How dangerous is Ransomware on smartphones?

Ransomware can also spread to smartphones and this can have equally serious consequences.

Ransomware is an undeniable threat to businesses and individuals, but we often see it infecting PCs. However, ransomware can also spread to smartphones, and this can have equally serious consequences. So how does smartphone ransomware work and how dangerous is it?

What is Ransomware on Smartphones?

Smartphone ransomware, also known as mobile ransomware, specifically targets smartphones rather than PCs. Many people forget that smartphones are vulnerable to malware, and ransomware is no exception.

Like PC ransomware, smartphone ransomware is used with the goal of holding your data hostage or stealing it outright. When ransomware infects a device, it typically encrypts the data stored on it. This can also prevent you from using your phone and changing your login PIN, leaving you completely unable to do anything.

Both iPhones and Android devices can be infected with smartphone ransomware. However, depending on the nature of the particular ransomware being used, one operating system may be more at risk than another.

Types of ransomware on smartphones

There is no shortage of portable ransomware programs that have been used in previous attacks. This long list has a few notable examples, including:

1. Cryptolocker.

2. ScarPackage.
3. DoubleLocker.
4. LeakerLocker.
5. LockerPin.
6. Worm.Koler.

Each of these programs works differently. For instance, Doublelocker only targets Android devices, while Cryptolocker infects both iPhones and Android phones. However, Cryptolocker is no longer in use and was discontinued in 2014.

At the same time, another form of ransomware, called ScarePackage, infected more than 900,000 phones in a one-month period.

Ransomware LeakerLocker also caused a lot of concern in 2017 when it was found to infect Android devices through the Google Play Store. This is a particularly interesting form of portable ransomware because it doesn't encrypt any files after infection. Instead, LeakerLocker locks your phone and then sets out to collect all kinds of valuable data, such as emails, social media messages, and browser data.

Android devices are more susceptible to all forms of malware than iPhones.

Why are smartphones targeted by ransomware?

There is a large amount of data stored on smartphones, including apps, contacts, photos, emails, saved passwords, etc. This makes smartphones a prime target for cybercriminals, which is why malware infections are increasing on these devices.

Spyware, adware, viruses and ransomware have all been used to infect smartphones and steal data, be it payment information, text messages or even browser activity.

Even if you obey the attacker's request and regain control of your smartphone, there is no way to know if they stole certain data during the infection. Of course, hackers are not ethical, so paying the ransom doesn't guarantee you'll get your data back.

Signs of smartphones infected with ransomware

Unlike many other forms of malware, ransomware creators often want the attention of their victims. This is because the attackers have to ask the victim for a ransom in order to regain control of the device along with their files.

Ransomware creators tend to issue a warning on the home screen, such as a laptop screen, indicating that your device is infected. On your phone, the lock screen or home screen may have a background change to notify you that you've been the target of a ransomware attack. Hackers often list their requirements in this notice, as well as how long you must comply before they steal or make your encrypted or stolen data public.

However, some mobile ransomware is used to steal data without being detected. In such a case, your sensitive information could be accessed and stolen without your knowledge. This is not typical for ransomware.

There are decryption tools available online for many forms of ransomware, especially those with a simpler design. On the other hand, if the ransomware hasn't locked your phone and is in the form of a malicious app, be sure to remove it immediately.