Why Did Chinese Spyware Linger in U.S. Phones?

By Jeremy Kirk

Archived: 2026-04-05 22:43:55 UTC

Data Privacy , Enterprise Mobility Management / BYOD , Governance & Risk Management

Code Sent Call Logs, Texts and More to Shanghai (jeremy_kirk) • November 16, 2016

In what's being chalked up as an apparent mistake, more than 120,000 Android phones sold in the U.S. were shipped with spying code that sent text messages, call logs and other sensitive data to a server in Shanghai.

See Also: ZTNA Buyer's Guide

The New York Times reported on Nov. 15 that Kryptowire, a mobile enterprise security company, discovered the code on a lower-end smartphone made by BLU Products of Doral, Fla. The phones are sold at Best Buy and Amazon.com, among other retail outlets.

Kryptowire says the code, which it found on a BLU R1 HD devices, transmitted fine-grained location information and allowed for the remote installation of other apps. Text message and call logs were transmitted every 72 hours to the Shanghai server, and once a day for other personally identifiable data, the company says.

It turns out, however, that other security researchers noticed suspicious and faulty code on BLU devices as early as March 2015, and it has taken nearly that long to remove it from the company's devices.

The finding, in part, shows the risk that can come in opting for less expensive smartphones, whose manufacturers may not diligently fix security vulnerabilities. It's also raising eyebrows because of the connection with China,

which has frequently sparred with the U.S. over cyber espionage.

BLU Products has now updated its phones to remove the spying code, which most likely would have never been detected by regular users. The code never informed phone users that it was collecting that data, a behavior uniformly viewed by many as a serious security concern.

The developer of the code, Shanghai Adups Technology Co., has apologized, contending that the code was intended for another one of its clients who requested better blocking of junk text messages and marketing calls.

Vulnerabilities Reported

BLU Products, founded in 2009, makes lower-end Android-powered smartphones that sell for as little as $50 on Amazon. Like many original equipment manufacturers, it uses software components from other developers.

The company uses a type of software from Adups that's nicknamed FOTA, short for firmware over-the-air. The software manages the delivery of firmware updates over-the-air, the term used for transmission via a mobile network. Firmware is low-level code deep in an operating system that often has high access privileges, so it's critical that it's verified and contains no software vulnerabilities.

Long before Kryptowire's announcement, Tim Strazzere, a mobile security researcher with RedNaga Security, contacted BLU Products in March 2015 after he found two vulnerabilities that could be traced to Adup's code. Those vulnerabilities could have enabled someone to gain broad access to an Android device.

Strazzere's colleague, Jon Sawyer, suggested on Twitter that the vulnerabilities might have not been there by mistake, but rather included as intentionally coded backdoors. He posted a tweet to *The New York Times* report, sarcastically writing, "If only two people had called this company out for their backdoors several times over the last few years."

Strazzere's experience in trying to contact both vendors last year is typical of the frustrations frequently faced by security researchers.

"I tried reaching out to Adups and never heard back," Strazzere tells Information Security Media Group. "BLU said they had no security department when I emailed them."

Strazzere says he also failed to reach MediaTek, a Taiwanese fabless semiconductor manufacturer whose chipsets that powered BLU phones also contained Adups software. To their credit, both Google and Amazon appear to have put pressure on device manufacturers to fix their devices when flaws are found, Strazzere says.

For Google, Android security issues - even if not in the core operating code - are a reputation threat, and for Amazon, a product quality issue. But devices sold outside of Amazon "might not have ever seen fixes," he says.

Officials at BLU couldn't be immediately reached for comment.

Attitude Change

The disinterest in the issues appears to have changed with *The New York Times* report, which lit a fire underneath Adups and BLU.

Adups addressed the issue in a Nov. 16 news release, writing that some products made by BLU were updated in June with a version of its FOTA that had actually been intended for other clients who had requested an ability to stop text spam.

That version flags messages "containing certain language associated with junk texts and flags numbers associated with junk calls and not in a user's contacts," the company says.

Manufacturers should be keeping close tabs on what software ends up on their devices. But it would appear that BLU only took action after Kryptowire notified it along with Google, Adups and Amazon.

"When BLU raised objections, Adups took immediate measures to disable that functionality on BLU phones," Adups says.

The greater worry is that these situations may sometimes not be simple mistakes. Security experts have long warned of the ability of advanced adversaries to subvert hardware and software supply chains. Also, the software vulnerabilities pointed out in the FOTA software by Strazzere in 2015 could have been taken advantage of by cybercriminals looking to steal bank account details or execute other frauds.

Strazzere advises that consumers should look at the pedigree of mobile manufacturers and take a close look at their security track record before making a decision on what device to buy.

"In the end, the consumer needs to vote with their wallet," he says.
