# LokiBot - bank trojan on Android turns into ransomware when you try to delete it

Security agents have discovered a new bank trojan on Android called LokiBot that turns into extortion code and locks the phone when the user tries to delete its admin rights.

Security agents have discovered a new bank trojan on Android called LokiBot that turns into extortion code and locks the phone when the user tries to delete its admin rights.

This malware is more like a banking trojan than ransomware and is also used primarily for that purpose. Like other banking Trojans on other phones, LokiBot displays fake login screens on popular applications. LokiBot targets mobile banking applications but also targets a number of other applications such as Skype, Outlook or WhatsApp.

## LokiBot is sold online for $ 2,000

Like Svpeng, CryEye, DoubeLocker, ExoBot and some other recent Android malware, LokiBot is sold on hacking forums at a price of $ 2,000 with Bitcoin.

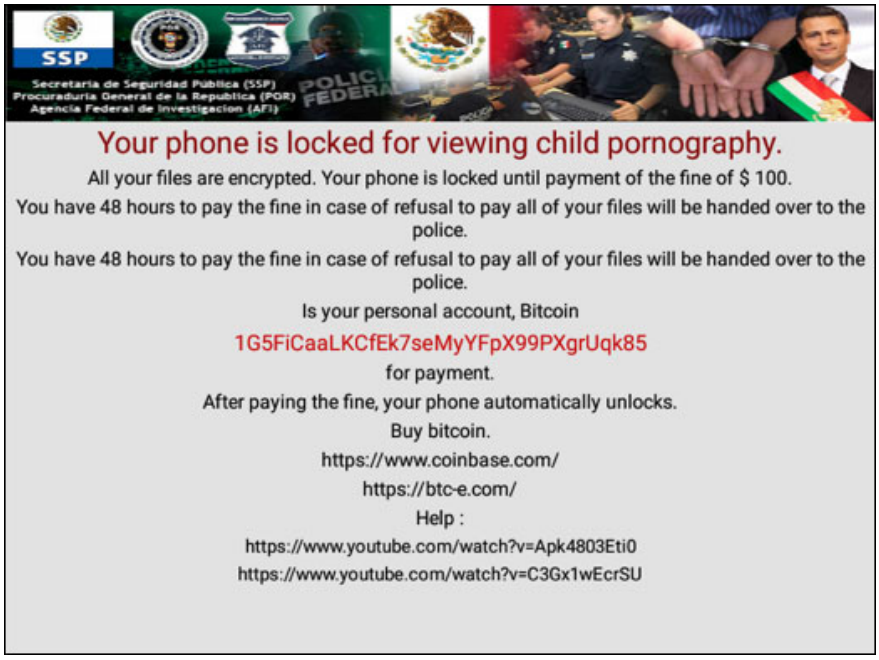
Compared to other bank trojans, LokiBot also has its own features. For new users, it can open mobile browsers and download URLs, set up SOCKS5 proxies to redirect external traffic.

It also automatically text messages back and sends SMS messages to all the victim's contacts, a feature commonly used to send spam to infect new users.

LokiBot also displays fake notifications to trick users into thinking they receive money in their bank accounts and open the banking application. When the user opens the notification, LokiBot will display the phishing screen inserted into the real application.

## LokiBot's behavior failed

This malware works on Android 4.0 and above and needs admin rights, so it will ask during installation. If the user detects a scam and deletes the admin rights, LokiBot will turn into extortion code but luckily, executing when switching to ransomware has an error and cannot encrypt the user file.




*Notice of extortion when LokiBot turns into extortion code*

According to SfyLabs, LokiBot's ransomware Go_Crypt function should have locked the screen and encrypted the file using the AES128 algorithm.

## But the phone is still locked

Although the file is not encrypted, the victim's phone screen is still locked and displays a $ 70 to $ 100 blackmail notice. To unlock you must open in Safe Mode and remove LokiBot.

Although extortion is not the main thing of LokiBot, the guys behind this malicious code still earn a good amount of money when the Bitcoin account has more than 1.5 million dollars.

Two weeks ago, ESET discovered DoubleLocker, ransomware on Android developed from Svpeng bank trojan. Unlike LokiBot, DoubleLocker is an extortion code from where and completely encrypted user files.