

Exploring Memory Forensics of Android Banking Trojan(Work in progress)

Szu Kai Yang

Department of Computer Information Technology, Purdue University

Problem

A new kind of Trojan recently emerged in the Android ecosystem over the past few years. This kind of Trojan will steal financial information from user and send it over to hacker's server. There are many forms of banking Trojan, some of them looks very like the real app and the others stole when user purchase.

The goal of this project was to explore memory differences of Android devices before and after infected by banking Trojan.

Method

- Acquire uninfected memory image
- Install Banking Trojan on Android device
- Trigger Banking Trojan
- Acquire infected memory image
- Analyze infected memory image

To verify the difference, a comparative analysis will be done between uninfected and infected image.

Hypothesis

Banking Trojan will create additional network process to send user data

What is Banking Trojan?

It is an Android Trojan malware that attempts to steal user's banking /financial information. Once successfully obtained the information, the malicious hacker can freely access to the banking account.

