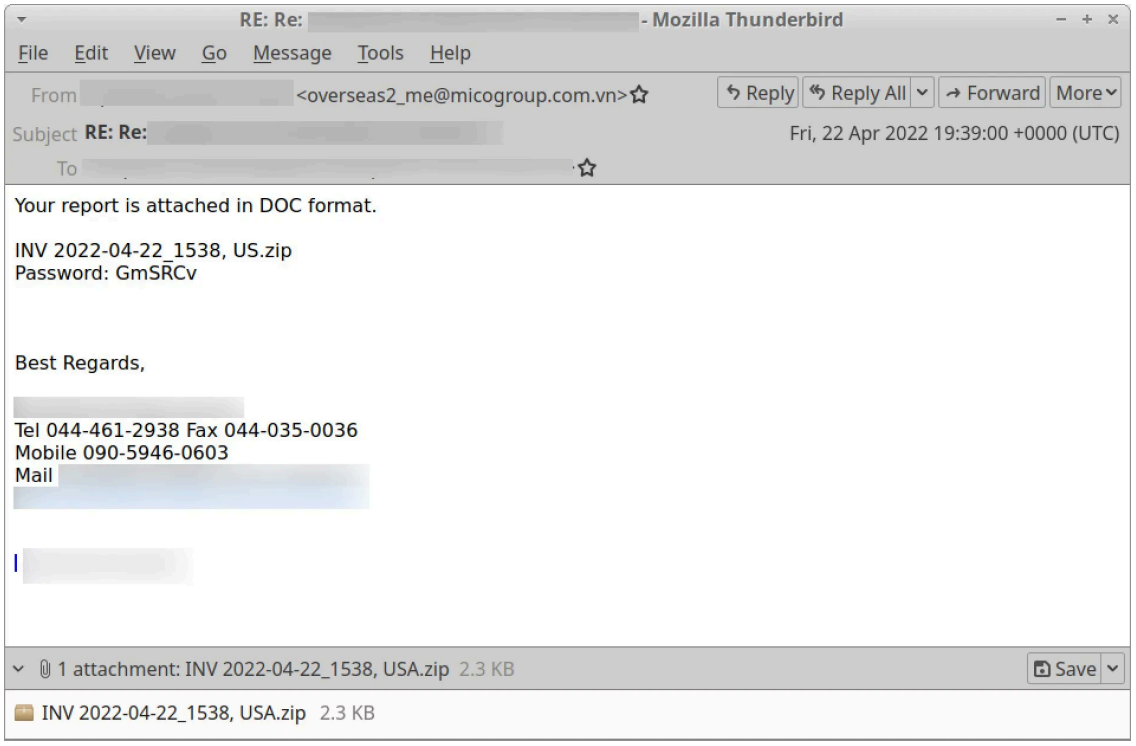
Emotet fixes bug in code, resumes spam campaign

By Jovi Umawing

Published: 2022-04-26 · Archived: 2026-04-05 20:32:54 UTC

Emotet threat actors resumed their email spam campaign on Monday after stopping it late last week to fix a bug.

The bug—a flaw in how Emotet is installed onto a system after a victim opens a malicious email attachment—forced the actors to prematurely halt their campaign.



Emotet is spammed around in emails claiming to contain invoices, forms, or payment details. The attachment is a password-protected ZIP file with a shortcut link file (has the .LNK extension) inside pretending to be a Word document file.

Normally, once users double-click the file, Emotet is loaded into memory, steals email addresses to use in future campaigns, and drops a payload, usually another malware like ransomware or Cobalt Strike. However, the bug happened immediately after the attachment was clicked.

You see, double-clicking the file sets off a chain. A command looks for a string hidden in the .LNK file containing code written in Visual Basic. This code is then appended to a new VBS file before executing that file. But, the shortcut file a command statically calls to does not match the actual name of the attached shortcut file. For example, the command code calls for “Password2.doc.lnk”, but the attached file itself is named “INVOICE 2022-04-22_1033, USA.doc”. This error breaks the infection chain.

Cryptolaemus (@Cryptolaemus1) has provided a more technical explanation in this Twitter thread:

Emotet's current use of .LNK files as attachments is a tried-and-tested tactic that can bypass antivirus detection and Mark-of-the-Web (MOTW) "marking." Mark of the Web is a Windows feature that determines the origin of a file downloaded from the Internet.

Our Threat Intelligence Team has seen APT threat actors use .LNK files in their attack campaigns (the Higaisa APTcomes to mind). It's no surprise that other cybercriminal groups have adopted this. Proponents of Emotet and IcedIDwere just some of them.

Emotet has been revolutionizing its way of reaching victims during its years of activity. Historically, it was spread via malicious Windows App Installer packages and malformed Word documents. Emotet is a sophisticated and versatile Trojan, which has been used by other criminal groups to drop their own malware, causing multiple system infections. Some of the files it drops are QBot, QakBot, TrickBot, and Mimikatz (a legitimate tool used to steal credentials).

BleepingComputer shareda list of attachment names the new Emotet email spam campaign is using, courtesy of Cofense, a security company specializing in email security:

- ACH form.zip
- ACH payment info.zip
- BANK TRANSFER COPY.zip
- Electronic form.zip
- form.zip
- Form.zip
- Form – Apr 25, 2022.zip
- Payment Status.zip
- PO 04252022.zip
- Transaction.zip

If you have received any emails bearing attachments with the above names, it would be wise to delete them immediately to prevent the risk of accidentally opening the attachment.

Stay safe out there!

About the author

Knows a bit about everything and a lot about several somethings. Writes about those somethings, usually in long-form.

Source: https://blog.malwarebytes.com/cybercrime/malware/2022/04/emotet-fixes-bug-in-code-resumes-spam-campaign/