Emotet Campaign Restarts After Seven-Week Hiatus

By Robert Lemos

Published: 2020-12-22 · Archived: 2026-04-05 23:12:33 UTC

4 Min Read

In October, three surges of spam laden with the Emotet downloader worked to spread the malware to vulnerable users' systems, starting a sequence that often results in a Ryuk ransomware infection or attempts to steal bank account credentials via the Trickbot banking Trojan.

On Oct. 30, with the completion of the third campaign, the group's spamming died down and almost no subsequent traffic appeared. Until now.

Seven weeks after the last major Emotet campaign, the cybercriminals behind the downloader have started up their attempts to compromise more systems, according to multiple cybersecurity organizations. Anti-spam crusader Abuse.ch noted on Dec. 22 that the cybercrime group had ramped up activity right before Christmas. The day before, messaging security provider Proofpoint noted that its systems were seeing more than 100,000 messages in various languages and with a variety of attachments or links.

The latest campaign could lead to compromised systems and threats to business networks, as most employees continue to work from home.

"What makes Emotet particularly dangerous for organizations is that it has been the primary foothold for the future deployment of other banking Trojans," says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint. "At this point, any mainstream banking Trojan may lead to devastating ransomware attacks."

While the company is still analyzing the latest Emotet variant, the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) called the malware campaigns "one of the most prevalent ongoing threats" in an advisory published in early October. The US government had seen an increase in Emotet-associated indicators since July, and which specifically targeted state and local governments, the advisory stated.

"Emotet is an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload," the advisory stated. "The malware then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives."

While the latest Emotet campaign started around mid-December, the activity became most apparent in the last few says. Proofpoint issued a short statement on Twitter on Dec. 21 that also displayed a screenshot of the social engineering used to attempt to get victims to turn off features of Microsoft 365 that block malicious documents.

"#Emotet returns after a short break just in time for the holidays," Proofpoint tweeted as part of the statement. "We're seeing 100k+ messages in English, German, Spanish, Italian, and more. Lures use thread hijacking with Word attachments, pw-protected zips, and URLs."

Emotet has often been the initial attack of a triad of malware: the Emotet downloader, the Ryuk ransomware, and the Trickbot banking trojan. The triple threat of malware has had enormous success. In June, the Cisco Talos Incident Response team stated that the majority of its engagements over the last year had been to clean up Ryuk ransomware. In early December, security services firm CrowdStrike stated that, of the more than 200 incidents the company investigated, 63% were financially motivated, and 81% of those incidents were ransomware attacks or an early stage attack that typically leads to ransomware.

Cybersecurity companies continue to attempt to disrupt the profitable cybercriminal attacks. In October, Microsoft, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and other cybersecurity firms banded together to attempt to disrupt the Trickbot botnet.

The latest data from the URLhaus database, which tracks malicious and suspicious domains, shows that Emotet spam activity has quickly increased in the past week.

This is not the first time that the Emotet group has taken a break. Spam volumes dropped in February 2020 and did not return until July, according to data from Cisco Talos.

"Emotet occasionally takes periodic breaks from sending malicious spam emails, as seen earlier this year," the company stated in a blog post.

While this version of Emotet could be similar to past versions, the developer of the malware chose to use dynamic libraries to allow for its functions to be easily updated, the CISA noted in its advisory.

"Emotet is difficult to combat because of its 'worm-like' features that enable network-wide infections," the agency stated. "Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities."

About the Author

Contributing Writer

Veteran technology journalist of more than 20 years. Former research engineer. Written for more than two dozen publications, including CNET News.com, Dark Reading, MIT's Technology Review, Popular Science, and Wired News. Five awards for journalism, including Best Deadline Journalism (Online) in 2003 for coverage of the Blaster worm. Crunches numbers on various trends using Python and R. Recent reports include analyses of the shortage in cybersecurity workers and annual vulnerability trends.

Source: https://www.darkreading.com/threat-intelligence/emotet-campaign-restarts-after-seven-week-hiatus/d/d-id/1339792