Android smartphones supply chain compromise

Reference: Memo [190607-2] Date: 07/06/2019 - Version: 1.0
Keywords: supply chain compromise, Android, smartphone, digital services
Sources: publicly available information

Key Points

- Two Android smartphone models have been sold with pre-installed malware affecting at least 20000 users in Germany alone.
- For app developers the introduction of undesirable functions might be the result of poor coding practices, or a deliberate criminal act to maximise the return on their investment.
- Since 2016, several Android-related supply chain compromises have been reported, affecting up to 141 Android smartphone models.

Summary

On June 6, the German Federal Office for Information Security (BSI) released alerts warning that two Android smartphones – Doogee BL700 and M Horse Pure 1 – were being sold with pre-installed malware. As regards the malware identity, the BSI alerts indicate that it is a variant of a backdoor Trojan analysed by the cyber-security firm Sophos Lab in October 2018 as 'Andr/Xgen2-CY'. This backdoor was embedded inside an app named SoundRecorder, included by default on uleFone S8 Pro smartphones.

This backdoor shows the following behaviour:

- Collecting data such as device's phone number, location information, Android ID, screen resolution, manufacturer, model, brand, etc. In the best case, this could be seen as app analytics.
- Sending SMS-s to one number in a hard-coded list in a covert manner. The malicious SMS code intercepts and deletes messages to or from any of the numbers in the list, so they never show up in the phone's text messaging app.
- Backdoor functions: contact a command and control (C2) server, get instructions, perform tasks such as download and install apps, uninstall apps, execute shell commands, open URL in browser.
- Staying invisible: the backdoor disguises itself as part of the Android library, all strings are encrypted, the backdoor implements anti-sandbox analysis features.

In Germany only, at least 20 000 IP addresses were observed connecting to the backdoor C2 servers on a daily basis.

Comments

A smartphone shipped from the factory, pre-installed with a potentially unwanted app (PUA) or even malware is a situation known as a supply chain compromise.

Many makers of Android phones and other mobile devices bundle in apps from third parties. Typically, these apps are installed in one of two locations used for privileged system apps, either the /system/app or /system/priv-app folders. In theory, the apps installed to these locations are supposed to be trusted system apps, such as a file manager or other utilities users expect to be there. In reality, app makers sometimes pay phone manufacturers to include their apps in the factory image.

For app developers, the introduction of undesirable functions in their apps could be:

- the result of poor coding practices, or
- a deliberate criminal act to maximise the return on their investment.

The online IT news outlet ZDNet has reported other Android related supply chain compromises:

- November 2016: several models of Android smartphones (including the BLU R1 HD) were observed with firmware that transmitted users' sensitive data to third-party servers without disclosure or the users' consent.
- December 2016: a downloader for Android malware was embedded in the firmware of 26 Android smartphone models.
- July 2017: versions of the Triada banking Trojan were found hidden in the firmware of several Android smartphones.
- March 2018: the same Triada Trojan was found embedded in the firmware of 42 other Android smartphone models.
- May 2018: Avast researchers found the Cosiloon backdoor Trojan in the firmware of 141 Android smartphones.

Other kinds of supply chain compromises have recently been analysed by CERT-EU:

- March 2019: Between June and November 2018, a sophisticated supply chain attack, dubbed ShadowHammer, involved ASUS Live Update Utility. See Memo [190326-1].
- March 2019: a number of tablets and smartphones from Polish, Chinese, and Hong Kong manufacturers were found to contain malware-infected firmware. See Memo [190301-1].
- April 2019: the Indian multinational IT outsourcing and consulting giant Wipro was compromised and its IT systems were used to launch attacks against some of the company's customers. See Memo [190417-1].
- April 2019: Docker Hub, an open repository of software containers, announced a breach affecting about 190 000 of its users. As the breach affects associated development platforms, it may impact several stages of software development workflows. See Memo [190430-1].