Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 216

ACG-CSB 082521216

Reference Number ACG-CSB 082521216

UNDERSTANDING THE RISK OF JOKER VIRUS ON ANDROID DEVICES

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and not classified as **"Restricted"** pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

The return of the '**Joker**' virus, which attacks Android devices and hides itself in various applications on the Google Play Store. This malware is capable of subscribing the user to payment services without their authorization and emptying their bank accounts without them noticing.

This malicious program has been detected in eight Play Store applications that Google has suppressed," say the Belgian authorities in a statement published this Friday on their website.

The '**Joker**' malware became famous in 2017 for infecting and robbing its victims by hiding in different applications. Since then, the Google Play Store defense systems have removed around 1,700 apps with the '**Joker**' malware before they were downloaded by users.

The '**Joker**' Trojan virus belongs to a family of malware known as Bread, whose objective is to hack cell phone bills and authorize operations without the user's consent.

Researchers from the cybersecurity company Quick Heal Security Lab, cited in the statement, explain that this virus can enter text messages, contacts and other information on the infected smartphone.

What makes this malware more dangerous is its ability to subscribe the affected Android user to paid services, usually Premium or the most expensive version, without their prior authorization.

In the beginning, apps infected with '**Joker**' or another Malware from this family carried out fraud via SMS, but then began to attack online payments. These two techniques take advantage of the integration of telephone operators with vendors, to facilitate the payment of services with the mobile bill. Both require verification of the

device, but not the user, thus they manage to automate payments without requiring any user interaction.

In fact, it is very common for those affected by 'Joker' to become aware of the theft until they review their account statement in detail. This is because the bank does not suspect an apparently 'normal' subscription and, generally, the charges are so small that they are not detected as unusual movements, so they do not even send a usage alert to the account holder.

The cybersecurity company Zscaler, cited by La Razón , made public the names of 16 other apps that, according to their analysis, also contain this malicious code:

- Private SMS
- Hummingbird PDF Converter - Photo to PDF
- Style Photo Collage
- Talent Photo Editor - Blur focus
- Paper Doc Scanner
- All Good PDF Scanner
- Care Message
- Part Message
- Blue Scanner
- Direct Messenger
- One Sentence Translator - Multifunctional Translator
- Mint Leaf Message-Your Private Message
- Unique Keyboard - Fancy Fonts & Free Emoticons
- Tangram App Lock
- Desire Translate
- Meticulous Scanner

Of course, the recommendation for Android users is to check if they have any of these apps installed on their smartphone and delete them immediately, since the fact that they are deleted from the Google Play Store does not imply automatic uninstallation from the computers where they were downloaded.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of **JOKER VIRUS:**

- Do not download any untrusted and unverified apps in Google Play store.

- Do not associate bank credit cards on Google play and any online payment system. If you have to buy an application or subscription online, use pre-paid credit cards such as PayMaya or Gcash wherein you can load only the exact amount that you need to pay. You will not worry about the hacker stealing your bank money since it is not signed in to any online account.

For additional information, please refer to the following websites:

- https://www.entrepreneur.com/article/381038
- https://www.androidheadlines.com/2021/08/joker-virus-apps.html
- https://www.indiatimes.com/technology/news/joker-virus-android-apps-547837.html

POINT OF CONTACT

Please contact **PMAJ ROVELITA ROBIÑOS AGLIPAY** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723 0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.