THREAT INTELLIGENCE & INCIDENT RESPONSE CASE STUDY

Anatomy of a Multi-Stage Task Scam & Infrastructure Attribution

Author: Gethyn (LeafoSec)

Classification: Open-Source Intelligence (OSINT) & Triage

Scope: Passive Reconnaissance & Deception Analysis

1. Executive Summary

This case study examines a live employment/task scam vector targeting a civilian user (k2dance). By combining human incident response, passive open-source intelligence (OSINT), and infrastructure analysis, this investigation maps out the full lifecycle of a modern financial fraud operation.

Rather than isolating the incident as a simple phishing message, the analysis uncovers a coordinated multi-layered operation leveraging brand hijacking of a legitimate UK craft shop, synthetic social proof, custom fraudulent logistics infrastructure (globalexpress7), and a shared multi-tenant backend server exposing critical administrative vulnerabilities.

2. Initial Vector & Brand Impersonation

The attack initiated via Telegram through an operator utilizing a synthetic burner persona ([Threat Actor Alias] / @Emily8899168). The lure promised a remote position offering a daily salary of £30–£50 with "no investment required," masking underlying money-mule mechanics by framing it as distributing wages to "other apprentices."

> **Brand Masking:** The threat actors explicitly weaponized the corporate identity of *TA AND MHT ONLINE LTD*, a registered UK entity operating the *Tegen Accessories* brand based in Brighton. Casual victims performing quick web checks encounter a real, established business, lending false legitimacy to the fraud.

3. Psychological Priming & Escalation Mechanics

The syndicate employed classic social engineering frameworks to manipulate the victim through distinct operational phases:

- **Micro-Transaction Priming:** The victim received multiple small fund transfers (£5 to £18) upfront. This normalization technique builds false trust and masks the illicit origin of the cash.

- **Synthetic Social Proof:** A TikTok video featuring an individual performing craft work was provided to establish human reality and operational safety.
- **Escalation & Boundary Testing:** The scammers introduced friction by demanding the victim handle secondary logistics payments and build social media syndication channels.
- **The Money Mule Conversion:** The final trap involved routing a large lump sum through the victim's personal account, requiring them to disburse payments to purported "other hires" while retaining a cut—effectively attempting to convert the victim into an unwitting money mule.

4. Incident Response & Human Triage

Upon identifying active indicators of compromise, structured containment protocols were executed:

- **Severing Communication:** The victim was advised to cut all contact immediately as the scammers transitioned to aggressive phone harassment.
- **Financial Containment:** The victim was instructed to immediately notify their financial institution regarding compromised card details.
- **Industry Collaboration:** Intelligence artifacts and screenshots were shared directly with the genuine, impersonated craft enterprise to coordinate an ongoing defense.

5. Passive Reconnaissance & OSINT Methodology

Operating under strict passive intelligence-gathering rules (avoiding any active disruption or intrusive hacking), the following OSINT workflow was executed:

Username & Profile Enumeration

Automated cross-platform enumeration was performed using **Sherlock** via a mobile terminal environment (Termux) targeting the operator's specific alias (`@Emily8899168`).

```
[*] Checking username @Emily8899168 on:
[+] AniWorld: https://aniworld.to/user/profil/@Emily8899168
[+] Blipfoto: https://www.blipfoto.com/@Emily8899168
[+] BoardGameGeek: https://boardgamegeek.com/user/@Emily8899168
[+] Chaos / YouTube / Mastodon instances...
[*] Search completed with 17 results (Single-use burner profile footprint confirmed)
```

Biometric and AI-powered reverse image searches confirmed that profile imagery was synthetic/stolen and completely decoupled from any verified personal identity.

Infrastructure & Network Pivoting

Investigation into the fraudulent logistics portal (`globalexpress7`) revealed matching DNS routing patterns, certificate details, and template structures shared with parallel scam rings abusing UK business registries.

6. Infrastructure Attribution & The "Cardboard Castle"

Pivoting from domain intelligence to infrastructure discovery uncovered the underlying hosting mechanics:

- **Target IP Discovery:** Mapping the domain resolved to core hosting infrastructure located in Bangkok, Thailand (`43.152.234.82`).
- **Shodan Analysis:** Querying the IP via Shodan revealed an exposed Remote Desktop Protocol (RDP port 3389) alongside multi-tenant Microsoft IIS and Nginx web servers.
- **The Scam Panel Factory:** Alternate ports exposed a modular array of administration panels featuring localized templates and multi-language support (including Chinese-language headers for logistics management platforms, alongside UK banking and numbering administration portals).
- **Technical Contrast:** This exposure highlighted a glaring contradiction—while projecting the slick, high-tech facade of a global logistics enterprise, the backend infrastructure operated as a brittle, misconfigured virtual server with poor administrative isolation.

7. Prevention & Defensive Takeaways

Task scams rely heavily on psychological pressure and velocity to prevent critical thinking. This case highlights key preventative measures:

- **Independent Verification:** Cross-referencing employers directly via official registries (such as Companies House) rather than trusting chat-provided links.
- **Infrastructure Auditing:** Checking domain registration timelines and reviewing technical threat feeds.
- **AI-Assisted Sanity Checks:** Integrating a quick query with an AI assistant or performing a structured review of job descriptions before sharing personal data can instantly expose anomalies and prevent financial exposure.

Published by LeafoSec | Ethical Threat Intelligence & Cybersecurity Research