Case report for event ID: 1005

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1005	Suspicious Attachment found in email	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.	Phishing	Low	Nov 28th 2025 at 19:39

Alert details

datasource: email

timestamp: 11/28/2025 11:37:05.272

subject: FINAL NOTICE: Overdue Payment - Account Suspension Imminent

sender: john@hatmakereurope.xyz

recipient: michael.ascot@tryhatme.com

attachment: ImportantInvoice-Febrary.zip

content: URGENT: Your account is 30 days past due and will be suspended today unless immediate payment is processed. Legal action will commence if payment is not received within 24 hours. Open the attached invoice immediately to view payment options and avoid legal consequences.

direction: inbound

Incident report

Edit report

Incident classification

True positive | False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

Time of activity: 11/28/2025 11:37:05.272
List of Affected Entities:

- sender: john@hatmakereurope.xyz
- recipient: michael.ascot@tryhatme.com
- attachment: ImportantInvoice-Febrary.zip

Reason for Classifying as True Positive:

- The email does not specify any company or services that need payment.
- The message requires the recipient to click the link, which can trigger malware execution.
- The email indicates social engineering: urgency to potentially deceive a recipient into following the given instructions.

Reason for Escalating the Alert:
- The file needs to be isolated
- The sender and domain need to be tracked and blocked

Does this alert require escalation?

Yes | No

Save and close alert

Complete IR:

Time of activity: 11/28/2025 11:37:05.272

List of Affected Entities:

- sender: john@hatmakereurope.xyz
- recipient: michael.ascot@tryhatme.com
- attachment: ImportantInvoice-Febrary.zip

Reason for Classifying as True Positive:

- The email does not specify any company or services that need payment.
- The message requires the recipient to click the link, which can trigger malware execution.
- The email indicates social engineering: urgency to potentially deceive a recipient into following the given instructions.

Reason for Escalating the Alert:

- The file needs to be isolated
- The sender and domain need to be tracked and blocked

Recommended Remediation Actions:

- Block the email
- Block the domain
- Isolate and delete attached zip file
- Pocket Training for awareness or post-shift meeting about how to handle similar intent type of email

List of Attack Indicators:

- Social Engineering - urgency

- Unclear details

- Attached zip file