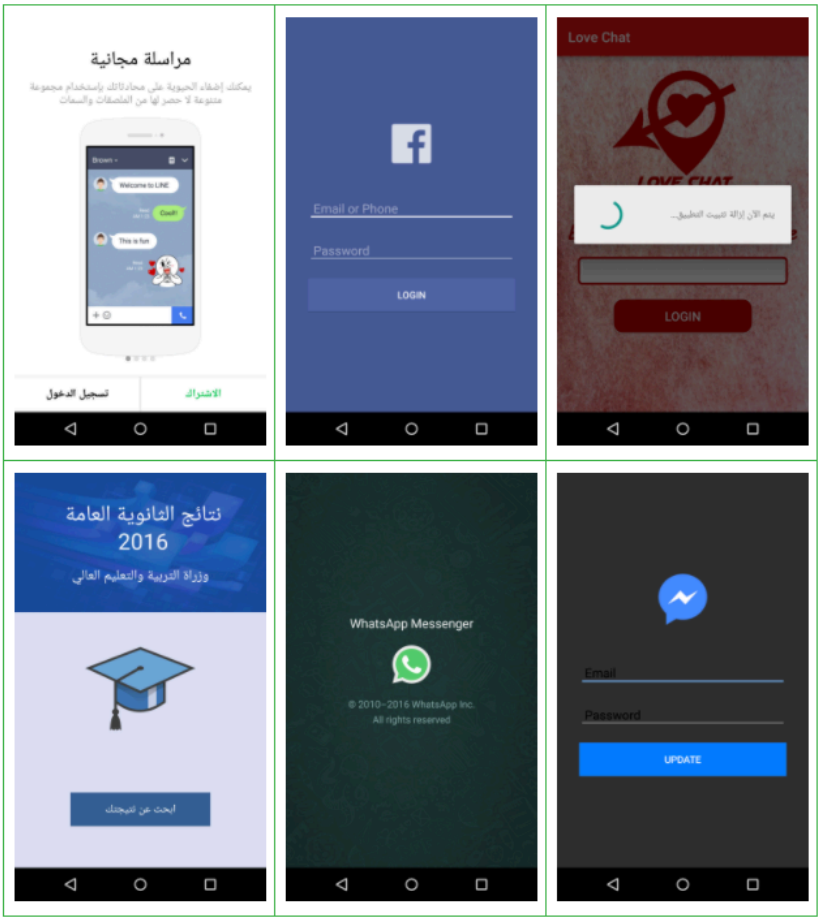
# FrozenCell: Multi-Platform Surveillance Against Palestinians

By Lookout

Published: 2017-10-05 · Archived: 2026-04-05 15:23:50 UTC




*FrozenCell has been seen masquerading as various well known social media and chat applications as well as an app likely only used by Palestinian or Jordanian students sitting their 2016 general exams.*

Lookout researchers have discovered a new mobile surveillanceware family, FrozenCell. The threat is likely targeting employees of various Palestinian government agencies, security services, Palestinian students, and those affiliated with the Fatah political party.

FrozenCell is the mobile component of a multi-platform attack we've seen a threat actor known as "Two-tailed Scorpion/APT-C-23," use to spy on victims through compromised mobile devices and desktops. The desktop components of this attack, previously discovered by Palo Alto Network, are known as KasperAgent and Micropsia. 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. We are continuing to watch it closely.

This threat is another proof point that attackers are clearly incorporating the mobile device into their surveillance campaigns as a primary attack vector. Government agencies and enterprises should look at this threat as an example of the kind of spying that is now possible given how ubiquitous mobile devices are in the workplace. Attackers are keenly aware of the information they can derive from these devices and are using multi-stage (phishing + an executable), multi-platform (Android + desktop) attacks to accomplish their spying.

All Lookout customers are protected from this threat.

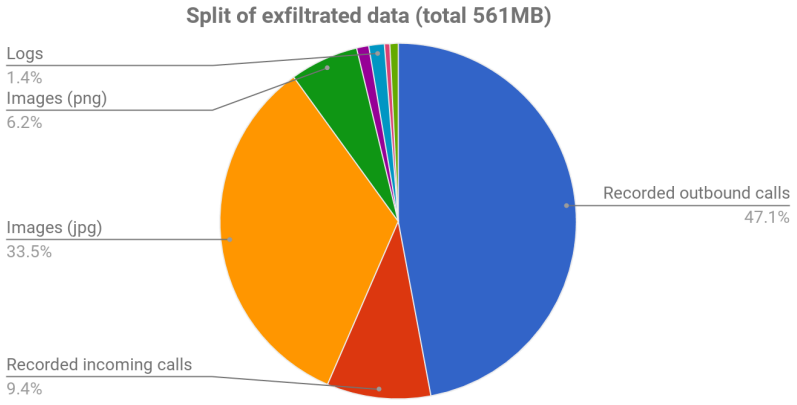
## What it does

FrozenCell masquerades as fake updates to chat applications like Facebook, WhatsApp, Messenger, LINE, and LoveChat. We also detected it in apps targeted toward specific Middle Eastern demographics. For example, the actors behind FrozenCell used a spoofed app called Tawjihi 2016, which Jordanian or Palestinian students would ordinarily use during their general secondary examination.

Once installed on a device FrozenCell is capable of:

- Recording calls
- Retrieving generic phone metadata (e.g., cell location, mobile country code, mobile network code)
- Geolocating a device
- Extracting SMS messages
- Retrieving a victim's accounts
- Exfiltrating images
- Downloading and installing additional applications
- Searching for and exfiltrating pdf, doc, docx, ppt, pptx, xls, and xlsx file types
- Retrieving contacts

The graph below represents a split of the types of data from only one misconfigured command and control server (out of over 37 servers). This is only a small picture of the threat actor's operations.




Some noteworthy files identified in content taken from compromised devices include passport photos, audio recordings of calls, other images, and a PDF document with data on 484 individuals. The PDF lists dates of birth, gender, passport numbers, and names.

## Potential targets

The actors behind FrozenCell used an online service that geolocates mobile devices based on nearby cell towers to track targets. This data shows a distinct concentration of infected devices beaconing from Gaza, Palestine.


*Early samples of FrozenCell used an online service for storing geolocation information of infected devices. Analysis of this telemetry 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.*

We were also able to link the FrozenCell's Android infrastructure to numerous desktop samples that are part of the larger multi-platform attack. It appears the attackers sent malicious executables though phishing campaigns impersonating individuals associated with the Palestinian Security Services, the General Directorate of Civil Defence - Ministry of the Interior, and the 7th Fateh Conference of the Palestinian National Liberation Front (held in late 2016). The titles and contents of these files suggest that the actor targeted individuals affiliated with these government agencies and the Fatah political party.

Some malicious files associated with these samples were titled the following:

- Council_of_ministres_decision
- Minutes of the Geneva Meeting on Troops (محضر اجتماع جنيف الخاص بقوات ا_من)
- Summary of today's meetings.doc.exe (ملخص إجتماعات اليوم)
- The most important points of meeting the memory of the late President Abu Omar may Allah have mercy on him - Paper No. 1 (أهم نقاط إجتماع ذكرى الرئيس الراحل أبوعمار رحمه الله - ورقة رقم)
- Fadi Alsalamin scandal with an Israeli officer - exclusive - watched before the deletion - Fadi Elsalameen (فضيحة فادى السلامين مع ضابط إسرائيلى- حصرى-شاهد وقبل الحذف-Fadi Elsalameen)
- The details of the assassination of President Arafat_06-12-2016_docx
- Quds.rar

Screenshots of some of the PDF contents:



Many of these executables are associated with various short links created using Bit.ly, a URL shortening service. After analyzing the traffic associated with these short links, we determined that each one was associated with a referral path from mail.mosa.pna.ps. MOSA is the Palestinian Directorate of Social Development whose mandate is to achieve comprehensive development, social security, and economic growth for Palestinian families, according to publicly available information on this ministry.

## Infrastructure

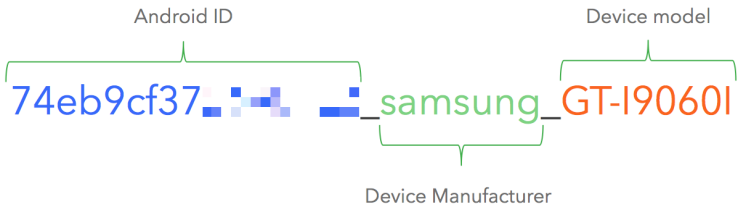
At the time of writing the following domains have either been used by this family or are currently active. We expect this list to grow given that this actor has changed its infrastructure numerous times in 2017.

cecilia-gilbert[.]comgooogel[.]orgmary-crawley[.]commydriveweb[.]comrose-sturat[.]infokalisi[.]xyzdebra-morgan[.]comarnani[.]infoacount-manager[.]infogooogel-drive[.]commediauploader[.]meacount-manager[.]netupload404[.]clubupload999[.]infoal-amalhumandevelopment[.]commargaery[.]coupload202[.]comgo-mail-accounts[.]comupload101[.]netsybil-parks[.]infodavos-seaworth[.]infoupload999[.]orgacount-manager[.]comlila-tournai[.]comaccount-manager[.]orgmediauploader[.]infokalisi[.]orgaryastark[.]infomavis-dracula[.]comkalisi[.]infogoogle-support-team[.]com9oo91e[.]comuseraccount[.]websiteaccounts-fb[.]comakashipro[.]comfeteh-asefa[.]comlagertha-lothbrok[.]info

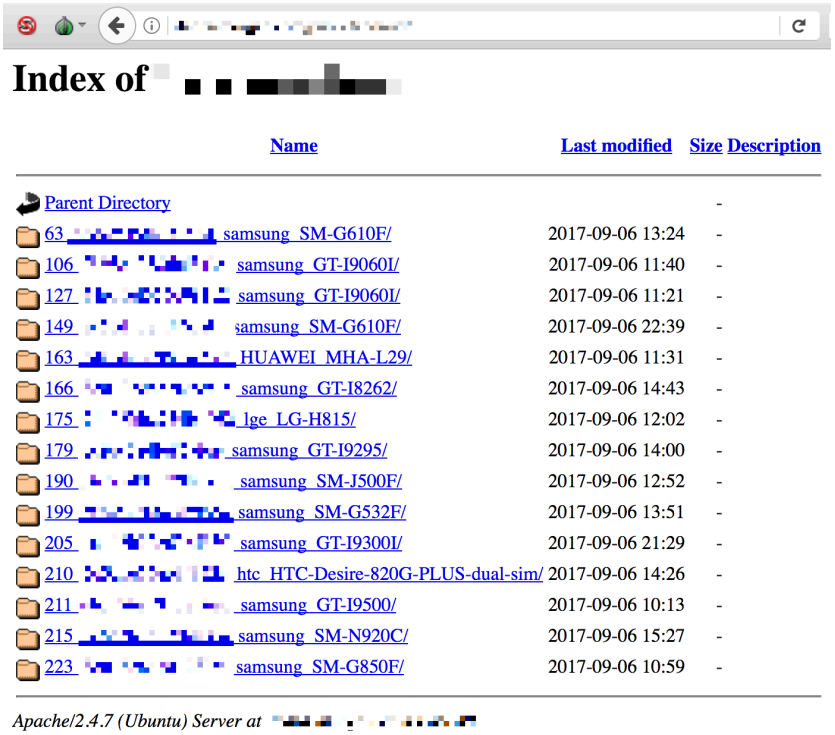
### OpSec fails and use of cryptography

While looking at this infrastructure, we identified that one of these domains has directory indexing enabled. This mistake in operational security allowed us to gain visibility into exfiltrated content for a number of devices. Continued mirroring suggests it is likely a regularly cleaned staging server. We sourced the over 561MB of exfiltrated data from this domain alone, all of which we found to be 7z compressed and password protected.

Password generation for compressed files takes place client-side with each device using a unique key in most scenarios. Key information consists of an MD5 hash of the device's Android ID, the device manufacturer, and the device model with each separated by an underscore. Visually, this can be represented as follows:




When combined with our analysis of indexed directories on C2 infrastructure, we were able to easily automate the generation of the password used by each device and, in turn, successfully decompress all exfiltrated content from compromised devices.



**Index of**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 63 samsung_SM-G610F/ | 2017-09-06 13:24 | - | |
| 106 samsung_GT-I9060I/ | 2017-09-06 11:40 | - | |
| 127 samsung_GT-I9060I/ | 2017-09-06 11:21 | - | |
| 149 samsung_SM-G610F/ | 2017-09-06 22:39 | - | |
| 163 HUAWEI_MHA-L29/ | 2017-09-06 11:31 | - | |
| 166 samsung_GT-I8262/ | 2017-09-06 14:43 | - | |
| 175 lge_LG-H815/ | 2017-09-06 12:02 | - | |
| 179 samsung_GT-I9295/ | 2017-09-06 14:00 | - | |
| 190 samsung_SM-J500F/ | 2017-09-06 12:52 | - | |
| 199 samsung_SM-G532F/ | 2017-09-06 13:51 | - | |
| 205 samsung_GT-I9300I/ | 2017-09-06 21:29 | - | |
| 210 htc_HTC-Desire-820G-PLUS-dual-sim/ | 2017-09-06 14:26 | - | |
| 211 samsung_GT-I9500/ | 2017-09-06 10:13 | - | |
| 215 samsung_SM-N920C/ | 2017-09-06 15:27 | - | |
| 223 samsung_SM-G850F/ | 2017-09-06 10:59 | - | |

*Apache/2.4.7 (Ubuntu) Server at*

While exfiltrated content is encrypted, information used to generate the password is plainly visible in the top level directories for each device. Taking this information from directory listings, like the one shown above, allowed for the decryption of all content. In this case, FrozenCell has primarily netted the actors behind it with recorded outbound calls followed closely by images and recorded incoming calls.

FrozenCell is part of a very successful, multi-platform surveillance campaign. Attackers are growing smarter, targeting individuals through the devices and the services they use most. Government agencies and enterprises should plan to be hit from all angles - cloud services, mobile devices, laptops - in order to build comprehensive security strategies that work.

### Indicators of Compromise (mobile)

**SHA1Package NameTitle**0ff709db71c63a925285ac109c7cd861f91363e3com.dev.chat.gochatGo
Chatfed082b2fd5687af48fb75245a55005d11f3551acom.app.chat.gochatGo
Chatddb148e8b700a08375b357d3be92fbb0bb11948dcom.dev.chat.gochatGo
Chatb9b0cded79369e84fc7cda1837d8c4019850f0fccom.facebook.updateFacebook
Updateba2caf83aa8667072bc23f904b684e628da1c7dccom.myapps.updateWhatsApp
Update7312db721b57a1d43ac520f617eac1798b5c1b3dcom.myapps.updateGoogle Play
Update8820f511e11f724f03a19174c9706e104dcbe6f3com.myapps.updateFacebook
Update2ff7f56726e41090c3ba16a5828114d1a5f8b6abcom.myapps.updateMessenger
Updateb3783f3a6c3bbec57fe588be6cab6483b165f99fcom.myapps.lineLINEc89f829f3a334bd4bd8d2bf7f5c7b2a5d82e63d2com.app.waupdateWhatsApp
Update30461be7eecfdc6d5638fdc6a43097aba1a2eedccom.wadev.appupdateWhatsApp
Update84d5ff14328d71d3fa3c03962734cc7179d2685ecom.myapps.updateFacebook
Update493a2d6129d9b2d0bbc49a5e07fb4123549b60dccom.app.waupdateWhatsApp

Update14841dd294bb1207f40d112377387b7d7e240ffecom.myapps.updateFacebook
Update9a74d68349fb5918c3c52b04cb0c011fc46000ebcom.app.fauFacebook
Updateceda754a6e6c034d1b8256c9ce7429ac0771c9e2com.dev.chat.lovechatLove
Chat125c380f573ff3e59290f313285d763939360c83com.app.waupdateWhatsApp
Update48a79ff5c9f711e86438aaf2335a28458ec02678com.app.updateWhatsApp
Update4a56b4968f2559459d98ab35a01a6b7b946d6ab8com.dev.updateFacebook
Update6d02734a39867f65948f01cc2c055b01fe83a252com.myapps.updateWhatsApp
Updateff675f6862fc4cb474f7e62406b1ad17d4128aefcom.facebook.updateFacebook
Update9b60a3513dcb53a12e67166ef6f721ad9d194a60com.facebook.updateFacebook
Update7877661025f315c7d1023c7e124756cab2a3f035com.mobile.updateFacebook
Updated098c57edc2eaaaac771deb0df1d00c1917cf92bcom.app.updateFacebook
Updateaf7552ad0794e9de4a33390b4669b941ef5b69c6com.dev.chat.lovechatLove
Chata5ee1f12a50d84d8283e9bfbec1050b989e07e78com.facebook.updateFacebook
Update1d3eccdf4fbd9ca548d85cdf3b6c6c813a3225aecom.askit.tawjihiTawjihi 2016

**Indicators of Compromise (desktop)**

**SHA1**5e706e34634cfb1fcae11ddf1260b540810b156590f93de55145b6577525421354ff05842cbe6271b53b01fccf08ceadc75f2041c00336c36cbc2ac4fe08

All these indicators can be found on AlienVault under the FrozenCell pulse.

---

Source: https://blog.lookout.com/frozencell-mobile-threat