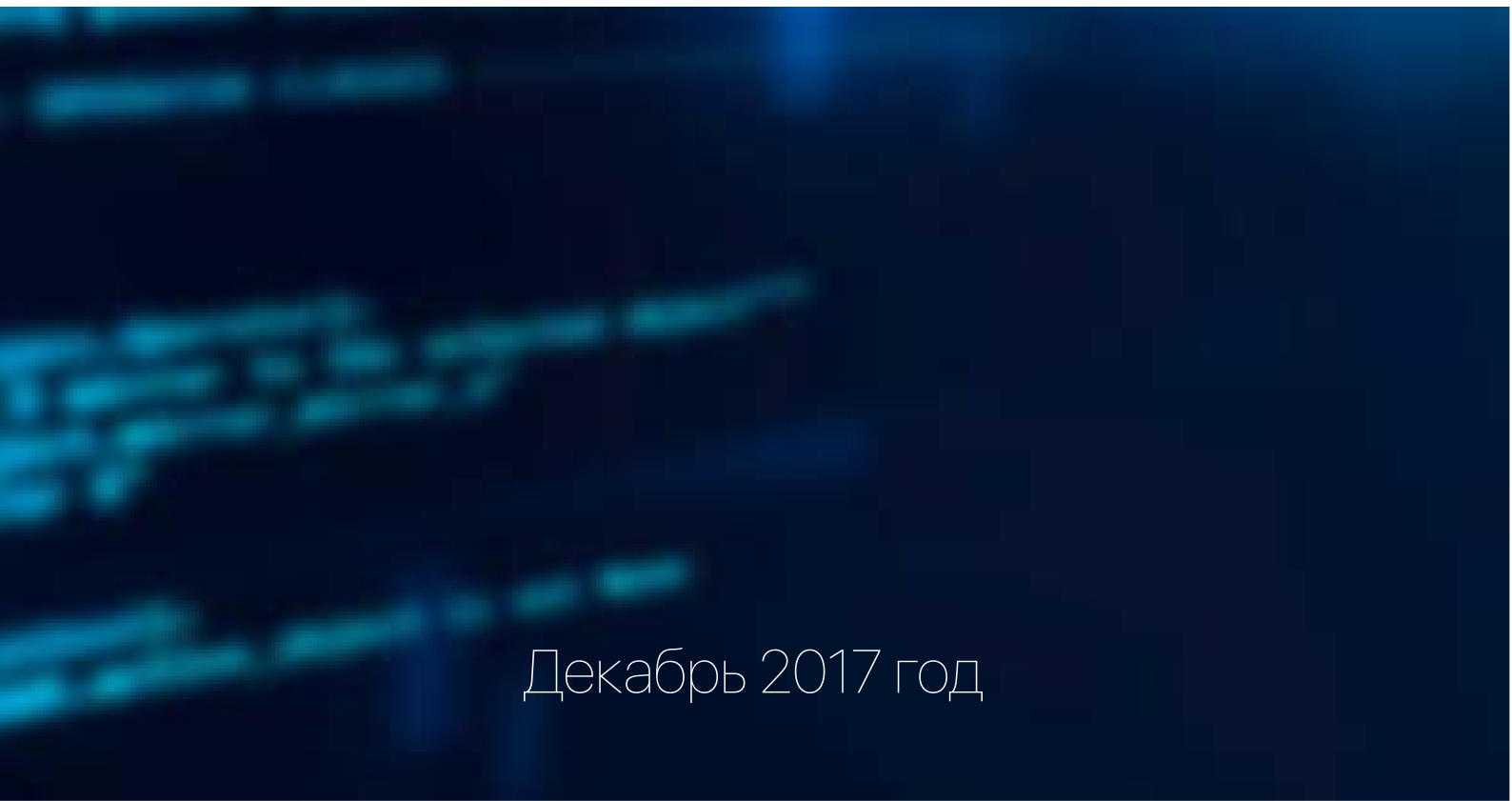

# Исследование защищенности мобильных кошельков для криптовалют



Декабрь 2017 год

# ОФИЦИАЛЬНАЯ ИНФОРМАЦИЯ (DISCLAIMER)

Данный отчет был подготовлен компанией Solar Security с целью исследования программных решений для операций с криптовалютами и испытания их функциональности. Отчет может быть использован исключительно в информационных целях.

Информация, полученная в результате проведенного исследования и изложенная в отчете, была получена при использовании технологии автоматического бинарного анализа, без осуществления реверс-инжиниринга (декомпиляции исходного кода).

Иная, содержащаяся в настоящем отчете информация была получена из источников, которые, по мнению Solar Security, являются надежными, однако Solar Security не гарантирует точности и полноты информации для любых целей.

Все упомянутые в Отчете товарные знаки являются собственностью их владельцев. Информация, представленная в этом отчете, не должна быть истолкована, прямо или косвенно, как информация, содержащая рекомендации Solar Security по инвестициям или использованию программных решений. Все мнения и оценки, содержащиеся в настоящем материале, отражают мнение авторов на день публикации и подлежат изменению без предупреждения.

Solar Security не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в данном отчете, включая опубликованные мнения или заключения, а также за последствия, вызванные неполнотой или неточностью представленной информации.

Дополнительная информация предоставляется по запросу.

# МЕТОДОЛОГИЯ

Для сравнения уровня защищенности были выбраны популярные мобильные «кошельки» для криптовалют – Airbitz[1], BitPay[2], Blockchain[3], Bread[4], Coinbase[5], Coins.ph[6], Copay[7], Luno[8] , Mycelium[9] и Xapo[10] . Все приложения рассматривались в вариантах для мобильных операционных систем iOS и Android.

Анализ безопасности кода осуществлялся автоматически, с помощью решения Solar inCode – российского программного продукта для проверки безопасности приложений. Решение использует методы статического, динамического и интерактивного анализа. При подготовке исследования модуль декомпиляции и деобфускации был отключен. Статический анализ производился в отношении бинарного кода мобильных приложений в автоматическом режиме.

Проанализировав приложения, Solar inCode сформировал отчеты, в которых была приведена общая оценка защищенности приложения по пятибалльной системе, список обнаруженных закладок, **известных** уязвимостей и ошибок, ранжированных по уровню критичности. Эти отчеты легли в основу данного исследования.

Оценка защищенности приложения считается автоматически и учитывает такие показатели, как количество различных типов известных уязвимостей критического и среднего уровня и частота их повторяемости в коде. Вклад количества критических уязвимостей более высок, при этом он не учитывает объем кода. Количество уязвимостей среднего уровня учитывается с поправкой на объем кода.

Основываясь на выборке из последних 500 сканирований, Solar inCode рассчитывает средний по отрасли уровень защищенности приложений. На момент подготовки отчета он составлял 2,3 балла.

[1]Airbitz Bitcoin Wallet for iOS v. 2.4.7; Airbitz - Bitcoin Wallet for Android v. 2.4.7.
[2]BitPay for iOS v. 3.9.1; BitPay for Android v. 3.9.1.
[3]Blockchain Bitcoin & Ether Wallet for iOS v. 2.4.6; Blockchain Bitcoin & Ether Wallet v. 6.8.2.
[4]Bread for iOS v. 2.0.4; Bread for Android v. 167.
[5]Coinbase Bitcoin Wallet for iOS v. 3.0.11; Coinbase Bitcoin Wallet for Android v. 5.0.2.
[6]Coins.ph Wallet for iOS v. 1.80; Coins.ph Wallet for Android v. 2.7.83.
[7]Copay Bitcoin Wallet for iOS v. 3.9.1; Copay Bitcoin Wallet for Android v. 3.9.1.
[8]Luno Bitcoin Wallet for iOS v. 4.0.6; Luno Bitcoin Wallet for Android v. 4.0.2.
[9]Mycelium Bitcoin Wallet for iOS v. 1.11; Mycelium Bitcoin Wallet for Android v. 2.9.10.3.
[10]Xapo Bitcoin Wallet & Vault for iOS v. 4.1.1; Xapo Bitcoin Wallet & Vault for Android v. 4.2.0.

# ВВЕДЕНИЕ

Компания Solar Security, разработчик продуктов и сервисов для целевого мониторинга и оперативного управления информационной безопасностью, представляет сравнение защищенности наиболее популярных мобильных биткоин-кошельков на базе iOS и Android.

Биткоин-кошелек – это программа, которая хранит закрытый (секретный) ключ, необходимый для доступа к криптовалюте, принадлежащей пользователю, и проведения транзакций с ней. Очевидно, что такое приложение должно обладать высоким уровнем защищенности.

Биткоин-кошельки делят на десктопные, мобильные, онлайновые и аппаратные. Мобильные биткоин-кошельки уже попадали в поле зрения СМИ и вендоров решений по информационной безопасности в связи с обнаружением уязвимостей, позволяющих злоумышленнику получить доступ к кошельку и похитить криптовалюту. Например, в 2013 году о такой уязвимости всех Android-приложений сообщала Bitcoin Foudation[1],

Это первое исследование, которое рассматривает угрозы безопасности мобильных биткоин-кошельков – от недостаточно надежных методов защиты паролей до уязвимости приложения к различным типам известных атак и эксплойтов.

При выборе приложений для сравнительного анализа учитывался критерий популярности (определяемый по числу скачиваний), а также то, насколько часто конкретное приложение попадает в различные рейтинги лучших криптовалютных кошельков.

Например, Blockchain, Coinbase, Coins.ph и Xapo для Android были скачаны свыше миллиона раз каждое. Это самые скачиваемые приложения в своем классе. Copay, Mycelium и Luno были загружены из Google Play свыше 500 000 раз. Помимо этих явных лидеров мы включили в исследование кошельки Airbitz, BitPay и Bread, которые не достигли отметки в полмиллиона скачиваний, однако их активно рекомендуют пользователи соответствующих тематических форумов и редакторы ИТ-изданий.

[1] Bitcoin.org. Android Security Vulnerability.

# НАЙДЕННЫЕ ОШИБКИ И ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ БИТКОИН-КОШЕЛЬКОВ ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ ANDROID

Сканирование показало, что чаще всего в мобильных биткоин-кошельках под Android встречаются такие известные уязвимости, как слабые алгоритмы хеширования, небезопасные реализации SSL и использование пустых паролей.

**Слабый алгоритм хеширования** повышает риски компрометации хранимой на устройстве информации – логинов, паролей и т. д. Например, хеш-функции MD2, MD5, SHA1 обладают известными уязвимостями. Нахождение коллизий для функций MD2 и MD5 не требует существенных ресурсов; аналогичная задача решена даже для более надежного SHA1. Если эти функции применяются для хранения ценной информации (например, паролей), её конфиденциальность может быть нарушена.

Кроме устойчивости к коллизиям, хеш-функция, применяемая для хранения паролей, должна быть не слишком быстрой, иначе она будет уязвима к атакам путём полного перебора.

**Небезопасная реализация SSL («пустой метод»)** приводит к тому, что при установлении защищенного соединения приложение проверяет не все параметры сертификата. Это позволяет злоумышленнику предоставить самоподписанный сертификат и реализовать с его помощью атаку Man-in-the-Middle («человек посередине»). Данная уязвимость может быть легко проэксплуатирована – например, при использовании жертвой публичного Wi-Fi. При этом конфиденциальность всех данных, передаваемых с помощью приложения, будет нарушена, а злоумышленник сможет произвольно менять запросы к серверу и выполнять любые действия с кошельком от имени легитимного пользователя.

**Пустой пароль.** Устранить угрозы безопасности, связанные с заданными в исходном коде пустыми паролями, очень сложно. Информация о том, что определённая учётная запись принимает пустой пароль, как минимум, доступна каждому разработчику приложения. Более того, после того, как приложение установлено, удалить из его кода пустой пароль можно только посредством обновления. Константные строки легко извлекаются из скомпилированного приложения декомпиляторами. Поэтому злоумышленник может просто скачать приложение, декомпилировать его с помощью инструментов, находящихся в свободном доступе в интернете, и узнать параметры специальной учётной записи. Если эти параметры станут известны злоумышленнику, администраторам системы придётся либо пренебречь безопасностью, либо ограничить доступ к приложению.

# НАЙДЕННЫЕ ОШИБКИ И ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ БИТКОИН-КОШЕЛЬКОВ ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ IOS

В iOS-версиях биткоин-кошельков чаще всего встречаются такие потенциальные уязвимости, как слабый алгоритм хеширования, слабый алгоритм шифрования и использование небезопасных параметров при установлении SSL-соединения.

**Небезопасные параметры SSL** – одна из наиболее серьезных потенциальных уязвимостей. Для установления защищённого соединения приложение должно проверять, что полученный сертификат соответствует запрошенному хосту, что срок сертификата не истёк, и что цепочка доверия восходит к одному из заданных в системе доверенных корневых сертификатов. Отключение любой из проверок (что и классифицируется как «небезопасные параметры SSL») может сделать приложения уязвимым к атаке Man-in-the-Middle и привести к компрометации передаваемых данных.

**Слабый алгоритм шифрования** не обеспечивает достаточной защиты для приложений, работающих с ценными данными. Например, криптоалгоритм DES из-за небольшой длины ключа (56 бит) может быть взломан методом полного перебора. В случае успеха злоумышленник получает доступ ко всем конфиденциальным данным пользователя.

# РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО АНАЛИЗА БЕЗОПАСНОСТИ БИТКОИН-КОШЕЛЬКОВ

Уровень защищенности Android-версий биткоин-кошельков:

| Мессенджер | Критические уязвимости | Уязвимости среднего уровня | Общий уровень защищенности |
|---|---|---|---|
| Bread | 0 | 3 | 4.4/5.0 |
| BitPay | 2 | 205 | 2.9/5.0 |
| Copay | 2 | 205 | 2.9/5.0 |
| Luno | 6 | 412 | 2.1/5.0 |
| Blockchain | 12 | 447 | 1.5/5.0 |
| Coinbase | 12 | 266 | 1.5/5.0 |
| Coins.ph | 11 | 424 | 1.5/5.0 |
| Airbitz | 17 | 715 | 1.1/5.0 |
| Xapo | 19 | 482 | 1.1/5.0 |
| Mycelium | 25 | 274 | 0.9/5.0 |

Как видно из таблицы, не самое популярное приложение Bread в несколько раз превосходит конкурентов по уровню защищенности (4,4 балла из 5). Это очень высокий показатель. Отсутствие известных критических уязвимостей и очень малое количество уязвимостей среднего уровня позволяет говорить о том, что приложение достаточно безопасно как в части защиты данных пользователей, так и в устойчивости к атакам с помощью троянов или известных эксплойтов.

Приложения BitPay и Copay разработки корпорации BitPay, Inc. обладают абсолютно одинаковым набором уязвимостей и, как следствие, одинаковым рейтингом. Они делят второе место. Достаточно неплохой результат продемонстрировало приложение Luno – примерно на уровне среднего значения по отрасли.

Ниже среднего расположились приложения Blockchain, Coinbase Coins.ph, Airbitz, Xapo и Mycelium. Эти приложения содержат практически те же типы уязвимостей, что лидеры рейтинга, но количество вхождений (повторов в коде) в этих биткоин-кошельках существенно выше.

# РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО АНАЛИЗА БЕЗОПАСНОСТИ БИТКОИН-КОШЕЛЬКОВ

Уровень защищенности iOS-версий биткоин-кошельков:

| Мессенджер | Критические уязвимости | Уязвимости среднего уровня | Общий уровень защищенности |
|---|---|---|---|
| Bread | 0 | 24 | 4.5/5.0 |
| BitPay | 4 | 211 | 2.4/5.0 |
| Copay | 5 | 306 | 2.2/5.0 |
| Luno | 5 | 422 | 2.2/5.0 |
| Blockchain | 11 | 283 | 1.6/5.0 |
| Coinbase | 11 | 283 | 1.6/5.0 |
| Coins.ph | 17 | 386 | 1.2/5.0 |
| Airbitz | 24 | 586 | 0.9/5.0 |
| Xapo | 56 | 414 | 0.3/5.0 |
| Mycelium | 148 | 504 | 0.0/5.0 |

Как можно видеть, Bread и в версии для iOS остается безусловным лидеров с еще более высоким показателем – 4,5 балла из 5. Очевидно, разработчик, компания Breadwallet, сознательно уделяет большое внимание безопасности, так как приложение не содержит потенциальных уязвимостей, которые часто возникают вследствие халатности и пренебрежения вопросами защищенности (как, например, слабый алгоритм хеширования).

Приложение Mycelium, которое заняло последнее место в сравнении Android-версий, продемонстрировало неожиданно высокий уровень защищенности iOS-версии - 2,4 балла из 5. Третье место разделили приложения Blockchain и Coinbase.

Удивительно низкий уровень защищенности был выявлен у приложения Xapo – в основном за счет большого числа вхождений критических уязвимостей.

# ВЫВОДЫ

Средний уровень защищенности биткоин-кошельков для платформ Android и iOS примерно равен. Но в каждом случае все зависит от выбора конкретного приложения: Mycelium в реализации для Android содержит гораздо больше потенциальных уязвимостей, чем для iOS, а BitPay и Copay, напротив, лучше использовать на Android-устройствах. Единственный биткоин-кошелек, показавший отличные результаты в обоих сравнениях, это приложение Bread.

В тройку наиболее защищенных биткоин-кошельков для Android вошли Bread, BitPay/Copay и Luno. Лидерами среди iOS-приложений для операций с криптовалютами стали Bread, Mycelium и Blockchain. Самый низкий совокупный результат у приложения Xapo.

Среди наиболее частых уязвимостей можно выделить небезопасную реализацию SSL, а также слабые алгоритмы шифрования и хеширования. Успешная эксплуатация этих уязвимостей может привести к компрометации логинов, паролей и всего трафика, идущего через приложение. На практике это грозит пользователям взломом кошелька и кражей криптовалюты.

Не все выявленные уязвимости одинаково легко эксплуатируются, однако приложения, оперирующие валютами, не должны небрежно относиться к любым потенциальным уязвимостям.

# КОНТАКТЫ


## Solar Security

127 015 г. Москва, ул. Вятская 35/4,
БЦ «Вятка» 1 подъезд

Телефон офиса: +7 499 755 07 70
Техническая поддержка: +7 499 755 02 20

Email: info@solarsecurity.ru

www.solarsecurity.ru