Proofpoint Threat Response 4.6.0 – Release Notes

June 2019

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) 4.6.0 deliver several features and enhancements for abuse mailbox handling, Closed Loop Email Analysis and Response (CLEAR), incident management and overall user experience.

CLEAR Enhancements

Better automated processing of Low-Risk abuse messages

PTR/TRAP 4.6.0 improves on the disposition delivered for abuse messages that were analyzed by Proofpoint Threat Intelligence via PhishAlarm Analyzer.

In PTR/TRAP 4.5.0, the **Unknown** abuse disposition was applied to incidents in two cases: when messages were deemed clean and when messages had a minor cause of concern but not enough to be labeled Malicious or Suspicious or Bulk. PTR/TRAP 4.6.0 introduces a new abuse disposition value called **Low-Risk**. This is applied to incidents whose abuse messages are deemed as clean by Proofpoint Threat Intelligence, thus reducing the number of delivered Unknown dispositions.

Incidents with Low-Risk disposition can be set up for automatic closure by enabling a pre-defined match condition in PTR/TRAP 4.6.0. The match condition is named **Close Incidents for Low Risk Email**.

Customers can continue to use the **Known-Good** abuse disposition when manually analyzing abuse message incidents, for delivering a clean verdict and executing appropriate response actions thereafter.

Abuse Feedback Email Notifications

PTR/TRAP 4.6.0 provides a new type of response called **Send Email Notification** that notifies reporters of abuse messages after a message has been analyzed automatically or manually. This response can be used to provide effective feedback to an abuse message reporter based on how the message was classified.

Using this response, the system can notify an abuse reporter when a message is automatically classified as Bulk or Low-Risk, and when a message is manually classified as Known-Good by a SOC analyst.

These email notifications can be setup as templates in System Settings. On upgrading from an older version to 4.6.0, the system will be setup with default templates for acknowledgment of bulk emails and clean emails.

TRAP Features and Enhancements

Automatic Undo Quarantines for TAP False Positive Alerts

PTR/TRAP 4.6.0 now includes the ability to ingest False Positive (FP) alerts from Targeted Attack Protection (TAP) and automatically restore emails that were previously quarantined by these alerts. This feature effectively addresses situations where TAP FP's previously required laborious manual undo-quarantine actions across incidents. The ability to automatically undo-quarantine can be enabled in the TAP source settings; this setting will be turned on by default after an upgrade to 4.6.0 from an older version.

For querying the presence of TAP FP's, the Incident List can now be filtered on FP alerts received from TAP.

The Incident Details API has also been enhanced with information about false positives. The API response includes the following event-level fields:

- **falsePositive** – an event-level Boolean field set for FP alerts/events
- **falsePositiveReceivedAt** – an event-level timestamp field denoting when the FP alert was received.
- **false_positive_count** – an incident-level field indicating the total FP's received for an incident

Reset Password for User Accounts in Active Directory

PTR/TRAP 4.6.0 supports a new type of response that can reset passwords for one or more Microsoft AD user accounts that were associated with an alert. This can be useful in cases where an alert indicates that a user account was associated with suspicious activity and a change of credentials would prevent further account compromise. After execution of this response, affected users will be forced to change their AD password during their next attempt to login.

With the availability of multiple Active Directory responses, PTR/TRAP 4.6.0 includes a new team-level permission called **Active Directory Responses**. This permission enables SOC team members to configure and manually execute the responses for disabling a user account or forcing a password reset.

Filter internal email domains for quarantine

PTR/TRAP 4.6.0 includes the ability to list internal email domains for use during the quarantine action. These domains can be configured under **System Settings → Internal Email Domains** and the use of this list can be activated under **System Settings → Quarantine Settings**. Activating the list of internal email domains will ensure that only mailboxes whose addresses belong to one of these domains are quarantined; mailboxes from any other domains will be excluded from quarantine and appear as skipped in the Incident Activity screen.

This ensures a cleaner quarantine experience without unnecessary failures corresponding to external domains. It improves the efficiency of a SOC analyst by focusing their time/attention towards genuine quarantine failures.

General Features and Enhancements

Progress Indicator on UI for CSV upload Sources

PTR/TRAP 4.6.0 features a detailed progress indicator for files uploaded into the Proofpoint Smart Search and Proofpoint CSV data sources. This enables PTR users to effectively track the progress of alert ingestions for large CSV files.

Improvements to accessing quarantine activity and actions

PTR/TRAP 4.6.0 includes a new Quarantines tab in Incident Activity that lists quarantine and undo quarantine actions for that incident. This tab can be reached with a single click from the Incident List by clicking on the **View** link next to the Quarantine label for an incident.

Customizable headers for emails added/removed from quarantine

When PTR/TRAP 4.6.0 is used in impersonation mode, the templated messages displayed as headers for quarantined emails can now be customized. These headers can be setup for each configured Exchange Server under System Settings, using plain text or HTML markup.

Bulk Action to set Incident-level fields

PTR/TRAP 4.6.0 includes a new bulk action called **Set Field** to set incident-level fields – **Incident Severity**, **Abuse Disposition**, **Classification** and **Attack Vector**. This action can also be applied to custom or user-defined incident fields, if they are enabled for use.

HTML and Plain-text Email Templates

All template types defined under **System Settings → Email Templates** now support both HTML and plain-text content types.

Bug Fixes

Date Picker widget in Reports

PTR/TRAP 4.6.0 contains a fix for the date picker widget used in several reports. The widget allows a user to pick a date correctly and renders the report after the complete date has been input.

Support for TLS v1.2 ciphers in LDAP

In PTR/TRAP 4.6.0, LDAP configurations created inside the Appliance Management Console support TLS v1.2 ciphers for communicating with configured LDAP servers.

Download and Upgrade Instructions

PTR/TRAP 4.6.0 requires a minimum of VMware ESXi 6.0. Please use Proofpoint CTS credentials to access downloaded images.

4.6.0 OVA File (Fresh Installs Only)
https://dl1.proofpoint.com/download/ThreatResponse/4.6.0/Proofpoint_Threat_Response_Installer-4.6.0.ova

4.6.0 IMG File (Upgrades Only)
https://dl1.proofpoint.com/download/ThreatResponse/4.6.0/Proofpoint_Threat_Response_Update-4.6.0.img

The API docs for PTR/TRAP 4.6.0 can be found at: https://ptr-docs.proofpoint.com/extensibility-guides/ptr-api/