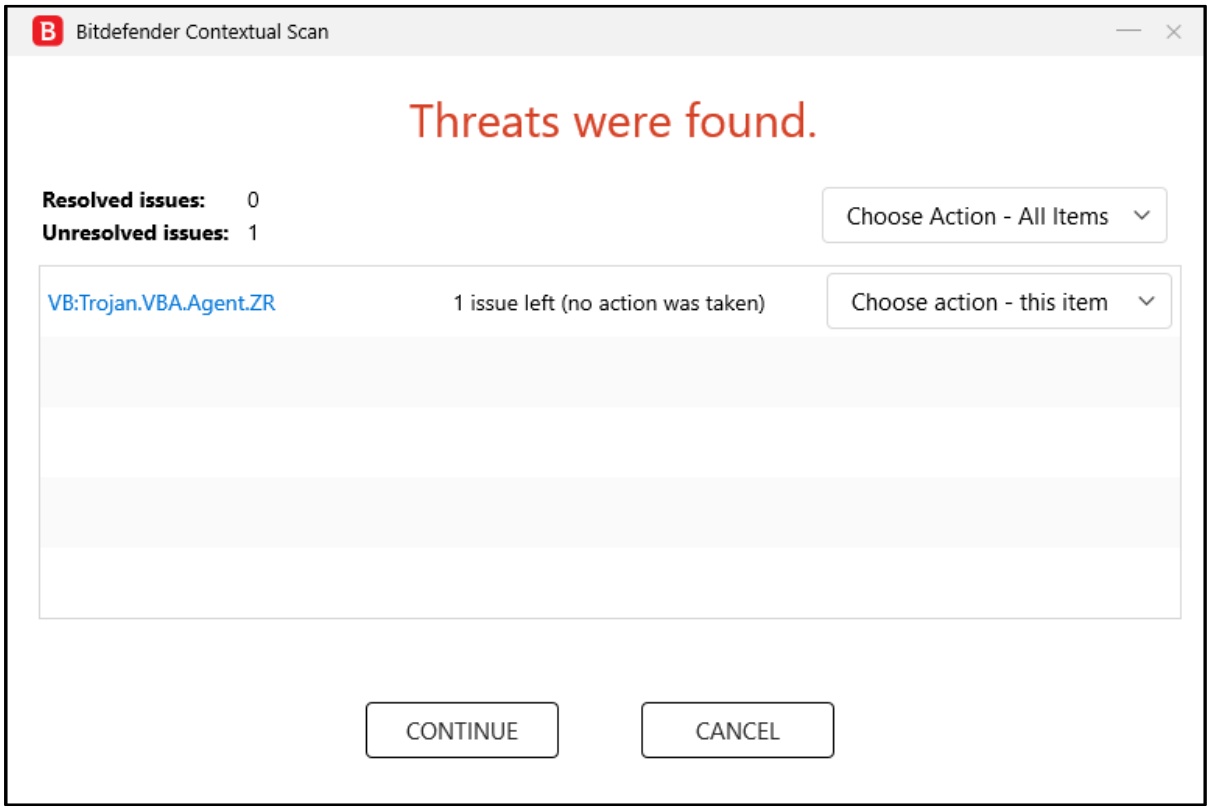
How to manually remove threats detected in e-mail attachments

This article will show you how to find and remove threats detected in e-mail attachments after a Bitdefender scan so that the Outlook .pst file or another email archive stored locally on your personal computer won't get quarantined or wiped out.

Overview

Bitdefender checks in real-time incoming & outgoing e-mails for cyber threats. It can also identify malware in email databases and email archives kept on the disk but cannot disinfect threats that are already there. When infected items are detected inside Outlook and Thunderbird, they usually cannot be cleaned because email archives cannot be repacked. At the end of the Bitdefender scan, you will be informed that no action has been taken against the e-mail attachments and asked to pick an action to remove the infection:

- **Take proper actions** – Outlook .pst files that cannot be disinfected are moved to quarantine to contain the infection. Quarantined files cannot be executed or opened, therefore the risk of getting infected disappears. Quarantined files older than 30 days are automatically deleted if they are not restored within this period.
- **Delete** – Permanently removes the entire .pst file from the disk.
- **Take no action** – No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.



Why won’t Bitdefender delete infected emails?

There is a risk you could lose the entire .pst file. Outlook .pst is a massive database file that contains all your emails and their attachments. Bitdefender must extract that infected email and attachment and put the database file back together without damaging it. This action is not technically possible, and most security solutions abort any attempt as it may irreparably corrupt the .pst file.

If the .pst file were simply deleted the result would be the loss of all emails going back years and years. Under normal circumstances, Bitdefender would simply move an infected file that cannot be disinfected to quarantine. But that would quarantine the entire email archive which is not ideal and the result is the same – all emails would be missing.

Also, if the email application is open, the scan cannot take any action because the email database is in use.

For all these reasons, the solution is not that simple. As burdensome as it may be to manually search the email subject and delete the infected email/attachment one by one, it is preferable to the prospect of losing all your emails.

How to safely remove threats detected in e-mail attachments

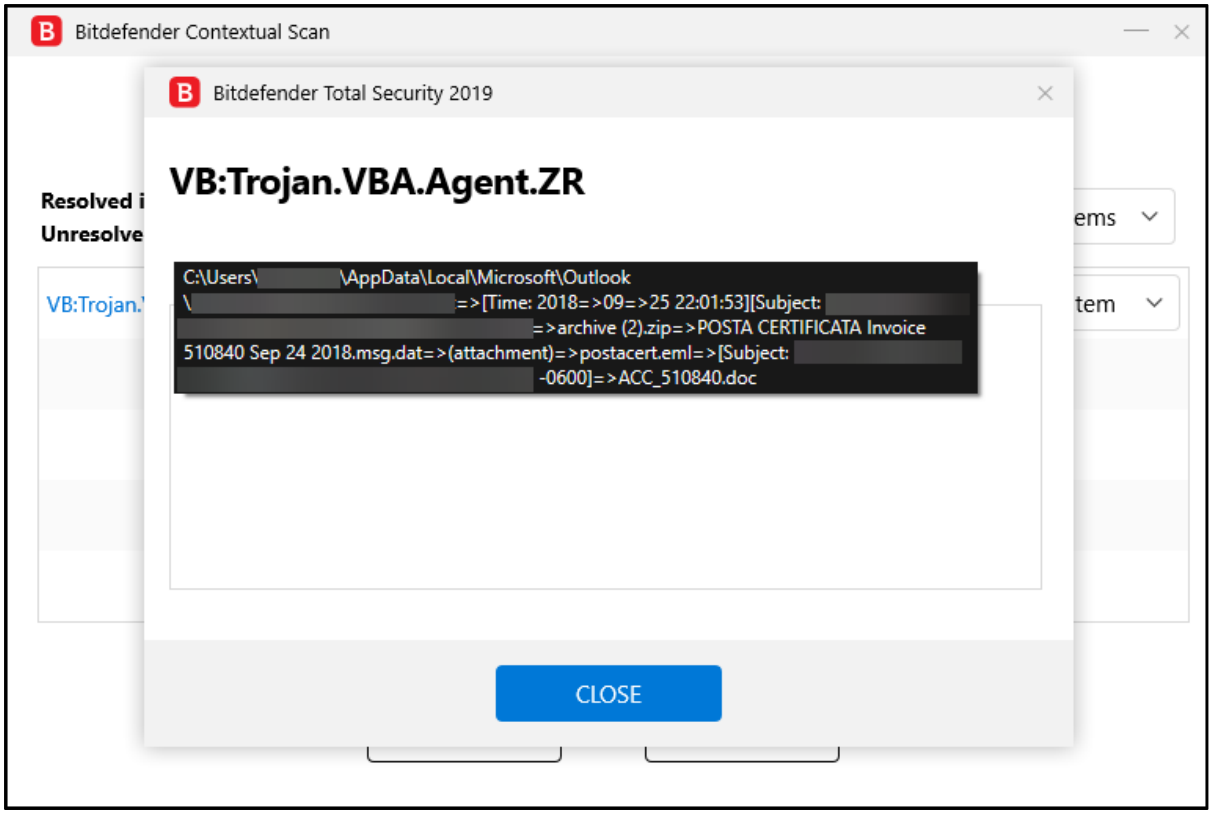
Sometimes it is necessary to locate the infected message using the information provided in the scan log and to manually delete the email that has an infected file attached.

If you scan your PC with Bitdefender and the scan log reports unresolved items (usually a Trojan) located in an email archive, make a note of what it found – particularly any reference to the actual email – and choose to take no action. This will allow you to locate the infected message later in Outlook / Thunderbird using the information provided in the scan report and to delete the email with an infected attachment manually, then empty the Deleted Items folder. This is the safest option, but it is recommended that you back up your emails first.

Here’s how to safely remove the infected e-mails from your computer:

1. Open the Bitdefender scan log and use the identification information (Subject, From, To) of the infected messages to locate them in the email client.

   You can open the scan log directly from the scan wizard, once the scan is completed, by clicking SHOW LOG.



To check the scan log later:

- Click on Notifications in the menu on the left-hand side of the Bitdefender interface.
- In the Critical tab, select the latest Bitdefender scan event to expand it.
- Bitdefender will provide an overview of the scan results. To open the scan log, click View log.

2. Go to the “Unresolved items” section of the Bitdefender scan log to see details about the infected email. The following information is available:
   - **Email archive** – E.g. C:\Users\YourUsername\AppData\Local\Microsoft\Outlook\Outlook.pst
   - **Time** – E.g. [2018=>09=>25. 22:01:53]
   - **Subject** – E.g. [Subject: POSTA CERTIFICATA Invoice]
   - **Sender** – E.g. [From: John Smith]
   - **Attachment name** – E.g. ACC_510840.doc

3. Next, open your email client – the software you use to send and receive emails. Typical examples include Microsoft Outlook and Mozilla Thunderbird.
4. Use the information found in the scan log to locate and delete all the infected messages.

ⓘ Note

If the detected e-mails cannot be found in your Inbox or other email account folders, they are most likely spam. Simply delete all emails in Spam / Junk.

5. At the end, make sure to empty the Deleted Items / Trash folder of your email app, otherwise emails containing malware will be detected again by future scans. Most email clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.

That’s how you can delete only those mails that contain viruses and not the entire .pst file.

If Bitdefender still detects infected emails that cannot be resolved, run a full System scan and send the log to our Support Team via the contact form. Check out this article to learn How to scan your PC with Bitdefender & export the scan log.