Система моніторингу та аудиту безпеки в ОС Android

Войтович О. П., Гурський М. В.
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
voytovych.op@gmail.com

Monitoring system and security audit in OS Android

O. Voytovych, M. Hurskyi
Department of information security
Vinnytsia National Technical University
Vinnytsia, Ukraine
voytovych.op@gmail.com

***Анотація* — на основі аналізу основних методів та шляхів поширення шкідливого програмного забезпечення в ОС Android, а також методів протидії від них, розроблено систему для моніторингу та аудиту безпеки в ОС Android.**

Ключові слова — Android; моніторинг; аудит; загрози та вразливості; шкідливе програмне забпезпечення.

***Abstract* – the main problems of Android OS protection are considered, namely breakthrough methods, types of malware and how to spread them. It is proved that existing methods cannot guarantee full security, since one of the main security problems with the Android OS is, first of all, the human factor. One of the ways out is the use of systems for monitoring. Based on the analysis of the main methods and ways of spreading malicious software on Android OS, as well as methods of counteracting them, developed a system for monitoring and auditing security in the Android operating system. The created software allows real-time monitoring of all Android OS systems and making decisions based on the received data in accordance with the security policy.**

Keywords – Android; monitoring; audit; threat and vulnerability; malware.

I. ВСТУП

Інформаційні технології розвиваються дуже стрімко. Кількість та об’єм інформації, яку потрібно захистити, збільшується кожного року. При викраденні інформації може постраждати не тільки особа, якої ця інформація стосується, а й компанія або ж навіть держава. На сьогоднішній день ринок мобільних пристроїв вже обігнав ринок персональних комп’ютерів. В той же час стрімке зростання обчислювальної потужності і можливостей мобільних пристроїв ставлять нові питання і проблеми в галузі забезпечення інформаційної безпеки. Поширення мобільних пристроїв тягне за собою зростання бажаючих заволодіти як фізично цими самими пристроями, так і інформацією, яка зберігається на них. Найбільше хакерів приваблює операційна система Android в силу своєї відкритості та широкої розповсюдженості [1]. Обсяги шкідливого коду ростуть з роками майже в геометричній прогресії. У зв'язку з високою популярністю пристроїв Android, в якому отримання root-прав робиться в пару дотиків, проблема встановлення додатків з недовірених джерел, і, як наслідок, збільшення ймовірності ненавмисного впровадження шкідливого коду на мобільний пристрій, актуальна як ніколи. Метою дослідження є покращення стану інформаційної безпеки мобільних пристроїв, шляхом аналізу головних загроз, способів їх проникнення в систему за рахунок створення системи моніторингу та аудиту безпеки. Система, у режимі реального часу, буде реагувати на усі зміни в роботі та надавати користувачу рекомендації щодо вирішення проблем.

II. АНАЛІЗ ОС ANDROID

Однією з найпопулярніших мобільний операційних систем є Android. Android (Андроїд) – операційна система для смартфонів, планшетних комп’ютерів, електронних книг, цифрових програвачів, наручних годинників, ігрових приставок, нетбуків, смартбуків, окулярів Google та інших пристроїв, яка написана на ядрі Linux і реалізації Java від Google. Спочатку розроблялася компанією Android Inc., яку потім купили Google.

Згодом Google ініціювали створення альянсу Open Handset Alliance (OHA), який зараз займається підтримкою і подальшим розвитком платформи. Android дозволяє створювати Java-додатки, що керують пристроєм через розроблені Google-бібліотеки. Android Native Development Kit дозволяє портувати (але не налагоджувати) бібліотеки і компоненти додатків, написані на мові C [1,2].

Основні переваги цієї системи: вільне та відкрите програмне забезпечення; широкий спектр виробників заліза, через що з'являються як бюджетні смартфони, так і дорогі флагмани, для кожної верстви населення; велика спільнота розробників, через відкритість системи; стрімкий розвиток; використання технологій віртуальної реальності; підтримка з боку провідних IT-компаній [1]. Однак така величезна кількість користувачів просто не могла залишитися без уваги з боку зловмисників. Побудувавши на розробці і поширенні шкідливих програм цілу індустрію зі своїми законами, вони стали вкрай небайдужі до будь-яких джерел легкої наживи. Разом із розвитком технологій створюються нові типи шкідливого програмного забезпечення. Більша частина ШПЗ створюється як для розповсюдження реклами, так і використовуючи вразливості у системі або неуважність користувача, для серйозних атак, наприклад на системи мобільного банкінгу або корпоративні системи [3].

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 програм, а також дистанційне видалення шкідливих додатків [4]. Важливим фактором, який ускладнює забезпечення належного рівня захищеності платформи Android, є її відкритість і надзвичайна фрагментованість. На ринку присутні сотні різних моделей мобільних пристроїв зі своїми програмними особливостями, якими їх наділили численні виробники. Але часто через різницю політики Google та компанії виробника пристрою страждають користувачі. Після оновлення системи до новішої часто відкриваються нові проблеми з роботою. Це відбувається тому, що Google зобов'язує усіх виробників дотримуватися їх політики та функціоналу, але кожна велика компанія використовує лише платформу від ОС, а поверх неї створює свою «оболонку» та впроваджує в неї власний функціонал. Саме через це виникають проблеми різного роду використання пристроями. Виправляють їх не досить швидко, а в деяких випадках й зовсім забувають [4].

III. МЕТОДИ ЗЛАМУ ТА ЗАХИСТУ

Через високу популярність системи, існує чимала кількість зловмисників, які хочуть викрасти дані або нашкодити користувачеві. Проаналізувавши загрози в операційній системі Android, визначено основні категорії загроз (рис. 1).

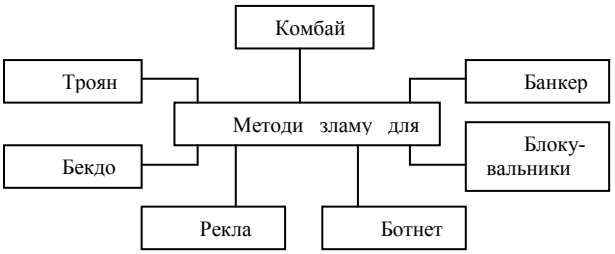


Рис. 1 – Класифікація методів зламу

Трояни – програми, які в основному викрадають дані і маскуються під легальні додатки. У Android це можуть бути СМС – трояни (віруси сімейства Android.SmsSend). Метою цих програм є відправлення текстового повідомлення на номери зловмисників [3].

Рекламні модулі – додатки із нав'язливою рекламою, які використовують розробники для монетизації додатків. Загалом вони не представляють загрози: користувач переходить на рекламне оголошення і розробник отримує гроші. Проте існують й інші рекламні модулі, які використовують зловмисники. Використовуючи методи соціальної інженерії вони рекламують своє шкідливе ПЗ.

Джерелом впровадження методу Backdoor.AndroidOS.Obad є – сайти для дорослих або підставні онлайн-магазини. Після завантаження додаток відправляє команди поповнення балансу мобільних телефонів і перехоплює відповіді, які надходять від банку, маскуючи свою діяльність під призначену для користувача. Не менш небезпечним є Android.Backdoor.114.origin – метод, за сценарієм якого, шкідливе ПЗ для Android-пристроїв, що встановлюються в якості системних додатків, непомітно для їх власників здійснює шкідливу діяльність [3,4].

У вересні попереднього року в Google Play з'явився троян Android.Sockbot.1. Цей програмний засіб має досить специфічний функціонал: перетворює заражений пристрій в зомбі. Точніше - в проксі-сервер, який дозволяє розповсюджувачам шкідливого коду анонімно з'єднуватися з іншими комп'ютерами. А ще - красти трафік і використовувати пристрій для DDoS-атак. Особисто користувачу це нічим не погрожує, а ось продуктивність, автономність смартфона і мобільний трафік всерйоз постраждають [5].

Основне завдання методу Trojan-Ransom.block полягає в шифруванні вмісту внутрішньої або карти

пам'яті смартфона і подальшому витягуванню грошей за повернення доступу до даних. Відразу після початку шифрування троян виводить на екран повідомлення про блокування доступу до пристрою за перегляд забороненого контенту. У повідомленні зловмисники вимагають оплатити «штраф», погрожуючи в іншому випадку оприлюднити дані користувача в публічних джерелах. Він блокує доступ до усіх файлів [6].

Підхід творців мобільних шпигунів до крадіжки грошей стає більш комплексним: справа вже не обмежується спеціальними банківськими троянцями, що мають на меті банківські додатки. Приклад такого методу - Trojan-SMS.AndroidOS.FakeInst.ep. Додаток, який використовує даний метод, показує користувачеві повідомлення, нібито від Google, з вимогою відкрити Google Wallet і ввести дані банківської картки (під приводом боротьби з кіберзлочинністю). Вікно з цим повідомленням не можна закрити, поки користувач не введе дані банківської картки.

Нещодавно був опублікований новий метод, який реалізує вразливість Stagefright, яка властива усім Android-пристроям від версії 2.4 до 5.1.1. Даний експлойт демонструє атаку за допомогою шкідливого MMS-повідомлення - для його здійснення зловмисникові потрібно знати лише номер телефону жертви. При цьому, користувачеві не потрібно навіть здійснювати ніяких дій з повідомленням (відкривати файл, кликати по посиланнях і т.п.), шкідливий код виповнюється автоматично. Також зловмисники можуть самі віддалено видалити повідомлення до того як користувач його побачить. В такому випадку смартфон може лише показати сповіщення про вхідне повідомлення. Незважаючи на наявність в Android спеціальної пісочниці безпеки, яка блокує для більшості додатків можливість доступу до призначених для користувача даних інших програм, можливо створення експлойтів, які отримують доступ до аудіо і відео-потокам смартфона, а також до внутрішнього сховища [3, 7].

Але, як вже відомо, штатних механізмів захисту, у ситуації, що склалася, вже не досить (рис. 2). Через політику безпеки, антивіруси не можуть захистити пристрій від самого користувача або від прихованих функцій в додатках, якщо в них не міститься раніше відома сигнатура вірусу. Для таких цілей можна використовувати програми для моніторингу системи.

Моніторинг - система збирання/реєстрації, зберігання та аналізу невеликої кількості ключових (явних або опосередкованих) ознак/параметрів опису даного об'єкта для винесення судження про поведінку/стан даного об'єкта в цілому. Тож для винесення судження про об'єкт у цілому на підставі аналізу характеристик його ознак [7].

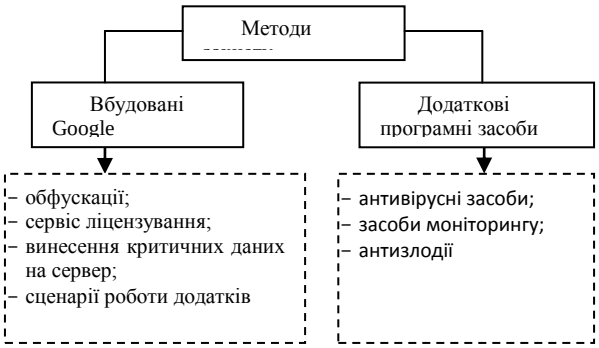


Рис. 2 – Методи захисту в ОС Android

Засоби для моніторингу призначені для того, щоб в режимі реального часу можна було бачити, що відбувається з системою та її складовими. Наприклад, моніторинг використання пам’яті, енергій акумулятора, активності, тощо. Часто моніторинг використовують при поломці або, у випадку, некоректної роботи пристрою. Моніторинг може бути активним і пасивним, під час якого здійснюється цілодобове спостереження та логування усіх дій системи, від зміни файлу до перепадів температури акумулятора, для подальшого аудиту. Активний моніторинг передбачає імітацію реального втручання або атаки на систему. Інформацію про кращі з них наведено у таблиці 1 [7].

ТАБЛИЦЯ 1 – ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ЗАСОБІВ МОНІТОРИНГУ

Назва додатку	**Переваги**	**Недоліки**
OS Monitor	моніторинг системи, список процесів, підключення до мережі, тощо	не підтримується усіма пристроями, рідко оновлюється
SD Maid	менеджер додатків; очищення від сміття	потрібні root-права
GSam Battery Monitor	статистика по стану батареї	потрібні root-права; висока ціна

У всіх них є один недолік – вони лише відображають «суху» інформацію. Для рядового користувача така робота є нерезультативною, оскільки це лише дані.

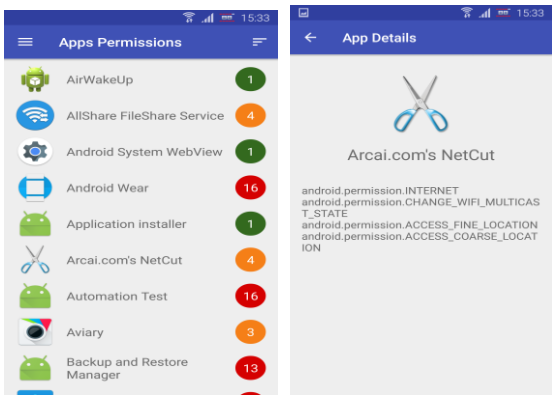
IV. РОЗРОБКА СИСТЕМИ

В ОС Android існує велика кількість даних, якою внутрішні системи обмінюються щосекундну. Сама компанія Google, згідно із ліцензійною згодою, збирає статистику «використання та діагностування». Здебільшого передаються відомості про роботу пристрою та виникаючі неполадки. Також, це може бути інформація про використання різних додатків та мережеві підключення (WiFi, Bluetooth). Вся інформація є анонімною. Але, якщо правильно прочитати цю інформацію, проаналізувати та прив’язати до подій, то можна створити досить надійну систему безпеки,

яка буде вчасно реагувати та запобігати несанкціонованим діям.

Саме тому було прийнято рішення об'єднати увесь такий функціонал в один додаток, додати систему аудиту та прийняття рішення. Будь-який користувач зможе в декілька кліків отримати структуровану інформацію про те, як і чим живе гаджет: чи можна встановлювати цей додаток, куди йдуть усі ресурси пристрою, чому так швидко сідає батарея, тощо.

Наприклад, у системі моніторингу є функція перевірки усіх додатків на наявність у них прав доступу. Більшість із прав є цілком безпечними, але частина із них можуть нанести непоправної шкоди, як видалення вмісту пам'яті чи списання коштів. Саме тому функція аудиту перевіряє кожен додаток і виділяє небезпечні (рис. 3).



а) б)

Рис. 3 - Вигляд вікна з функціонуванням додатку (а – менеджер додатків; б – вікно із правами додатку)

Після перевірки прав, система також перевіряє навантаження на ядра, CPU, GPU, RAM і, якщо якийсь додаток сильно навантажує систему, то користувачу пропонуються шляхи вирішення проблеми.

За схожим принципом відбувається перевірка на через мірне використання трафіку, внутрішньої пам'яті, активні процеси, оптимізації енергопостачання систем та додатків, менеджеру додатків.

Структурно система розбита на два модулі: модуль моніторингу та модуль аудиту. В свою чергу модуль моніторингу розбитий на класи, кожен з яких займається перевіркою та моніторингом за власним сценарієм та параметрами. Система аудиту слідкую за кожним класом та, в залежності від ситуації, надає користувачу усю необхідну інформацію та рекомендації для подальшого розвитку подій. Також модуль аудиту пов'язує усю інформацію від кожного класу моніторингу та перевіряє роботу усієї системи на випадок нештатних ситуацій (швидка втрата заряду, витік пам'яті, перегрівання, тощо).

Таким чином, разом із користувачем, додаток може забезпечити досить надійний захист від несанкціонованого доступу до персональних даних.

V. ВИСНОВКИ

Отже, було доведено актуальність даної розробки. Також, було розглянуто основні проблеми захисту ОС Android, а саме методи зламу, типи шкідливого програмного забезпечення та способи їх поширення. Відповідно до них було виділено основні методи протидії від несанкціонованих дії зловмисників. Доведено, що існуючі методи не можуть гарантувати повної захищеності, оскільки однією з головних проблем безпеки при роботі з ОС Android, перш за все, є людський фактор.

Одним із виходів проблеми є використання систем для моніторингу. За допомогою аудиту, користувач може спостерігати усі дії системи, отримувати від системи рекомендації для вирішення проблеми та мінімізувати ризики. Реалізований програмний засіб дозволяє у режимі реального часу слідкувати за усіма системами ОС Android та приймати рішення на основі отриманих даних відповідно до політики безпеки.

Література References

[1] D. Sovetskyi, Y. Baryshev. Protection tool against malware for Android operating systems // Inżynier XXI wieku projectujemy przyszlosc, monografia [pod red: Jacek Rysiński] - Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. - pp. 367- 372. -

[2] IT threat evolution Q1 2017. Statistics [Електронний ресурс]. – Режим доступу: URL: https://securelist.com/analysis/quarterly-malware-reports/78475/it-threat-evolution-q1-2017-statistics/- Назва з екрану.

[3] Войтович О. П., Гурський М. В., Куперштейн Л. М., Сніговий Д. С. Засіб моніторингу для операційної системи Android // Вісник ХНУ : серія Технічні науки. - №3 (249). -2017. - С. 236-241

[4] Войтович О. П. Дослідження інцидентів безпеки в ОС Android. / О. П. Войтович, М. В. Гурський // Тези доповідей XLVI Науково-технічної конференції Вінницького національного технічного університету. ФІТКІ – Вінниця, 2017 р.

[5] Куперштейн, Л. М., Прокопчук, С. О., Буда, А. Г. Захист файлів в операційній системі Android // Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації» м. Вінниця, 19-21 квітня 2016 року. - Вінниця: ВНТУ, 2016. - С. 74-76.

[6] Tips for keeping your Android device safe / [Електронний ресурс] – Режим доступу: URL https://support.google.com/android/answer/6215472?hl=en/ / - Назва з екрану

[7] Fewer security vulnerabilities found in 2015 [Електронний ресурс]. – Режим доступу: URL: https://ictinstitute.nl/security-vulnerabilities-2015/ - Назва з екрану.

[8] Enck W., Ongtang M., McDaniel P. Understanding android security //IEEE security & privacy. – 2013. – №. 1. – С. 50-57.