What is rooting malware? What can you do to protect yourself?

Rooting malware works by gaining root access to the victim's phone. This gives the malware more control over the phone.

Owning a rooted phone is often a positive thing that people wish for, but not always. Sometimes, a malicious program can root your device without your knowledge, causing you to face many problems with no benefit.

So, what is rooting malware, how does it work, and how do you keep yourself safe? Let's learn with TipsMake through the following article.

What is rooting malware?

Rooting malware works by gaining root access to the victim's phone. This gives the malware more control over the phone, allowing it to perform some really nasty actions while lurking on the victim's system.

The term 'root' itself is not a bad thing. In fact, people root their phones all the time. When you root your phone, you have administrative access to its data and operating system. This gives you much finer control over the hardware and the applications installed on it.

However, the key difference between rooting your phone yourself and malware doing it for you is that malware does things without your permission or without your knowledge. And while you know well what's going on,

malware is using higher permissions to wreak havoc on your system.

Luckily, rooting malware is one of those rare viruses you can download to your phone. However, the level of danger it can pose is enormous.

How does rooting malware spread to phones?

Usually, rooting malware gets into your phone through an infected app. This could be a legitimate app containing rooting malware or an app specifically designed to trick people into downloading it.

Regardless of the malware's attack vector, you probably won't find it in rogue root apps. That's because the malware developer doesn't want the victim to know that their phone is rooted. As a result, you are more likely to find rooting malware in apps that don't involve rooting so the malware can do its job undetected.

You will often find these infected apps on shady third-party websites that advertise app file downloads. However, that doesn't mean the official app stores are immune to rooting malware.

On October 28, 2021, Lookout Threat Lab found 19 apps infected with the AbstractEmu malware on the Google Play Store, 7 of which were rooted. One of these infected apps racked up 10,000 downloads before it was taken down by Google.

Therefore, it is important to always be on the lookout for malware on your phone, even if it is available on the official app store. The fact that the application appears on the official store does not mean that it is 100% safe.

What does rooting malware do?

After rooting malware gets into your phone, it first gains root access to the phone, then essentially unlocks the entire system for the malware to exploit.

From here, what the malware does depends largely on the intentions of its creator. If a malware developer wants to collect personal information, he can ask the malware to do so. If a malware developer wants to make money,

he can set up a program that displays too many ads.

In fact, once rooting malware gets a foothold on your system, the developers behind can use that entrance to download and install even more malware. And because it has root access, the malware can do it without any additional permissions from you.

The AbstractEmu malware that the article mentioned above even installs a completely new application on the phone, called "Settings Storage". The application itself does not contain malicious code and if you try to open it, it will close and load the default installation application of the operating system.

However, even though it doesn't contain any malicious code by itself, it will sometimes contact developer servers and download malicious code. This is something malware can easily do with root access.

How to avoid downloading rooting malware?

The best defense against rooting malware is to stay vigilant. For malware to be able to attack you, you need to download and install an infected app. Therefore, recognizing where malware-infected apps tend to hide is an important step in protecting yourself from them.

Third-party sites are the most notorious for malware. There are a few websites and app stores that people find trustworthy, but in general, most websites have ulterior motives or don't have the proper security setup to scan uploaded apps.

Therefore, try to maintain the use of official channels if you can. If you must access a third-party application website due to restrictions, make sure you get it from a trusted source.

However, as mentioned earlier, the official app stores are also not completely immune. Luckily, you have a valuable tool in your arsenal for detecting shady apps. Malware on official app stores doesn't last long. Therefore, if you want to stay safe, look for apps that:

1. Been on the app store for a while

2. Has a high number of downloads. These apps are much less likely to contain malware than new apps with low download counts.

These apps often use some sort of method to get downloads as fast as possible. They can disguise themselves as a much-loved app or advertise themselves as a must-have for fans of a hot new movie or game. Don't download these apps blindly; instead, be careful and make sure you don't leave your phone in the hands of malware!

And, of course, there are anti-virus solutions on smartphones. While downloading anti-virus software on mobile phones was once considered unnecessary, smartphone malware has become all too common and should not be taken lightly.

You finished reading the article "**What is rooting malware? What can you do to protect yourself?**" 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.

© 2019 TipsMake.com