# FluBot, Software S1067 | MITRE ATT&CK®

Archived: 2026-04-05 18:13:20 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Mobile | T1453 | | Abuse Accessibility Features | FluBot abuses accessibility features in three ways: steal application credentials, evade detection and removal, and send SMS for lateral movement.[4] |
| Mobile | T1517 | | Access Notifications | FluBot can access app notifications.[1] |
| Mobile | T1437 | .001 | Application Layer Protocol: Web Protocols | FluBot can use HTTP POST requests on port 80 for communicating with its C2 server.[1] |
| Mobile | T1637 | .001 | Dynamic Resolution: Domain Generation Algorithms | FluBot can use Domain Generation Algorithms to connect to the C2 server.[1] |
| Mobile | T1521 | .002 | Encrypted Channel: Asymmetric Cryptography | FluBot has encrypted C2 message bodies with RSA and encoded them in base64.[1] |
| Mobile | T1646 | | Exfiltration Over C2 Channel | FluBot can send contact lists to its C2 server.[1] |
| Mobile | T1628 | .002 | Hide Artifacts: User Evasion | FluBot can use `locale.getLanguage()` to choose the language for notifications and avoid user detection.[1] |
| Mobile | T1629 | .001 | Impair Defenses: Prevent Application Removal | FluBot can use Accessibility Services to make removal of the malicious app difficult.[2] |
| | | .003 | Impair Defenses: Disable or Modify Tools | FluBot can disable Google Play Protect to prevent detection.[1][3] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Mobile | T1417 | .002 | Input Capture: GUI Input Capture | FluBot can add display overlays onto banking apps to capture credit card information.[1] |
| Mobile | T1406 | | Obfuscated Files or Information | FluBot can obfuscated class, string, and method names in newer malware versions.[1] |
| Mobile | T1660 | | Phishing | FluBot has been distributed via malicious links in SMS messages.[3] |
| Mobile | T1636 | .003 | Protected User Data: Contact List | FluBot has used the contact list to infect more devices.[1][3] |
| | | .004 | Protected User Data: SMS Messages | FluBot can intercept SMS messages and USSD messages from Telcom operators.[1] |
| Mobile | T1604 | | Proxy Through Victim | FluBot can use a SOCKS proxy to evade C2 IP detection.[1] |
| Mobile | T1582 | | SMS Control | FluBot can send SMS phishing messages to other contacts on an infected device.[1][2] |
| Mobile | T1409 | | Stored Application Data | FluBot has collected credentials, banking details and other information from the victim device.[3] |

Source: https://attack.mitre.org/software/S1067