

Goontact iOS and Android malware

Lookout is constantly discovering and researching new threats to protect and advise our customers

Background and Discovery Timeline

The Lookout Threat Intelligence team has discovered a new mobile app threat targeting iOS and Android users in China, Korea and Japan. The malware, named Goontact, targets users of illicit sites, typically offering escort services, and steals personal information from their mobile device. The types of sites used and the information they exfiltrate suggest that the ultimate goal is extortion or blackmail.

These sextortion scams are exploiting Chinese-, Japanese- and Korean-speaking people across multiple Asian countries. The scam begins when a potential target is lured to one of the hosted sites where they are invited to connect with sex workers. Account IDs for secure messaging apps such as KakaoTalk or Telegram are advertised as the best forms of communication and the individual initiates a conversation. In reality, the targets are communicating with Goontact operators.

Capabilities and Affected Parties

Targets are convinced to install (or sideload) a mobile application on some pretext, such as audio or video problems. The mobile applications in question have no real user functionality, except to steal the victim's address book, which is then used by the attacker ultimately to extort the target for monetary gain. Additional data that can be exfiltrated includes:

- Device Identifiers - Phone number - Contacts - SMS Messages - Photos on external storage - Location information

Key Findings

1. Operated by an active crime group and continuously being developed.
2. There are both iOS and Android components of this surveillanceware.
3. Victims are lured in on illicit sites that act as middlemen to set up chats and dates with women.

How Lookout Detects and Protects Against Surveillanceware Campaigns

Lookout Security Intelligence teams are continuously discovering and researching new threats to protect and advise our customers by combining static and dynamic analysis with our machine learning engine. Devices with Lookout installed can detect and be alerted to this specific campaign, and Lookout also protects against other sophisticated surveillanceware that could go undetected.

To learn more about the technical specifications of this campaign, including IOCs, read the full article [here](#).

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

[Click here to learn more about Threat Advisory](#)