УДК 004.056.56:342(043.2)

Юрій Старовойт, Владислав Фотул
Олександр Туровський, д.т.н., професор.
(Національний авіаційний університет, Україна)

Безпека персональних даних при авторизації в публічному WI-FI

У приміщеннях, з публічним Wi-Fi, можуть використовуватись сторінки для авторизації Wi-Fi, які називаються перехоплюючими сторінками. Однак, якщо такі сторінки не належним чином налаштовані власником або якщо зловмисники втручаються у процес авторизації, то персональні дані користувача можуть бути викрадені. Тому, забезпечення безпеки персональних даних користувачів є важливим питанням.

Мета цього дослідження полягає у розгляді принципів роботи сторінок авторизації, виявленні проблем безпеки та описі можливих загроз для персональних даних користувачів.

Більшість джерел, присвячених захисту інформації в публічних мережах, зазвичай зосереджуються на дослідженнях вразливостей протоколів для Wi-Fi, але сторінки авторизації можуть представляти додатковий спектр загроз, який не отримав достатньої уваги від дослідників. Тому ця публікація є інформативною.

Сьогодні важко уявити публічне місце, яке не пропонує відкритий доступ до Wi-Fi. Згідно з звітом світових аналітиків про ризики в, більше половини людей, які перебувають в готелі або ресторані, намагаються підключитися до мережі за перші хвилини. Зазначено, що це може бути пов'язано з сильним сигналом Wi-Fi, який змушує 55% людей ділитися будь-якою інформацією про себе.

Для того, щоб отримати доступ до бездротового з’єднання, користувач зазвичай повинен зайти на сторінку закладу, де йому будуть запропоновані умови користування Wi-Fi та збір персональної інформації, такої як електронна пошта, номер телефону та інші приватні дані, або використати логін та пароль, надані власником. Для входу також може знадобитися авторизація через соціальні мережі за допомогою власних особистих даних.

Зловмисникам можуть знадобитися навіть непотрібні дані користувача, оскільки вони можуть бути використані для створення повноцінного профілю користувача, який може бути проданий на чорному ринку. Такий профіль містить важливу інформацію про користувача, таку як його захоплення, інтереси, звички, місцезнаходження та інші дані, які можуть бути використані для налаштування персоналізованих рекламних кампаній або для здійснення шахрайства. Крім того, зловмисники можуть використовувати украдені дані для здійснення атак на інші сервіси, такі як онлайн-банкінг або соціальні мережі, використовуючи отримані дані для підміни особистості користувача та імітації його поведінки. Отже, збереження персональних даних від небажаних осіб є критично важливим для забезпечення безпеки користувачів в онлайн-середовищі.

Також важливо зазначити, що зловмисники можуть використовувати викрадену інформацію для спаму, фішингу та інших атак, які мають на меті здійснення шахрайства та шкоди користувачеві. Наприклад, шахраї можуть відправляти фішингові листи, в яких проситимуть користувача надіслати свої облікові дані або оплатити якісь послуги, використовуючи ім'я та логотип відомих компаній, що сприймається користувачем як дійсний запит. Крім того, зловмисники можуть використовувати викрадені дані для зламу аккаунтів, які містять фінансову інформацію, та здійснювати шахрайські операції. У загальному, зловмисники можуть використовувати викрадену інформацію для здійснення різних видів кіберзлочинності, тому дуже важливо дотримуватися правил безпеки в Інтернеті та захищати свої дані.

Так, специфіка методів, які обирає хакер, може значно впливати на безпеку даних користувачів. Наприклад, зловмисники можуть використовувати різні методи атак, такі як фішингові атаки, введення SQL-запитів, крадіжку сесій, встановлення шкідливого програмного забезпечення і т.д. Застосування цих методів дозволяє зловмисникам отримувати доступ до облікових даних та інших конфіденційних даних користувачів, які вони можуть використовувати для своїх злочинних цілей. Тому важливо дотримуватись правил безпеки та використовувати надійні паролі, двофакторну аутентифікацію, виключати автозаповнення форм, використовувати захищені протоколи передачі даних, оновлювати програмне забезпечення та оперативні системи, і т.д.

Атака Captive Portal Hijacking є широко поширеною і небезпечною. Зловмисники можуть підробити сторінку авторизації та створити мережу з ідентичним іменем для виманювання користувачів на свою підроблену сторінку. При підключенні до такої мережі, зловмисник отримує доступ до пристрою користувача та може здобути конфіденційну інформацію, таку як облікові дані до різних джерел. Зловмисник також може маніпулювати вмістом сторінки та змусити користувача вводити свої платіжні дані та іншу чутливу інформацію. Часто користувачі необачні та відчуваються надто захищеними, що забезпечує успішність таких атак.

Однією з наступних проблем є відкритий канал передачі інформації між пристроєм користувача та сторінкою авторизації, а також після входу до мережі. Шифрування трафіку потребує додаткових конфігурацій та знань, якими власники часто нехтували. Це може призвести до крадіжки даних навіть до того, як вони будуть відправлені до провайдера, через атаку man-in-the-middle. Незважаючи на те, що більшість веб-сторінок зараз має протокол HTTPS, що шифрує трафік на відміну від HTTP, сторінка авторизації часто блокується цим протоколом, оскільки є втіленням перехоплювача трафіку та його розшифрування. Щоб підтвердити з'єднання, користувачі мають натиснути кнопку погодження на небезпечному каналі передачі інформації. Однак, така звичка може наражати користувачів на небезпеку. Важливим аспектом безпеки сторінок авторизації є законність збору персональних даних провайдером. Дослідження М. Маннана та інших виявили публічні мережі, які збирали інформацію та встановлювали відстеження активності та місця положення пристроїв, навіть до того, як користувач надав свою згоду. Крім того, були

випадки розсилання даних стеження до 34 третіх сторін, які використовували їх для формування маркетингових та спам баз даних.

Мета подальшого дослідження полягає в тому, щоб дослідити, яку інформацію можуть отримати провайдер та зловмисник, якщо вони втрутяться в процес авторизації в публічному Wi-Fi за допомогою скануючого додатку та створеного безпечного тестового середовища. Ми також плануємо вивчити, чи можна зменшити виток персональних даних, підвищуючи усвідомленість користувачів про небезпечність володіння приватною інформацією сторонніми особами. Крім того, ми прагнемо дізнатися, чи буде ефективним використовувати програмне забезпечення, що забороняє відстеження пристрою, а також локальні та мережеві програми, що блокують тіньове розповсюдження інформації про користувача, з метою зменшення загрози витоку даних в публічних Wi-Fi мережах.

Список літератури

[1] How to Avoid Public WiFi Security Risks [Електронний ресурс] – 2022. – режим доступу: https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

[2] Public Wi-Fi: An ultimate guide on the risks + how to stay safe [Електронний ресурс] – 2021. - режим доступу: https://us.norton.com/blog/privacy/public-wifi

[3] The Top 7 Dangers of Public Wi-Fi for Businesses [Електронний ресурс] – – 2019 – Режим досутпу: https://www.wgu.edu/blog/7-dangers-public-wifi-businesses2112.html#close

[4] The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data [Електронний ресурс] — 2023 – Режим досутпу: https://www.forbes.com/advisor/business/public-wifi-risks/