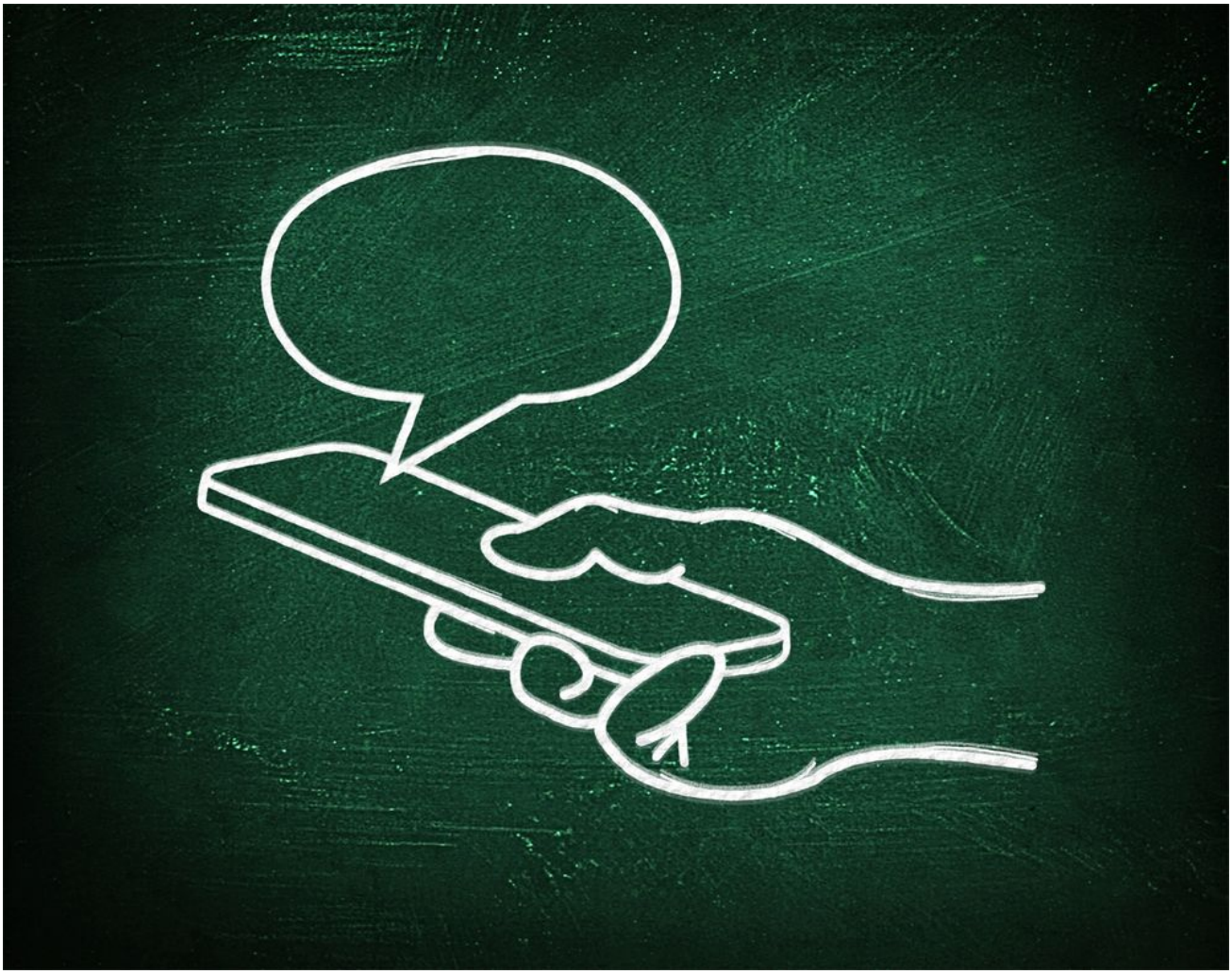
Android SLocker Variant Uses Coronavirus Scare to Take Android Hostage

Anti-Malware Research
4 min read

Silviu STAHIE
May 04, 2020



The coronavirus pandemic is an opportunity for criminals who try to take advantage of people's thirst for information. Unfortunately, Android users can fall prey to malware attacks using the COVID-19 cover, especially if they sideload apps by circumventing the installation process through the official Play Store.

Users are always facing risks when using technology, especially when it's connected to the Internet. One of the ways to increase your possible exposure to Android malware is to install apps outside of regular vendor-endorsed channels..

And what better way to get people's attention than by using an app that's simply called "About Koronavirus." Users with a voracious appetite consume everything that's coronavirus-related, and in this case, the app would lock the screen of the phone, prompting people to pay for a code to return the control of their device.

While it's not as damaging as ransomware, the average user will have a hard time distinguishing between threats, as the result is the same, and that's getting locked out of your device.

Sideloading is dangerous

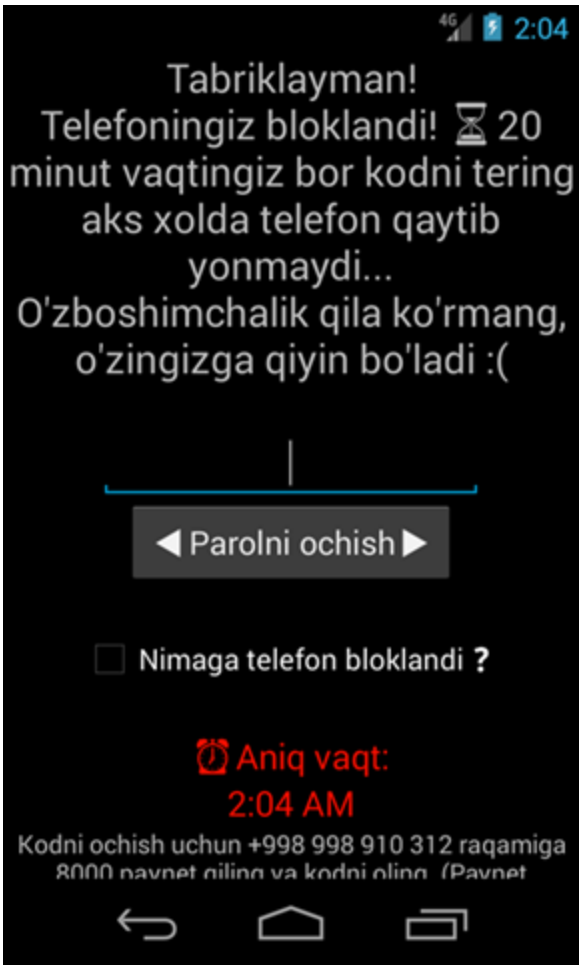
People should generally be wary of installing applications from sources outside of official ecosystems, like the Play Store. It's a sure way of compromising a phone, whether it's through malware designed to lock the phone or to steal personal or financial information.

Bitdefender telemetry picked up a malware variation of a SLocker – a consecrated piece of malware that locks the user out. The phone itself and the data are not affected, but the phone becomes unusable, as the home screen is no longer accessible. It's not a terribly clever piece of software – and it could'nt be much more, given how Android is built – , and there are ways to remove it even after it became active.

The app is called "Koronavirus haqida", which translates into "About Coronavirus." The package name is "com.lololo" (MD5: 476b68a650223780ec73f804e639b7ce) and after the user installs the application and runs it, the screen is locked and displays a simple ransomware message, in the Uzbek language.

To make the threat even more convincing, the attacker says that you can only pay within 20 minutes, after which the phone won't be usable. The good news is that the time limit is false, as there's nothing like that implemented in the code. The bad news is that the phone is genuinely locked, which means that none of the buttons will work, and it survives a system reboot.

Depending on the Android version, the SLocker will behave differently, depending on the level of access permitted by the OS. Newer Android versions, from 8.0 and upwards, won't allow the app to lock the buttons, but users still can't delete the app normally.



This is the rough translation:

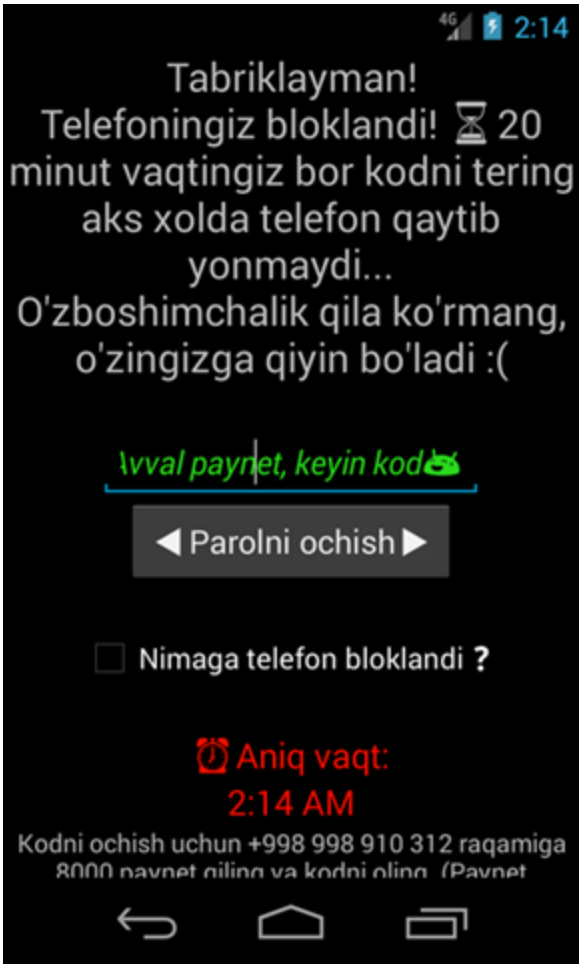
```
Congratulations!
Your phone is blocked! You have 20 minutes to enter the code, otherwise the phone will not turn on again …
Don't see this as an arbitrary message, it will be difficult for you 😕
Unlock password
Exact time
To unlock the code, call +998 998 910 312 Make 8000 paynet and get the code. (Don't ask for the code without Paynet, I won't tell you anyway)
```

If the user enters the wrong code, a simple message is displayed: “Avval paynet, keyin kod 😅“ that translates to “First paynet then code.”

And here comes the strange part, as the code expected by the app is actually the phone number, 998 998 910 312, without the “+” sign. It’s hardcoded into the app, so it’s the same one for anyone foolish enough to install the malware.

Just unlocking the phone by entering the right code doesn’t remove the application. It will continue to run in the memory until it’s removed. If the user kills the app from memory and reruns it, the phone will be locked once more.

You will also notice a checkbox, with the text “Nimaga telefon blocklandi?”, translating to “Why is the phone blocked?”. When the checkbox is selected, the following message is shown: “You have installed something prohibited from the internet on your phone. If you do not PayNet within the specified time, your phone will not light up again. ☎ Get the code by dialing + 998 99 891 03 12 for 8000 PayNet sum! “, 0”.



Lessons to be learned

Once the user runs the malware and locks the phone, it can only be removed via the Android Debug Bridge (adb) or Safe Mode. If the correct code is entered and the screen unlocked, the app can be removed from the OS as well, through the usual methods.

The malware is not as aggressive as others, but the fact that’s trying to make use of the coronavirus scare is likely to help it get more traction.

What’s equally interesting about this SLocker malware is the fact that it’s not entirely original. In fact, it’s most likely a copy of some older versions; it was just adapted to the COVID-19 pandemic.

When we look closer at the file structure, we see there’s an image in “\res\drawable\” named “image_1.png” that has a message in Russian, and not in Uzbek. The likely explanation is that it’s leftover from the previous versions of the screen locker.

The translation “you were blocked for cheating.”

In the past few months, the malware was reported in Ukraine, Russia, numerous countries in Central Asia, including Kazakhstan and Turkmenistan, and parts of India and North Africa.

Various samples with the same package name (Virus or ELOSTORA VIRUS labels), have been identified as well. However, they have no relation to the Coronavirus, but appeared after COVID-19 became a pandemic.

Indicators of compromise:

MD5	First seen on
6e3d57271a1c0e8e79c88d15f3897bab	Nov 30 2019
698aa564ba543d8b0bb247471554672b	Feb 21 2020
1dfc2e6f96727ab1bb37bc5ac303dc62	Mar 09 2020
8fc2e3254eabdfceee843c6bc3367f6c	Mar 09 2020
c89cd578e2a647671ce7254d3fab41dc	Mar 20 2020

TAGS

anti-malware research

AUTHOR

two decades,
ween.