ПРОБЛЕМИ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧА ПРИ ВИКОРИСТАННІ НЕОФІЦІЙНИХ ПРОШИВОК ДЛЯ ANDROID СМАРТФОНІВ

Главчев Д.М., Борисов П.С., Попелло М.С.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Смартфон зараз є не лише засобом зв'язку, але й пристроєм для виконання робочих завдань, виконання банківських операцій, тощо. Такий спектр можливостей є зручним користувачу, але він є привабливим для зловмисників, які хочуть отримати доступ до конфіденційних даних, або банківських рахунків.

Google піклується про безпечність додатків, тому компанією була створена спеціальна система дозволів (Permissions), за допомогою яких можна відкривати додатку доступ до мережі інтернет файлової системи, даних користувача [1]. Завдяки цій системі, додаток «калькулятор» який просить в користувача доступ до списку контактів буде викликати підозру, цей доступ можна заблокувати. Але чи можна довіряти самій операційній системі (ОС), яка встановлена на смартфоні? Адже, існує багато різноманітних форумів, де користувачам пропонуються оновлені народними умільцями прошивки, які дозволяють старий телефон оновити до нової версії ОС, підвищити швидкодію. Умови привабливі, тому користувачі можуть піти на такий крок і встановити сторонню прошивку.

Компанія Google надає можливість скачати початковий код операційної системи, який розміщено на сайті AOSP у відкритому доступі[2]. Тому кожен бажаючий може скачати та виконати зборку повноцінної операційної системи модифікувавши її будь-яким чином. Додавання до операційної системи «сплячого процесу», який має доступ до мережі інтернет, даних користувача, тощо, не є великою проблемою. Достатньо створити відповідний додаток-сервіс, та розмістивши його код у директорії vendor проекту, та створивши bp файл, скомпілювати разом с ОС. Крім того, можна модифікувати вже встановлені в систему додатки для здійснення дзвінків, тощо, щоб вони передавали дані зловмисникам. Для доступу до сплячого в системі процесу можна застосувати AIDL інтерфейс, за допомогою якого, будь-який додаток зможе дані у сервісу. При цьому, додаток не потребуватиме необхідності мати доступ до чутливої інформації, тому не буде викликати підозр в користувача. А так як окрім прошивок зловмисники можуть створювати свої версії популярних додатків, можна тільки здогадатися, куди підуть усі дані, до яких вбудований процес зможе отримати доступ. Запобігти цим проблемам можна, якщо не встановлювати на смартфон неофіційні версії прошивок та додатків.

Література:

1. Android Permissions Overview. URL: https://developer.android.com/guide/topics/permissions.
2. Android OS Core Topics. AOSP. URL: https://source.android.com/core.