УДК 004.05

Гурський М. В.
Войтович О.П.

Дослідження інцидентів в ОСAndroid

Вінницький національний технічний університет

Анотація: *стрімкий розвиток мобільних технологій ставить під загрозу інформаційну безпеку користувачів. Велика кількість бажаючих заволодіти конфіденційною інформацією відкриває нові проблеми захисту. Дослідження комп'ютерних інцидентів є потужнім засобом для усунення проблем такого роду.*
***Ключові слова*:** ОС Андроїд, мобільний пристрій, комп'ютерний інцидент, експерт, зловмисник, AndroidDebugBridge.

Abstract:*The rapid development of mobile technology threatens the security of user information. A large number of people willing to seize sensitive information open new protection problems. Forensic is a powerful tool to avoid such problems.*
Keywords: Android OS, mobile device, forensics, expert, attacker, AndroidDebugBridge.

Людина стає все більш залежною від мобільних пристроїв. З різкими змінами технологій та зростанням обчислювальної потужності велика частина щоденних справ перейшла до мобільних пристроїв. Кожен використовує їх за своїм власним сценарієм. Задачі, які вони виконують різні: від звичайного нагадування про події до складних банківських операцій на великі суми грошей [1]. Але завжди там де є важлива інформація є той, хто хоче нею заволодіти.

Розслідування комп'ютерних інцидентів (Forensics) дозволяє виявити приховані функції додатків або сервісів на факт витоку конфіденційної інформації або несанкціонованої зміни вмісту. За допомогою спеціальних засобів та методів можна дізнатися яким способом відбувався або може відбутися витік та які саме дані були втрачені. Сама ж експертиза відбувається за алгоритмом зображеному на рис. 1. Перш за все потрібно ідентифікувати загрозу та виявити канали, по яким відбувається витік. Потім потрібно ізолювати шкідливий додаток від та відібрати усі його права до компонентів пристрою. Далі, за можливістю, за допомогою логів, які зберігаються в системі, визначити, обсяг втрачених даних або нанесеної шкоди та зафіксувати їх на випадок надання доказів. Після чого отримані дані зберегти, а додаток видалити із системи [2].

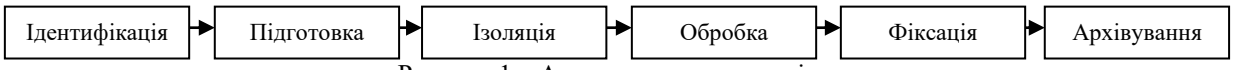

Рисунок 1 – Алгоритм методу аналізу загрози

Далеко не завжди виробники мобільних пристроїв зацікавлені у наданні достатніх засобів для проведення дослідження комп'ютерних інцидентів через питання приватності даних користувачів. Зокрема останнім часом широкий резонанс викликала подія, щодо доступу до персональних даних мобільного пристрою iPhone заарештованого терориста [3]. На думку Федерального Бюро Розслідування, компанія виробник має надати усю їм необхідну інформацію з пристрою злочинця, але політика Apple не передбачає розголошення приватних даних своїх клієнтів, навіть якщо це необхідно при співпраці з уповноваженими структурами. На відміну від Apple, компанія Google має вбудований автоматизований механізм, який дозволяє в будь-який момент часу отримати необмежений доступ до будь-якого вмісту файлів та даних будь-якого пристрою Android із встановленими сервісами Google [4].

Заходи, що вживаються компанією Google щодо забезпечення безпеки мобільної платформи Android приносять свої плоди: з кожною новою версією ця ОС отримує чергові поліпшення і стає більш захищеною. Однак незважаючи на це однією з головних загроз для користувачів Android-пристроїв, як і раніше залишаються шкідливі програми, кількість і різноманітність яких неухильно зростає. Серед інструментів протидії їм корпорацією відзначається поява вбудованої в ОС антивірусної надбудови, що попереджає користувачів про потенційну небезпеку встановлюються або вже інстальованих програм, а також дистанційне видалення шкідливих додатків [5].

Ситуація на ринку програмних засобів аналізу складу мобільних пристроїв суттєво відрізняється від ситуації з ПК, оскільки більшість виробників смартфонів вважають за краще

використовувати власні операційні системи. З цієї причини великий і вибір інструментальних засобів роботи з мобільними пристроями. Незважаючи на різноманіття продуктів, всі вони отримують дані з пристрою за допомогою фізичного або логічного клонування. Фізичне клонування має на увазі побітове копіювання всієї фізичної пам'яті, в той час як логічне - працює тільки з віртуальною пам'яттю. Фізичне клонування дозволяє відновлювати видалені файли, але логічне простіше для розуміння і використання. Тому бажано, по можливості, використовувати обидва методи клонування даних. Розрізняють програмні засоби forensics, які зберігають цілісність оригінального джерела даних і отриманої з нього інформації, та позасудові рішення, які не гарантують відсутності зворотного потоку інформації. Збереження цілісності не тільки підкріплює довіру з боку експерта, але і дозволяє використовувати це джерело для повторного аналізу. Також всі інструментальні засоби ділять на рішення для аналізу сім-карт, безпосередньо вмісту мобільних пристроїв і інтегральних продуктів, що забезпечують вилучення даних з обох джерел. Зазвичай, щоб охопити широкий ряд мобільних пристроїв і сім-карт, експерту потрібно набір з декількох рішень.

Існують системи для повного технічного аналізу Android-пристрою, проблема лише у тому, що у відкритому доступі їх немає. Але так як Android – це різновид Linux системи, то одним з найпотужніших інструментів є AndroidDebugBridge. ADB – це інструмент, який встановлюється з Android-SDK та дозволяє керувати пристроєм за допомогою ПК. Працює на будь-яких Android-пристроях та має такі функції:

- перегляд логів;
- копіювання файлів з\на пристрій;
- встановлювати\видаляти додатки
- видаляти\очищати\перемонтовувати розділи system та data;
- перепрошивати розділ system;
- виконувати різні скрипти управління;
- використання системної відладки;
- керувати мережевими параметрами.

Для роботи на ПК потрібно встановити AndroidSDKPlatform. Після підключення Android-пристрою до ПК та увімкнення відладки управління виконується через командну строку Windows.

Зрозуміло, що абсолютного захисту не існує. Через свою популярність ОС Android завжди буде привертати більшу увагу зловмисників. Навіть найновіші оновлення не можуть гарантувати безпеки. В даний момент технічна експертиза розвинута не так сильно, як сама ОС. Звичайний користувач не в змозі використовувати методи аналізу типу ADB. Але в перспективі, коли ця ланка стане більш розвинутою, системи дослідження комп’ютерних інцидентів стануть доступнішими та отримають більш зручний інтерфейс, тоді використання мобільних пристроїв стане набагато безпечнішим [6].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Lessard J., Kessler G. AndroidForensics: SimplifyingCellPhoneExaminations. – 2010.

[2] GettingstartedwithAndroidForensics [Електронний ресурс]. – Режим доступу:URL: http://resources.infosecinstitute.com/getting-started-android-forensics/- Назва з екрану.

[3] War encryption [Електронний ресурс]. – Режим доступу:URL: http://www.theguardian.com/technology/2016/fbi-apple-pr-war-encryption-mobile-security- Назва з екрану.

[4] Examinationofmobiledevices: Tools[Електронний ресурс]. – Режим доступу:URL: http://www.securityinfowatch.ru/view.php?section=articles&item=576/- Назва з екрану.

[5] AndroidForensicsFocus [Електронний ресурс]. – Режим доступу:URL: https://articles.forensicfocus.com/2012/09/12/android-forensics/- Назва з екрану.

[6] AndroidDebugBridge [Електронний ресурс]. – Режим доступу:URL: http://4pda.ru/forum/index.php?showtopic=383300- Назва з екрану.

Гурський Максим Васильович, студент, Вінницький національний технічний університет, м. Вінниця, факультет інформаційних технологій та комп’ютерної інженерії, 1БС-12б, amazing.vn.ua@gmail.com

Войтович Олеся Петрівна, к.т.н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

HurskiyMaxym, student, Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, 1BS-12b, amazing.vn.ua@gmail.com

VoitovychOlesyaPetrivna, Ph.D. docent, docent of Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, chair of information security.