Emotet Sending Malicious Emails After Three-Month Hiatus

cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/

March 7, 2023

Key Points:

- 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.

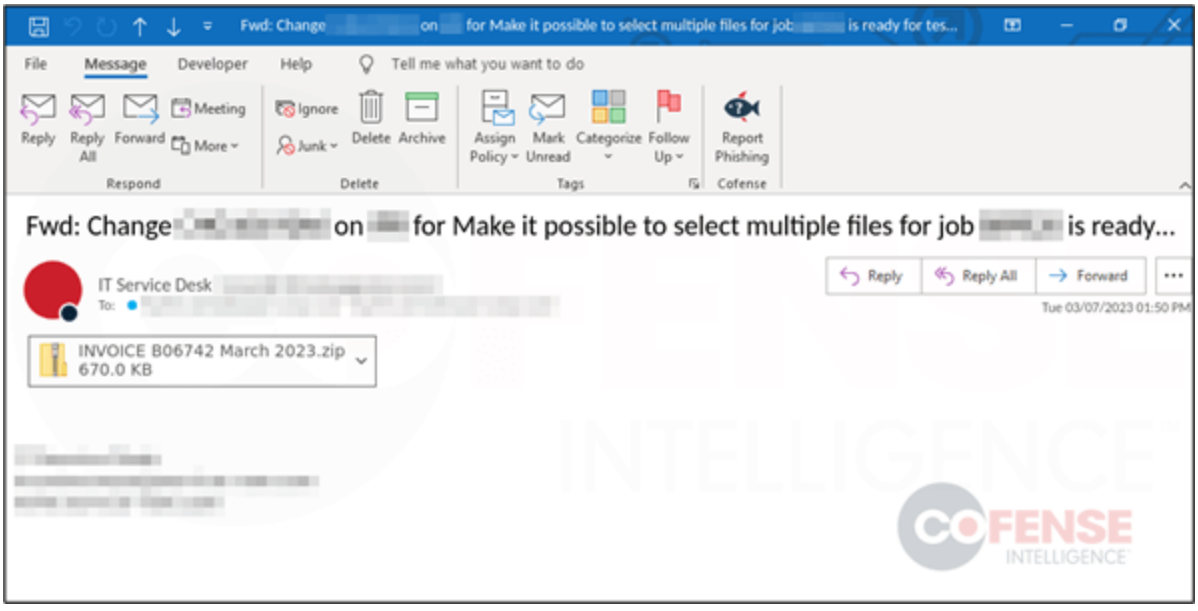

Figure 1: Sample Emotet email with attached .zip file.

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.

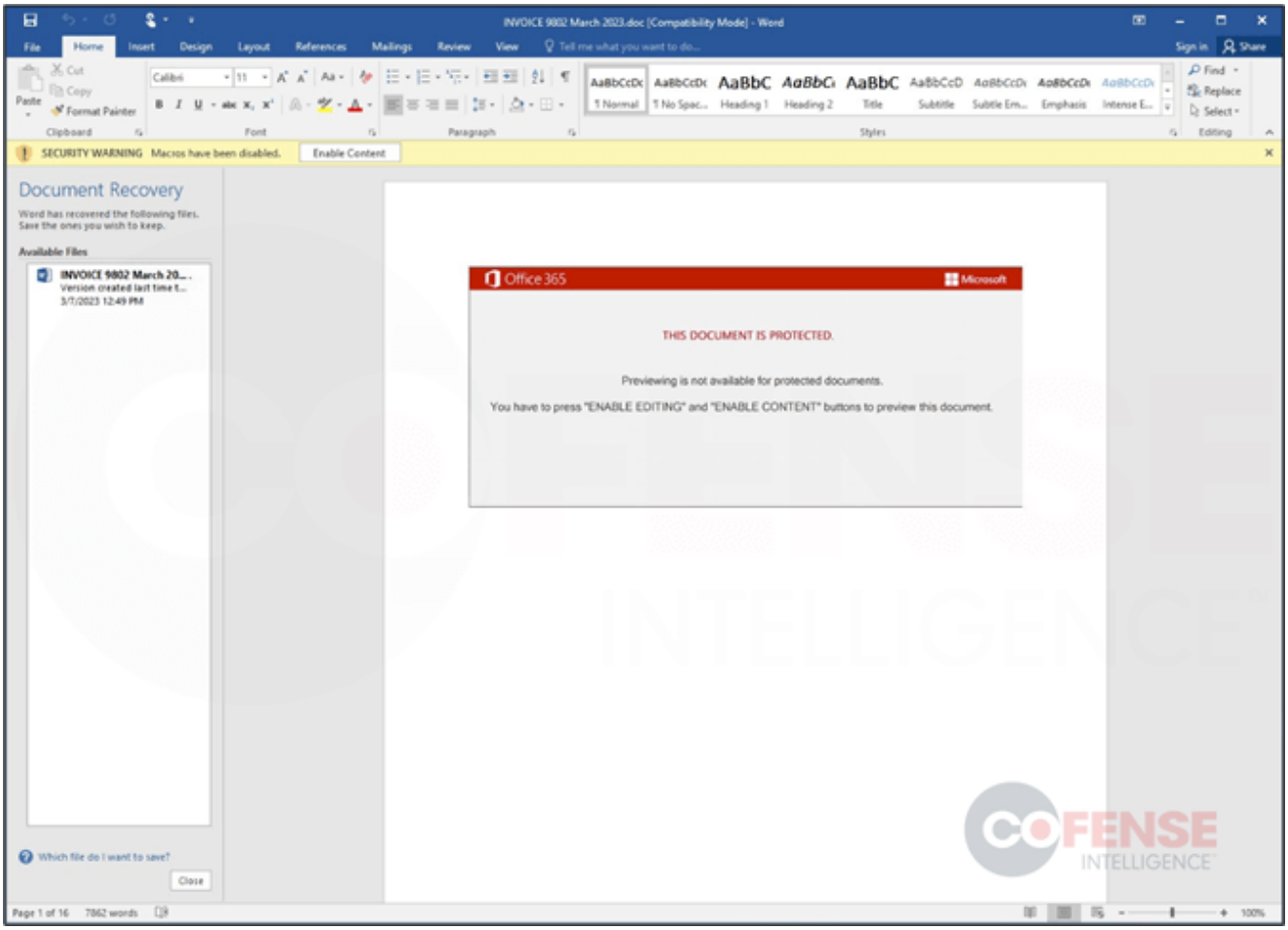

Figure 2: Office document with macros to download and execute Emotet.

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.