Proofpoint Threat Response 5.0.1 – Release Notes

December 2019

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) version 5.0.1 delivers fixes to defects affecting version 5.0.0 and enhancements in Closed Loop Email Analysis and Response (CLEAR).

Enhancements

Running Scripted Responses Following a CLEAR Rescore

PTR 5.0.1 supports the ability to run a scripted response when an abuse message (submitted via CLEAR) has been reanalyzed by Proofpoint, thus enabling a host of customized workflows (with a PTR-licensed appliance).

CLEAR-ID Displayed Under Incident Activity for Easier Follow-Up With Proofpoint

After the reanalysis of a reported abuse message, PTR/TRAP 5.0.1 displays a CLEAR-ID associated with such a reanalysis. The ID can be found on the *Incident Activity* page. Note that if a customer reports a false negative (FN) or false positive (FP) to Proofpoint based on the abuse disposition from the CLEAR reanalysis, they should include the CLEAR-ID. This enables the support team to act on the request promptly.

TAP Connectivity Errors Displayed Under Source Errors

In the event of a connectivity error between the Proofpoint TAP source and PTR/TRAP 5.0.1, the problem is highlighted in *Source Errors* alongside the username.

Defect Fixes

PTR/TRAP Installation Failures With Hypervisors Running Over Certain CPU Types

PTR/TRAP 5.0.1 fixes a problem related to 5.0.0 concerning the inaccessibility of the UI after installation because of a compatibility issue with certain CPU models on servers running VMware ESX.

PTR/TRAP Installation Failures With IP Address Conflicts for Docker Interfaces

PTR/TRAP 5.0.1 fixes a problem related to 5.0.0 concerning the inaccessibility of the UI after installation because of a network address conflict with interfaces running Docker used internally on the appliance. If the network address range used by Docker overlaps with any others in the PTR/TRAP VM's environment, certain internal services do not remain functional. In PTR/TRAP 5.0.1, the Initial Configuration Wizard allows you to define the IP subnets to be used by these Docker services, thus preventing any conflict.

Initial Configuration Wizard Enforces a Minimum Length for Password

The Initial Configuration Wizard in PTR/TRAP 5.0.1 requires a minimum length of seven characters with respect to the system administrator password, thus resolving the issue of appliance inaccessibility due to an empty password.

CLEAR: Quarantines Work With Multiple Exchange Servers/Domains

PTR/TRAP 5.0.1 includes a fix involving abuse messages that could not be quarantined if the reporting end-user mailboxes resided on Exchange servers or domains different from those hosting the abuse mailbox.

CLEAR: Handling of Messages With Invalid Characters in Message-ID

Abuse messages forwarded to PTR/TRAP by PhishAlarm Analyzer sometimes contained invalid characters (spaces) and/or missing delimiters in the Message-ID, thus preventing PTR/TRAP from finding the original message. PTR/TRAP 5.0.1 handles these cases competently by ensuring that an original message can be located using the Message-ID.

CLEAR: Handling a Large Number of Abuse Messages With Large Attachments

When several hundred abuse messages with large-sized attachments are reported simultaneously (into an abuse mailbox), PTR/TRAP 5.0.1 processes them more efficiently and create alerts and incidents.

Download Instructions

PTR/TRAP 5.0.1 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

- 5.0.1 OVA File (Fresh Installations and Upgrades from 3.x, 4.x) – Download OVA and SHA-256.
- 5.0.1 IMG File (Upgrades from 5.0.0) – Download IMG and SHA-256.

The API documentation for PTR/TRAP 5.0.1 can be found here.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.0.1. There are a few changes in the following sections in both guides.

- The virtual machine requirements include a slightly bigger HDD for the base system.
- The required ports for network communication include new entries for clustered deployments.
- The initial configuration wizard consists of a different set of steps as compared to older versions.

Upgrade Instructions: 3.x to 4.x

The upgrade process from a 3.x or a 4.x version requires a new virtual machine to be set up using the 5.0.1 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.0.1. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.0.1. The FAQ (Frequently Asked Questions) section contains answers to several common queries about the upgrade process.

Upgrade Instructions From 5.0.0

Upgrading from PTR/TRAP 5.0.0 to 5.0.1 can be completed “in place” (on the appliance) using the IMG file. Refer to the Console Guide for instructions.

Note: An issue in PTR/TRAP 5.0.0 prevents rolling back to 5.0.0 after the appliance has been upgraded and running 5.0.1. Before upgrading the appliance from 5.0.0 to 5.0.1, it is advisable to take a VM snapshot first.