简译版

# 值得关注的七个移动安全威胁

**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** | 7 Current Mobile Security Threats To Watch Out For | | |
| **原文作者** | Guest Author | **原文发布日期** | 2019 年 8 月 27 日 |
| **作者简介** | Guest Author 是一位移动应用程序设计师和 IT 专家。 | | |
| **原文发布单位** | Security Boulevard | | |
| **原文出处** | https://securityboulevard.com/2019/08/7-current-mobile-security-threats-to-watch-out-for/ | | |
| **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。<br>• 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。<br>• 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。<br>• 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。 | | |

# 值得关注的七个移动安全威胁

Guest Author

2019 年 8 月 27 日

2019 年，随着越来越多的员工通过移动设备（主要是智能手机）访问其所需的大部分数据，移动安全成为企业 IT 安全的首要关注点。如今，企业最有价值的资产通常是数据，因此移动设备数据泄露对各种规模的企业都构成了巨大的威胁。下面，我们将介绍企业现在和不久的将来需要关注的七个移动威胁。

## 数据泄漏

数据泄露是企业最常见的威胁之一。根据 Ponemon 研究所的调查分析，在未来两年内，公司发生数据泄露的可能性高达 28%。

“不幸的是，最大的威胁通常来自用户本身的不当行为——对企业自身应用产生的数据管理不善，特别是分享机制。目前来说，这是数据泄露最常见的原因。但是，企业可以通过正确的移动安全解决方案（例如赛门铁克和 CheckPoint 提供的解决方案）轻松防范此类威胁。” 1day2write 和 NextCoursework 移动安全分析师比艾塔·麦克斯韦尔（Beata Maxwell）指出。

企业可以对员工开展简单的教育培训和实施最佳工作实践，以防止员工错误传送敏感数据，或向错误的对象（攻击者）发送敏感信息——就是这么简单。

## 网络钓鱼和诈骗攻击

另一种可以通过更好的实践轻松防范的威胁是社会工程攻击 - 如诈骗邮件。我们都知道诈骗邮件是如何运作的：攻击者使用用户熟悉的邮箱向其发送邮件，邮件中包含恶意链接，一旦用户点击链接，恶意软件就会传播到用户的设备上。对此类诈骗保持警惕，是防范此类威胁的最佳实践。企业应就这些事项对员工开展培训——想当然地认为他们已经了解此类威胁是很严重的错误。

## 不安全的网络

移动设备的安全性，取决于它用于发送和接收数据的网络的安全性。该威胁也可以通过

更加警惕的行为加以防范。开放式网络通常是最不安全的( 例如机场、商场和咖啡馆的网络 ),因此请不要使用这些网络发送和接收敏感数据。

WriteMyX 和 BritStudent 移动应用程序开发员道格·约翰逊( Doug Johnson )警告说：“此外，还存在诸如网络冒充这样的威胁。例如，攻击者冒充用户认为的某人，诱骗用户登录其恶意网络。”

## 过时的设备

很多制造商并不对其设备进行更新，尤其是在为操作系统打补丁方面，这导致用户容易遭受攻击。为了防范此类威胁，建议企业选择安全性高的制造商，同时强烈建议企业将自身的安全策略与这些安全更新相适应和匹配。

## 挖矿劫持

你可能听说过挖矿劫持 - 这是一种盗用其他设备挖掘加密货币的做法，会严重影响被盗用设备的性能。这曾经只是桌面电脑面临的问题，但是与其他威胁一样，挖矿已经转向了移动设备。要想防范此类威胁，用户要当心恶意应用程序和恶意广告软件的下载。一旦下载了这些恶意程序和广告软件，用户的设备就可能沦为挖矿劫持的目标。

## 间谍软件

你所认识的人在你设备上安装的间谍软件，可能是设备安全的最大威胁之一——这可能令人难以置信。你可能认为自己没有什么可担心的，但是你所从事的工作可能意味着：对其他人而言，你处理的数据和信息是有价值的。用户可以下载简单的恶意软件和反病毒检测软件，来防范间谍软件，并且这种方法的成本也比较低。

## 短信钓鱼

就像电子邮件网络钓鱼一样，短信钓鱼（ SMiShing ）是指：攻击者通过短信向用户发送一个电话号码，诱骗用户拨打该电话号码，这会导致用户设备的数据泄露。应对该威胁的解决方案是：对员工开展培训，告知他们不要拨打发送到他们设备的未知号码——就像警告他们警惕网络钓鱼电子邮件一样。谨慎对待可疑活动，可以在很大程度上保护企业移动设备的安全。

# 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

*安天实验室更多信息请访问：* http://www.antiy.com（中文）
http://www.antiy.net（英文）
*安天企业安全公司更多信息请访问：* http://www.antiy.cn
*安天移动安全公司（AVL TEAM）更多信息请访问：* http://www.avlsec.com