# FrozenCell, Software S0577 | MITRE ATT&CK®

Archived: 2026-04-02 12:00:00 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Mobile | T1532 | | Archive Collected Data | FrozenCell has compressed and encrypted data before exfiltration using password protected .7z archives.[1] |
| Mobile | T1429 | | Audio Capture | FrozenCell has recorded calls.[1] |
| Mobile | T1533 | | Data from Local System | FrozenCell has retrieved device images for exfiltration.[1] |
| Mobile | T1407 | | Download New Code at Runtime | FrozenCell has downloaded and installed additional applications.[1] |
| Mobile | T1420 | | File and Directory Discovery | FrozenCell has searched for pdf, doc, docx, ppt, pptx, xls, and xlsx file types for exfiltration.[1] |
| Mobile | T1430 | | Location Tracking | FrozenCell has used an online cell tower geolocation service to track targets.[1] |
| Mobile | T1655 | .001 | Masquerading: Match Legitimate Name or Location | FrozenCell has masqueraded as fake updates to chat applications such as Facebook, WhatsApp, Messenger, LINE, and LoveChat, as well as apps targeting Middle Eastern demographics.[1] |
| Mobile | T1636 | .004 | Protected User Data: SMS Messages | FrozenCell has read SMS messages for exfiltration.[1] |

| Domain | ID | Name | Use |
| --- | --- | --- | --- |
| Mobile | T1409 | Stored Application Data | FrozenCell has retrieved account information for other applications.[1] |
| Mobile | T1426 | System Information Discovery | FrozenCell has gathered the device manufacturer, model, and serial number.[1] |
| Mobile | T1422 | System Network Configuration Discovery | FrozenCell has collected phone metadata such as cell location, mobile country code (MCC), and mobile network code (MNC).[1] |

Source: https://attack.mitre.org/software/S0577/