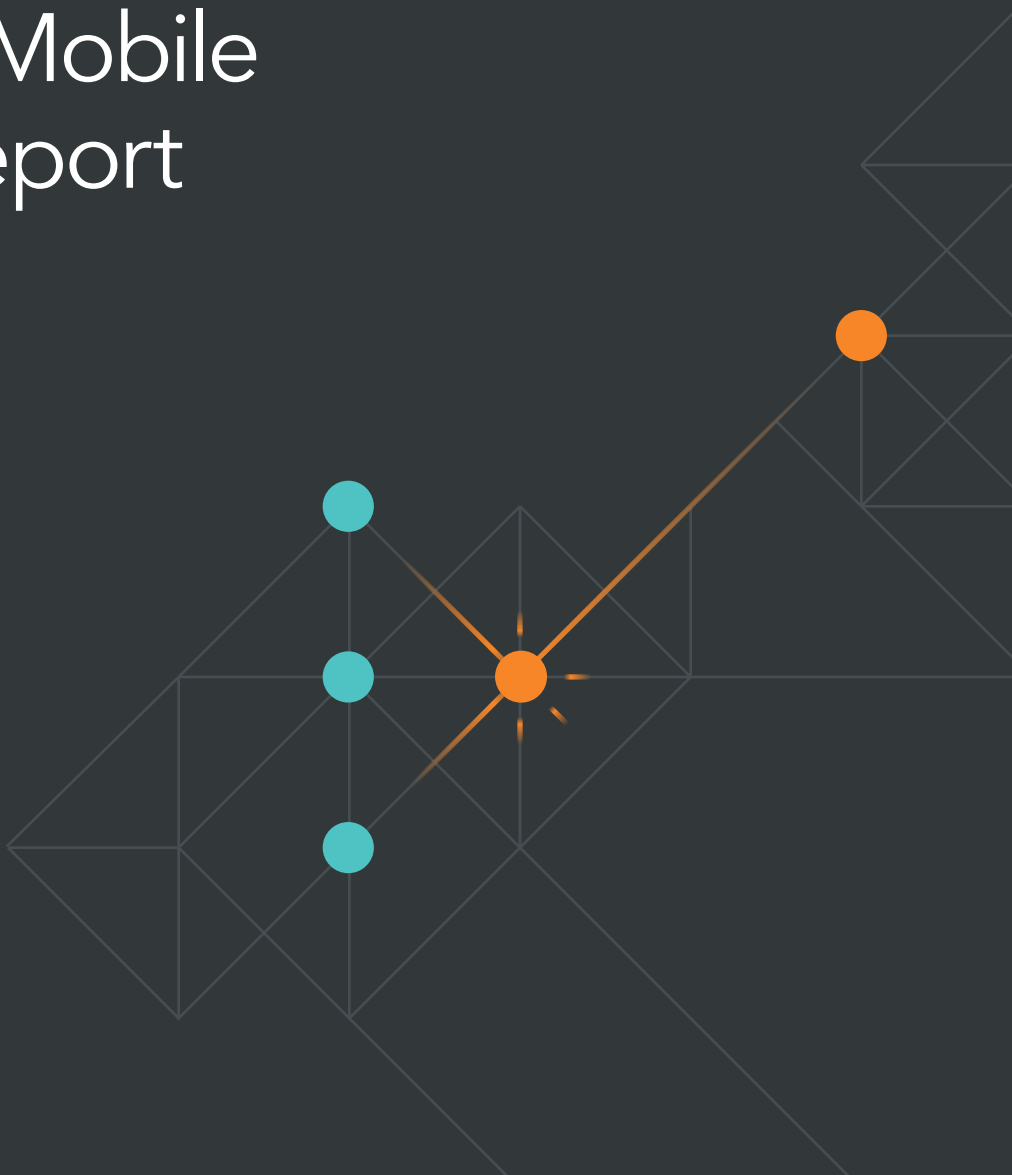
Lookout

Q3 2017

Lookout Mobile Threat Report



EXECUTIVE SUMMARY

The Mobile Threat Report is a collection of Lookout mobile threat-discoveries and commentary.

Mobile threat actors are increasingly becoming more proficient and prolific, increasing the sophistication of their attacks. At the same time, employees are accessing work data through their mobile devices on a daily basis. Over 60% of employees across the globe say they access their organization's customer, partner, and employee data on their mobile device, according to a new Lookout survey. It's more important than ever for organizations to know what threats they face, and how those threats can cause data loss, compliance infringement, and brand reputation damage.

All Lookout customers are protected from the threats listed in this report.

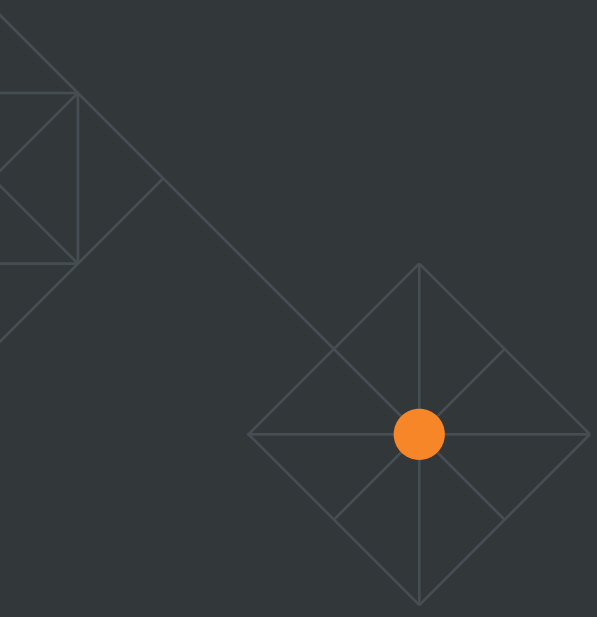
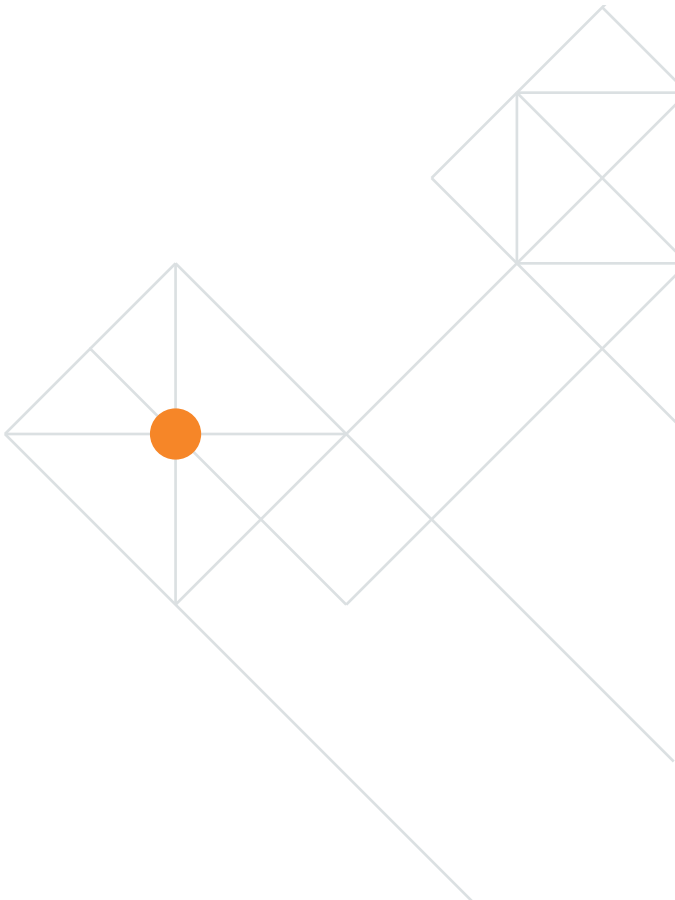


TABLE OF CONTENTS

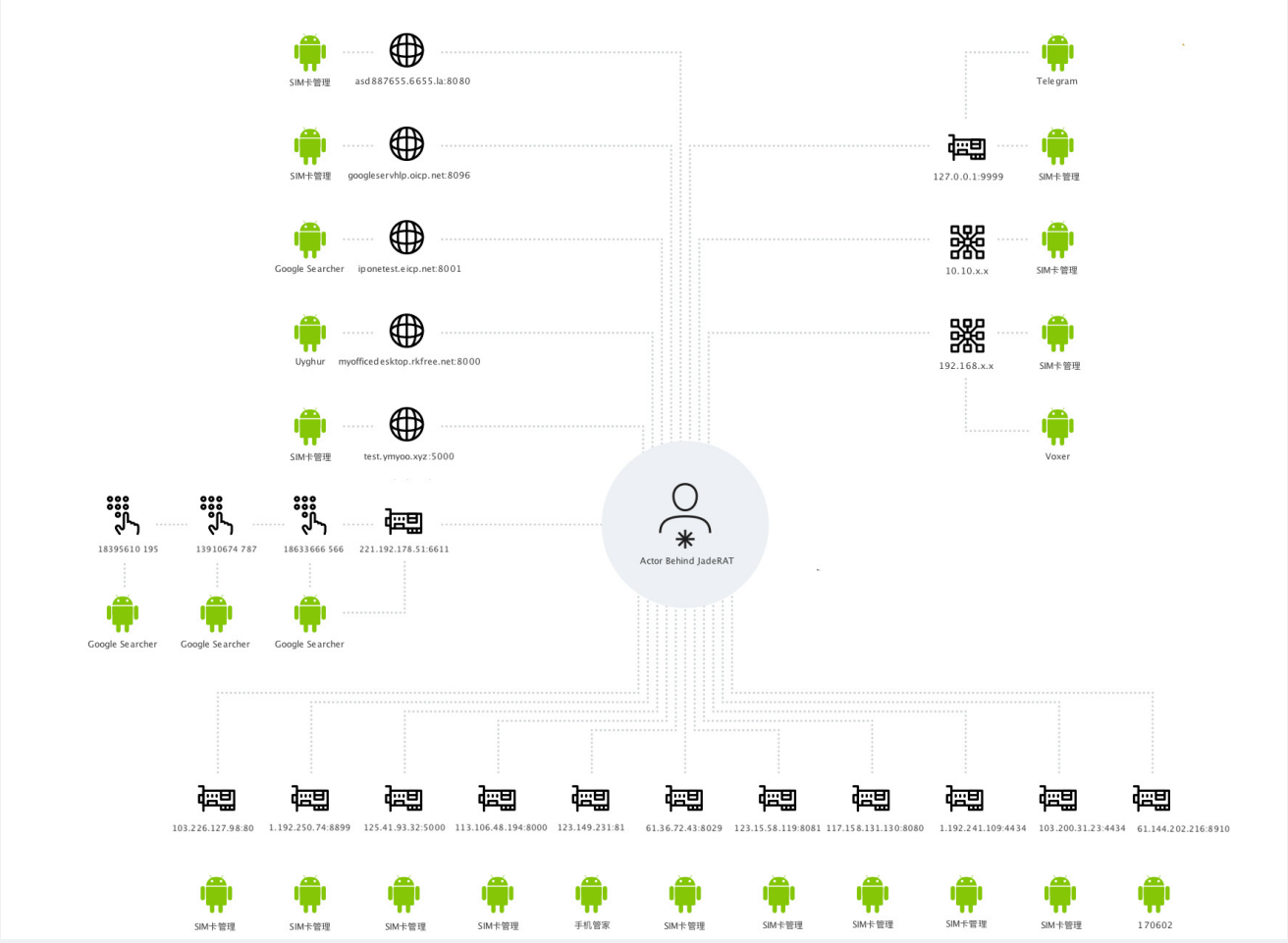


JadeRAT

Lookout researchers are monitoring the evolution of an Android surveillanceware family known as JadeRAT. JadeRAT is an example of a mobile APT (mAPT), or an advanced persistent threat that uses mobile as a capability. We believe the threat may be connected to a government sponsored APT group. While our analysis has identified several possible leads that could tie this surveillanceware family to the Naikon APT, Scarlet Mimic, or one of several other groups operating in the region, at this point in time we do not have conclusive evidence to confirm this.

JadeRAT operators have a significant degree of control over compromised devices. The malware supports over 60 commands that allow operators to retrieve sensitive information and profile victims. This includes location, contacts, accounts, call logs, text messages, and more.

Get more details



JadeRAT actor infrastructure

Frozencell

FrozenCell is also an example of an mAPT. It is the mobile component of a multi-platform attack used to spy on victims through compromised mobile devices and desktops. We believe the attack is associated with a threat actor known as "Two-tailed Scorpion/APT-C-23."

FrozenCell masquerades as fake updates to chat apps like Facebook, WhatsApp, Messenger, LINE, and LoveChat. Once installed on the device, the threat can record calls, geolocate a device, exfiltrate images, download and install additional apps, retrieve contacts, and more.

We discovered 561MB of exfiltrated data from 24 compromised Android devices while investigating this threat. More data is appearing daily, leading us to believe the actors are still highly active.

Get more details

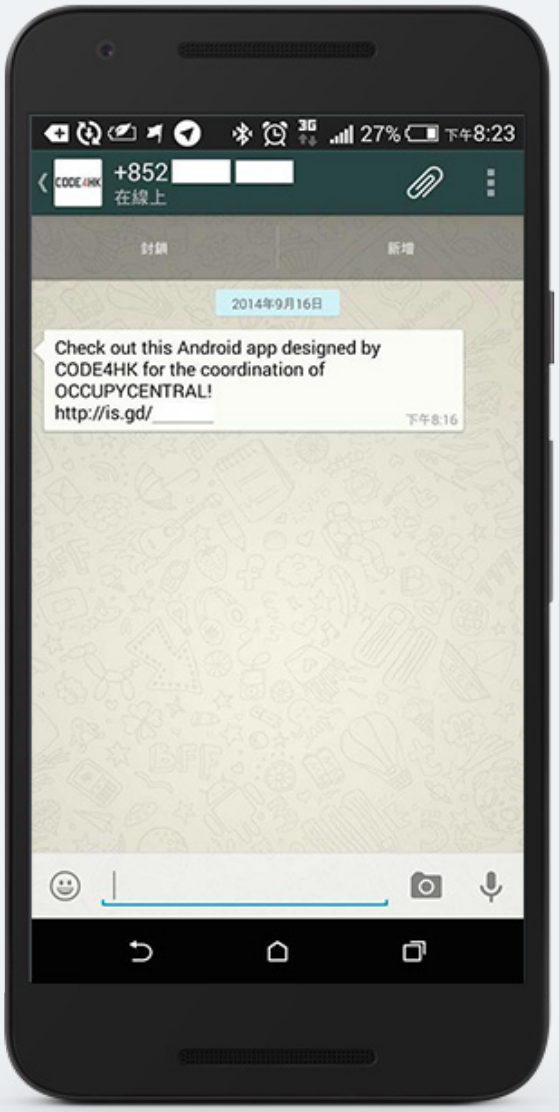
FrozenCell analysis shows infected devices are completely based in Gaza, Palestine. It has not been confirmed whether these are from test devices or the devices of victims.

xRAT

xRAT is an mAPT with extensive data collection functionality and the ability to remotely run a suicide function to avoid detection. The malware is associated with the high-profile Xsser / mRAT malware, which made headlines after targeting both iOS and Android devices of pro-democracy Hong Kong activists in late 2014.

Lookout identified xRAT due to a combination of suspicious capabilities it uses, such as dynamically loading additional code, executing native libraries, using specific ciphers, and accessing sensitive user information. xRAT gathers browser history data, call logs, text messages, contacts, email account usernames and passwords.

Get more details



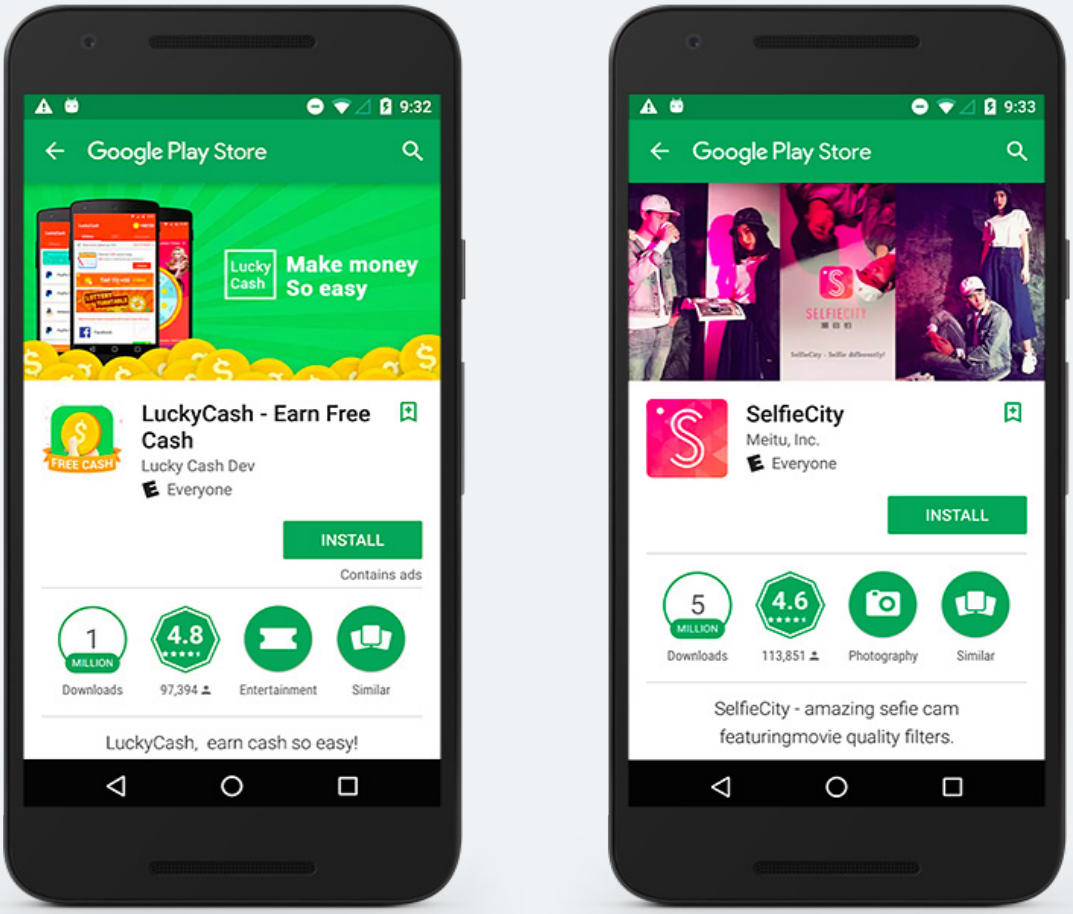
Example of an xRAT phishing message.

Igexin

Lookout discovered an advertising software development kit (SDK) called Igexin that had the capability of spying on victims through otherwise benign apps by downloading malicious plugins. Over 500 apps available on Google Play used the Igexin ad SDK. Apps containing the affected SDK were downloaded over 100 million times across the Android ecosystem. Examples include weather apps, internet radio apps, photo editors, health and fitness apps, and more.

While not all of these apps have been confirmed to download the malicious spying capability, the operators could have introduced malicious functionality at their convenience.

Get more details



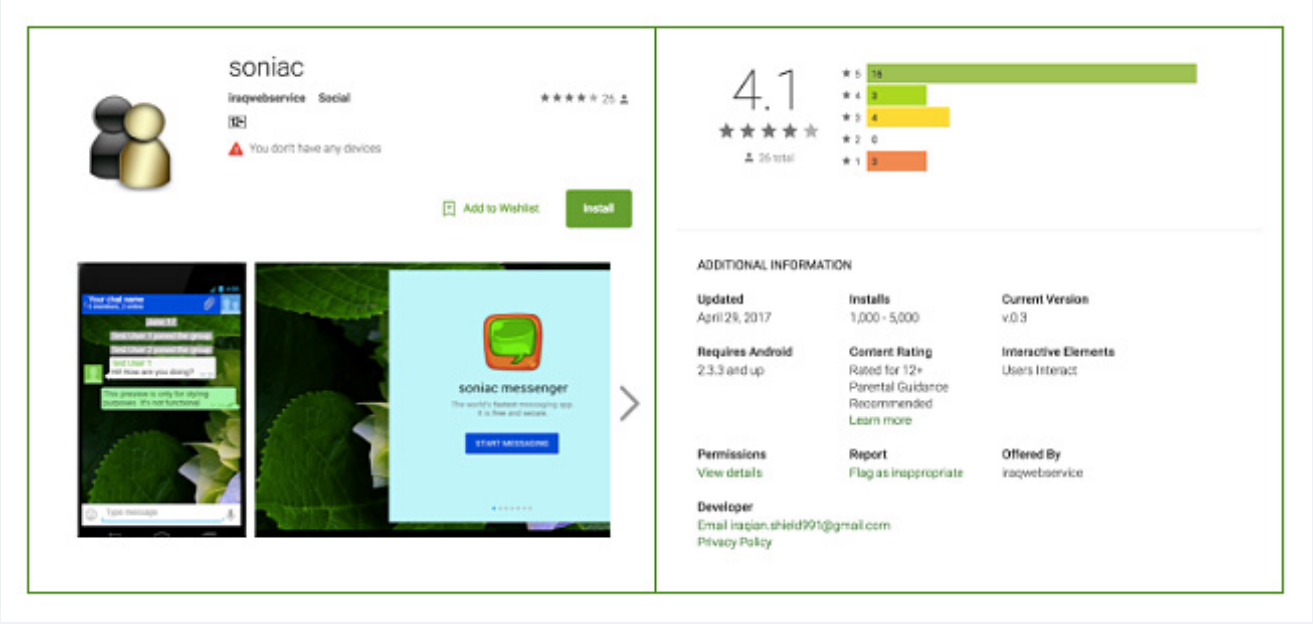
Examples of Igexin-impacted apps that were once in the Google Play Store.

SonicSpy

Lookout researchers have identified over a thousand spyware apps related to a threat actor likely based in Iraq. Belonging to the family "SonicSpy," these samples have been aggressively deployed since February 2017, with several making their way onto the Google Play Store.

We found one malicious app was able to silently record audio, take photos with the camera, make outbound calls, send text messages to attacker-specified numbers, and retrieve information such as call logs, contacts, and information about Wi-Fi access points.

Get more details



Example of a malicious SonicSpy app called "Soniac," that was in the Google Play Store.

Want to learn more about mobile threats?

Contact our team today or check out our Threat Advisory Services. If you found this helpful, you may also be interested in:

Mobile Risk Matrix

Use this framework to understand how threats like the ones above and risks can impact enterprise data through mobile devices.

Learn more

Data compromise via mobile threats explainer

Get a full explainer on mobile threats – from Wi-Fi attacks to malicious employee behaviors – in this blog from Lookout Security Researcher Andrew Blaich's.

Learn more

Machine learning in mobile security webinar

Watch this webinar to learn what machine learning can and can't do to solve today's mobile security problems.

View webinar