



Enquire Now

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)  
> Security (<https://www.bleepingcomputer.com/news/security/>)  
> FluBot Android malware targets Finland in new SMS campaigns

# FluBot Android malware targets Finland in new SMS campaigns

By **Bill Toulas** (<https://www.bleepingcomputer.com/author/bill-toulas/>)  
May 10, 2022 01:19 PM 0



Finland's National Cyber Security Center (NCSC-FI) has issued a warning about the FluBot Android malware infections increasing due to a new campaign that relies on SMS and MMS for distribution.

FluBot is looking to steal financial account credentials of its victims by overlaying phishing pages on top of the legitimate banking and cryptocurrency applications.

Additionally, it can access SMS data, perform phone calls, and monitor incoming notifications to snatch temporary authentication codes like one-time passwords (OTP), required besides the regular login credentials.



The Finnish authorities issued a similar warning last year after detecting the distribution of 70,000 malicious messages in just 24 hours (<https://www.bleepingcomputer.com/news/security/finland-warns-of-flubot-malware-heavily-targeting-android-users/>).

This time, no specific numbers have been provided, but the NCSC-FI stated ([https://www.kyberturvallisuuskeskus.fi/fi/varoitus\\_1/2022](https://www.kyberturvallisuuskeskus.fi/fi/varoitus_1/2022)) that "thousands of malicious messages are circulating" to potential victims.

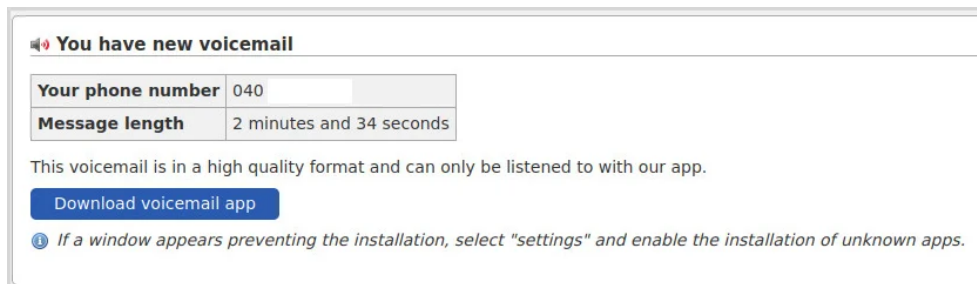
## SMS lures

The FluBot operators use SMS messages claiming to contain links to voicemail, missed call notifications, or alerts about incoming money from an unknown financial transaction.



Samples of FluBot SMS spotted in Finland (NCSC-FI)

The links in these messages take the victim to a website that hosts the FluBot APK, which the victims are asked to download and install to learn about the transaction details.



**Bogus voicemail alert urging the user to download an app (NCSC-FI)**

The application requests victims to grant risky permissions on Android, such as accessing SMS data, managing phone calls, and reading the user's address book.

Threat actors use the contacts list to push a second-wave SMS from compromised devices. Because these messages come from a known source, the recipients are more likely to open them and infect their devices.

The attackers don't waste any opportunity to monetize and if the malicious SMS reaches an iPhone user, they are redirected to premium subscription frauds and other scams.

NCSC-FI clarifies that simply opening the links does not install malware on your device, yet users should avoid installing APKs outside the official Play Store.

## What to do if infected

If your device is already infected with FluBot, a resetting the system to factory defaults should get rid of the malware. If you restore from a backup, it's important to make sure that it does not contain the malware.

If you suspect using a banking application after the infection, contact your bank and follow their instructions. Additionally, monitor all your transactions closely and report any fraudulent activities immediately.

It is also recommended to reset passwords for accounts used from the compromised device.

If you are an iPhone user who has inadvertently subscribed to premium services via a FluBot SMS, contact your carrier and request them to cancel the subscription. If possible, place a permanent ban on subscriptions to these services.

## Related Articles:

German automakers targeted in year-long malware campaign

(<https://www.bleepingcomputer.com/news/security/german-automakers-targeted-in-year-long-malware-campaign/>)

Ukraine warns of “chemical attack” phishing pushing stealer malware

(<https://www.bleepingcomputer.com/news/security/ukraine-warns-of-chemical-attack-phishing-pushing-stealer-malware/>)

Phishing attacks target countries aiding Ukrainian refugees

(<https://www.bleepingcomputer.com/news/security/phishing-attacks-target-countries-aiding-ukrainian-refugees/>)

EmoCheck now detects new 64-bit versions of Emotet malware

(<https://www.bleepingcomputer.com/news/security/emocheck-now-detects-new-64-bit-versions-of-emotet-malware/>)

Emotet botnet switches to 64-bit modules, increases activity

(<https://www.bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/>)

---

**ANDROID** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ANDROID/](https://www.bleepingcomputer.com/tag/android/))

**FINLAND** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FINLAND/](https://www.bleepingcomputer.com/tag/finland/))

**FLUBOT** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FLUBOT/](https://www.bleepingcomputer.com/tag/flubot/))

**MALWARE** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/](https://www.bleepingcomputer.com/tag/malware/))

**PHISHING** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/](https://www.bleepingcomputer.com/tag/phishing/))

**SMS** ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SMS/](https://www.bleepingcomputer.com/tag/sms/))

---