The computer landscape has changed drastically in the last decade with the introduction of mobile devices. Along with this massive shift is the software operating these devices, the mobile operating systems and the attacks intended to exploit these lite/skinny operating systems.

Per Kaspersky’s Lab, in 2017 they detected over 5.7 million malicious installation packages, over 94,000 mobile banking Trojans, and over 544,000 mobile ransomware Trojans.

Some of the trends they witnessed were:

* Rooting Malware
* Wireless Application Protocol (WAP) Billing Trojans
* Mobile Ransomware

Just how far has mobile malware come? Let’s take a quick look at it’s history first.

The Firsts

The first Android Botnet was discovered in 2010 and was distributed through third party markets in China. The purpose of the botnet was to establish a C&C communication and leak sensitive information to a remote server, download APK’s, and execute other commands given by the remote user. It also used TCP sockets to communicate and work with multiple instances on the same device.

The first iOS malware/worm was discovered in 2009. The malware targeted jailbroken iPhones through SSH connections. It acted as a ransomware, manipulating the device and requesting the user send $5 as payment to reset the phone to it’s previous settings and removal of the malware. This malware was possible due to SSH root access through poor password security and simplicity.

Present

In present day, mobile malware is much more sophisticated. They gain super-user rights by exploiting system vulnerabilities that allow the malware to install modules in system folders, allowing it to persist, even if the phone is reset to factory default settings. Most Android Trojans are distributed to through the Google Play Store.

In April 2017, Kaspersky Labs observed new rooting malware being distributed through the Google Play Store where it not only installed modules into the system, it also injected malicious code into the system runtime libraries. This malware was identified as Dvmap.

To bypass Google Play Store security checks, the malware creators used a very interesting method: they uploaded a clean app to the store at the end of March, 2017, and would then update it with a malicious version for a short period of time. Then they would upload a clean version back on Google Play the very same day. Another interesting component of the Trojan was that it could support 64-bit version and 32-bit version of Android, something that is considered rare.

WAP Billing Trojans were also popular in 2017. These Trojans would receive a list of links from a command and control server, follow them and click on page elements using a specific JavaScript file. It would visit pages with WAP subscriptions, with the money being taken from the user’s mobile account. A page with WAP billing usually redirects to a mobile operator page where the user confirms they agree to pay for the services.

Most security researches believe the up and coming malwares are modular Trojans used for crypto-currency mining. Due to the rise in the price of crypto-currency, Trojans that can assist in the mining efforts allow for a more profitable business. However, these malware’s can alert a end user of an infection since crypto mining is resource intensive, it can deplete a devices battery fairly quickly and lead to device failure.