УДК 681.12

М. В. Гурський
О. П. Войтович

ЗАСІБ МОНІТОРИНГУ ДЛЯ ОС ANDROID

Вінницький національний технічний університет;

Анотація

На основі аналізу основних методів та шляхів поширення шкідливого програмного забезпечення в ОС Android, розроблено програмний засіб для моніторингу вхідного/вихідного трафіку усіх системних та встановлених програмних застосунків.

Ключові слова: операційна система, Android, гаджет, безпека, системи моніторингу, додаток, шкідливе програмне забезпечення, конфіденційність.

Abstract

Software for monitoring of all system and installed application's output and input network traffic is developed based on analysis of main methods and ways of malware spreading in Android

Keywords: operating system, Android, gadget, security, monitoring system, application, malware, privacy.

Вступ

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.

Метою роботи є покращення стану інформаційної безпеки мобільних пристроїв, шляхом аналізу головних загроз, способів їх проникнення в систему за рахунок моніторингу та аудиту програмних додатків, встановлених на мобільних пристроях.

Результати дослідження

Шляхи потрапляння ШПЗ можуть бути різними (рис. 1): від звичайного SMS-повідомлення до заздалегідь розробленої та точної атаки на конкретну людину. Щороку з'являються нові технології, які впроваджуються розробниками пристроїв та активно використовуються користувачами в подальшому. Кожна така технологія не може одразу тестуватися в усіх ймовірних сценаріях роботи, тому, зазвичай, саме в них міститься найбільша кількість вразливостей [1]. Часто, отримуючи ту чи іншу інформацію за допомогою різних сервісів миттєвих повідомлень, можна також отримати ШПЗ на власний пристрій. Велику небезпеку становлять публічні або недовірені мережі, оскільки будь-хто може перехоплювати або змінювати інформацію під час сеансу [2].

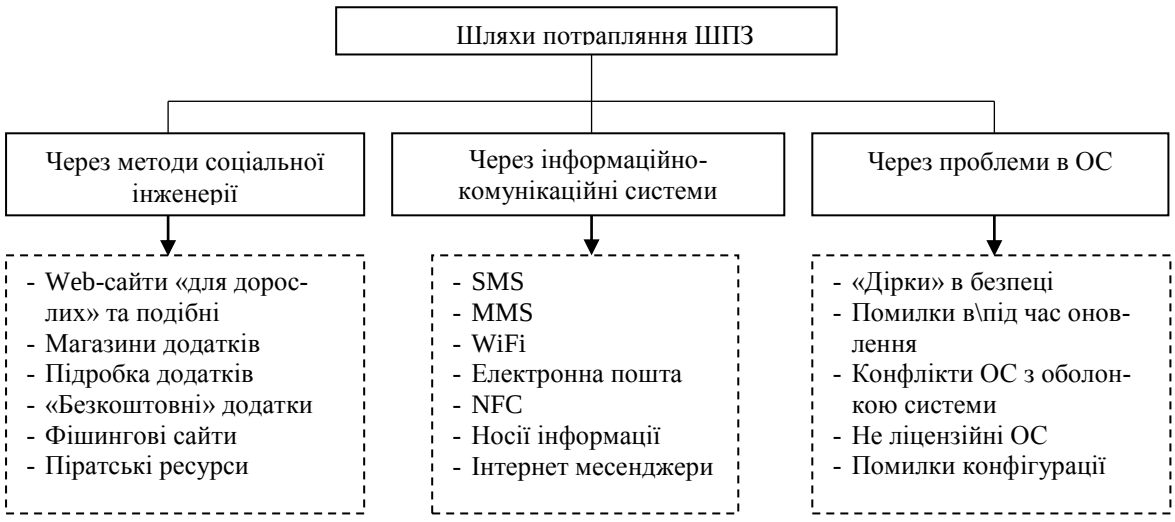

Рисунок 1 – Шляхи потрапляння ШПЗ на Android-пристрій

Однією з головних проблем безпеки при роботі з ОС Android, завжди залишався людський фактор. Якою б захищеною не була операційна система, безтурботність, неуважність, самовпевненість і проста необізнаність рано чи пізно може зіграти поганий жарт з користувачем. Само по собі ШПЗ не може потрапити на пристрій жертви з сучасною ОС, тому в своєму арсеналі зловмисники завжди мають методи соціальної інженерії [3].

Після потрапляння будь-якого ШПЗ на Android-пристрій, жертва ще довго може нічого не знати про це. Більшість таких додатків маскуються та чекають нагоди для виконання своїх задач. Так, деякі з них, можуть при підключенні до мережі Інтернет одразу надіслати вкрадену конфіденційну інформацію, а інші чекають, наприклад, поки користувач не використає свої банківські реквізити [4].

Одним із виходів проблеми є використання програм-моніторів. З їх допомогою користувач може самостійно аналізувати усі дії системи та мінімізувати ризики. Розроблений засіб для моніторингу дозволяє отримувати інформацію про вхідний\вихідний трафік кожного системного або встановленого додатку з правами на використання мережі Інтернет. Будь-якому ШПЗ потрібно мати вихід до мережі для завантаження додатків файлів, отримання інструкцій від розробника, передавання конфіденційної інформації, тощо.

Для того, щоб програмний засіб для моніторингу правильно функціонував, перш за все потрібно отримати від операційної системи повний список усіх встановлених та системних програмних пакетів. Далі потрібно проаналізувати отриманий список додатків на наявність у них прав для доступу до мережі Інтернет. Отримавши інформацію, формується новий список, в якому відсіюються додатки без доступу до мережі Інтернет, і потім виводиться у сортованому вигляді на інтерфейс користувача та додається інформація про вхідні/вихідні дані кожного додатку.

Висновки

Доведено, що запропоновані методи не можуть гарантувати повної захищеності, оскільки однією з головних проблем безпеки при роботі з ОС Android, перш за все, є людський фактор. Якою б захищеної не була операційна система, безтурботність, неуважність, самовпевненість і проста необізнаність рано чи пізно піддає небезпеці власника розумного пристрою.

Реалізований програмний засіб дозволяє у режимі реального часу слідкувати за доступом усіх встановлених та системних додатків до мережі Інтернет.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Мельников Д. А. Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА. – 2013.

2) Effectivness of malware protection on android and evaluation of android antivitus apps / R. Fedler, J. Schutte, M. Kulicke // Applied and integrated security. – 2014. – P. 7–13, 26–32.

3) Zhou Y., Jiang X. Dissecting android malware: Characterization and evolution //Security and Privacy (SP), 2015 IEEE Symposium on. – IEEE, 2015. – С. 95-109.

4) Войтович О. П. Дослідження інцидентів безпеки в ОС Android. / О. П. Войтович, М. В. Гурський // Тези доповідей XLV Науково-технічної конференції Вінницького національного технічного університету. ФІТКІ – Вінниця, 2016 р.

Гурський Максим Васильович — студент групи БС-16м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: amazing.vn.ua@gmail.com

Войтович Олеся Петрівна — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Hurskyi Maksym V. — Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : amazing.vn.ua@gmail.com

Voitovych Olesya P. — Cand. Sc. (Eng), Assistant Professor of Information Security, Vinnytsia National Technical University, Vinnytsia