中国支付清算协会文件

中支协发〔2020〕193号

中国支付清算协会
关于加强防范ATM取款攻击的风险提示

各有关会员单位：

支付卡产业联盟安全标准委员会[1]和ATM行业协会[2]于2020年10月7日发布紧急公告称，ATM终端的现金取款安全性受到新的威胁——ATM取款攻击，中国支付清算协会对公告进行了编译，现对相关会员单位风险提示如下：

[1] Payment Card Industry Security Standards Council,简称PCI-SSC。该机构旨在通过提供数据驱动和安全解决方案，帮助企业检测、减轻和防止网络攻击和破坏，从全球领域的跨行业层面，提高支付环境安全。

[2] Automatic Teller Machine Industry Association,简称ATMIA。是代表全球自动取款机行业的非营利性行业协会。在全球70个国家的650家公司中，为1.1万名会员提供服务，会员包括金融机构、终端机部署商、设备制造商、程序供应商和增值服务商等。

一、运作原理

ATM 取款攻击是指犯罪分子入侵银行支付系统，操纵欺诈监测控制台，篡改客户账户余额、取款限额、交易记录等要素，达到在短时间内通过 ATM 机大量（在账户实际余额范围内）或超量（超出账户实际余额）取款的行为。

欺诈份子一般不直接攻击 ATM，而是通过网络钓鱼或社会工程学攻击等方式，在金融机构支付系统中注入恶意软件，获取系统管理权限，远程入侵并控制欺诈监测后台，解除取款次数和额度限制，篡改账户密码和余额，然后将创建的虚假账户或使用持有账户（以不正当方式获取的账户、借记卡或信用卡）分发给“跑腿人”，有序安排他们在指定的 ATM 终端按照计划安排取款。

银行类金融机构和非银行支付机构将面临大规模协同攻击的风险。此类攻击行为具有高度组织、精心策划、行动迅速的特点，风险损失可高达数百万美元，且覆盖面较广。

二、检测建议

在系统层面，对 ATM 取款攻击的检测建议包括：一是加强对底层账户交易金额、次数、周期、间隔等行为的监控；二是采用全天候监控功能，如文件完整性监控软件；三是及时预警，发现可疑行为后立即报告；四是开发并优化突发事件响应管理系统；五是检查非常规流量来源（如 IP 地址）；六是检查未经授权的网络工具使用情况。

三、预防措施

由于ATM取款攻击的攻击时间短、风险损失大，因此事前预防工作至关重要。建议采取以下措施:

（一）严格管理系统访问权限

对涉及账户余额、交易限制和访问权限管理的模块，尤其是提供支持和管理功能的系统设置多因素身份验证和多重核准机制。对具有访问权限的决策采取严密的系统隔离措施，保证没有任何一个用户ID可独立执行“敏感”功能。

（二）强化监测机制，定期开展系统安全检查

检查内容包括软件安全补丁更新、系统漏洞扫描、渗透测试、文件完整性检查、访问控制权限和访问权限使用历史等。

（三）重视系统预警信号

采用ATM取现攻击的犯罪分子，研究系统漏洞和制定攻击计划的周期可长达几月。金融机构应提高对系统检测预警信号的重视程度。

（四）选择可信软件供应商

构建完整的软件安全机制，保证软件供应商能提供可持续性优化更新服务。

（五）严格遵守PCI数据安全标准

PCI数据安全标准是在全球范围内，在业内专家的实践研究中制定出的国际标准，内容涵盖多因素身份验证、安全补丁更新、文件完整性监控等内容，可辅助发现ATM取现攻击。

（六）加强内部管理

建设或优化员工监控系统，防止“监守自盗”；对员工开展持续性反网络钓鱼培训；设置强口令，并严格密码管理工作。

中国支付清算协会

2020年10月29日

中国支付清算协会秘书处　　2020年10月30日印发