FluBot Malware Gang Arrested in Barcelona

therecord.media/flubot-malware-gang-arrested-in-barcelona/

March 8, 2021

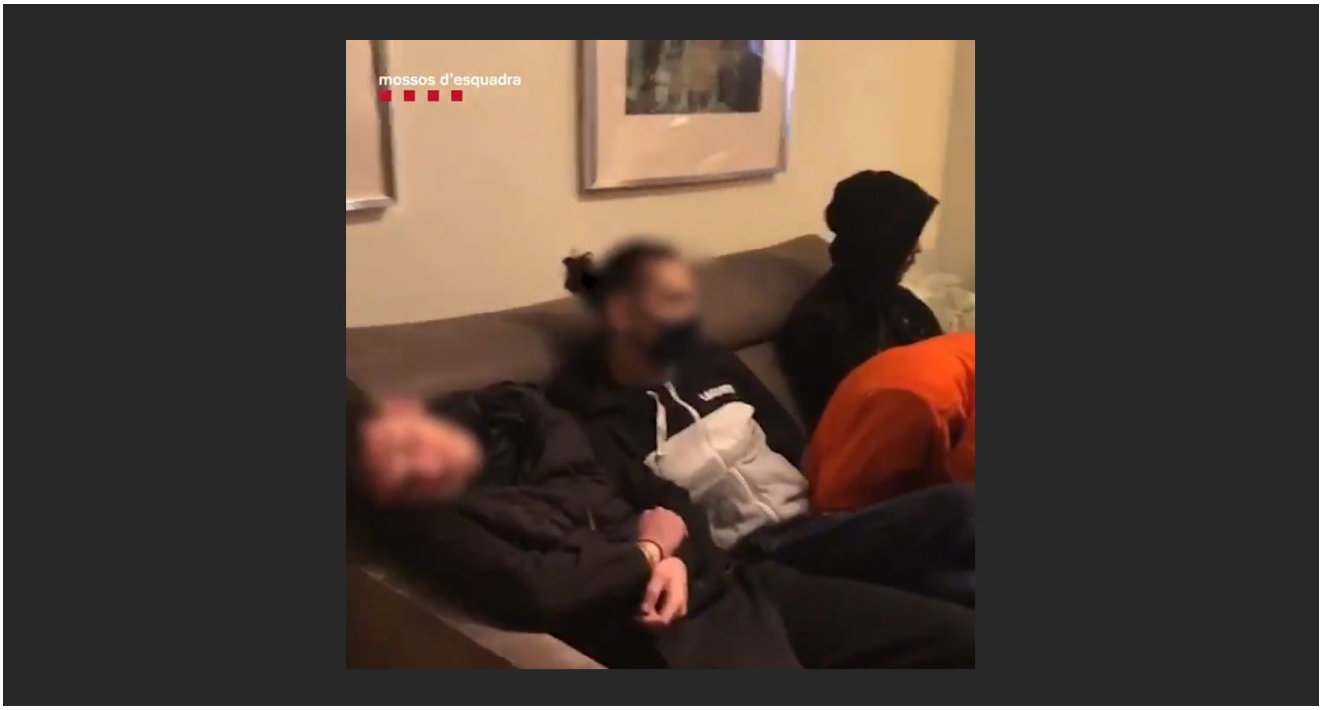

Image: Mossos d'Esquadra

Catalan police arrested four suspects last week on suspicion of distributing FluBot, an Android malware strain that infected at least 60,000 devices, with most victims located in Spain.

Four men, aged between 19 and 27, were arrested in Barcelona on Tuesday, March 2.

Members of the Mossos d'Esquadra (the local Catalan government's police force) raided the suspects' apartments and seized cash, laptops, documents, and mobile devices. Some of the mobile devices were still sealed and were allegedly bought with their victims' money, officials said.

> Desmantellem grup criminal especialitzat en l'#Smishing o l'estafa amb missatges SMS, amb els quals obtenien dades bancàries i del telèfon mòbil de les víctimes. Dos dels integrants, que formaven la cúpula, ja són a presó pic.twitter.com/d2XiWa0rCP
>
> — Mossos (@mossos) March 5, 2021

The suspects were arraigned in front of a judge on Thursday, March 4. Two members, deemed the leaders of the gang, were detained, while the other two were set free but required to appear in court every 15 days.

Suspect names were not released, according to local data privacy regulations; however, Catalan police said that one of the two FluBot gang leaders appeared to have been in charge of the technical side of the operation, being the one who wrote the malware code and created fake bank login pages.

97% of FluBot's victims were located in Spain

The FluBot malware, also known as the Fedex Banker or Cabassous, has been active since late 2020. The malware was designed as a banking trojan for Android devices. It would infect devices and abuse the Android Accessibility service to show fake login screens for mobile banking portals.

The malware would collect banking credentials and send the data back to its command and control server. Here, the FluBot gang would abuse the credentials and the full control they had over victim devices to access bank accounts, intercept and bypass bank verification codes, and steal funds from victims' accounts.

"In addition to making money transfers, the perpetrators made purchases of high-end cell phones with the victims' cards, which were sent to people living in the province of Madrid, to whom the scammers paid to receive the packages," Mossos d'Esquadra also added on Friday.

To spread to new victims, the malware relied on sending SMS spam messages to an infected user's contacts list. Catalan officials said they tracked at least 71,000 spam SMS messages sent by the group.

However, the number is believed to be much larger. In a report last week, Swiss security firm PRODAFT said that after managing to gain access to FluBot's command and control server, they tracked the malware to 60,000 devices and discovered that the FluBot operators had collected phone numbers for 11 million users, 97% of which were Spanish citizens.

The number represented around 25% of Spain's population. In an interview last week, PRODAFT told *The Record* their discovery prompted them to report their findings to Spanish law enforcement, which would explain last week's crackdown against the FluBot gang.

In the meantime, security researchers reported that the malware appears to be still active and spreading. The malware is advertised in underground hacking forums and its creators are believed to be still at large.

> Looks like it isn't dead after all. Even after succesful police intervention #Flubot campaing is still going, eh? @B0rys_Grishenko @500mk500 @CERT_OPL @PPiekutowski
>
> — Piotr Kowalczyk (@pmmkowalczyk) March 7, 2021

Tags

- Android
- Android malware
- arrest
- banking trojan
- FluBot
- police
- smartphone
- Spain

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.