New FluBot Campaign Sweeps through Europe Targeting Android and iOS Users Alike

By Filip TRUȚĂ

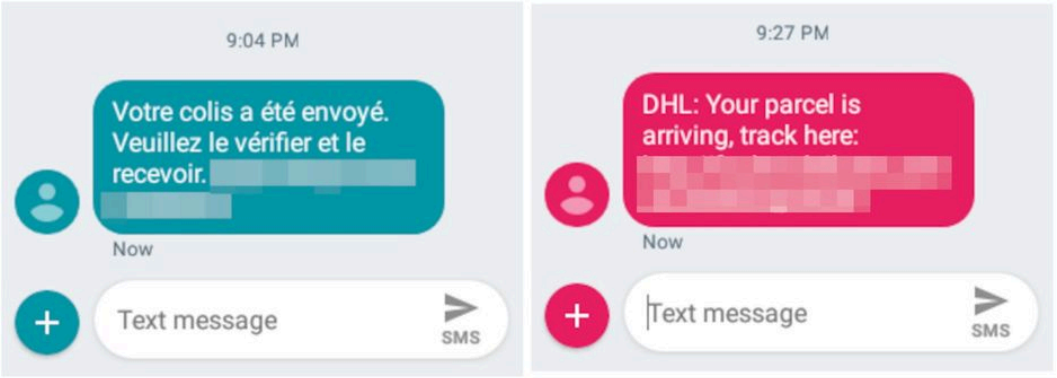
Archived: 2026-04-05 22:35:01 UTC

FluBot operators are targeting European countries with a renewed smishing campaign, leaping from one country to another in an intense push to sneak data-stealing malware onto people's phones.

Initially detected around Easter in Bitdefender's home country, Romania, the latest FluBot campaign uses the same smishing techniques as before: an SMS advertising fake content – typically a voice message. Android and iPhone users are receiving the texts in nearly equal doses this time, but Android users are still the primary target.

FluBot spares no one

It all starts with an SMS advertising fake content behind a tainted link.

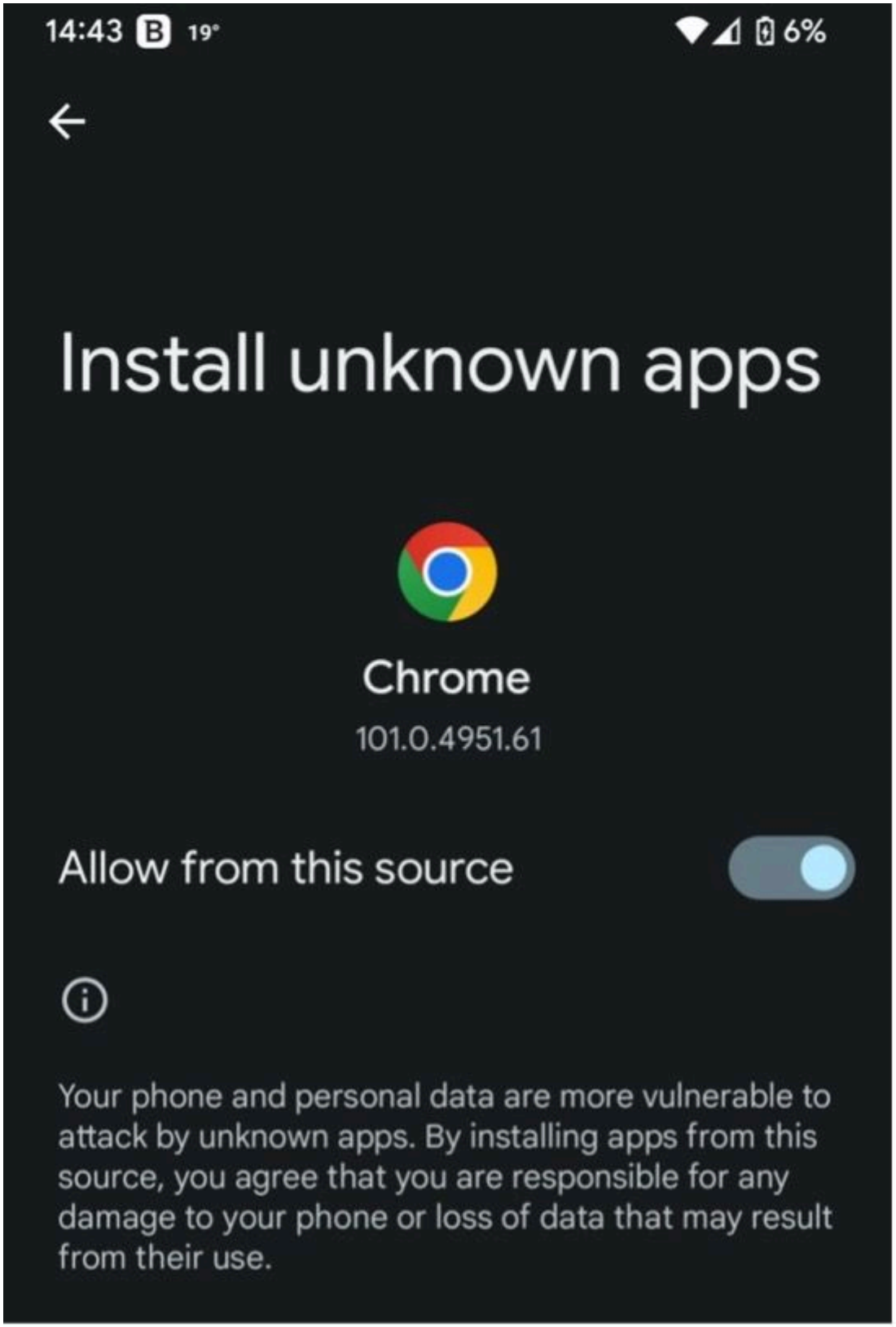


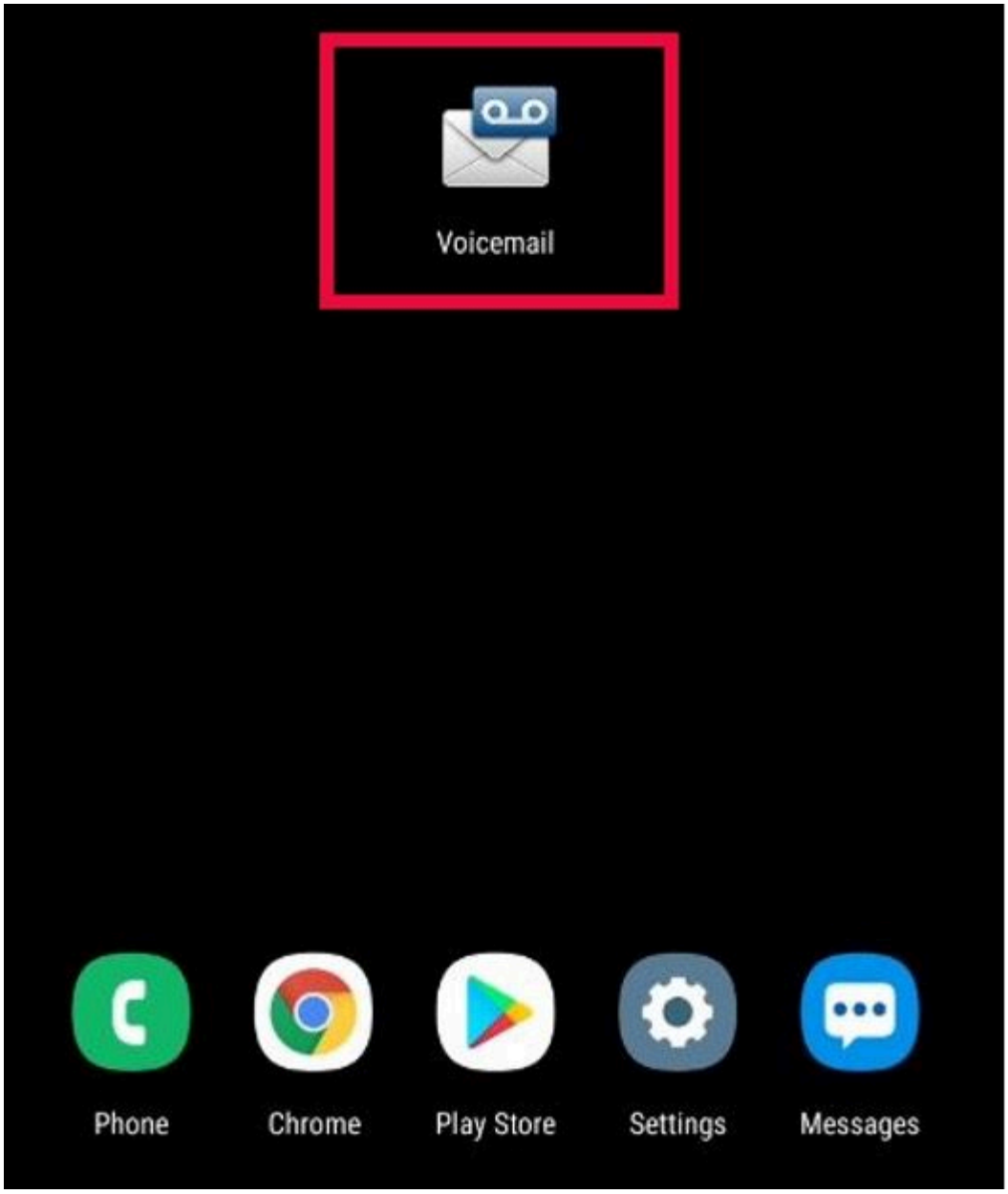
Credit: Bitdefender

Credit: kyberturvallisuuskeskus.fi

Credit: Bitdefender

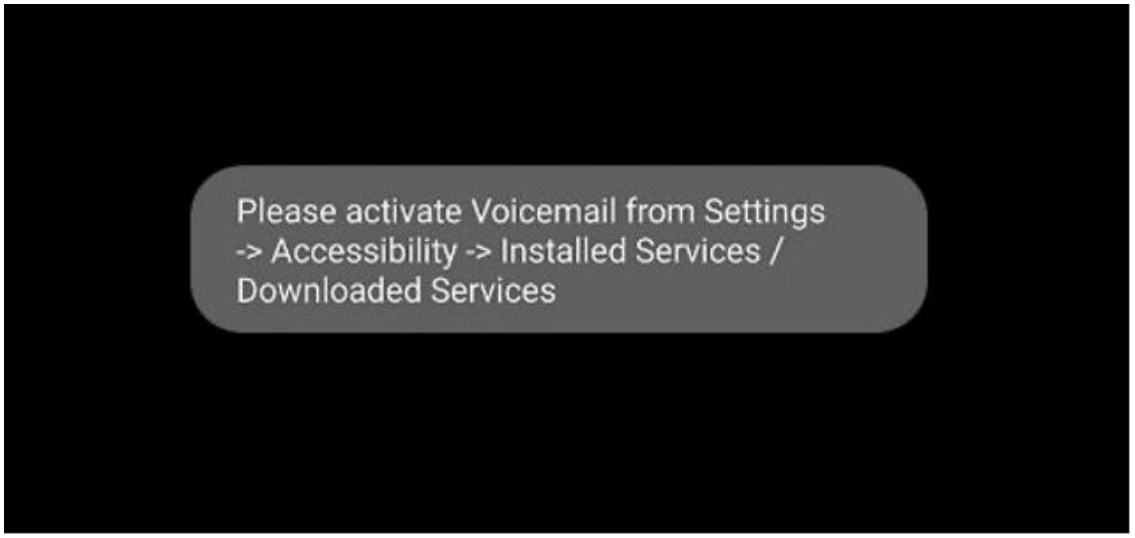
If users access the link, an installation prompt asks them for permission to install an unknown app – in this case, a fake Voicemail app purportedly required to listen to the voice message.


14:43
19°
6%
Install unknown apps
Chrome
101.0.4951.61
Allow from this source
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.



Credit: Bitdefender

The attackers' main objective here is to get users to install the FluBot banking trojan with their own hands. If the victim follows through with the instructions, the fake Voicemail app (FluBot) requests Accessibility permissions to give itself full access to areas of interest on the phone.

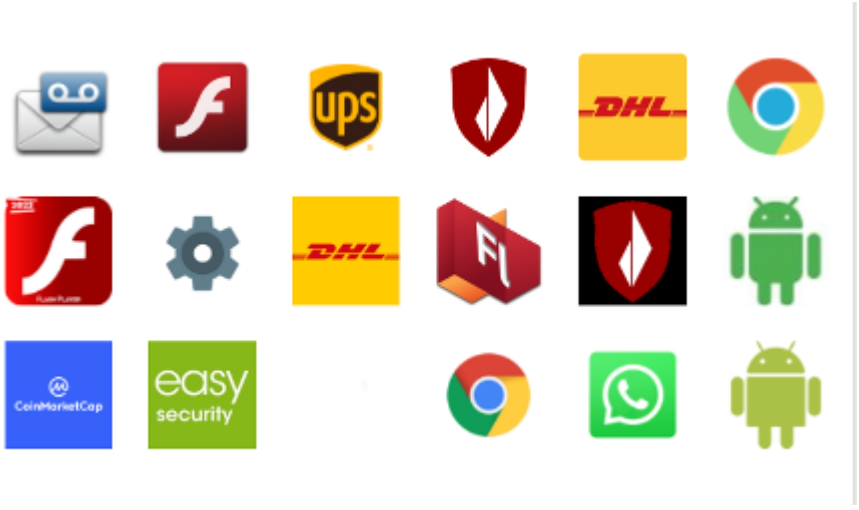


Credit: Bitdefender

If granted access, FluBot collects the victim's Contacts and uses the SMS app to continue spreading malicious links throughout the mobile ecosystem, all while stealing data and sending it to the C&C server. It also uses its Accessibility privileges to make it hard for the user to uninstall the app.

💡

A typical banking Trojan, FluBot is designed to siphon credit card information and credentials, enabling cybercriminals to not just steal money, but also to raid victims' various accounts. Here is a list of application icons that FluBot mimics.



Credit: Bitdefender

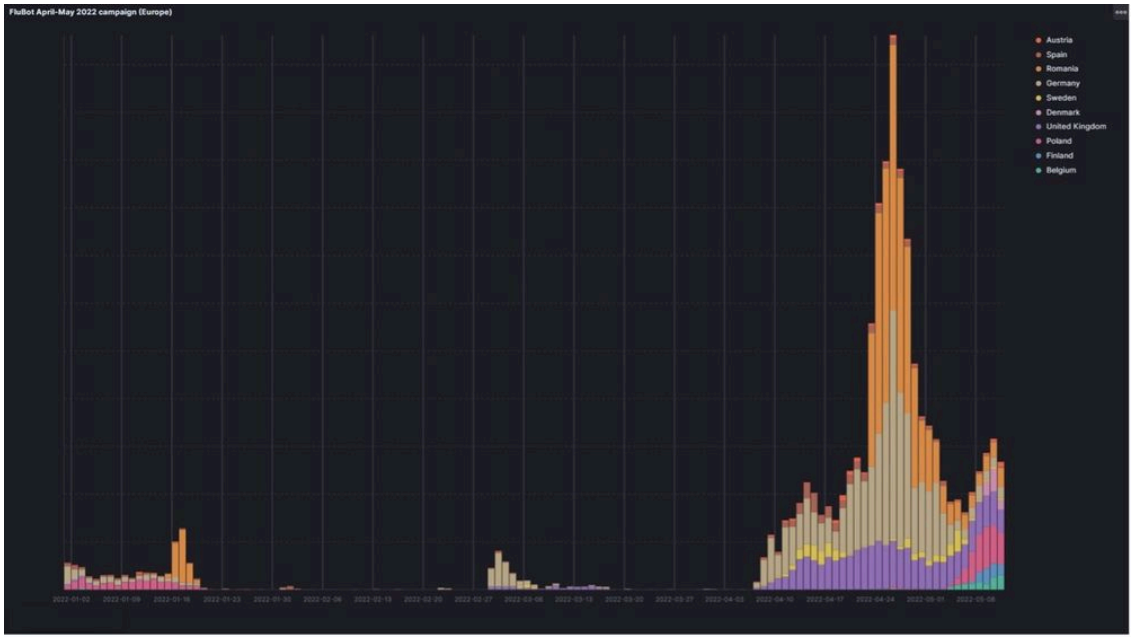
FluBot doesn't run on iOS. But when iPhone owners access the infected links, they are redirected to phishing sites and subscription scams. In the example below, a typical survey scam unfolds. Victims are encouraged to answer a few market research questions for a *guaranteed* iPhone 13.


WhatsApp
18:37
48%
AA
Loading...
Please wait. This won't take long.

Credit: Bitdefender

Most of Europe targeted

Following the Easter campaign unfolding in Romania, Bitdefender started monitoring FluBot activity more closely across the Old Continent and noticed a considerable spike in April-May.

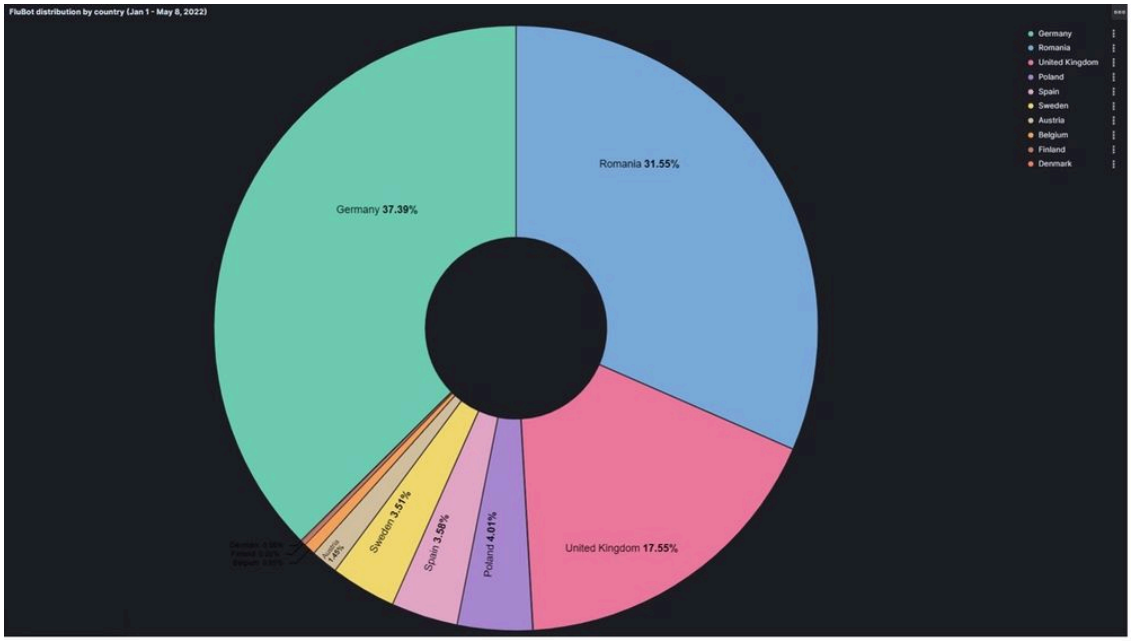


Spike in FluBot activity (Europe). Credit: Bitdefender

This coincides with reports not just from Romania, but from Finland as well. Fins are at their second major run-in with FluBot in six months. Both campaigns have seen highly localized messages with decent wording, suggesting that FluBot operators are investing more time and effort to expand their reach – in terms of both platform and language.

Finland spike in FluBot. Credit: Bitdefender

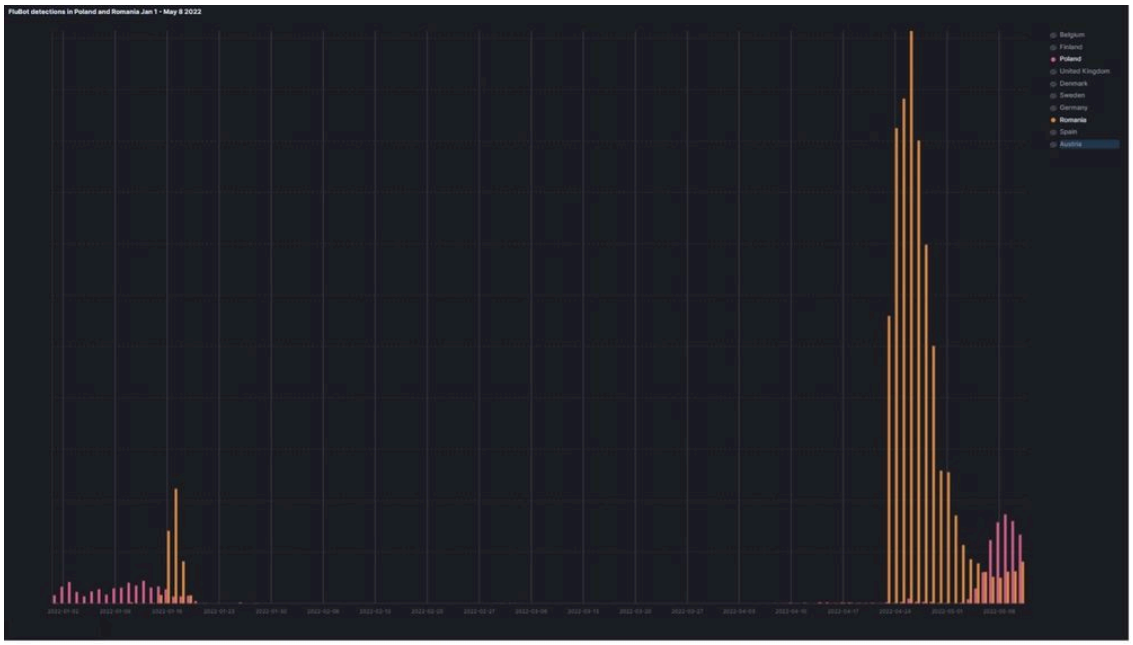
This time, most of Europe is targeted in a concerted effort from FluBot operators. The most targeted countries are Germany, Romania, UK, Poland, Spain, Sweden, Austria, Finland, and Denmark. Romania and Germany are by far the most-targeted regions in this rejuvenated FluBot campaign, with a combined 69% share, as the chart below shows.



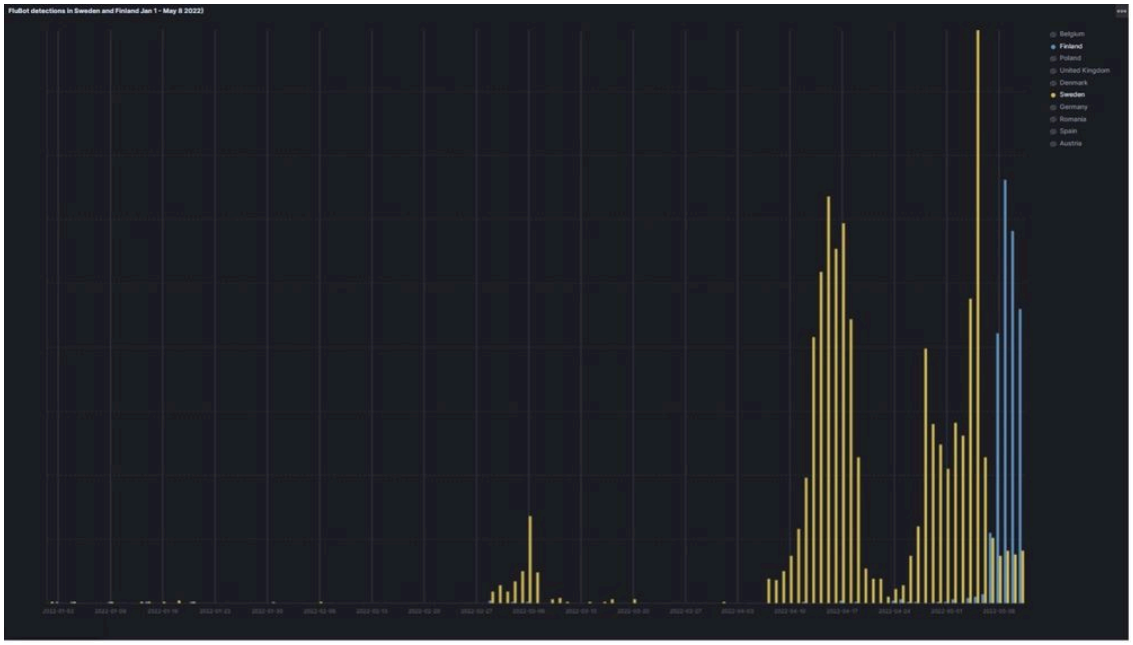
Top targeted regions. Credit: Bitdefender

While multiple regions were hit around the same time, placing random pairs of countries side by side shows more clearly that attack peaks don't actually coincide. This suggests that individual, localized campaigns were programmed from the start.

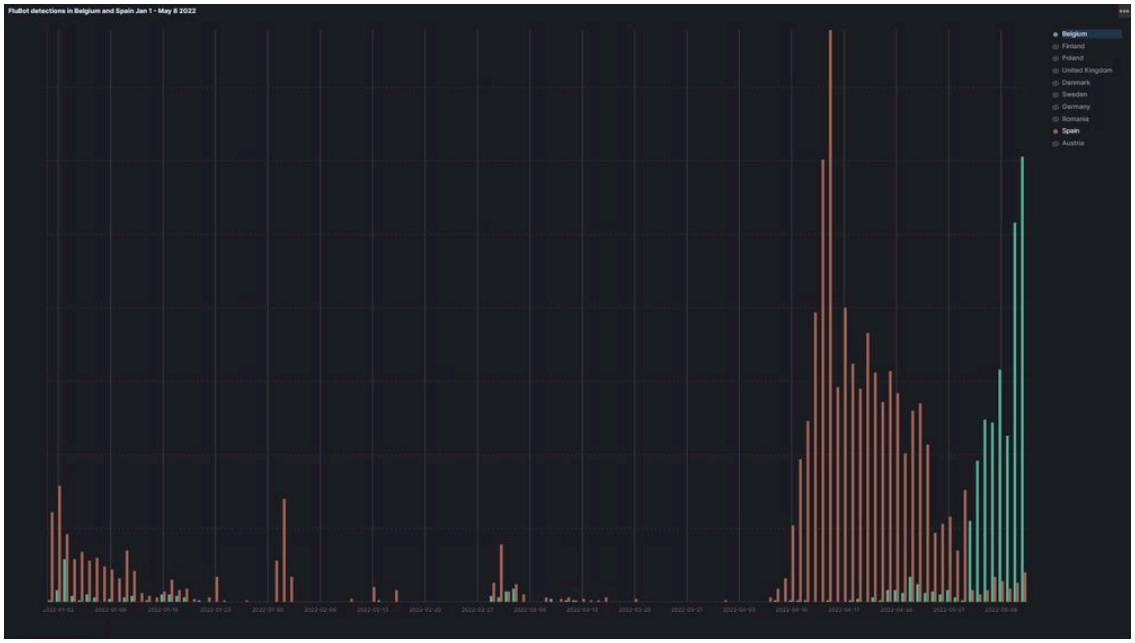
For example, detections started ramping up in Poland just as attacks were dwindling in Romania.



Fins and Swedes were targeted in a similar fashion, with detections in Sweden dwindling as the Finland campaign started ramping up.



Belgium and Spain offer more examples of this behavior.



All in all, FluBot operators seem to be concentrating on localizing smaller, individual campaigns on individual countries.

Likely not the last of FluBot we'll see this year

Despite arrests of multiple people suspected of operating the malware, FluBot campaigns have actually intensified in recent times, meaning there's no reason not to expect more waves of attacks in the future. In fact, due to this aggressive campaign, we could say FluBot is helping raise awareness about smishing as an attack avenue. At Bitdefender, we are pushing on multiple fronts to raise awareness of this social engineering attack vector.

Because FluBot activity is rising, Bitdefender highly recommends that users install a security solution capable of detecting not just FluBot itself, but also any social engineering vector designed to deploy malware. Your security app must be able to nip the problem in the bud.

With the new Scam Alert feature, **Bitdefender Mobile Security for Android** thwarts smishing attacks before users even interact with the malicious content.

Bitdefender Mobile Security for iOS also protects iPhone users against campaigns commanded by FluBot operators, steering them clear of any incoming phishing or fraudulent links.

Source: https://www.bitdefender.com/blog/labs/new-flubot-campaign-sweeps-through-europe-targeting-android-and-ios-users-alike/