CERT-EU

Free smartphones for low-income households shipped with malware

Threat Memo - TM 20-008 - Date: 20/01/2020 – Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cyberespionage	Supply chain compromise Personal data leakage	World	Telecom, citizens	A1

Key Points

- Free smartphones being issued in a welfare program contained irremovable malware.
- The company issuing the phones has denied this software is malware, but this is repudiated by public knowledge.
- The inclusion of data leaking malware is on the rise and could possibly develop into a business model.

Summary

Malwarebytes has published a report[1] on Android phones being shipped with malware to unsuspecting users by Lifeline Assistance, a US government-funded program providing low-income households with cheap cell service and, in some programs, a free smartphone. In this case, provider Assurance Wireless offered the infected smartphone (a Unimax U683CL[2]) along with free data, texts and minutes.

The first malicious application, known as Wireless Update, has the capability of automatically installing applications without user consent. Malwarebytes has identified it as a variant of Adups, an application by a Chinese company previously seen collecting user data, creating backdoors and developing auto-installers. Wireless Update cannot be removed without rendering the phone unusable.

The second malware, Android/Trojan.Dropper.Agent.UMX, serves as the device's Settings-app, its removal effectively rendering the device unusable. Malwarebytes has identified this app as Chinese and discovered it executes another malware named HiddenAds, known for aggressively throwing up advertisement to the user.

In a comment on the publication of the story, Sprint (owner company of Assurance Wireless) states it is aware of the issue and is in touch with the device manufacturer but that Sprint, based upon its own initial testing, does not believe these applications to be malware.

The US Federal Communications Commission (FCC), responsible for Lifeline Assistance, responded to Forbes[3] stating the fund does not allow the offering of a smartphone.

Comments

The documented history[4][5][6] of Adups and HiddenAds malware (collection of user data such as contact lists, text messages, locations, application data) repudiates the Sprint assertion regarding the nature of the apps.

Pre-installed mobile device malware – a form of supply chain compromise - is on the rise, with this case being particularly noteworthy since the smartphones were offered in a welfare program for households unable to afford a smartphone on their own budget. More generally, it could possibly become a business model to offer cheaper smartphones with a secondary payment in personal data.

[1] https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/

[2] https://fccid.io/P46-U683CL/External-Photos/External-Photos-4185064

[3] https://www.forbes.com/sites/thomasbrewster/2020/01/09/us-funds-free-android-phones-for-the-poor---but-with-permanent-chinese-malware/

[4] https://www.digitaltrends.com/mobile/kryptowire-adups-news/

[5] https://www.kryptowire.com/kryptowire-discovers-mobile-phone-firmware-transmitted-personally-identifiable-information-pii-without-user-consent-disclosure/

[6] https://www.bleepingcomputer.com/news/security/android-adups-backdoor-became-active-5-months-affected-43-phone-vendors/