Mobile APT (mAPT) SpyWaller May Include Western Targets

By Lookout

Published: 2018-01-10 · Archived: 2026-04-05 13:40:34 UTC

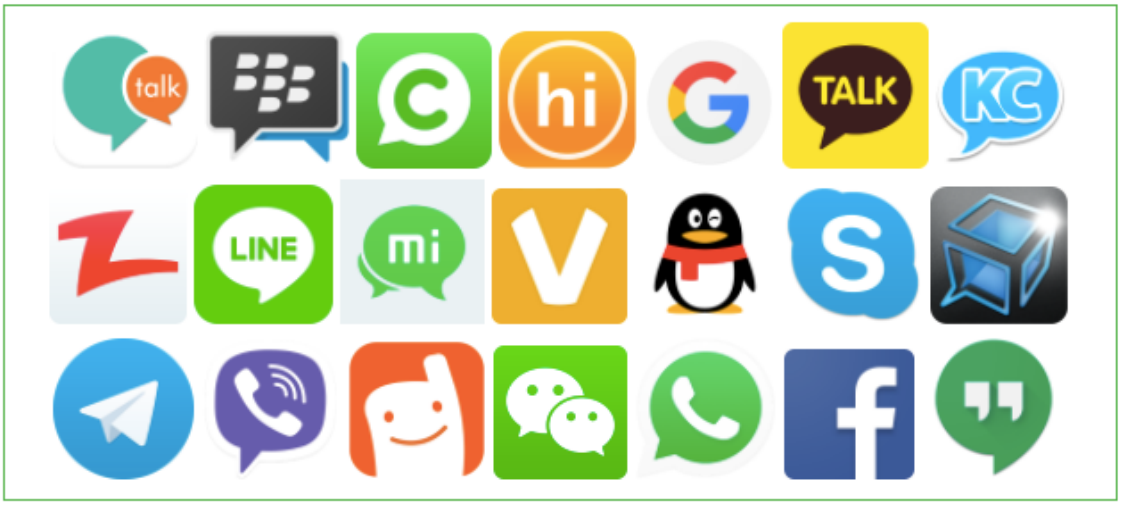
Lookout has discovered new variants of the SpyWaller surveillanceware with advanced espionage capabilities. The variants now target Facebook Messenger, WhatsApp, and Google Hangouts among others, suggesting they

are being used against Western targets.

SpyWaller's continual evolution and sophistication indicates an actor with significant resources is behind its development. Due to this, and that it appears quite targeted, Lookout considers it an mAPT — an APT that has evolved to focus on mobile devices. All Lookout customers are protected from this threat.

What is SpyWaller

The SpyWaller family was first discovered in 2014 and came to the attention of security researchers due to its use of iptables in order to drop network connections made by specific antivirus applications. These early samples were capable of retrieving sensitive information from a number of messaging apps and concealed this malicious functionality in encrypted asset files that were loaded during execution. The actors behind SpyWaller have been busy evolving their tool, according to our analysis of the samples in the Lookout dataset, most notably by expanding the number of apps that it can retrieve data from, and reimplementing all information gathering functionality in native code as opposed to the Java layer.



Applications that the latest versions of SpyWaller targets include AireTalk, BlackBerry Messenger, Coco, Hi, Google Services Framework, Kakao Talk, KeeChat, Zapya, Line, MiTalk Messenger, Oovoo, QQ, Skype, TalkBox Voice Messenger, Telegram, Viber, Voxer Walkie Talkie Messenger, WeChat, WhatsApp, Facebook, Google Hangouts, and Wi-Fi credentials. The majority of these apps are for messaging and communication however others are for file sharing.

The latest SpyWaller variants are capable of accessing the sensitive data of over 20 different apps, in addition to being able to record calls, capture surrounding audio, track a device's location, take pictures with the camera, and retrieve a list of installed packages.

Initial infection is followed by requests to command and control infrastructure for the latest native code component that contains the bulk of SpyWaller's surveillanceware functionality. While we found the native code that is bundled up in the app is somewhat obfuscated, the latest binary served up by attacker infrastructure was not, and contains new code to target Facebook and Google Hangouts. These improvements in capability suggest that the actor behind SpyWaller may be deploying it in campaigns outside of China, where we believe the majority of previous activity to have been conducted.

SpyWaller can attempt to elevate its privileges and most variants have been found to include exploits for local vulnerabilities. Analysis indicates that attacker infrastructure can also provide additional exploits if necessary. If SpyWaller is able to elevate its privileges it attempts to establish persistence by copying various files to the /system/bin/ directory via the dd command. When deobfuscated this full command is:

mount -o remount system /system;dd if=<apk data data directory>/files/update of=/system/bin/update;chmod 6777 /system/bin/update;

The latest versions of SpyWaller primarily communicate on the non-standard port of 5353 to IPs that reside in China. The following addresses are associated to recent SpyWaller variants.

These IPs can be geolocated to within China, visualized in the map above. 4 IPs are concentrated near the Xinjiang province in northwest China, 2 to the coordinates near Shandong, and 1 to each of the remaining highlighted points.

SHA-1

- f8740bb04fa884a65e16c6bfa0a169bc6e80ada3
- e479391f1ab93ade71792011f7b5c146d39cfb52

- 323868c190dfd57147916ea6cfcd1ab6034d02b6
- 5a71bfb4625e4f77351563ef1c626f4020946d6c
- 0d45a20ea6921efc1ec371e076499efb4221d6e8
- 73d54c9e7a382a37cbeb291ac27b8292dfafa93d
- 55e7dd8f80f946acf66bd97b2edce712e25fedd5
- 2bb1f2de60fa18d28b5a39542960d33e03b5b688
- 17cdb01db464b8b63cb3a74e9e8bd7ddd1dba390
- 3eddfdc3fd61962c789c581d0f0634e380200bc5
- c9e6b17cc5aef4749fc69f6a81a2ab2c99057971
- 397426e98c080c7f74d0362e538e2fcd2b81e8e7
- f101e27d225a7c61444b3fd2b700f8df1f89c2c4
- 2c3ea07b2600a271868735d31518fb3297945dfa
- 5c80615b010b261794e14b32a1a2804cc5b04b88

Authors

Michael Flossman

Head of Threat Intelligence

Michael is Head of Threat Intelligence at Lookout where he works on reverse engineering sophisticated mobile threats while tracking their evolution, the campaigns they are used in, and the actors behind them. He has hands-on experience in vulnerability research, incident response, security assessments, pen-testing, reverse engineering and the prototyping of automated analysis solutions. When not analysing malware there’s a good chance he’s off snowboarding, diving, or looking for flaws in popular mobile apps.

Stop Cyberattacks Before They Start With Industry-Leading Threat Intelligence.
