УДК 004.49

АНАЛІЗ ЗАСОБІВ МОНІТОРИНГУ БЕЗПЕКИ ДОМЕННИХ ІМЕН ТА IP АДРЕС

ANALYSIS OF DOMAIN NAME AND IP ADDRESS SECURITY MONITORING TOOLS

Анастасія Омельчук, Леся Булатецька

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

***Abstract**. Collecting and analyzing data about domain names and IP addresses helps to detect cyber threats. A service like AbuseIPDB provides tools for this. Additionally, Shodan and VirusTotal allow for detecting hosts on the Internet and analyzing files for malware, enabling quick response to threats.*

Основні методи виявлення загроз доменних імен та IP-адрес включають: моніторинг реєстрації нових доменів для виявлення потенційних фішингових сайтів; перевірку WHOIS-інформації для виявлення підозрілих доменів; використання систем для блокування доступу до відомих шкідливих IP-адрес і доменів; встановлення правил на рівні DNS для блокування небезпечних доменів; моніторинг мережевого трафіку для виявлення підозрілих підключень; застосування автоматизованих систем для блокування потенційних загроз; аналіз журналів для виявлення незвичайної активності. Ці методи можна використовувати окремо або в комбінації для ефективного виявлення та запобігання загрозам, пов'язаним з доменними іменами та IP-адресами.

З огляду на зростання кількості кіберзлочинності, які часто включають в себе атаки на мережеві ресурси, збір та аналіз даних про домени та IP-адреси може надати корисну інформацію для аналітики, такої як тенденції в реєстрації доменів, типи серверів, що використовуються. Є багато сервісів, які надають інструменти для виявлення потенційних кіберзагроз, аналізу безпеки мережі та ідентифікації шкідливих або небажаних активностей в Інтернеті. Сервіс AbuseIPDB спеціалізується на виявленні і відстеженні шкідливих IP-адрес та надає інструменти для ідентифікації зловмисних активностей, дозволяє користувачам звітувати про підозрілі IP-адреси та надає API для інтеграції з різними системами. Shodan – це пошукова система для виявлення підключених до Інтернету вузлів, сканує Інтернет, збираючи інформацію про різні вузли, для оцінки безпеки мережі, виявлення вразливостей та аналізу інфраструктури. VirusTotal – це онлайн-сервіс, що дозволяє аналізувати файли та URL-адреси на наявність шкідливого програмного забезпечення та надає детальний звіт про знайдені загрози.

Збір даних з різних сервісів та їх аналіз дозволить ефективно відстежувати та реагувати на загрози, пов'язані з IP-адресами та доменними іменами. Такий збір зручно виконувати за допомогою Telegram-бота. Боти дозволяють користувачам отримувати інформацію та виконувати операції, не покидаючи месенджер, що робить їх використання більш зручним та ефективним.

Бібліографія

1. Омельчук А. А. Розробка інструментарію для перевірки доменних імен та IP-адрес на зловмисність. *Молода наука Волині: пріоритети та перспективи досліджень* : матер. XVIII міжнар. науково-практ. конф. аспірантів і студентів., м. Луцьк, 14-15 травня 2024 р. Луцьк, 2024. С. 381-383.