火眼公司的移动威胁报告

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	The FireEye Mobile Threat Report		
原文作者	Jason Steer	**原文发布日期**	2015 年 2 月 27 日
作者简介	Jason Steer 目前就职于火眼公司并担任首席安全战略官一职，擅长从事应用安全、电子邮件安全、邮件加密、网络安全、网络威胁评估、网页应用安全等领域的工作。 http://www.linkedin.com/profile/view?id=2518050&authType=NAME_SEARCH&authToken=IyHy&locale		
原文发布单位	火眼公司		
原文出处	https://www.fireeye.com/blog/threat-research/2015/02/the_fireeye_mobilet.html		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
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。

火眼公司的移动威胁报告

Jason Steer

2015 年 2 月 27 日

今天，我们发布了题为《资金流失：对 700 万 iOS 和 Android 应用程序的移动威胁综合评估》的移动威胁报告。

报告显示，处于 Android （安卓操作系统）平台的移动设备包含机密的个人数据、照片、用户定位；并且更多的是包含机密的商业信息、合同和知识产权。同样，移动设备也为攻击者指引了新的攻击方向。基于 2014 年间对超过 700 万移动应用程序的分析，我们发现：当今移动用户面临多方风险，包括：

* 恶意应用程序一旦被安装就会盗取信息
* 由开发商编写的存在安全隐患的合法应用程序
* 合法应用程序使用非安全且有侵略性的广告库
* 绕过 Google 官方检测的恶意软件/侵略性广告软件伪装为“安全”软件
* 身份盗用
* 优惠电话和短信诈骗

然而，由于 iOS 应用程序商店严格的审核进程使得处于 Apple iOS （苹果操作系统）的恶意软件还非常罕见。我们发现了一条 iOS 恶意软件用于逃避 Apple App Store （苹果应用程序商店）审核的新型传输通道。攻击者可利用企业/点对点准备金提取向终端用户传递（要么是通过 USB 连接，要么通过无线传播）恶意应用程序。我们发现超过 1400 个可

在互联网内公开使用的 iOS 应用程序，这些程序署名并分散使用企业准备金提取档案将会引发安全问题。

对 CISO（首席信息安全官）来说，这意味着什么？

世界各地的人们正在接受移动设备。随着消费者倾向于选择能够使生活更便捷的更简易，更轻巧的设备这一趋势的出现，个人电脑制造商目睹了个人电脑和平板电脑销量的下降。我们花费在移动设备上的时间要多于看时间的时间。我们选择安装的应用程序（而不是使用网页）可改善用户的在线体验并确保可以挽回一批又一批的用户。在用户与互联网是如何互相作用方面，我们已抵达其转折点。

应用程序是现代日程生活中我们完成工作、购物、办理银行业务，使用社会媒体和许多其它目的在线体验的未来。移动设备也是现今我们拥有的最重要的装备；它们包含了我们的日记、通讯录、邮件、照片、视频、雇主信息好许多其它重要并机密的信息。至今我们的移动设备仍缺乏确保自身及其所携带信息安全的安全性。

移动设备面临来自制造商、网络供应商和网站运营商的安全和隐私风险，然而，应用程序商店和应用程序开发商才是对移动设备最大的风险。风险应用程序被下载后，其随后的行为会对其所处设备内的所有信息造成威胁：

* 此类应用程序可自行复制并上传个人联系方式，捕获所有已安装应用程序的细节，亦或是追踪 GPS 坐标。

* 恶意软件可具有恶意意图，盗取银行账户信息、复制邮件、收集 VPN（虚拟专用网络）认证信息。

* 当然，也没有永远不会出错的开发商：他们常常会编写出可以使应用程序置身被攻击的危险中的存在安全漏洞的代码。

作为消费者和企业，我们需要更好的了解所使用的应用程序有何用途。

合法的应用程序商店正在努力工作已鉴别哪些是有害的应用程序。然而，攻击者会继续为安全攻击冲锋陷阵就需要我们确保被下载的应用程序是安全的。第三方应用程序商店提供在其它商店无效的应用程序目录，为更多的恶意应用程序“合法化”提供了一个避风港。

应用程序商店供应商、应用程序开发商，组织和消费者需要加强对当今他们所面临的来自移动应用程序的威胁和风险的理解。对消费者来说，了解应用程序行为应是用户感知的关键所在。对企业来说，他们已安装的移动设备和应用程序应是他们的终端战略中要去理解和保护的关键所在。