New American

Written by **Joe Wolverton, II, J.D.** on January 10, 2020

Federally Subsidized Smartphones Contain Chinese Spyware

https://media.blubrry.com/1462062/mcdn.podbean.com/mf/web/ra9txm/Federally_Subsidized_Smartphones_Contain_Chinese_Spyware.mp3
Podcast: Play in new window | Download ()
Subscribe: Android | RSS | More

Smartphones being given by the federal government to low-income people have Chinese spyware installed, spyware that can't be removed and that gives agents of Beijing considerable control over those subsidized phones.

According to researchers quoted in various media reports of the discovery of the malware, the Android OS devices given to people participating in the federally funded and FCC-managed Lifeline Assistance program are pre-loaded with applications that give the Chinese access to private data, including contacts and texts, and that allow the company that developed one of the apps to remotely download additional apps to the phone without user participation.

The origin of the "free phones" for welfare recipients was reported by *The New American* in 2011:

> Those who actually have to pay for their telephone service may have noticed a Universal Service Fund charge on their monthly bills. Mandated by the Telecommunications Act of 1996, the fund consists of money extorted from all telecommunications providers — currently 14.4 percent of each company's interstate and international end-user revenues (adjusted quarterly by the Federal Communications Commission). The companies, in turn, pass on that cost to their customers, who end up paying more for telephone service than they otherwise would.

The money collected from the Universal Service Fund charge is used to fund the Lifeline Assistance program.

Regarding the privacy vulnerability of the government-funded phones, *Forbes* reported:

> The affected device is a UMX phone shipped by Assurance Wireless and one of the preinstalled malware, according to MalwareBytes senior analyst Nathan Collier, is the creation of a Chinese entity known as Adups. Though the tool looks and operates as a Wireless Update program, it's capable of auto-installing apps without any user consent, which it starts doing immediately, according to a MalwareBytes analysis of a device, shared with *Forbes* ahead of publication. Adups hadn't responded to a request for comment at the time of publication.
>
> "This opens the potential for malware to unknowingly be installed in a future update to any of the apps added by Wireless Update at any time," Collier wrote in a blog post published Thursday.
>
> Historically Adups tools have been caught siphoning off private data from phones, including the full-body of text messages, contact lists and call histories with full telephone numbers.

Assurance Wireless is a division of Virgin Mobile and has of yet not commented on the story.

Another app pre-installed on the UMX phones is the Settings app. The Settings app is critical to the function of the phone and as such cannot be removed without rendering the phone useless. Unlike other phones' native settings apps, the UMX Settings app — developed by the Chinese — grants the developer the ability to remotely install hidden ads onto the phone without user permission.

Samsung phones seem particularly prone to being programmed with apps controlled by the government of China. As reported by The Verge:

> Using packet analysis tools on a Galaxy S10, the author discovered some strange traffic coming out of Device Care's storage scanner, which looks for junk files that can be deleted to free up space. That scanner was sending data back to Chinese domains — and because storage scanners generally need access to all of the files on your computer, the data could include almost anything.

Unlike the UMX phones, the Galaxy S10 is available for sale to anyone and is not confined to those receiving their phones and service from government subsidies. This puts everyone who owns the S10 — which also runs on the Android operating system — at risk of having the phone manipulated by agents of the government of China.

Again, from The Verge:

> The scanner utility was made in collaboration with Qihoo 360, a Chinese security company that has occasionally made headlines for complying with national censorship directives. But it wasn't clear from the scan which data was being sent back to Qihoo and why, which led the Redditor to worry about spyware. And since the app was built into Samsung's operating system, there is no way for concerned users to remove it.

For its part, Samsung issued a statement promoting its careful protection of users' data and privacy and claiming that the information being collected by the Device Care storage scanner on Galaxy S10 smartphones "is fully managed by Samsung's device care solution."

Regarding the Chinese software pre-installed on the Galaxy S10, the ancient maxim of caveat emptor seems apt. The ubiquity of smartphones and the vulnerability of data stored locally and in the cloud makes owning and using a smartphone a risk that every user of such a device knows or should know that he is running.

In the case of the UMX smartphone being sent to people participating in the federal government's Lifeline Assistance program, users don't have a choice of which device they receive.

Some consider such a restriction to be unfair and yet another example of the poor being penalized for their poverty.

For example, the *Forbes* article closes with the following question: "But the case in the U.S. has another element in that low-income folk who have been endangered. The question worth asking is: Is privacy only for the rich?"

While persecuting a person for his poverty is certainly immoral and indefensible, there is a way to avoid allowing the Chinese communist regime to have access to and control of data stored on the smartphones of more than seven million participants in the Lifeline Assurance program's subsidized cell service.

Abolish the program.

The entirety of power granted to the federal government is set forth in the U.S. Constitution. There is no provision in that document that gives the federal government authority to tax phone company customers and use the money thus collected to provide cellphones and cellular service to people at low or no price.

No government-funded phones, no Chinese spyware stealing data stored by people on government-funded phones.

As with so many other "problems," the solution is enforcement of the enumerated powers of the U.S. Constitution.

Image: Screenshot of a U.S. Cellular ad