Proofpoint Threat Response 5.0.0 – Release Notes

October 2019

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) 5.0.0 is a major release with a new platform which offers many enhancements. This release strengthens system integrity relating to appliance management, Closed Loop Email Analysis and Response (CLEAR), and Incident Management (via UI and APIs) by delivering performance, reliability, and usability improvements across these areas of the product.

Platform

The underlying Linux platform in PTR/TRAP 5.0.0 has been updated to a new version, namely CentOS 7, and includes the kernel and many system libraries. This version increases the stability, security, reliability, and performance of the appliance and enables Proofpoint to better support future enhancements to the platform.

New Appliance Management Console

The updated platform in PTR/TRAP 5.0.0 includes a new Appliance Management Console for monitoring and managing the system. The console offers several system management operations that are commonly used and lays the groundwork for future enhancements. It is accessible to PTR/TRAP Admin users via web browser and by visiting the appliance at https://appliance_host_or_ip:8080. Refer to the New Console Guide for additional details about the user interface.

Simplified System Shell

PTR/TRAP 5.0.0 employs a simplified system shell for SSH-based access. The shell requires a few basic commands to be configured in order to diagnose networking and offers a way to switch to the system-level shell. It also eliminates the need for a temporary shell license in order to enable easier access to the system, if necessary.

CLEAR Features and Enhancements

Better Classification of Reported Abuse Messages

To drive higher automation value with CLEAR, PTR/TRAP 5.0.0 incorporates changes in the CLEAR reanalysis engine that create fewer abuse messages classified with an “Unknown” disposition.

Messages previously classified with the “Unknown” disposition that have been analyzed by Proofpoint Threat Intelligence as part of the CLEAR workflow are now evaluated by the Threat Operation Center’s (TOC’s**)** rulesets, which are actively curated by Proofpoint Threat Researchers and updated regularly. After applying these rules, several messages are reclassified with “Suspicious,” “Bulk,” or “Low-Risk” dispositions and returned to PTR/TRAP for automatic response handling. This leads to a significant reduction in messages with an “Unknown” disposition that would otherwise require manual analysis by a Security Operations Center (SOC) team member.

Re-Attempting Quarantines and Undo-Quarantines With Increasing Back-Offs

PTR/TRAP 5.0.0 includes enhancements for carrying out quarantine and undo-quarantine operations on email messages as well as completing them more reliably.

These operations are known to fail at times, owing to connectivity issues or aggressive throttling by mail servers, namely Exchange, O365, and Gmail. Given such intermittent issues, PTR/TRAP 5.0.0 includes the ability to attempt a quarantine or an undo-quarantine several times on every message until the operation succeeds. The number of attempts is configurable as a global value under **System Settings → Quarantine Settings**. When an attempt results in failure, PTR/TRAP 5.0.0 backs off for a limited time before its next attempt. This interval increases over subsequent attempts since the mail server remains unavailable and is likely to continue causing failures. The intervals are set to the following values with a random jitter between 1,600 and 2,400 milliseconds:

# Retries	1	2	3	4	5	6	7	8	9	10
Back-off Intervals	2s	4s	6s	10s	4m	6m	20m	33m	53m	1 hr.

Any subsequent attempts beyond 10 are spaced one-hour apart.

Consequently, automatic and manual quarantine as well as undo-quarantine operations triggered in PTR/TRAP 5.0.0 can expect much higher rates of success when confronted with throttling. Ultimately, this translates into a reduced burden on the SOC analyst team in terms of monitoring and time wasted on follow-up measures.

Prioritized Email Headers for Easier Manual Inspection

SOC analysts continue to encounter incidents in email messages that require manual inspection before a response is confirmed. The "X-headers" associated with an email message often contain important information for analysts to understand about the context of a message, and thus classify a message correctly.

PTR/TRAP 5.0.0 provides a way to define a set of headers under **System Settings → Prioritized Email Headers**. These headers, when displayed in the *Alerts* tab of an incident associated with an email message, appear at the top of the list and are emphasized. This enables an analyst to prioritize them and to expedite the review process.

Further, PTR/TRAP 5.0.0 improves on the visual presentation of the email X-headers by displaying them clearly with options to view and download the headers in plain-text format.

Automatic Updates to Incident Severity Based on CLEAR Abuse Dispositions

As part of the CLEAR workflow for handling abuse messages, PTR/TRAP automatically sets the Incident Severity field based on the Abuse Disposition provided after a CLEAR reanalysis of a reported message.

Abuse Disposition	**Incident Severity**
Malicious	Critical
Suspicious	High
Bulk	Low
Low-Risk	Low

Messages with an “Unknown” abuse disposition do not change the incident severity in any way. The incident severity is also not downgraded to a less severe value.

Ultimately, SOC analysts can use incident severity to determine the extent of a threat across abuse message incidents and to prioritize the threat for further action.

Quarantine and Undo-Quarantine Email Notifications for Manual Operations

PTR/TRAP 5.0.0 provides a SOC analyst with the option to send end user email notifications during manual responses involving a quarantine or an undo-quarantine action carried out at the incident level or as a bulk action. These manual responses now include the selection of an appropriate email template that is used to notify the end users of a quarantine or an undo-quarantine action.

Undo-Quarantine Email Notifications for TAP False Positives

The Proofpoint Targeted Attack Protection (TAP) source in PTR/TRAP 5.0.0 can be set up to use an email notification template to inform any affected end users that a TAP false-positive alert resulted in an automatic undo-quarantine action.

Recipients of Quarantine Email Notifications Displayed Under Incident Activity

The Incident Activity section in PTR/TRAP 5.0.0 has been improved to show a list of end users who were notified via email of any quarantine or undo-quarantine actions carried out on their messages (in their mailboxes). This list of users is displayed at the end of the chain of messages that were subject to a quarantine or an undo-quarantine as a collapsible field.

Ability to Remove Proofpoint Threat Response Prefix in Email Templates

Email Templates for “Quarantine,” “Undo-Quarantine,” and “Abuse Feedback” in PTR/TRAP include the following title in the “Subject” field: *Proofpoint Threat Response*. In PTR/TRAP 5.0.0, this title is displayed in the editable “Subject” field of the email template. Importantly, removing this title removes it from any email notifications sent using these templates.

Incident Management Features and Enhancements

Basic and Detailed Modes for Global Search

“Global Search” in PTR/TRAP 5.0.0 includes two new modes of search, thus allowing the user to choose between faster search performance and more information.

The “Basic” mode of search runs at a great rate for all queries and returns fewer columns. Note that it excludes the “Campaign” and the “Infection Confidence” columns.
The “Detailed” mode of search includes all columns and has also been implemented to run slightly faster than its counterpart. A SOC analyst can switch between these modes by employing “User Preferences”.

Filter on Timestamps

PTR/TRAP 5.0.0 includes the ability to specify both date and time with filters on the **Created Within** and **Closed Within** fields. This is especially useful for dealing with a considerable number of daily incidents.

Filter on Quarantine Successes or Failures

PTR/TRAP 5.0.0 includes a new filter for incidents involving email messages that are associated with quarantine activity. This filter can be set up to search for incidents with a certain number of **Successful Quarantines** and/or a certain number of **Failed Quarantines**. This is useful when looking for incidents requiring manual examination for quarantine or undo-quarantine operations.

Purge Manually Created Incidents

Incident Purges in PTR/TRAP 5.0.0 includes a new option whereby manually created incidents that are not associated with any alerts or alert sources can also be purged. This option is available when selecting *Alert Sources* for those incidents to be purged and by choosing **Include Incidents With No Alerts**.

PTR/TRAP API Enhancements

The API documentation for PTR/TRAP 5.0.0 can be found at https://ptr-docs.proofpoint.com/extensibility-guides/ptr-api/ Refer to the documentation for details concerning these APIs.

API to Update Incident Description

PTR/TRAP 5.0.0 provides a new API to add or to update the *Incident Description* field for a given incident. The value specified in the API can be overwritten or appended to the existing description of the incident.

API to Close an Incident

PTR/TRAP 5.0.0 provides a new API to close a given incident. The comment to be appended to the closure of the incident can be specified as a parameter to the API.

Enhancements to “Get Incident Details API”

The Get Incident Details API has been enhanced to include the following fields of an incident:

- Incident Comment Objects
  - Username (who made the comment)
  - Comment Value
  - Comment Timestamp (when it was added)
- Closure Timestamp for a Closed Incident
- Closure Comments for a Closed Incident

In order to enable faster responses for incidents with a considerable number of events, the API supports a new query parameter called **expand_events**. If it is set to false, the API response contains an array of event IDs instead of full event details. The user can follow up with calls to the Alerts API for specific event id's in this array to obtain details about those events.

Additionally, note that in this case, the response does not include the **false_positive_count** key for an incident.

General Features and Enhancements

Invalidate Password for User Accounts in Active Directory

PTR/TRAP 5.0.0 supports a new type of response that can invalidate passwords for one or more Microsoft Active Directory (AD) user accounts that were associated with an alert.

This can be useful in cases where an alert indicates that a user's account was possibly compromised and a severe action, such as disabling the user account, can lead to collateral damage, e.g. Loss of files /resources associated with the user's organizational structure and privileges. Instead, this response can be used to set the user account's AD password to an inaccessible, random value, thus locking the user's account and preventing any further damage.

As soon as this response has been executed, affected end users must contact their IT administrator to set their account passwords to a known value once their accounts have been sanitized.

Enable/Disable an LDAP Server

PTR/TRAP 5.0.0 provides a flag to enable or disable LDAP syncs with a configured LDAP server under **System Settings → LDAP servers**. This is useful when dealing with a considerable number of LDAP servers whereby servers can be selectively disabled during maintenance downtimes or as part of configuration changes.

Query Custom LDAP Attributes for User Enrichment

PTR/TRAP 5.0.0 allows a system administrator to specify one or more custom LDAP attributes that are to be queried on an LDAP server and configured, under **System Settings → LDAP servers**, in addition to specifying the standard list of attributes already being queried. Such attributes can contain useful information about the end users on that LDAP server and can provide data pertaining to alerts involving those end users.

Ability to Enter Multiple Internal Email Domains

For deployments that deal with a considerable number of whitelisted email address domains to be quarantined, PTR/TRAP 5.0.0 enables a system administrator to set up several domains using a comma-separated list of domain values, under **System Settings → Internal Email Domains**.

Consolidated SOC Email Notifications for Large CSV Uploads

SOC email notifications that relate to *Incident Changes* and deal with conditions associated with *Incident Updates*, are used to notify the SOC analyst team about new alerts in an incident when the *New Alert* flag is enabled. This flag is used when uploading large CSV files containing several hundred rows, such as a Smart Search CSV Upload and a Proofpoint CSV Upload. In such cases, the SOC team receives a notification for every row in the CSV file.

PTR/TRAP 5.0.0 includes an option to consolidate the indefinite quantity of email notifications into a single email, which is sent after the alerts from the CSV file have been processed. The setting can also be programmed to not send any emails. Note that the *Link Alerts* option must be turned on. The option to specify this setting is available when editing the Smart Search CSV or Proofpoint CSV alert source.

Download Instructions

PTR/TRAP 5.0.0 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

5.0.0 OVA File (Fresh Installations and Upgrades) – Click here to download

An IMG file cannot be used for upgrading from previous versions and hence is not available for this release. Please refer to the **Upgrade Instructions** below for details about upgrading to PTR/TRAP 5.0.0.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions about installing 5.0.0. There are a few changes in the following sections on both guides.

- The virtual machine requirements include a slightly bigger HDD for the base system.
- The required ports for network communication include a few new entries for clustering if you plan to set up PTR/TRAP as a clustered deployment.
- The initial configuration wizard consists of fewer steps than its predecessor (used to set up older versions).

Upgrade Instructions

Since PTR/TRAP 5.0.0 provides an overhauled platform, the upgrade process, for all intents and purposes, differs as compared to previous versions. A new virtual machine must be set up using the 5.0.0 OVA file and data must be migrated from the older version of PTR/TRAP to the new one. Please refer to the Upgrade Guide for detailed instructions on how to upgrade an older version of PTR/TRAP to 5.0.0. The section entitled FAQ (Frequently Asked Questions) contains answers to several common queries about the upgrade process.

Upgrades from PTR/TRAP 5.0.0 to future releases will be conducted “in place” on the new appliance (as was done for earlier upgrades).