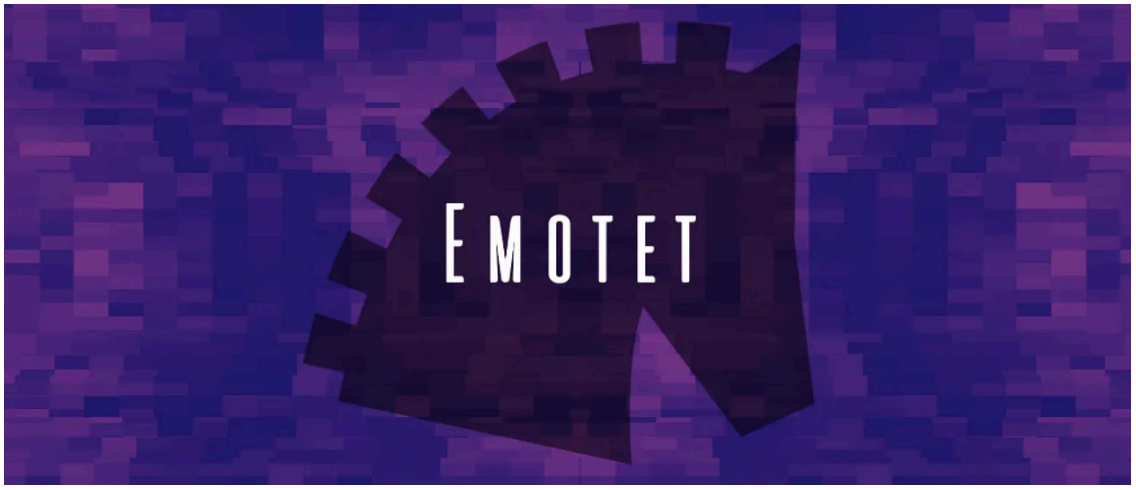
Microsoft, Italy, and the Netherlands warn of increased Emotet activity

By Written by Catalin Cimpanu, ContributorContributor Sept. 23, 2020 at 1:31 p.m. PT

Archived: 2026-04-05 17:08:25 UTC



Security

Two weeks after cyber-security agencies from France, Japan, and New Zealand published warnings about an uptick in Emotet activity, new alerts have been published this past week by agencies in Italy and the Netherlands, but also by Microsoft.

These new warnings come as Emotet activity has continued to increase, dwarfing any other malware operation active today.

"It has been very heavy for [Emotet] spam lately," Joseph Roosen, a member of Cryptolaemus, a group of security researchers who track Emotet malware campaigns, told *ZDNet* during an interview today.

"I received about 400 emails at my [dayjob] Monday when it is normally only about a dozen or less than 100 on a good day," Roosen said, putting the recent spike in perspective.

"This has been the case the last two weeks."

Emotet returned in July but is now spamming at full capacity

Emotet, by far today's largest malware botnet, has been dormant for most of this year, from February until July, when it made its comeback.

The Emotet crew was hoping for a quick return to full capacity, but its comeback was spoiled and delayed for almost a month by a vigilante who kept hacking into Emotet's infrastructure and replacing its malware with animated GIFs.

Unfortunately, that didn't last long, and Emotet operators eventually found a way to stop the hacker and are now back in full control over their botnet, which they are now using to churn out more and more spam every day.

These spam emails come with malicious files attached, which infect the host with the Emotet malware. The Emotet gang then sells access to these infected hosts to other cybercrime gangs, including ransomware operators.

Many times, and especially in large corporate environments, an Emotet infection can turn into a ransomware attack within hours.

That's why cyber-security agencies and CERT teams in France, Japan, New Zealand, Italy, and the Netherlands are treating Emotet spam campaigns with so much fear and respect, and why they're releasing alerts to the companies in their respective countries to bolster defenses for Emotet's spam trickery.

And Emotet has a large bag of tricks when it comes to its spam operations.

Roosen, who's been tracking the botnet for years now, says that Emotet is currently favoring the use of a technique called "email chains" or "hijacked treads."

The technique relies on the Emotet gang first stealing an existing email chain from an infected host and then answering the email chain with its own reply (using a spoofed identity), but by also adding a malicious document, hoping to trick existing email chain participants into opening the file and infecting themselves.

Emotet has been using this technique since October 2018 and has favored it across the years, using it many times before.

The technique is quite clever and effective and has also been detailed in a report published today by Palo Alto Networks.


emotet-email-chains.jpg
Image: Palo Alto Networks

But the alerts from Microsoft and Italian authorities also warn of another recent change in Emotet spam campaigns, which are now also leveraging password-protected ZIP files instead of Office documents.

The idea is that by using password-protected files, email security gateways can't open the archive to scan its content, and won't see traces of Emotet malware inside.

Roosen told ZDNet that Emotet has been using this technique sparingly since mid-2019, but recently they started to increase its prevalence among the Emotet spam campaigns, hence why Microsoft and others are now reacting to its sudden appearance.

> Emotet joined the password-protected attachment bandwagon with a campaign starting Friday. The campaign slowed down over the weekend (typical of Emotet) but was back today in even larger volumes of emails in English, as well as in some European languages. pic.twitter.com/POppQ51uMX
>
> — Microsoft Security Intelligence (@MsftSecIntel) September 22, 2020

The most dangerous iOS, Android malware and smartphone vulnerabilities of 2019

Security

Source: https://www.zdnet.com/article/microsoft-italy-and-the-netherlands-warn-of-increased-emotet-activity/