# Emotet Sending Malicious Emails After Three-Month Hiatus

Archived: 2026-04-05 13:24:43 UTC

The Cofense Intelligence team continues to see the Emotet malware family being leveraged across the threat landscape. To protect against the many threats out there, it's important to know about the various types of malware that exist and how they have evolved over time. One of the most serious malware families is Emotet, a type of banking trojan that has been around since 2014. We will cover the history of Emotet at the end of our findings.

## What is Emotet?

Emotet was first discovered in 2014 by security researchers who were tracking a malicious network traffic pattern. It was quickly identified as a Trojan virus that could gain access to computers through email attachments or malicious links sent via email campaigns or social media messages. In worm-like fashion, it spread from one computer to another, stealing confidential information and personal data from unsuspecting users.

At first, Emotet was primarily used for financial fraud, stealing bank account numbers and credit card details from unsuspecting victims. But as its capabilities grew, so did its scope—from financial fraud to espionage and political sabotage. As other malicious actors became aware of the power of Emotet, they began using it to launch larger-scale attacks on businesses, government agencies, and even healthcare providers.

**Recent Key Findings:**

- Emotet malicious email activity resumed Tuesday, March 7, 2023 at 8:00am EST.
- Malicious emails contain attached .zip files that are not password protected.
- The attached .zip files deliver Office documents with malicious macros, which in turn download and execute the Emotet .dll.
- It is unclear how long this round of email activity will last, as periods of activity in 2022 varied widely.

After several months of inactivity, the Emotet botnet resumed email activity this morning at 8:00am EST. The malicious emails seem to be replying to already existing email chains, with the addition of an attached .zip file (Figure 1). The .zip files are not password protected. The themes of the attached files include finances and invoices.

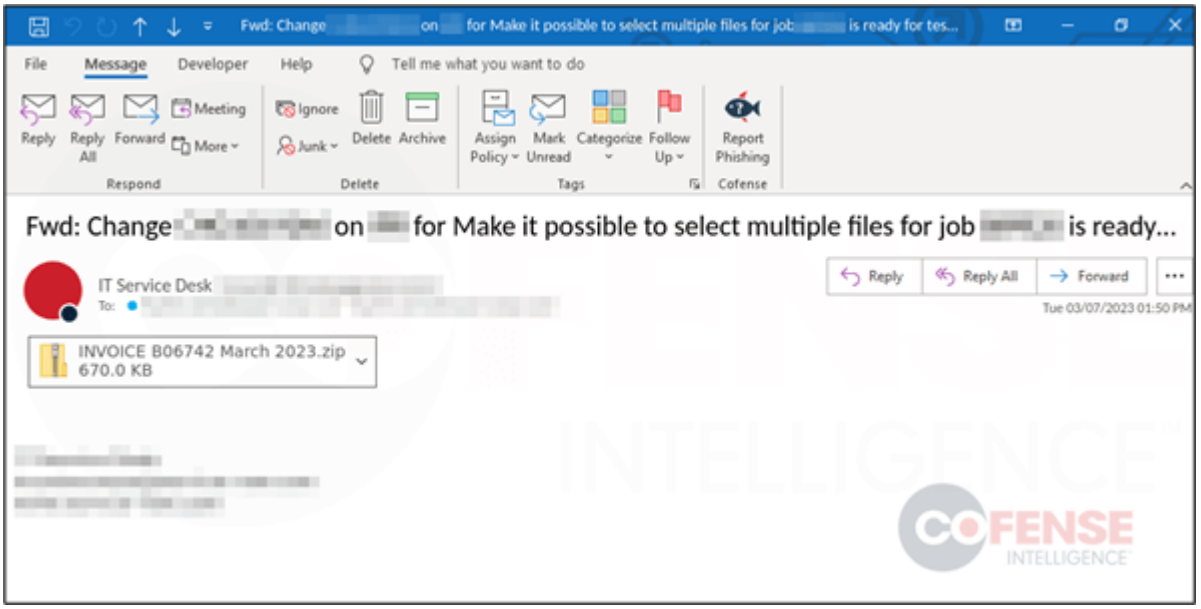


*Figure 1: Sample Emotet email with attached .zip file.*

The .zip files attached to these recent Emotet emails contain an Office Document with macros (Figure 2). Once opened, the user is prompted to “Enable Content”, which will allow the malicious macros to run. The macros will download an Emotet .dll from an external site and execute it locally on the machine.

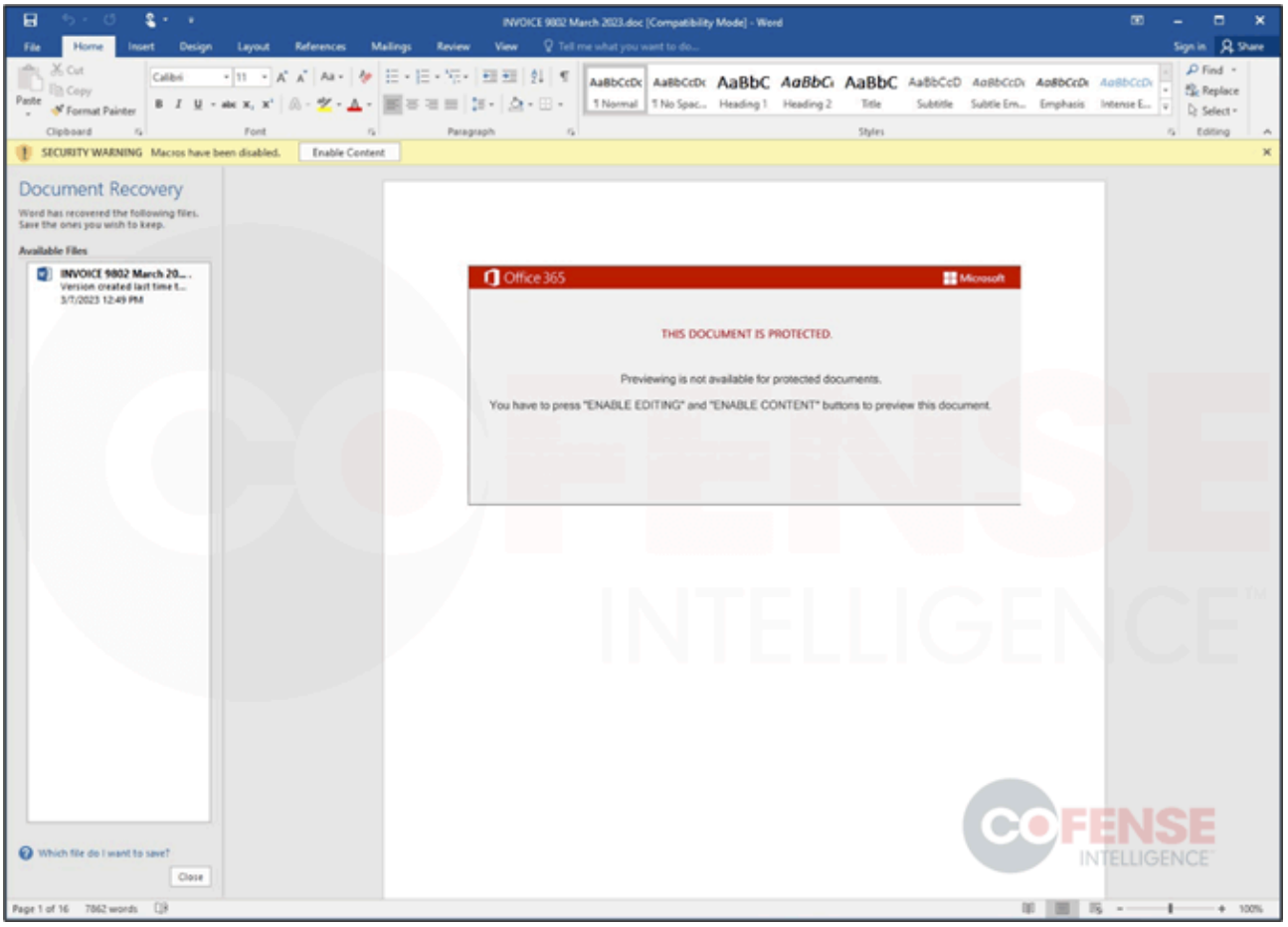


*Figure 2: Office document with macros to download and execute Emotet.*

It is unclear how long this round of email activity will last. While an earlier round of activity in 2022 extended across multiple weeks, the last round occurred over less than two weeks in November 2022, with more than three months of inactivity on either side.

## Modern Emotet Attacks

Today's version of Emotet is even more sophisticated than its predecessors. It can now be used for ransomware attacks—where attackers encrypt files on computers until victims pay a ransom—and distributed denial-of-service (DDoS) attacks—where attackers overwhelm websites with traffic until they crash or become inaccessible for legitimate visitors. Additionally, modern versions of Emotet are now able to steal passwords from web browsers and spread itself across networks without user interaction.

Cybersecurity professionals must stay up-to-date on the latest threats like Emotet so they can protect their networks against these dangerous forms of malware. While it is impossible to predict when and where new forms of malware will appear next, vigilance is key in mitigating any damage caused by these malicious actors before it's too late.

With Cofense, you can take security to the next level by providing simulations that teach users about Emotet and how to spot it. Current customers can log into PhishMe and simply search for "emotet" when creating a new scenario. There are multiple scenarios to choose from so you can create a bespoke playbook for training end users on this threat and how to spot it. Cofense can take it a step further by removing malicious emails that contain Emotet malware automatically and before users even see them. If you are interested in learning more about Emotet and how Cofense can better train end users, please reach out to sales@cofense.com.

---