Chapter 6
Mobile Malware

Geogen G.
SRM University, India

Poovammal E.
SRM University, India

ABSTRACT

Why should everyone know about mobile malware? With the introduction of Internet of Things (IoT) and Cloud, you can't survive in a disconnected world. Thus from your home appliances to your window curtains, everything is connected to Internet which can be accessed through your hand held mobile device. Unlike Personal Computers, these devices give Hackers a greater attack landscape. Back in 2004, when the first mobile malware was introduced, we never thought that it would get such a big threat space, as we see today. So, we discuss the History of Mobile malwares and its categories with its motives. We also discuss few signs that indicate the presence of a mobile malware. To conclude we categorize the battle against malware into two namely prevention and response, which is forensically analysed using Static/Dynamic Methods/Tools.

INTRODUCTION

Smartphone usage is expected to reach 2082.7 million globally this year *(Number of smartphone users worldwide from 2014 to 2019 (in millions), Marlene Greenfield, Vice President, Hearst Magazines)* and mobile applications are going to become more and more important than ever. Companies are looking forward to create newer innovative apps to connect with suppliers, distributors and end users. Even though mobiles revolutionized the way in which data is exchanged, and delivery of services, it also created new security challenges. Compared to PC users, mobiles are always switched on and connected but large group of mobile users are tech illiterate which makes it difficult to update mobiles with security patches, once it is sold. Major share of worries related to mobile application security arise due to:

- No or Irregular vulnerability checking of mobile apps.
- Poor encryption and data leakage.
- Insecure data Storage, etc.

DOI: 10.4018/978-1-5225-9866-4.ch006

Malware in general covers all sorts of malicious software or codes written to harm you or your system. Let us introduce the terms one by one which are categorized as Malware:

- **Virus and Worms:** Virus is a malicious program/file which attaches itself to a genuine program mostly to an executable file and spreads from one system to another, leaving infections as it travels (Siciliano,2015). Virus uses stealthy techniques to remain hidden and unnoticed and the main purpose of virus is to reach protected networks. The major difference between virus and worm is the trigger by human or event. Virus needs a human/event trigger (like executing a file, clicking the icon etc) for propagating from system to system. Unlike Virus, Worm can replicate itself and spread from one system to all connected systems eating away system memory and network resources causing, web servers, network servers etc to stop responding.
- **Trojans and Backdoors:** Trojans are non-self-replicating malicious programs which can delete, block, modify, copy data without users authorization once allowed. But Trojans will be present as some useful email alert or new security path. When user allows the attachment or path, Trojans gain access to your system, in turn allowing hackers to gain remote access to your system. This remote hidden secondary access which bypasses all security measures is commonly referred as Backdoor.
- **Rootkits:** It is a combination of two words, Root and Kit. Root is UNIX/Linux term which is equivalent to Administrator in windows. Kit represents a group of programs which allow someone to obtain the root/admin privilege, without end users' knowledge. Rootkits are mainly deployed for two reasons: remote command/Control and Software Eavesdropping. They are non-self-propagating threats with three snippet codes in it. They are a dropper, a loader and a Rootkit. A dropper is a good looking link or attachment which prompt user to click on it. Once clicked, dropper launches the Loader Program and deletes itself. Loader program uses some exploits like buffer overflow and loads the Rootkit into memory. According to their function, Root kits are divided into User Mode Root kits, Kernel Mode Root kits, Hybrid Root kits, Firmware Root kits, Virtual Root kits, Generic Root kits etc(cooper,2016)
- **Logic Bombs:** They are programs designed to trigger when certain conditions are met like a particular time or log-off or after specific number of data base entries etc. Software Time Bomb is considered as a logic bomb because when the target time or date is reached, it executes. Until the time reaches, logic bomb will be in sleeping/dormant modes which make them hidden from antivirus.(Kelly,2015)
- **Key Loggers:** A highly specialized software or hardware tool designed to intercept and record every keystroke made on the machine, allowing the attacker to gain huge amount of sensitive information like username/password etc silently. Most of the sophisticated Key loggers can intercept virtual key strokes too.
- **Rouge Security Software:** Rogue AV (rogue antivirus) or rogue security software is a rogue (a form of Internet fraud using computer malware) that deceives or misleads users into paying money for fake. Rogue security software has become a growing and serious security threat in desktop/ mobile computing in recent years (Bonadea, 2015)
- **Ransomware:** These are also known as Crypto Virus. It is a type of malware that attacks (mostly through email attachments) the system and prevents/limits users from accessing their system. It will take the control of the system and demands a ransom to undo it. Some Ransomware applications act like police or government agency, claiming that users' system is locked down for security