Proofpoint Threat Response 5.6.0 – Release Notes

August 2021

Overview

PTR/TRAP 5.6.0 introduces significant enhancements to the processing of messages reported via the Abuse Mailbox Monitor / CLEAR as well as major database performance improvements related to processing and storing alert information.

The enhancements pertaining to alert processing for CLEAR should greatly benefit scenarios where several recipients are included in a single suspicious message reported by an end user. Consequently, an analyst will experience fewer alerts created per incident. This leads to better visibility of abuse message reporters and ultimately, it improves the overall system performance over time.

All customers who use PTR/TRAP for abuse mailbox monitoring with CLEAR are advised to upgrade to this version, thus improving the general stability and performance of PTR/TRAP.

CLEAR Enhancements

New Alert Model for Abuse Mailbox Monitor / CLEAR Source

This release introduces a new alert model for the Abuse Mailbox Monitor / CLEAR alert source whereby a *single* alert is created for each reporter of an abuse message irrespective of how many recipients there are on the "To" and "CC" lines of the message. This change departs from the previous system behavior where an alert was created for every recipient on the "To" and "CC" lines of a reported message.

The following scenarios illustrate how this change is beneficial to security analysts as well as the system.

	Previous Behavior	**New Behavior – 5.6.0**
Identification of the Abuse Reporter	An alert created for every To/CC recipient made it difficult to identify who reported the message.	Only one alert is created. The Target or Recipient field denotes the reporter.
Alerts for Legitimate Recipients	An alert was created for every To/CC recipient regardless of whether they were internal to the organization or not.	Only one alert is created per abuse reporter. None of the alerts denote an external recipient or email domain.
Multiple Reports of the Same Abuse Message	Each abuse report created alerts for every To/CC recipient; for example, a message sent to 100 recipients and reported by two users would create 200 alerts.	Each abuse report creates one alert; for example, a message sent to 100 recipients and reported by two users will create two alerts.

Peer Following of "To" and "CC" Recipients for Quarantine Actions

PTR/TRAP 5.6.0 introduces a new capability to quarantine message copies from recipients on the "To" and "CC" lines of a message as a part of manual and automated response actions. This capability ensures that messages in need of remediation are removed from the To/CC recipients.

Furthermore, a new checkbox option is visible for the **Move Email to Quarantine** response to enable *Peer Following*. Note that the checkbox appears in the automatic match condition response as well as the manual response within an incident.

Default Behavior: Move Email to Quarantine Response with Peer Following

For a manual response action, the new checkbox option is the default. Disenable it if the message should not be quarantined for "To" and "CC" recipients.

Following an upgrade to 5.6.0, automatic match condition responses are defined as follows:

- Abuse Mailbox Monitor match conditions that include a quarantine response have the *Peer Following* option enabled by default; this maintains parity with previous behavior for quarantining message copies for "To" and "CC" recipients.

- Other sources, such as TAP and Smart Search, that include a quarantine response, *do not* have the *Peer Following* option enabled by default; however, it can be enabled.

Database Indexes to Accelerate CLEAR Alert Processing

PTR/TRAP 5.6.0 adds various database indexes to accelerate the alert processing of Abuse Mailbox alerts. This should mitigate the effects of situations where large volumes of alerts overwhelm the alert processing queue and lead to alerts without incidents that cannot be accessed via the UI.

Bug Fixes

Error Exporting Reports to PDF

PTR/TRAP 5.6.0 addresses a bug that prevented a report from being exported to a PDF file, affecting versions 5.4.2, 5.5.0, and 5.5.1.

Abuse Mailbox Polling Failures Due to EWS API Request Failures (No Longer Require Restarts)

PTR/TRAP 5.6.0 handles request failures from EWS API's more efficiently by continuing to poll for subsequent alerts if individual requests fail due to lack of EWS API response. This fix eliminates the need for rebooting the system to recover it from a "jammed" state.

Vulnerability Fix Pertaining to Cross-Site Tracking (XST)

PTR/TRAP 5.6.0 addresses vulnerabilities related to Cross-Site Tracking (XST) Attacks.

Download Instructions

PTR/TRAP 5.6.0 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

- 5.6.0 OVA File (Fresh Installations and Upgrades From 3.x, 4.x) – Download OVA and SHA-256.
- 5.6.0 IMG File (Upgrades From 5.x) – Download IMG and SHA-256.
- 5.6.0 VHDX File (AWS AMI Installations) – Download VHDX and SHA-256.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.6.0. There are a few changes in the following sections in both guides. Please refer to the PTR AWS Installation Guide for instructions concerning the installation of 5.6.0 on AWS.

Upgrade Instructions: 3.x to 4.x

Customers using PTR/TRAP versions 3.x to 4.x are highly encouraged to upgrade to version 5.6.0 to benefit from new feature improvements and security hardening.

The upgrade process from a 3.x or a 4.x version requires a new virtual machine to be set up using the 5.6.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.6.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.6.0.

Upgrade Instructions From 5.x

Upgrading from PTR/TRAP 5.x to 5.6.0 can be completed "in place" (on the appliance) using the IMG file. Refer to the Console Guide for instructions.

AWS Deployments – Upgrade Instructions

The upgrade process for AWS deployments requires a new EC2 instance to be set up using the 5.6.0 VHDX file. Data must be migrated from the older version of PTR/TRAP to 5.6.0. Refer to the AMI Installation Guide for detailed instructions for deploying PTR/TRAP 5.6.0 on AWS.