TLP: White[1]

Advisory- Android Ransomware known as MalLocker.B

Dear Constituents,

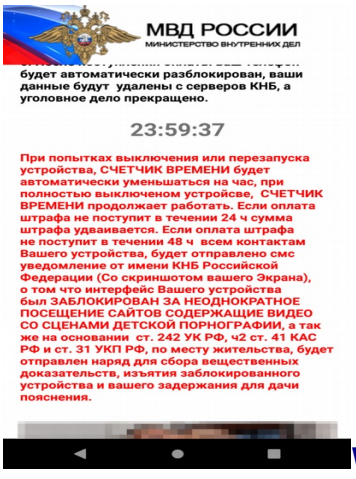
Security researchers has recently detected a ransomware known as MalLocker.B that is hidden inside Android apps. It appears to be affecting most android devices, the ransomware itself abuses the functionality of the phone and it does not encrypt files as we usually know about Ransomware, but it prevents the user from accessing his/her mobile phone.

How it Works

This ransomware uses 2 techniques that take advantage of the following components on Android and showing ransom note:

- The “call” notification, among several categories of notifications that Android supports, which requires immediate user attention. This is the function that activates for incoming call to show details of the caller. MalLocker.B uses it to show a window that covers the entire area of the screen with details about the incoming caller.
- The “onUserLeaveHint()” callback method of the Android Activity this is when users want to push an app into the background and switch to a new app, and it triggers when pressing buttons like Home or Recents. MalLocker.B abuses this function to bring its ransom note back into the foreground and prevent the user from leaving the ransom note for the home screen or another app.

Once it installed, the ransomware takes over the phone's screen and prevents the user from dismissing the ransom note — which is designed to look like a message from local law enforcement telling users they committed a crime and need to pay a fine. *(as shown below is a MalLocker ransom note)*



What to do

1 CERT Tonga adopts the Traffic Light Protocol

- Users are advised to avoid installing Android apps they downloaded from third-party locations such as forums, website ads, or unauthorized third-party app stores.

Reference

- https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransnomware/

Please for more information you can contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga