УДК 004.056.5

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ВРАЗЛІВОСТІ МЕСЕНДЖЕРА WHATSAPP

З останнім часом проблема безпеки програмного забезпечення є однією з самих важливих в області інформаційної безпеки. Особливо, якщо використовуються найбільш популярні безкоштовні месенджери. Так по інформації Internet енциклопедії зі вільним контентом – Вікіпедії, кількість активних користувачів WhatsApp на початок 2020 року становить близько 1 мільярда, а кількість повідомлень, що відправляються, приблизно 65 мільярдів за тиждень. Звичайно, така величезна база користувачів WhatsApp – очевидна мета кіберзлочинців.

Зрозуміло, офіційні магазини додатків – App Store в iOS і Google Play в Android – досить серйозно ставляться до проблеми безпеки програмного забезпечення. В інтернеті картина далеко не настільки оптимістична, чим і користуються хакери, спамери та інші кіберкримінальні елементи. Відомі випадки, коли зловмисники видавали шкідливе програмне забезпечення за офіційний додаток WhatsApp. Відповідно, після завантаження і установки комп'ютер, смартфон або інший гаджет опинявся скомпрометований. Однак, найчастіше хакери використовували і використовують уразливості безпосередньо в самому мессенджері WhatsApp.

Під час пересилки повідомлень в WhatsApp застосовується наскрізне шифрування і розшифрувати інформацію, що циркулює, можуть тільки одержувач і відправник. Таким чином, дане шифрування дозволяє захиститися безпосередньо від перехоплення під час передачі даних. Однак, така функція абсолютно не захищає повідомлення після дешифрування на пристроях користувачів.

У WhatsApp передбачено створення резервної копії повідомлень та іншого контенту в Android і iOS. Ця важлива функція дозволяє відновлювати випадково видалені повідомлення. Крім резервної копії в хмарах Google Drive, iCloud також існує локальна резервна копія на пристроях

користувачів. Резервні файли, що зберігаються на Google Drive та iCloud, не зашифровані, і звичайно ці хмарні сервіси можуть бути уразливі так само, як і локальні резервні копії.

Починаючи з жовтня 2014 року, WhatsApp належить Facebook Inc. За останні роки соціальна мережа Facebook багаторазово піддавалася критиці. У 2016 році WhatsApp оновив політику конфіденційності, дозволивши робити доступною інформацію з WhatsApp в Facebook. У січні 2019 року починається створення єдиної інфраструктури для всіх платформ обміну повідомленнями: Facebook, Instagram, і WhatsApp. Таким чином, сьогодні кожен сервіс працює як окремий додаток, але частина переданої інформації, наприклад, час останнього використання сервісу, номер телефону та інші дані відправляються через єдину мережу.

Протягом багатьох років статус WhatsApp (короткий рядок тексту) був єдиним способом повідомити, чим ви займаєтеся в даний момент. Потім ця функція переросла в WhatsApp Status, що представляє собою клон популярної опції Stories в Instagram. Але соціальна мережа Instagram від самого початку призначена для публічного використання (при бажанні можна зробити свій профіль прихованим). З іншого боку, месенджер WhatsApp орієнтований для приватного спілкування з друзями, родиною, родичами, тобто, передбачається, що статус користувача WhatsApp повинен бути приватним. На жаль це не так. За замовчуванням будь-який зі списку контактів користувача WhatsApp може переглядати його статус. Однак в WhatsApp можна управляти видимістю свого статусу. У розділі Settings (Налаштування) > Account (Акаунт) > Privacy (Конфіденційність) > Status (Статус) є три варіанти конфіденційності:

- My contacts (Мої контакти).
- My contacts except ... (Контакти, крім ...).
- Only share with ... (Поділитися з ...).

Перевагою WhatsApp є те, що всі заблоковані контакті не можуть бачити статус незалежно від налаштувань конфіденційності. Також, як і у випадку з опцією Stories в Instagram, будь-які відео і фотографії, додані в статус, зникнуть через 24 години.

Все сказане дозволяє зробити висновок, що існують досить неоднозначні проблеми безпечного використання мессенджера WhatsApp пов'язані з конфіденційністю даних і поширенням важливої інформації. Крім того, відомі критичні уразливості програмного забезпечення ме-

сенджера, за допомогою яких зловмисники можуть віддалено скомпрометувати пристрій і викрасти захищені повідомлення чату та файли.

До честі Facebook Inc потрібно відзначити, що виявлені вразливості WhatsApp не залишаються без уваги, а випускаються відповідні оновлення. Крім того, в рамках програми винагород за виявлені вразливості у програмному забезпечені компанії, дослідники отримують фінансову винагороду. Так на початку 2020 роки за виявлені вразливості високого ступеня небезпеки, що дозволяють зловмисникам віддалено викрадати файли персональних комп'ютерів під управлінням Windows і macOS, дослідник отримав винагороду $12500. Звідси можна зробити ще один висновок про необхідність своєчасного оновлення програмного забезпечення для забезпечення безпеки. Той малий час, витрачений на оновлення, дозволяє заощадить масу зусиль і коштів, витрачених на чистку комп'ютера або смартфона від вірусів або дещо чого гірше, начебто крадіжки, відновлення цінної інформації та спілкування з кіберзлочинцями.

Одержано 01.05.2020