# New Surveillanceware in Google Play Targeting Middle East

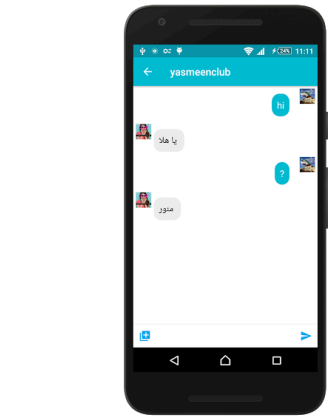
By Lookout

Published: 2018-04-16 · Archived: 2026-04-05 15:29:19 UTC

Lookout researchers have identified a new, highly targeted surveillanceware family known as Desert Scorpion in the Google Play Store. Lookout notified Google of the finding and Google removed the app immediately while also taking action on it in Google Play Protect. The app ties together two malware families - Desert Scorpion and another targeted surveillanceware family named FrozenCell - that we believe are being developed by a single, evolving surveillanceware actor called APT-C-23 targeting individuals in the Middle East.

We've seen this actor rely heavily on phishing campaigns to trick victims into downloading their malicious apps, specifically on Facebook. Even sophisticated actors are using lower cost, less technologically impressive means like phishing to spread their malware because it's cheap and very effective, especially on mobile devices where there are more ways to interact with a victim (messaging apps, social media apps, etc.), and less screen real estate for victims to identify potential indicators of a threat.

Lookout customers are protected against this threat and additionally we have included a list of IOCs at the end of this report.




# Dardesh (Unreleased)

**Dardesh App** **Social**

Teen

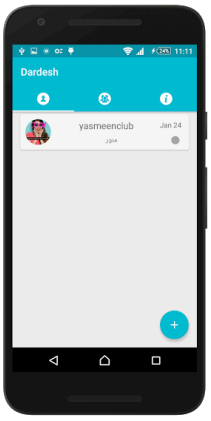
This app is in development. It may be unstable.

You don't have any devices.

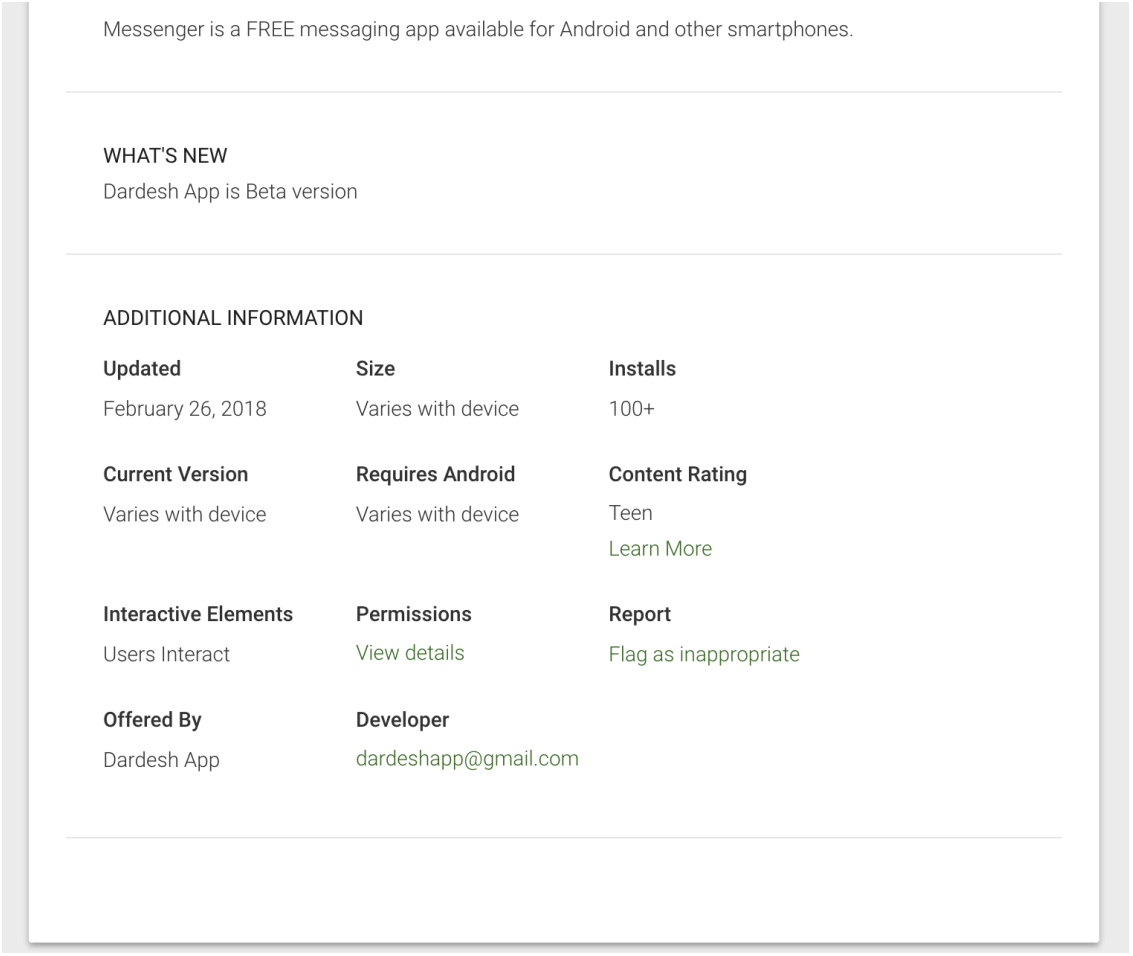
Add to Wishlist

Install




Messenger is a FREE messaging app available for Android and other smartphones.




*The Dardesh app associated with Desert Scorpion.*

## The potential actor and who they target

Our current analysis strongly suggests Desert Scorpion is being deployed in targeted attacks against Middle Eastern individuals of interest specifically those in Palestine and has also been highlighted by other researchers. We have been able to tie the malware to a long-running Facebook profile that we observed promoting the first stage of this family, a malicious chat application called Dardesh via links to Google Play. The Lookout Threat Intelligence team identified that this same Facebook profile has also posted Google Drive links to Android malware belonging to the FrozenCell family attributed to APT-C-27. These factors, in combination with the fact that the command and control infrastructure used by Frozen Cell and Desert Scorpion resides in similar IP blocks, supports the theory that the same actor is responsible for operating, if not developing, both families.


Like
Follow
Share
Send Message
كلمات راقت لي
@kalmat1990
Home
Posts
Reviews
Videos
Photos
About
Community
Create a Page
كلمات راقت لي is at نابلس جبل النار.
March 3 at 11:56am · Nablus, Palestine ·
يرجى إرسال أي أسئلة لديكم إلينا عبر Messenger. ! شكرًا على تواصلكم معنا علىمرحبًا
تطبيق دردش. تواصلو معنا هنا
https://play.google.com/store/apps/details?id=com.dardesh.v1
See Translation
كلمات راقت لي
Publisher
Send Message
Always Open
Community
See All
Invite your friends to like this Page
5,086 people like this
5,119 people follow this
About
See All
Typically replies instantly
Send Message
play.google.com/store/apps/details?id=com.da
Publisher
Hours
Always Open
Suggest Edits
Pages liked by this Page
ضع بصمتك
Like
خواطر رحّال
Like
القادم اجمل بعون الله
Like
English (US) · Español · Português (Brasil) ·
Français (France) · Deutsch
Privacy · Terms · Advertising · Ad Choices


## What it does

The surveillance functionality of Desert Scorpion resides in a second stage payload that can only be downloaded if the victim has downloaded, installed, and interacted with the first-stage chat application. The chat application acts as a dropper for this second-stage payload app. At the time of writing Lookout has observed two updates to the Dardesh application, the first on February 26 and the second on March 28. The malicious capabilities observed in the second stage include the following:

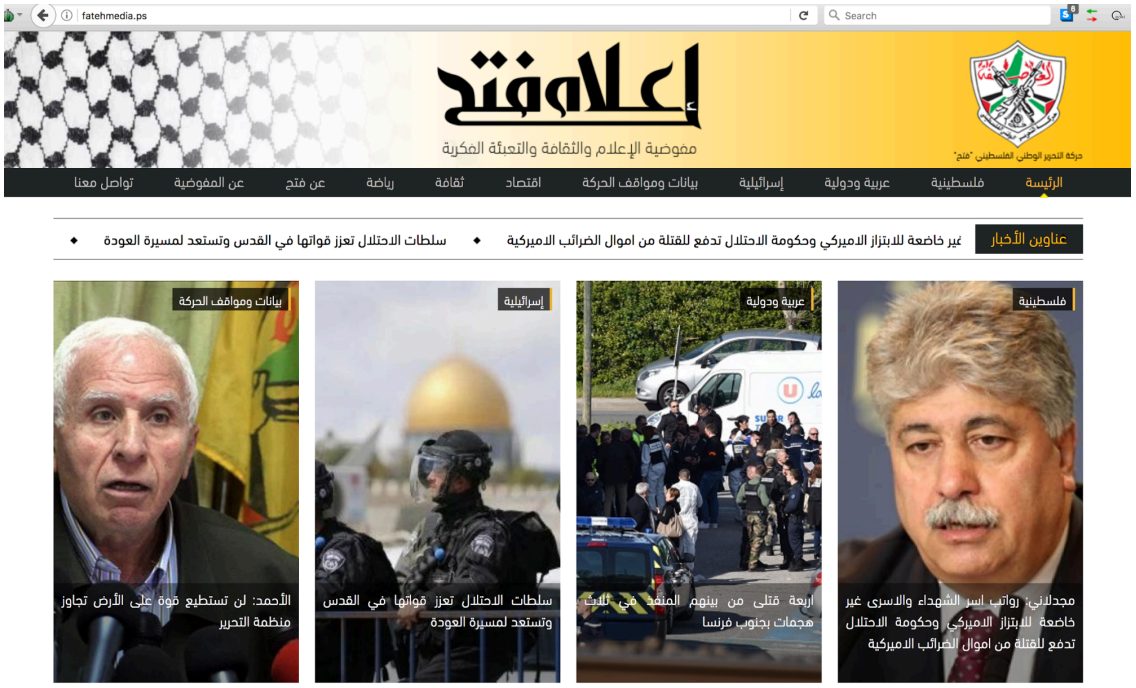
- Upload attacker-specified files to C2 servers
- Get list of installed applications
- Get device metadata
- Inspect itself to get a list of launchable activities
- Retrieves PDF, txt, doc, xls, xlsx, ppt, pptx files found on external storage
- Send SMS
- Retrieve text messages

- Track device location
- Handle limited attacker commands via out of band text messages

- Record surrounding audio
- Record calls
- Record video
- Retrieve account information such as email addresses
- Retrieve contacts
- Removes copies of itself if any additional APKs are downloaded to external storage.
- Call an attacker-specified number
- Uninstall apps
- Check if a device is rooted
- Hide its icon
- Retrieve list of files on external storage
- If running on a Huawei device it will attempt to add itself to the protected list of apps able to run with the screen off
- Encrypts some exfiltrated data

Desert Scorpion's second stage masquerades as a generic "settings" application. Curiously, several of these have included the world "Fateh" in their package name, which may be referring to the Fatah political party. Such references would be in line with FrozenCell's phishing tactics in which they used file names to lure people associated with the political party to open malicious documents. Desert Scorpion's second stage is capable of installing another non-malicious application (included in the second stage) which is highly specific to the Fatah political party and supports the targeting theory.


العاصفة
فتح
حركة التحرير الوطني الفلسطيني
إعلام فتح
مفوضية الإعلام والثقافة والتعبئة الفكرية




The Lookout Threat Intelligence team is increasingly seeing the same tradecraft, tactics, and procedures that APT-C-23 favors being used by other actors. The approach of separating malicious functionality out into separate stages that are later downloaded during execution and not present in the initial app published to the Google Play Store, combined with social engineering delivered via social media platforms like Facebook, requires minimal investment in comparison to premium tooling like Pegasus or FinFisher. As we've seen with actors like Dark Caracal, this low cost, low sophistication approach that relies heavily upon social engineering has still been shown to be highly successful for those operating such campaigns. Given previous operational security errors from this actor in the past which resulted in exfiltrated content being publicly accessible Lookout Threat Intelligence is continuing to map out infrastructure and closely monitor their continued evolution.

**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.

---