УДК 004.491.22 **Технические науки**

Митрошина Екатерина Валерьевна, *студентка,*
5 курс электротехнического факультета
Пермский национальный исследовательский политехнический университет
e-mail: mitroshina.katya@inbox.ru

АНАЛИЗ ОСНОВНЫХ НАПРАВЛЕНИЙ ФИШИНГОВЫХ АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА С ЦЕЛЬЮ ПОВЫШЕНИЯ ИХ БЕЗОПАСНОСТИ

Аннотация: В статье представлен обзор различных типов мобильных фишинговых атак. А также рассмотрены основные методы обнаружения и снижения фишинговых атак.

Ключевые слова: Мобильное приложение, Фишинг, Смишинг, Вишинг.

Abstract: This article provides an overview of various types of mobile phishing attacks. And also describes some methods of detection and mitigation phishing attacks.

Keywords: Mobile Application, Phishing, Smishing, Vishing.

Мобильный фишинг (англ. Mobile Phishing) – развивающаяся угроза безопасности в современном мире. В мобильной фишинговой атаке злоумышленник обычно отправляет SMS-сообщение, содержащее ссылки к веб-страницам фишинга или приложениям, запрашивающим учетные данные при посещении. Атаки могут также инициироваться с помощью сообщений электронной почты, загруженных в браузере мобильных устройств [1].

Специалисты приходят к такому выводу, что количество мобильных фишинговых атак значительно увеличилось в течение последних нескольких лет для различных платформ на мобильных устройствах. По сравнению с традиционными пользователями программного обеспечения, установленного на

компьютере, пользователи мобильного приложения более уязвимы для фишинговых атак. Эксперты сходятся во мнении о некоторых общих, хорошо известных причинах для этой уязвимости:

1) В небольшом устройстве пользователю довольно трудно проверить подлинность страницы, что подтверждает частные гиперссылки, поскольку URL не всегда выводятся на экран в мобильных браузерах.

2) Мобильные пользователи менее осведомлены о параметрах безопасности, чтобы остановить или предотвратить фишинговые атаки.

3)Большинство законных мобильных приложений требуют от пользователей ввести свои учетные данные с очень простым пользовательским интерфейсом, что помогает злоумышленнику довольно легко придумать поддельные приложения или простые веб-сайты, имитирующие законные пользовательские интерфейсы [1].

Основные методы фишинга на основе уязвимостей инфраструктуры мобильных устройств:

1. Размер экрана.

У мобильных устройств в основном небольшой размер экрана. Эти небольшие экраны создают трудности, чтобы увидеть полный URL, когда пользователи переходят по ссылке. Поэтому многие пользователи не знают, когда они находятся не на официальных сайтах при просмотре страниц в Интернете. Кроме того, следует учесть, что маленький размер экранной клавиатуры способен привести и к ошибке в наборе адреса.

2. Приложения.

Создание и развертывание злонамеренного программного обеспечения (ПО) не требует высокого уровня знаний и особых навыков убеждения пользователей для того, чтобы заставить их установить вредоносное ПО. Многие владельцы мобильных устройств принимают предложения игр, незнакомого ПО или привлекательных изображений, даже в тех случаях, если они совсем не уверены в источнике ПО [2].

3. Задержки обновлений ПО.

Несвоевременное обновление ПО позволяет злоумышленникам легло использовать эту уязвимость. Во-первых, многие телефоны младших версий не обновляются никогда, так как не имеют возможности поддержки более новой версии ПО. Во-вторых, пользователи мобильных устройств не устанавливают обновления сразу же по нескольким причинам, например, процедура обновления занимает длительное время, телефон разряжается и тому подобное.

4. Смишинг (англ. Smishing).

Другой популярный метод фишинга использует SMS-сообщения. Этот метод называют «смишинг». Данный метод работает так же как и фишинг, но вместо электронной почты, жертва получает обычное текстовое сообщение SMS. SMS-сообщение содержит ссылку на фишинговый сайт. Как вариант пользователю мобильного устройства предлагается отправить в ответном SMS-сообщении конфиденциальную информацию, например, платёжные реквизиты или персональные параметры доступа на информационно-платёжные ресурсы в сети Интернет. После того как только пользователь получает такое сообщение от телефонного номера, рекомендуется сообщить поставщику услуг сотовой связи.

5. Wi-Fi фишинг.

Фишинг Wi-Fi происходит, когда пользователь соединяется с Интернетом через общедоступные точки Wi-Fi. WiFiPhisher – инструмент, способный находить беспроводные сети, защищенные с использованием протокола WPA, и выводить их точки доступа из строя, затем создает поддельную WPA страницу, запрашивающую подтверждение пароля. Из-за сбоя в работе точки доступа, пользователь вынужден искать другие доступные точки, и сам не зная того подключается к поддельной сети. Это позволяет злоумышленнику выполнять атаки "человек посередине" а также использовать поддельные точки доступа для перехвата трафика.

6. Вишинг (англ. Vishing).

Вишинг — это один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленник, используя телефонную коммуникацию и играя определенную роль, например, сотрудника

банка и т.д., под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или подталкивают к совершению определенных действий со своим карточным счетом.

Методы обнаружения мобильных фишинговых атак.

Обычно системы обнаружения фишинга для мобильных устройств содержат механизм на основе фильтрации: черный список и белый список.

Механизм фильтрации: в этой технике проверяются URL - адреса. Фильтрация может быть выполнена на основе набора правил или на основе выявления статистических различий между законным и мошенническим содержанием. Данный метод может эффективно обнаруживать смишинг, вишинг и Wi-Fi фишинг.

«Черный список»: метод на основе человеческих проверок, при котором составляется список веб - сайтов, известные как фишинговые ссылки. В настоящее время такой метод поддерживается различными браузерами, которые обмениваются данными с доверенными серверами, чтобы получить черный список URL - адресов.

«Белый список»: в этом методе пользователи указывают сайты, которым они доверяют. Метод может быть применен для обнаружения атаки, где может быть предусмотрено множество законных номеров, чтобы остановить получение нежелательных SMS, содержащие поддельные веб - адреса, например смишинг.

Методы снижения мобильных фишинговых атак.

Несмотря на то, что довольно сложно определить поддельные мобильные приложения, существует несколько способов, позволяюшие снизить фишинговые атаки на мобильных устройствах:

а) Использовать официальные приложения: пользователи должны загружать приложения только из официальных магазинов.

б) Обучение пользователей: обучение пользователей очень важно, чтобы запретить пользователям переходить по неизвестным ссылкам.

в) Использовать безопасные браузеры: браузеры с функциями безопасности устраняют вредоносное программное обеспечение и сайты фишинга для защиты пользователей.

г) Контроль магазина приложений: поставщики должны предпринять дополнительные меры, прежде чем позволить разработчикам загружать приложения для общего доступа.

д) Решения в области безопасности: так же как и для обычных настольных компьютеров, разработчики средств защиты предлагают антивирусные программы для мобильных устройств. Такие программы устраняют вредоносные атаки на мобильных устройствах.

Библиографический список:

1. Mobile Phishing Attacks and Mitigation Techniques. [Электронный ресурс] // Journal of Information Security. URL: http://www.scirp.org/journal/jis/ (дата обращения: 23.01.2017).

2.Мобильный фишинг. [Электронный ресурс]. URL: http://sec4all.net/modules/myarticles/article.php?storyid=1402 (дата обращения: 23.01.2017).

3. Обзор методов борьбы с фишинговыми атаками. [Электронный ресурс]. URL: http://www.itsec.ru/articles2/focus/obzor-metodov-borby-s-fishingovymi-atakami-2 (дата обращения: 24.01.2017).

4. Почему работает фишинг и как с ним бороться. [Электронный ресурс]. URL: https://blog.kaspersky.ru/how-to-avoid-phishing/5411/ (дата обращения: 25.01.2017).