УДК 004.738.5(043.2)

О.В. Дубчак,
О.О. Левченко,
Я.С. Мазур
Національний авіаційний університет, Київ

ЗАСОБИ ПРОТИДІЇ ВЕБВІДСТЕЖЕННЮ

Відповідно до результатів дослідження за 2022 р. приблизно 78% громадян України користуються послугами мережі Інтернет щоденно, а 82% - щотижнево [1]. Як відомо, у 2022 р. кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла відповідно у 18,3 та 2,2 рази відносно показників попереднього періоду [2]. Загроза порушення конфіденційності має бути основним важелем обачливості користувачів під час відвідування глобальної мережі, оскільки необхідне програмне забезпечення містить веббраузери, однією із уразливостей яких є вебвідстеження.

Технологія вебвідстеження - відбиток браузера (ВБ), що є глобальним ідентифікатором, який робить його власника більш впізнаним на часто відвідуваних інтернет - ресурсах, багато в чому небезпечніше інших уразливостей веббраузерів. ВБ фіксує отриману ресурсом від браузера цілісну картину та ідентифікує користувача, навіть за умови внесення змін до налаштувань браузера. Пристрій позначається унікальною цифровою міткою у вигляді хеш-суми, знятої з налаштувань браузера. У результаті створюється база міток для ідентифікації користувачів, з якою під час наступного відвідування інтернет - ресурсу проводиться порівняння ВБ пристрою. За умови збігу відбувається однозначна ідентифікація [3].

Гарантовано дієві засоби захисту від зчитування ВБ наразі не розроблені, однак є способи, застосування яких дозволяє зменшити унікальність веббраузера: зміна налаштувань браузера; браузер Firefox з модифікованими налаштуваннями [4]; спеціалізовані розширення для браузера (Chameleon – модифікація значень User-Agent [5]; Canvasblocker – захист від збору цифрових відбитків з Canvas [6]; Canvas Defender – приблизно аналогічно Canvasblocker;[7] User-Agent Switcher – приблизно аналогічно Chameleon;[8] використовувати одночасно краще одне розширення); вимкнення Flash; вимкнення JavaScript; використання

Firefox із файлом user.js від ghacks; браузер Brave; Tor браузер без Tor Network; використання віртуальної машини; використання окремих пристроїв/браузерів [4].

У результаті проведеного аналізу заходів щодо зменшення унікальності веббраузера, одним з найоптимальніших визначено застосування спеціалізованих розширень, що дозволяють надати: різноманітність вибору; можливість налаштувати захист від ВБ на власний розсуд; зручний і зрозумілий інтерфейс (майже не потрібно стикатися з налаштуваннями безпосередньо браузера); можливість застосування до будь-якого браузера. Слід зазначити, спеціалізовані розширення часом можуть і не виправдати очікувань [4]. Також слід зауважити, що всі розширення захищають лише від одного параметру ВБ (для Chameleon і User-Agent Switcher - це User-Agent, а для Canvasblocker та Canvas Defender – відбиток Canvas) [5-8].

Висновок: найкраще рішення протидії ВБ-поєднання захисту від різних варіантів зчитування ВБ в одному розширенні (наприклад, захист від відбитка Canvas, WebGL, звукового відбитка, відстеження роздільної здатності екрану та апаратного відстеження).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Дослідження КМІС. [Електронний ресурс] - Режим доступу: https://www.ukrinform.ua/rubric-technology/3497671-blizko-78-ukrainciv-sodna-koristuutsa-internetom.html]*
2. *Звіт Державного центру кіберзахисту. [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit*
3. *Savannah Copland The Top Browser Fingerprinting Techniques Explained/ [Електронний ресурс] - Режим доступу: https://fingerprint.com/blog/browser-fingerprinting-techniques/*
4. *Septimiu-Vlad Mocan. Browser Fingerprinting and You (What It Is, How It Works, How It Violates Your Privacy, and What You Can Do) [Електронний ресурс. – Режим доступу: https://www.technadu.com/browser-fingerprinting/102454/*
5. *Chameleon [Електронний ресурс]– Режим доступу: https://github.com/sereneblue/chameleon.*
6. *CanvasBlocker [Електронний ресурс] – Режим доступу: https://github.com/kkapsner/CanvasBlocker*
7. *Canvas Defender [Електронний ресурс] /. – Режим доступу: https://addons.mozilla.org/uk/firefox/addon/no-canvas-fingerprinting/.*
8. *User-Agent Switcher [Електронний ресурс] – Режим доступу: https://addons.mozilla.org/en-US/firefox/addon/uaswitcher/?src=gitlab*