Dissecting Android Malware

Nandanam Vikas

02/08/2016

As we all know that the usage of smartphones is increasing rapidly as the technology is also emerging and taking the world into a new dimension. The usage of smartphones is increasing rapidly but there is also increase in the malware in the smartphones especially in Android phones. According, to the paper published the objective of the paper is to detect and reduce the malware in Android smartphones. The authors have taken 1260 samples of malware which are categorized into 49 different families. The observation of the malware in android smartphones will be compared with samples which are obtained. The observation is done in three phases, firstly the entire malware sample collected is sent for research. Secondly, a timeline analysis of each malware is done to analyze behavior, characteristics etc. Finally, evolution based study shows the anti-malware which are lagging behind. Malware timeline analyses the time at which the malware is detected, examines the contents and locates the sources of malware. To eliminate the malware it is tested with the existing malware and verified.

Malware characterization illustrates the occurrence of malware from installation till enclosing malicious payload. In installation, repackaging it is where popular apps are disassembled and enclosed with a malicious payload and uploaded to android market. According to the study around 86% are repackaged malware where 28 families are in built and 27 families gather user information without users knowledge. The update attack, this attack is quite difficult to detect because here malicious payload is not enclosed rather update malicious packages are included which are downloaded automatically at the runtime. Drive by download, shows ads or puts links and when user clicks goes to the malicious sites or download malicious apps without the users approval. Coming to malicious payloads, privilege escalation is where a flaw in the system architecture or design helps the intruders to attack. As android has many open source libraries there can be vulnerabilities at platform level itself which can also be names as root exploit. It is very difficult to detect these as they are encrypted and decrypted at runtime. Remote control is the attack which has affected 93% of smartphones it is where malware families encrypt the URL and remote servers which leads to malicious attacks. It is also observed that with the payloads by sending SMS the users confidential information like phone number user details are gathered.

——	AVG	Norton	Lookout	Trend Micro
Samples detected	689	254	1003	966
Percentage	54.7%	20.2%	79.6%	76.7%

Malware detection is most challenging phase as the above mentioned malware can be attacked at any level of smartphones including their platform level. The authors have conducted a test to detect malware by using different antivirus software. Before scanning for malware an iterative script is placed in app. In the process of scanning if malware is detected and alert window appears in this way it is observed two times with a wait of 30 and 60 seconds respectively.The results shown are not satisfactory. With the observation it can be stated that the companies preparing the app should improve the design of app which easily and efficiently detects the malware.

This is my github repository link: `https://github.com/Nandanam/Latex.git`