Even after so many efforts by Google like launching bug bounty program and preventing apps from using Android accessibility services, malicious applications somehow manage to get into Play Store and infect people with malicious software.

The same happened once again when security researchers discovered at least 85 applications in Google Play Store that were designed to steal credentials from users of Russian-based social network VK.com and were successfully downloaded millions of times.

The most popular of all masqueraded as a gaming app with more than a million downloads. When this app was initially submitted in March 2017, it was just a gaming app without any malicious code, according to a blog post published Tuesday by Kaspersky Lab.

However, after waiting for more than seven months, the malicious actors behind the app updated it with information-stealing capabilities in October 2017.

Besides this gaming app, the Kaspersky researchers found 84 such apps on Google Play Store—most of them were uploaded to the Play Store in October 2017 and stealing credentials for VK.com users.
Other popular apps that were highly popular among users include seven apps with between 10,000 and 100,000 installations, nine with between 1,000 and 10,000 installations, and rest of all had fewer than 1,000 installations.

Here’s How Cyber Criminals Steal Your Account Credentials:
The apps used an official SDK for VK.com but slightly modified it with malicious JavaScript code in an effort to steal users’ credentials from the standard login page of VK and pass them back to the apps.

Since 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/her account through a standard login page did not look suspicious at all.
The stolen credentials were then encrypted and uploaded to a remote server controlled by the attackers.

“The interesting thing is that although most of these malicious apps had a described functionality, a few of them were slightly different—they also used malicious JS code from the OnPageFinished method, but not only for extracting credentials but for uploading them too,” Kaspersky said.

Researchers believe that the cybercriminals use stolen credentials mostly for promoting groups in VK.com, by silently adding users to promote various groups and increase their popularity by doing so, since they received complaints from some infected users that their accounts had been silently added to unknown groups.

The cybercriminals behind these apps had been publishing their malicious apps on the Play Store for more than two years, so all they had to do is modify their apps to evade detection. Since VK.com is popular mostly among users in CIS countries, the malicious apps were targeting Russian, Ukrainian, Kazakh, Armenian, Azerbaijani, Romanian, Belarusian, Kyrgyz, Tajik, and Uzbek users.

The apps did so by first checking the device language and asked for login credentials from users with one of the above-mentioned languages.

In addition, researchers also noted that they found several other apps on Google Play Store that were submitted by the same cyber criminals and published as unofficial clients for the popular messaging app Telegram.

“These apps were not only masquerading as Telegram apps, they were actually built using an

open source Telegram SDK and work almost like every other such app," the researchers said, adding that these apps also add infected users to promoted groups/chats based on a list received from their server.

How to Protect Your Device From Such Malicious Apps
All the apps, including the credential-stealing apps (detected as Trojan-PSW.AndroidOS.MyVk.o) and malicious Telegram clients (detected as not-a-virus:HEUR:RiskTool.AndroidOS.Hcatam.a), have since been removed by Google from the Play Store.

However, those who have already installed one of the above apps on their mobile devices should make sure their devices have Google Play Protect enabled.

Play Protect is Google's newly launched security feature that uses machine learning and app usage analysis to remove (uninstall) malicious apps from users Android smartphones to prevent further harm.

Although it is a never-ending concern, the best way to protect yourself is always to be vigilant when downloading apps from Google's official Play Store, and always verify app permissions and reviews before you download one.

Moreover, you are strongly advised to always keep a good antivirus app on your mobile device that can detect and block such malicious apps before they can infect your device, and always keep your device and apps up-to-date.

PS: Click on the link below to sign up for my Online E-Course CRM Training. Make sure you confirm your subscription by clicking on the link sent to you. Thanks.

Related posts:

40,000 Customers Affected By Credit Card Breach On OnePlus

Hidden Backdoor Found In WordPress Captcha Plugin Affects Over 300,000 Sites

Three Hackers Plead Guilty to Creating IoT-based Mirai DDoS Botnet

Oops... Some HP Laptops Shipped With Hidden Keylogger

Google Researcher Releases iOS Exploit—Could Enable iOS 11 Jailbreak

Largest Crypto-Mining Exchange Hacked; Over $70 Million in Bitcoin Stolen