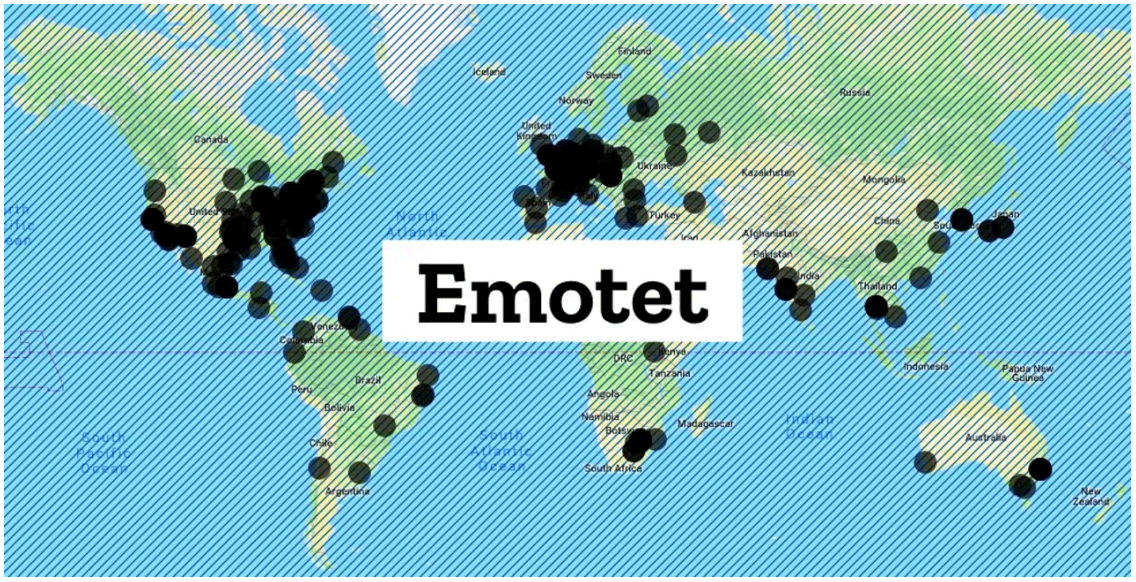
France, Japan, New Zealand warn of sudden spike in Emotet attacks

By Written by Catalin Cimpanu, ContributorContributor Sept. 7, 2020 at 7:48 p.m. PT

Archived: 2026-04-05 18:31:35 UTC



Security

Cyber-security agencies from France, Japan, and New Zealand have published security alerts over the past week warning about a large uptick in Emotet malware attacks targeting their respective countries.

Emotet activity described in the alerts refers to email spam campaigns that originated from Emotet infrastructure and targeted companies and government agencies in the three countries.

Victim organizations who received the emails, opened, and then ran the attached documents were at risk of getting infected with one of today's most dangerous malware.

Joseph Roosen, a member of Cryptolaemus, a group of security researchers who track Emotet malware campaigns, told *ZDNet* that the Emotet botnet has been particularly active in recent weeks, and especially active in the three countries.

For example, Roosen said New Zealand had been heavily targeted by Emotet operators via emails originating from E3 (one of the three mini-botnets that make the larger Emotet infrastructure).

On the other hand, while E3 was busy spamming New Zealand, Roosen said that all three mini-Emotet botnets (E1, E2, and E3) were targeting Japan. According to CERT Japan, these Emotet spam waves led to a tripling of Emotet sightings tripled last week, causing experts to sound a sign of alarm.


Image: CERT Japan

But while Japan and New Zealand have been under heavy spam waves, things were lighter in France, where, Roosen said, Emotet spam waves haven't been at the same levels as in the other two countries.

Nonetheless, Emotet infected computers on the network of the Paris court system, turning heads, making headlines, and triggering a state of emergency among French officials.

The French Interior Ministry reacted by blocking all Office documents (.doc) from being delivered via email, and France's cyber-security agency ANSSI followed through with an official cyber-security alert on Monday, urging government agencies to pay attention to the emails they're opening.

Conversations hijacking

According to all three alerts, the attacks appear to have been the same.

Emotet operators used their old trick of infecting one victim and then stealing older email threads. The group would then revive these old conversations, add malicious files as attachments, and target new users with a legitimate-looking conversation.

Users part of the conversations, or those added on, would often open the malicious files attachments added to the email thread out of curiosity and get infected.

In the recent campaigns that targeted France, Japan, and New Zealand, Emotet appears to have used Windows Word documents (.doc) and password-protected ZIP archive files as the malicious email attachments, attacks that have been seen targeting companies in other countries as well.

All three security alerts contain sound advice for anyone looking for ways to prevent or deal with Emotet infections, regardless of the country of origin.

At one point or another, Emotet will switch targeting and go after other countries, as the botnet can send out spam in multiple languages, according to cyber-security firm Proofpoint.

But the best Emotet advice ZDNet can give is in regards to systems that have been found to be already infected. In this case, companies should take down their entire networks and audit each system. This is because Emotet has features that allow it to spread laterally to the entire network, and Emotet is also often used to download other malware, including ransomware. Taking infected systems or the entire network offline while systems are scanned and re-imagined is the best way to avoid an even more costly security incident.

Security
