Исследование защищенности мобильных приложений для мгновенного обмена сообщениями.

2017 год

ОФИЦИАЛЬНАЯ ИНФОРМАЦИЯ

Данный отчет был подготовлен компанией Solar Security с целью исследования программных решений для мгновенного обмена сообщениями 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 бесплатные мобильные приложения для мгновенного обмена сообщениями – Facebook Messenger[1], QQ International[2], Signal[3], Skype[4], Slack[5], Telegram[6], Viber[7], WeChat[8] и WhatsApp[9]. 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, 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 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 2,2 балла.

1 Facebook Messenger for iOS v. 103.0; Facebook Messenger for Android v. 103.0.0.12.69.
2 QQ International for iOS v. 4.8.2; QQ International for Android v. 5.1.2.
3 Signal for iOS v. 2.6.15; Signal for Android v. 3.28.4.
4 Skype for iOS v. 6.30; Skype for Android v. 7.29.
5 Slack for iOS v. 3.12; Slack for Android v. 2.27.0.
6 Telegram for iOS v. 3.16.1; Telegram for Android v. 3.16.
7 Viber for iOS v. 6.6.0; Viber for Android v. 6.6.0.888.
8 WeChat for iOS v. 6.5.4; WeChat for Android v. 6.5.4.
9 WhatsApp for iOS v. 2.17.2; WhatsApp for Android v. 2.17.24.

ВВЕДЕНИЕ

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

При выборе мессенджеров для сравнительного анализа учитывались несколько критериев.

Первый – это общепризнанный показатель популярности IM-приложения – ежемесячное число активных пользователей (monthly active users - MAU).

Второй – популярность мессенджера в России и третий – позиционирование мессенджера как «защищенного», «безопасного».

В качестве объектов исследования мы выбрали WhatsApp (ежемесячное число активных пользователей – около 1,2 млрд[10]), Facebook Messenger (ежемесячное число активных пользователей – свыше 1 млрд[11]), QQ International и WeChat с аудиторией активных пользователей в 899 млн и 806 млн соответственно[12]. Также в исследование вошли Skype (ежемесячная аудитория – 300 млн[13]), Viber (260 млн[14]) и Slack[15] (4 млн активных пользователей ежедневно).

И, наконец, мы включили в исследование мессенджеры, создатели которых заявляют, что главная характеристика их мобильных приложений – защищенность. Это Telegram (около 100 млн пользователей[16], 6 млн в России[17]) и Viber. Мы не смогли обнаружить достоверной статистики по популярности последнего, но пройти мимо мессенджера, который рекомендуют Эдвард Сноуден[18] и Брюс Шнайер[19], было бы неправильно.

10 Insider. 11 главных цифр из отчета Facebook.

11 VC.ru. Ежемесячная аудитория Facebook Messenger достигла отметки в 1 млрд пользователей.

12 Techinasia. WeChat reaches 800m active users, but it's close to the bamboo ceiling.

13 MSPoweruse. Skype has more than 300 million monthly active users, will get bots.

14 Expandedramblings.com. By the Numbers: 26 Amazing Viber Stats (January 2017).

15 Expandedramblings.com. 38 Amazing Slack Statistics (November 2017).

16 Ведомости. Аудитория Telegram Павла Дурова достигла 100 млн человек.

17 Ведомости. База активных пользователей Telegram в России за год выросла в 3 раза и достигла 6 млн.

18 The Daily Dot. Edward Snowden tells you what encrypted messaging apps you should use.

19 Open Whisper Systems.

НАЙДЕННЫЕ ОШИБКИ И ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ

Сканирование мессенджеров показало, что наиболее частые критические уязвимости приложений-мессенджеров для платформы Android – это слабые алгоритмы хеширования, небезопасные реализации SSL, использование пустых паролей, слабые алгоритмы шифрования и небезопасные алгоритмы дополнения при шифровании.

Все эти уязвимости можно разделить на две группы, в зависимости от характера возможной эксплуатации:

Уязвимости приложения, ослабляющие защищенность хранимой и обрабатываемой информации. Слабый алгоритм хеширования, слабый алгоритм шифрования, недостаточно стойкие параметры алгоритма шифрования повышают риски компрометации хранимой на устройстве информации – логинов, паролей, переписки и т. д. Как правило, уязвимости такого типа могут быть проэксплуатированы при помощи вредоносного программного обеспечения, которое в свою очередь подразделяется на универсальные трояны-сборщики либо трояны, написанные специально под конкретное приложение.

Уязвимости, позволяющие проводить атаку Man-in-the-Middle («человек посередине»). Небезопасная реализация SSL («пустой метод») приводит к тому, что при установлении защищенного соединения приложение проверяет не все параметры сертификата. Это увеличивает риск подмены сертификата и перехвата данных, которые пользователь передает посредством мессенджера. Данная уязвимость может быть достаточно легко проэксплуатирована при использовании общественного Wi-Fi, в этом случае злоумышленник пропускает через себя весь трафик между мессенджером жертвы и сервером.

Те же уязвимости чаще всего встречаются в iOS-версиях мессенджеров – **слабый алгоритм хеширования и шифрования, небезопасная реализация SSL (в том числе при использовании библиотеки AFNetworking).** В отличие от платформы Andoid, для платформы iOS первая группа уязвимостей является менее опасной (если к устройству не был применен Jailbreak).

РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО АНАЛИЗА БЕЗОПАСНОСТИ МЕССЕНДЖЕРОВ

Уровень защищенности Android-версий приложений для мгновенного обмена сообщениями:

	Критические уязвимости	Уязвимости среднего уровня	Уязвимости низкого уровня	Общий уровень защищенности
Signal	0	6	7	4.3 / 5.0
Facebook Messenger	4	17	15	1.8 / 5.0
Slack	4	18	17	1.7 / 5.0
Telegram	3	20	18	1.4 / 5.0
Skype	3	23	15	1.2 / 5.0
Viber	2	20	18	1.2 / 5.0
WhatsApp	4	22	16	0.9 / 5.0
QQ International	8	21	22	0.4 / 5.0
WeChat	5	26	17	0.4 / 5.0

Как видно из таблицы, Signal в несколько раз превосходит конкурентов по уровню защищенности (4,3 балла из 5). Это очень высокий показатель. Отсутствие серьезных уязвимостей 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.

В приложениях Facebook Messenger, Slack, Telegram, Skype, Viber и WhatsApp для Android был обнаружен схожий набор уязвимостей, однако в Facebook Messenger и Slack эти уязвимости встречались реже. Этим обусловлены более высокие баллы Facebook Messenger и Slack – 1,8 и 1,7 баллов соответственно. Больше всего уязвимостей обнаружено в китайских мессенджерах QQ International и WeChat (оба разрабатываются компанией Tencent Holdings Ltd).

Те же мессенджеры в версии для мобильной операционной системы iOS демонстрируют большее количество уязвимостей – как по типам, так и по частоте встречаемости в коде. Тем не менее, Signal и Facebook Messenger остаются в числе лидеров по уровню защищенности.

РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО АНАЛИЗА БЕЗОПАСНОСТИ МЕССЕНДЖЕРОВ

Уровень защищенности iOS-версий приложений для мгновенного обмена сообщениями:

	Критические уязвимости	Уязвимости среднего уровня	Уязвимости низкого уровня	Общий уровень защищенности
Facebook Messenger	12	291	0	1.5 / 5.0
Viber	15	654	0	1.3 / 5.0
Skype	17	324	0	1.2 / 5.0
Signal	20	79	0	1.1 / 5.0
WhatsApp	21	332	0	1.0 / 5.0
Slack	23	330	0	0.9 / 5.0
Telegram	77	420	0	0.2 / 5.0
QQ International	891	2276	0	0.0 / 5.0
WeChat	1532	1624	0	0.0 / 5.0

Как можно видеть, QQ International и WeChat и в версии для iOS остаются самыми ненадежными мессенджерами с большим отрывом по числу найденных уязвимостей.

ВЫВОДЫ

Версии мессенджеров для платформы Android оказались более защищенными по сравнению с реализациями под iOS. Скажем, средний балл трех наиболее защищенных Android-приложений – 2.6, тогда как для iOS этот показатель равен 1.3.

Среди наиболее частых уязвимостей можно выделить:

- небезопасную реализацию SSL
- алгоритмы шифрования и хеширования

Успешная эксплуатация этих уязвимостей может привести к компрометации логинов, паролей и переписки пользователей.

Не все выявленные уязвимости одинаково легко эксплуатируются, однако мессенджеры, которые позиционируются, в первую очередь, как защищенные, не должны небрежно относиться к любым потенциальным уязвимостям.

В тройку наиболее защищенных мессенджеров для Android вошли Signal, Facebook Messenger и корпоративный мессенджер Slack. При этом Signal, рекомендованный Эдвардом Сноуденом, действительно показал очень высокий результат. Хорошее качество кода продемонстрировали Facebook Messenger и Slack, который позиционируется как корпоративный мессенджер и уже получил звание самого быстрорастущего[24] бизнес-приложения в истории.

Лидерами среди iOS-приложений для мгновенного обмена сообщениями стали Facebook Messenger, Viber и Skype – впрочем, с не самыми высокими баллами за защищенность. Четвертое место с небольшим отставанием занял Signal.
Китайские мессенджеры QQ International и WeChat оказались наименее защищенными вне зависимости от платформы.

24 Fast company. With 500,000 Users, Slack Says It's The Fastest-Growing Business App Ever

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