Phishing Campaign Analysis Report (Redacted – Option B)

Author: Sławomir Cieślik
Date: December 2025
Report type: Technical / Analytical (DFIR / SOC)
Scope: Passive analysis only, no interaction with attacker-controlled infrastructure

Redaction notice (Option B): Domain names are preserved for contextual clarity, while specific URL paths, parameters, and backend endpoints have been removed. This document is intended for educational and portfolio purposes and follows responsible disclosure principles.

1. Executive Summary

The purpose of this report is to document a technical analysis of a suspicious email campaign observed in the wild, which attempted to lure recipients into interacting with a fake parcel tracking link. Detailed investigation confirmed that the campaign was designed to harvest user credentials by redirecting victims through a chain of intermediate domains to a phishing backend hosting a counterfeit login panel.

Although the campaign demonstrates relatively low technical sophistication, it still represents a credible threat to end users due to social engineering techniques, visual imitation of legitimate services, and the exploitation of routine user behavior related to shipment notifications.

2. Scope and Methodology

The analysis was conducted using a defensive DFIR-oriented approach and focused on understanding attacker infrastructure, application behavior, and potential impact, without performing any active interaction with the phishing backend.

Specifically, the investigation included inspection of the phishing email structure, review of embedded hyperlinks, observation of browser behavior during navigation, passive network traffic analysis using browser Developer Tools, and local decoding of encoded parameters encountered during redirection.

Actions such as form submission, credential entry, automated testing, fuzzing, or exploitation attempts were intentionally excluded to avoid interacting with or supporting attacker operations.

3. Analysis Environment Preparation

All analysis activities were performed within an isolated virtual machine environment to minimize risk and maintain operational security. The virtual machine ran Windows 11 x64 and was hosted using VMware virtualization software.

Host-to-guest integration features such as clipboard sharing, drag-and-drop, and shared folders were disabled. A snapshot was created prior to analysis to allow rapid rollback in case of unexpected behavior.

Network traffic was observed passively. Browser Developer Tools were used for application-level inspection, while Wireshark was enabled on the host system to provide additional visibility into outbound traffic patterns.

4. Phishing Email Analysis

The phishing email was formatted using HTML and presented itself as a routine shipment tracking notification. The visual and textual cues were crafted to encourage immediate user interaction.

Closer inspection of the embedded links revealed that they were not associated with any known or legitimate logistics provider. Instead, the links pointed to externally hosted domains unrelated to parcel delivery services.

Domains observed during email analysis:
Lure domain: waterautomation.com
Intermediary redirector: zasobygwp.pl

5. Redirection Chain Analysis

Upon user interaction, the phishing link initiated a multi-stage redirection process. The initial request was directed to a lure domain, which subsequently forwarded the request through an intermediary redirector before attempting to load content from the phishing backend.

This layered redirection approach is commonly used to obscure the final destination, evade basic detection mechanisms, and complicate manual inspection by end users.

Phishing backend domain: admin.eastend.in

6. Backend Routing Anomaly

Initial attempts to access the phishing backend resulted in HTTP 404 responses, indicating either incomplete deployment or conditional routing logic. Further analysis revealed that modifying the URL structure—without changing the domain itself—caused a fully functional login panel to be displayed.

This behavior strongly suggests misconfigured routing rules on the backend, such as improper rewrite handling or hardcoded path dependencies. Such issues are frequently observed in hastily deployed phishing kits and indicate low implementation maturity.

7. Payload Analysis (Base64)

During one stage of the redirection process, a parameter encoded using Base64 was observed. Local decoding was performed to avoid external communication with attacker-controlled infrastructure.

The decoded content did not directly correspond to the visible plaintext URL, suggesting the use of simple obfuscation mechanisms. This technique is commonly used to track user clicks, identify sessions, or bypass basic filtering systems.

8. Technical Conclusions

Based on the collected evidence, the analyzed activity can be confidently classified as a credential harvesting phishing campaign. The attacker infrastructure consists of a lure domain, an intermediary redirector, and a phishing backend hosting a counterfeit authentication interface.

Despite its relatively low technical sophistication and visible implementation flaws, the campaign poses a genuine risk to less experienced or inattentive users.

9. Recommendations

It is recommended to report the identified domains to appropriate CERT or abuse response teams to facilitate takedown efforts. Organizations should consider blocking the domains at DNS or proxy level and continue educating users on recognizing phishing attempts, particularly those themed around parcel delivery.

10. Final Notes

This report was prepared for educational and portfolio purposes. All analysis activities were conducted using passive techniques only and adhere to ethical security research and responsible disclosure standards.