Updated: Mobile security firm claims Xiaomi Mi4 carries pre-installed malware - MEDIANAMA

By Riddhi Mukherjee

Published: 2015-03-09 · Archived: 2026-04-05 19:53:48 UTC

Update: Xiaomi's response to Medianama:

> We have concluded our investigation on this topic — the device Bluebox obtained is 100% proven to be a counterfeit product purchased through an unofficial channel on the streets in China. It is therefore not an original Xiaomi product and it is not running official Xiaomi software, as Bluebox has also confirmed in their updated blog post.
> 1) Hardware: Xiaomi hardware experts have looked at the internal device photos provided to us by Bluebox and confirmed that the physical hardware is markedly different from our original Mi 4.
> 2) IMEI number: Xiaomi after-sales team has confirmed that the IMEI on the device from Bluebox is a cloned IMEI number which has been previously used on other counterfeit Xiaomi devices in China.
> 3) Software: Xiaomi MIUI team has confirmed that the software installed on the device from Bluebox

> is not an official Xiaomi MIUI build as our devices do not come rooted and do not have any malware pre-installed.
> As this device is not an original Xiaomi product, and not running an official Xiaomi MIUI software build, Bluebox's findings are completely inaccurate and not representative of Xiaomi devices. We believe Bluebox jumped to a conclusion too quickly without a fully comprehensive investigation (for example, they did not initially follow our published hardware verification process correctly due to language barrier) and their attempts to contact Xiaomi were inadequate, considering the severity of their accusations.

The company also mentioned that it "takes all necessary measures to crack down on the manufacturers of fake devices or anyone who tampers with our software." Xiaomi also informed that it hasn't yet received any meaningful reports of counterfeit Mi phones outside of China. However, keeping in mind the possibility it is working on an English version of their verification app (that certifies the authenticity of Mi hardware).

Earlier: San Francisco-based mobile security company Bluebox has claimed that it found pre-installed malware, adware and spyware in Xiaomi Mi4. The company claimed that it found an app called Yt Service pre-installed in the Mi4 it tested, which installs "an adware service called DarthPusher that delivers ads to the device among other things."

Bluebox mentions that this app disguises the adware to look like it's a Google service and "tricks users' to think its a safe app. Besides Yt Service, some of the other suspicious apps Bluebox found pre-installed on the Mi4 included PhoneGuardService classified as a Trojan, AppStats classified as riskware and SMSreg classified as malware.

It's worth noting that Xiaomi's VP International Hugo Barra informed Bluebox that:

> We are certain the device that Bluebox tested is not using a standard MIUI ROM, as our factory ROM and OTA ROM builds are never rooted and we don't pre-install services such as YT Service, PhoneGuardService, AppStats etc. Bluebox could have purchased a phone that has been tampered with, as they bought it via a physical retailer in China. Xiaomi does not sell phones via third-party retailers in China, only via our official online channels and selected carrier stores.

Subsequently, Xiaomi conducted "in-depth testing" on the device Bluebox had based its report and informed that the device is indeed a counterfeit and a "very good one at that." In fact, it seems the counterfeit device was initially able to pass Xiaomi's verification app.

The question seems to be if the counterfeit is really that good and it took a mobile security company and the manufacturer a few days to verify if it's authentic or not, **what are consumers supposed to do?**

We've written to Xiaomi and will update once we hear back.

The Xiaomi Mi4 went on sale last month in India. In December last year, Xiaomi's India head Manu Kumar Jain had claimed that they had sold one million handsets in India since its launch in July. It's also worth noting that Xiaomi is working towards launching its own e-commerce store in India as well. Barra had confirmed this to Livemint in November last year, and in February Jain told PTI that the process will take "anywhere between three to nine months."

Security and privacy issues with Xiaomi

In August last year, security firm F-Secure had found that Xiaomi's MIUI-based smartphones were sending user data – including text messages, contacts, phone numbers, ISP's name, IMEI number and other details – back to Xiaomi's server, whether users signed up for the company's cloud-based services or not. F-Secure also found that this data wasn't encrypted.

At the time, the Chinese smartphone maker had for the first time acknowledged that its phones were sending text messages back to its servers. However, the company said that this was being done to test whether text messages sent out by a user could possibly be sent over using data connection instead of carrier's SMS gateway to save user's money. Barra also mentioned that this option is turned on by default. More on how Xiaomi deals with user's data here.

A couple of months later, the Indian Air Force issued an alert note to its staff and their family members that warned them against using any Xiaomi products, saying that the company was stealing not just their phone numbers and IMEI (device identifier) number, but was also accessing their phone calls and personal text messages. At the time, Barra told Medianama that they do not collect any information without user permission. "Users will always be notified beforehand in situations when we require your personal information, and will have to approve the request." He also mentioned that they are also migrating their services and corresponding data for Indian users from their Beijing data centers to Amazon AWS data centers in Singapore and USA, which is expected to be fully complete by the end of this year. The company also plans to setup a local data center in India in 2015. More on that here.

For You

- Read Reasoned by Nikhil Pahwa: How AI is changing our world
- Sign up for MediaNama's Daily Newsletter to receive regular updates
- Sponsor a MediaNama Event

Post navigation

National Payments Corporation of India (NPCI) has linked 15 crore bank accounts with their Aadhar numbers under the Pradhan Mantri Jan…

Facebook last week started rolling out changes which could affect businesses which measure their success by the number of likes…
