The New York Times

# *Secret Backdoor in Some U.S. Phones Sent Data to China, Analysts Say*

**By MATT APUZZO and MICHAEL S. SCHMIDT** NOV. 15, 2016

Security contractors recently discovered preinstalled software in some Android phones that monitors where users go, whom they talk to and what they write in text messages. Credit Emilio Morenatti/Associated Press

WASHINGTON — For about $50, you can get a smartphone with a high-definition display, fast data service and, according to security contractors, a secret feature: a backdoor that sends all your text messages to China every 72 hours.

Security contractors recently discovered preinstalled software in some Android phones that monitors where users go, whom they talk to and what they write in text messages. The American authorities say it is not clear whether this represents secretive data mining for advertising purposes or a Chinese government effort to collect intelligence.

International customers and users of disposable or prepaid phones are the people most affected by the software. But the scope is unclear. The Chinese company that wrote the software, Shanghai Adups Technology Company, says its code runs on more than 700 million phones, cars and other smart devices. One American phone manufacturer, BLU Products, said that 120,000 of its phones had been affected and that it had updated the software to eliminate the feature.

Kryptowire, the security firm that discovered the vulnerability, said the Adups software transmitted the full contents of text messages, contact lists, call logs, location information and other data to a Chinese server. The code comes preinstalled on phones and the surveillance is not disclosed to users, said Tom Karygiannis, a vice president of Kryptowire, which is based in Fairfax, Va. “Even if you wanted to, you wouldn’t have known about it,” he said.

Security experts frequently discover vulnerabilities in consumer electronics, but this case is exceptional. It was not a bug. Rather, Adups intentionally designed the software to help a Chinese phone manufacturer monitor user behavior, according to a document that Adups provided to explain the problem to BLU executives. That version of the software was not intended for American phones, the company said.

“This is a private company that made a mistake,” said Lily Lim, a lawyer in Palo Alto, Calif., who represents Adups.

The episode shows how companies throughout the technology supply chain can compromise privacy, with or without the knowledge of manufacturers or customers. It also offers a look at one way that Chinese companies — and by extension the government — can monitor cellphone behavior. For many years, the Chinese government has used a variety of methods to filter and track internet use and monitor online conversations. It requires technology companies that operate in China to follow strict rules. Ms. Lim said Adups was not affiliated with the Chinese government.

At the heart of the issue is a special type of software, known as firmware, that tells phones how to operate. Adups provides the code that lets companies remotely update their firmware, an important function that is largely unseen by users. Normally, when a phone manufacturer updates its firmware, it tells customers what it is doing and whether it will use any personal information. Even if that is disclosed in long legal disclosures that customers routinely ignore, it is at least disclosed. That did not happen with the Adups software, Kryptowire said.

According to its website, Adups provides software to two of the largest cellphone manufacturers in the world, ZTE and Huawei. Both are based in China.

Samuel Ohev-Zion, the chief executive of the Florida-based BLU Products, said: “It was obviously something that we were not aware of. We moved very quickly to correct it.”

He added that Adups had assured him that all of the information taken from BLU customers had been destroyed.

The software was written at the request of an unidentified Chinese manufacturer that wanted the ability to store call logs, text messages and other data, according to the Adups document. Adups said the Chinese company used the data for customer support.

Ms. Lim said the software was intended to help the Chinese client identify junk text messages and calls. She did not identify the company that requested it and said she did not know how many phones were affected. She said phone companies, not Adups, were

responsible for disclosing privacy policies to users. “Adups was just there to provide functionality that the phone distributor asked for,” she said.

Android phones run software that is developed by Google and distributed free for phone manufacturers to customize. A Google official said the company had told Adups to remove the surveillance ability from phones that run services like the Google Play store. That would not include devices in China, where hundreds of millions of people use Android phones but where Google does not operate because of censorship concerns.

Because Adups has not published a list of affected phones, it is not clear how users can determine whether their phones are vulnerable. “People who have some technical skills could,” Mr. Karygiannis, the Kryptowire vice president, said. “But the average consumer? No.”

Ms. Lim said she did not know how customers could determine whether they were affected.

Adups also provides what it calls “big data” services to help companies study their customers, “to know better about them, about what they like and what they use and there they come from and what they prefer to provide better service,” according to its website.

Kryptowire discovered the problem through a combination of happenstance and curiosity. A researcher there bought an inexpensive phone, the BLU R1 HD, for a trip overseas. While setting up the phone, he noticed unusual network activity, Mr. Karygiannis said. Over the next week, analysts noticed that the phone was transmitting text messages to a server in Shanghai and was registered to Adups, according to a Kryptowire report.

Kryptowire took its findings to the United States government. It plans to make its report public as early as Tuesday.

Marsha Catron, a spokeswoman for the Department of Homeland Security, said the agency “was recently made aware of the concerns discovered by Kryptowire and is working with our public and private sector partners to identify appropriate mitigation strategies.”

Kryptowire is a Homeland Security contractor but analyzed the BLU phone independent of that contract.

Mr. Ohev-Zion, the BLU chief executive, said he was confident that the problem had been resolved for his customers. “Today there is no BLU device that is collecting that information,” he said.

http://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html?smid=li-share&_r=2