УДК 004.451

Д.С. Ющик, магистрант (БГТУ, г. Минск)

УЯЗВИМОСТИ И УГРОЗЫ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Использование мобильных устройств растет. Компания Ericsson прогнозирует, что к середине 2020 году в мире будет более шести миллиардов пользователей смартфонов

Мобильные устройства прочно вошли в нашу жизнь: мессенджеры, банкинг, бизнес-приложения, личные кабинеты сотовых операторов – при современном ритме жизни мы используем эти приложения практически ежедневно. Согласно данным, общее число пользователей мобильных банковских приложений приближается к двум миллиардам, что составляет порядка 40% всего взрослого населения.

В сентябре 2018 года из официального магазина приложений было изъято 40 программ, поскольку они были заражены XcodeGhost, вредоносным ПО, предназначенным для превращения устройств Apple в крупномасштабную бот-сеть. Несмотря на хвалебную защиту Apple, вредоносная программа не только пробиралась сквозь нее, но и накладывалась поверх легитимных приложений, что затрудняло ее обнаружение.

Приложения для мобильных устройств можно классифицировать по множеству критериев, но в контексте безопасности приложений нас интересуют следующие: по месту расположения приложения и по типу используемой технологии передачи данных.

По месту расположения приложения*:*

- SIM-приложения – приложение на SIM-карте, написанное в соответствии со стандартом SIM Application Toolkit (STK);
- Web-приложения – специальная версия Web-сайта;
- мобильные приложения – приложения, разработанные для определенной мобильной ОС.

По типу используемой технологии взаимодействия с сервером:

- Сетевые приложения – используют собственный протокол общения поверх TCP/IP, например HTTP;
- SMS-приложения – приложения на основе SMS (Short Messaging Service);
- Приложение обменивается с сервером информацией с помощью коротких текстовых сообщений;
- USSD-приложения – приложения на основе USSD (Unstructured Supplementary Service Data). Сервис основывается на передаче коротких сообщений, схожих с SMS, но имеет ряд отличий;

- IVR-приложения – приложения, базирующиеся на технологии IVR (Interactive Voice Response). Система основана на заранее записанных голосовых сообщениях и тональном наборе.

Именно приложения, разработанные для определенной мобильной ОС с использованием специализированного API сейчас наиболее распространены, так как полностью используют возможности мобильного устройства.

Были выявлены типовые угрозы для мобильных приложений включающие в себя:

- Секретные данные в открытом виде;
- Небезопасные каналы передачи информации;
- Наличие отладочного кода;
- Внедрение SQL-операторов;
- Межсайтовый скриптинг (XSS);
- Отсутствие проверок входящих данных;
- Неправильная расстановка прав доступа;
- Слабая криптография.

Самые популярные типы вредоносное ПО для мобильных устройств:

- **Вредоносное банковское ПО:** Как отмечает Dark Reading, количество вредоносных мобильные программ, нацеленных на сервисы онлайн-банкинга растет: хакеры стремятся скомпрометировать пользователей, которые предпочитают вести свой бизнес, в том числе совершать денежные переводы и платежи, с мобильных устройств.
- **Мобильные программы-вымогатели:** изначально созданные для ПК, программы-вымогатели «блокируют» важные данные пользователя, такие как документы, фотографии и видео, зашифровывали эту информацию, а затем требуют выкуп за ее расшифровку. Если выкуп не выплачивается вовремя все файлы удаляются или просто блокируются и навсегда становятся недоступными для пользователя.
- **Мобильное шпионское ПО** загружается на ваше устройство как программа, отслеживает вашу активность, регистрирует ваше местоположение и изучает важную информацию, такую как имена пользователей и пароли к аккаунтам электронной почты или сайтам онлайн магазинов. Во многих случаях шпионское ПО поставляется вместе с другими считающимися безопасными программами и спокойно собирает данные в фоновом режиме. Вы даже можете не замечать его присутствия до тех пор, пока не снизится производительность устройства, или вы не запускаете на планшете или смартфоне антивирусную проверку.

- **Вредоносное ПО, передающееся через MMS:** производители вредоносных программ ищут способы использования текстовой коммуникации как способа доставки вредоносного ПО. Даже если пользователи не открывали вложение или не читали текст, вредоносное ПО все равно разворачивалось на устройстве и давало хакерам доступ к вашему смартфону.
- **Мобильное рекламное ПО:** рекламное ПО в своем развитии шагнуло далеко вперед от надоедливых всплывающих окон и простого сбора данных. Доход многих создателей рекламы зависит от количества кликов и загрузок.
- **SMS-троянцы:** киберпреступники заражают мобильные устройства, охотясь за тем, что пользователи больше всего любят в своих телефонах – текстовыми сообщениями. SMS-троянцы устраивают настоящий финансовый хаос, отправляя SMS-сообщения на премиум-номера по всему миру, в разы увеличивая телефонные счета пользователей.

Методика аудита безопасности клиентской части мобильного приложения, разработанная исследовательским центром Digital Security, основана на опыте анализа защищенности различных по функциональности и сложности приложений, таких как ERP-системы, автоматизированные банковские системы, банк-клиенты, веб-приложения, системы управления базами данных и др.

Процесс анализа приложения состоит из нескольких базовых этапов:

– Анализ архитектуры клиентской части приложения;
– Составление модели угроз;
– Аудит безопасности кода;
– Стресс-тестирование (fuzzing);
– Реализация угроз в соответствии с логикой приложения.

ЛИТЕРАТУРА

1. Positive Technologies [Электронный ресурс] // Positive Technologies. – 2003-2020. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/mobile-application-security-threats-and-vulnerabilities-2019/. – Дата доступа: 25.01.2020.

2. ПРОЕКТ "ИТ-ЗАЩИТА" [Электронный ресурс] // ИТ безопасность. – 2003-2020. – Режим доступа: http://itzashita.ru/mobilnyie-ustroystva/problemyi-bezopasnosti-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-5.html. – Дата доступа: 05.01.2020.