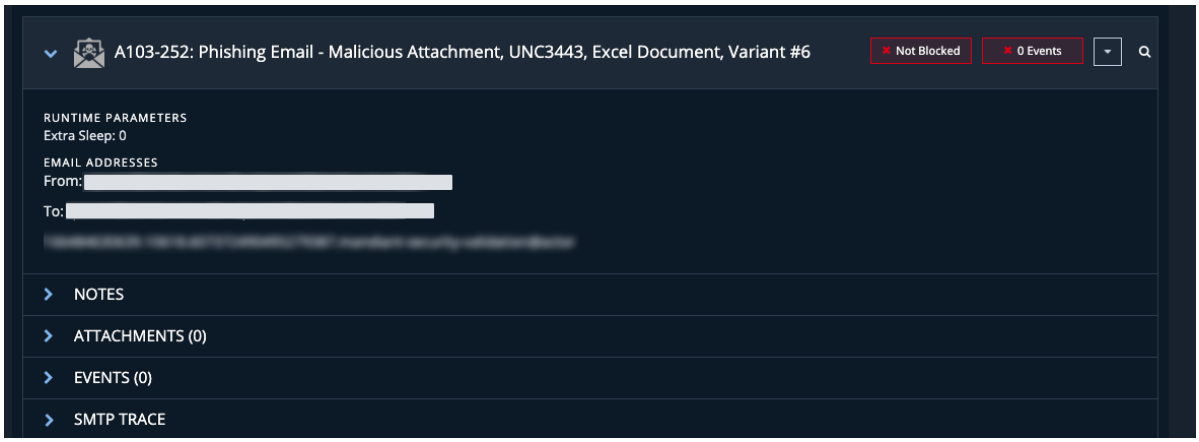
UNDERSTANDING EMAIL ACTION RESULTS

Job results from an Email Action provide information about whether the Action was blocked. In the following screenshot, we can see that our malicious file was not blocked, meaning that we could have a misconfiguration of our firewall or other security technology responsible for blocking such content.



Email Job Results

Email Actions are considered to be in a blocked state when any of the following occurs.

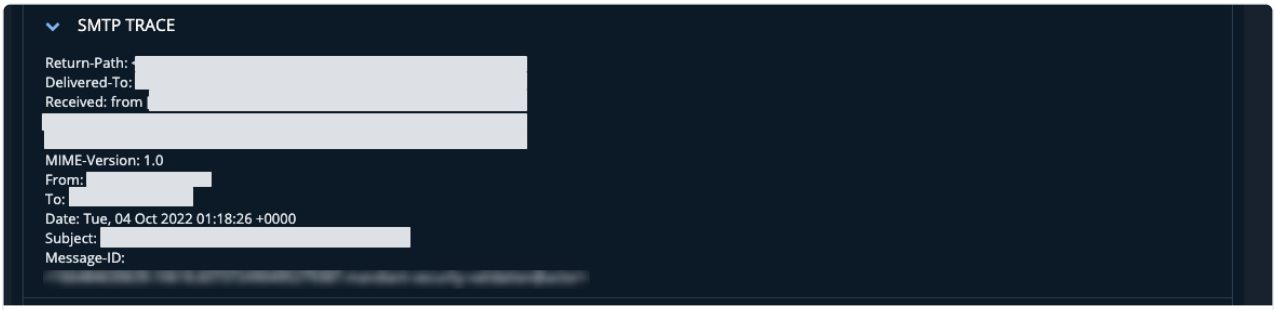
- Email is bounced to the Sender
- Email arrives at the Recipient but does not contain what is expected (bytes were modified)
- Email is not received in the timeframe specified in **Settings > Email Actions** (see **Configuring Global Email Action Settings (https://docs.mandiant.com/home/configuring-global-email-action-settings)**)

SMTP Trace

Message-IDs are critical for tracing the path of a message through an SMTP server chain. Because SMTP is a store-and-forward protocol, and messages may transit several servers between the two Actors, tracing the email based solely on source and destination IP address is not practical.

To facilitate SMTP tracing, Email Action Job results contain useful information for testing data-loss prevention controls:

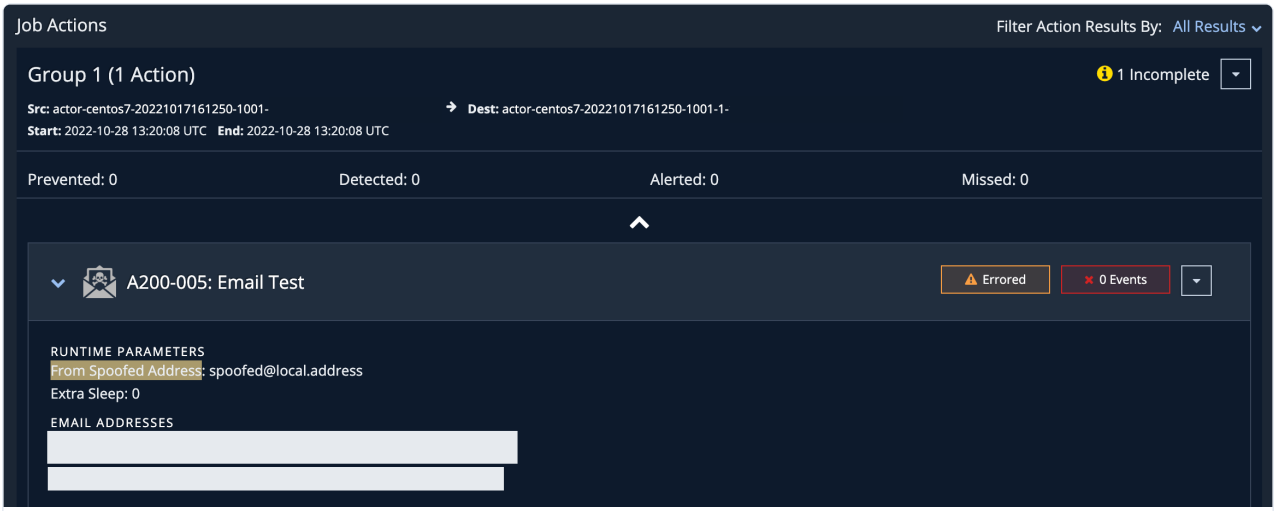
- **SMTP Trace information**: When an email is received by the destination Actor, MSV records and display the SMTP Trace Information in the Email Log section of the results. This information primarily consists of "Received:" headers.
- **Message-ID header**: A unique identifier in each Email Theater email that MSV sends. This information ensures that the Message-ID header is known; otherwise, it would've been assigned automatically by the receiving SMTP server and may not be available to the user.



SMTP Trace Information

Spoofed Email Address

Email Action Results may include a spoofed email address. This address appears under runtime parameters and is used to simulate forging an address in phishing attempts targeted at a recipient. For more information on spoofed email addresses and the supported server types, see **Running Email Actions (https://docs.mandiant.com/home/msv-running-email-actions)**.



Spoofed Email Runtime Parameter