Безопасность при использовании мобильных устройств

Как могут взломать ноутбук или телефон, что необходимо для безопасной работы с мобильным устройством в любом месте.

Может ли ваше устройство подвергнуться риску подвергнуться заражения, взлома или повреждения? Конечно. Исследователи из Кембриджского университета выяснили, что в 87% всех смартфонов Android имеется как минимум одна критическая уязвимость, а Zimperium Labs в начале 2015 года подсчитала, что 95% устройств Android можно взломать с помощью простого текстового сообщения.

Apple также не обладают иммунитетом. В сентябре 2015 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.

Вывод? Если у вас есть мобильное устройство, вам угрожает опасность.

Популярные типы вредоносного мобильного ПО

Вредоносное ПО для мобильных устройств несравнимо по объему и сложности со своим «коллегой» для ПК, но профессионалы в области IT-безопасности наблюдают резкое увеличение количества вредоносного мобильного ПО, предназначенного для использования уязвимостей в смартфонах и планшетах. Давайте рассмотрим некоторые самые популярные его типы:

- **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. В третьем квартале 2015 года было обнаружено более 1,6 миллиона инсталляционных пакетов вредоносных программ, многие из которых были предназначены для проникновения на устройства пользователей, развертывания и сбора логинов и паролей для входа в банковские системы. Затем эти данные отправлялись обратно на командный сервер злоумышленников. В третьем квартале 2015 года мобильные банковские троянцы стали самой быстрорастущей угрозой в дикой природе.
- **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 (обычно в биткойнах) все файлы удаляются или просто блокируются и навсегда становятся недоступными для пользователя. По данным International Data Group (IDG), 74% компаний сообщили о случаях нарушения безопасности в 2015 году, причем программы-вымогатели были одной из наиболее часто встречавшихся угроз. Создатели этого типа вредоносного ПО

использовали улучшенную производительность смартфонов и анонимную сеть Tor для заражения устройств и шифрования хранящиеся на нем данных.

- **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. Как отмечает Krebs on Security, шпионское ПО теперь -это крупный бизнес: например, компания mSpy создает «легитимные» приложения для родителей или супругов, чтобы они могли «отслеживать» своих детей или партнеров. По иронии судьбы, mSpy был взломан в мае 2015 года, развенчав само понятие «безопасных» шпионских программ.
- **Вредоносное ПО, передающееся через MMS:** производители вредоносных программ ищут способы использования текстовой коммуникации как способа доставки вредоносного ПО. Как отмечает CSO Online, уязвимость Stagefright в медиа-библиотеке Android позволила злоумышленникам отправлять текстовое сообщение с вложенным вредоносным ПО на любой мобильный номер. Даже если пользователи не открывали вложение или не читали текст, вредоносное ПО все равно разворачивалось на устройстве и давало хакерам доступ к вашему смартфону. Проблема была быстро исправлена, но была доказана возможность текстовых сообщений как способа заражения мобильных устройств.
- **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. Согласно ZDNet, некоторые из них разработали специальный код «malvertising», который может заражать и запускать ваше устройство, заставляя его скачивать определенные типы рекламного ПО, которое позволяет злоумышленникам похищать личную информацию.
- **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. В 2015 году Android-устройства пользователей подверглись заражению банковским троянцем, который мог перехватывать текстовые сообщения, содержавшие финансовую информацию, а затем отправлять киберпреступникам по электронной почте копию этих сообщений, тем самым предоставляя им всю необходимые данные для проникновения в банковские аккаунты пользователей.

Современные мобильные устройства очень сложны, и это дает злоумышленникам возможности для проведения атак. Для взлома вашего смартфона может быть использовано буквально все — от Wi-Fi и Bluetooth до динамика и микрофона.

Аналитики Positive Technologies опубликовали исследование распространенных сценариев атак на мобильные устройства и приложения. В нашей статье – главные тезисы этого документа.

Как атакуют мобильные устройства и приложения

Существует пять основных сценариев атаки. Среди них:

- **Физический доступ**. Если телефон был украден или потерян, владелец отдал его в сервис или подключил к поддельному зарядному устройству по USB — все это открывает возможность для атаки.
- **Вредоносное приложение на устройстве**. Иногда такие приложения могут попасть на устройство даже из официальных источников, Google Play и App Store (для Android, для iOS).
- **Атакующий в канале связи**. Подключившись к недоверенному Wi-Fi, прокси-серверу или VPN, мы становимся уязвимыми для атак в канале связи.
- **Удаленные атаки**. Атакующий может действовать при этом удаленно, пользуясь серверами мобильных приложений или иными службами для доставки эксплойта.
- **Атаки на серверную часть**. Отдельно от всего можно рассмотреть атаки на серверную часть мобильных приложений, поскольку в этом случае доступ к устройству злоумышленнику не требуется.

Поговорим подробнее о каждом из вариантов и обсудим возможные способы защиты от таких атак.

Атаки с физическим доступом

Есть несколько главных сценариев атак с физическим доступом. Как правило, они подразумевают доступ человека напрямую к смартфону: это происходит в том случае, если устройство украли, владелец его потерял или отнес в сервис. Однако есть и достаточно необычный способ атаки, для которого используется вредоносная зарядная станция. Рассмотрим именно его.

Зарядная станция, к которой вы подключаете свой смартфон по USB, вполне может оказаться не совсем безопасной. Для современных версий ОС Android и iOS при подключении с смартфона к ПК по USB требуется разрешение на доступ к устройству. Однако на Android 4.0 и ниже этого не требовалось. В итоге при подключении таких устройств к скомпрометированным или установленным хакерами зарядным станциям, открывается возможность для атаки. Ее сценарий может выглядеть так:

- На вашем смартфоне с версией Android 4.0 или ниже доступна отладка по USB.
- Вы подключаетесь к зарядной станции по USB-кабелю.
- Вредоносная зарядная станция выполняет команду adb install malware.apk, чтобы установить вредонос на ваше устройство.
- Вредоносная зарядная станция выполняет команду adb am start com.malware.app/.MainActivity для запуска этого вредоносного приложения.
- Запущенный троян пробует различные техники повышения привилегий, получает права root и закрепляется в системе. Теперь ему доступны все хранимые данные, включая аутентификационные (логины, пароли, токены) от всех установленных приложений, а также неограниченный доступ к любому приложению во время исполнения.

Как защититься

В первую очередь, будьте внимательны и не оставляйте телефон и планшет без присмотра в общественных местах. Обязательно установите пароль для разблокировки устройства или включите биометрическую защиту, если это возможно. Не повышайте привилегии до административных (jailbreak или root), отключите отображение уведомлений на заблокированном экране.

Атаки с помощью вредоносных приложений

Есть несколько источников таких приложений:

- Официальные магазины приложений — Google Play и App Store. Редко, но даже в официальных маркетах можно найти вредоносное приложение, которое может нанести ущерб вам и вашим данным. Часто такие приложения стараются заполучить побольше установок с помощью кликбейтных названий типа «Super Battery», «Turbo Browser» или «Virus Cleaner 2019».
- Неофициальные сайты и магазины приложений (third-party appstore). Для Android-устройств достаточно разрешить установку из недоверенных источников, а затем скачать apk-файл приложения с сайта. Для iOS-устройств достаточно перейти по ссылке в браузере Safari, подтвердить установку сертификата на устройство, после чего любое приложение в этом неофициальном магазине станет доступно для установки прямо из браузера.
- Пользователь может установить скачанное из интернета приложение с помощью USB-подключения.
- Для Android-устройств доступна возможность загрузки части приложения при переходе по ссылке — механизм Google Play Instant.

При установке на смартфон в зависимости от полученных разрешений вредоносные приложения будут иметь доступ к некоторым хранимым данным, микрофону, камере, геопозиции, контактам и т. п. Также они получат возможность взаимодействия с другими установленными приложениями через механизмы межпроцессного взаимодействия (IPC/XPC). Если установленные приложения содержат уязвимости, которые можно проэксплуатировать через такое взаимодействие, вредоносное приложение сможет этим воспользоваться. Особенно актуально это для Android-устройств.

Помимо этого, вредоносное приложение может попытаться получить повышенные привилегии в системе, проэксплуатировав уязвимости, позволяющие получить root-права или jailbreak.

Как защититься

Для защиты от подобных атак рекомендуется в первую очередь избегать установок приложений из недоверенных источников. С осторожностью необходимо устанавливать и приложения с подозрительными названиями даже из официальных магазинов приложений, так как никакие проверки не работают идеально. Своевременно обновляйте ОС и приложения, чтобы исключить возможность атак через известные уязвимости.

Атаки в канале связи

Для того чтобы злоумышленник смог действовать из канала связи, ему необходимо выполнить атаку «человек посередине», то есть чтобы весь трафик, передаваемый между клиентским мобильным приложением и серверной частью проходил через устройство злоумышленника. Иногда в приложениях встречаются уязвимости, позволяющие такие атаки. К примеру, обычно при установке защищенного соединения клиентское приложение проверяет подлинность сертификата сервера и соответствие его параметров параметрам сервера. Однако иногда разработчики для удобства при работе над приложением отключают такие проверки, забывая включить их обратно в релизной версии. Как итог, приложение принимает любой сертификат сервера для установки защищенного соединения, в том числе и сертификат злоумышленника.

Даже если проверка сертификатов происходит корректно, у злоумышленника остается лазейка: под неким предлогом вынудить жертву установить на свое устройство сертификат злоумышленника как доверенный. Кроме того, если приложение само по себе безопасно работает с сервером, но содержит ссылки на сторонние ресурсы, загружаемые по HTTP, это все равно составляет возможность для проведения фишинговых атак.
Если злоумышленнику удастся получить контроль над трафиком между клиентским приложением и сервером, то это даст ему целый ряд возможностей:

- подменять ответы сервера, например для подмены реквизитов банковских операций или фишинга;
- подменять запросы клиентского приложения, например изменяя сумму перевода и счет получателя;
- перехватывать данные, например логины, пароли, одноразовые пароли, данные банковских карт, историю операций.

В итоге он узнает логины и пароли жертвы от различных аккаунтов и сможет использовать их для похищения данных, кражи денег.

Как защититься

Не подключайтесь к сомнительным точкам доступа, не используйте прокси- и VPN-серверы, которым вы не доверяете свою личную и банковскую информацию. Не устанавливайте сторонние сертификаты на устройство. Как правило, большинство популярных мессенджеров и приложений соцсетей хорошо защищены от подобных атак; если, например, вдруг какое-то из этих приложений отказывается работать через текущее Wi-Fi-подключение, это может означать, что данная точка доступа небезопасна и лучше от нее отключиться, чтобы не подвергать опасности остальные приложения, в том числе ваш мобильный банк.

Удаленные атаки

Некоторые уязвимости в мобильных приложениях можно проэксплуатировать удаленно, и для этого даже не требуется контролировать передачу данных между приложением и сервером. Многие приложения реализуют функциональность по обработке специальных ссылок, например myapp://. Такие ссылки называются deeplinks, и работают они

как на Android, так и на iOS. Переход по такой ссылке в браузере, почтовом приложении или мессенджере может спровоцировать открытие того приложения, которое умеет такие ссылки обрабатывать. Вся ссылка целиком, включая параметры, будет передана приложению-обработчику. Если обработчик ссылки содержит уязвимости, то для их эксплуатации будет достаточно вынудить жертву перейти по вредоносной ссылке.

Аналогичный образом в мобильных устройствах могут обрабатываться более привычные ссылки http:// и https:// — они могут быть переданы приложению вместо браузера, в некоторых случаях это может происходить без подтверждения со стороны пользователя.
Для Android-устройств переход по ссылке может спровоцировать загрузку Instant App, что делает возможным удаленную эксплуатацию уязвимостей, связанных с установкой вредоносного приложения.

Как защититься

Своевременная установка обновлений приложений и ОС в данном случае — единственный способ защититься. Если у вас нет возможности установить обновление или оно еще не вышло, можно временно прекратить использование уязвимого приложения: удалить его с устройства или просто разлогиниться.

Атаки на серверную часть

Для атаки на сервер мобильного приложения злоумышленнику, как правило, достаточно изучить, как происходит взаимодействие клиентского приложения с сервером, и уже исходя из собранной информации о точках входа попытаться видоизменять запросы с целью обнаружить и проэксплуатировать уязвимости. Зачастую устройство серверной части мобильного приложения ничем не отличается от веб-приложения. Как правило, устроены серверы мобильных приложений еще проще и часто представляют из себя json- или xml-api, редко работают с HTML-разметкой и JavaScript, как это часто делают веб-сайты.
Если сравнивать уязвимости веб-приложений и серверных частей мобильных приложений, то мы видим, что следующие уязвимости преобладают в мобильных приложениях:

- недостаточная защита от подбора учетных данных: 24% веб-приложений и 58% серверов мобильных приложений содержат такие уязвимости,
- ошибки бизнес-логики: 2% веб-приложений и 33% серверов мобильных приложений.

Исследования показывают, что зачастую пользователи приложений могут получать доступ к данным других пользователей: к номерам карт, имени и фамилии, номерам телефонов и т. п. Причем, доступ может ошибочно предоставляться как от имени другого пользователя так и вовсе без аутентификации, что обусловлено наличием недостатков аутентификации и авторизации.

Как защититься

В данном случае обычный пользователь мало что может сделать. Однако можно снизить риски пострадать от атак на сервер, если использовать сложный пароль, а также настроить двухфакторную аутентификацию с помощью одноразовых паролей во всех критически важных приложениях, которые это позволяют сделать. Чтобы минимизировать вероятность успешной атаки на мобильное приложение, его разработчики должны проверять возможность реализации каждого из описанных сценариев. При разработке нужно учитывать различные модели нарушителей, а некоторые меры защиты необходимо предпринять еще на стадии проектирования.

Хорошей рекомендацией для разработчиков будет внедрение практики безопасной разработки (security development lifecycle, SDL) и регулярный анализ защищенности приложения. Такие меры не только помогут своевременно выявить потенциальные угрозы, но и повысят уровень знаний разработчиков в вопросах безопасности, что повысит уровень защищенности разрабатываемых приложений в долгосрочной перспективе.

Выводы : какие меры необходимо использовать по защите вашего устройства

Итак, как защитить ваше мобильное устройство от вредоносного кода? Попробуйте выполнить эти простые шаги:

- **Используйте безопасный Wi-Fi.** Хотя переход на зараженный веб-сайт это не предотвратит, использование защищенных паролем Wi-Fi-соединений не позволяет нежелательным третьим сторонам следить за вами или совершать атаки типа «man-in-the-mobile» между вашим устройством и нужным вам адресатом.
- **Следите за своей электронной почтой.** Возможно, устройства и изменились, но угроза остается неизменной: многие злоумышленники все еще используют вредоносные вложения электронной почты, чтобы заразить ваш телефон или планшет. Не нажимайте на ссылки в письмах и других сообщениях, так как они могут направить вас на фишинговые или вредоносные сайты. Это относится ко всем мобильным платформам.
- **Быть последовательным.** Скачивайте приложения только из надежных источников. Это гарантия того, что приложения являются легитимными и не содержат вредоносных мобильных программ.
- **Установите антивирусную защиту.** Теперь антивирусные решения есть и для мобильных устройств. Установите антивирусное решение из надежного источника, запускайте его регулярно, чтобы обеспечить чистоту вашего устройства. Также следите за тем, чтобы вредоносное ПО не маскировалось под защиту от вирусов: скачивайте только легитимные приложения из надежных источников.
- **Не получайте на своем устройстве права суперпользователя.** Это увеличивает риск заражения со стороны недоверенных сторонних источников. Оставайтесь в курсе и получайте выгоду от автоматических обновлений и исправлений безопасности.