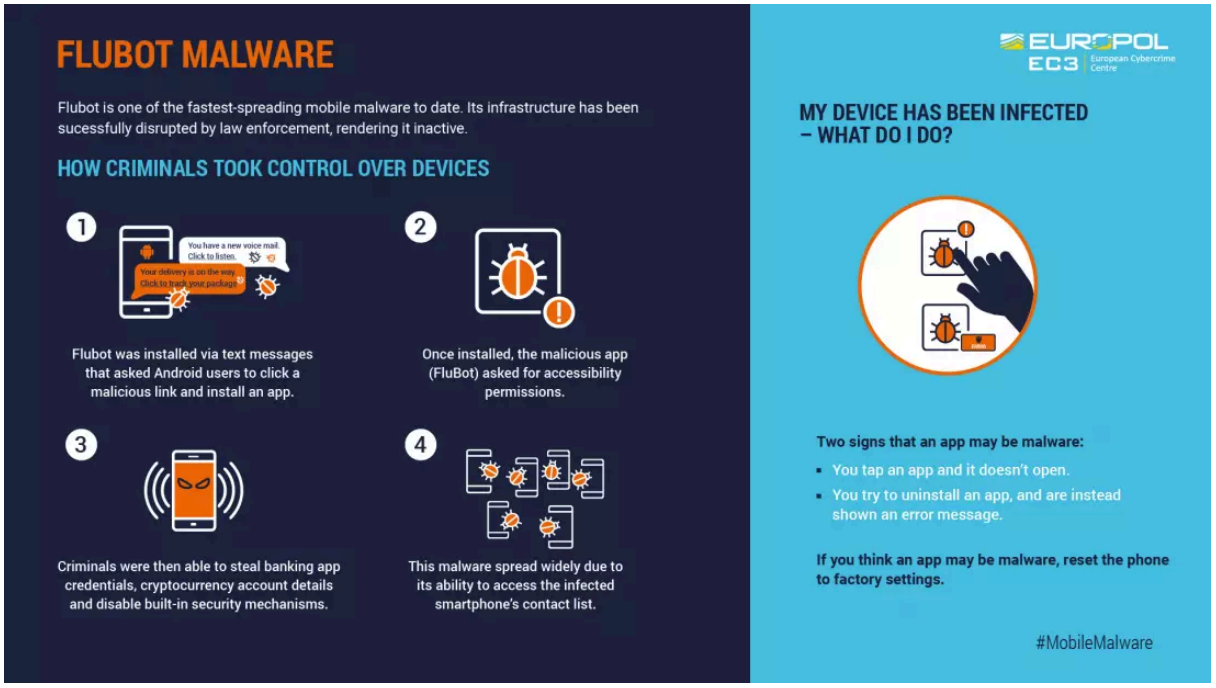
Takedown of SMS-based FluBot spyware infecting Android phones

By Europol

Published: 2022-06-01 · Archived: 2026-04-02 12:25:03 UTC

An international law enforcement operation involving 11 countries has resulted in the takedown of one of the fastest-spreading mobile malware to date. Known as FluBot, this Android malware has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world. Its infrastructure was successfully disrupted earlier in May by the Dutch Police (Politie), rendering this strain of malware inactive.

- 

- 

This technical achievement follows a complex investigation involving law enforcement authorities of Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands and the United States, with the

coordination of international activity carried out by Europol's European Cybercrime Centre (EC3).

The investigation is ongoing to identify the individuals behind this global malware campaign.

Here is how FluBot worked

First spotted in December 2020, FluBot has gained traction in 2021 and compromised a huge number of devices worldwide, including significant incidents in Spain and Finland.

The malware was installed via text messages which asked Android users to click a link and install an application to track to a package delivery or listen to a fake voice mail message. Once installed, the malicious application, which actually was FluBot, would ask for accessibility permissions. The hackers would then use this access to steal banking app credentials or cryptocurrency account details and disable built-in security mechanisms.

This strain of malware was able to spread like wildfire due to its ability to access an infected smartphone's contacts. Messages containing links to the FluBot malware were then sent to these numbers, helping spread the malware ever further.

This FluBot infrastructure is now under the control of law enforcement, putting a stop to the destructive spiral.

International police cooperation

With cases spreading across Europe and Australia, international police cooperation was central in taking down the FluBot criminal infrastructure.

Europol's European Cybercrime Centre brought together the national investigators in the affected countries to establish a joint strategy, provided digital forensic support and facilitated the exchange of operational information needed to prepare for the final phase of the action. The J-CAT, hosted at Europol, also supported the investigation. A virtual command post was also set up by Europol on the day of the takedown to ensure seamless coordination between all the authorities involved.

My device has been infected – what do I do

FluBot malware is disguised as an application, so it can be difficult to spot. There are two ways to tell whether an app may be malware:

- If you tap an app, and it doesn't open
- If you try to uninstall an app, and are instead shown an error message

If you think an app may be malware, reset the phone to factory settings.

Find out more on how to protect yourself from mobile malware.

The following authorities took part in the investigation:

- Australia: Australian Federal Police
- Belgium: Federal Police (Federale Politie / Police Fédérale)

- Finland: National Bureau of Investigation (Poliisi)
- Hungary : National Bureau of Investigation (Nemzeti Nyomozó Iroda)
- Ireland: An Garda Síochána
- Romania: Romanian Police (Poliția Română)
- Sweden: Swedish Police Authority (Polisen)
- Switzerland: Federal Office of Police (fedpol)
- Spain: National Police (Policia Nacional)
- Netherlands: National Police (Politie)
- United States: United States Secret Service
