# A Forensic Analysis of Joker-Enabled Android Malware Apps

Chen Shi, Chris Cheng, and Yong Guan

**Content**

This project aims at developing a set of automated Android Malware vetting tools to discover all the malicious behaviors of Android Malwares in the forms of files in the local storage, SQLite database, or data sent to remote 3-party server(s). to establish a dictionary-like Android malware database that includes malware themselves (malicious code and variant) with all the detected IP addresses, URLs and malicious behaviors as well as other types of evidence data(e.g., the list of permissions required).

This presentation will introduce the basics, challenges, and limitations of the current Android malwares detection, and provide a detailed explanation about the usefulness and availability of information about list of permissions required and potential private information leakage by malicious apps (e.g. http://wap.thaiza.com/ → browser cookie and timestamp. In addition, the presentation will elaborate our methodology and large-scale experimental evaluation of the approaches we use to build android malware analysis databases. Overall, application developers and researchers will learn how to take advantage of the database and search the analysis result for certain android packages to prevent app code being infected by malware.

In addition, this presentation will demonstrate a well-known malware named Joker (also known as Bread), which has infected over 17,000 Android apps since its first release and has evolved into numerous different variants. Both static and dynamic program analysis approaches (Evihunter) were applied on analyzing the malicious code, detecting malicious behaviors and retrieving evidentiary data like the file path and its corresponding evidence types.Through the analysis of code, we discovered that Joker not only leverage all kinds of cloaking and obfuscation techniques in attempt to be undetected, but also use dynamic package loading to hide its malicious payload. In order to automate the fraud subscribe process, Joker developers utilize injected clicks, custom HTML parsers and SMS receivers so that it will not require any interaction from the user. When the infected app gets installed, it carries out either SMS fraud which sends text messages to premium-rate numbers or WAP billing fraud where a user's mobile account will be paying for the charges of the subscriber's bill. According to Google's recent report, having three or more active variants of Joker on their official app market at the same time is very common and at peak times of activity, there are up to 23 different versions of Joker family submitting to the Google Play Store in one day.

As many different variants are active on the air, we collected 12 samples from 46 infected apps which have been removed from Google Play Store. In some versions of the Joker variants, the final payload is delivered through a direct URL obtained from the listed command and control (C&C) server. In these variants, the C&C address has been hidden in the code utilizing the string obfuscation where the string "sticker" was used to break the C&C address and hide it from the simple grep or string search in order to pass the vetting process. In some versions, the infected Google Play app uses a stager payload to retrieve the final payload where the stager payload URL was encoded in the code and was encrypted using Advanced Encryption Standard (AES). Upon an infected app gets started, it downloads the stager payload first then utilizes the stager payload to execute the malicious final payload. In addition, we have discovered that some variants of Joker even leverage two-stager payload downloads in order to retrieve the final payload. As for these infected apps, it downloads the stage one payload, which downloads the stage two payload, which finally loads the malicious Joker payload.

**Keywords:** Mobile Forensics, Android Malware, Digital Evidence