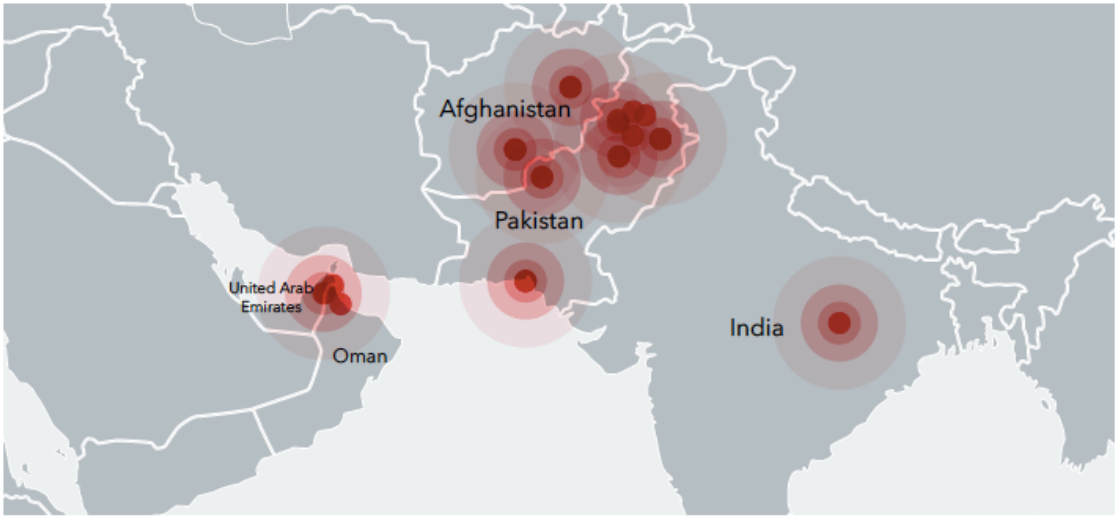
Stealth Mango and Tangelo | Surveillanceware Stealing Data

By Lookout

Published: 2018-05-18 · Archived: 2026-04-02 11:11:09 UTC

Lookout Security Intelligence has discovered Android and iOS surveillanceware tools targeting government officials, diplomats, military personnel, and activists, specifically in Pakistan, Afghanistan, India, Iraq, and the UAE. Additionally, data from U.S., Australian, and German officials and military have been swept up in the campaign we believe is being run by members in the Pakistani military.

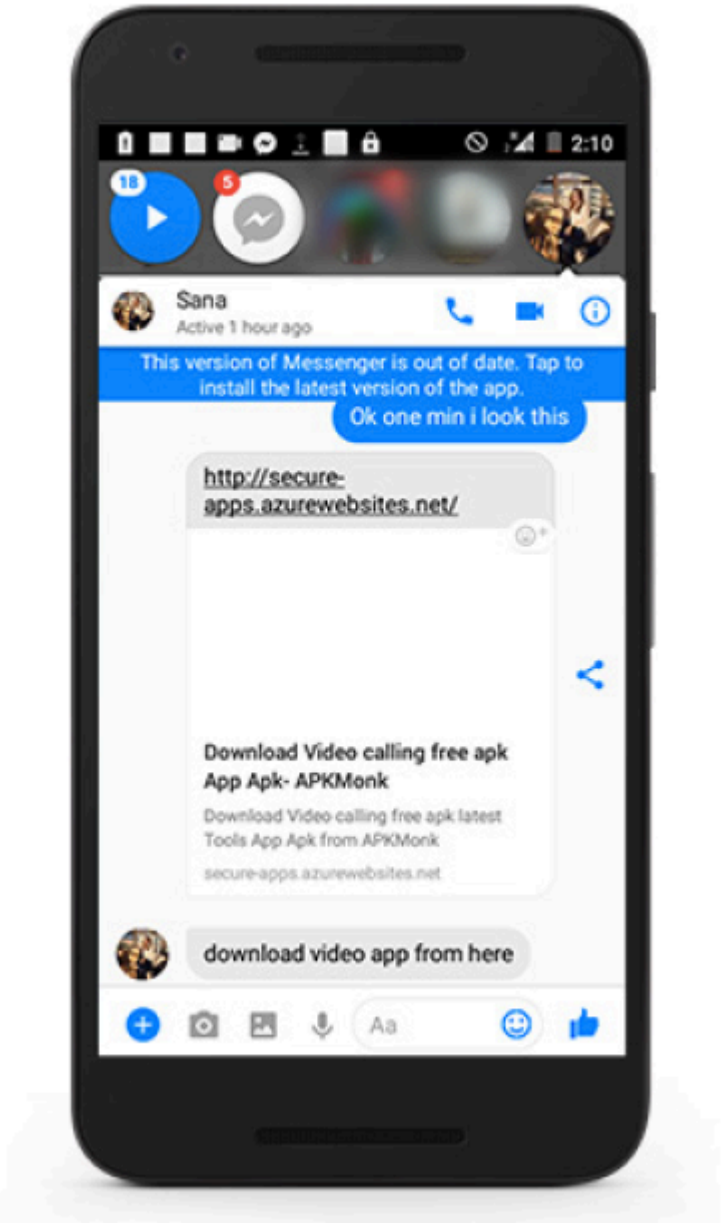
We're calling these surveillanceware families Stealth Mango (Android) and Tangelo (iOS).



GPS coordinates pulled from the EXIF data of exfiltrated images is centered around Pakistan, Afghanistan, India, and the United Arab Emirates.

The Lookout Security Intelligence team alerted Google to the existence of Stealth Mango during our investigation. The company states: "Google identified the apps associated with this actor, none of the apps were on the Google Play Store. Google Play Protect has been updated to protect user devices from these apps and is in the process of removing them from all affected devices."

Phishing and distribution



Phishing message sent through Facebook Messenger.

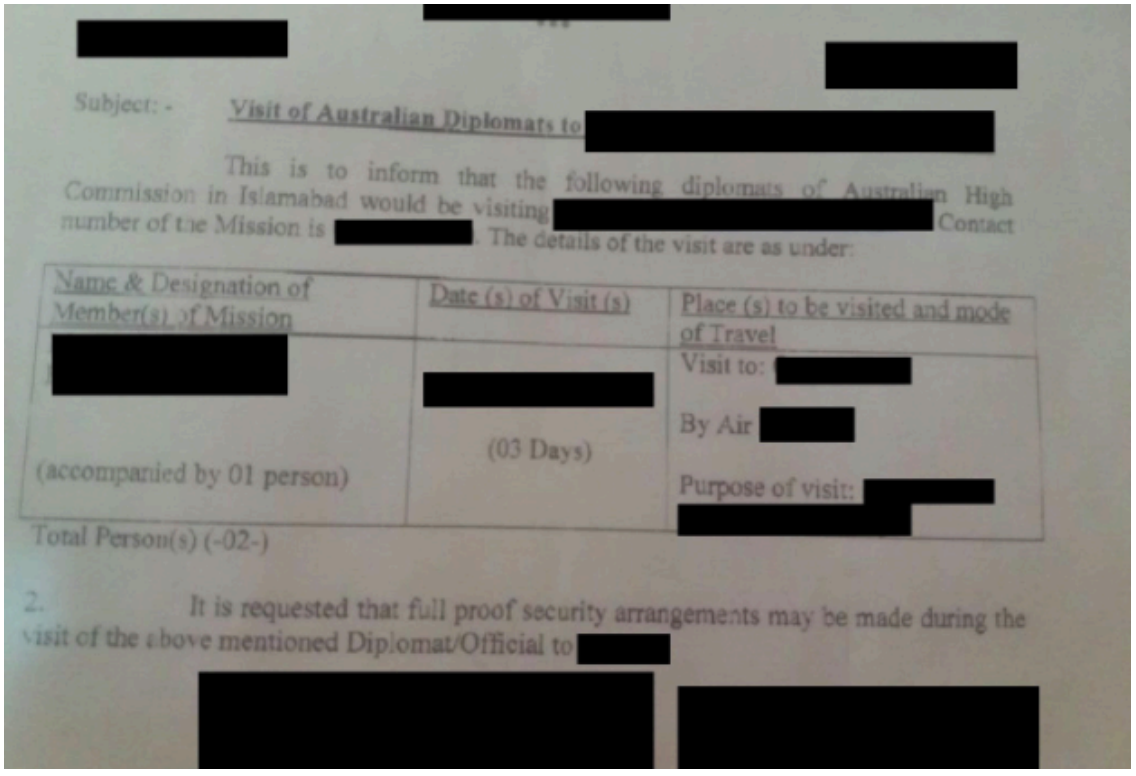
The actors behind Stealth Mango typically lure victims via phishing messages sent by fake Facebook personas, but in some cases may have used physical access to victims' devices. As was the case with previous actors we've

reported on, such as Dark Caracal, the actor behind Stealth Mango has stolen a significant amount of sensitive data from compromised devices without the need to resort to exploits of any kind.

Exfiltrated content

The majority of this content we analyzed has information that would be of great interest to a nation state actor. This includes:

- Letters and internal government communications
- Detailed travel information
- Pictures of IDs and passports
- GPS coordinates of pictures and devices
- Legal and medical documents
- Developer information including whiteboard sessions, account information, and test devices
- Photos of the military, government, and related officials from closed door meetings including U.S. Army personnel



Subject: - Visit of Australian Diplomats to [redacted]

This is to inform that the following diplomats of Australian High Commission in Islamabad would be visiting [redacted] Contact number of the Mission is [redacted]. The details of the visit are as under:

Name & Designation of Member(s) of Mission	Date (s) of Visit (s)	Place (s) to be visited and mode of Travel
[redacted] (accompanied by 01 person)	[redacted] (03 Days)	Visit to: [redacted] By Air [redacted] Purpose of visit: [redacted]

Total Person(s) (-02-)

2. It is requested that full proof security arrangements may be made during the visit of the above mentioned Diplomat/Official to [redacted]

Details around travel in and around Pakistan from Australian diplomats.

Exfiltrated content was found to contain military photos including a series of images from an event with military attendees from numerous countries including U.S. Army personnel.

Attacker personas

We have also identified, as part of this investigation, several individuals who we believe are responsible for the development of other commodity Android and iOS spyware tools that share many similarities to Stealth Mango and Tangelo. These individuals all belong to the same freelance developer group for hire, which says it has a physical presence in India, Pakistan, and the United States.

Authors

Andrew Blaich

Head of Device Intelligence

Andrew Blaich is Head of Device Intelligence at Lookout where he is focused on mobile threat hunting and vulnerability research. Prior to Lookout, Andrew was the Lead Security Analyst at Bluebox Security. He holds a Ph.D. in computer science, and engineering from the University of Notre Dame in enterprise security and wireless networking. In the past Andrew has worked at both Samsung and Qualcomm Research. Andrew is a regular presenter at security conferences including BlackHat, RSA, Kaspersky SAS, SecTor, SANS DFIR, Interop, and ACSC. In his free time he loves to run and hack on IoT.

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.
