УДК 004.056:004.773.3

ПІДХІД ЦИФРОВОГО КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ПОВІДОМЛЕНЬ ЕЛЕКТРОННОЇ ПОШТИ

Шедін Д.А.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків,
Україна
тел. +38(099) 533-26-57

The increasing prevalence of cyber threats and phishing attacks in our daily lives has made it more crucial than ever to be vigilant about the emails we receive. Even though email services come with built-in security features, they are not always reliable. Analyzing the sender's domain and email headers is an additional way that helps clients quickly identify potential vulnerabilities and take appropriate action. The currently available external tools require more effort from the user to collect this information in one place and do not always show data in an easy-to-read format. My user-friendly and simple-to-install browser extension is the solution that allows to get this information without leaving the email client.

У сучасну епоху цифрових комунікацій, коли електронна пошта є невіддільною частиною нашого повсякденного життя, загрози, що поширюються нею, залишаються значною небезпекою, зростаючи майже на 30% щорічно [1]. Більшість поштових клієнтів мають вбудовані фільтри спаму, які автоматично визначають і переміщують сумнівні листи в спеціальний розділ або видаляють їх. Однак ці методи не завжди ефективні для виявлення складніших загроз, таких як ексфільтрація даних, підробка, шкідливе програмне забезпечення, фішинг та інші. Таким чином, зростає потреба в додаткових рішеннях, які можуть допомогти користувачам визначити потенційно ризиковані електронні листи.

Під час проведення досліджень при написанні кваліфікаційної роботи бакалавра було розроблене розширення для браузера з інструментом, яке надає інформацію про електронне повідомлення одразу у поштовому клієнті, не покидаючи його. Крім зручності, серед інших переваг розробки можна виділити легкість встановлення (використовуючи вебмагазин браузера), безпечність (дані передаються в зашифрованому вигляді та не зберігаються), можливість інтеграції мікросервісу до інших систем (на основі REST API).

Самий підхід базується на обробці та цифровому аналізі домену відправника, заголовків повідомлення та його контенту. На рисунку 1 представлений приклад відображення результатів для тестового повідомлення.

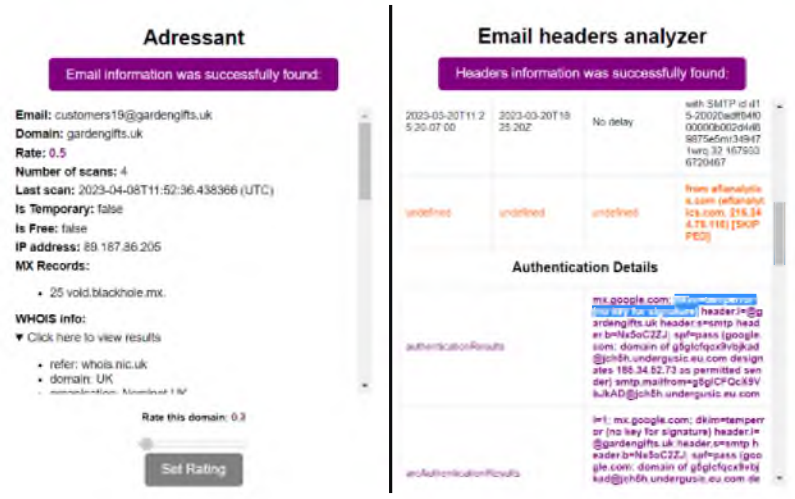

Рисунок 1 – Приклад застосування розширення

Як видно на рис. 1, інструмент складається з двох розділів: «Adressant» та «Email headers analyzer». Перший надає загальні дані про домен відправника, а саме:

- загальний рейтинг на основі досвіду користувачів;
- кількість сканувань та дата останнього;
- чи є він безплатним (тобто поштова адреса може бути вільно створена);
- чи є він тимчасовим (тобто самостійно знищується через певний час);
- IP адреса;
- MX записи (визначають сервер, відповідальний за отримання повідомлень електронної пошти від імені домену);
- WHOIS результати (реєстраційна інформація про власника домену).

Другий розділ дозволяє користувачу переглядати інформацію про:

- відправника та отримувачів;
- шлях повідомлення з моменту відправлення до його прибуття (базуючись на «Received» даних);
- результати автентифікації (DKIM, SPF, DMARC);
- деталі повідомлення та його контенту (ідентифікатори, посилання та інші)
- X-headers (додаткові нестандартні та невідсортовані заголовки).

Розширення автоматично виділяє потенційні вразливості та інші ключові деталі, тому може бути корисним як для звичайних користувачів, так і для спеціалістів з кібербезпеки та криміналістики.

Список використаних джерел:

1. ESET. (2023). ESET Threat Report T3 2022. WeLiveSecurity. https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf