Over 780,000 email accounts compromised by Emotet have been secured

therecord.media/over-780000-email-accounts-compromised-by-emotet-have-been-secured/

July 12, 2021

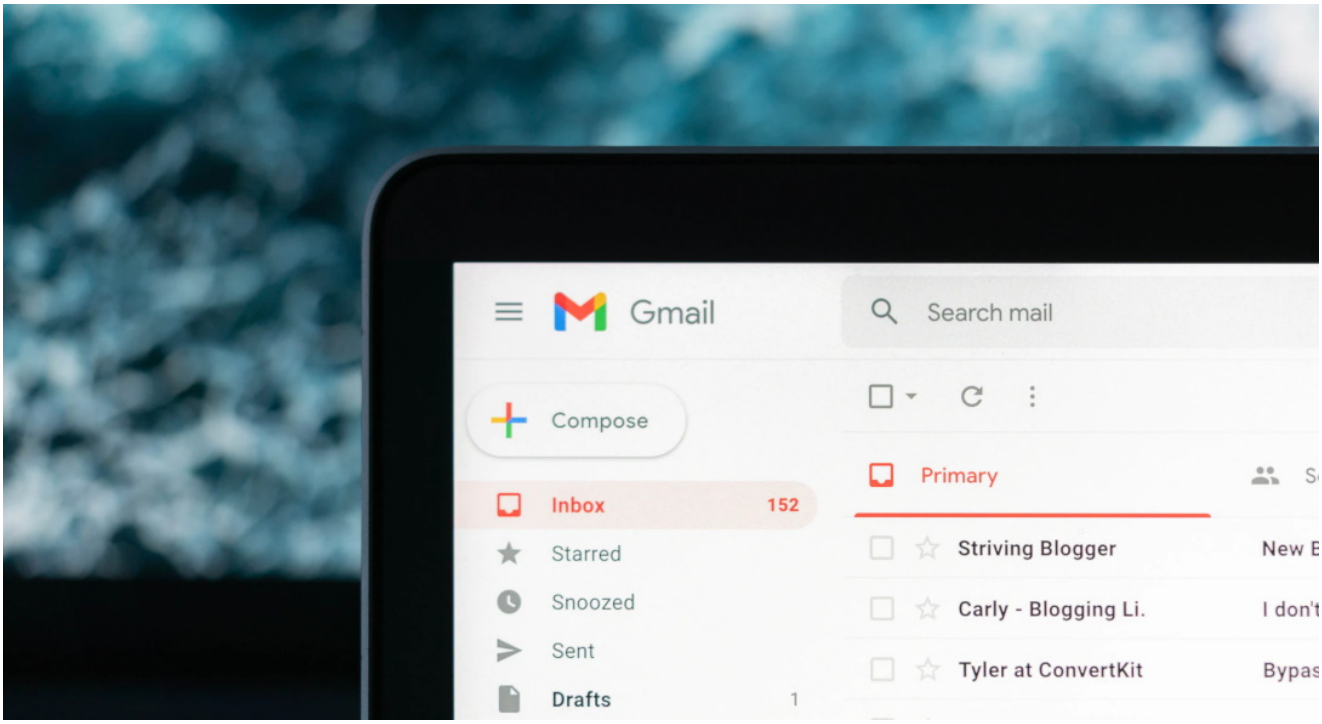

Image: Striving Blogger // Unsplash

More than 780,000 email accounts compromised by the now-defunct Emotet malware gang have been re-secured by their respective owners, cybersecurity organization Spamhaus said last month.

- The email accounts were compromised after users were tricked into infecting their computers with the Emotet malware.
- Using automated scripts, the Emotet malware dumped passwords from browsers and email clients, accessed victims' email accounts, and hijacked old email threads by sending new messages to known contacts containing malicious Office documents laced with malware in order to make new victims.
- When authorities seized and shut down the servers used by the Emotet gang in January 2021, they also gained access to the list of emails the criminal group had been using to spread their malware.
- The list is believed to contain 4,324,770 email addresses, according to a copy the FBI provided to Troy Hunt, the security researcher behind the Have I Been Pwned service.
- In a blog post last month, Spamhaus said it also received a smaller list of 1.3 million email addresses compromised by Emotet, from a law enforcement partner.

- Since mid-April, the organization had reached out to the companies and email service providers behind the addresses, asking them to re-secure accounts by resetting their passwords.
- In total, Spamhaus said it reached out to 22,000 domain owners and 3,000 organizations to whom the compromised 1.3 million email addresses belonged to.
- Two months later, Spamhaus said that more than 60% of the 1.3 million addresses have now been re-secured.
- This was a **very important step** because the owners of the Emotet malware are still at large, and access to those email accounts could be sold to other criminal organizations or used by the Emotet gang if they decide to come back.
- However, many other email accounts remain compromised. End users and companies can check if their email addresses had been seen in Emotet email campaigns using the Have I Been Pwned service or a special website created by Dutch police.

Tags

- Dutch police
- email
- email account
- Emotet
- Have I Been Pwned
- malware
- password reset

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.