УДК 004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.083

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ МЕСЕНДЖЕРА SIGNAL

Рєзніченко Д.Ю.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: dymytrii.rieznichenko@nure.ua

This work is devoted to a forensic investigation of the Signal messenger developed by Open Whisper Systems. The internal structure of the messenger, as well as its mechanisms for protecting confidential user data, will be considered. In addition, the working directories of the Signal messenger in the Android and Windows operating systems will be investigated.

У сучасному світі питання захисту конфіденційних даних має найвищій пріоритет для будь-якої компанії, яка розробляє власну систему обміну мультимедіа та швидкими текстовими повідомленнями між користувачами. З цією метою, розробники мобільних додатків (зокрема месенджерів) намагаються реалізувати у власному програмному продукті найбільш сучасні та ефективні криптографічні рішення, а деякі компанії навіть створюють власні протоколи шифрування. Але, чи є ці рішення та протоколи настільки надійними та, чи дозволяють вони безпечно зберігати дані на кінцевому пристрої користувача – відповідь на ці питання можна знайти у даній роботі.

Останнім часом дуже швидко набирає популярність месенджер Signal від компанії Signal Technology Foundation. Даний месенджер надає користувачам можливість створювати зашифровані повідомлення, пересилати медіафайли, а також здійснювати безпечні голосові та відеодзвінки. Також, Signal Messenger надає користувачу велику кількість налаштувань безпеки: розблокування месенджера за відбитком пальця (або пароля), відключення можливості створення скриншотів у приватних чатах, захист IP-адреси під час голосових дзвінків та інше.

Крім вищезазначених механізмів безпеки, у месенджері Signal використовується власний криптографічний протокол Signal Protocol (раніше – TextSecure Protocol) від компанії Open Whisper Systems. Варто також додати, що Signal Protocol працює разом з наступними алгоритмами і протоколами: XEdDSA та VXEdDSA (створення та перевірка цифрових підписів), X3DH (встановлення спільного секретного ключа між сторонами спілкування), PQXDH (додатковий протокол встановлення спільного секретного ключа разом із можливістю його взаємної автентифікації), Double Ratchet (використовується для шифрування повідомлень на основі спільного секретного ключа) та Sesame (використовується для управління

сеансами шифрування повідомлень у асинхронному середовищі з різними типами пристроїв)[1].

Далі розглянемо, де месенджер зберігає дані користувача. Так, комп'ютерна версія месенджера Signal зберігає дані користувача (разом із артефактами) у локальній директорії «%AppData%\Signal\». У цій директорії можна знайти папку «\databases» із зашифрованим файлом, який має назву «Databases.db». Мобільна версія месенджера Signal зберігає аналогічну базу даних у закритій директорії «data\data\org.thoughtcrime.securesms\databases\signal.db» (потрібні root-права для доступу). Загалом, ці два файли містять у собі однакову інформацію (артефакти) про користувача та є зашифрованими криптографічним алгоритмом AES у режимі AES-GCM. Цікавим є той факт, що у випадку з комп'ютерною версією месенджера Signal, криптографічний ключ для розшифрування бази даних «Databases.db» зберігається у тій самій директорії (поряд із базою даних) у файлі «config.json» у відкритому вигляді.

У мобільній версії месенджера вищезазначений криптографічний ключ можна знайти у директорії «data\keystore\"username"\». Варто підмітити, що для розшифрування бази даних на мобільній версії месенджера Signal, окрім ключа, потрібно ще використати рядки «ciphertext» та «authTag», які можна знайти у директорії «\org.thoughtcrime.securesms\shared_prefs\»[2].

Розшифрування вищезазначених баз даних може проводитися з використанням інструмента «SQLCipher»[3], який є доповненням для програмного забезпечення SQLiteStudio, що дозволяє переглядати вміст баз MySQL. У директорії «%AppData%\Signal\» можна також знайти папку «Network», в якій знаходиться файл «Trust Tokens», що зберігає значення довірених токенів. Ці токени використовуються месенджером для автентифікації користувача на серверах додатку. Самі токени зберігаються у зашифрованому вигляді. Інший файл у тій же папці, який має назву «Network Persistent State», зберігає інформацію про налаштування HTTP-сервера та тип мережного з'єднання, які використовує додаток Signal.

Крім усього вищезазначеного, у директорії «%AppData%\Signal\» можна також знайти наступні корисні артефакти: папка «Session Storage» (інформація про сесії користувача), папка «logs» (зберігається інформація про всі запити, які здійснює додаток по відношенню до сервера, разом із посиланнями на конкретні ресурси), папка «attachments.noindex» (локальне сховище графічних зображень месенджера), папка «stickers.noindex» (локальне сховище стікерів, які використовує користувач у чатах), файл «ephemeral.json» (містить інформацію про розміри вікна месенджера та місце розташування цього вікна на робочому столі), файл «Local State» (містить значення криптографічного ключа, який використовується для шифрування локальних технічних файлів месенджера), файл «Preferences» (містить значення «солі», яка додається до ідентифікатора користувацького

пристрою, а також деякі дані про мови інтерфейсу, які використовує користувач).

Тепер розглянемо внутрішню будову бази даних «Databases.db». Загалом, у даному файлі можна знайти такі основні таблиці (артефакти): «groups» (містить ідентифікатор групи, перелік учасників, назву групи тощо), «mms» (архів текстових повідомлень користувача разом із часовими мітками), «one_time_prekeys» (перелік одноразових ключів, які використовуються для створення безпечних сесій у месенджері), «identities» (ідентифікатор користувача, персональний криптографічний ключ, ім'я користувача тощо), «sms» (схожа на «mms», але містить більше інформації про повідомлення), «storage_key» (ключ, який використовується для розшифрування файлів із локального сховища даних користувача) та інші. Наостанок необхідно розглянути, яким чином месенджер Signal зберігає медіафайли, які користувачі пересилають у чатах. Як вже було сказано раніше, комп'ютерна версія месенджера зберігає медіафайли (фото та відео) і ці дані знаходяться у директорії «%AppData%\Signal\attachments. noindex» (в Android взагалі створюється окреме ізольоване сховище). Усередині даної директорії знаходиться велика кількість папок, імена яких, як правило, складаються з двох символів (число та буква латинського алфавіту). Цікавим є те, що переслане через користувацький чат графічне зображення, месенджер зберігає у декількох папках одразу: в одній – повноцінне зображення (розмір, наприклад, 1152x2048 пікселів), а у другій – його обрізана копія (розмір 150x150 пікселів). Причому, кожен новий пересланий медіафайл зберігається в іншу папку (вибір папки відбувається випадковим чином). Крім усього вищезазначеного, якщо переглянути метадані цих зображень, то можна побачити, що їх розмір (простір, який вони займають на диску), а також значення параметра «Bit depth» (інформація про кольори зображення) теж відрізняються. Варто також додати, що месенджер автоматично видаляє практично всі корисні метадані зображень та інших медіафайлів. Загалом, варто зробити висновок, що месенджер Signal є доволі цікавим додатком з точки зору цифрової криміналістики, оскільки він надає велику кількість механізмів захисту, але паралельно самостійно створює слабкі місця у власній системі безпеки (наприклад, зберігає криптографічні ключі у відкритому вигляді).

Список використаних джерел:

1. Technical information [Електронний ресурс] // 2024. Режим доступу: https://signal.org/docs/. Decrypting Signal DB for Android [Електронний ресурс] // 2021. Режим доступу: https://rado0z.github.io/Decrypt_Android_Database.SQLCipher Community Edition [Електронний ресурс] // 2024. Режим доступу: https://www.zetetic.net/sqlcipher/open-source/.