Zen: A Complex Campaign of Harmful Android Apps

conference.hitb.org/hitb-lockdown002/sessions/zen-a-complex-campaign-of-harmful-android-apps/

Android malware authors go to great lengths to come up with increasingly clever ways to monetise their apps. The author (or a group) presented during my talk shows quite the range, from simply repacking apps with a bespoke advertising SDK to writing a sophisticated rooting trojan with new techniques never seen in other harmful apps.

Their most complex creation is called “Zen”. Zen bundles exploits to gain privileged root access. It then uses this access to create fake Google accounts on devices. These accounts are created by abusing accessibility service with additional help from code injection.

Apart from that, authors also wrote click fraud and spammy apps, mostly because of the increasing difficulty of obtaining a reliable Android exploit and security improvements in newer Android versions.

I will present all the different kinds and variations of malware coming from this group, highlighting the most interesting, complex and unusual technical details. This includes circumventing CAPTCHA images and a number of persistence mechanisms, including the modification of Android framework files.