Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:52:39 UTC

Tool: FrozenCell

Names	FrozenCell
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Lookout) 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
Information	<https://blog.lookout.com/frozencell-mobile-threat>
MITRE ATT&CK	<https://attack.mitre.org/software/S0577/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:FrozenCell>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool FrozenCell

Changed	Name	Country	Observed	
APT groups				
	Desert Falcons	[Gaza]	2011-Oct 2023	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=55a7b2c6-82a3-4d18-82ce-082a5c8da2c2