



CASE STUDY

Taking apart a smishing kit that beat SMS 2FA

Public-sector impersonation (threat intel) · Threat-intel investigation & kit reverse-engineering

Court-ready evidence & takedown package

Anonymised under NDA. Client and identifying details are withheld. PXL Security LTD · Sofia, Bulgaria · pxlsec.com



CASE STUDY

Taking apart a smishing kit that beat SMS 2FA

Sector	Public-sector impersonation (threat intel)
Engagement	Threat-intel investigation & kit reverse-engineering
Outcome	Court-ready evidence & takedown package

9 sensitive field types harvested by the kit	real-time OTP/PIN relay defeating SMS-2FA	0 data submitted to attacker infra
--	---	--

THE CHALLENGE

A smishing campaign impersonating a national e-services / fine-payment portal was harvesting payment and identity data. The goal was attribution and takedown evidence — without touching victims or submitting any data.

HOW IT UNFOLDED

1. Collected and hash-sealed infrastructure and the live page kit for chain-of-custody.
2. Reverse-engineered the single-page-app kit and mapped the victim funnel and the full set of harvested fields.
3. Identified real-time exfiltration over a same-origin websocket, with the hosting server itself acting as the operator backend.
4. Assessed capability: live PIN and OTP relay indicated an interactive operator defeating SMS-2FA and 3-D Secure in real time — a high-capability kit, not a static dump.
5. Clustered the infrastructure and attributed it to a phishing-as-a-service operation reused across multiple countries and lures.

KEY FINDINGS

High	Real-time OTP/PIN relay defeating SMS-2FA / 3-D Secure
High	Phishing-as-a-service kit reused across countries
Medium	Self-hosted collection backend behind a reverse proxy

IMPACT

Active, scaled theft of payment cards and identity data from citizens, with two-factor authentication bypassed in real time.

OUTCOME

Hashed, court-ready evidence and multi-party takedown packages (registrar, hosting, national CERT, browser blocklists, certificate authority) suitable for law-enforcement handover. All analysis was retrieval-only — no data was ever submitted to the attacker's infrastructure.

TECHNIQUES

Kit reverse-engineering · Threat intelligence · OTP/2FA-relay analysis · Chain-of-custody · Attribution

SERVICES

Vulnerability Research & Exploit Dev · Red Teaming

Work with PXL Security

Independent offensive-security testing since 2014 — penetration testing, red teaming and secure development, delivered by senior engineers with evidence for every finding and a retest to prove the fix.

Request a proposal: pxlsec.com/contact · hello@pxlsec.com

PXL Security LTD · 12 Vasil Levski Blvd., 1142 Sofia, Bulgaria · VAT BG203239331