Mobile Security Threat and Countermeasure

Zuleika G. Lopez (*Author*)
Computer Engineering and Science Department
Polytechnic University of Puerto Rico
San Juan, Puerto Rico
zuleikaglopez@gmail.com

Abstract — It is more common to have mobile devices such as smartphones or tablets as part of your daily routine. Despite the high-risk of losing important data, more companies are agreeing to let their employees bring their personal devices to the work area. Some companies provide to their employees smartphones, tablets, and other devices to be used as company tools. Therefore, more employees are using their mobile devices for their personal usage as well as for business purposes. These devices are used in a variety of ways, such as e-mail service where sensitive company information may be exchanged, or even access the companies own host or server in order to approve transactions. Managing this information in such a way is a security risk that companies undergo, sometimes without even knowing about them. Hackers take advantage of such opportunities to gain sensitive information; this is why they need more people to use their mobile devices for work related activities. The hackers have been redirecting their sight from the traditional Data Centers to mobile devices. This poster discusses different malwares and how the hackers could reach your "hand" and which is the most likely information that they look for. It will present statistical data regarding the most commonly infected mobile devices at a global scale. The focus of the research is examining several applications that hackers use to invade the user's privacy and explain how each tool works. The objective is to make awareness of these threats to the business community and to the average user. Hackers are closer than people think.

Keywords — Hackers; Mobile Threat; MITM Proxy; Malware; BYOD; Sniffing

I. INTRODUCTION

This poster will present the latest mobile threats and demonstrate the kind of data that Hackers are interested in. The purpose is awareness for the general population and business employees about the possibility of intrusion.

The objective of the poster is to build awareness of threats to the general user and to the business community.

- Present how mobile device technology is impacting the enterprises.
- Discuss the information that Hackers are looking for.
- How the Hackers can obtain personal and business data and demonstrate the MITM proxy tool that Hackers use for attack.
- Suggest and recommend some tips to prevent or minimize Hacker attacks.

The poster is distributed in several parts: The first part is analyzing the statistics from past to the future years, and the mobile device data usage such as Tablets and Smartphones that are increasing considerably. In addition to remark the increasing percentage of the acceptance of such devices and contrast present mobile device malware, and the countries with the highest infected market in the world. Another goal for this paper is to observe the real reason for attacks (mostly based on money). The most important topic is to gain knowledge about the latest mobile virus and tools that Hackers use for attacks. Therefore, a test was performed using the Man-in-the-Middle (MITM) proxy software to demonstrate the decrypted information that Hackers will obtain. It shows to the users how explicit their data/communication was. The final section suggests different activities to prevent or minimize Hacker attacks