УДК 004.75+004.77
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.508

МЕТОДИ ЗАХИСТУ ВІД НАЙПОШИРЕНІШИХ ЗАГРОЗ WI-FI МЕРЕЖАМ

Зозуля А.С., Медведєв Є.О.
Науковий керівник – ст. викл. Медведєв Є.О.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
тел. +38(057) 702-14-30,
e-mail: andrii.zozulia@nure.ua, eugene.medvedev@nure.ua

Unauthorized access to Wi-Fi networks provides hackers with the ability to intercept sensitive information such as passwords, credit card numbers, or personal data transmitted over the network. The theses discuss the main types of attacks on Wi-Fi networks and provide recommendations for minimizing the success of such attacks.

Отримання несанкціонованого доступу до Wi-Fi мереж надає хакерам можливість перехоплювати чутливу інформацію, таку як паролі, номери кредитних карток або особисті дані, що передаються через мережу. Шляхом експлуатації вразливостей безпеки Wi-Fi атакувальники можуть виконувати зловмисні дії, які посягають на безпеку та конфіденційність кожного, хто підключений до мережі. Крадіжка ідентичності, фінансові шахрайства та соціальний інжиніринг - лише деякі приклади потенційних наслідків атак на мережу.

Існують кілька ознак, на які варто звернути увагу. По-перше, перевірте список пристроїв, підключених до вашої Wi-Fi. Якщо ви побачите невідому адресу, це може бути сигналом попередження. Також звертайте увагу на будь-які несподівані сповільнення швидкості Інтернету або неочікуване використання даних. Це можуть бути ознаки того, що хтось використовує вашу Wi-Fi без вашого відома.

Найнебезпечніші загрози Wi-Fi.

Давайте поближче розглянемо найбільші загрози безпеки Wi-Fi, щоб ви могли краще зрозуміти і вирішити потенційні ризики для вашої мережі.

1.Дезавтентифікація. Зазвичай маршрутизатори відправляють повідомлення про дезавтентифікацію неактивним пристроям для ефективного управління підключенням. Однак хакери експлуатують цей процес WLAN, щоб виконати атаки дезавтентифікації. На відміну від атак, які крадуть інформацію, дезавтентифікація спрямована на відключення пристрою за допомогою відправлення фальшивих кадрів дезавтентифікації. Ці підроблені кадри змушують цільовий пристрій вважати, що він відключений, і змушують його повторно підключитися до мережі.

Мета атакувальника. Більшість атак на Wi-Fi починаються з дезавтентифікації. Як тільки цільовий пристрій повторно підключається до компрометованої мережі, атакувальник використовує цю можливість для перехоплення, маніпулювання або моніторингу потоку даних між пристроєм та Wi-Fi мережею. Пристрій, вважаючи, що він пережив стандартне повторне підключення, може несвідомо передавати чутливі дані, такі як паролі або особиста інформація. Конкретні дії залежать від цілей атакувальника, але загальна мета полягає в тому, щоб скористатися повторним підключенням для компрометації безпеки пристрою або мережі.

Заходи безпеки. Пакети дезавтентифікації, використовувані в атаках, не є зашифрованими, але досить легко знайти MAC-адреси та WLAN SSID. Покращіть безпеку вашої Wi-Fi, активуючи протоколи шифрування WPA3. Крім того, ви можете активувати функцію Захищених Керуючих Кадрів (PMF), вперше через WPA3. Якщо ви використовуєте WPA2, переконайтеся, що він налаштований безпечно. В рамках поточного стандарту безпеки PMF забезпечує те, що пакети дезавтентифікації передаються за допомогою спільного ключа, що дозволяє вашому пристрою впізнавати їх як законні повідомлення від відомого маршрутизатора.

2.Злий двійник. Це тип загрози, коли зловмисник створює фальшиву, незахищену Wi-Fi мережу, яка виглядає як легітимна, оскільки використовує той самий ідентифікатор SSID. Ця обманлива мережа змушує користувачів підключатися, вважаючи її надійною точкою доступу Wi-Fi. Хоча це зазвичай відбувається у громадських місцях, таких як кав'ярні або аеропорти, це також може трапитися вдома з приватною мережею.

Фальшива точка доступу зазвичай привертає людей до підключення, оскільки атакувальник робить вид, що вона пропонує кращу силу сигналу, ніж мережа, яку вона імітує. Крім того, вони можуть використовувати атаку дезавтентифікації, щоб змусити пристрої людей відключитися від реального Wi-Fi та несвідомо підключитися до фальшивої мережі.

Мета атакувальника. Після підключення користувача до зловмисної двійниці, атакувальник може моніторити всі ваші дані. Це може включати дані для входу, які ви вводите у банківському додатку або іншу чутливу інформацію, яку ви відправляєте через Інтернет. Атакувальник також може встановити шкідливе програмне забезпечення.

Заходи безпеки. Щоб захистити себе від таких атак, уникайте виконання дій, які передбачають введення важливих паролів, коли ви підключені до громадської точки доступу Wi-Fi. Якщо вам доведеться це зробити, переконайтеся, що ви встановили зашифроване з'єднання, перевіривши веб-адресу, яка починається з https://. Для підвищення захисту у громадських місцях розгляньте можливість використання Віртуальної Приватної мережі (VPN). Крім того, уникайте будь-яких незахищених бездротових мереж, які не вимагають пароля.

3. Атака " Brute Force". Brute Force - це метод, який передбачає вгадування пароля Wi-Fi шляхом систематичної спроби всіх можливих комбінацій для отримання несанкціонованого доступу до мережі. Цей метод ґрунтується на наполегливості зловмисника та припущенні, що пароль не є дуже складним або довгим. Бази даних з популярними паролями та комбінаціями символів також можуть використовуватися для прискорення процесу.

Мета атакувальника. Маючи правильний пароль Wi-Fi, атакувальник отримує необмежений доступ до всіх пристроїв, підключених до домашньої мережі. Він може потенційно проникнути в інші пристрої в мережі та отримати доступ до загальних ресурсів. Також є можливість перехоплення та запису всього потоку даних в мережі без шифрування.

Заходи безпеки. Використовуйте складний, унікальний пароль для вашої мережі Wi-Fi і оновлюйте його регулярно. Використання фрази з буквами, цифрами та символами високо рекомендовано. Переконайтеся, що ви змінили стандартні облікові дані, які поставляються з вашим маршрутизатором, оскільки стандартні паролі легко доступні та часто використовуються для атак. Крім того, розгляньте можливість обмеження кількості пристроїв, які можуть підключатися до вашої мережі, щоб зменшити ризик несанкціонованого доступу.

4. Атака на Маршрутизатор. Деякі моделі маршрутизаторів вразливі до порушень безпеки через вразливості в прошивці. Оскільки багато бездротових маршрутизаторів використовують Linux як основу, виробники часто включають відкриті програми, які можуть мати недоліки. Хакери можуть використовувати ці розриви, щоб виконувати команди на маршрутизаторі, надаючи їм повний контроль.

Мета атакувальника. Одержавши контроль, атакувальник може змінювати налаштування, вимикати функції безпеки та забезпечувати постійний доступ до меню маршрутизатора без виявлення. Захоплений маршрутизатор може потім бути використаний зловмисником для приєднання до ботнету, мережі компрометованих пристроїв. Це дозволяє запускати атаки на інші мережі, такі як атаки відмови в обслуговуванні (DoS) або відправка спам-повідомлень.

Заходи безпеки. Слід слідкувати за інформацією про вразливості маршрутизатора, відвідуючи сторінки підтримки, специфічні для вашої моделі маршрутизатора, а також авторитетні веб-сайти з кібербезпеки. Регулярно перевіряйте оновлення прошивки, щоб усунути можливі вразливості.

5. Віддалена Атака. Ця загроза полягає в тому, що хакер намагається отримати доступ до Wi-Fi мережі з відстані, зазвичай через Інтернет. Один з поширених методів - це сканування мережевих пристроїв, які налаштовані на віддалений доступ, часто використовуючи стандартні порти. Після ідентифікації хакер може використовувати методи, такі як атаки

"Brute Force", щоб намагатися розшифрувати паролі та отримати контроль над Wi-Fi мережею.

Мета атакувальника. Зміни в налаштуваннях меню маршрутизатора дозволяють атакувальникові отримати його контроль. Після цього вони можуть інтегрувати компрометований маршрутизатор в ботнет або маніпулювати доступом до Інтернету пристроїв, підключених до Wi-Fi. Ця маніпуляція може включати перенаправлення веб-трафіку на сервер, контрольований атакувальником. В результаті вони можуть потенційно захопити паролі або розмістити шкідливе програмне забезпечення в домашню мережу.

Заходи безпеки. Активуйте віддалений доступ лише тоді, коли це необхідно, та використовуйте складний пароль для входу в меню маршрутизатора. Також найкраще створити окремий обліковий запис користувача для віддаленого доступу, відмінний від того, який ви використовуєте для локального доступу. Крім того, ви можете скористатися можливістю визначення діапазону IP-адрес. Це означає, що тільки бездротові пристрої з певним відповідним IP-адресую матимуть змогу отримати доступ до маршрутизатора віддалено. Для додаткової безпеки деякі маршрутизатори також блокують меню після певної кількості неуспішних спроб входу або збільшують затримку після кожної неуспішної спроби, перш ніж дозволити наступний вхід.

Висновки. Забезпечення безпеки підключень Wi-Fi є надзвичайно важливим у сучасному світі. Приймаючи попередні заходи для забезпечення безпечного доступу та захисту вашої мережі від потенційних загроз, ви створюєте безпечне цифрове середовище, та гарантуєте безпеку даних, які циркулюють у вашій мережі.

Список використаних джерел

1. E. Tews and M. Beck, “Practical Attacks against WEP and WPA,” in Proceedings of the Second ACM Conference on Wireless Network Security, ser. WiSec ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 79–86. [Online]. Available: https://doi.org/10.1145/1514274.1514286

2. M.Ghering, “Evil Twin vulnerabilities in Wi-Fi networks,” Bachelor Thesis, Radboud University, 2016. [Online]. Available: https://www.cs.ru.nl/bachelors-theses/2016/Matthias Ghering 4395727 Evil Twin Vulnerabilities in Wi-Fi Networks.pdf (дата звернення: 20.02.2024)

3.Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” Proceedings of the IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

4. Антипов, І. Є. Удосконалення моделі Wi-Fi мережі з метою запобігання вторгненням / І. Є. Антипов, Є. Ю. Бондар, Т. А. Василенко // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. – Харків, 2014. – Вип. 177. - С. 60 - 63.