

简译版 黑客瞄准移动支付应用，该如何防御？

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	As Hackers Target Mobile Payment Apps, Here's How to Keep Them at Bay		
原文作者	卡洛斯·亚松森 (Carlos Asuncion)	原文发布日期	2019 年 12 月 27 日
作者简介	卡洛斯·亚松森是 Shape Security 公司解决方案工程师经理。 https://www.darkreading.com/author-bio.asp?author_id=5341		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/theedge/as-hackers-target-mobile-payment-apps-heres-how-to-keep-them-at-bay/b/d-id/1336625		
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	<ul style="list-style-type: none"> 本译文译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。 		

黑客瞄准移动支付应用，该如何防御？

卡洛斯·亚松森

2019 年 12 月 27 日

零售商应保持警惕，以减少和预防三种最常见的移动应用诈骗。

消费者喜欢使用智能手机购买商品和服务。但是，随着越来越多的零售商发布带有 APP 内付款方式的移动应用，我们必须谨慎考虑诈骗威胁。提供移动应用进行 APP 内购买的零售商，应特别注意“无实体卡诈骗”（card not present fraud）。

假设有一家名为 Smoothie Shop 的沙冰店；其移动应用可以保存客户的信用卡信息，以方便 APP 内购买。这就为至少三种潜在的诈骗行为打开了大门。

在第一种情况下，诈骗者劫持现有的 Smoothie Shop 账户。由于该账户已在应用中保存了信用卡信息，诈骗者需要做的就是：走进 Smoothie Shop，向移动应用出示已保存的信用卡信息，就可以刷其他人的信用卡购买沙冰了。

在第二种情况下，诈骗者也是劫持 Smoothie Shop 账户，但是该账户未保存信用卡信息。这会促使诈骗者从暗网或其他电子市场购买被盗的信用卡信息，然后将获取的信用卡信息添加到 Smoothie Shop 账户和应用中。然后，他们就可以前往最近的商店，使用被盗的信用卡购买沙冰了。

为什么诈骗者更乐意劫持现有账户，而不是创建新账户来进行诈骗呢？这是因为精明的诈骗者知道，相比于全新账户，具有良好交易记录的、3-6 个月以上的“老”账户受到的审查更少。

最后，在第三种或更复杂的情况下，诈骗者使用僵尸程序工具（或人工点击）来创建数百个假的 Smoothie Shop 账户。一旦诈骗者可以访问多个假账户，他就可以根据需要添加任意数量的被盗信用卡进行 APP 内购买了。

那么，零售商和消费者应该如何保护自己呢？

防止账户劫持（ATO）

有很多方法可以防止或至少显著减少 ATO 的数量——例如防止“撞库攻击”（credential

stuffing)。企业的目标是，防止诈骗者从账户劫持中获得经济利益。如果劫持账户的成本/工作量超过了该账户的价值，那这对诈骗者来说就没有吸引力了，他们很可能会转向其他地方。

控制账户创建过程

我们可以使用验证码来限制僵尸程序和脚本创建账户的权限。但是，中等级别的诈骗者能够绕过这些功能，并且消费者也不怎么喜欢使用验证码。防止批量创建账户，需要收集设备级别的信息，以限制单个设备创建新账户的数量。迫使诈骗者使用多个设备可能会降低其回报率，使其转向其他地方。

确保客户未使用泄露的凭证登录

NIST 提出了一组有关身份鉴别和数字身份的建议，这些建议对于当今的数据泄露事件很有借鉴意义。使用已泄露凭证登录到店铺网站或移动应用的客户，最有可能被劫持账户和诈骗。

围绕信用卡滥用问题建立控制措施

合法客户可能需要在其账户/设备中添加一张（或两张）信用卡。任何试图添加第三张或更多信用卡的账户/设备都应受到仔细检查，并被限制添加信用卡。存储的信用卡也应绑定到设备而非账户。这样，如果诈骗者通过新设备劫持了账户，就无法利用存储的信用卡信息执行诈骗了。这需要在设备级别使用强大且唯一的标识符。

移动应用对客户来说更方便，而且能够刺激零售商的业务发展，因此消费者和零售商都有责任保护这些应用。零售商必须改善应用的开发和监控过程，以保护其客户并避免数据泄露，这一点很重要。毕竟，虽然使用移动应用购买商品很方便和有趣，但是如果不必担心信用卡信息被盗，那就锦上添花了。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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>