Android Malware Detection And Prevention

Prajakta Ashok Kumbhar¹, Nisha Chhagan Gondhali², Prof. Sulakshana Mane

¹Computer Engineering, Bharati Vidyapeeth College Of Engineering
²Computer Engineering, Bharati Vidyapeeth College Of Engineering
³Asst. Prof Sulakshana Mane, Computer Engineering, Bharati Vidyapeeth College Of Engineering

Abstract— As the growth of internet and technology is increasing day by day, the use of smartphones, computers, tablets are also increasing rapidly. In the smartphone, Market among the other operating systems android smartphones are generally preferred by the many of the people. As android smartphones are easy to use and operate. Nevertheless, everything has two aspects smartphones bring so much convenience for the people at the same time it also brings security threat. Malicious application has a big threat to the mobile security. Thus, an efficiency security analysis and detection method is important and necessary. this paper detects and prevent the malicious attacks which are threat to mobile security.

Keywords—Android application analysis, security, malware.

I. INTRODUCTION

Mobile phones in the past are simple devices capable of performing some basic phone functions, by the release of newer smartphone operating system, mobile phones began to include advanced features like desktop which caused naive users (and made application developers) to think differently about mobile devices. Nowadays, Smart phones - Mobile phones with advanced features such as always on full-featured web browsers, Internet Connectivity, and multimedia capabilities - have become extremely popular. Additional applications such as games, productivity and communications are developed by third-party developers for entertainment purpose. The developed third-party application can be placed directly on the Android market, and there won’t be any review on the application. While using Android phone for the first time, it requires application to be signed once, Google uses these signature for bookkeeping. Users can download Android application [1] from anywhere, not only from Google play (Android Market). There have been a handful (plenty) of malicious applications in Android; most of these applications were available in Third party application store and in markets other than Android. The Android market is open for all developers for their easy use; this constraint also allows ease of entry to malware developers. But with the convenience of use of android smartphone threat to its security also comes along with it. The number of malware attacks on the android system are increasing day by day. Different malware applications are causing threat to mobile security. Malware is a malicious software which is specifically designed to disrupt, damage or gain unauthorized access to mobile system. Such Applications are pretended to be normal and useful application. As soon as user installed such applications they perform some background tasks which are threat to device integrity. They perform some malicious tasks such as stealing user’s information, SMS, Contacts, login credentials, or subscribing to premium services without user permission. The growth of malware is increasing day by day figure Fig. 1 the exponential growth of malware since early days when arguably, using antivirus was not necessary.
II. MALWARE

The malware are termed as malicious software that is designed specifically to target a mobile device system, such as tablet or smartphone to damage or disrupt the device. Most mobile malware is designed to disable a mobile device, allow a malicious user to remotely control the device or steal personal information stored on device. Once malware gets itself into the system by different media like copying of external devices onto the system and mostly by downloading the files from the internet, it checks the vulnerabilities of the system and infects the system if the system is highly vulnerable. The concern for the rate of spread of malware today is a global phenomenon, especially as it spreading double over the internet which is a means of global communication. Today's malware can do many things, such as: stealing and transmitting the contact list and other data, locking the device completely, giving remote access to criminals, sending SMS and MMS messages etc. Mobile malware causes serious public concern as the population of mobile phones is much larger than the population of PCs.

III. MOTIVES TO CREATE MALWARE

A. Novelty and Amusement
Some malware causes mischief or damage in a way that appears to be intended to amuse the author. For example, Ikee. Changed the wallpaper of infected iPhone devices, and sent anti-religion text messages text messages from Android phones. Many pieces of malware fall into this category and no other.

B. Selling User Information
Mobile operating system APIs provide applications with large amounts of information about users. Applications can query mobile APIs for the user's location, list of contacts, browser and download history, list of installed applications, and IMEI (the unique device identifier). Although we cannot know for sure why malware collects this information, we hypothesize that this data is being sold by malware distributors for financial gain. Advertising or marketing companies might be willing to...
purchase users' locations, browsing histories, and lists of installed applications to improve behavioral profiling and product targeting. However, advertising libraries in legitimate applications already routinely collect user location, and web-based advertisements already track browsing habits.

C. Stealing User Credentials
Credentials could be used directly by malware authors for greater financial gain, but financial fraud can be difficult to perpetrate and requires specialization. People use smartphones for shopping, banking, e-mail, and other activities that require passwords and payment information. Banks rely on cell phones for two-factor authentication. Users may also save authentication and payment credentials in text documents on their phones (for example, to use the phone as a mobile password manager). This makes cell phones a target for credential theft. Three pieces of malware in our data set target user credentials by intercepting SMS messages to capture bank account credentials.

D. Premium-Rate Calls and SMS
Legitimate premium-rate phone calls and SMS messages deliver valuable content, such as stock quotes, technical support, or adult services. The cost of a premium-rate call or SMS is charged to the sender's phone bill. Premium rate calls can cost several dollars per minute, and premium-rate SMS messages can cost several dollars per message. In Android and Symbian, malware can completely hide premium-rate SMS messages from the user. Premium-rate SMS attacks could feasibly go unnoticed until the user's next phone bill.

E. SMS Spam
SMS spam is used for commercial advertising and spreading phishing links. Commercial spammers are incentives to use malware to send SMS spam because sending SMS spam is illegal in most countries. Sending spam from a compromised machine reduces the risk to the spammer because it obscures the provenance of the spam. Furthermore, the use of SMS may lend more authenticity to spam than e-mail because phone contacts are often more intimately acquainted than e-mail contacts. 8 of the malicious Symbian and Android applications send SMS spam.

F. Search Engine Optimization
Many web sites rely on search engines for traffic, which makes web site owners desire high visibility in search engine results. Search engines rank web sites per how relevant each web site is to a given search term. An engine's perception of relevance is influenced by the rate at which users click on the web sites returned for a search term. A web site will rise in the results for a search term if many people search for that term and then click on that web site. Malware can be employed to improve a website's ranking in search engine results. This type of malware sends web requests to the search engine for the target search term. The malware then fraudulently clicks" on the search result that corresponds to the target web site. Thus, the web site's rank for that search term will increase.

IV. MALWARE METHOD OF PROPAGATION
The basic method of propagation of malware is either self-propagation or user interaction. A malware like worm does not require any user intervention before its execution occur. It can copy itself and causing occasional execution without the intervention of host program or its user. Virus on the other hand is a user-interaction oriented malware that always looks for a host program for its execution and consequent infection. Other malware might not require any of these methods for its propagation, but may adopt internet medium for their spreading. Mobile malware on the other hand, adopt mobile phone network on the internet to propagate itself, but this action is usually curtailed by the internally built defense mechanism in the network mobile phone. Another opportunity for mobile malware to propagate is through the direct pair-wise communication resources i.e. Bluetooth, Wi-Fi, and Infrared.
V. MALWARE DETECTION TECHNIQUES

A. Signature-Based malware detection
Signature-based detection works by scanning the contents of computer files and cross-referencing their contents with the “code signatures” belonging to known viruses. A library of known code signatures is updated and refreshed constantly by the anti-virus software vendor. If a viral signature is detected, the software acts to protect the user’s system from damage. Suspected files are typically quarantined and/or encrypted to render them inoperable and useless. Clearly there will always be new and emerging viruses with their own unique code signatures. So once again, the anti-virus software vendor works constantly to assess and assimilate new signature-based detection data as it becomes available, often in real time so that updates can be pushed out to users immediately and zero-day vulnerabilities can be avoided. A pattern-marching approach commercial antivirus is an example of signature based malware detection where the scanner scans for a sequence of byte within a program code to identify and report a malicious code. This approach to malware detection adopts a syntactic level of code instructions to detect malware by analyzing the code during program compilation. This technique usually covers complete program code and within a short period. However, this method has limitation by ignoring the semantics of instructions, which allows malware obfuscation during the program’s run-time.

B. Behavior-Based malware detection
The suspicious behavior approach, by contrast, does not attempt to identify known viruses, but instead monitors the behavior of all programs. It involves behavior based Heuristics and Generic Detections. If one program tries to write data to an executable program, for example, the antivirus software can flag this suspicious behavior, alert a user, and ask what to do. Unlike the signature based approach, the suspicious behavior approach therefore provides protection against brand-new viruses that do not yet exist in any virus dictionaries. However, it can also sound many false positives in recent years, however, sophisticated behavior analysis has emerged, which analyses processes and calls to the kernel in context before deciding, which gives it a lower false positive rate than rules based behavior monitoring. Unlike heuristics or fingerprint-based scanners, behavior blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system. If the behavior blocker detects that a program is initiating would-be malicious behaviors as it runs, it can block these behaviors in real-time and/or terminate the offending software. This gives it a fundamental advantage over such established anti-virus detection techniques such as fingerprinting or heuristics. While there are literally trillions of different ways to obfuscate and rearrange the instructions of a virus or worm, many of which will evade detection by a fingerprint scanner or heuristic, eventually malicious code must make a well-defined request to the operating system. Given that the behavior blocker can intercept all such requests, it can identify and block malicious actions regardless of how obfuscated the program logic appears to be.

VI. CONCLUSION
In this paper, what is meant by malware exactly and motives behind creation of different threatening malware is provided comprehensively. We have also specified the method of propagation of these malwares. We have also compared and reviewed most well-known malware detection technique. The presented detection techniques are feasible, but large scale testing is required to determine real world performance. As Android malware evolves the efficacy of these measures will decrease.
REFERENCES