УДК 681.12

О. А. Дубик[1]
О. П. Войтович[2]

ЗАСІБ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ВМІСТУ НА САЙТІ

[1] Вінницький національний технічний університет;

Анотація
Вивчено та проаналізовано способи виявлення шкідливого вмісту на сайті , з'ясовано алгоритми виявлення шкідливого коду, досліджено та проаналізовані існуючі програми та сервіси виявлення шкідливого вмісту на сайті.

Ключові слова: сайт, шкідливий код, сервіси перевірки і виявлення.

Abstract
The methods of detection of harmful content on the site have been studied and analyzed, malware detection algorithms have been found out, existing programs and services of detection of harmful content on the site have been investigated and analyzed.
Keywords: site, malicious code, verification and detection services.

Вступ

На сьогоднішній день великий відсоток зараження комп'ютерів шкідливим програмним забезпечення відбувається через веб-сайти. Шкідливе програмне забезпечення – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. До загроз для сайтів відносять SQL-ін'єкції, які можуть додавати на сайти шкідливі iframe [3].

Метою роботи є покращення безпеки кіберпростору шляхом аналізу методів визначення наявності на сайті шкідливого коду.

Результати дослідження

Для усунення проблем безпеки діагностика повинна складатись з двох етапів:

1. Перевірки файлів і бази даних на хостингу на наявність серверних шкідливих скриптів;
2. Перевірки сторінок сайту на вірусний код, приховані перенаправлення і інші проблеми, які, часом, неможливо виявити статичним сканером файлів [4].

Для аналізу коду та вмісту сайту використовується статичний і динамічний аналіз сторінки (рис.1). Статичний аналіз сторінок - це пошук шкідливих фрагментів коду (переважно javascript), спам-посилань і спам-контенту, фішингових сторінок та інших статичних елементів на сторінці, що перевіряється і в підключаємих файлах [1].

Виявлення подібних фрагментів виконується на основі бази сигнатур або деякого набору регулярних виразів. Якщо шкідливий код постійно присутній на сторінці або в завантажуваних файлах, а також відомий веб-сканеру (тобто він доданий в базу сигнатур), то веб-сканер його виявить. Динамічний або іноді його ще називають "поведінковим". Якщо веб-сканер використовує динамічний метод, він буде не просто аналізувати вихідний код сторінки або файлів, але ще і намагатися робити якісь операції, емулюючи дії реального відвідувача. [2]. Після кожної дії або за певних умов робот сканера аналізує зміни і накопичує дані для підсумкового звіту.

Серед існуючих сканерів сайтів до найефективніших можна віднести такі: веб-сканер QUTTERA, веб-сканер ReScan.pro, веб-сканер Sucuri, Redleg's File Viewer, VirusTotal. Розглянемо кожен із них детальніше (табл. 1).

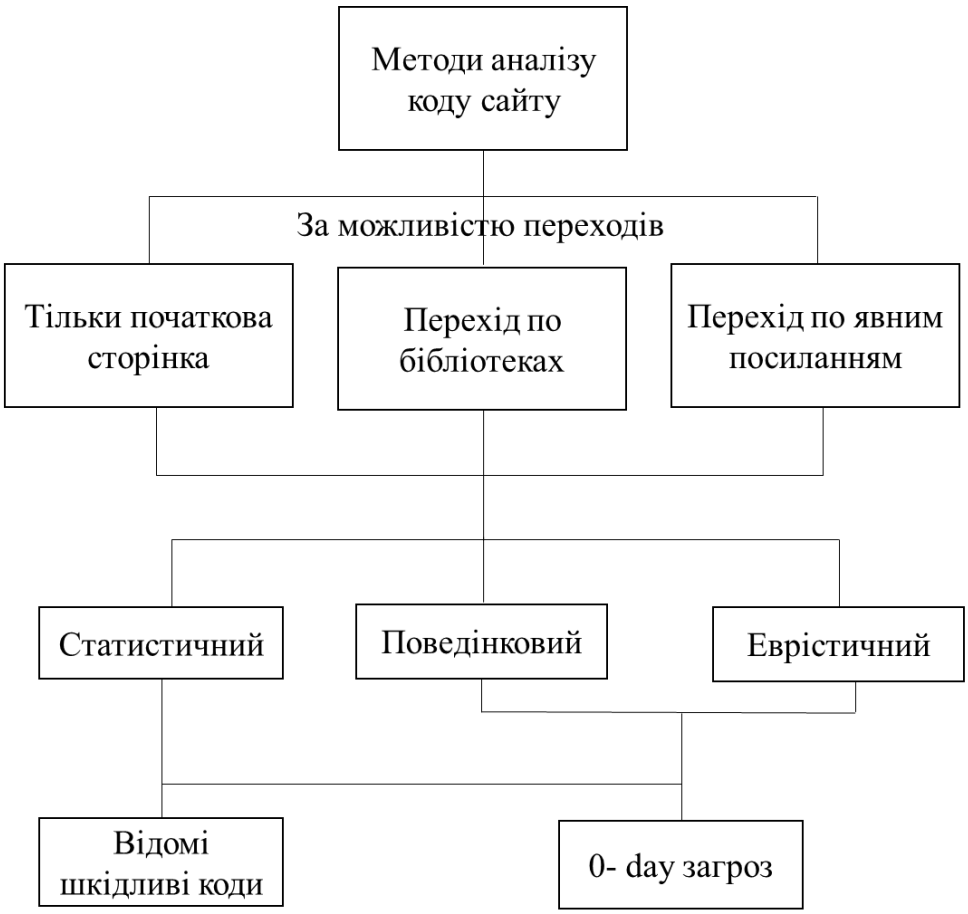

Рис. 1 – Класифікація методів аналізу коду

Таблиця 1 – Результат аналізу різних сканерів шкідливого коду

Назва сканеру	Особливості	Переваги	Недоліки
Веб-сканер QUTTERA.	- безсигнатурний аналіз. - динамічний аналіз сторінок, - виявлення 0-day загроз.	Добре виявляє загрози, пов'язані з завантаженням або розміщенням троянів, завірусованних виконуваних файлів. Є можливість перевірки одразу декілька сторінок. Безкоштовний	Оскільки сервіс безкоштовний, треба буде почекати.
Веб-сканер ReScan.pro	- динамічний аналіз - статичний аналіз - поведінковим аналізом статичний аналіз шукає вірусні	Сканує фрагменти на сторінках і в завантажуються файли, а базою чорного списку визначаються ресурси, що завантажуються з заражених доменів. Ходить по внутрішнім посиланнях, тому крім основного URL перевіряє ще кілька суміжних сторінок сайту. Безкоштовний.	Оскільки сервіс безкоштовний, є ліміт на перевірку – 3 запити з одного IP на добу
Веб-сканер Sucuri	- сигнатурний аналіз - евристичний аналіз	Відправляє запити до декількох URL на сайті з різними User Agent / Referer. Виявляє спам-посилання, дор-сторінки, небезпечні скрипти. Крім того, вміє перевіряти актуальні версії CMS і веб-сервера.	Списки перевірених сайтів з результатами індексується пошуковими системами
Redleg's File Viewer	- статичний аналіз - аналіз підключених на сторінці файлів	Користувач може задати параметри User Agent, referer, параметри перевірки сторінки.	Застарілий і незручний інтерфейс

В результаті даного дослідження було виявлено, що кожен з найпопулярніших на сьогоднішній день сканерів має певні недоліки, але в загальному кожен з них досить непогано виконує поставлену задачу.

Висновки

У ході дослідження було встановлено основні способи виявлення шкідливих файлів та шкідливого коду на сайті. Також було виявлено та проаналізовано найефективніші сервіси для сканування сайтів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Марков, А.С. Статический сигнатурный анализ безопасности программ [Текст] / А.С. Марков, А.А. Фадин // Программна я инженерия и информационная безопасность. –2013. –No 1(1). –С. 50-56.
2. Марков А. С. и др. Эвристический анализ безопасности программного кода //Вестник Московского государственного технического университета им. НЭ Баумана. Серия «Приборостроение». – 2016. – №. 1 (106).
3. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013
4. Войтович О. П. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів / О. П. Войтович, В. О. Вітюк, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. - 2013. - № 3. - С. 4-9.

Дубик Олександр Анатолійович — студент групи 1БС-17мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: oleksandr.dubik@gmail.com.

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Alexander Dubik - *student of the group 1БС-17мс, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksandr.dubik@gmail.com.*

Supervisor: ***Voitovich Olesya Petrovna.*** — *Cand. tech Sciences, assistant professor of information security, Vinnytsia National Technical University.*