

Malware and user security bugs are found in top free VPN applications

For every five applications listed in the top 150 free Android VPN apps on Google's Play store, one is flagged as a potential source of malware.

For every five applications listed in the top 150 free Android VPN apps on Google's Play store, one is flagged as a potential source of malware. In addition, 1/4 of the VPN application in this list is also said to contain security flaws that seriously affect users' privacy, such as DNS leaks that reveal users' DNS queries to their ISPs. .

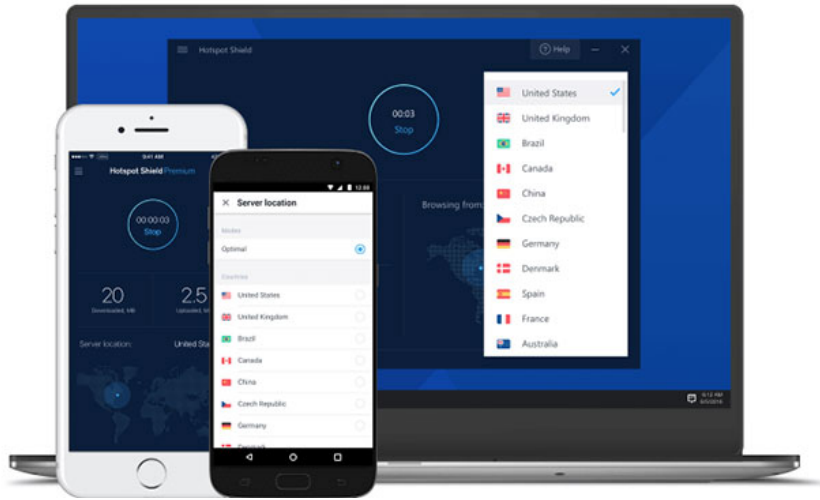


1. Why should I stop using VPN for free immediately?

According to security expert Simon Migliano, Head of Research at Head of Research, the company behind the Top10VPN service, these Android VPN applications have been downloaded and installed about 260 million times according to the reported data. reported by Google itself. And this will be a scary source of malicious code if companies do not soon make corrective measures.

The in-depth study initiated by Top10VPN has been developed and published as a risk indicator, designed to help Android users understand exactly the security risks they face at high risk. when installing a free VPN application on your smartphone or tablet.

According to Simon Migliano's analysis and as mentioned before, one out of every five free VPN applications is tested, with a total of 27 applications being a potential source of malware when tested. Check with VirusTotal, greatly increasing the level of risk that users are at risk.



The problem becomes even worse when up to 25% of top VPN applications are affected by DNS security leaks. Specifically:

'This security vulnerability occurs when VPN applications cannot force DNS requests through encrypted traffic to its own DNS servers, and instead allow requests to be made directly to the ISP's default DNS servers. Although the rest of the traffic may be confidential, the leaked data will suffice to reveal the user's browsing history to ISPs and any third-party DNS server operators. Which they can use'.

Issues found in the top ten free VPN applications (most downloaded and installed) on the Google Play store as follows:

Application (installation)

Rights risks

DNS leak

Functional risks

Virus / malware

Hotspot Shield is free

(50 million installments)

Discovered

Is not

Discovered

Is not

SuperVPN

(50 million installments)

Discovered

Have

Discovered

Is not

Hi VPN

(10 million installments)

Discovered

Have

Discovered

Is not

Hotspot Shield Basic

(10 million installments)

Discovered

Is not

Not detected yet

Is not

Psiphon Pro

(10 million installments)

Discovered

Is not

Discovered

Is not

Turbo VPN

(10 million installments)

Not detected yet

Have

Not detected yet

Is not

VPN Master

(10 million installments)

Not detected yet

Have

Discovered

Is not

Snap VPN

(10 million installments)

Discovered

Have

Discovered

Is not

Hola

(10 million installments)

Discovered

Have

Discovered

Is not

SpeedVPN

(10 million installments)

Discovered

Is not

Discovered

Is not

The study of Top10VPN also said that experts have found rights that are difficult to penetrate as well as code functions that make users of these VPN applications at risk of privacy, this problem may be encountered on About 85% of all free VPN applications are tested.

In addition, the team also found access rights and user privacy codes as follows:

1. Location tracking (over 25% of applications are tested).
2. Access device status information (about 38% of applications tested).
3. Use cameras, microphones and the ability to secretly send SMS (insignificant).
4. Use featured code to collect data about the end user's location (on about 57% of applications tested).

As detailed in the methodology section of the test results report, Migliano's team has installed each of one of the 150 most popular VPN applications on Android smartphones, at the same time running the test. VPN connection of these applications with the ICaly Netalyzr Internet connection analysis utility.



On the same VPN connection, researchers have conducted various IP tests using the online browserleaks.com platform compared with other control tests that are also implemented on the same device. without using any VPN connection.

1. Google paid a fine of 50 million euros after allegedly violating the General Data Protection Act in France

When asked if users' privacy violations still appear in paid versions of these VPN applications, Migliano said:

'Although we do not upgrade to premium (paid) versions and conduct additional tests, I am confident that the key privacy issues will still exist, such as : DNS leaks, intrusion rights and risk code functionality. Basically, when you upgrade to the paid version, these applications still run on the platform of the free version, only to be added a few more advanced features'.

Simon Migliano is also the expert behind a previous analysis of the top 20 free VPN and iOS applications, leading to the conclusion that most of these applications are nearly impossible to protect. Privacy protection of users. As well as not having any support for users after the study was revealed.

Again, privacy is a painful issue that we must consider before using any application or service today.

See more;

1. Microsoft shook hands with VirusTotal in resolving malicious code issues that affected MSI files
2. The Internet is experiencing a huge problem with C / C ++, causing developers to "sweat"
3. The corner of getting rich: A company hung a \$ 1 million prize for anyone who hacked WhatsApp and iMessage
4. The provisions of the Criminal Code relate to the field of information technology and telecommunications networks

You finished reading the article "**Malware and user security bugs are found in top free VPN applications**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.