Proofpoint Threat Response 5.1.0 – Release Notes

March 2020

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) version 5.1.0 delivers several key benefits and enhancements, spanning Closed Loop Email Analysis and Response (CLEAR), Targeted Attack Protection (TAP) false positives, quarantine reporting, and system maintenance.

Platform – AWS

PTR/TRAP 5.1.0 introduces the option to deploy the application in the Amazon Web Services (AWS) public cloud. For customers who wish to benefit from the many features supported by the product but are averse to setting up any on-premises infrastructure for it, PTR/TRAP can now be deployed as an Amazon Machine Image (AMI) within an AWS Elastic Compute Cloud (EC2) instance. Customers must instantiate **their respective** PTR/TRAP AMIs within EC2. (This is similar to setting up a Virtual Machine (VM) in their own datacenters.)

This platform offering complements the existing deployment option for PTR/TRAP on VMware. Both platform offerings support the same features for alert ingestion, alert enrichment, incident management, and reports. The key differences with the AMI offering pertain to the underlying platform:

- The underlying operating system is Amazon Linux 2;
- Upgrades to a newer version must be performed by moving data between the old and new instances; and
- High Availability, while it is not offered, can be compensated for by using a variety of tools and features in AWS, such as Termination Protection, Elastic Block Storage (EBS) snapshots, AWS Cloud Watch, or other preferred methods.

The AWS Installation Guide contains a detailed set of steps for deploying PTR/TRAP in AWS.

The Console Guide includes some important differences in the platform pertaining to appliance management activities.

CLEAR Enhancements

Improved Categorization of Reported Abuse Messages That Are Spam

PTR/TRAP 5.1.0 introduces a new **Spam** disposition for reported abuse messages following a reanalysis by Proofpoint Threat Intelligence. This enables new workflows for security teams so that they can differentiate responses to spam messages from those to malicious messages and thus leverage the benefits of increased automation. Ultimately, security teams can analyze the volume of reported spam messages and drive changes to their email spam engines that reduce or prevent spam traffic from entering their environment over time.

Better Controls for Triggering Match Conditions on Reported Abuse Messages

PTR/TRAP 5.1.0 allows for a more granular control on the “triggering” of match conditions for reported abuse messages. Given the following scenarios, match conditions can now be set up to “trigger”

- when a reported abuse message is received in PTR/TRAP as a new alert,
- after a reported abuse message is reanalyzed by Proofpoint Threat Intelligence, or
- both of the above.

Such granular control enables several use cases based on the updated abuse disposition value, such as

- reassigning an abuse incident based on initial and final disposition values,
- notifying end-users *after* the message is given a disposition with a specific value and
- sending incident data, including the abuse disposition to an external system (SIEM, ticket mgmt., etc.).

Running Additional Responses Following a CLEAR Re-analysis

Building on the ability to run Scripted Responses in 5.0.1, PTR/TRAP 5.1.0 allows the following responses to be run after an abuse message (submitted via CLEAR) has been reanalyzed by Proofpoint:

- Disable a user account in active directory.
- Reset a user account password in active directory.
- Invalidate a user account password in active directory.
- Custom Responses (requires a *full Threat Response* license).

Note that the responses relating to active directory can be leveraged to protect the accounts of special users, namely VIPs/employees in sensitive roles, if there is reason to believe that a message reported by them was dispositioned as malicious and/or if they were victims of a phishing attack.

Running Match Conditions Following a CLEAR Analysis Based on LDAP Attributes

PTR/TRAP 5.1.0 supports the ability to run match conditions based on the values of LDAP attributes associated with an abuse message reporter, when an abuse message (submitted via CLEAR) has been reanalyzed by Proofpoint. This enables security teams to trigger automated responses based on the abuse reporter’s role, location, etc. For example:

- Notify the end-user via email in a specific language based on the user’s location.
- Assign the abuse incident to a special team based on the user’s role (executive, payroll employee, etc.).

Support for SENDER Tag in End-User Abuse Feedback Email Templates

The end-user email template for abuse feedback in PTR/TRAP 5.1.0 supports the use of the *SENDER* tag in addition to the existing tags, namely *RECIPIENT*, *SUBJECT*, and *RECEIVED DATE*. When the email template is used to send out an email notification to the abuse reporter, the SENDER tag is substituted with the email address of the envelope sender (in the *original* reported abuse message).

Utilization of this tag lets security teams include additional context about the abuse message in the email notification. Moreover, it educates users to exercise caution if they receive future emails from the specified sender.

PTR/TRAP Enhancements

Ability to Automatically Close Incidents Reopened for TAP False Positive Alerts

PTR/TRAP 5.1.0 provides the ability to automatically close an incident that was reopened upon receiving a False Positive (FP) alert from Targeted Attack Protection (TAP). Previously, such reopened incidents could be set up to perform an automatic “undo quarantine” action on any previously quarantined messages. Currently, such incidents can be configured to close automatically, subject to the following conditions:

- The incident was previously closed and was reopened owing to an FP alert.
- All “automatic undo quarantine” actions have been successfully completed.

This allows you to focus only on incidents with FP alerts that require manual action such as those involving failed "undo quarantine" operations.

Improved Counts for Quarantined Messages in Abuse Incidents

PTR/TRAP 5.1.0 has implemented an improved method for displaying the counts of messages that were quarantined in an abuse incident. Previously, message counts for both successful and failed quarantine actions reflected the latest attempt of that action on messages associated with the incident. Currently, these counts reflect the cumulative value over all quarantine attempts (automatic and manual) made during the time in which the incident exists.

System Maintenance Features and Enhancements

These capabilities enable a system administrator to ensure that PTR/TRAP is loaded with the most relevant and recent incidents over time and have the system performant in a way that the user interface functions efficiently.

Scheduled Purges

PTR/TRAP 5.1.0 introduces the ability to create and manage schedules to purge incidents regularly and automatically. System administrators can set up one or more "purge schedules" which run at specified intervals and act on specific filters, namely *Alert Sources* and *Incident Creation Date Range*.

Schedules can be *enabled* or *disabled* based upon your preference. At the end of a scheduled run, an email notification can be sent to an administrative user for any follow-up. Moreover, the results of each scheduled run can be viewed under *Incident Purges* in *System Settings*. Note that this section contains details of a "purge" operation, including its configuration and results.

Purge Filter for False Positive Incidents

PTR/TRAP 5.1.0 includes a new filter for both scheduled and manual incident purge operations. Essentially, the filter permits system administrators to target incidents whose alerts are *only* false positives received from TAP (Targeted Attack Protection). Thus, system administrators can manage false positive incidents that provide little value to the security team and eliminate any clutter in reports and metrics associated with incident management.

Bulk Action to Purge Incidents

PTR/TRAP 5.1.0 lets system administrators "trigger" an incident purge as a bulk action from the *Incident List*. The bulk action can be executed on any filtered list of *closed* incidents. For example, a system administrator can filter incidents that are assigned to a non-existent analyst or associated with the value of a specific incident field (*Severity*, *Classification*, *Attack Vector*, etc.) and perform a purge operation on these incidents.

This feature can only be used by system administrators (belonging to the "Admins" team). Further, the bulk action can only be triggered when selected incidents are in the "closed" state.

Download Instructions

Please refer to the 5.1.1 Release Notes for instructions to download PTR/TRAP 5.1.1, instead of version 5.1.0.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.1.0 on VMWare.

Please refer to the PTR AWS Installation Guide for instructions concerning the installation of 5.1.0 on AWS.

Upgrade Instructions from versions older than 5.0.0

The upgrade process from a 3.x or a 4.x version requires a new virtual machine to be set up using the 5.1.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.1.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.1.0. The FAQ (Frequently Asked Questions) section contains answers to several common queries about the upgrade process.

Upgrade Instructions From 5.0.0 and above

Upgrading from PTR/TRAP 5.0.0 and above 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. Before upgrading the appliance from 5.0.0, it is advisable to take a VM snapshot first.