Emotet Attack Causes Shutdown of Frankfurt's IT Network

Archived: 2026-04-05 14:46:10 UTC

The city of Frankfurt, Germany, became the latest victim of Emotet after an infection forced it to close its IT network. But the financial center wasn't the only area that was targeted by Emotet, as there were also incidents that occurred in Gießen and Bad Homburg, a town and a city north of Frankfurt, respectively, as well as in Freiburg, a city in southwest Germany.

The infection started after an employee of the Fechenheim (a district in Frankfurt) civil registry clicked on an Emotet-laden attachment from a malicious spam email, apparently sent by a city authority. Alarms were raised by the security system, prompting officials to restrict city services and take the IT system off the network as a precautionary measure.

Germany has been a frequent target over the past few weeks by threat actors employing Emotet (and in general has been a target for malicious activity in 2019 according to data from the Trend Micro™ Smart Protection Network™ infrastructure). In fact, the German Federal Office for Information Security (BSI) issued a press release warning the public about malicious spam emails that carry Emotet.

First detected in 2014, Emotet has become one of the most notorious malware families of the past few years. Its original iteration was as an information-stealing banking malware — however, it has since undergone multiple evolutions, including acting as a loader for other malware families. It went into hiatus earlier in the year but came back afternews- cybercrime-and-digital-threats a few months with a vengeance. This recent spate of attacks on Germany is likely a continuation of Emotet's comeback campaigns.

Recommendations and solutions

Despite all the changes Emotet has undergone, spam mail remains the malware's most prominent distribution method. The most effective strategy organizations can implement is to educate their employees regarding email threatsnews- cybercrime-and-digital-threats and to encourage them to follow the recommended security best practices when accessing their emails. This includes always double-checking an email for any red flags, as well as refraining from clicking any links or downloading any attachments haphazardly.

Combating threats like Emotet calls for a multilayered and proactive approach to security that involves protecting all fronts — gateway, endpoints, networks, and servers. Trend Micro endpoint solutions such as Trend Micro

Smart Protection Suites and Worry-Free™ Business Security can protect users and businesses from these threats by detecting malicious files and spammed messages, as well as blocking all related malicious URLs.

To bolster their security capabilities and further protect their end users, organizations can consider security products such as the Trend Micro Cloud App Security™ products solution, which uses machine learning (ML) to help detect and block spam and phishing attempts. If a malicious email is received by an employee, it will go through sender, content, and URL reputation analysis, which is followed by an inspection of the remaining URLs using computer vision and AI to check if website components are being spoofed. The solution can also detect suspicious content in the message body and attachments and provide sandbox malware analysis and document exploit detection.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
