亚信安全 新闻稿
[即时发布]

零售行业 O2O 盛行　或成黑客窃取数据目标

零售业成金融卡信息泄密主要受害者　亚信安全提醒零售业者强化安全防御

【亚信安全】-【2015 年 11 月 26 日】O2O 等新型业态为传统零售业的转型带来了巨大的机遇，但与此同时，日趋严重的数据外泄风险却在阻碍着这一转型的实现。亚信安全近期发布的《跟着信息走》研究报告显示，零售业数据外泄占到了信用卡和银行卡资料泄密事件的 47.8%，其带来的巨大风险很有可能导致零售业者的转型失利。亚信安全建议，零售业者应该建立数据更加严密和主动的防御机制，包括终端安全、无线安全和数据中心数据、供应商网络接入监控等管控机制，防御以窃取数据为目标的 APT 攻击。

亚信安全的分析指出，PoS 机存储器窃取程序是零售业数据外泄事件的最主要诱因，该恶意程序能够让黑客匿名发动远程攻击，窃取受感染的 PoS 机存储的银行卡账号、消费记录等用户信息。一旦成功，黑客就可以利用这些窃取的信息复制信用卡，还可以用其进行身份诈骗或在地下黑色市场进行出售。

O2O 的盛行则给零售业的数据保护带来了更大的风险。在典型的 O2O 商业模型中，终端消费者通过手机 APP 提交消费需求，并完成订单确认、支付等一系列流程，消费者联系方式、在线支付账号等高价值数据也将随之存储到零售企业的数据库之中。由于服务流程从线下转移到了线上，因此黑客有更多的机会抓住网络服务中的漏洞，并窃取这些高价值数据。例如，黑客可以利用网络钓鱼等社会工程攻击方式，发动更复杂的针对性攻击，而不需要像以前那样在 PoS 机中植入存储器窃取程序。

亚信安全业务发展总监童宁指出：“零售业之所以成为黑客攻击的重点目标，主要是因为其携带了大量受地下市场欢迎的高价值数据，可以给攻击的发动者带来不菲的预期收益。而 O2O 业态不仅产生了更多的高价值数据，还降低了黑客发动数据窃取攻击的难度，因此，我们预计未来会有更多的零售业者陷入数据窃取的风险之中。”

一旦大规模的信息外泄事件真的发生，那么零售业者将陷入极大的困境之中。首先，这些外泄的个人信息将可能导致消费者的资金被窃取，给零售业者带来高额的赔偿或诉讼成本。更为致命的是，信息外泄事件将严重损害企业的品牌价值及商业声誉，让其在激烈的市场竞争中陷入不利的局面。在 2013 年发生的美国零售企业 Target 信息外泄事件中，黑客就窃取了高达 7000 万笔的用户信息，产生的直接损失就达到几亿美元。

毫无疑问，在网络安全上的预防措施上会比在攻击过后进行补救更有效，成本效益也更高。因此，零售业者需要充分认识到数据窃取威胁的严重性，并采取更加严密的网络安全防护措施。例如实行白名单机制，只允许特定的程序运行；定期修补系统并进行漏洞扫描；在系统管理端与客户端进行安全加固等。

针对黑客往往采取 APT 攻击来窃取数据的特点，亚信安全建议零售业者在公司网络中使用多层防火墙，并使用亚信安全深度威胁发现平台（Deep Discovery，DD）等具备入侵侦测功能的信息安全防护系统，对网络流量进行周密的侦测，及时发掘恶意的内容、通讯与行为，迅速响应攻击者，并在网络、网关与终端进行进一步的拦截，以确保的企业的数字资产不因网络攻击而受损。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com