

There's a reason your inbox has more malicious spam—Emotet is back



reader comments

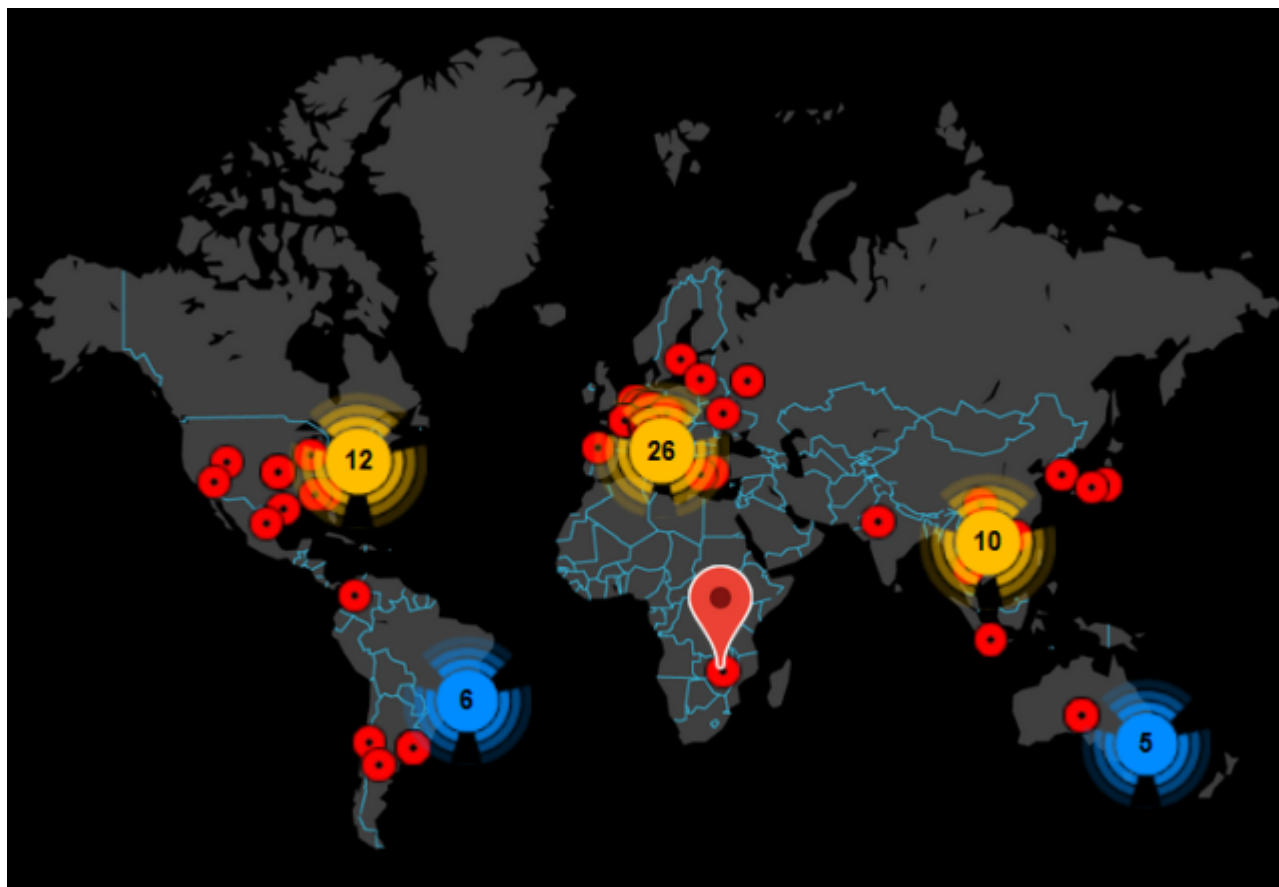
69 with 40 posters participating

Share this story

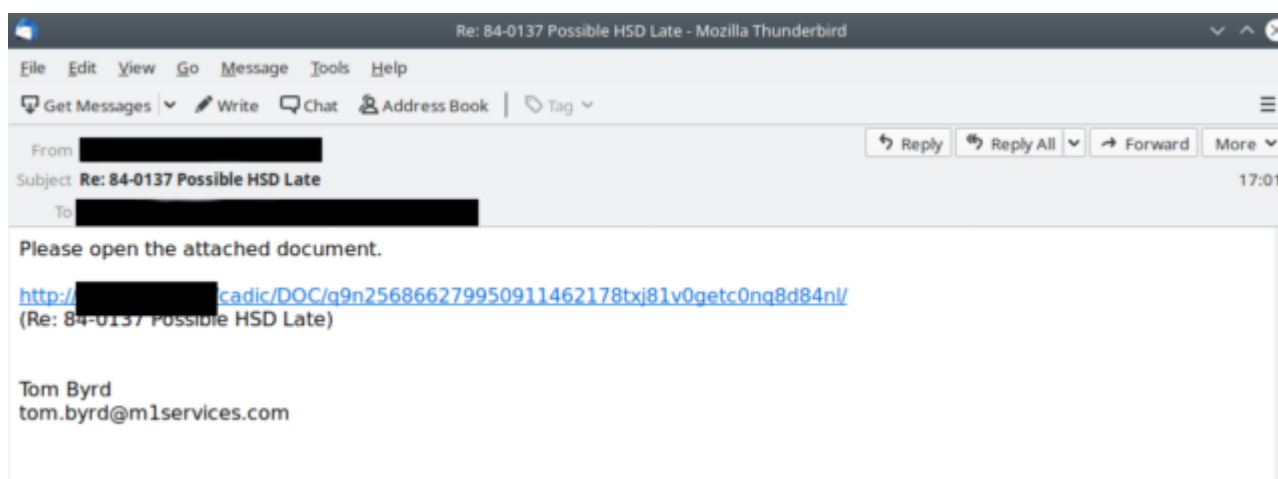
Emotet, the world's most costly and destructive botnet, returned from a five-month hiatus on Friday with a blast of malicious spam aimed at spreading a backdoor that installs ransomware, bank-fraud trojans, and other nasty malware.

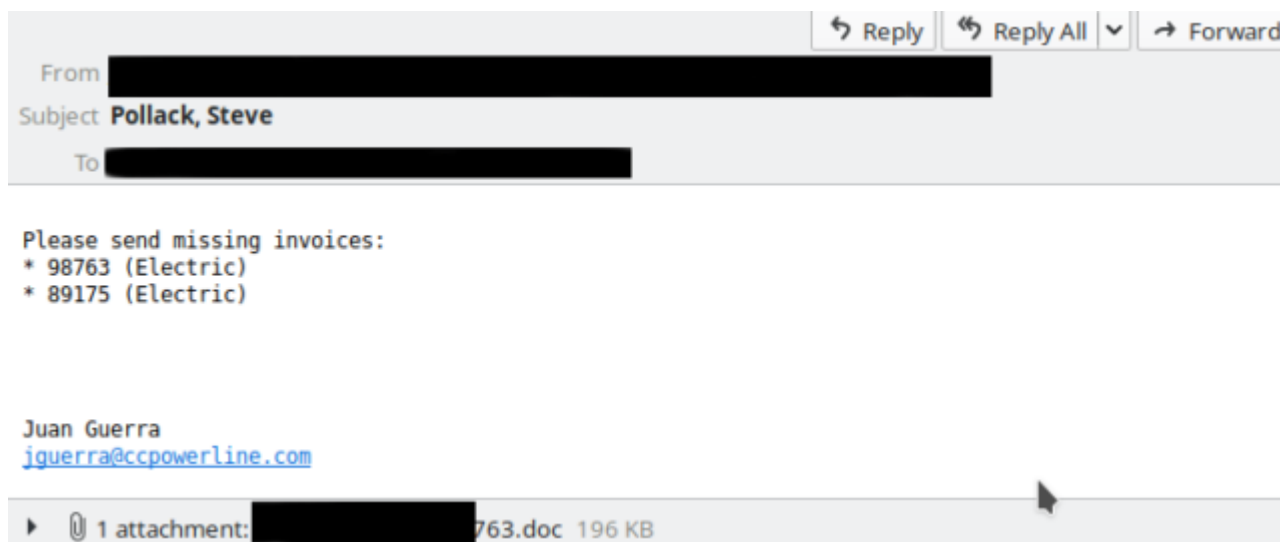
The botnet sent a hefty 250,000 messages during the day, mostly to people in the United States and the United Kingdom, Sherrod DeGrippe, senior director of threat research and detection at security firm Proofpoint, told Ars. Other researchers said targets were also located in the Middle East,

South America, and Africa. The botnet followed its characteristic pattern of sending either a malicious document or link to a malicious file that, when activated, installs the Emotet backdoor.



Enlarge / A map showing where Emotet hit on Friday. The botnet gave its first indications of a return on Tuesday, with small message volumes being sent out. Email samples that appeared on Twitter accounts from threat monitors abuse.ch and Spamhaus looked like this:





Emotet's resurgence on Friday was also spotted by antivirus provider Malwarebytes and Microsoft.

Box of tricks

Emotet has proven to be one of the more resourceful threats to face people in recent years. Emails often appear to arrive from a person the target has corresponded with in the past. The malicious messages often use the subject lines and the bodies of previous email threads the two have participated in. Emotet gets this information by collecting the contact lists and inboxes of infected computers.

The technique has a dual benefit. It tricks the target into thinking the message can be trusted because it comes from a known friend, acquaintance, or business associate who is following up on a previously discussed matter. The inclusion of authentic content also makes it harder for spam filters to detect the emails as malicious.

Another of Emotet's clever tricks: it steals usernames and passwords for outgoing email servers. The botnet then uses the credentials to send mail from those servers rather than relying on its own infrastructure. Because the trusted servers send the malicious messages, they're harder for security products to detect and block.

Hit and run

DeGrippo said that the last time Emotet had shown itself was during a five-day run in early February, that delivered about 1.8 million messages. The botnet is known for making big blasts for short periods of time and then going silent for weeks or months at a time. Last September, it woke from a four-month slumber.

The group is known for taking long breaks and regularly taking time off during weekends and major holiday seasons. True to its normal pattern, the latest Emotet activity had completely stopped on Saturday morning, as this post went live. Besides allowing its workers to maintain a healthy work-life balance, the schedule makes campaigns more successful.

“The key for most threat actors is to minimize the time between when [malicious mail] hits the inbox and when it gets opened by the target.” DeGrippo explained. “The longer that time elapses, the bigger the risk to the threat actor that their payload won’t get delivered because of mitigating controls.”

Emotet messages include malicious Microsoft Word documents or PDF files or URLs that link to malicious Word files. The Word documents contain macros that, when activated, install the Emotet backdoor. The backdoor typically waits a period of days before installing follow-on malware, such as the banking trojan TrickBot or the Ryuk ransomware.

Researchers have published indicators of compromise from Friday’s message blast [here](#), [here](#), and [here](#).

Emotet is yet another reminder that people should be highly suspicious of files and links sent in email, particularly if they seems out of context, such as when a friend sends an invoice. People should be doubly suspicious of any Word document that requires macros be enabled before content can be

viewed. There is rarely any reason for consumers to use macros, so a good household rule is to never enable them for any reason. A better policy still is to open Word documents in Google Docs, which prevents any malware from getting installed on the local computer.

<https://arstechnica.com/?p=1692725>