ПРИНЦИП РОБОТИ АТАКИ SNAILLOAD

Ніконенко Д.В., В'юхін Д.О., Голобородько Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі питання кібербезпеки набувають все більшої актуальності, адже, попри постійне оновлення антивірусів та захисного програмного забезпечення, кіберзлочинці не стоять на місці й постійно знаходять нові способи обходу існуючих механізмів захисту.

Метою доповіді є розгляд SnailLoad - нового типу атаки побічного каналу, що дозволяє віддаленому зловмиснику визначати активність користувача в інтернеті, зокрема, які вебсайти він відвідує або які відео переглядає, навіть без безпосереднього доступу до його мережевого трафіку.

Основна ідея SnailLoad полягає у використанні варіацій затримки (latency) в мережевому з'єднанні жертви для отримання інформації про її онлайн-активність [1]. Зловмисник спочатку створює контрольований сервер і спонукає жертву завантажити з нього невеликий нешкідливий файл, наприклад, зображення або стилістичний файл CSS. Це може статися під час відвідування жертвою певного вебсайту або перегляду реклами, де вбудовано посилання на сервер зловмисника. Важливо, що цей файл не містить шкідливого коду, тому антивірусні програми не виявляють загрози.

Під час завантаження файлу сервер зловмисника навмисно передає дані дуже повільно, що дозволяє йому постійно відстежувати зміни в затримці мережевого з'єднання жертви. Ці зміни можуть бути викликані іншою активністю користувача, наприклад, переглядом відео або відвідуванням інших вебсайтів. Кожен тип контенту має унікальний "відбиток" — специфічний патерн змін затримки, обумовлений розміром і частотою передачі пакетів даних. Аналізуючи ці патерни, зловмисник може визначити, який саме контент споживає жертва.

Атака типу SnailLoad становить серйозну загрозу для конфіденційності користувачів, оскільки дозволяє зловмиснику виступати в ролі "людини посередині" (man-in-the-middle) без фактичного перехоплення чи дешифрування трафіку [2]. Завдяки особливостям побічного каналу, атакуючий може повністю приховано спостерігати за онлайн-активністю жертви - наприклад, які відео вона переглядає або які сайти відвідує. При цьому весь трафік залишається зашифрованим і ніщо не викликає підозри в користувача, що робить виявлення атаки вкрай складним.

Подальші дослідження допоможуть розробити ефективні стратегії протидії таким загрозам та забезпечити більшу конфіденційність і безпеку в Інтернеті.

Список літератури

1. Gast S., Czerny R., Juffinger J., Rauscher F., Franza S., Gruss D. "SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript". Graz University of Technology, 2024. URL: https://www.snailload.com/snailload.pdf.

2. "SnailLoad: Exploiting Remote Network Latency Measurements Leak User Activity". SnailLoad Official Website, 2024. URL: https://www.snailload.com/.