National Cyber Security Centre

2106011034-NCSC

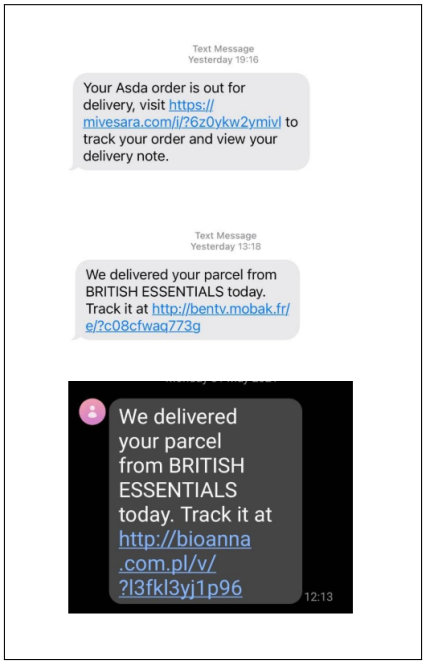
A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

FluBot - Android Text Message Scam
2021-06-01

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type	The NCSC has received reports of a spyware software labeled FluBot affecting Android users in Ireland. FluBot is used by malicious parties to steal passwords and sensitive data from the victims' mobile device. It will access victims' contacts and spread the malicious application through further text messages. The messages typically contain a link for the victim to click on to get details of a missed package delivery. This link will direct the victim to a fake website replicating the legitimate delivery companys site. The victim will then be asked to download two .apk files which are banking trojans. Users will then be prompted to manually override and allow an untrusted app download. The following are examples of FluBot text messages: 
Products Affected	Android devices. **Note:** Apple devices are not currently affected by this malware.
Impact	Data & financial loss
Recommendations	If you receive a message as described above the NCSC advises: • **DO NOT** click on the link, and delete the message. • If you are expecting a delivery, check it through the companies official website. • If you have clicked on the link and installed the app - perform a factory reset on the device. (**Note:** If you do not have backups you will lose data). • When restoring backups do not restore from any backups created **after** you installed the malicious app as these will be infected. • Reset passwords on any accounts used after you installed the app. If you use the same passwords on other accounts, change these also. • Ensure that the Google Play Protect service is switched on.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie