УДК 004.656.2

Мосєвніна А. С., здобувач вищої освіти;
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ОГЛЯД ОБМАННИХ СИСТЕМ ДЛЯ ВИЯВЛЕННЯ АТАК ХАКЕРІВ, ЗАСНОВАНИХ НА МЕТОДІ АНАЛІЗУ ПОВЕДІНКИ ВІДВІДУВАЧІВ ВЕБСАЙТІВ ТА ІНШИХ ВІДОМИХ МЕТОДАХ ВИЯВЛЕННЯ АТАК ХАКЕРІВ

Ключові слова: обманні системи, методи аналізу поведінки, альтернативні методи захисту, поведінковий аналіз, вебсайти.

Вступ. У сучасному світі, коли віртуальний простір став невід'ємною частиною нашого повсякденного життя, кібербезпека стала критично важливою сферою для захисту даних та інформаційних ресурсів. Збільшення кількості кіберзагроз та атак хакерів у всесвітньому масштабі поставило завдання перед розробниками систем безпеки та дослідниками: як ефективно виявляти та запобігати цим загрозам? Один із важливих підходів до вирішення цієї проблеми – аналіз поведінки відвідувачів вебсайтів.

Актуальність. Актуальність теми обумовлена не лише зростанням кількості кіберзлочинів, але й їх складністю та різноманітністю. Обманні системи, які базуються на аналізі поведінки відвідувачів вебсайтів, змогу інноваційний підхід до цієї проблеми. Ці системи дають можливість не тільки виявляти атаки на ранніх стадіях, але і робити це з високою точністю. Тому огляд таких систем і методів стає надзвичайно актуальним для фахівців з кібербезпеки та розробників, які працюють над захистом вебресурсів та інформації в онлайн-середовищі.

Кіберзлочинці постійно вдосконалюють свої методи, але традиційні системи виявлення атак часто стають неефективними в умовах нових загроз. Навіть більше, досвідчені хакери намагаються щосили імітувати законну кіберповедінку, щоб залишатися непоміченими, а популярні вебсайти стають основними жертвами кібератак. Досвідчені зловмисники зазвичай імітують феномен натовпу, щоб вивести з ладу системи виявлення вторгнень (так званий флеш-натовп). Існує багато інших прикладів імітації атак, як-от розсилка спаму електронною поштою та вербування учасників бот-мереж [1].

Методи аналізу поведінки відвідувачів вебсайтів стали одним зі способів боротьби з такими імітаціями та атаками. Основна ідея полягає в тому, щоб виявити нестандартну або надзвичайну поведінку користувачів, яка може свідчити про потенційну загрозу. Це включає в себе виявлення незвичних *IP*-адрес, змін у швидкості перегляду сторінок, підозрілих запитів на сервер, інші відмінності в поведінці.

Один зі способів реалізації цього підходу – використання машинного навчання і штучних нейронних мереж. Інтуїтивно зрозуміло, коли справжня

поведінка користувача розпізнається, можна відповідно розрізнити неправильну та ненормальну поведінку. З цією метою машинне навчання найбільш підходить для виявлення кібератак на основі аналізу поведінки користувачів. Гіпотеза полягає в тому, щоб дізнатися типову поведінку користувача. Отже, система може ефективно виявляти аномальну поведінку, тоді як протоколи безпеки можуть подавати сповіщення про потенційну атаку [2]. Наприклад, якщо користувач зазвичай відвідує лише певні сторінки і раптово починає запитувати неіснуючі URL, це може бути ознакою атаки.

Ще одним із сучасних підходів до виявлення кібератак, заснованих на аналізі поведінки, є використання аналізу логів. Логи – це записи, які фіксують події, що відбуваються в системі. Вони можуть містити інформацію про різні події, які відбуваються в системі, зокрема дії компонентів і пристроїв, як-от вебсервери, бази даних і брандмауери. Рівень журналювання визначає, як багато інформації збирається і зберігається в журналах. Зазвичай текстові журнали призначені для читання людьми і містять позначки часу, які вказують, коли були створені записи у журналі [3]. Аналізуючи ці логи, можна виявити незвичайні або підозрілі дії, що можуть свідчити про потенційні атаки. Аналіз логів передбачає створення моделей, які описують нормальну поведінку системи і користувачів. Ці моделі можуть бути створені на основі історичних даних логів і можуть включати в себе різні параметри, як-от часові штампи, типи подій, користувачів, які здійснюють дії тощо. Потім система може відстежувати поточну поведінку системи і порівнювати її з цими моделями. Якщо система виявить відхилення від нормальної поведінки, вона може видаляти сигнали або сповіщати адміністратора про можливу кібератаку. Цей підхід дає змогу виявляти атаки, які можуть бути невидимими для традиційних методів виявлення, як-от антивірусні програми або фаєрволи.

Також існують системи, які аналізують не тільки технічні аспекти поведінки, але і психологічні. Вони враховують фактори швидкості набору тексту, мовний стиль та інші аспекти. Отже, ефективним способом перевірки біометричних властивостей користувачів може стати взаємодія користувача з певними пристроями, як-от клавіатура. Користувача можна навіть верифікувати на основі того, як він використовує певні додатки. Протягом останніх трьох десятиліть було проведено кілька досліджень з використання динаміки натискання клавіш для верифікації користувачів під час входу в систему та для вільного набору текстів. Було запропоновано використання миші для біометричної верифікації. Основною перевагою цього варіанта є його доступність без додаткових витрат, однак все ще існує низка проблем, які необхідно вирішити для того, щоб зробити метод оперативною технологією [4]. Ці психологічні та поведінкові аспекти аналізу можуть допомогти підвищити безпеку системи та зменшити ризик несанкціонованого доступу. Для успішного впровадження таких біометричних методів верифікації необхідно продовжувати дослідження та вдосконалювати технології для забезпечення їх надійності та ефективності.

Однак важливо пам’ятати, що жодна система виявлення атак не є абсолютною. Зловмисники постійно адаптуються до нових методів захисту, і

системи виявлення атак повинні також постійно розвиватися і оновлюватися. Тому для успішного виявлення та запобігання атакам необхідно вдосконалювати і підтримувати системи в актуальному стані.

Висновки

У цій роботі був проведений огляд обманних систем для виявлення атак хакерів, зокрема тих, що базуються на аналізі поведінки відвідувачів вебсайтів та інших передових методах виявлення атак. Сучасний кіберпростір вимагає ефективних рішень для захисту інформації та вебресурсів від небезпеки кіберзлочинів, і ця тема є надзвичайно актуальною.

Ці системи представляють інноваційний підхід, який дає змогу не лише виявляти атаки на ранніх стадіях, але і робити це з високою точністю. Вони використовують методи машинного навчання, аналізу логів і навіть психологічні аспекти для виявлення аномальної поведінки користувачів, що може свідчити про потенційну загрозу.

Огляд обманних систем для виявлення атак хакерів, заснованих на аналізі поведінки, відкриває широкий спектр можливостей для підвищення рівня кібербезпеки та захисту інформації. Розуміння цих методів і їх впровадження може сприяти більш ефективній боротьбі з кіберзлочинністю в сучасному цифровому світі.

Список використаних джерел

1. Yu S., Guo S., Stojmenovic I. Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace. *IEEE Transactions on Computers*. 2015. Vol. 64. № 1. P. 139–151. DOI: 10.1109/TC.2013.191.

2. Cyberattack Detection Framework Using Machine Learning and User BehaviorAnalytics / A. Alshehri, N. Khan, A. Alowayr, M. Y. Alghamdi. *Computer Systems Science and Engineering* 2023. № 44(2). P. 1679–1689. DOI: 10.32604/csse.2023.026526.

3. Kołodziej J., Repetto M., Duzha A. Cybersecurity of Digital Service Chains Challenges, Methodologies, and Tools. 2022. 267 p. DOI: 10.1007/978-3-031-04036-8.

4. Identity theft, computers and behavioral biometrics / R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafic, A. Camtepe, B. Lohlein, U. Heister, S. Moller, L. Rokach, Y. Elovici. *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics, ser. ISI'09*. Piscataway, NJ, USA: IEEE Press, 2009. P. 155–160.