EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:

Information stealers

Trojans

Ransomware

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

What made Emotet so dangerous?

Long lasting — Started as a banking Trojan in 2014, evolving over time.

Go-to-solution for criminals — It acted as a door opener for other computers, allowing unauthorised access to other malware families.

Polyphormic — It changed its code each time it was called up.

Resilient — Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.

Protect yourself from malware

Always check your emails carefully and watch out for:

attachments or embedded links from unknown senders.

messages with a sense of urgency asking you to download something.

offers with a promise of reward that sounds too good to be true.