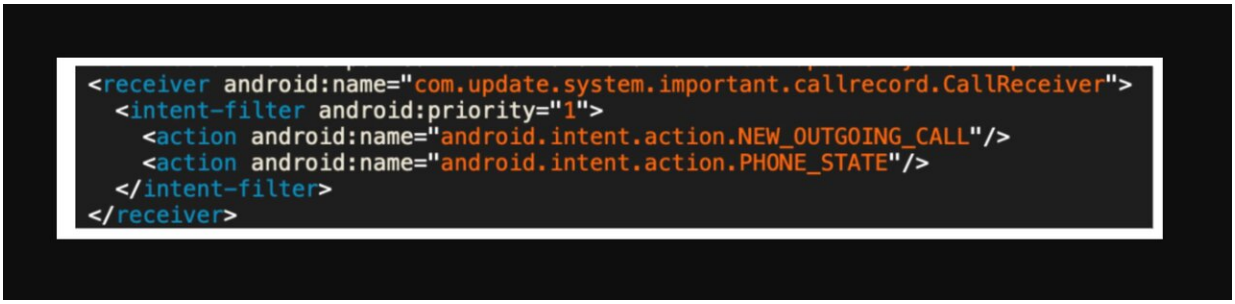
A new advanced Android malware posing as system update

March 28 2021, by Sarah Katz



AndroidManifest malware. Credit: Zimperium

In recent weeks, Zimperium zLabs researchers revealed unsecured cloud configurations exposing user data across thousands of legitimate Android and iOS applications. Now, zLabs is advising Android users about a clever and malicious new Android app.

This latest malware takes the form of a System Update application in order to steal data, images, messages and usurp control over entire Android phones. After assuming control, attackers can record audio and phone calls, view browser history, take photos and access WhatsApp messages, among other activities.

zLabs researchers uncovered this alleged System Update app after detecting an application flagged by the z9 malware engine powering

zIPS on-device detection. An investigation showed this activity to trace to an advanced spyware campaign with intricate capabilities. Researchers sealed the deal after confirming with Google that such an app never existed nor was planned to ever be released on Google Play.

With an extensive list of compromise capabilities, this malware can steal messages off instant messenger systems and their database files using root, examine the default browsers bookmarks and searches, inspect bookmark and search history from Google Chrome, Mozilla Firefox and Samsung Internet browsers, search for files with the specific extensions .doc, .docx, .pdf, .xls and .xlsx; examine clipboard data and notifications content, take periodic photos via the front or rear camera, view installed applications, steal images and video, monitor via GPS, steal phone contacts and SMS messages as well as call logs and exfiltrate device information such as device name and storage data. Moreover, the malware can even conceal itself by hiding its icon from the devices' menu.

This malware works by running on Firebase Command and Control (C&C) upon installation from a non-Google third party apps store, listed under the names "update" and "refreshAllData". To enhance its sense of legitimacy, the app contains feature information such as the presence of WhatsApp, battery percentage, storage statistics, type of Internet connection and Firebase messaging service token. Once the user selects to "update" the existing information, the app infiltrates the affected device. Upon dissemination, the C&C receives all relevant data, including the new generated Firebase token.

While the Firebase communication makes the necessary commands, the dedicated C&C server uses a POST request to gather the stolen data. Notable actions that trigger exfiltration by the app include adding a new contact, installing a new application via Android's contentObserver or receiving a new SMS.

More information: Yaswant, A. "New Advanced Android Malware Posing as 'System Update.'" Zimperium Mobile Security Blog, Zimperium, 26 Mar. 2021, blog.zimperium.com/new-advance … ng-as-system-update/