УДК 004.056.5

Ю. В. Баришев
Є. С. Дремлюга

БІБЛІОТЕКА PYTHON ДЛЯ ОБФУСКАЦІЇ HTTP ТРАФІКУ

Вінницький національний технічний університет;

Анотація

Проаналізовано відомі методи та технології обфускації, що використовуються для захисту мережевого трафіку від несанкціонованого доступу та перехоплення. Розглянуто різноманітні сценарії використання бібліоттек Python для обфускації HTTP трафіку та її можливості в контексті забезпечення конфіденційності та безпеки даних. Запропоновано структуру та методику застосування цієї бібліотеки для захисту веб-застосунків та інших сервісів, що використовують HTTP протокол. Визначено ключові аспекти використання бібліотеки, включаючи її ефективність, надійність та можливості інтеграції з відомими системами.

Ключові слова: Python, обфускація, HTTP трафік, конфіденційність даних, безпека мережі.

Abstract

Existing obfuscation methods and technologies used to protect network traffic from unauthorized access and interception are analyzed. Various scenarios of Python libraries usage for the HTTP traffic obfuscation and its applicability in the context of ensuring confidentiality and data security are considered. The structure and method of using this library for the protection of web applications and other services using the HTTP protocol are proposed. The key aspects of the library's usage including its efficiency, reliability and possibilities of integration with existing systems are defined.

Keywords: Python, obfuscation, HTTP traffic, data privacy, network security.

Вступ

Сучасні веб-застосунки та сервіси все більше використовують HTTP протокол для обміну даними з клієнтами. Зростання цифрової активності породжує необхідність забезпечення безпеки та приватності інформації, переданої через мережу. У цьому контексті виникає потреба в ефективних засобах обфускації HTTP трафіку, які б забезпечували захист від перехоплення та аналізу даних.

Метою цієї роботи є покращення захисту конфіденційності HTTP трафіку шляхом розробки бібліотеки Python, яка забезпечує можливість його обфускації. Основний акцент зроблено на вивченні методів та алгоритмів, що використовуються для захисту передаваних даних від несанкціонованого доступу.

Досягнення поставленої мети передбачає аналіз ефективності розробленої бібліотеки в різних умовах та середовищах, а також її порівняння з відомими рішеннями. В результаті роботи очікується розробка інструменту, який дозволить розробникам забезпечити підвищений рівень безпеки під час обміну даними через HTTP протокол.

Результати дослідження

У результаті проведеного дослідження була успішно розроблена бібліотека Python, яка забезпечує можливість обфускації HTTP трафіку[1]. Ця бібліотека є інструментом для розробників, який дозволяє захистити дані, що передаються через HTTP протокол, від несанкціонованого доступу.

Основна функціональність бібліотеки полягає в обфускації HTTP запитів та відповідей, що дозволяє зберігати конфіденційні дані у безпечному вигляді під час їх передавання мережею. Бібліотека може взаємодіяти з різними API та виконувати обфускацію відповідно до специфікацій та потреб користувача.

Додатково, для забезпечення ефективності та гнучкості обфускації був розроблений HTTP WebSocket сервер. Цей сервер є проміжним рівнем, який з'єднує клієнтів WebSocket з REST API [2]. Роботу сервера та результат парсингу зображено на рис. 1

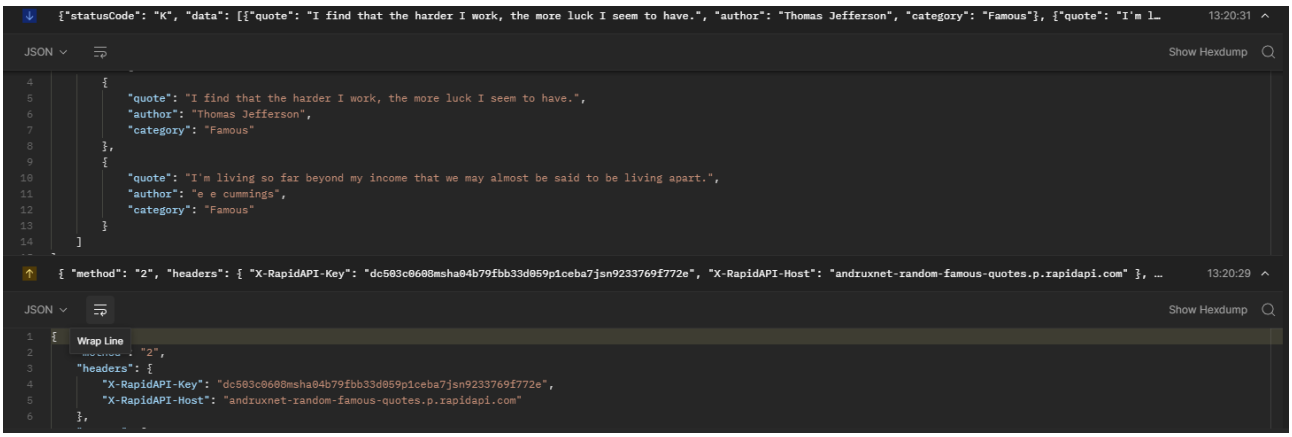

Рис. 1. Результат роботи парсера

Використовуючи цей підхід, вдалося покращити безпеку та конфіденційність шляхом інкапсуляції HTTP запитів у повідомлення WebSocket, що захищає прямий HTTP-трафік від можливого перехоплення.

Крім того, для зручності використання було реалізовано динамічний аналіз документації Swagger для відображення кінцевих точок API [3]. Приклад коду для налаштування кінцевих точок API показано на рисунку 2.

```
{
    "openapi": "3.0.0",
    "info": {
      "title": "Sample API",
      "description": "API for managing sample data.",
      "version": "1.0.0"
    },
    "servers": [
      {
        "url": "https://andruxnet-random-famous-quotes.p.rapidapi.com/",
        "description": "Production server"
      }
    ]
  }
```

Рис. 2. Налаштування динамічного аналізу документації Swagger

Це дозволяє здійснювати передавання даних у реальному часі та серіалізацію відповідей у різних форматах з мінімальними зусиллями від розробника. Такий підхід допомагає забезпечити ефективну роботу системи в умовах реального середовища.

Висновки

Результуючи виконану роботу, було успішно розроблено бібліотеку Python для обфускації HTTP трафіку, яка виявляє значний потенціал для підвищення безпеки та конфіденційності веб-застосунків. Ця бібліотека не лише дозволяє ефективно взаємодіяти з різними API, але й забезпечує зручний механізм перевірки ефективності обфускації даних. Розроблене HTTP WebSocket слугує проміжним рівнем між клієнтами WebSocket та REST API, що додає шар захисту і забезпечує безпечну передачу HTTP-трафіку від потенційного перехоплення.

Узагальнюючи, ця робота відкриває нові можливості для підвищення рівня безпеки веб-застосунків та оптимізації управління HTTP трафіком, сприяючи створенню більш захищених та ефективних мережевих з'єднань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Network Traffic Obfuscation: An Adversarial Machine Learning Approach / G. Verma та ін. *MILCOM 2018 - IEEE Military Communications Conference*, м. Los Angeles, CA, 29–31 жовт. 2018 р. 2018. URL: https://doi.org/10.1109/milcom.2018.8599680 (дата звернення: 08.03.2024).
2. Masse M. REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces. O'Reilly Media, Incorporated, 2011. 112 с.
3. Ponelat J. S., Rosenstock L. L. Designing APIs with Swagger and OpenAPI. Manning Publications Co. LLC, 2022. 424 с.

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Дремлюга Єгор Сергійович — студент групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: western.ant2@gmail.com

Yurii Baryshev — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.

Yehor Dremliuha — student of group 1BS-20b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: western.ant2@gmail.com.