Subject: **Prevention Against Password Stealing Apps On Google Play Store Advisory No 02- January, 2018**

1. Introduction. Recently, the security researchers have discovered around 85 android applications on Google Play Store that are designed to steal credentials from users of **Telegram** (instant messaging service) and **VK** (a Russian-based social networking service). These malicious apps are successfully downloaded millions of times. The most popular amongst all is masqueraded itself as a gaming app. When this app was initially submitted, it was just a gaming app without any malicious code. However, after few months, the malicious actors behind the app updated it with information-stealing capabilities. These malicious applications have been detected and removed by Google from the Play Store.

2. **Summary of Malicious App**

a. **Malware name**

(1) Trojan-PSW.AndroidOS.MyVk.o

(2) HEUR:RiskTool.AndroidOS.Hcatam.a

b. These apps looked like they came from VK.com - for listening to music or for monitoring user page visits, requiring a user to login into his account through a standard login page (fake page).

3. **Technique Used.** The apps used an official SDK for VK.com but slightly modified it with malicious JavaScript code to steal users' credentials from the standard login page of VK and pass them back to the apps' servers.

4. **Mode of Operation**

a. Once the user enters his credentials on fake login page, they are stolen.

b. The stolen credentials are then encrypted and uploaded to a remote server controlled by the attackers.

5. **Recommendations.** In order to prevent user's data from being vulnerable to theft, the following is suggested:-

a. Enable *Google Play Protect* security feature on the device. This feature will remove (uninstall) malicious apps from user's Android smartphone to prevent further harm.

b. Download apps from Goggles Official Play Store vigilantly and always verify app permissions and reviews before downloading any app.

c. Backup your files regularly.

d. Install an antivirus app (e.g. Avast) on Smartphone that can detect and block malicious apps before they can infect a device.

e. Always keep the device OS and apps up-to-date.