Журнали подій операційних систем Android в комп'ютерно-технічній експертизі

Юрій Божко

старший судовий експерт, Сумський НДЕКЦ МВС України, м. Суми, Україна,
e-mail: yuriybozhko93job@gmail.com

Розглянуто дослідження журналів подій операційних систем Android в комп'ютерно-технічній експертизі. Проаналізовано типи записів журналів подій, проблеми, з якими можуть зіткнутися експерти під час вилучення та аналізування даних. Наведено приклади записів із різними типами повідомлень, розглянуто можливості використання цієї інформації для збирання доказів.

Ключові слова: *журнали подій; Android, цифрова криміналістика, комп'ютерно-технічна експертиза, лог-файли, root-доступ, Android Debug Bridge, цифрові докази, мобільні пристрої.*

Android operating system event logs in computer forensics

Yurii Bozhko

The paper outlines the study of Android operating system event logs in computer forensics. Types of event log entries and problems forensic experts face when extracting and analyzing data are analyzed. The author provides examples of entries with different types of messages and considers the possibilities of using this information for evidence collection.

Keywords: *event logs; Android; digital forensics; computer forensics; log files; root access; Android Debug Bridge; digital evidence; mobile devices.*

Відомості з журналів подій можуть містити інформацію, яка з тих чи тих причин недоступна під час дослідження інших джерел. Дослідження таких журналів дає змогу отримати дані про активність пристрою, інформацію про взаємодії між застосунками та в деяких випадках відтворити послідовність дій, що відбулись у певні проміжки часу. Також аналіз записів дає змогу виявити та дослідити шкідливу активність, яка може бути спричинена шкідливим програмним забезпеченням. Журнали операційної системи можуть також допомогти виявити технічні проблеми, які можуть бути пов'язані з помилками в роботі операційної системи.

Проте при спробі отримати доступ до журналів подій ОС Android можуть виникати різні проблеми, пов'язані з обмеженнями системи безпеки, політикою конфіденційності та технічними аспектами. Найбільш частою проблемою при спробі дослідити журнали може бути обмежений доступ через налаштування безпеки. Наприклад, у сучасних версіях Android (починаючи з Android 4.1 Jelly Bean) доступ до системних журналів значно обмежений через міркування безпеки. У більшості випадків застосунки можуть зчитувати тільки власні журнали. Для доступу до системних журналів, які містять інформацію про дії інших застосунків і системних процесів, потрібен root-доступ. Більш сучасні версії Android застосовують шифрування пристрою. Без доступу до ключа шифрування (пароль, PIN-код або біометричні дані) вилучити інформацію з розділів системи, які містять зокрема й журнали, не виявляється можливим. Ще однією проблемою є обмежена тривалість зберігання журналів. Зазвичай записи журналів Android не зберігаються тривалий час і можуть бути автоматично перезаписані новими подіями. Такий алгоритм роботи означає, що важливі записи можуть бути перезаписані, якщо пристрій працював тривалий час або був активним

довгий час після події, що підлягає розслідуванню.

Шифрування журналів деяких застосунків, особливо тих, що орієнтовані на конфіденційність (наприклад, месенджери або фінансові застосунки). Такі застосунки можуть шифрувати власні журнали подій або не зберігати їх взагалі. Це обмежує можливість вилучення та дослідження даних із таких застосунків через звичайний доступ до системних журналів.

Наявність стороннього шкідливого програмного забезпечення на пристрої може впливати на роботу системи в такий спосіб, щоб спотворити або видалити журнали подій або записи з них. Деяке шкідливе програмне забезпечення може навмисно змінювати системні журнали для приховування своєї активності.

Журнали подій в Android можуть містити багато різних типів записів, які стосуються роботи як системи, так і застосунків. Слід зазначити, що записи журналів ОС Android зазвичай позначаються літерами, які виокремлюють тип запису, наприклад:

I — інформаційні повідомлення (Info);

E — помилки (Error);

W — попередження (Warning);

D — повідомлення про налагодження (Debug).

Записи журналів подій зазвичай починаються з «таймстемпу» дати й часу події. Деякі записи можуть містити інформацію про процес та PID, що дає змогу відстежувати, який застосунок або системна служба генерувала подію.

Наприклад, розберемо такі рядки з журналів:

- 07-08 21:15:42.789 1234-1234/com.android.packageinstaller I/PackageInstaller: App installed: com.example.maliciousapp. Цей запис повідомляє про встановлення застосунку з ідентифікатором com.example.maliciousapp. Запис має тип I (інформаційний). Аналізування таких записів допомагає виявити, коли і який застосунок було встановлено, що може бути корисним зокрема при аналізуванні шкідливого програмного забезпечення;
- 07-08 17:00:12.321 8901-8901/com.android.browser D/BrowserActivity: Visiting URL: https://www.example.com. Даний запис фіксує інформацію про відвідування веб-сайту https://www.example.com через браузер. Запис має тип D (повідомлення про налагодження);
- 07-08 16:30:00.789 5678-5678/com.android.cameraI/CameraService:Picture taken, resolution: 4032x3024, storage location: /storage/emulated/0/DCIM/Camera/IMG_20210708_163000.jpg. Такий запис фіксує активність камери та повідомляє про створену фотографію, указує її ім'я, формат, роздільну здатність та шлях, де був збережений кінцевий файл. Запис має тип I (інформаційний);
- 07-08 16:45:30.654 3456-3456/com.android.bluetooth W/BluetoothAdapter: Bluetooth is disabled, attempting to enable. Запис попереджає, що Bluetooth був вимкнений, але система намагається його увімкнути. Запис має тип W (попередження);
- 07-08 14:32:45.789 2345-2345/com.example.app E/AndroidRuntime: FATAL EXCEPTION: main
  Process: com.example.app, PID: 2345
  java.lang.NullPointerException: Attempt to invoke virtual method 'int java.lang.String.length()' on a null object reference
  at com.example.app.MainActivity.onCreate(MainActivity.java:45)
  at android.app.Activity.performCreate(Activity.java:7325)
  at android.app.Instrumentation.callActivityOnCreate(Instrumentation.java:1234). Цей запис свідчить про помилку в застосунку com.example.app. Має тип E (помилка);
- 07-08 18:15:42.321 4567-4567/com.example.app D/NetworkManager: Sending request to URL: https://api.

example.com/data. Запис указує, що додаток com.example.app намагається відправити запит до URL https://api.example.com/data. Запис має тип D (повідомлення про налагодження). За допомогою таких записів можна проаналізувати взаємодію між додатками, та іншу активність, що також може бути важливим під час аналізування шкідливого програмного забезпечення.

Зазвичай для дослідження журналів подій операційних систем Android необхідний повний доступ до пристрою (PIN код, пароль, біометричні дані), повна копія файлової системи з ключами шифрування або повна копія фізичного носія досліджуваного пристрою з ключами шифрування.

Дослідження журналів подій Android у деяких випадках може бути важливим для цифрової криміналістики, оскільки вони можуть містити ключову інформацію про дії користувача, застосунків та роботу системи.

Перелік джерел посилання

1. Google Developers Documentation, офіційна документація щодо інструменту logcat для збору та аналізу системних журналів Android. URL: https://developer.android.com/tools/logcat (дата звернення: 03.09.2024).
2. XDA developers, налаштування та використання ADB для доступу до журналів Android. URL: https://www.xda-developers.com/beginners-guide-to-the-android-debug-bridge/ (дата звернення: 05.09.2024).
3. Satish Bommisetty, Rohit Tamma, Heather Mahalik. Practical Mobile Forensics. Packt Publishing Ltd, 2014. 328 p.