5 types of malware on Android

Malware or malware can affect mobile devices as well as computers. A little bit of knowledge and proper precautions can protect you from threats like ransomware and sextortion scam.

Malware or malware can affect mobile devices as well as computers. But don't be too scared! A little bit of knowledge and proper precautions can protect you from threats like ransomware and sextortion scam.

5 types of malware on Android

What is malware (malware)?

Malware is software that has malicious intent. There are many different types of malware, such as viruses, worms, trojans, spyware, adware (adware), etc.

1. Distinguish malware, viruses and Trojan horses

The common point of almost all malware is making money. Depending on the type of malware, the performance of the device may be affected, personal information may be stolen or intruders can access your account. That's just some potential consequences.

Ransomware: Keep your device hostage

Ransomware is a type of malware that "keeps your device for ransom", by locking the device so it cannot be used until you pay the ransom and it has attacked Android devices in 2014.

Svpeng is a combination of ransomware and payment card theft. For Russians (the object Svpeng originally created to target), Svpeng will display a screen to enter credit card details, each time a user accesses Google

Play, then it will send information to the cybercrime gang created it.

For users in the US and UK, it will introduce itself as an FBI, lock the user's device and say there is child pornography on it. After that, the user will have to pay a fine to unlock the device.

Svpeng also checks to see if a banking application has been installed, although it is unclear what it will do with that information.

Russian police arrested the creator of Svpeng in early April 2015, after he stole more than 50 million rubles ($ 930,000) and infested malware with more than 350,000 Android devices.

The application installs without your consent

Do you have any applications that allow you to open links within them without having to access the browser? The page display element for you in that situation is called Webview - and if you are one of 950 million people running Android 4.3 Jellybean or below, you need to know about this vulnerability.

While browsing Webview, you will be vulnerable to Universal Cross-Site Scripting (UXSS). This means that if you accidentally click on a malicious link, an attacker can execute any malicious code that they want through JavaScript - completely ignore the security mechanisms that often protect you. An attacker can use this vulnerability to automatically install any application they want on your device.

Google has no plans to fix this vulnerability in Android 4.3 or below. The best way to avoid being targeted by attackers is to upgrade to the latest Android version as soon as possible or avoid using Webview, by opening a link in a secure browser such as Chrome, Firefox or Dolphin.

Your phone is turned off, right?

Android / PowerOffHijack is malware that enters the device's shutdown process, so it seems to be turned off, but actually works. That way, it can secretly make calls, take photos and do more than that - all without your control.

Unlike the first type of malware discussed in this article, Android / PowerOffHijack affects Android 5.0 and above and requires root access to operate.

As of February 18, about 10,000 devices were infected. So do you need to worry about your device? The answer is not so. Unless you download apps from Chinese app stores, you can at least be safe from this threat.

The hidden application contains malware that does not work

In February, certain Android apps helped users earn more money. A game that requires patience, an IQ test, and a history app, all sounds safe, doesn't it? And you will never think they have problems, if they are still functioning normally for a month before doing anything suspicious, right? However, each of these applications is downloaded more than five million times and has activation code for pop-ups, if you click, it will lead to fake websites, run illegal processes, or catch Download and install the unwanted application.

Filip Chytry of Avast Antivirus showed clues to let you know if you have this type of malware:

Every time you unlock the device, an ad will appear. It is a warning sign of a problem, for example, your device is infected, outdated or filled with pornography. This, of course, is a complete lie.

Google has suspended these applications from Google Play Store, so as long as you don't download them from another source, you'll be fine.

Sextortion Malware

Cyber ??criminals in Korea have created fake social networking profiles of attractive women, to attract people to cybersex, then they extort money by threatening to launch the video on YouTube.

This is where malware invades. Criminals pretend that they encounter audio problems with the selected software (such as Skype) and persuade victims to download the chat application according to their instructions. In fact, this chat app will steal victims' contacts to send to blackmailers. Criminals use contact information to more effectively blackmail, by threatening to share videos with their close friends and family.

Android Installer Hijacking

Nearly 50% of all Android devices are at risk of being attacked by the "Android Installer Hijacking" vulnerability. Simply put, when you download a legitimate application, the installer can be hacked to allow the application you do not want to be installed in the location of that legitimate application. This happens in the background, while you are reviewing the rights of the application you want to install, by setting up a harmless application and installing the following malware or by hiding real permissions. which application requires.

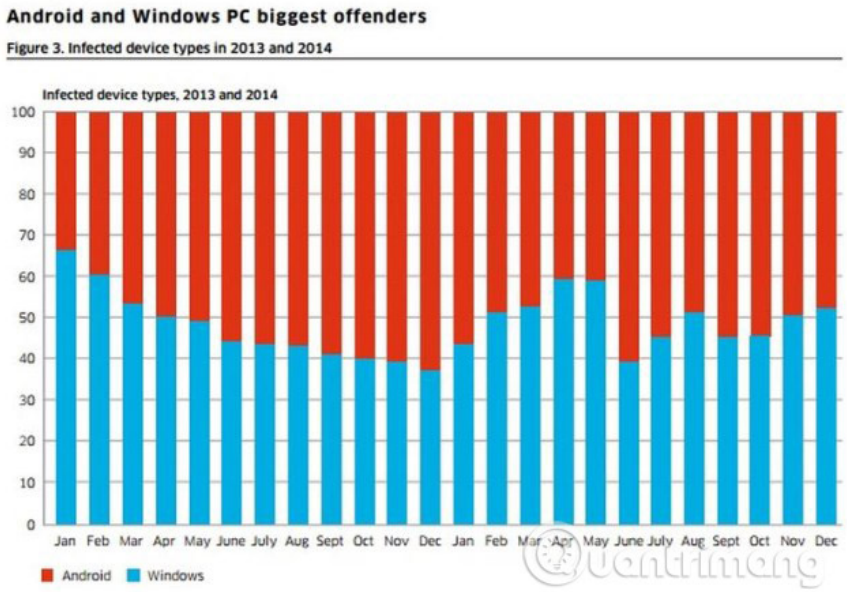
This vulnerability affects third-party application stores, such as the Amazon App Store. Android 4.4 devices become safe with this.

According to Palo Alto Networks, who discovered this vulnerability, if you have affected devices, the best way to avoid accidentally downloading malware, is to install the application only from Google Play Store.

Is malware a big problem?

Alcatel-Lucent conducted a study showing that 16 million mobile devices were attacked by malware in 2014.

Motive Security Labs malware report - H2 2014, reviewed all popular mobile device platforms, found that malware-infected Android devices were equal to the amount of Windows laptops infected, with the infection rate between Android devices and Windows is 50/50.



According to Verizon, malware on mobile devices is not a big deal. From Verizon's 2015 data breach investigation report with the title, 'I Got 99 Problems and Mobile Malware Isn't Even 1% of Them':

'On average 0.03% of smartphones every week - out of tens of millions of mobile devices on Verizon's network - have been infected with' high-end 'malware.

Verizon considers most malware infected on Android devices as mediocre "fake jewelry", and others only waste resources but do not cause significant damage. Does that mean we don't need to worry about malware on our mobile device? Not really.

Users cannot ignore mobile devices because they are very vulnerable to attack. Cybercriminals are using many other methods to break into our system, so we should focus on the methods that are currently being discovered.

You still need to pay attention to the risks to keep yourself safe. Malware may be a small problem today, but research from Lookout (a mobile security company) shows that malware on mobile devices is increasing, especially ransomware.

Keep your Android device safe

1. Top best antivirus application for Android phones

When you hear 97% of malware on mobile devices is available on Android (according to a F-Secure report), you will definitely think Android devices are not safe. Just remember that as long as you stick with official applications from Google Play Store, you won't encounter any malicious software. As shown here, malware exists and thrives in unofficial app stores and is largely unregulated.

Download only the app when there is a good reason to believe it is safe, such as if you know the developer well, or if it is a copy of the official application stored by a trusted source. .

Scan and delete malware

Malwarebytes Anti-Malware has released a version for Android that can help you scan and delete malware on your Android device.

Link download: https://download.com.vn/android/malwarebytes-anti-malware-for-android/download

There are many other threats that are likely to affect Android devices more. It is important not to be caught off guard, by:

1. Learn the signs of malware infection on Android.
2. Do not download anything unless you know it's a trustworthy source.

Have you ever encountered malware on your smartphone? Do you worry about malware? And how do you protect your device? Let us know in the comments section below!

See more:

1. Risks from malware and how to prevent it
2. Remove root malware (malware) on Windows 10 computers
3. 9 things to do when detecting a computer infected with malware