Список використаних джерел:

1. Distributed Denial of Service. URL: https://stormwall.pro/knowledge-base/termin/ddos-protection

2. DDoS-атаки/ URL: https://aws.amazon. com/ru/shield/ddos-attack-protection/

Ключові слова: DDoS-атаки, ресурси, мережевий контроль, трафік, аналіз, злом, несанкціонований доступ.

Ключевые слова: DDoS-атаки, ресурсы, сетевой контроль, трафик, анализ, взлом, несанкционированный доступ.

Keywords: DDoS-attack, resource, network control, analysis, traffic, hack, unauthorized access.

Табала Ксенія Андріївна

Національний університет «Одеська юридична академія»,

студентка 2-го курсу факультету кібербезпеки та інформаційних технологій

ЦИФРОВІ ВІДБИТКИ ВЕБ-БРАУЗЕРІВ

Фінгерпрінтинг - це унікальний ідентифікатор, який створюється з застосуванням технології створення цифрового «відбитка» пристрою комунікації користувача. Ця технологія базується на аналізі інформації, яку веб-браузер відправляє на Інтернет-ресурси, якій користувач відвідує.

На основі декількох типів даних, які можна отримати завдяки запитуючому Інтернет-ресурсу, а саме: мовних налаштувань, встановлених шрифтів, часовому поясу, версії веб-браузера та його плагинів тощо - створюється унікальний «цифровий відбиток» веб-браузера. Завдяки використанню фінгерпрінтингу існує можливість розпізнати окремого користувача за створеним цифровим відбитком. Аналізуючи поведінку користувача веб-браузера в Інтернеті,

Інтернет-ресурси можуть використовувати отриману інформацію у комерційних, або інших цілях [1].

Чому створюються відбитки браузерів?

Відбитки веб-браузерів використовуються з метою запобігання шахрайства, а також «крадіжки особистості». Користувач Інтернету може навіть не підозрювати яку кількість інформації про себе він «віддає» Інтернет-ресурсам, без будь-якої згоди на те. З підвищенням кількості зібраних даних формується цифровий профіль користувача, який містить: стать, вік, сімейний та фінансовий стани, інтереси, звички тощо.

Небезпека для користувача зі створенням цифрових відбитків полягає у:

- загрозі конфіденційності;
- присвоєнні глобального унікального ідентифікатору;
- регенерації шкідливих *cookies* та фіксації IP-адреси.

Загроза конфіденційності є головною причиною чому користувачу потрібно враховувати можливості технології фінгерпрінтинг. Ця технологія набагато підступніше, ніж файли *cookies*. Від відбитків веб-браузерів складніше захиститися тому, що неможливо дізнатися: їдеться збір даних користувача чи ні.

Фінгерпрінти як глобальний ідентифікатор полягають у тому, що відбитки веб-браузера роблять його власника відомим не лише на часто відвідуваних Інтернет-ресурсах, але і в різних цифрових платформах. Фіксуючи цілісну картину, яку Інтернет-ресурс отримує від веб-браузера, фінгерпрінтинг ідентифікує користувача навіть при змінах в налаштуваннях веб-браузерів. Цифрові відбитки можуть звести нанівець конфіденційність як ділової, так і особистої переписки користувача.

Фінгерпрінти як регенератор шкідливих *cookies* та фіксатор IP-адреси користувача полягає у тому, що цифровий відбиток веб-браузера може не лише відновити всю бібліотеку *cookies*, але й знайти користувача за його основними мережевими даними [1].

Способи захисту від фінгерпрінтингу в Інтернеті

Існує багато способів змінити відбитки веб-браузерів та зробити їх менш унікальними - оновлення веб-браузерів, використання типових плагинів, видалення нестандартних шрифтів з операційної системи тощо.

Система може «забувати» про веб-браузери окремої конфігурації. Це показує тест, в якому користувач відвідує експериментальний Інтернет-ресурс декілька разів, а потім повертається на нього через деякий час. Результати цього тесту не є надто точними. Унікальність веб-браузерів, з яких заходили на Інтернет-ресурс повторно через 2 – 2,5 тижні, знижувалась на 30% та більше. Вважається, що зміни наступають вже після 5 днів відсутності активності.

Ще кращий результат можна отримати при зміні часового пояса. Користувачі, які мешкають у різних часових поясах, виставляли неправильний час, а після відвідування Інтернет-ресурсу змінювали його на правильне. У користувача з найбільш віддаленим (від початкового показника) часовим відрізком унікальність знижувалась максимально [2].

Гарантовано дієвих засобів захисту від фінгерпрінтингу допоки не було знайдено, однак є загально прийняті заходи для радикального зниження унікальності веб-браузера. Досить ефективно відключення виконання Flash, Javascript та WebGL. Це набагато ускладнює визначення унікальності веб-браузера.

Засоби, ефективні проти *cookies*, можуть не працювати проти технології фінгерпрінтингу. Наприклад, режим «Інкогніто» у веб-браузері блокує виконання деяких небажаних сценаріїв, однак ніяк не змінює відбитки веб-браузера і навіть навпаки – його легше впізнати серед інших [3].

Робота з UMatrix

Набагато кращих результатів дозволяє отримати використання спеціалізованого плагіну uMatrix – інтерактивного блокувальника будь-яких запитів, що відправляє Інтернет-ресурс при зверненні веб-браузера до нього. Він дозволяє вибірково заборонити відправлення даних на домени, що викликаються при загрузці скриптів, фреймів, систем статистики при зверненні веб-браузера до Інтернет-ресурсу [4].

Гнучкість налаштувань цього плагіну дозволяє отримати користувачу повний контроль над підключенням його веб-браузера до всіх доменів, пов‘язаних з використанням поточного Інтернет-ресурсу. Користувач сам вирішує, з якими доменами здійснювати обмін приватною інформацією – тим самим він повністю контролює особисту конфіденційність.

Таким чином, можна констатувати, що технології створення відбитків веб-браузерів базуються на зборі великої кількості даних про пристрій комунікації користувача. Повністю захиститися від фінгерпрінтингу неможливо, але існує можливість мінімізації ймовірності ідентифікації користувача шляхом встановлення спеціалізованих плагінів, що дозволяють керувати виконанням сценаріїв (особливо Java та Flesh), які відвідуються на сторінках Інтернет-ресурсів.

Список використаних джерел:

4. Отпечатки браузеров fingerprints. Часть 1 : Веб сайт. URL: https://whoer.net/blog/ru/unikalnye-otpechatki-brauzera-fingerprints-chast-1/ (Дата звернення: 1.11.2021).

5. Отпечатки браузеров fingerprints. Часть 2. : Веб сайт. URL: https://whoer.net/blog/ru/unikalnye-otpechatki-brauzera-fingerprints-chast-2/ (Дата звернення: 1.11.2021).

6. Фингерпринт: что это такое и как это скрыть? : Веб сайт. URL: https://vc.ru/u/738105-adspower-browser/212732-fingerprint-otpechatok-brauzera-chto-eto-takoe-i-kak-ego-skryt (Дата звернення: 1.11.2021).

7. uMatrix. : Веб сайт. URL: https://addons.mozilla.org/ru/firefox/addon/umatrix/ (Дата звернення: 1.11.2021).

Ключові слова: відбитки браузерів, Інтернет-ресурси, система.

Ключевые слова: отпечатки браузеров, Интернет-ресурсы, система.

Keywords: browser fingerprints, Internet resourses, system.

Науковий керівник*: к.т.н., доц. Задерейко О.В.*