PTA Cyber Security Alert

26-November-2019

Android Camera App Spying Security Threat

Summary:

A new Security threat is found to target the Android-based Camera devices. As the mobile devices are constantly collecting, storing and sharing different types of data, with or without user's knowledge, hence, making goldmines for the attackers. A detailed analysis of the Google and Samsung Camera app was performed by the global security researchers and it is found that, by manipulating specific actions and circumventing different storage permission policies, an attacker can control the application to take photos, record videos and phone calls, access stored photos/videos and even locate the user from GPS metadata.

Once the malicious application starts, it creates a persistent connection back to a Command and Control (C&C) server and waits for commands and instructions from the attacker, who is operating the C&C server's console from anywhere in the world. Even closing the app does not terminate the persistent connection.

Recommendations:

- Update the application to the latest version as both of the vendors have reportedly fixed the aforementioned vulnerability.
- Only install applications from official Google Play Store or Vendor's official App store and pay close attention to permissions requested by the apps during the installation
- Always be vigilant and run the application with minimum necessary permissions. Please follow the recommended Android Apps permissions best practices: https://developer.android.com/training/permissions/usage-notes

- Avoid download/use of cracked and pirated software
- Keep the mobile device's security up-to-date with vendor's recommended anti-virus software and regularly perform anti-virus scans
- Regularly perform backups of important data

References:

- https://info.checkmarx.com/wp-vulnerability-report-android-camera-app
- https://nakedsecurity.sophos.com/2019/11/21/android-camera-bug-could-have-turned-phones-against-their-users/