Reporting Classification Mistakes to Commtouch

The Commtouch email security solution delivers a high rate of spam detection. However, no solution is perfect and sometimes unsolicited or malicious messages are mistakenly approved and sent to the end-users (false negatives) or legitimate business and personal correspondence may be mistakenly identified as unsolicited or malicious (false positives). By reporting any cases of false negatives and, more importantly, any cases of false positives to Commtouch, it is feasible to improve the overall performance even further. This will require you to set in place a special mechanism, either an automatic one that makes it more convenient for your customers to apply or a manual one that they should be educated to utilize.

To identify the reason for the mistake, Commtouch must be given the ability to analyze each report, sometimes looking into the actual filtered email. In the case of false negatives, the entire message is required for analysis. However, since these messages are considered spam by the end-user, the assumption is that privacy is not violated because the user already considers the messages to be unwanted. Analyzing the entire message is known to help significantly in avoiding repetition of the same mistake, taking into account the possibility that in the case of false positives, business confidentiality and privacy considerations must be applied. While in the case of false positives you can send the entire message for analysis, it is still sufficient to forward to Commtouch only the RefID record per-message.

Automatic Reporting Procedure

Commtouch recommends that you implement an automatic procedure in your application enabling your customers to report cases of false negatives and false positives with a click of a button. To implement this functionality, your developers should use the function calls ReportFN() and ReportFP() in the Commtouch SDK API. Alternatively, you can have the messages sent to one of your own email addresses and setup a procedure to forward the original message to Commtouch for analysis via email addresses detailed in the following section. If you choose this method, you should ensure that the original message is attached to ensure that all the original message-headers are also sent to Commtouch for analysis. Depending on your application, there could be various ways to implement the automatic reporting procedure. Commtouch's development team is available to assist you with specific recommendations.

Manual Reporting Procedure

When sending filtered messages to Commtouch for analysis, it is important to note that the original messages must be attached to your email report rather than forwarded to Commtouch. This is to ensure that all the original message-headers are also sent to Commtouch for analysis. Reports that do not contain the original message-headers cannot be analyzed.

Spam classification errors should be reported to the following addresses:

- False Negative to reportfn@blockspam.biz
- False Positive to reportfp@blockspam.biz

VOD classification errors should be reported to the following addresses:

- False Negative to reportfn@vodlab.biz
- False Positive to reportfp@vodlab.biz

WORKING PROCEDURE

Commtouch is unable to analyze old messages because spam characteristics are dynamically changing over short periods of time due to the nature of spam distribution methods. It is therefore, very important that you send reports about classification mistakes as soon as possible. In general, you should avoid sending reports that are older than one week.

Commtouch has set in place auto and semi-auto procedures to process your reports. To avoid delays in receiving a quality response, it is recommended that you comply with the working procedures detailed in this document (for example, ensure that reports of the same type are sent to the correct email address at Commtouch; use the correct syntax in the Subject line of the email reports, etc.).

For these procedures, your customers should be educated that whenever the end-users experience cases where the application failed to identify spam or blocks non-spam message, they should manually and individually report these mistakes to Commtouch by attaching and sending the messages to the above email addresses. Alternatively, they may attach and send the messages to one of your technical support email addresses, from which you will set up a procedure to forward them to Commtouch for analysis. For false negatives, the entire message including the original message-headers must be sent for analysis. For false positives, if the entire message is not attached and sent, then the customer must ensure that the RefID record is included per-message.

False Negative Reports to Commtouch

In order to analyze reports of false negatives, Commtouch's Monitoring team must review the actual email and determine why it was overlooked. Therefore, in reporting cases of false negative you must include the original filtered email as a MIME attachment. Do not forward the original filtered email to Commtouch because all the original headers may be lost.

The Subject line of your reports to Commtouch should include the following:

FN Report <Your Company Name> <Date of submission>

When reporting cases of VOD false negatives, the original email must be archived in a password-protected ZIP file to be extracted by Commtouch. The password for extracting the false negatives should be "infected".

False Positive Reports to Commtouch

In order to allow fast processing by the Commtouch's Monitoring team, your report to Commtouch about cases of false positive should contain a predefined format, as described in this document. Note that some of the stages in analyzing your report are fully automated. If you do not comply with the following instructions, then the response back by Commtouch may be delayed.

The Subject line of your reports to Commtouch should include the following:

FP Report <Your Company Name> < Date of submission >

There are only two ways to report cases of false positives to Commtouch: either send the RefID of each email within the body of the email report (one line per RefID record), or attach the original email containing the RefID record in a zip file. You may send mixed email reports containing both the list of RefID records and several other original emails in MIME attachment.

RefID records

RefID records are Commtouch's references to the transactions between your application and the Commtouch's Datacenter. Each filtered message receives its own RefID record. This value is used for diagnostics purposes by Commtouch to track the transaction and the reason that was determined for blocking. Note that some of the stages in analyzing your report are fully automated. Without the RefID, Commtouch is unable to analyze the report. The RefID is passed from Commtouch's embedded Detection Engine to your application. Typically, it is then added by your application to filtered emails as

a special x-header. The RefID may have a different format and structure depending on the version of the embedded Detection Engine.

When sending original filtered emails as MIME attachments you may group and archive several messages within one or more ZIP file(s). You should not, however, archive the messages in nested ZIP files. If you feel that it is necessary to protect the archive files with a password, then you transmit the password in advanced to your technical account manager at Commtouch and avoid changing the password too often to avoid confusion.

You should designate one or more focal points in your organization to send email reports to Commtouch (i.e., determined by the geography). Commtouch recommends creating a distribution list in your organization that will send email reports and receive responses from Commtouch rather than designating email addresses of individuals. Contact your technical account manager at Commtouch to notify the focal point and avoid sending email reports by other individuals.

Reports about Confirmed Solicited Bulk Email Misclassifications

If you reviewed your customer's report about cases of false positive before sending the report to Commtouch and you have found beyond any doubt that these misclassified messages include solicited bulk email traffic (i.e., newsletters or mailing lists) that Commtouch should not block in the future, you may redirect the report to the following email address:

- False Positive (confirmed solicited) to reportso@blockspam.biz

With the exception of the targeted email address, sending reports about misclassified solicited bulk email should comply with all the guidelines as specified above for reporting cases of false positives.

Otherwise, if you are not sure that the report is made of confirmed solicited bulk email, then all reports about cases of false positives should go to the following email address as previously noted:

- False Positive to reportfp@blockspam.biz

Commtouch Response to Reports

The objective of reporting spam classification errors is to fix these mistakes as soon as possible without draining too many valuable resources from you and your customers. Commtouch will make an effort to fix confirmed mistakes immediately. If you choose to receive Commtouch replies, please contact your technical account manager at Commtouch. The response from Commtouch to you will be sent once a week, typically on a Wednesday. The response will include short and clear information, per-report.

Reports about cases of false positives are analyzed by Commtouch's Monitoring team and if found to be justified, the mistakes are fixed. If no justification is found, no action is taken. The Monitoring team is committed to reply back in a timely manner and specify the list of actions applied per report. Commtouch will not reply to your customers (end-users), but only to you as coordinated with your Commtouch technical account manager.

The reply to reports about cases of false positive is contained in MS-Excel format that is sent to you over email and will include the following information, one line per-report:

<RefiD><Date of received report from you><Status: Fixed or Rejected>

The Monitoring team will not reply to reports about cases of false negative. However, this should not discourage you from sending these reports because our experience indicates that customers reporting cases of false negative enjoy better spam detection rate than others.

Thank you for your cooperation!

THE COMMTOUCH TEAM