National Cyber Security Centre

2110142049-NCSC

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

NCSC Alert

FluBot - New Android Text Message Scam Targeting Irish Users 2021-10-28

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.*

Description

The NCSC is aware of the SpyWare malware known as FluBot affecting Android users in Ireland. The NCSC has previously released an Alert regarding FluBot in June 2021 - analysis of previous waves of this campaign suggests that Irish users may be targeted in the near future. FluBot is used by malicious parties to steal passwords and sensitive data from a victim's mobile device. It will access victims' contacts and spread the malicious application through further text messages.

The theme of this new campaign relates to voicemail messages, with a link for the victim to click to receive the voicemail. This link will direct a potential victim to a fake website where they will be prompted to install a new voicemail app in order to listen to a new message. The victim will then be asked to download a .apk file which is a banking trojan. Users will then be prompted to manually override and allow an untrusted app download. Figure 1 is an example of a FluBot text message:

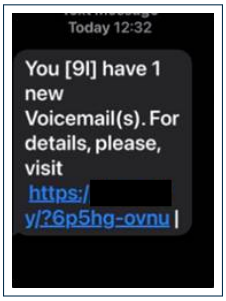
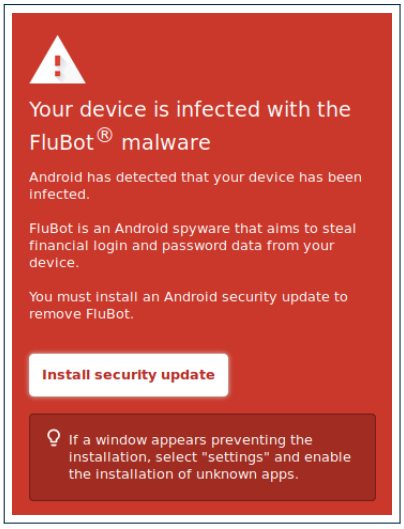


Figure 1: FluBot SMS

Figure 2, Figure 3 and Figure 4 below are examples of websites that FluBot directs a victim to:



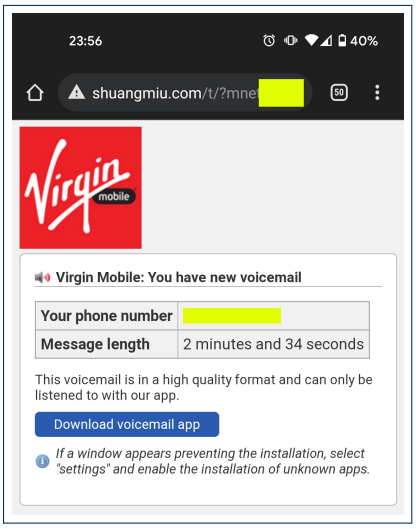


Figure 2 & 3: Websites Hosting Malicious App

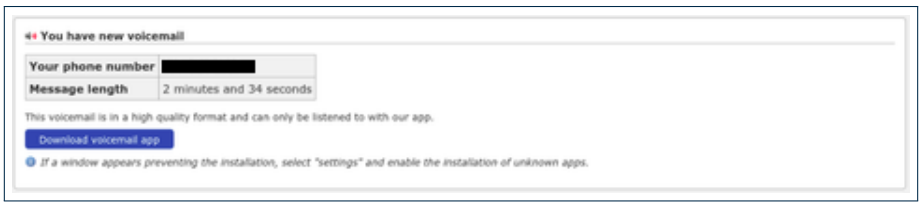


Figure 4: Website Hosting Malicious App

Products Affected

Android devices.

Note: Other mobile devices (Apple iPhones, Windows devices) can still receive the messages, however the malicious application is designed to only work with the Android operating system at this time.

Impact

Data & financial loss.

Recommendations

If you receive a message as described above the NCSC advises:

- **DO NOT** click on the link, never reply to the message, and delete the message immediately.
- Be wary of messages informing of a new voicemail with a link included.

If you have clicked on the link and/or installed an app:

- Perform a factory reset on the device. (**Note:** If you do not have backups you will lose data).
- If you have entered in your bank account details inform your bank immediately.
- Contact your mobile provider for further advice.
- 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.
- Review the BPFI FraudSMART advisory for further advice.

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