中国银联仿冒钓鱼基础设施调查报告

Vincent Yang
OwO Network, LLC / NOC

2026 年 5 月 6 日

正式事件调查报告

摘要

本文记录一起高置信度银行卡钓鱼事件。攻击者通过仿冒“中国银联”的短信，引导受害人访问 https://up.cnpayglobal.com/。事件发生于受害人在日本〒 104-0061 东京都中央区银座 3 丁目 3-13 附近消费之后，坐标约为 35.6728586, 139.7624018。钓鱼网站收集银行卡验证信息和短信一次性验证码；页面交互后，受害人收到银行关于人民币 11,987.95 元网上支付的验证短信。受害人还观察到，点击获取验证码后页面保持加载或转圈状态约 1 至 2 分钟；该现象符合实时中继流程特征，也可能意味着后台人员正在手动使用提交的银行卡信息进行下游消费。该判断目前仍为调查假设，并非已证实事实。技术分析显示，主要诱导域名及关联基础设施属于托管在 104.225.145.101 的域名集群，该 IP 与 IT7 Networks Inc / AS25820 相关。钓鱼网站还呈现出与 Vite.js 构建的 Web 应用一致的实现特征。RDAP 记录显示，该域名集群普遍使用 NameSilo 注册商、DNSOWL nameserver 和 PrivacyGuardian 隐私保护。

关键词：钓鱼攻击；中国银联仿冒；短信发送方标识伪造；银行卡欺诈；RDAP；NameSilo；AS25820

1 事件概述

表 1: 案件元数据

字段	内容
报告日期	2026-05-06
事发时间窗口	2026-05-05，在银座现场消费后不久；银行支付验证短信随后出现（以受害人设备本地时间为准）
事发地点	日本〒 104-0061 东京都中央区银座 3 丁目 3-13 附近；坐标 35.6728586, 139.7624018
主要钓鱼 URL	https://up.cnpayglobal.com/
根域名	cnpayglobal.com
观察到的托管 IP	104.225.145.101
网络 / ASN	IT7 Networks Inc / AS25820
资产来源	749079eec0_202605060859 资产数据.csv
RDAP 查询时间	2026-05-06 16:12 UTC

受害人在日本〒 104-0061 东京都中央区银座 3 丁目 3-13 附近消费后不久，收到仿冒“中国银联”的短信。短信声称受害人的信用卡境外支付功能已关闭，并要求通过 https://up.cnpayglobal.com/ 重新认证。该网站展示仿银联的银行卡认证界面，并要求填写银行卡号、CVV/CVN2、有效期、手机号和短信验证码等敏感信息。

受害人点击获取验证码后，页面保持加载或转圈状态约 1 至 2 分钟。该延迟符合实时中继或人工辅助欺诈流程的特征。一种合理的调查假设是，后台人员可能正在将受害人提交的银行卡信息手动输入到下游消费流程中，例如机票或酒店订单；这类流程也可能与常见的低价机票、酒店代购欺诈相关。该判断基于页面行为和随后出现的银行支付验证短信，不能直接证明具体下游商户或消费类别。

钓鱼页面右上角显示 English 选项，但受害人观察到点击无效。结合中文短信诱导、银联主题页面和中文交互流程，该特征支持本次活动主要面向身处日本的中文用户或中国银联持卡人的判断。

短信发送方标识被仿冒，且事件与银座现场消费在时间和地点上高度相关，因此符合短信发送方标识伪造或伪基站活动的特征。但该判断仍属于基于受害端证据的推断；若要最终确认短信投递机制，需要运营商侧日志或执法机关调取的电信记录。

2 证据

以下截图为主要受害端证据，分别记录诱导短信、银行支付验证短信、钓鱼落地页和银行卡信息收集表单。

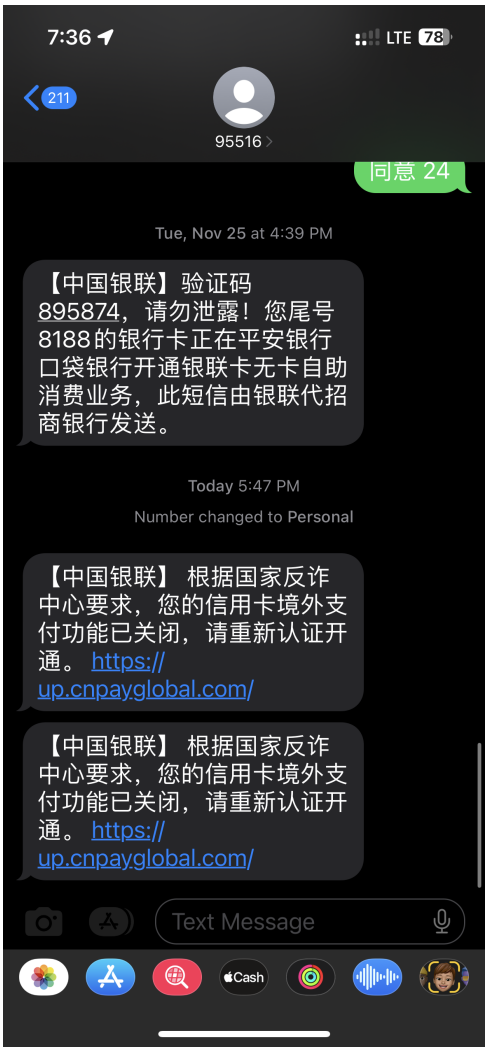

图 **1:** 仿冒中国银联的短信诱导信息，其中包含 `https://up.cnpayglobal.com/`。

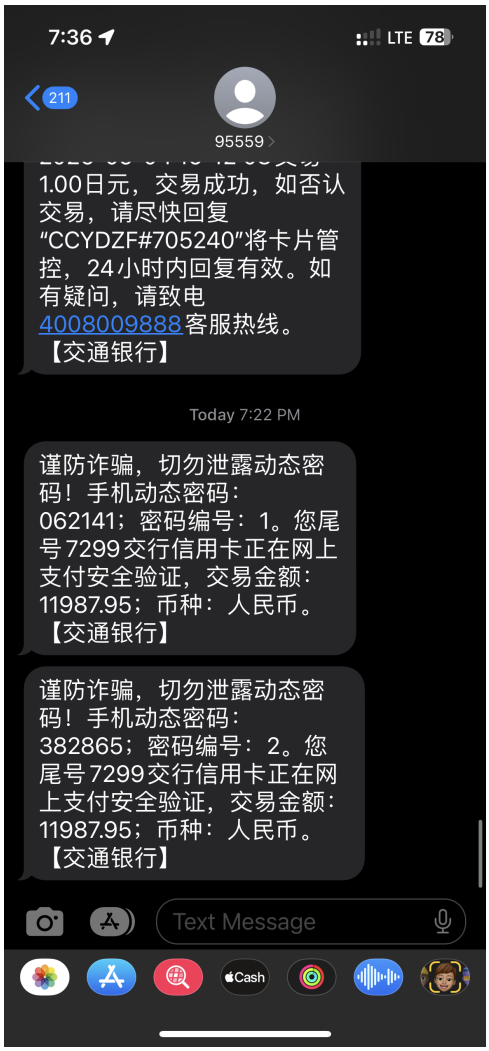

图 **2:** 银行短信显示人民币 11,987.95 元网上支付验证请求。

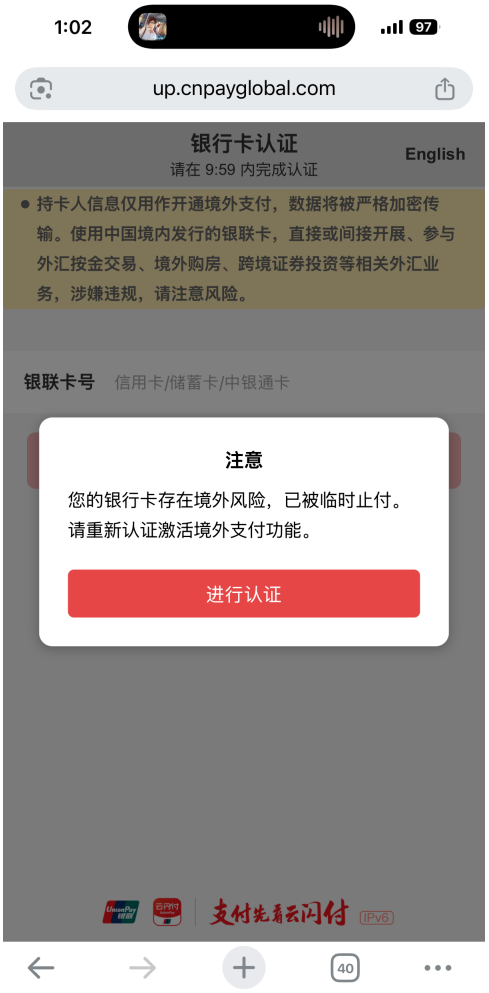

图 3: up.cnpayglobal.com 钓鱼落地页展示仿银联银行卡认证弹窗。

图 4: 银行卡信息和 OTP 收集表单要求输入 CVN2/CVV、有效期、密码、手机号和短信验证码。

3 攻击链分析

根据现有证据，攻击链可概括如下：

1. 受害人在日本〒 104-0061 东京都中央区银座 3 丁目 3-13 附近完成消费。
2. 受害人收到仿冒中国银联的短信。
3. 短信诱导受害人访问 https://up.cnpayglobal.com/。
4. 钓鱼页面要求输入完整银行卡验证数据和短信一次性验证码。

5. 获取验证码后页面加载约 1 至 2 分钟，疑似攻击者在后台实时中继或人工对接真实支付流程。

6. 一种合理的调查假设是，提交的银行卡信息被人工用于下游消费，例如机票或酒店订单；该点尚未被独立证实。

7. 钓鱼页面右上角 English 按钮点击无效，说明该流程更可能主要面向在日本的中文用户。

8. 受害人随后收到银行短信，提示一笔人民币 11,987.95 元的网上支付验证。

9. 受害人确认该网站为钓鱼网站，并已向注册商、注册局和托管网络举报。

4 基础设施指标

4.1 主要指标

表 2: 主要失陷指标

指标	值
主要诱导主机	`up.cnpayglobal.com`
根域名	`cnpayglobal.com`
托管 IP	`104.225.145.101`
观察到的 Web 构建框架	Vite.js
ASN	`AS25820`
网络名	IT7NET
注册商	NameSilo, LLC
注册商 IANA ID	1479
注册商 abuse 联系方式	`abuse@namesilo.com`
IP/ASN abuse 联系方式	`abuse@sioru.com`
Nameserver	`NS1.DNSOWL.COM`; `NS2.DNSOWL.COM`; `NS3.DNSOWL.COM`

4.2 FOFA 资产数据

供应的资产文件包含 27 行数据（含表头）。下表汇总了在 `104.225.145.101` 上观察到的去重关联主机。

表 3: 基于 FOFA 数据的 104.225.145.101 钓鱼基础设施

主机	端口	页面标题	根域名
cn.lianhezf.com	80 / 443	银行卡认证	lianhezf.com
cn.up-hwrz.com	80 / 443	银行卡认证	up-hwrz.com
cn.yinlianasia.com	80 / 443	银行卡认证	yinlianasia.com
cn.uphwzf.com	80 / 443	银行卡认证	uphwzf.com
cn.yinlianworld.com	80 / 443	银行卡认证	yinlianworld.com
cn.jingwaizf.com	80 / 443	银行卡认证	jingwaizf.com
zgyinlian-zf.com	80 / 443	银行卡认证 / 400	zgyinlian-zf.com
cn.uprenzheng.com	80 / 443	银行卡认证	uprenzheng.com
cn.upjprz.com	80 / 443	银行卡认证	upjprz.com
zhifu-oversea.com; cn.zhifu-oversea.com	80 / 443	银行卡认证 / 空	zhifu-oversea.com
104.225.145.101	80 / 443 / 888 / 22	银行卡认证 / 400 / 403	无

5 RDAP 和 WHOIS 结果

表 4 的注册时间主要采用 Verisign 注册局 RDAP。NameSilo 注册商侧日期有时会显示为前一日，这是注册商侧归一化日期与注册局精确 UTC 时间戳之间的差异。

表 4: 域名 RDAP 摘要

域名	查询时状态	注册时间	到期时间
cnpayglobal.com	client transfer prohibited	2026-05-05 01:35:56 UTC	2027-05-05 01:35:56 UTC
lianhezf.com	client transfer prohibited	2026-04-02 03:45:27 UTC	2027-04-02 03:45:27 UTC
up-hwrz.com	client transfer prohibited	2025-12-20 05:55:48 UTC	2026-12-20 05:55:48 UTC
yinlianasia.com	client hold; client transfer prohibited	2026-04-21 03:27:59 UTC	2027-04-21 03:27:59 UTC
uphwzf.com	client transfer prohibited	2025-12-25 08:15:20 UTC	2026-12-25 08:15:20 UTC
yinlianworld.com	client hold; client transfer prohibited	2026-04-04 03:08:18 UTC	2027-04-04 03:08:18 UTC

域名	查询时状态	注册时间	到期时间
jingwaizf.com	client hold; client transfer prohibited	2025-11-19 08:25:35 UTC	2026-11-19 08:25:35 UTC
zgyinlian-zf.com	client transfer prohibited	2025-11-22 17:22:02 UTC	2026-11-22 17:22:02 UTC
uprenzheng.com	client hold; client transfer prohibited	2025-12-13 04:15:48 UTC	2026-12-13 04:15:48 UTC
upjprz.com	client hold; client transfer prohibited	2025-12-13 04:24:00 UTC	2026-12-13 04:24:00 UTC
zhifu-oversea.com	client hold; client transfer prohibited	2025-12-06 03:07:12 UTC	2026-12-06 03:07:12 UTC

表 5: 注册商和 DNS 共性模式

字段	观察值
注册商	NameSilo, LLC
IANA Registrar ID	1479
注册商 support	support@namesilo.com
注册商 abuse	abuse@namesilo.com; +1.480.524.0066
隐私保护服务	PrivacyGuardian.org / See PrivacyGuardian.org
隐私保护记录中的常见电话	+1.3478717726
DNS 服务商	DNSOWL
DNSSEC	未进行 delegation signing

表 6: 104.225.145.101 的托管 RDAP 摘要

字段	值
Network handle	NET-104-225-144-0-2
地址段	104.225.144.0–104.225.159.255
Network name	CL-104-225-144-0-20
类型 / 状态	Assignment / active
IP 注册主体	IT7 Networks Inc
IP 注册主体地址	530 W 6th Street, Los Angeles, CA 90014, United States
关联注册主体	Cluster Logic Inc
Abuse 联系方式	abuse@sioru.com; +1-408-260-5757
NOC / 技术 / 管理联系	arin-noc@sioru.com; arin-tech@sioru.com; arin-admin@sioru.com

表 7: AS25820 的托管 RDAP 摘要

字段	值
AS number	AS25820
AS name	IT7NET
状态	Active
注册主体	IT7 Networks Inc
注册主体地址	4974 Kingsway Ave, Suite 668, Burnaby, BC V5H 4M9, Canada
Abuse 联系方式	abuse@sioru.com; +1-408-260-5757
NOC / 技术 / 管理联系	arin-noc@sioru.com; arin-tech@sioru.com; arin-admin@sioru.com

6 分析结论

综合判断，该事件为高置信度仿中国银联银行卡钓鱼攻击。主要依据如下：

1. 短信仿冒中国银联，并诱导访问非官方的新注册域名。
2. cnpayglobal.com 注册于 2026-05-05，与事件时间窗口一致。
3. 钓鱼页面要求输入 CVV/CVN2、有效期、手机号和短信验证码。
4. 页面交互后出现人民币 11,987.95 元真实银行支付验证短信。
5. 获取验证码后的 1 至 2 分钟加载延迟符合实时中继流程特征，也可能指向人工辅助的下游消费尝试。
6. English 按钮无效且主要交互路径为中文，支持“面向在日本中文用户或银联持卡人”的目标画像。
7. 钓鱼网站疑似使用 Vite.js 构建，该技术指纹可用于日志检索、文件系统取证和关联站点聚类。
8. FOFA 资产数据显示，同一 IP 上存在多个“银行卡认证”主题相似站点。
9. RDAP 记录显示注册商、DNS 服务商、隐私保护服务和托管 IP 存在高度重合。
10. 多个关联域名查询时已处于 client hold 状态，说明该集群可能已被部分 abuse 流程识别或处置。

7 已采取行动

受害人已经向 NameSilo 举报 `cnpayglobal.com`，并要求停止全部 DNS 解析。该事件也已提交给 `.com` 注册局 Verisign。受害人还通过 RDAP 查询到的 AS25820 / IT7 Networks abuse 联系方式提交了举报。

8 建议后续行动

建议要求 NameSilo 和 Verisign 对 `cnpayglobal.com` 设置 `client hold` 或等效暂停状态，复核并暂停关联域名，保全注册资料、账户登录记录和 DNS 变更日志，关联分析 Privacy-Guardian 和 NameSilo 账户元数据，并检索同账户、同付款方式、同登录 IP 或同隐私资料注册的更多域名。

建议要求 IT7 Networks、Cluster Logic 和 AS25820 停止 `104.225.145.101` 上的钓鱼内容，保全 Web server 日志、反向代理日志、SSH 日志、控制面板日志、后台操作面板日志、浏览器自动化痕迹、下游订单提交日志、客户记录和付款记录，识别并暂停控制该主机的客户，并排查相邻网段中相似的银联或境外支付钓鱼页面。由于该站点疑似使用 Vite.js 构建，处置方还应检索 Vite 构建产物、带哈希的 JavaScript 和 CSS 资源、source map 残留以及部署路径，以关联其他同源站点。

如果受害人输入过卡号、CVV/CVN2、有效期、手机号或验证码，应视为银行卡已泄露。建议发卡行立即换卡，在换卡前关闭线上、境外和非面对面支付能力，并保全人民币 11,987.95 元支付尝试的风控和授权日志，包括商户描述、设备指纹、交易渠道元数据，以及如存在则保全机票、酒店或旅行类商户线索。同时建议向手机运营商提交事件时间、地点和短信截图，要求调查银座附近是否存在短信发送方标识伪造或伪基站活动。

9 结论

综合短信证据、钓鱼页面截图、FOFA 资产数据、RDAP 记录和 Vite.js 实现指纹，可以确认以 `https://up.cnpayglobal.com/` 为核心的关联域名构成一组仿冒中国银联的银行卡钓鱼基础设施。获取验证码后的 1 至 2 分钟延迟，以及 English 按钮无效的中文交互流程，进一步支持“实时中继式欺诈”和“面向在日本中文银联用户”的判断。建议立即下线、保全日志，并由注册商、注册局、托管商、银行和运营商进行跨主体关联调查。

A 中文处置列表

`up.cnpayglobal.com`

cnpayglobal.com
cn.lianhezf.com
cn.up-hwrz.com
cn.yinlianasia.com
cn.uphwzf.com
cn.yinlianworld.com
cn.jingwaizf.com
zgyinlian-zf.com
cn.uprenzheng.com
cn.upjprz.com
zhifu-oversea.com
cn.zhifu-oversea.com
104.225.145.101