АНАЛІЗ АТАК ПО КЛОНУВАННЮ МАРШРУТИЗАТОРА

Якимчук М.Д., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний світ наразі не може існувати без Інтернету та мережі. Маршрутизатор відіграє в ній ключову роль, забезпечуючи передавання даних між сегментами. **Метою доповіді** є проведення аналізу атаки по клонуванню маршрутизатора.

Однією з можливих атак як зловмисників так і "білих"-хакерів є атаки типу «людина посередині» (MITM), а саме атака клонуванням маршрутизатора. Вона передбачає створення ідентичної копії маршрутизатора перехоплення або модифікації трафіку.

Під час атаки «злий двійник» зловмисник створює підроблену Wi-Fi-мережу, яка імітує легітимну точку доступу, щоб обманом змусити жертву підключитися до неї та викрасти конфіденційну інформацію. Основний принцип цієї атаки полягає у розгортанні фальшивої бездротової мережі з тим самим SSID, що й у справжньої точки доступу, яку необхідно скомпрометувати. Ця атака можлива лише якщо більшість пристроїв, таких як смартфони та ноутбуки тощо, при виборі Wi-Fi-з'єднання орієнтуються лише на ідентифікатор SSID, не маючи механізмів для розрізнення автентичних і підроблених мереж з однаковою назвою та типом шифрування. Користувачі, не підозрюючи небезпеки, автоматично підключаються до мережі з найсильнішим сигналом, що часто виявляється шкідливою копією [1].

Одним із найпоширеніших сценаріїв реалізації атаки є використання механізму Captive Portal. Ця система, зазвичай застосовувана у громадських Wi-Fi-мережах, змушує користувача пройти авторизацію перед отриманням доступу в інтернет. Зловмисник може створити підроблену сторінку входу, схожу на офіційний портал авторизації, і тим самим змусити жертву ввести облікові дані або іншу конфіденційну інформацію. Отримані дані можуть використовуватися для подальших атак, перехоплення трафіку або компрометації корпоративних і особистих акаунтів. Успішне клонування маршрутизатора може призвести до перехоплення конфіденційної інформації, здійснення атак MITM, впровадження шкідливого програмного забезпечення та порушення стабільності роботи мережі. Протистояти атаці такого виду можливо за допомогою аналізу аномалій у трафіку, перевірці цифрових сертифікатів пристроїв та фізичної ідентифікації обладнання. Для захисту мережі необхідно використовувати захищені протоколи зв'язку, сегментувати мережу, контролювати доступ і відстежувати зміни в інфраструктурі.

Список літератури

1. Reddy B. I., Srikanth V. Review on Wireless Security Protocols (WEP, WPA, WPA2 and WPA3) // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. — 2019.