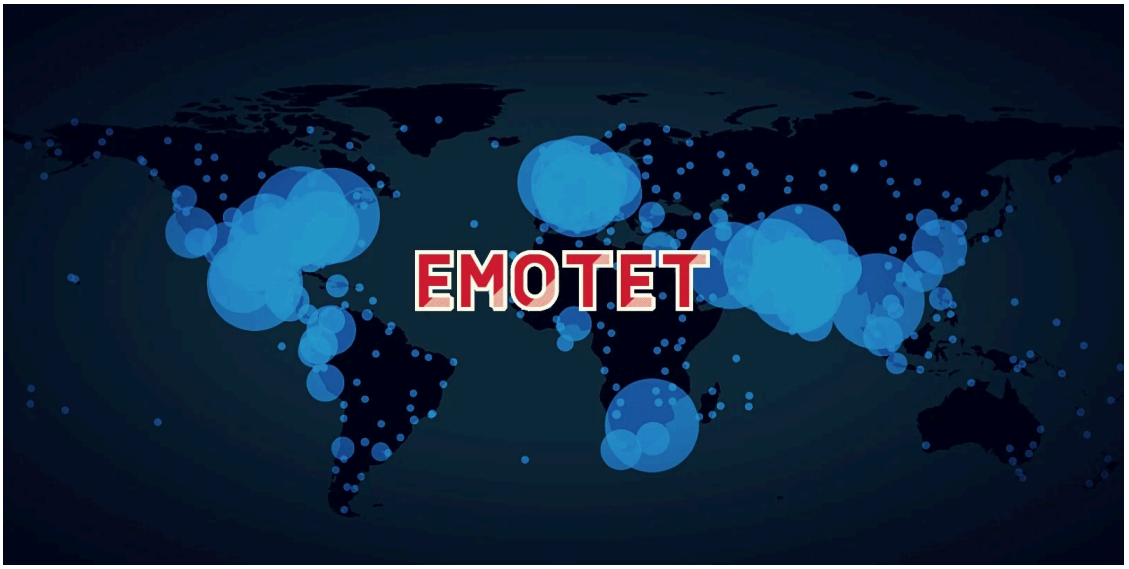
# Emotet malware infects users again after fixing broken installer

By Lawrence Abrams

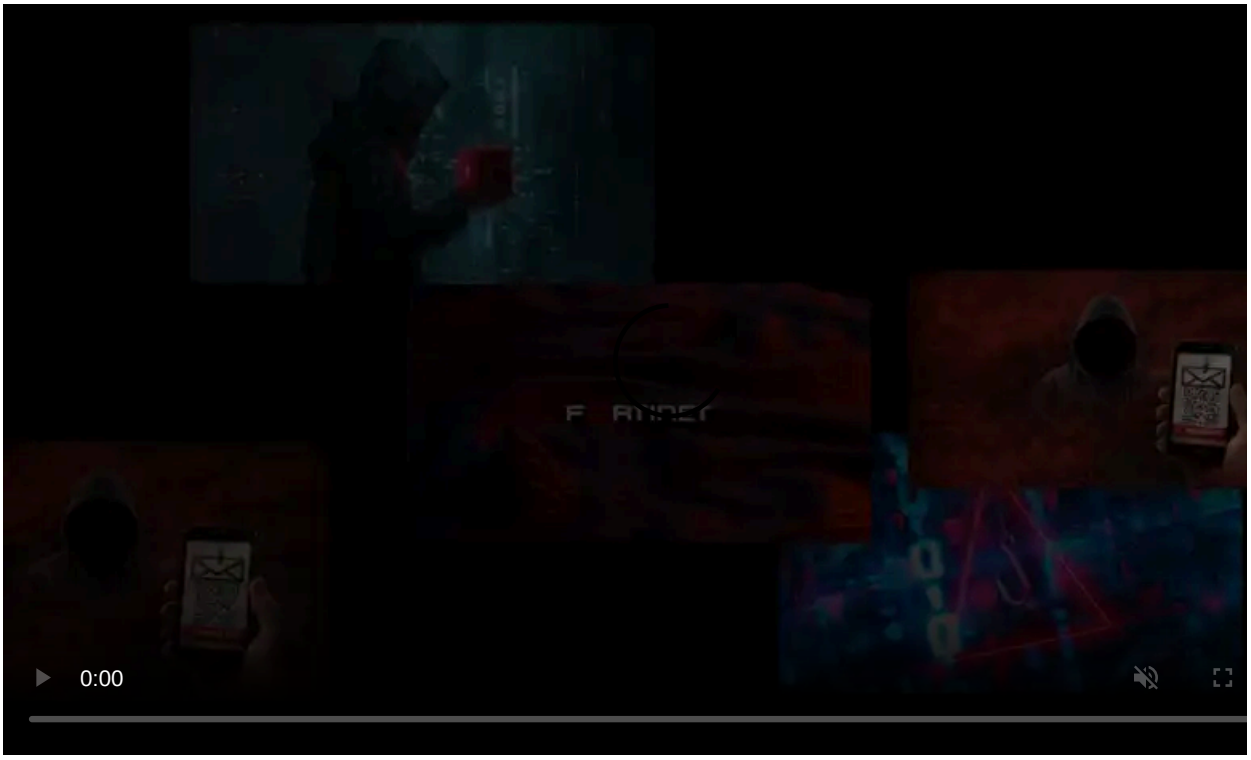
Published: 2022-04-25 · Archived: 2026-04-06 03:13:02 UTC

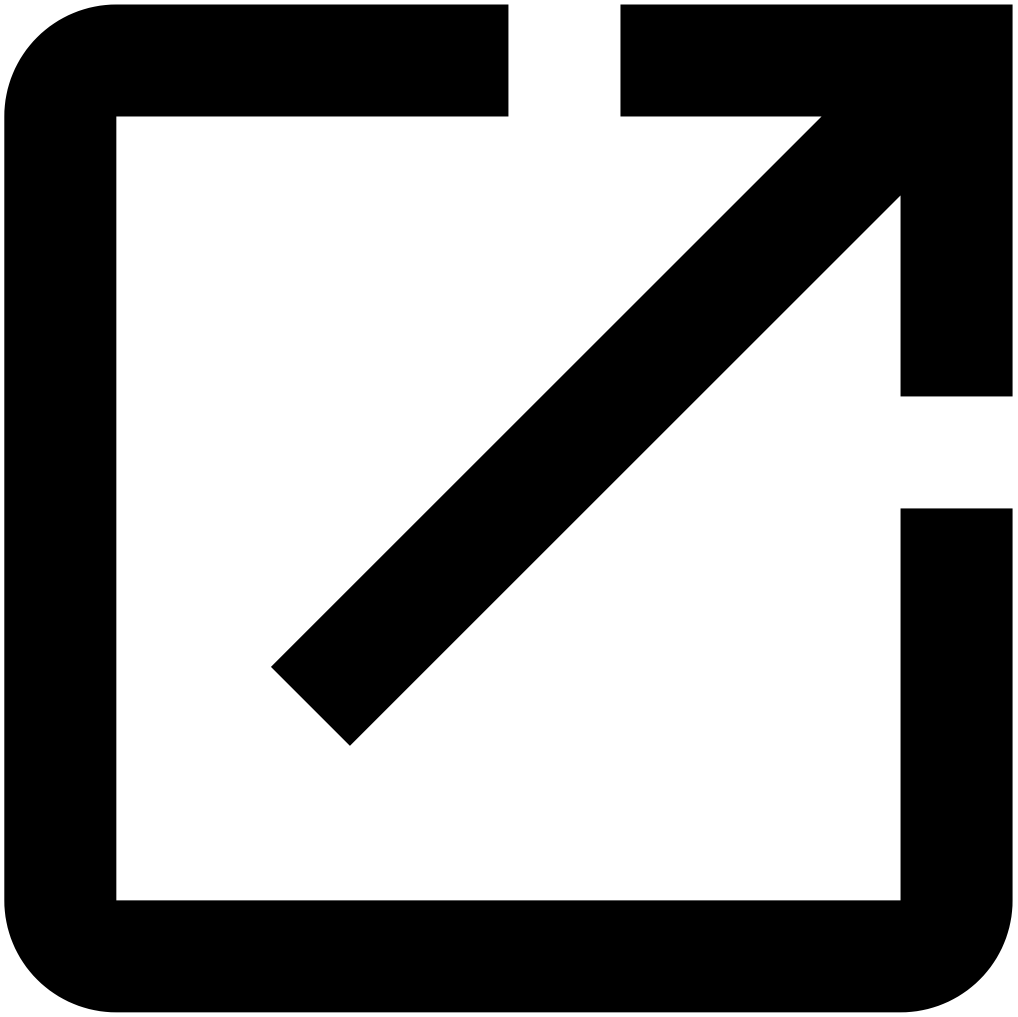



The Emotet malware phishing campaign is up and running again after the threat actors fixed a bug preventing people from becoming infected when they opened malicious email attachments.

Emotet is a malware infection distributed through spam campaigns with malicious attachments. If a user opens the attachment, malicious macros or scripts will download the Emotet DLL and load it into memory.

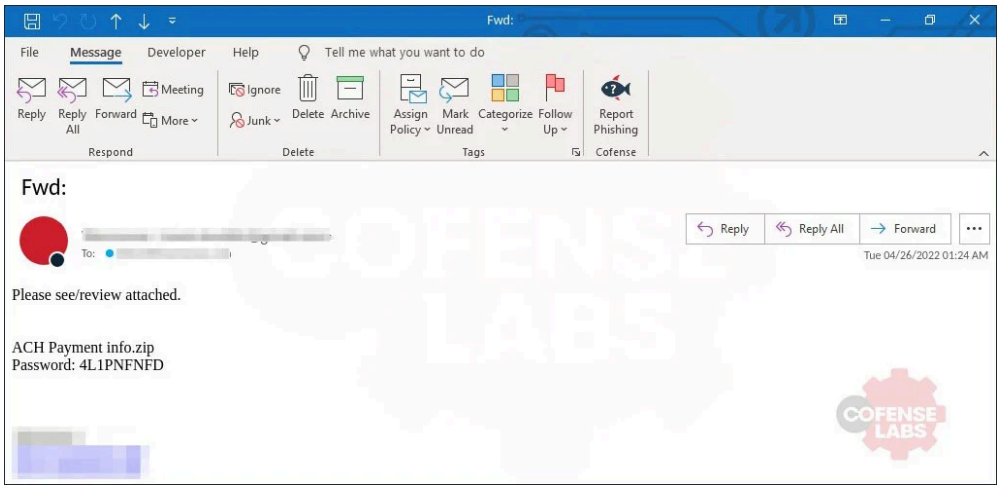
Once loaded, the malware will search for and steal emails to use in future spam campaigns and drop additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks.


0:00



## Buggy attachments broke the Emotet campaign

Last Friday, the Emotet malware distributors launched a new email campaign that included password-protected ZIP file attachments containing Windows LNK (shortcut) files pretending to be Word documents.




**Current Emotet phishing email example**

*Source: Cofense*

When a user double-clicked on the shortcut, it would execute a command that searches the shortcut file for a particular string that contains Visual Basic Script code, appends the found code to a new VBS file, and executes that VBS file, as shown below.

```
C:\Windows\system32\cmd.exe /v:on /c findstr "rSIPPswjwCtKoZy.*" Password2.doc.lnk
> "%tmp%\VEuIqlISMa.vbs" & "%tmp%\VEuIqlISMa.vbs"
```

**Emotet shortcut commands from Friday's campaign**

*Source: BleepingComputer*

However, this command contained a bug as it used a static shortcut name of 'Password2.doc.lnk,' even though the actual name of the attached shortcut file is different, like 'INVOICE 2022-04-22_1033, USA.doc'.

This caused the command to fail, as the Password2.doc.lnk file did not exist, and thus the VBS file was not created, as explained by the Emotet research group Cryptolaemus.

Cryptolaemus researcher Joseph Roosen told BleepingComputer that Emotet shut down the new email campaign at approximately 00:00 UTC on Friday after discovering that the bug was preventing users from becoming infected.

Unfortunately, Emotet fixed the bug today and, once again, started spamming users with malicious emails containing password-protected zip files and shortcut attachments.

These shortcuts now reference the correct filenames when the command is executed, allowing the VBS files to be created correctly and the Emotet malware to be downloaded and installed on victims' devices.

```
C:\Windows\system32\cmd.exe /v:on /c findstr "glKmfOKnQLYKnNs.*"
"INVOICE 2022-04-25_1033,USA.doc.lnk" > "%tmp%\YlScZcZKeP.vbs" &
"%tmp%\YlScZcZKeP.vbs"
```

**Fixed Emotet attachment command**

*Source: BleepingComputer*

Email security firm Cofense told BleepingComputer that the used attachment named used in today's Emotet campaigns are:

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

If you receive an email with similar password-protected attachments, it is strongly advised that you do not open them.

Instead, you should contact your network or security admins and let them examine the attachment to determine if they are malicious or not.



---

Source: https://www.bleepingcomputer.com/news/security/emotet-malware-infects-users-again-after-fixing-broken-installer/