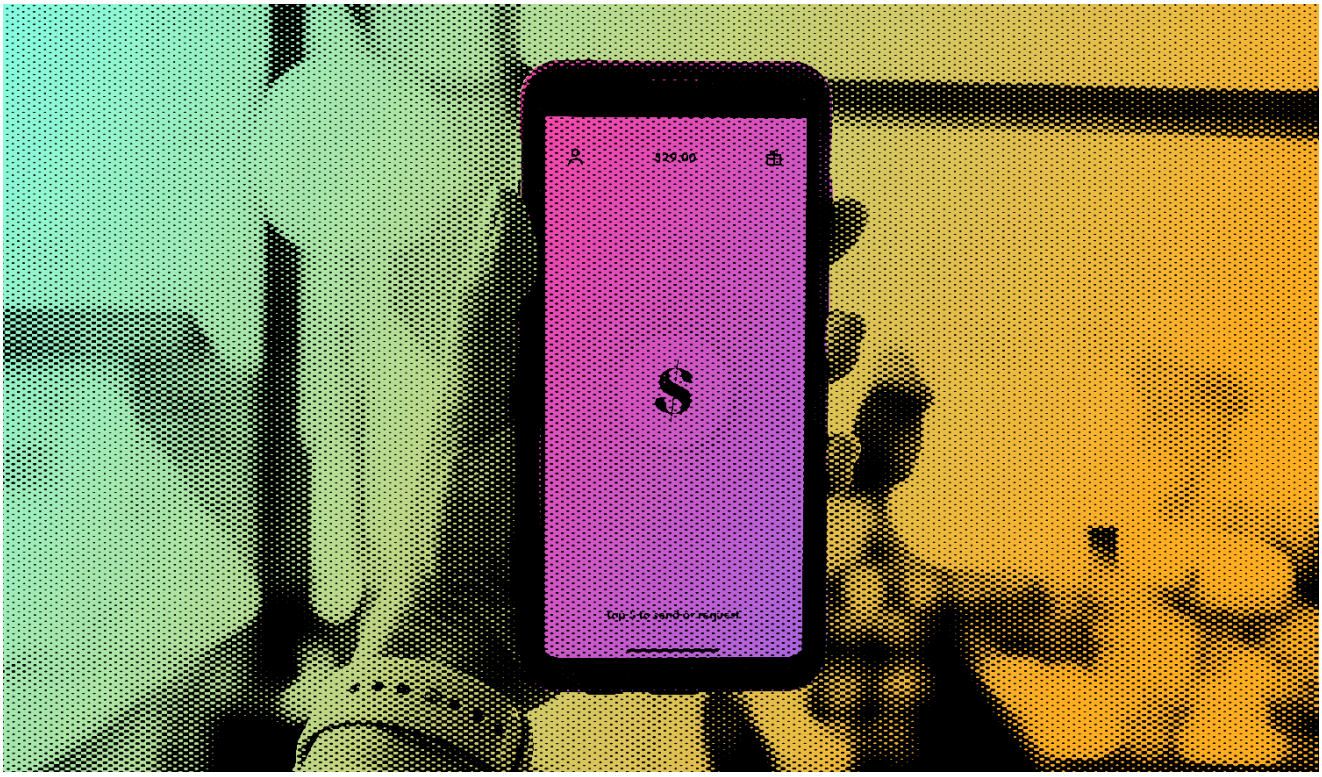
Despite arrests in Spain, FluBot operations explode across Europe and Japan

therecord.media/despite-arrests-in-spain-flubot-operations-explode-across-europe-and-japan/

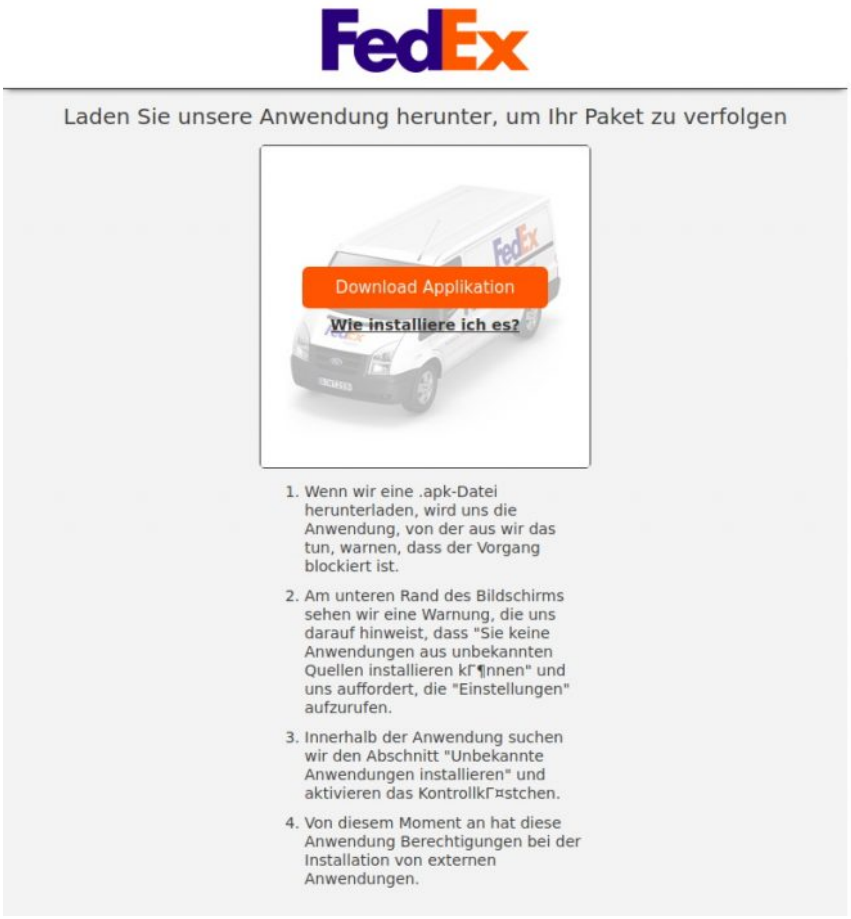
April 26, 2021



Cyber-security agencies in Germany and the UK warned the general public this month about a spike in SMS spam messages spreading the FluBot Android malware.

In security alerts published by Germany's Federal Office for Information Security (BSI) and the UK National Cyber Security Centre (NCSC), the two agencies said that malware gangs are sending malicious links to users via SMS posing as legitimate package delivery services.

If users click the links, they are taken to a website posing as DHL or FedEx, where they are told to install an app to track a parcel meant to be delivered at their location.



But BSI and NCSC officials say the apps are loaded with a new form of Android malware known as FluBot, Cabassous, or the FedEx Banker.

First seen at the end of last year, this malware has slowly become one of the most active operations in the Android cybercrime ecosystem.

Categorized as a classic Android banking trojan, the malware operates by relying on users downloading boobytrapped apps from the internet and then side-loading them on their devices, despite repeated security warnings from the Android OS.

Once a device is infected, the app uses the Android Accessibility service to overlay fake login screens on top of official apps and collect users' credentials, which it then sends to a remote command and control server.

The FluBot operators then use the collected credentials to access banking apps and empty accounts. Since the FluBot operators have full control over an infected device, they can also easily bypass any SMS-based two-step verification process.

One FluBot distributor gang arrested in Spain

Currently, the malware is advertised on underground cybercrime forums, where miscreants rent it and then distribute it to users across the world.

In fact, the first time we heard about this malware is after one of these FluBot distributor groups launched a massive SMS spam campaign that targeted Spanish users and infected more than 60,000 devices.

But while Spanish authorities reacted promptly and arrested four suspects believed to have been involved with this campaign, other groups renting the FluBot malware are still at large and appear to have launched their own operations targeting German and UK users as well.

Now, in an attempt to avoid similar incidents like the one in Spain, where the malware made tens of thousands of victims in the span of a few weeks, German and UK cybersecurity officials are trying to raise awareness of this new threat before it is too late.

Expansion beyond Spain, Germany, and the UK in the works

However, more cybersecurity agencies might soon need to warn their own users as well.

New intelligence shared this week suggests that FluBot distributors have already expanded operations and have launched SMS spam campaigns targeting users in other countries, including Japan, Italy, Norway, Sweden, Finland, Denmark, Poland, and the Netherlands.

> #Cabassous (#FluBot) actors are heavily developing new overlay targets and also performing an environmental checks (av) before it executing the banker payload. Interesting new countries and developments coming from this private group in such a short period of time. pic.twitter.com/0pWXHaMa1j
>
> — ThreatFabric (@ThreatFabric) April 26, 2021

> First time to see a Japanese flavor version of #FluBot.
> FYI @papa_anniekey @bl4ckh0l3z https://t.co/ujgxoBEDee pic.twitter.com/5qfBr7BQdj
>
> — にのせき (@ninoseki) April 26, 2021

Tags

- Android
- Android malware
- Cabassous
- DHL
- Europe
- FedEx
- FluBot
- Germany
- Japan
- malware
- NCSC

- smartphone

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.