Using TRAP to Accelerate Abuse Mailbox Processing

Security awareness training helps organizations and users recognize phishing emails, and it instructs them to send suspicious emails to an abuse mailbox. But what happens to an email once it's been forwarded to the abuse mailbox?

Less Defined Processes Mean More Risk

You may have a well-documented process and staff assigned to monitor the abuse mailbox. Or, if you're like many organizations, you have relegated the abuse mailbox to an "I'll get to it when I have time" project.

In either case, the suspicious email that was forwarded to the abuse mailbox still resides in the original recipient's mailbox. That's a real risk if the message is truly malicious. In the worst-case scenario, the user assumes that because the IT or messaging team hasn't responded, the email is OK to open or click. This opens the door to ransomware, credential phishing, data theft and more.

Due to time constraints, reviewing messages in the abuse mailbox is often a low priority. This message analysis is not difficult, just time consuming. It involves looking at the message components to determine whether it's malicious. This can include several steps, such as:

- Creating an incident
- Deconstructing email headers
- Checking sender IP address
- Checking sending domain
- Reviewing sender reputation
- Analyzing links that lead to credential phishing or malware
- Analyzing attachments for threats, malware or other active content

The analysis process can yield a quick hit against a reputation system. But it takes longer if multiple systems need to be reviewed. In either case, analyzing messages in the abuse mailbox is always tedious and redundant.

Protection Through Automation

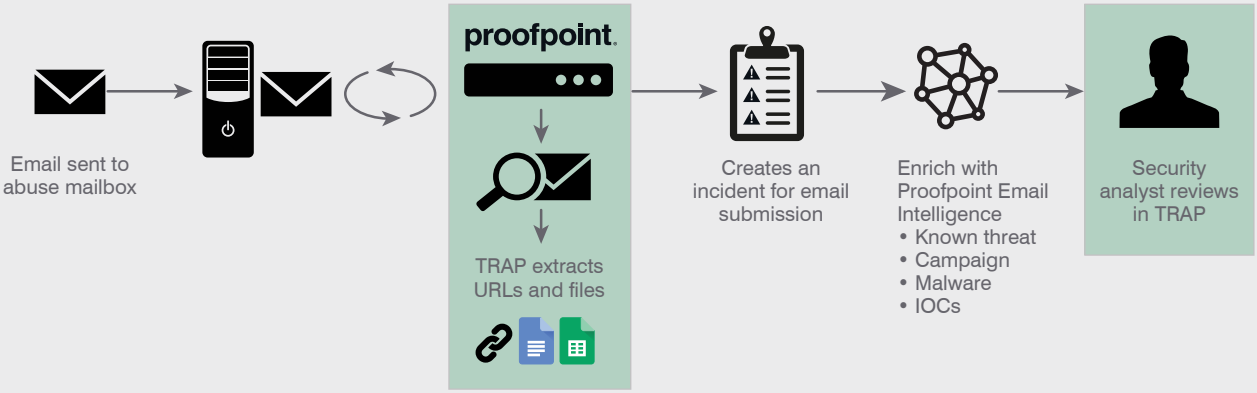
Proofpoint Threat Response Auto-Pull (TRAP) provides a better way to solve this problem. TRAP monitors the abuse mailbox for new messages from users. These messages are automatically dissected and analyzed against multiple intelligence and reputation systems. This determines if any of the content matches malicious markers. Each of the manual steps that an analyst would take are automatically performed in seconds. As a bonus, TRAP automatically geolocates suspect IP addresses and connects the suspicious email to any number of recent campaigns in the extensive Proofpoint database.

Messages may contain credential phishing templates, malware links, and attachments. All of these can be surfaced by automatically comparing them against our industry-leading reputation and intelligence systems to identify truly malicious messages.TRAP comes with the required reputation and intelligence feeds built in, so integration and setup times are minimal.

Eradicating Malicious Messages

Your messaging administrators can initiate "manual" or "auto-pull" on malicious messages to pull them out of the sender's mailbox. And if messages were forwarded to other users or distribution lists, the retraction follows the trail to pull the messages out and place them in a quarantine that admins can access. Using this process, those sent to the abuse mailbox are not only identified as malicious, but they are removed from the end-user's mailbox, eliminating further risk.

Whether it's a handful, dozens or hundreds of messages sent to the abuse mailbox, Proofpoint customers who use TRAP can take advantage of this capability today at no extra charge.



How TRAP monitors the abuse mailbox

LEARN MORE

For more information, visit **proofpoint.com/us/products/threat-response-auto-pull** or contact your Proofpoint representative to request a free trial.