Avoiding malware on the move

9 July 2020, by David Bradley

Credit: CC0 Public Domain

Mobile devices are a fairly ubiquitous feature of our lives. Some would say that their huge and yet compact computing power has made life easier for millions of people by providing information, entertainment, and services at a tap or a swipe. Of course, every technology has its abusers and our always-connected smartphones, tablets, and laptops are no different.

Writing in the *International Journal of Internet Technology and Secured Transactions*, researchers from India discuss the security measures available for mobile devices that utilize Google's Android operating system. They suggest that the more open nature of Android and its applications ecosystem can in some sense make it more vulnerable to malware than the rather more closed and cloistered operating system used by devices manufactured by Apple. Indeed, evidence suggests that 97 percent of malware targets Android rather than any other operating system on mobile devices.

The team has analysed hundreds of Android apps from the official store and unofficial download repositories. They used applied permission-based and behavioural footprinting methods to detect malware. Shockingly, they demonstrated that almost 13 percent of the apps on the official Play store had some kind of malware. This figure was more than double at 28 percent for third-party stores.

Much malware discussed in the context of conventional desktop computing is associated with criminal activity such as harvesting bank details and logins, duplicating and spreading the malware further afield, and creating zombie computers. Zombie PCs not only propagate the malware further but they are recruited into a bot-net and provide the controllers with the computing power to manipulate large numbers of PCs for carrying out denial of service attacks on large corporate or governmental networks with malicious or hacktivist intent.

The team found that almost all of the malware in Android apps was created to steal personal information from the infected device and send it to a remote server. Given that even legitimate applications do this endlessly, it is difficult to see where the line is being drawn. Nobody wants their personal and private information stolen whether by a small third-party app or a major corporate organization such as a search engine or social media company.

As such, the team has also assessed a number of the most prominent apps aimed at precluding infection with mobile viruses and malware. Unfortunately, even the best antimalware apps tested could detect a mere seven of twelve different classes of malware found on Android systems. The underlying reason is that new, zero-day malware, is emerging all the time.

"There remains a need for efficient anti-malware software that accurately detects and avoids malware families," the team writes.

More information: Sangeeta Rani et al. Android application security: detecting Android malware and evaluating anti-malware software, *International Journal of Internet Technology and Secured*

Transactions (2020). DOI: 10.1504/IJITST.2020.108142