Android Malware Analysis: Coper/Octo

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

The increasing use of mobile devices for sensitive tasks, such as e-banking, has made them a primary target for cybercriminals. This thesis provides an in-depth examination of the Coper/Octo e-banking trojan, addressing its capabilities to steal credentials and facilitate remote access. By analyzing its infection vectors, persistence mechanisms, and communication strategies, this research sheds light on the evolving threats facing Android devices.

Thierry Pfeiffer

Introduction

Android's vast user base and the flexibility to install apps from untrusted sources have made it an attractive target for malware developers. Coper/Octo is an e-banking trojan that is sold as Malware-as-a-Service to cybercriminals. It employs remote access capabilities, keylogging, and overlays attacks to steal login credentials and commit financial fraud, posing a significant risk to individuals and organizations.
It is crucial to understand the operational mechanisms of threats such as Coper/Octo to enhance detection and defense techniques and systems against modern Android threats.

Methods

This research combines static and dynamic analysis techniques, along with an emulator replicating an infected device, to examine Coper/Octo's functional mechanisms.
In the static analysis a sample is examined without executing it. This involves the studying of the app's code and included files to reveil the usage of obfuscation techniques and used permissions.
In the dynamic analysis the malware is executed in a controlled environment to interact with the device and to observe its runtime behavior like network communication.

Goals

This work had the following main goals:

- Determine the core functionalities of the malware
- Examine how the malware achieves persistence
- Investigate how the an infected device communicates to the command and control servers
- Development of a tool to simulate the communcation with C&C servers
- Analyze the configurations to determine the targeted apps

Results

The investigation identified two active major versions of the malware, designated „Octo" and „Octo2," which were utilized in campaigns targeting users in Turkey and Switzerland.A comparison of the two versions revealed ongoing refinements to already sophisticated anti-detection and anti-analysis techniques.
A domain generation algorithm (DGA) within Octo2 was successfully reverse-engineered to predict future command and control (C&C) domain names associated with infected samples. The study also examined the evolution of obfuscation and protection techniques for the malicious payload, highlighting notable enhancements in this area. Furthermore, the investigation explored the enhanced remote access capabilities of Octo2, providing comprehensive documentation and analysis. The study also documented a noteworthy campaign that targeted Swiss citizens, employing an unconventional delivery mechanism—physical mail—to distribute the malware.