ЗАЩИТА ОТ ВРЕДОНОСНЫХ И ФЕЙКОВЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Зинов Д.А., Нурмухаметов В.Р*.*

студент 4 курс, г. Бирск, ФГБОУ ВО Бирский филиал БашГУ

Мухаметшина Г.С.

к.э.н., доцент, г.Бирск, *ФГБОУ ВО Бирский филиал БашГУ*

Согласно свежим данным StockApps, общее количество людей, пользующихся мобильными телефонами во всём мире, приблизилось к 5,3 миллиардам, или 67% населения мира. Революция в мире мобильных устройств привела к тому, что телефон потерял основную функцию средства для совершения звонков и отправки коротких сообщений и стал инструментом для развлечений, учёбы, ведения бизнеса и многого другого. Для реализации этих функций используются мобильные приложения, доступные в специализированных магазинах, таких как Apple Store или Google Play.

Миллиарды пользователей смартфонов наслаждаются удобством и развлечениями, которые предлагают современные мобильные технологии. Расширяющиеся возможности различных приложений, программного обеспечения и технологий делают наши телефоны важными инструментами для навигации в современном мире. Но по мере того, как число пользователей смартфонов продолжает расти, растет и число кибер-преступников, нацеленных на мобильные телефоны, особенно с использованием поддельных (фейковых) приложений.

Поддельные приложения создаются кибер-преступниками и содержат вредоносный код, предназначенный для кражи ваших данных. Внешний вид и функции поддельных приложений структурированы таким образом, чтобы имитировать легитимное приложение и обманным путем заставить пользователей скачать эти фейковые приложения. Когда вы устанавливаете стороннее приложение, оно запрашивает разрешение на доступ к вашим данным. Поддельные приложения используют это, чтобы получить доступ к вашей личной информации, часто без вашего ведома.

Основные способы подделки приложений.

Существует множество категорий, в которые подпадают поддельные приложения в зависимости от злого умысла кибер-преступника при их создании. Вредоносное ПО – это любой код, который подвергает риску пользователя, данные пользователя или устройство пользователя. Тип вредоносного ПО, интегрированного в поддельное приложение, может варьироваться в зависимости от функций и возможностей, и оно может относиться к любой из следующих категорий.

Имитация популярных программ.

Чем приложение популярнее, тем больше его фейковых версий будет создано. При реализации этого способа упор делается на человеческую психологию. Многие люди хотят быть в тренде и иметь на своих телефонах самые популярные приложения. Этим и пользуются мошенники: они создают клоны подобных программ, но с «побочными» функциями: перехватом вводимого текста и данных банковских карт, снятием скриншотов и т. д. Визуально они мало чем отличаются от легитимных: те же иконки, наименования, да и название производителя может быть похоже на настоящее, что показывает история о WhatsApp и его фейковом аналоге. Мало того, подделываются даже сами магазины приложений! Например, в 2014 году была обнаружена фейковая копия магазина Google Play.

При этом злоумышленники не ограничиваются только такими популярными приложениями, как WhatsApp и другие. Киберпреступники чётко следуют тенденциям происходящего в обществе. Растёт популярность криптовалют — и появляется приложение, которое выдаёт себя за известную программу для обмена криптовалютой. Появилась COVID-19 — и поддельные приложения для «борьбы с болезнью» не заставили себя ждать. Приближающиеся или проходящие крупные спортивные, культурные, политические мероприятия тоже являются поводами для выпуска множества поддельных программ.

Имитация запрещённых приложений.

Не секрет, что во многих странах по разным причинам (религиозным, этическим и т.д.) запрещены те или иные приложения. Далеко за примерами ходить не надо: в России

заблокирована социальная сеть LinkedIn, в Индии — TikTok. Мошенники подделывают запрещённое приложение и публикуют его в магазине с похожим названием и уверением в том, что оно действительно работает как оригинальное. Так, после запрета TikTok в Индии весьма быстро появилось приложение «TikTok Pro», но уже от другого производителя и с совсем другими функциями.

Злоумышленники рассчитывают на тот же фактор человеческой психологии, когда человек хочет иметь у себя на телефоне то, что популярно во всём мире, и готов ради этого ставить приложения из любого источника, не озадачиваясь вопросами информационной безопасности.

Внешние загрузки

Приложения можно установить не только из магазина, но также и с любого сайта: достаточно скачать файл определённого формата и использовать его для инсталляции. Этот способ доступен для телефонов на базе как Android, так и iOS. И здесь перед злоумышленниками открывается очень большой простор для действий: если магазины приложений регулярно проводят проверки размещённого в них контента, то владельцы сайтов этим не занимаются. К потребности в подобных загрузках приводят такие факторы, как запрет приложений определённых категорий в соответствии с законодательством, маркетинговая активность и некоторые другие. Также злоумышленники могут атаковать легитимные сайты с целью подмены безопасных приложений на вредоносные или создавать свои копии этих сайтов, выкладывая туда опасные программы.

Легитимные приложения с нелегитимной активностью.

Ещё один способ обмануть пользователя с целью получения его данных — создать легитимное приложение, которое начнёт осуществлять свою нежелательную активность спустя некоторое время. Примером может служить Barcode Scanner, который долгое время позиционировался как удобное приложение для сканирования штрих-кодов, а затем внезапно начал настойчиво показывать рекламу.

Использование уязвимостей приложений

Не всегда утечка данных из мобильных устройств может происходить по причине установки фейковой программы. Злоумышленники могут использовать уязвимости официальных приложений. Так, из-за ошибки в коде приложения Facebook могла быть реализована утечка данных 50 млн пользователей. Не остаётся без внимания злоумышленников и архитектура приложений. Используемые хранилища, алгоритмы шифрования, протоколы передачи данных — всё это исследуется хакерами для дальнейшего использования во вред пользователям.

Основные способы защиты от фейковых приложений

Лучшая защита от загрузки поддельных приложений – и, как следствие, уязвимости данных, — это точно знать, что необходимо искать. Ключевой момент – это понимание того, как проверить приложение перед его загрузкой. Обратив внимание на несколько критических факторов, прежде чем вы нажмете кнопку загрузки, вы сможете лучше защитить себя от вредоносного приложения, попавшего на ваше устройство.

Каждый пользователь мобильного устройства сам несёт ответственность за его безопасное использование и в силах сократить площадь атаки на нём. И для этого даже необязательно обладать развитыми навыками в информационных технологиях или информационной безопасности. Прежде всего необходимо закрепить основное правило: скачивать приложения только из официальных магазинов. Скачивание приложений или установочных файлов из других источников создаёт очень большой риск. При скачивании приложения из официального магазина необходимо проверять производителя, рейтинг приложения и количество установок. Если есть сомнения, дополнительную информацию могут дать комментарии пользователей, установивших приложение ранее. Для установки официального мобильного приложения можно перейти в магазин по ссылке с сайта производителя этой программы. Тогда не потребуется искать приложение по его названию и риск установки фейка будет сведён к минимуму. Ещё один способ убедиться в легитимности приложения — связаться с его производителем и уточнить интересующие вас вопросы. Следует избегать приложений, которые заведомо запрещены на территории страны — с вероятностью 99,9 % это будет поддельная программа, которая займётся сбором ваших личных данных, например. Для установленного приложения необходимо контролировать запрошенные доступы. Например, калькулятор не должен запрашивать доступ к галерее или контактам. Кроме контроля предоставляемых доступов во время установки приложения, необходимо регулярно проводить ревизию ранее предоставленных доступов. Также стоит удалять неиспользуемые приложения. Это позволит не только минимизировать риски утечки информации, но и очистить память телефона. Нельзя забывать и об элементарных правилах кибергигиены. На телефоне должен быть установлен пароль и его нельзя оставлять в общественных местах без присмотра — тогда у злоумышленников будет меньше возможностей для установки приложений без ведома хозяина гаджета. Полезно не подключаться к сетям Wi-Fi в общественных местах: они могут быть взломаны злоумышленниками, и тогда передаваемые между телефоном и сервером данные могут быть перехвачены либо модифицированы.

Еще один важный и очень простой шаг – поддерживать ваши приложения в обновленном состоянии. Регулярные обновления могут повысить безопасность вашего смартфона и снизить уязвимость к атаке. Убедитесь, что вы разрешаете обновления только непосредственно из настроек вашего телефона, и никогда не делайте это на подозрительном веб-сайте, платформе социальных сетей или даже из какого-либо приложения, обещающего обновить вашу систему.

Рекомендации для разработчиков приложений

Для того чтобы пользователь не пострадал от действий легитимного приложения, разработчики также должны соблюдать ряд правил. Одним из первых шагов должно стать внедрение системы управления информационной безопасностью в компании — разработчике приложений. Это позволит внедрить лучшие практики с целью защиты среды разработки и корпоративной сети, снижения вероятности утечки исходного кода приложения через различные каналы связи и т. д. Другим шагом должно быть внедрение концепции безопасной разработки SDL. Это позволит минимизировать количество ошибок и уязвимостей на этапе проектирования и разработки приложения. Также необходимо применение специализированных инструментов, например сканеров кода. Следует постоянно повышать осведомлённость разработчиков приложений по вопросам современных тенденций в части киберугроз. Помогут прогнозы Gartner, отчёты вендоров и интеграторов и т. д. Перед публикацией приложения в магазинах рекомендуется провести независимый анализ защищённости. Внешняя экспертиза поможет выявить новые угрозы. Необходимо регулярно обновлять приложения, не только добавляя пользовательские функции, но и исправляя программу при появлении информации об уязвимостях в ней и о методах эксплуатации этих уязвимостей. В случае если установочный файл приложения размещён на сайте, а не в магазине, необходимо регулярно проверять его на предмет нелегитимной модификации.

Приложения вошли в нашу жизнь всерьёз и надолго. И это касается не только мобильных программ, но и приложений для умных телевизоров и прочих гаджетов. Мошенничество, связанное с подобным «софтом», будет развиваться и приобретать новые направления. Борьба с этим видом преступности должна вестись всеми действующими лицами: разработчиками, владельцами магазинов приложений и, конечно же, самими пользователями. Именно совместные усилия помогут минимизировать риск использования подделок с последующей потерей данных и денежных средств пользователей.

Литература

1. Хлебников А. А. Информатика. Учебник. М.: Феникс, 2017. 448 с.

2. Ю. Родичев "Нормативная база и стандарты в области информационной безопасности" , 2017 г.

3. А. Бабаш, Е. Баранова, Д. Ларин "Информационная безопасность. История защиты информации в России", 2015 г.

4. А. Бирюков "Информационная безопасность: защита и нападение" 2-е изд., 2017 г.