УДК 004

АНАЛИЗ WIFIPHISHER, КАК СРЕДСТВА РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Филатова Д.А., студентка гр.ИТб-132, IV курс
Научный руководитель: Асанов С.А., старший преподаватель
Кузбасский государственный технический университет имени Т.Ф. Горбачева
г. Кемерово

Одним из важных аспектов информационной безопасности является знание методов и инструментов «врага». Очень часто хакерам приходится что-либо взламывать, а в частности – пароли. Программа Wifiphisher является весьма действенным инструментом для этих целей. Она предназначена для фишинговой атаки на WiFi сети ради получения паролей от точек доступа и другой персональной информации. Wifiphisher основан на атаке социальной инженерии, т.е. программа не содержит каких-либо инструментов для брутфорсинга. Это простой способ получить учётные данные от сайтов или пароли от WPA/WPA2.

Требования

- Kali Linux. Хотя Wifiphisher работает и на других дистрибутивах, Kali Linux является официально поддерживаемым дистрибутивом, следовательно, все новые функции тестируются в первую очередь на этой платформе.
- Как минимум один беспроводной адаптер, который поддерживает режим AP. Драйверы должны поддерживать технологию netlink.
- Как минимум один беспроводной адаптер, который поддерживает режим монитора и способен к инъекциям.

Принцип работы

1. Пользователь принудительно отключается от активного хот-спота. Wifiphisher постоянно подавляет все устройства, подключенные к целевой точке доступа, рассылая пакеты deauth клиентам от имени точки доступа и к точке доступа от имени клиента.
2. Пользователь подключается к враждебному хот-споту. Wifiphisher сканирует радиоэфир и копирует настройки точек доступа. Затем создаётся поддельный хот-спот, смоделированный на основании данных легитимного. Также включается сервер NAT/DHCP, который перенаправляет нужные порты с компьютера злоумышленника к настоящей точке доступа. В результате, из-за глушения Wi-Fi, клиенты начинают подключаться к враждебной точке (правда, это происходит не полностью автоматически: пользователю нужно подтвердить действие в ОС). После этого пользователи становятся жертвой атаки типа Man in the middle (человек посередине).
3. Пользователю отправляется реалистично выглядящая страница с настройками конфигурации маршрутизатора. Wifiphisher использует мини-

мальный веб-сервер, который реагирует на запросы HTTP и HTTPS. Как только жертва запрашивает страницу из интернета, Wifiphisher отвечает страницей с запросом учётных данных. Например, можно спросить подтверждение пароля WPA по причине апгрейда программного обновления маршрутизатора.

Применение

Программа запускается командой wifiphisher, после чего отображается список обнаруженных точек доступа. Далее процесс останавливается сочетанием клавиш Ctrl+C и предлагается выбрать цель (Рис. 1).

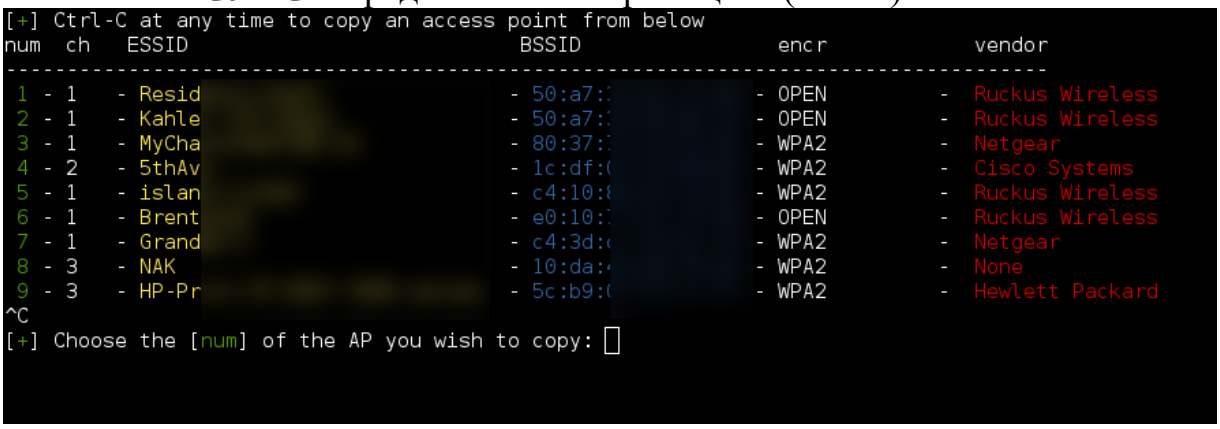

Рис. 1.

Тем временем пользователь на своём устройстве видит поддельную страницу конфигурации маршрутизатора (Рис. 2).

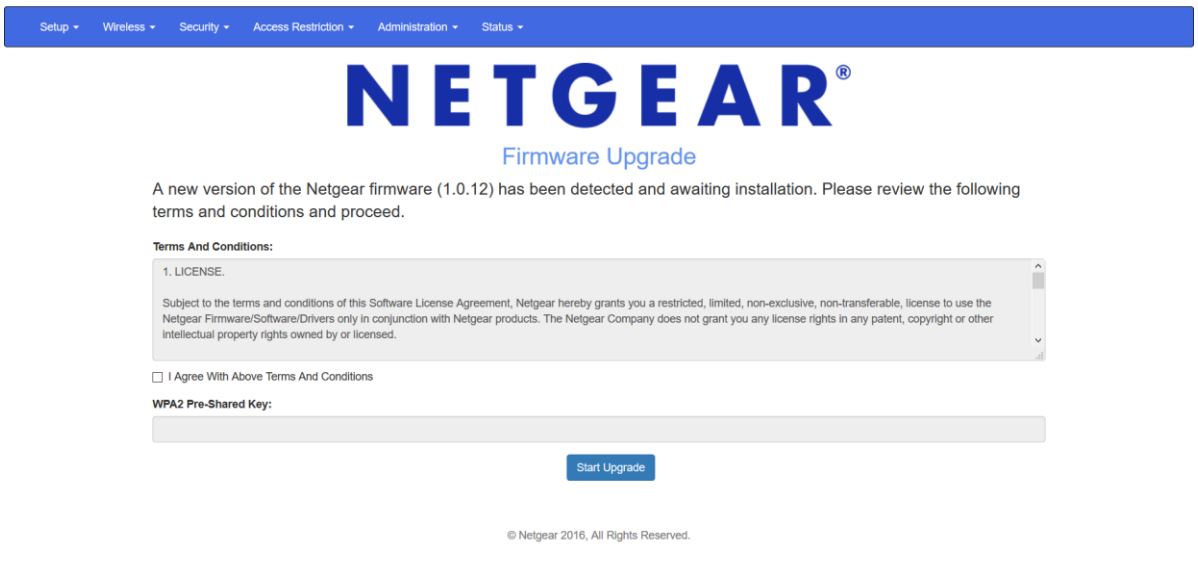

Рис. 2.

На рисунке 3 приведён пример успешной атаки.

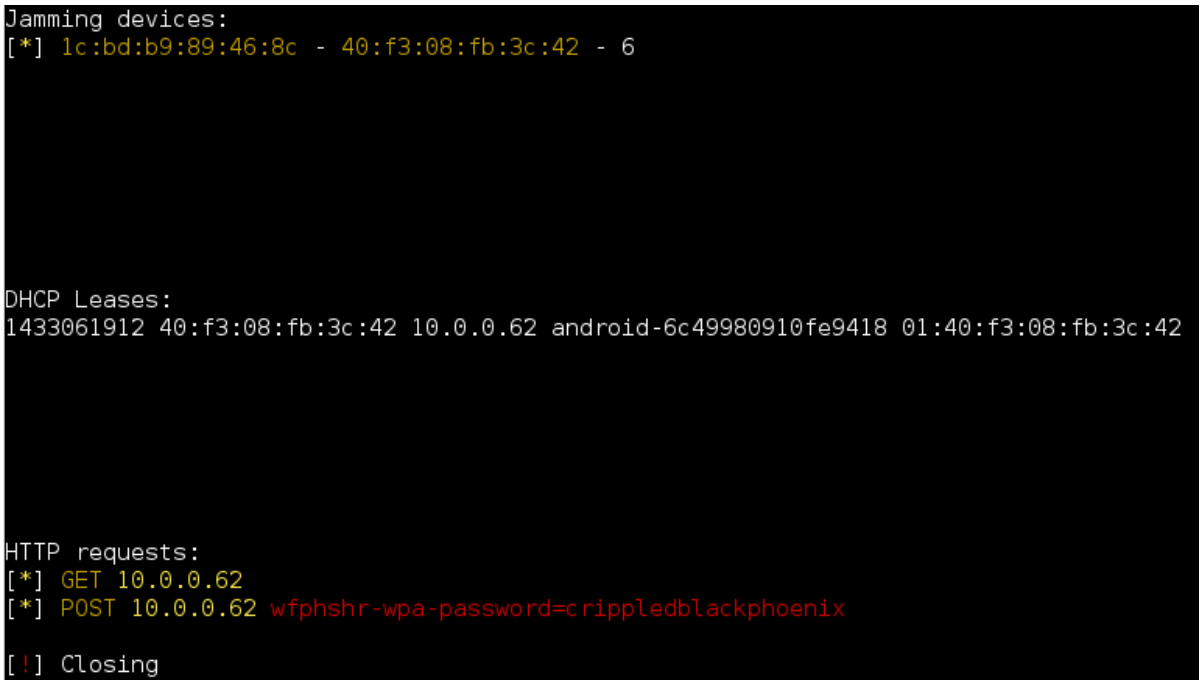

Рис. 3.

Плюсы и минусы

Минусом данной программы является то, что в отличие от аналогов Wifiphisher никак не проверяет полученные от пользователя данные. Это значительно снижает автоматизацию. Атакующий прямо во время атаки сам должен проверить полученный пароль путем подключения к легитимной точке доступа и принять решение о продолжении или прекращении атаки. Недавно в Wifiphisher появился новый ключ -qS. Если его указать, то программа прекращает свою работу после первых полученных учётных данных, даже если они неправильные. Альтернативные программы, например, Fluxion можно оставить работать на долгое время, и она не даст пользователю подключиться к оригинальной точки доступа, пока он не введёт правильный пароль от WiFi, после чего программа завершает свою работу, сохраняя полученные данные.

Серьезным преимуществом и главной особенностью Wifiphisher является то, что программа, помимо точек доступа, позволяет получать пароли от веб-сайтов под предлогом доступа к бесплатному Интернет-соединению. В настоящее время реализован сценарий получения пароля от Facebook. Так же можно самостоятельно написать сценарий для любого сайта. При реализации данной атаки достаточно одного беспроводного интерфейса — того, на котором поднимается точка доступа с «бесплатным» WiFi, во время атаки не нужно глушить другие точки доступа.

Заключение

Подводя итог, можно сделать вывод, что бороться с Wifiphisher практически невозможно. Кардинальным средством защиты является только отключение Wi-Fi адаптера. В качестве мер, позволяющих значительно снизить риск реализации атаки, необходимо применять следующие: не стоит вводить пароли на подозрительных страницах; необходимо включить «подтверждение подключения» даже к известным сетям; использовать VPN; использовать

утилиты аудита радиоэфира для выявления аномалий; не использовать критично-важные программы (например, банк-клиент) в открытых сетях.

Список литературы:

1. wifiphisher - Инструменты Kali Linux. [Электронный ресурс] – Режим доступа: свободный. https://kali.tools/?p=380
2. Codeby.net - портал для программистов и сисадминов. [Электронный ресурс] – Режим доступа: свободный. https://codeby.net
3. GitHub - wifiphisher/wifiphisher: Automated victim-customized phishing attacks against Wi-Fi clients. [Электронный ресурс] – Режим доступа: свободный. https://github.com/wifiphisher/wifiphisher