The Joker Malware

Android was notoriously famous for potentially being open to various malwares and viruses due to its inherent nature of being open source and allowing the installation of applications from external sources i.e. which are often not verified by the Google play store. However, in certain instances the malwares has been known to creep in through various applications. One such malware is the Infamous 'Joker'.

What is Joker Malware

The Joker Malware was specifically designed to stay under the radar of Google's detection and verification process which is designed for the apps. It goes without saying that it is extremely difficult or almost impossible for iOS devices because of their extremely high security measures and verification process.

The malware is designed to hide within basic utility or function apps and then creep into devices through the permission of access granted by the individual and then eventually capture text messages and contact lists which provide the personal information to the potential wrongdoers who end up committing identity theft, fraud or other hacks and crimes.

It has also been reported that the malware can actually sign up the infected device or subscribe to some premium services by using the saved information and collecting information from the received OTPs , as authentication of transactions, which then eventually gets billed to the user of that device, without their knowledge.

The vulnerable groups and known apps

Google does remove the apps from the play store as soon as they are detected but they do keep popping up through minor fixes and changes in the code. The apps and websites known to embed the code of this malware include:

- All Good PDF Scanner
- Mint Leaf Message-Your Private Message
- Unique Keyboard – Fancy Fonts & Free Emoticons
- Tangram App Lock
- Direct Messenger
- Private SMS

National Commission for Women, India

CyberPeace Foundation

Autobot Infosec

- One Sentence Translator – Multifunctional Translator
- Style Photo Collage
- Meticulous Scanner
- Desire Translate
- Talent Photo Editor – Blur focus
- Care Message
- Part Message
- Paper Doc Scanner
- Blue Scanner
- Hummingbird PDF Converter – Photo to PDF
- All Good PDF Scanner

- Com.imagecompress.android
- Com.relax.relaxation.androidsms
- Com.cheery.message.sendsms
- Com.peason.lovinglovemessage
- Com.contact.withme.texts
- Com.hmvoice.friendsms
- Com.file.recovefiles
- Com.LPlocker.lockapps
- Com.remindme.alram
- Com.training.memorygame
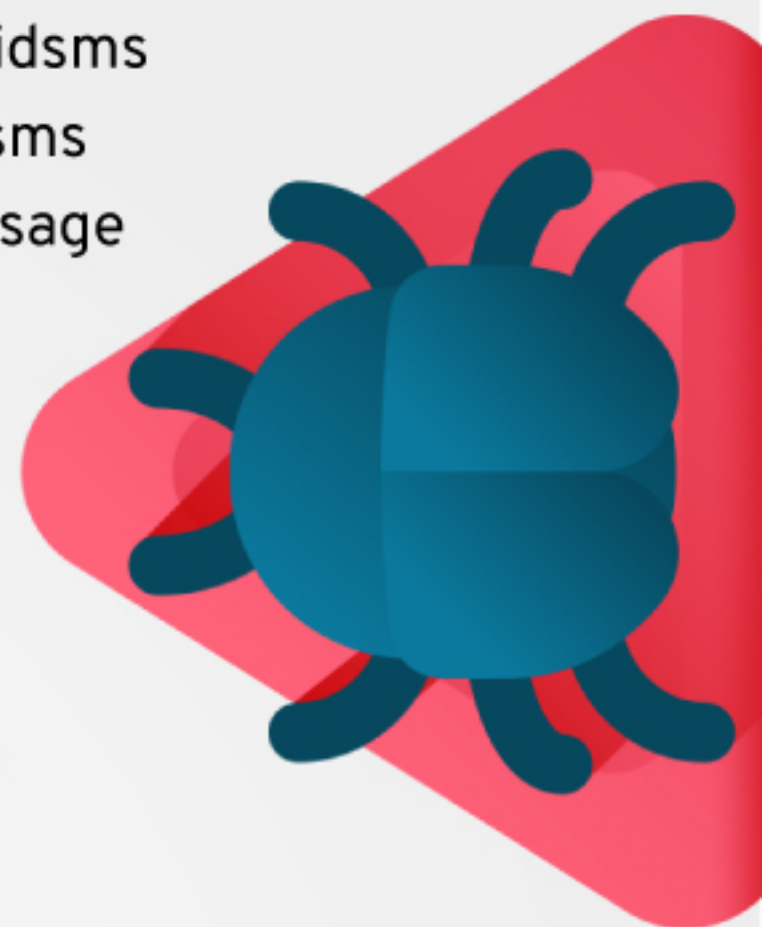
While the apps are constantly getting removed and the bugs allowing the malware to exist are updated through security fixes and updates, there exists a large majority of people who are either unaware of the potentially dangerous nature of these apps hence never delete the or install an antivirus or even update their phone after the release of security updates. These people will be the most vulnerable group as they will never realise the problem until they actually suffer the consequence.

Advisories against Joker Malware

Update the android devices with the latest security updates as soon as they are released by google. One will receive the notification about the update as soon as it is released. While downloading utility apps, always look further into the developer and app details to find any red flags. such as the origin, other apps which they have created, the rating of the app on the store, responses to the reviews etc. An app with an unusually low review to downloads ratio or a developer who is never heard should raise red flags before downloading any application.

The basic functionality apps like PDF viewers and converters and scanners are a lot of the time present in the smartphones, one doesn't always require to download them in a new device. Never download an application with an unknown source or outside of Google play store as these apps are not vetted or don't follow the Google Play store policies which is harmful for the device.

In latest versions of android, one can disallow the access to various data points in a device such as access to text messages or contact list. For example, for a utility app designed to open pdf files, access to text messages or contact lists can probably be avoided. Never download free anti-virus software as it increases bloatware and can often cause more harm than benefit. Look for affordable antivirus solutions which are often bundled with VPNs at affordable prices.

National Commission for Women, India   CyberPeace Foundation   Autobot Infosec