

万事达卡境外批量盗刷

事件分析



关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85% 头部互联网企业，每年帮助客户减少数十亿资金损失。

目 录

关于威胁猎人	2
一、多家银行短时间内集中出现异常交易	4
二、攻击者使用的技术手段分析	6
2.1 黑产疑似通过枚举或批量试探获取 DPAN	7
2.2 将 DPAN 当作普通 PAN 进入无卡支付流程	8
2.3 利用缺少持卡人认证的交易场景，降低盗刷阻力	8
三、总结	9

2026 年 9 月 25 日前后，多名境内万事达卡持卡人陆续反馈，在本人未出境、未发生相关消费且实体卡始终在身边的情况下，突然收到来自巴西等境外地区的异常交易提醒，部分交易发生于凌晨，金额达到数千巴西雷亚尔，涉及巴西雷亚尔、乌拉圭比索等币种，交易记录中部分显示与 Apple Pay 相关。

随着相似案例集中出现，公开信息显示，此次异常交易并非局限于单一银行或单一卡种，多家发卡机构的万事达信用卡均出现未经授权的境外消费；其中部分交易被银行风控系统及时拦截，也有部分已成功入账，并进入后续核查及资金处置流程。

当“人在家中坐，账单海外来”再次出现，威胁猎人同步展开专项情报调研。本报告将围绕此次万事达卡境外盗刷事件，**重点分析攻击者可能使用的技术手段，并结合支付通道利用及境外盗刷变现等环节的实际活动**，还原本次信用卡盗刷事件可能经过的完整攻击链路。

一、多家银行短时间内集中出现异常交易

从威胁猎人目前监测到的公开反馈来看，此次异常交易在 9 月 25 日至 26 日期间迅速集中暴露，以下是事件相关时间线：

万事达卡境外盗刷事件时间线

基于监测与公开反馈整理，仅反映事件公开进展



截至2026年9月29日，威胁猎人共收集169篇相关公开贴文，并对其中支付截图进行逐图核对，共形成143笔可编码金额事件。

现有样本显示，本次异常交易主要集中在9月26日前后；不同币种之间存在较明显的金额分层，其中57笔巴西雷亚尔交易中，3,000—5,000 BRL区间最多，共26笔，而27笔英镑交易中，有25笔金额不超过1英镑，此外还出现USD、UYU、PYG等多个币种。异常交易对应的商户名称也较为分散，覆盖个人姓名、支付平台、餐饮、药房、手机零售、网站及机构等多种类

型，暂未发现大量交易集中于单一商户。

整体来看，本次事件呈现出短时间集中爆发、多地区多商户分散交易以及金额明显分层等特征。其中，大量极小额英镑交易可能与支付凭证测活或支付通道测试有关，而巴西雷亚尔交易则更多集中于较高金额区间。



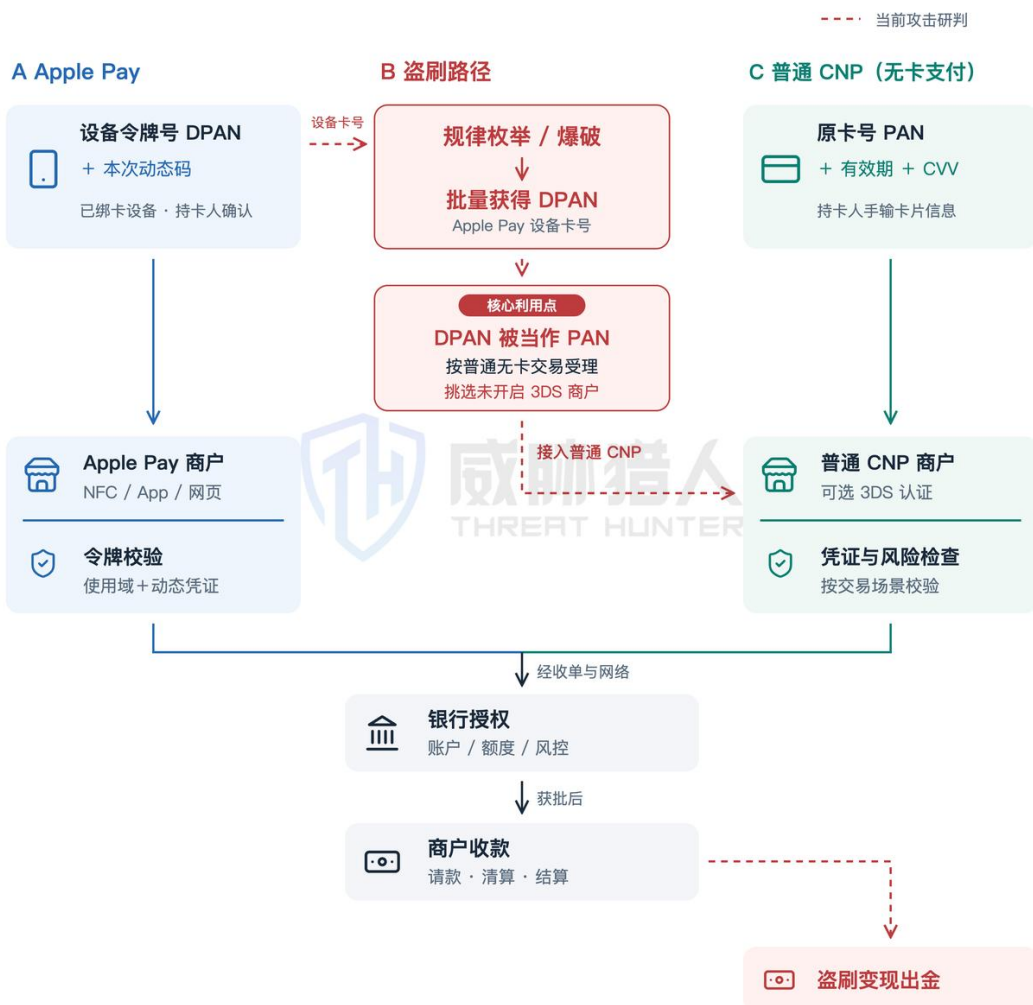
那么，在持卡人未出境、实体卡未离身的情况下，攻击者究竟可能通过哪些技术路径完成远程盗刷？下文将围绕这个问题展开分析。

二、攻击者使用的技术手段分析

结合目前公开测试披露及受害者交易信息，威胁猎人认为，本次事件值得重点关注的一条潜在攻击路径是：

攻击者疑似批量获取 Apple Pay 设备卡号 DPAN，并将其作为普通银行卡号提交至无卡支付渠道，在支付链路未有效执行 Token 使用范围及持卡人认证的情况下，完成未经授权交易。

盗刷攻击链路对比



需要强调的是，截至目前，相关机构尚未公布最终技术调查结论。以下攻击链路属于基于现有公开信息形成的技术研判，具体风险源仍有待进一步验证。

2.1 黑产疑似通过枚举或批量试探获取 DPAN

大规模同步盗刷的前提，是攻击者已批量掌握了可用于支付的卡片标识信息。与传统盗刷中“窃取原始银行卡号”不同，本次事件的关键起点指向 Apple Pay 的设备卡号（DPAN）。

银行卡绑定 Apple Pay 后，会生成设备卡号 DPAN。正常情况下，DPAN 需要在限定场景中配合动态交易凭证使用。

根据黑产相关社区披露，部分设备卡号疑似存在一定的分配规律。攻击者可能基于已知 BIN

或 Token Range 批量构造候选号码，再通过支付反馈筛选可用 DPAN。



2.2 将 DPAN 当作普通 PAN 进入无卡支付流程

本次事件的核心疑点，是 DPAN 与普通银行卡号之间的使用边界是否被有效执行。

正常 Apple Pay 支付中，DPAN 需要配合动态交易凭证使用，并经过 Token 使用范围和交易场景校验；普通 CNP（无卡支付）则通过商户网付入口提交银行卡号、有效期、CVV 等信息完成授权。

威胁猎人目前监测到的相关信息及测试反馈来看，部分 Apple Pay 设备卡号疑似可以脱离正常 Apple Pay 支付流程，通过普通无卡支付入口提交，并被作为普通 PAN 接受处理。也就是说，本应受 Token 使用场景限制的 DPAN，疑似能够被普通 CNP 支付链路作为银行卡号接受并进入后续授权流程。



2.3 利用缺少持卡人认证的交易场景，降低盗刷阻力

在上述攻击手法下，攻击者还会进一步需要寻找认证要求较弱的交易环境。

例如：

1. 未启用或未强制执行 3DS 身份认证；
2. 未有效检查 CVV 等

当商户侧缺少强认证，同时支付链路又未有效校验 CVV、Token 使用范围或动态交易凭证时，仅凭 DPAN 与有效期等有限信息，也可能进入后续授权流程。

因此，攻击者利用的可能是多个环节叠加形成的校验缺口：商户端缺少额外认证，支付处理环节未有效限制 DPAN 的使用场景，最终交易又通过了发卡行授权。

三、总结

本次事件反映出的核心风险，并不只是单笔信用卡盗刷本身，而是**数字钱包凭证在脱离原有支付场景后，是否仍可能被其他支付链路接受和授权**。如果这一边界确实存在被绕过或者被爆破的情况，其风险将从传统的卡号泄露问题，进一步扩大为数字钱包令牌使用范围与无卡支付认证

机制之间的衔接问题。

目前仍有几个关键问题有待进一步验证，包括攻击者如何批量获得 DPAN、具体哪个支付环节未有效限制 Token 使用范围，以及小额测试与后续较高金额交易之间是否存在明确关联。

后续威胁猎人将持续关注相关异常交易背后的收单机构、支付通道、认证方式及交易关联特征，以进一步还原此次事件的完整攻击链路。



关注“威胁猎人”

公司官网: www.threathunter.cn

合作邮箱: Marketing@threathunter.cn