简译版

最新的移动安全威胁及其预防方法

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 Latest Mobile Security Threats and How to Prevent Them		
原文作者	乔治·普拉西斯（George Platsis）	**原文发布日期**	2020 年 6 月 15 日
作者简介	乔治·普拉西斯与私营、公共和非营利部门合作，帮助其解决战略、运营和培训需求。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/the-latest-mobile-security-threats-and-how-to-prevent-them/		
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。		

最新的移动安全威胁及其预防方法

乔治·普拉西斯

2020 年 6 月 15 日

最近几个月，新冠疫情大大增加了很多企业对移动功能的依赖性。随着越来越多的公司开始使用移动应用、虚拟专用网（VPN）和热点等，移动通信比以往任何时候都更加普及了。

鉴于我们对移动功能日益增强和前所未有的依赖性，每个人都应该关注移动安全——这不仅仅是安全专家的责任。

移动安全基础：与技术无关

“移动设备已迅速取代了家庭和工作场所中的个人计算机（PC）。”欧洲刑警组织（Europol）指出，“我们的手机或平板电脑实际上是微型计算机，因此应受到保护。与 PC 或笔记本电脑相比，他们面临相同甚至更多的威胁。”

尽管如此，我们却还在犯错。根据 Verizon《2020 年移动安全指数》报告，接受调查的公司中有 43%承认，出于权宜、便利或经济利益，或者缺乏预算或专业知识等原因，他们牺牲了安全性。

显然，领导者和团队成员之间存在脱节。企业需要从上到下，更好地理解和交流实现业务和安全目标需要做什么。但是，随着企业网络中的移动端点不断增加，出现安全漏洞的机会也在增加。

当今常见的移动威胁

处于 IT 安全行业内外部的公司——从 Kaspersky 到 CSO 再到 Business Matters——一致认为，2020 年移动安全威胁包括以下几类：

- 数据泄漏
- 不安全的 Wi-Fi
- 网络诈骗
- 网络钓鱼和社会工程学攻击

- 间谍软件
- 网络安全措施差，包括弱口令，不正确或不使用多因子身份鉴别（MFA）等。
- 技术控制不佳，例如不正确的会话处理，过时的设备、操作系统以及加密控制。

在大多数情况下，即使威胁不断演变，这些问题也是可以解决的。那么，为什么我们的网络仍然在遭受攻击呢？Verizon 报告指出："速度优于安全"。满足业务目标（无论是时间、资金还是避免繁琐的安全目标）的需要，通常是速度优于安全的主要原因。这就是安全运营中心经常被大量告警淹没的原因。

了解文化和风险至关重要

考虑一下：我们是为了便利和提高生产力，还是为了安全和风险最小化而设计移动应用呢？答案是便利和提高生产力。

同样的问题也适用于移动设备的使用。我们随身携带笔记本电脑、平板电脑和手机，不是因为它们不容易被攻击或风险低。实际上，移动设备很容易遭受攻击，使用它们会增加风险。我们使用移动设备（而且不像对固定设备那样对其进行保护）的原因是，它们能够使我们的生活更轻松并提高生产力。

因此，如何防止移动威胁损害企业及其数据，与选择何种技术解决方案无关。相反，这是一个供需关系以及权重分配问题。

优先考虑事项：从便利性到数据

为了降低移动应用的风险，改善移动安全状况，企业首先需要确定对各种移动功能的需求。我们说的是什么类型的功能呢——能作为权重的任何因素。

这些功能可能包括：

- 便利性
- 生产力
- 网络性能，包括负载、停机时间和升级。
- 业务部门之间的跨职能协同

- 数据可访问性，包括数据分类。
- 安全性
- 隐私性
- 成本和维护

给不同的影响因子分配权重并不容易。实际上，这需要企业的利益相关者参与进来，以确定每种功能如何满足业务需求并为其分配权重。

下一步是匹配供需。如果存在漏洞或风险，就进行应对和监控。

在应对风险时，没有完美的解决方案，只有满足需求的合适方案，尤其是在风险不确定的情况下，例如在网络安全中。因此，只有在处理了重大问题之后，才能部署策略。这些策略包括但不限于：

- 将应用程序列入黑白名单
- 使用自带设备（BYOD）vs 工作和个人使用设备完全隔离
- 网络限制和相关费用。例如，企业意识到向其所有员工发布热点的成本更高，但是愿意接受这一成本，以确保员工仅使用经过批准的网络设备，阻止其使用公共甚至家庭 Wi-Fi。
- 端点检测和监控功能 vs 隐私和网络性能挑战。
- 强制使用 VPN，这不能停留在书面上，而是要从技术上解决。
- 移动设备管理（MDM）平台配置，包括限制甚至终止使用某些或所有移动应用和功能。

“移动安全”几乎已经代表“安全”

鉴于我们大量使用移动设备，“移动安全”几乎已经代表“安全”了。无论哪个端点正在访问数据，企业都会面临相同的战略挑战。

关键是：为了确保安全的移动运营，企业需要研究一系列不一定是技术问题的问题。例如，5G 供应链可信吗？物联网（IoT）在生态系统中扮演什么角色？有哪些潜在的隐私责任？

相比每天休息几个小时的员工，始终在线的员工真的有更高的生产力吗？

移动安全问题很复杂。企业需要从简单的解决方案开始，例如掌握基础安全措施，了解业务需求并确定要承担的风险。解决了这些问题后，再解决其他问题就更加容易了。

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，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿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