

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК У ЕЛЕКТРОННИХ ЛИСТАХ

Вінницький національний технічний університет;

Анотація

У сучасному інформаційному середовищі фішингові атаки є одним із найпоширеніших та найнебезпечніших методів соціальної інженерії, що використовуються для викрадення конфіденційної інформації. Щороку кількість фішингових атак зростає, що призводить до значних фінансових втрат як для підприємств так і для звичайних користувачів. Кіберзлочинці постійно вдосконалюють методи маскування, тому звичайні методи захисту, такі як фільтрація спаму та чорні списки, не завжди працюють. У даній роботі досліджено основні методи виявлення фішингових листів, зокрема аналіз заголовків електронних повідомлень, перевірку URL-адрес та аналіз вкладень. Запропоновано підхід до автоматизованого аналізу електронних листів із використанням мови програмування Python та інтеграції з API VirusTotal і Google Safe Browsing.

Ключові слова: фішинг, кібербезпека, електронна пошта, аналіз заголовків, перевірка URL, автоматизація.

Abstract

In the modern information environment, phishing attacks are one of the most dangerous social engineering methods used to steal confidential information. The number of phishing incidents is increasing annually, leading to significant financial losses for both businesses and individual users. Attackers constantly improve their masking techniques, making traditional protection methods such as spam filtering and blacklists less effective. This paper explores the main methods for detecting phishing emails, including email header analysis, URL verification, and attachment inspection. An approach to automated email analysis using Python and integration with VirusTotal and Google Safe Browsing APIs is proposed.

Keywords: phishing, cybersecurity, email, header analysis, URL verification, automation.

Вступ

Одним із основних методів кібератаки є фішингові атаки, що спрямовані на викрадення облікових даних та отримання доступу до конфіденційної інформації. За результатами звітів міжнародних організацій з кібербезпеки, фішинг є найпоширенішою формою соціальної інженерії та складає понад 90% всіх кіберзлочинів. Зловмисники постійно вдосконалюють свої методи, використовуючи техніки підміни електронних адрес відправників, маскування URL-адрес, додавання шкідливих вкладень та соціальну інженерію. Це обумовлює необхідність розробки ефективних методів виявлення та блокування подібних атак [1].

Для виявлення фішингових атак проводиться аналіз заголовків електронних листів, що складається з перевірки механізмів автентифікації відправника, зокрема технологій для перевірки достовірності домену, цифрових підписів та автентифікаційних політик [2, 3]. У базах шкідливих сайтів, таких як VirusTotal і Google Safe Browsing перевіряються URL-адреси листів. Крім того, здійснюється аналіз вкладень, який перевіряє формат файлів та здійснює перевірку їхніх хешів для виявлення відомих загроз.

Результати дослідження

Під час дослідження було проаналізовано сучасні методи виявлення фішингових атак та можливості їх автоматизованої перевірки. Основну увагу приділено аналізу заголовків електронних листів, перевірці посилань на потенційно шкідливі ресурси та оцінці вкладених файлів щодо можливих фішингових загроз.

Для реалізації такого аналізу розглянуто можливість використання мови програмування Python [4], що має широкі можливості для обробки електронних листів та перевірки їх вмісту. Зокрема, досліджено сервіси VirusTotal [5] та Google Safe Browsing [6], які можуть бути використані для

перевірки посилань і файлів на наявність фішингових загроз. Схему роботи програмного засобу наведено на рис. 1.



Рисунок 1 – Схема роботи програмного засобу для перевірки електронних листів

Аналіз заголовків електронних листів дає змогу визначити підроблені адреси відправників, що використовуються для обману отримувачів. Перевірка URL-адрес дозволяє виявляти посилання, які ведуть на потенційно небезпечні ресурси, використовуючи бази даних шкідливих сайтів. Аналіз вкладень допомагає ідентифікувати підозрілі файли за їхніми гешами та форматами, що зменшує ризик зараження пристроїв користувачів.

Отримані результати можуть бути використані в подальшій розробці програмного засобу, що дозволить автоматизувати процес аналізу електронної пошти та підвищити рівень безпеки користувачів.

Висновки

Такий засіб дозволить в автоматичному режимі перевіряти електронні листи на наявність фішингових ознак. Це підвищить рівень захисту інформаційної безпеки користувачів та зменшить ризики викрадення даних. Подальші вдосконалення можуть бути спрямовані на впровадження методів машинного навчання для підвищення точності аналізу фішингових повідомлень, а також на розширення бази відомих загроз шляхом використання технологій спільного аналізу великих обсягів даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. APWG Phishing Trends Report [Електрон. ресурс] – Режим доступу: <https://www.apwg.org/trendsreport>
2. Штонда, Р., Черниш, Ю., Терещенко, Т., Терещенко, К., Цикало, Ю., & Поліщук, С. (2024). Класифікація та методи виявлення фішингових атак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 69–80. <https://doi.org/10.28925/2663-4023.2024.24.6980/>
3. Гарнага В. А. Neural networks in phishing attacks. Молодь в науці: дослідження, проблеми, перспективи 2023: Матеріали Всеукраїнської науково-практичної інтернет-конференції / Він. нац. техн. ун-т., Вінниця, 2023.
4. Welcome to Python. Python.org [Електрон. ресурс] – Режим доступу: <https://www.python.org/>
5. Google Safe Browsing API Documentation [Електрон. ресурс] – Режим доступу: <https://developers.google.com/safe-browsing>
6. Virustotal. How it works [Електрон. ресурс] – Режим доступу: <https://docs.virustotal.com/docs/how-it-works>

Ростецький Володимир Богданович — студент групи ІБС-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vova.rost777@gmail.com

Rostetskiy Volodymyr B. – student 1BS-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vova.rost777@gmail.com

Науковий керівник : Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk@vntu.edu.ua

Supervisor : Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical