УДК 004.056.5:004.89

Безуський Олексій Вікторович,

здобувач другого (магістерського) рівня вищої освіти Харківського національного університету радіоелектроніки

Бабич Матвій Геннадійович,

студент Харківського радіотехнічного фахового коледжу

Піксасов Михайло Михайлович,

к.т.н., доцент кафедри кібербезпеки Харківського національного автомобільно-дорожнього університету

ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ HTTP-ЗАПИТІВ ДЛЯ ЗАХИСТУ ВЕБЗАСТОСУНКІВ ВІД КІБЕРЗАГРОЗ

Анотація. Розглянуто підхід до підвищення захищеності вебзастосунків шляхом інтелектуального аналізу HTTP-запитів. Обґрунтовано доцільність поєднання сигнатурних методів виявлення атак, аналізу поведінкових характеристик мережевого трафіку та алгоритмів машинного навчання. Запропоновано функціональну структуру інтелектуальної системи, орієнтованої на виявлення потенційно небезпечних запитів, оцінювання рівня кіберзагроз і підтримку прийняття рішень щодо реагування на інциденти інформаційної безпеки.

Ключові слова: інформаційна безпека, кіберзагрози, HTTP-запити, вебзастосунки, машинне навчання, виявлення аномалій, аналіз мережевого трафіку.

Зростання кількості веборієнтованих інформаційних систем супроводжується розширенням поверхні атак і підвищенням вимог до забезпечення їхньої інформаційної безпеки. Одним з основних каналів взаємодії користувачів із вебзастосунками є протокол HTTP, запити якого можуть використовуватися для реалізації атак, спрямованих на порушення конфіденційності, цілісності та доступності інформаційних ресурсів. До поширених загроз належать SQL-ін'єкції, міжсайтове виконання сценаріїв (Cross-Site Scripting, XSS), несанкціоноване звернення до ресурсів, автоматизований підбір облікових даних та зловживання функціональними можливостями [1, 2].

Традиційні засоби захисту вебзастосунків, зокрема Web Application

Firewall (WAF), переважно використовують набори правил для ідентифікації відомих ознак атак. Незважаючи на ефективність такого підходу щодо типових кіберзагроз, його можливості можуть бути обмежені під час виявлення модифікованих атак і нетипових послідовностей запитів, які не відповідають заздалегідь визначеним сигнатурам. Це обумовлює доцільність застосування інтелектуальних методів аналізу, здатних враховувати не лише структуру окремого HTTP-запиту, а й особливості поведінки користувачів та характер взаємодії з інформаційними ресурсами [3, 4].

Метою роботи є обґрунтування підходу до побудови інтелектуальної системи аналізу HTTP-запитів, що забезпечує виявлення потенційних кіберзагроз на основі комплексного оцінювання структурних, змістових і поведінкових характеристик мережевого трафіку. Для досягнення поставленої мети запропоновано використовувати багаторівневий аналіз HTTP-запитів, який передбачає попередню обробку вхідних даних, формування інформативних ознак, виявлення відхилень від типової поведінки та визначення рівня потенційної небезпеки.

На етапі попередньої обробки здійснюється виділення основних характеристик HTTP-запиту. Додатково враховуються частота звернень до інформаційних ресурсів, повторюваність запитів, послідовність доступу до окремих сторінок і результати попередніх операцій. Використання зазначених характеристик дає змогу сформувати багатовимірне представлення мережевої активності для подальшого аналізу.

Основною особливістю запропонованого підходу є поєднання сигнатурного аналізу з інтелектуальним оцінюванням аномальності HTTP-запитів. Сигнатурний компонент призначений для виявлення відомих шаблонів атак, тоді як інтелектуальний компонент орієнтований на встановлення відхилень від характерних параметрів легітимної взаємодії з вебзастосунком. Така організація аналізу дозволяє враховувати як окремі

підозрілі конструкції у запитах, так і сукупність поведінкових ознак, які можуть свідчити про спроби реалізації кіберзагроз.

Для інтелектуальної класифікації HTTP-запитів доцільно розглядати алгоритми Random Forest, Gradient Boosting та методи виявлення аномалій, зокрема Isolation Forest. Вибір конкретного алгоритму повинен визначатися характеристиками навчальних даних, співвідношенням легітимних і шкідливих запитів, обчислювальною складністю та вимогами до оперативності виявлення загроз. Використання моделей машинного навчання створює можливість встановлення статистичних закономірностей, які складно формалізувати за допомогою фіксованих правил.

Функціонування інтелектуальної системи передбачає послідовне виконання операцій отримання HTTP-запиту, нормалізації даних, виділення ознак, сигнатурної перевірки та інтелектуального аналізу. На підставі отриманих результатів формується інтегральна оцінка потенційної небезпеки, відповідно до якої запит може бути віднесений до категорії легітимних, підозрілих або потенційно шкідливих. Для підозрілих запитів передбачається додаткова перевірка, тоді як запити з високим рівнем ризику можуть бути заблоковані відповідно до встановленої політики безпеки.

Важливим аспектом побудови системи є забезпечення можливості адаптації до змін характеру мережевого трафіку. Для цього доцільно передбачити накопичення результатів аналізу, перевірку коректності класифікації та періодичне оновлення інтелектуальної моделі на основі перевірених даних. Це дозволяє враховувати зміни поведінки користувачів і появу нових способів реалізації атак без необхідності повного перегляду архітектури захисту.

Таким чином, застосування інтелектуальних методів аналізу HTTP-запитів є удосконаленням засобів захисту вебзастосунків. Поєднання

сигнатурного виявлення відомих атак із машинним навчанням створює передумови для підвищення адаптивності систем захисту та розширення можливостей ідентифікації нетипової шкідливої активності. Подальші дослідження доцільно спрямувати на експериментальне обґрунтування вибору алгоритмів класифікації, оптимізацію набору інформативних ознак і визначення умов практичного застосування системи для аналізу HTTP-трафіку в режимі реального часу.

Список використаних джерел

1. OWASP Foundation. SQL Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.

2. Shaheed A., Kurdy M. H. D. B. Web Application Firewall Using Machine Learning and Features Engineering. Security and Communication Networks. 2022. Article ID 5280158. DOI: https://doi.org/10.1155/2022/5280158

3. Dawadi B. R., Adhikari B., Srivastava D. K. Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. Sensors. 2023. Vol. 23, No. 4. Article 2073. DOI: https://doi.org/10.3390/s23042073

4. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg : National Institute of Standards and Technology, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-94