Charger Malware Calls and Raises the Risk on Google Play

By bferrite

Published: 2017-01-24 · Archived: 2026-04-24 02:08:26 UTC

Several weeks ago, Check Point Mobile Threat Prevention detected and quarantined the Android device of an unsuspecting customer employee who downloaded and installed a 0day mobile ransomware from Google Play dubbed "Charger." This incident demonstrates how malware can be a dangerous threat to your business, and how advanced behavioral detection fills mobile security gaps attackers use to penetrate entire networks.

Charger was found embedded in an app called EnergyRescue. The infected app steals contacts and SMS messages from the user's device and asks for admin permissions. If granted, the ransomware locks the device and displays a message demanding payment:

You need to pay for us, otherwise we will sell portion of your personal information on black market every 30 minutes. WE GIVE 100% GUARANTEE THAT ALL FILES WILL RESTORE AFTER WE RECEIVE PAYMENT. WE WILL UNLOCK THE MOBILE DEVICE AND DELETE ALL YOUR DATA FROM OUR SERVER! TURNING OFF YOUR PHONE IS MEANINGLESS, ALL YOUR DATA IS ALREADY STORED ON OUR SERVERS! WE STILL CAN SELLING IT FOR SPAM, FAKE, BANK CRIME etc… We collect and download all of your personal data. All information about your social networks, Bank accounts, Credit Cards. We collect all data about your friends and family.

The ransom demand for 0.2 Bitcoins (roughly $180) is a much higher ransom demand than has been seen in mobile ransomware so far. By comparison, the DataLust ransomware demanded merely $15. Payments are made to a specific Bitcoin account, but we haven't identified any payments so far.

Adware commonly found on Play collects profits from ad networks, but mobile ransomware inflicts direct harm to users. Like FakeDefender and DataLust, Charger could be an indicator of a wider effort by mobile malware developers to catch up with their PC ransomware cousins.

Similar to other malware seen in the past, Charger checks the local settings of the device and does not run its malicious logic if the device is located in Ukraine, Russia, or Belarus. This is likely done to keep the developers from being prosecuted in their own countries or being extradited between countries.

Most malware found on Google Play contains only a dropper that later downloads the real malicious components to the device. Charger, however, uses a heavy packing approach which it harder for the malware to stay hidden, so it must compensate with other means. The developers of Charger gave it everything they had to boost its evasion capabilities and so it could stay hidden on Google Play for as long as possible.

The malware uses several advanced techniques to hide its real intentions and makes it harder to detect.

- It encodes strings into binary arrays, making it hard to inspect them.

- It loads code from encrypted resources dynamically, which most detection engines cannot penetrate and inspect. The dynamically-loaded code is also flooded with meaningless commands that mask the actual commands passing through.
- It checks whether it is being run in an emulator before it starts its malicious activity. PC malware first introduced this technique which is becoming a trend in mobile malware having been adopted by several malware families including Dendroid.

Emulator and location conditions for the malware's activity

Check Point Mobile Threat Prevention customers are protected from Charger and similar malware.

Check Point's Analysis and Response Team (ART) disclosed the finding to Android's Security team who took the appropriate security steps to remove the infected app and added the malware to Android's built-in protection mechanisms.

Charger SHA256 hash: 58eb6c368e129b17559bdeacb3aed4d9a5d3596f774cf5ed3fdcf51775232ba0
