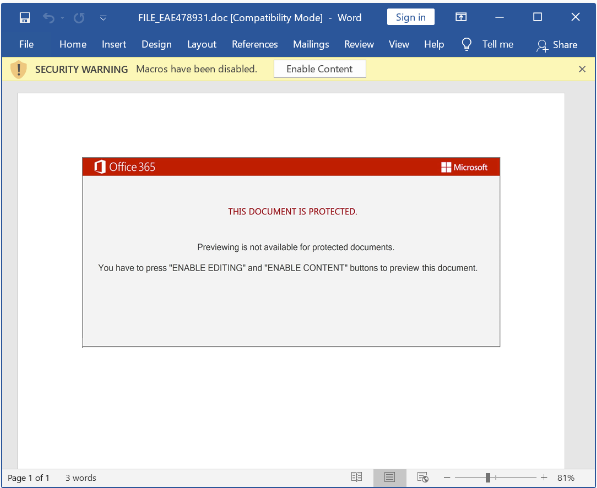
Wireshark Tutorial: Analyzing Emotet Infection Traffic

To understand network traffic caused by Emotet, you must first understand the chain of events leading to an infection. Emotet is commonly distributed through malicious spam (malspam) emails. The critical step in an Emotet infection chain is a Microsoft Word document with macros designed to infect a vulnerable Windows host.



Malspam spreading Emotet uses different techniques to distribute these Word documents.

The malspam may contain an attached Microsoft Word document or have an attached ZIP archive containing the Word document. In recent months, we have seen several examples where these ZIP archives are password-protected. Some emails distributing Emotet do not have any attachments. Instead, they contain a link to download the Word document.

In previous years, malspam pushing Emotet has also used PDF attachments with embedded links to deliver these Emotet Word documents.

A diagram of a computer program

Description automatically generated with medium confidence

A flowchart of network activity we might find during an Emotet infection.

A diagram of a computer network

Description automatically generated