2016 Release 6 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 13-December-2016

2016 Release 6 of TRITON AP-EMAIL with Email Cloud Module includes the following product updates and corrections.

- *What's new in 2016 Release 6?*
    - *Limited availability: Secure suspicious attachments*
- *Resolved issues in this release*

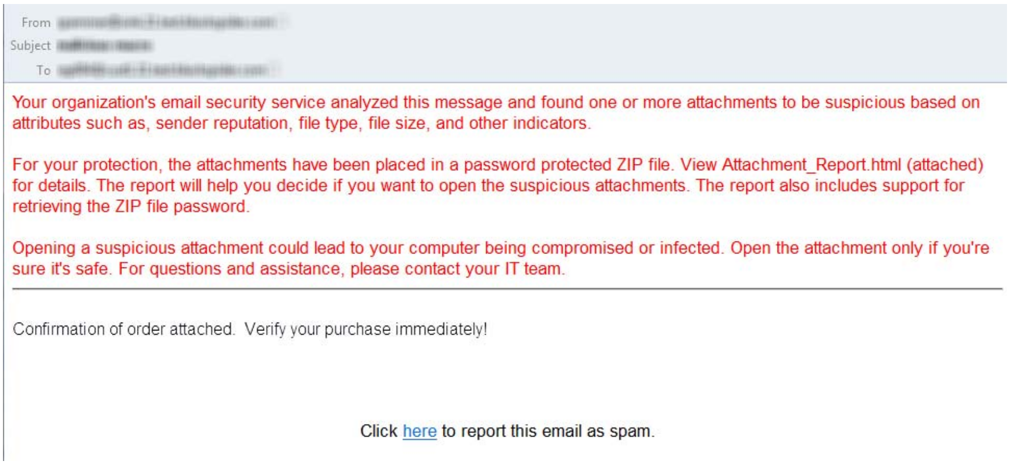
What’s new in 2016 Release 6?

TRITON AP-EMAIL with Email Cloud Module | 13-December-2016

Limited availability: Secure suspicious attachments

For cyber criminals, attaching malicious files to emails continues to be a very effective attack strategy. TRITON AP-EMAIL performs rigorous analysis of attachments, including sending suspicious files to a sandbox for observation and analysis (optional feature). However, even when a file passes analysis, some attributes of the attachment can continue to make it suspicious. These attributes include sender and domain reputation, attachment file type, attachment size, and the spam score of the message, among others.

Email administrators now have the option to secure suspicious attachments in a password protected zip file that is delivered to the recipient along with a report that includes the message details, a preview of the attachment content, and a link that the recipient can use to retrieve the zip file password. The email is also annotated with a customizable message. Below is a sample of a message delivered with a secured attachment.



From [redacted]
Subject [redacted]
To [redacted]

Your organization's email security service analyzed this message and found one or more attachments to be suspicious based on attributes such as, sender reputation, file type, file size, and other indicators.

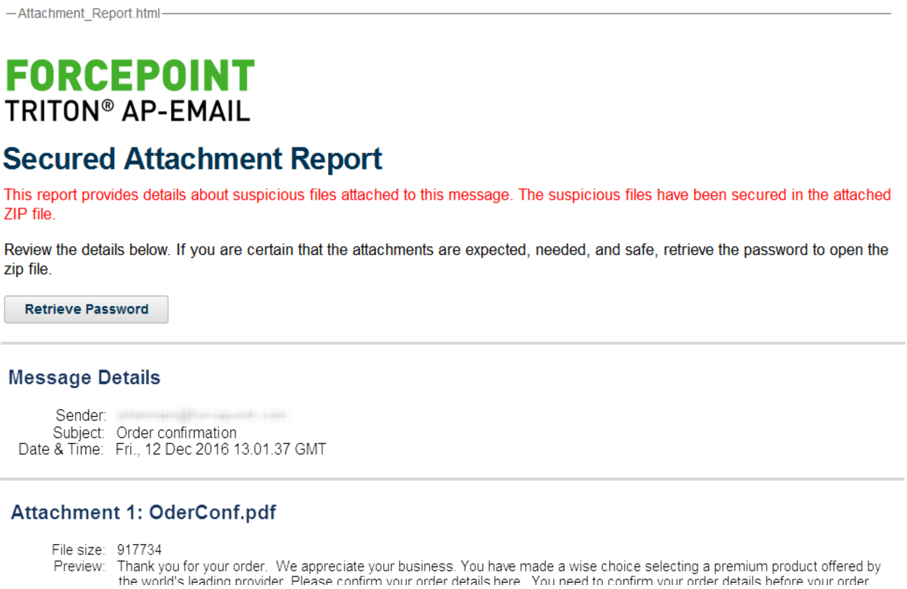
For your protection, the attachments have been placed in a password protected ZIP file. View Attachment_Report.html (attached) for details. The report will help you decide if you want to open the suspicious attachments. The report also includes support for retrieving the ZIP file password.

Opening a suspicious attachment could lead to your computer being compromised or infected. Open the attachment only if you're sure it's safe. For questions and assistance, please contact your IT team.

Confirmation of order attached. Verify your purchase immediately!

Click here to report this email as spam.

Here is a sample Secured Attachment Report.



Attachment_Report.html

FORCEPOINT
TRITON® AP-EMAIL

Secured Attachment Report

This report provides details about suspicious files attached to this message. The suspicious files have been secured in the attached ZIP file.

Review the details below. If you are certain that the attachments are expected, needed, and safe, retrieve the password to open the zip file.

Message Details

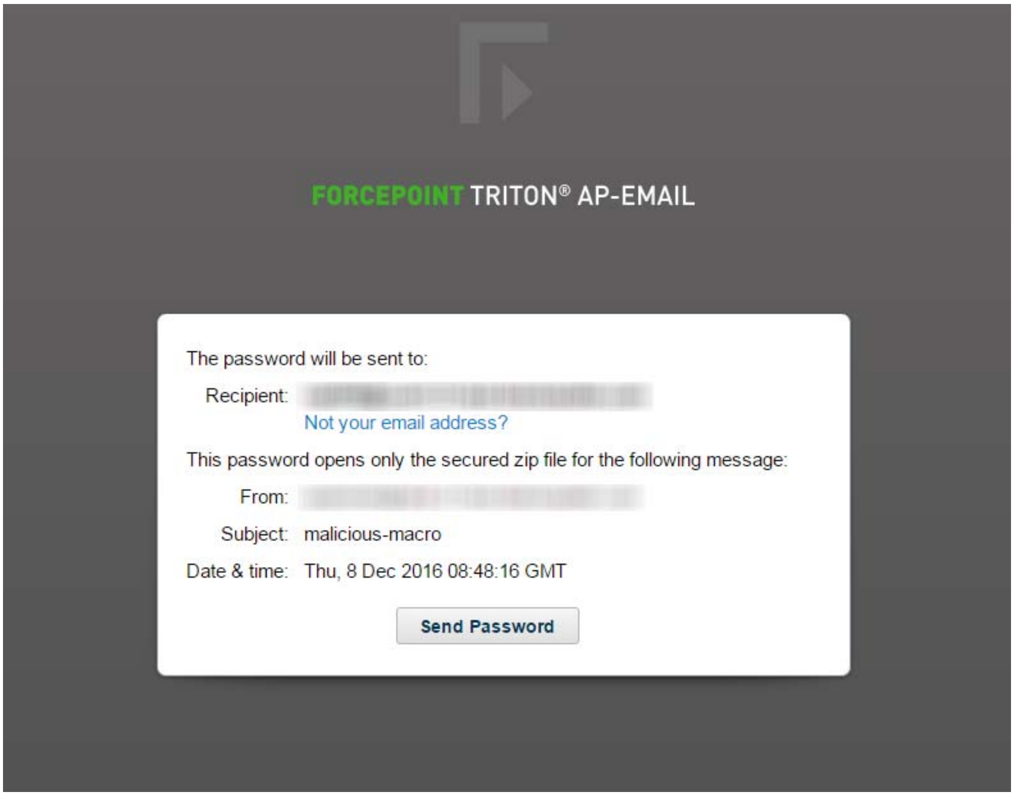
Sender: [redacted]
Subject: Order confirmation
Date & Time: Fri., 12 Dec 2016 13.01.37 GMT

Attachment 1: OderConf.pdf

File size: 917734
Preview: Thank you for your order. We appreciate your business. You have made a wise choice selecting a premium product offered by the world's leading provider. Please confirm your order details here. You need to confirm your order details before your order

By securing the attachment in this way, the recipient and organization have the time and information needed to take a fully considered action.

Should the recipient choose to retrieve the zip file password by clicking the **Retrieve Password** link, they are taken to a Forcepoint TRITON AP-EMAIL portal to confirm their request. Once confirmed, a separate email is sent containing the password.



The password will be sent to:

Recipient: [redacted]
Not your email address?

This password opens only the secured zip file for the following message:

From: [redacted]
Subject: malicious-macro
Date & time: Thu, 8 Dec 2016 08:48:16 GMT

Only the original recipient can receive the password. If a message with secured file attachments is forwarded, recipients of the forwarded message must ask the original recipient for the password.

Should you choose to enable the feature and secure suspicious file attachments, it's very important that you prepare your users to receive them and take appropriate action. Users should know that:

1. Their email security service analyzes email attachments for malicious content. When found, the attachment is not delivered.
2. The email security service also looks for suspicious file attachments. An attachment can be suspicious for several reasons including the reputation of the sender or sending domain, attachment file type, attachment size, the spam score of the message, and other attributes.
3. When a suspicious attachment is found:
   - The attachment is placed in a password protected zip file and delivered, along with the original message, to the intended recipients.
   - A **Secured Attachment Report** is also attached to the original message. The report includes the message details, a preview of the attachment content, and support for retrieving the password for the secured zip file.
4. Recipients should carefully examine the Secured Attachment Report to help determine if the attachment is safe.
5. Opening a suspicious attachment could lead to the computer being compromised or infected. Recipients should open the attachment only if they're sure that it's safe. If in doubt, contact the IT team for assistance.
6. If a user receives a forwarded copy of a message with the secured zip file, they need to ask to original recipient for the password. Only the original recipients can retrieve the password.

The **Secure suspicious attachments** feature is enabled at the policy level (per policy).

To enable the feature:

1. In the portal go to **Email** > **Policies** > ***policy_name*** and select the Content Filter tab.
2. In the Inbound Content Filter section, enable **Secure suspicious attachments**.
3. Click the adjacent **Customize settings** link to review and customize the message that is inserted into the original message.
4. You can also add sender addresses or domains to exclude from the secure attachment rule.
5. Save your changes.

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 13-December-2016

- When an end-user used the **Report as spam** feature to report a message as spam, some URLs were constructed in such a way that the TRITON AP-EMAIL service could not process the URL.
- Customizing the **Subject line prefix** value (default string) of a notification email (Email > Policy Management > Notification Email > *selected_policy*), did not change the string that was inserted into the Subject line of a quarantined message. The default value was still inserted.
- When processing a very large CSV file for bulk upload of personal email subscriptions (Email > Personal Email Subscriptions > Bulk Upload), the process sometimes failed due to a timeout error.
- The service response to SPF (Sender Policy Framework) error messages has been changed to reduce "unknown" results and improve interpretation of whether or not an email message is spoofed.
- Defang parsing of HTML email messages containing embedded fonts or media has been improved, allowing such messages to be delivered, rather than being quarantined.