4 Android VPN applications with over 500 million downloads were found to be ad fraud

Up to now, malware and viruses have always been a headache for Google Play Store managers.

Up to now, malware and viruses have always been a headache for Google Play Store managers. The problem of malicious code floating, malicious applications appearing on the Google Play Store is increasingly being better controlled, but it seems unable to be completely cleaned up despite Google has been really trying and serious in developing declaration of restraint measures on a large scale, continuously.

Besides malware, the problem of Android adware abuse is also often mentioned as one of the reasons for the user experience for this operating system. Recently, a researcher from an independent security team based in New Zealand Andy Michael found two Android VPN applications with total downloads and installs of more than 500 million with abusive advertising. . These apps not only play ads themselves in the background, but even play ads outside the app, including the home screen.

1. Don't trust VPN apps on Google Play, this is why

The number of apps that contain ad abuse software in the category of security applications like VPNs is increasing

The applications mentioned by Mr. Andy Michael include: Hotspot VPN, Free VPN Master, Secure VPN and Security Master by Cheetah Mobile. It is worth noting that all of these applications originated from Hong Kong as well as China, where the majority of mobile device users often rely on VPNs to bypass the limits of the Great Firewall.

As of the time of writing, the above mentioned applications are still operating on the Play Store without any action from Google. According to statistics, the number of applications that contain adware in the category of security applications such as VPN or antivirus is on the rise, showing that mobile application developers have a clear grasp. The fact that users often put more trust in security-related applications, thereby taking advantage of their own beliefs to make profit, specifically here is the abuse of advertising.

1. Authentication tool on many enterprise VPN applications was bypassed by hackers

App Name	Developer	Origin	Install Counts
Hotspot VPN - Free Unlimited Fast Proxy VPN	HotspotVPN 2019	Hong Kong	> 500,000
Free VPN Master - Fast secure proxy VPN	Freemaster2019	Hong Kong	> 1,000,000
Secure VPN - Unlimited Free & Super VPN Proxy	SEC VPN	Hong Kong	> 5,000,000
Security Master - Antivirus, VPN, AppLock, Booster	Cheetah Mobile	Beijing	> 500,000,000

4 ad fraud VPN apps are mentioned by Andy Michael

Disruptive advertising behavior - abuse of advertising

In addition to containing advertising APIs from both Google and Facebook, Hotspot VPN, one of four applications named and developed by Andy Michael by HotspotVPN 2019, also contains a hidden script with the task of automatically displaying ads. Full screen at any time - regardless of whether the application is running in the background or being opened directly - resulting in a significant drain on battery life and CPU resources, resulting in overall device performance Serious impact and negative impact on user experience with the system.

The same is the case with the Free VPN Master application developed by Freemaster2019. This free VPN tool used a separate code snippet to serve Google ads, with both APK files sharing the same code and file structure.

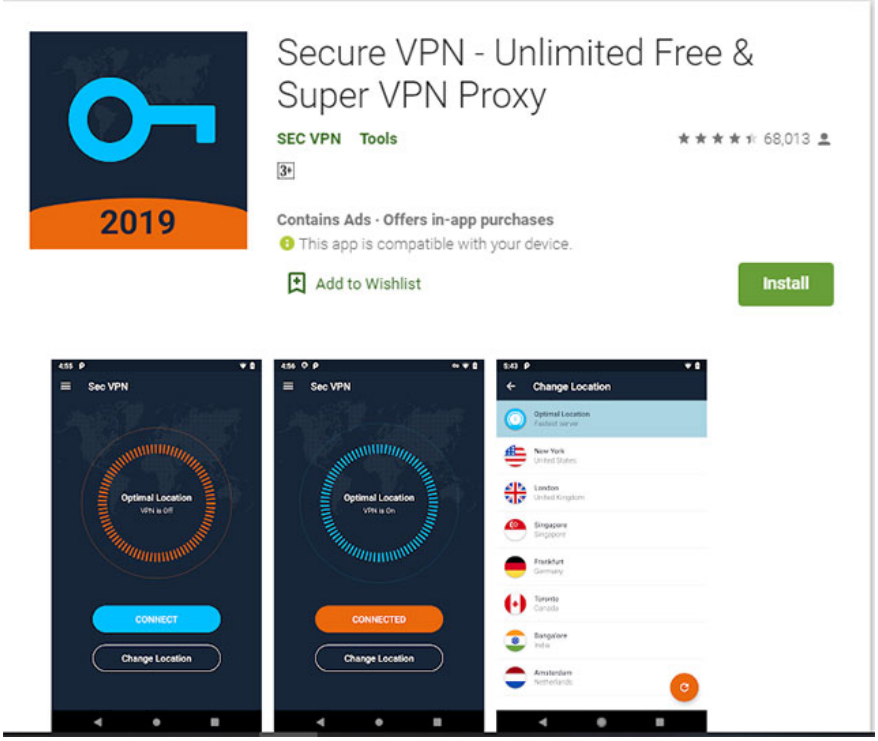
1. Why is using a VPN something that online gamers should do?

Security researcher Andy Michael concludes that the two applications have very similar characteristics, with minor modifications in the code found to have been tampered with using the same tool.

'If apps are forced to stop from Android settings, they will stop serving abusive ads. However, if you only need to open the application once, the aforementioned behavior will be reactivated again, 'the New Zealand expert said.

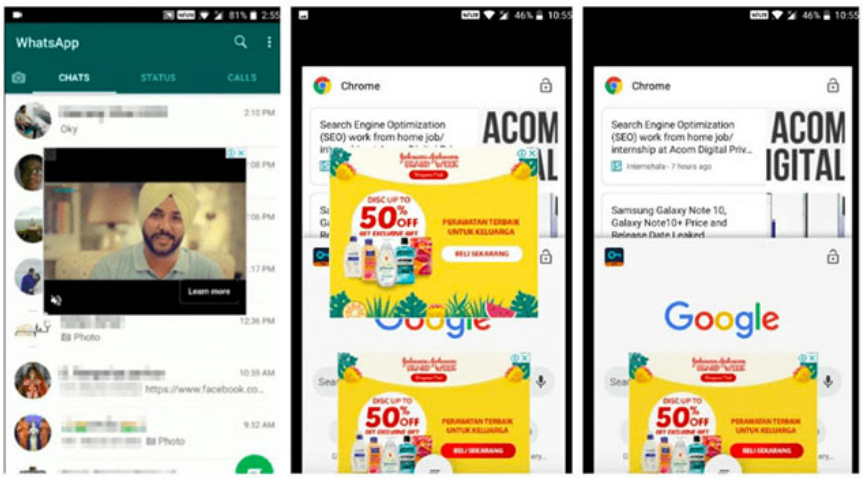
The third application on the list, SEC VPN's Secure VPN, can be considered the 'worst' advertising abuse VPN tool. It distributes ads even when the user is using other apps and sometimes gets hidden on the home screen, causing the application icons to be hidden.

1. The worst privacy protection VPN users should avoid



SEC VPN's Secure VPN can be considered as the 'worst' advertising abuse VPN tool.

Secure VPN was also found to have references to scripts that record all activities, including advertisements that have been displayed, ads that have been clicked and removed by the user . implying that they are used to track and display ads based on actual user activities.



Ads obscure the screen, causing discomfort in the Secure VPN application

Not only that, Security Master, the last application on the list, also uses a more sophisticated method of displaying ads, such as when the user is trying to return to the main screen or when clicked. certain options.

In fact, the fact that mobile apps are abusive in advertising is not new information, which is sometimes a good way for app developers to profit from the apps they do. out was completely free. However, distributing ads while apps are running in the background can lead to significant abuse of resources on devices such as batteries and

CPUs, which can greatly impact the experience of user.

1. Cloudflare launches integrated VPN service in app 1.1.1.1, speeding up faster and more safely

Cheetah Mobile's Security Master application with more than 25 million downloads

For its part, Cheetah Mobile is also one of the application developers that has been touched by Google after it detected click fraud, causing a series of applications with hundreds of thousands of downloads. removed from Play Store.

'Developers are always looking for ways to misuse ads or cheat clicks because every time an ad is displayed or clicked on, they get revenue. VPNs and antivirus are one of the most commonly used applications on mobile phones, so it is understandable that these fraudulent behaviors are appearing in such applications. , said Michael.

Of course Google understands this situation and they have a strict management policy related to adware and ad abuse in general, as follows:

'We do not allow applications that contain deceptive, disruptive, or abusive ads to appear on the Play Store. Ads are only displayed while the application is active in the main screen. We consider ads served within apps as part of the application. Ads displayed in the application will have to comply with all our policies. '

Google is currently scrutinizing Hotspot VPN, Free VPN Master, Secure VPN and Security Master applications as reported by Andy Michael. If everything happens as described by a New Zealand expert, the chances of the above applications being forced to be removed from the Play Store is very high.

1. Malicious software and user security flaws are found in leading free VPN apps

Play Store and ad abuse issue

This is not the first time that Google has launched aggressive crackdowns to limit the spread of harmful apps on its world's largest mobile app distribution platform.

Just in August, Lukas Stefanko, an ESET team security researcher, compiled a list of 204 apps on the Google Play Store with a total of 438 million downloads and installations detected. fraud, advertising abuse, and even distribution of other types of malware.

1. Google 'purged' 24 applications downloaded nearly 500,000 times containing malicious malware

Harmful app type	Number of apps	Number of installs
AdFraud	42	419,000,000+
Adware	112	8,600,000+
HiddenAds	10	6,430,000+
Subscription Scam	3	3,000,000+
Fake Antivirus	10	1,386,000+
RAT/Spyware	24	10,210+
Credit card phishing	2	105+
Fake VPN	1	50+
sum	**204**	**438,426,365+**

List of number, categories and number of downloads of fraudulent advertising applications according to statistics of Lukas Stefanko

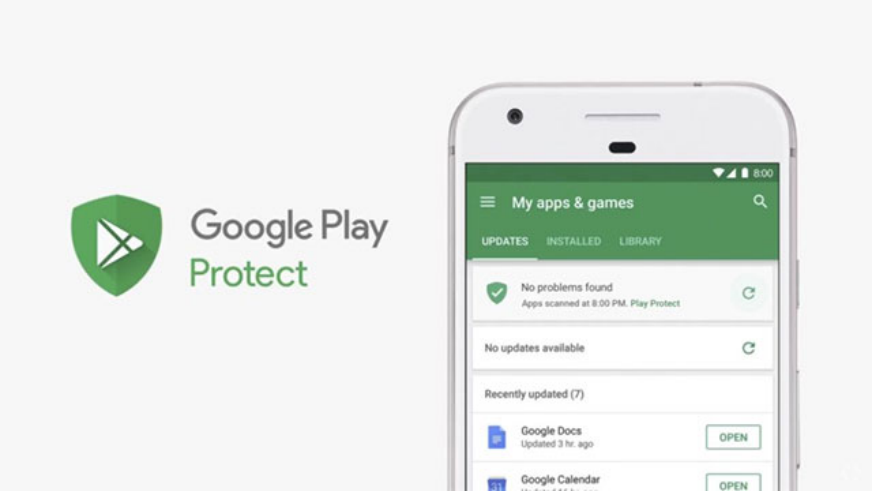
Although Mountain View's anti-malware efforts have achieved some success when hundreds of thousands of malicious applications have been removed from the Play Store, there are still many issues that the platform has. are facing, especially at the remote control and defense stage.

The complex problem lies with the open nature of Android, which makes copying and malicious applications able to get out of Google's control relatively easily and put users at risk.

'Keeping the Android ecosystem safe is not an easy task, but we firmly believe that Google Play Protect is an important security layer and can provide the necessary protection for all devices and data. user data, while maintaining freedom, diversity and openness - elements that make Android's great experience. '

The fact that a legitimate app store like Google Play constantly contains malicious apps is a major cause of the growing security and privacy concerns on mobile devices in general. The current. Android users are often advised not to download apps from third-party sources to avoid malware. But unfortunately, the fact has proven that Play Store's 'genuine' apps aren't always secure.

1. Just finding the security bug is paid by Google, Vietnamese white hat hackers can join



Google Play Protect is the key security of Play Store app store

We all know that one of the prerequisites for application security is to consider the name of the developer of the application. However, according to network security experts, users also carefully review the reviews of other users about the application that they intend to install on the device.