How does malware get into smartphones?

Malicious apps are disastrous for smartphone users. Regardless of whether you use iOS or Android, it will be terrible if the application is infected with malware.

Malicious apps are disastrous for smartphone users. Regardless of whether you use iOS or Android, it will be terrible if the application is infected with malware. Google Play Store is flooded with malicious applications, while Apple App Store reputation is also affected.

Why do bad guys want malware to infect smartphones with malware-infected apps? There are two simple reasons: Money and data. There are countless applications out there. So how to avoid malware from entering the application? Let's learn through the article today.

How does malware get into smartphones?

1. The application is infected with malware everywhere
2. How are applications infected with malware?
    1. Malvertising (malicious ad)
    2. Application reprint
    3. Sell ??application
3. Does Apple or Google have help?
    1. Apple
    2. Android
4. How to avoid detection of malware
5. Remove malware on mobile devices

The application is infected with malware everywhere

It is difficult to measure the extent of malware infected mobile applications. One thing is clear: no single mobile operating system is free. Recently, Android users encounter attacks of HummingWhale, Judy and Xavier, while iOS users face XcodeGhost.

A study published in 2014, part of the ANDRUBIS project, tested more than a million Android applications (the exact number is 1,034,999). Sampled applications come from a variety of sources, including informal markets, torrents, websites that offer pirated applications and even Google Play Store.

Of the 125,602 applications sampled from Google Play Store, 1.6% are malicious applications (equivalent to 2009 applications).

Data on malicious apps for the App Store are very rare. There are only a few cases of malicious applications recorded on iOS devices. IOS applications minimize the risk of malware infection significantly compared to Android applications. Pulse Secure's mobile threat report 2015 estimates that 97% of malware on mobile devices is targeted at Android devices. Report F-Secure State of Cyber ??Security 2017 figures up to 99%. In 2013, the US Department of Homeland Security estimated only 0.7% of malware on mobile devices targeted at iOS devices. A contrast is quite obvious.

How are applications infected with malware?

What do you think makes an application infected with malware? Developers? Crime gang? Personal harm? Or is the government? These capabilities can occur in a number of ways.

The most obvious is the fake developer: An individual designing malicious apps and publishing them on Play Store (or something similar). Fortunately for users, there are not too many malicious apps on Play Store.

That's probably for one reason: The effort required to develop, launch and build an application, and turn it into malicious is too big. By the time the application becomes popular enough to actually make a profit (perhaps by clicking on ads or data theft), malware developers can also make more money through businesses. Ad collection.

Normally, you will see malicious code inserted into an existing application, then re-published. This process uses a number of different techniques.

Malvertising (malicious ad)

Malvertising is a common disaster of the 21st century. The mechanism is simple: Malicious advertising is distributed through official channels. You don't expect a malicious attack through a legitimate application, so they attack users unexpectedly.

The most typical example of malvertising Android is Svpeng banking Trojan. Trojans are installed primarily through malware-infected Google AdSense ads, targeting Google Chrome and Android users. In fact, you don't really have to click on the ads to get malware, just see the ad is already infected.

Application reprint

Legitimate applications downloaded from an official application store are infected with malware. Then, they are reprinted using the official name of the application, to a variety of other application stores (possibly legal or not).

A major feature of application reprints is small variations in the application name. For example, instead of Microsoft Word (official release of Microsoft), it would be Micr0soft W0rd. Charger, Android ransomware and malwareising-malware, Skinner, also use this tactic (with some other tactics).

Sell ??application

Over time, a legitimate application developer will sell their valuable application. Applications will gradually come to users. Then, reliable updates are also provided to users.

However, there is no document about specific attack methods for these legitimate applications. Similar issues occur regarding Chrome extensions. A popular Chrome extension has access to user data. With thousands of users, this is a real gold mine. Honey's developers tried to minimize the number of malware.

Amit Agarwal sold his Chrome extension to an unidentified individual, and saw the next application update "incorporating ads into extensions", which is out of his control. . His achievements have now become a means to spread advertising.

Does Apple or Google have help?

As the owner of the largest and most popular app store, these tech giants are responsible for protecting their users. Most of them do very well. That malicious applications get into the app store is harmful to users, as well as the reputation of these firms.

Apple

Apple is definitely the 'leader' when it comes to protecting iOS users from malicious applications. The process of creating and uploading applications to the App Store is quite complicated and requires many checks. In addition, an iOS app has a smaller distribution range than Android apps.

Android

Google had to work very hard to reduce the number of malicious applications in Play Store. With a reputation of being at risk of being compromised, Google introduced Play Protect, a 'mobile security shield'. Play Protect actively scans the user's device for malicious applications. Moreover, Play Protect also automatically scans Play Store to find malicious applications, suspend harmful developers and delete infringing applications.

How to avoid detection of malware

While Google and Apple make concerted efforts to keep users' devices free of malware, malware developers try to avoid detection. There are a few common ways that an attacker will hide their malicious code like:

1. Download malicious code after installation.
2. Mix malicious code into "clean" code.
3. Time delay / guide the application to wait before downloading or deploying.
4. Based on distribution through external sources (for example, malicious advertising).
5. Hide malicious applications in other media.

As you can see, there are many methods to make malicious applications or malicious code in the application hidden from users.

Remove malware on mobile devices

As you have seen, there is a significant amount of malicious code that can enter an application. Furthermore, malware developers have a number of methods for users to be unable to detect malicious code, until it enters the phone.

How can you avoid downloading a malicious application?

1. Download applications only from official app stores
2. Avoid third-party app stores.
3. Check if you are downloading an application from an official or reputable developer.
4. Read app reviews. They will give you the information you need.
5. Always turn on the application verification tool.

6. Do not be fooled by free apps.
7. Update your phone regularly.

There are many malicious applications out there, especially if you are using an Android device. But by understanding the threats and remembering the tips in this article, you and your device will be safe.

Do you encounter malware on mobile devices? Are you using an Android or iOS device? What happened to your smartphone? Let us know your opinion in the comment section below!

See more:

1. Remove root malware (malware) on Windows 10 computers
2. Top best antivirus application for Android phones
3. How to scan and repair computers infected with viruses or malware