US Government-funded Android phones come preinstalled with unremovable malware

reader comments

85 with 66 posters participating, including story author

Share this story

An Android phone subsidized by the US government for low-income users comes preinstalled with malware that can’t be removed without making the device cease to work, researchers reported on Thursday.

The UMX U686CL is provided by Virgin Mobile’s Assurance Wireless program. Assurance Wireless is an offshoot of the Lifeline Assistance program, a Federal Communications Commissions plan that makes free or government-subsidized phones service available to millions of low-income families. The program is often referred to as the Obama Phone because it expanded in 2008, when President Barack Obama took office. The UMX U686CL runs Android and is available for $35 to qualifying users.

Researchers at Malwarebytes said on Thursday that the device comes with some nasty surprises. Representatives of Sprint, the owner of Virgin Mobile, meanwhile said it didn’t believe the apps were malicious.

The first is heavily obfuscated malware that can install adware and other unwanted apps without the knowledge or permission of the user. Android/Trojan.Dropper.Agent.UMX

contains striking similarities to two other trojan droppers. For one, it uses identical text strings and almost identical code. And for another, it contains an encoded string that, when decoded, contains a hidden library named com.android.google.bridge.Liblmp.

Once the library is loaded into memory, it installs software Malwarebytes calls Android/Trojan.HiddenAds. It aggressively displays ads. Malwarebytes researcher Nathan Collier said company users have reported that the hidden library installs a variant of HiddenAds, but the researchers were unable to reproduce that installation, possibly because the library waits some amount of time before doing so.

The malware that installs these programs is hidden in the phone's settings app. That makes it virtually impossible to uninstall, since the phone can't operate properly without it. "Uninstall the Settings app, and you just made yourself a pricey paper weight," Collier wrote.

The second unpleasant surprise delivered by the UMX U686CL is something called Wireless Update. While it provides a mechanism for downloading and installing phone updates, it also loads a barrage of unwanted apps without permission. The app is a variant of Adups, an app from a China-based company by the same name. In 2016, researchers caught Adups surreptitiously collecting user data on hundreds of thousands of low-cost phones from BLU.

"From the moment you log into the mobile device, Wireless Update starts auto-installing apps," Collier said. "To repeat: there is no user consent collected to do so, no buttons to click to accept the installs, it just installs apps on its own."

While all of the installed apps Malwarebytes examined were clean and free of malware, the presence of a feature that automatically installs apps poses an unacceptable risk,

particularly since removing the feature prevents the phone from receiving updates. Collier's post classified Wireless Update as malware, but Jérôme Segura, Malwarebytes' head of threat intelligence, told me its actual classification is a PUP, or potentially unwanted program, since there's no evidence the apps that are installed are malicious.

In any event, the two apps analyzed by Malwarebytes make use of the UMX U686CL a bad choice. The fact that it's made available to low-income users only worsens the insult. Malwarebytes said it notified Assurance Wireless of its findings and asked why the phone it sells comes with preinstalled malware. So far, no one has responded. In an email, Sprint officials said: "We are aware of this issue and are in touch with the device manufacturer Unimax to understand the root cause, however, after our initial testing we do not believe the applications described in the media are malware."

It's not hard to find online discussions like this one complaining of annoying displayed ads and apps automatically installing on the device without user permission. A similar thread discusses ads that display on the homescreen even when a browser isn't running.

Over the years, preinstalled malware has been found on a raft of low-cost Android phones from a variety of providers and manufacturers. An incomplete list includes a backdoor on hundreds of thousands of BLU devices, a powerful backdoor and rootkit also on BLU devices, and covert downloaders on 26 different phone models from various manufacturers.

It seems the price people often pay for low-cost phones is compromised security and privacy. While many users may not be able to afford them, buying phones from mainstream and well-known providers located outside of China is likely to be a better choice.

Post updated at 1/9/2020, 3:24 PM California time to add

comment from Sprint.

https://arstechnica.com/?p=1641785