An In-Depth Analysis of the Banking Trojan Copybara and Strategies for Mitigation

Degree programme : BSc in Computer Science
Thesis advisor : Prof. Dr. Benjamin Fehrensen
Expert : Andreas Fischer

In an era when financial services increasingly transition to the digital realm, trojans like Copybara target banking apps for monetary gain. By in-depth analyzing both the malware and the modus operandi, we were able to study and understand the attacker. Based on the gathered intel, a complete monitoring of the attack events against real customers was set up and reported to the authorities.

Introduction

Malicious software, or malware, continues to pose significant threats to computer systems. As users shift from personal computers to mobile devices, malware is increasingly targeting mobile phones. This project aimed to analyze and reveal the functionality of Copybara, an Android-specific banking trojan, addressing the rising threat of mobile malware.

Methods

To understand Copybara's functionality and methods of privilege escalation, comprehensive static and dynamic analyses on multiple samples of Copybara were conducted. Indicators of Compromise (IoCs) identified during these analyses were used to collect additional samples of the same malware family and uncover more command and control (C2) servers. Due to insecure server configurations, it was possible to record the entire C2 attack communications. By injecting a script into the C2 admin panel, the attackers were tracked, and a detailed persona was created.

Goals

The primary goal was to uncover significant vulnerabilities that pose risks to users, involving the following steps:

- Identify persistency mechanisms and functionalities of the malware.
- Analyze the communication, configuration and distribution of the malware.
- Build an emulator which allows communicating to the CC server.
- Identify potential countermeasures and propose mitigations.

Results

The investigation revealed that real life attacks predominantly targeted Android systems in Italy. By intercepting and analyzing C2 channel communications, ongoing attacks were identified and documented. These findings were promptly reported to the Italian authorities, helping to prevent fraudulent transactions from being executed. The attempted thefts ranged from € 1'000 to € 50'000, averaging over € 15'000 in potential losses per day. As a result of the collected metadata, the attacker could be tracked across multiple campaigns and reported to CERTFin. Multiple C2 instances were observed, with the malware exhibiting significant similarities in code structure and function calls, but minor changes indicating ongoing development.

Jens Hubler
IT Security

Robin Michael Renker
IT Security