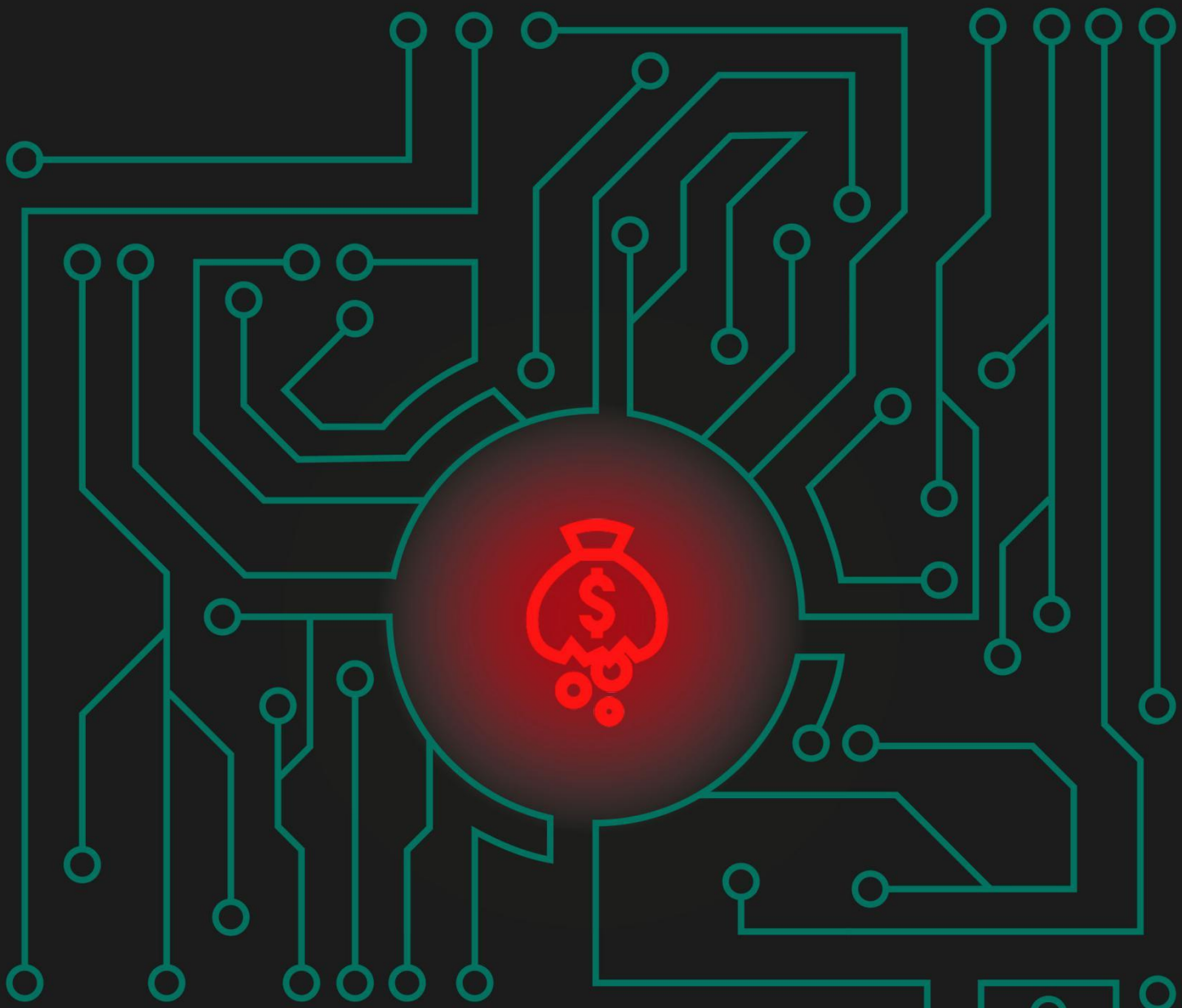
在面临针对性攻击时，最佳的企业防御措施是将传统反恶意软件技术与补丁管理、主机入侵检测、默认拒绝白名单策略和威胁情报相结合的多层方法——将保护视为一个持续的过程，并用工具和专业知识予以支持。欢迎您订阅我们的 APT 情报报告，我们将为您提供调查和研究结果，包括全面的技术数据。请不要忘记修复人为漏洞，社会工程手段仍然是网络攻击者的一个关键切入点，所以教育和与员工沟通是非常重要的。

任何持有个人数据的组织都有责任有效保护这些数据。如果攻击导致个人信息被盗，公司应该提醒其客户，以便他们能够采取措施来减少任何潜在的损害。

对于消费者来说，主要的威胁之一仍然是移动恶意软件。以下章节将探讨 2017 年移动威胁的演变。

最后，永远不要忘记采取基本的安全措施，如强效密码、常规软件更新、将不需要的功能关闭。这些措施对于保护联网设备（无论是家庭打印机还是重要的医院设备）能够起到很大的作用。

2017 年，人们得到了很多教训，特别是企业。2018 年，我们将印证我们是否真得学到了这些教训。



2017 年的移动威胁

Roman Unuchek
高级恶意软件分析师

2017 年的移动威胁

简介

对于消费者来说，移动恶意软件可能是最大的威胁之一，尤其是 Android 用户。2017 年，植入木马的应用程序被下载了数万次甚至更多，导致受害者被大量广告淹没、遭到勒索软件攻击或“被订阅”付费短信和 WAP 服务。移动恶意软件增加了新的技术，以规避检测，绕过安全措施并利用新的服务。与 2016 年一样，许多此类应用程序可通过 Google Play 商店等知名来源轻松获得。

以下是对 2017 年主要移动威胁的综述。

Root 型恶意软件

在过去的几年里，root 型恶意软件一直是 Android 用户最大的威胁。这种木马非常先进，功能很多，而且也很受欢迎。它们的主要目标是向受害者展示尽可能多的广告，并悄悄地安装和启动推广的应用程序。在某些情况下，弹出窗口和汹涌的广告可能会导致设备无法使用。

这种恶意软件通常会尝试通过利用设备漏洞或使用先前感染获得的权限来获取 root 权限。Root 权限使得木马几乎能够做任何事情，木马通常会安装模块来获得持续性，即使将设备重置为出厂设置之后也无法删除恶意软件。

利用 Google Play 商店传播 root 型木马的情况并不罕见：Dvmap（Trojan.AndroidOS.Dvmap.a）从 Google Play 商店下载并安装了超过 5 万次，它将其恶意代码注入系统库；我们发现近 100 个被 Ztorg 木马感染的应用程序上传到 Google Play 商店，其中一个应用被安装了超过 100 万次。这些应用程序在未打补丁的设备上利用旧的已知漏洞获得 root 权限，之后它们将模块安装到系统目录中以获得持续性并悄悄安装其他应用程序。

尽管与 2016 年相比，2017 年遭到 root 型恶意软件攻击的用户数量有所下降，但是今年排名前 30 位的最受欢迎的 Android 木马中有近一半（12 个）是 root 型恶意软件，而 2016 年有 22 个。我们认为 root 型木马的减少主要是因为 Android 设备的使用日益减少——在现代智能手机和平板电脑上，这种木马无法利用漏洞来获得 root 权限。

但是，这并不意味着 root 型木马背后的网络犯罪分子已经停止了攻击。一些犯罪分子只是放弃了 root 权限，但仍积极展示广告和下载其他应用程序。另外，从设备中删除这些应用程序仍然很难，因为它们可能会滥用系统功能。

我们还发现，Ztorg 木马开始探索赚钱的新途径，例如攻击移动支付系统。我们发现了两个具有这种恶意功能的应用程序——它们被从 Google Play 商店下载了数万次。它们能够发送付费短信，并删除所有收到的短信，悄悄地从受害者的手机账户中偷钱。此外，在我们的研究中，我们发现 Ztorg 的一些附加模块使用一个 JS 文件，所以它们也可以通过对 WAP 计费站点的点击劫持来窃取资金。

WAP 计费点击劫持

Ztorg 并不是唯一针对 WAP 计费服务的恶意软件。在 2017 年，我们发现这种恶意软件有所增加。这种功能并不新鲜（早在 2015 年 Trojan-SMS.AndroidOS.Podec 就攻击了 WAP 计费服务），但是我们在 2017 年看到了许多新的热门木马。受到攻击的用户数量是 2016 年的 2.4 倍。

这些木马中的大多数从它们的 C&C 中心接收 URL。它们在受害者不知情的情况下打开链接，甚至访问这些链接，有时使用特殊的 JS 文件点击访问的网页上的按钮。这些网页可能是广告，对受害者来说基本上无害（除非是恶意广告，如 Ztorg 木马传播的那些广告），但有时页面中包含 WAP 计费服务，我们发现了一些 JS 文件专门用来点击 WAP 计费页面。

通常，移动网络运营商使用自己的网页完成 WAP 支付交易，但是这些木马可以通过点击“同意”按钮绕过这些页面。另一层安全是交易的短信通知，但是这也被绕过了，因为大多数木马都能够悄悄删除收到的短信。

银行恶意软件

银行恶意软件也引入了新功能，在 2017 年，我们看到了几种偷钱的新技术。FakeToken 的一些变种攻击了 2000 多个金融应用程序。该木马用钓鱼窗口覆盖真实应用程序，以窃取用户的凭证——我们发现，FakeToken 的变种攻击应用程序来预订出租车、门票和酒店，甚至支付交通罚款。

通常，Android 操作系统更新包含新的安全功能，其主要目的是保护用户，防止恶意软件造成伤害。但是恶意软件总能找到绕过安全功能的方法。2017 年 7 月，我们发现 Svpeng（Trojan-Banker.AndroidOS.Svpeng.ae）通过滥用无障碍辅助服务（accessibility service）为自己授予任何权限。

“无障碍辅助服务”是一项系统功能，可让应用程序开发人员为残障用户或暂时无法与设备完全交互的用户创建应用程序。然而，该木马要求用户使用无障碍服务，然后授予自己发送短信、阅读联系人、拨打电话等所需的权限。而且，这个木马悄无声息地覆盖了其他的应用程序，并将自己添加到设备管理员列表中。它通过点击系统对话框中的按钮成功阻止卸载。使用无障碍辅助服务也使该木马能够窃取从应用程序的用户界面输入的数据，甚至能够作为击键记录器。

2017 年 8 月，我们发现了 Svpeng 木马的另一个变种。该变种也滥用无障碍辅助服务，但其主要目的是锁定设备，加密受害者的文件并要求受害者支付赎金来解锁和解密。这并不是移动银行木马的新功能，FakeToken 木马的一个变种就具有文件加密功能。

总的来说，Svpeng（Trojan-Banker.AndroidOS.Svpeng.q）是 2017 年最受欢迎的手机银行木马，但与 2016 年相比，受到攻击的用户数量下降了 1.5 倍。2017 年，另一个流行的木马是通过垃圾短信传播的 Asacub（Trojan -Banker.AndroidOS.Asacub）。2017 年排名前 30 位的移动银行木马中，Asacub 的变种数量是 2016 年的 3 倍（12 个），2016 年只有 4 个。

勒索软件的兴衰

2017 年上半年，移动勒索软件文件数量大幅增长，比 2016 年全年增长了 1.6 倍，但在 2017 年 6 月以后，这一数字又回落到了较早的水平。在这个激增浪潮中，绝大多数（83%）移动勒索软件属于 Congur 家族（Trojan-Ransom.AndroidOS.Congur）。它们大多数是相当简单的木马：要求设备管理员权限，然后更改设备密码或设置新的密码。然后，攻击者用中文发送一条信息，要求受害人通过中国流行的聊天工具 QQ 联系他们。

在 2017 年，移动勒索软件的变化并不大；它们中的大多数仍然使用相同的技术来锁定设备。我们没有发现很多用户遭到移动加密器攻击的例子。

结论

使用移动设备的人越多，移动设备的使用范围越广，移动恶意软件就越有可能出现和发展。这是攻击者、设备软件开发者和安全行业之间的持续竞争。但用户不一定要成为受害者，他们可以做采取很多措施来保护自己、设备和存储在设备上的数据。这包括从信誉良好的在线商店下载应用，并在下载应用之前与开发人员确认。我们还建议用户使用可靠的安全解决方案，如卡巴斯基移动杀毒软件：Web Security & Applock。

KASPERSKY lab

安天实验室简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

欢迎您访问安天网站（http://www.antiy.cn/Security_Product/index.html）了解关于安天产品的更多信息，如您有任何疑问和需要，请发邮件至 sales@antiy.cn 或致电 010-82893723。