GBS GLOBAL APPLIED KNOWLEDGE

GBS Anti-spam and Anti-virus Policy

GBS will apply many anti-spam and anti-virus checks to incoming email. These checks are applied at the GBS mail relays, through which most of our incoming mail passes.

Local Blacklists

The address and name of the sending system is looked up in a local blacklist and the message is rejected if there is a match.

Public Blacklists

The address of the sending system is tested against various public blacklists. These blacklists have been chosen because they are known to be effective, have a reputation for few false positives (that is mistaken listings), have suitable listing methodologies, and provide good information on why particular addresses have been blacklisted. We use three public blacklists.

Whitelisting

If a blacklisted site needs to get mail through to us, we would generally expect them to fix the problem that lead to their being listed and delist themselves.

Intrusion Detection Architecture

Stage 1 Anti-virus checking

All messages are scanned for viruses, worms, etc, using our chosen Tier 1 Anti-virus software. If a virus is detected which appears on a list of those known to forge sender addresses, the message is simply discarded, as rejecting it would cause an error message to be sent to an innocent third party. Otherwise, the message is rejected.

Stage 2 AV checking: Second tier AV

Messages that make it past Tier 1 AV are then scanned using an open-source Tier 2 anti-virus scanner, which can pick up some malware that Tier 1 provider does not

(and vice versa). It also can detect some classes of "phishing" messages (malicious messages attempting to fool victims into entering their financial details into bogus websites).

Tier 2 AV scanner website

The use of two virus scanners makes the service more robust. One or the other can go down, and messages can still be allowed through with confidence. Since they will update their signature databases with different frequencies and timeliness, this will also tend to narrow the window of vulnerability where a new virus can sneak in before signatures for it are available.

Spam filtering with SpamAssassin

SpamAssassin is a popular open-source software package which applies a variety of textual and other tests to messages in order to estimate the likelihood that they are spam. This likelihood is represented as a number, the spam score. So SpamAssassin assigns a score to each message it sees, which can subsequently be used to determine the message's disposition.

SpamAssassin is run on the main GBS mail relays. It scans all messages coming in to the mail relays from networks outside of GBS. It adds headers to a scanned message containing indications of the spam score assigned to it, and the mail system then continues processing the message as normal.

Thresholds

The main control over the spam filtering is a number called the threshold. Messages rated with a score equal to or greater than the threshold are filed in the likely spam folder; messages rated less than the threshold are not affected, and will be delivered to your inbox (unless there are subsequent filtering rules in place which might affect it).

At any given threshold there is always a chance that a spam message is filed in your inbox (a false negative) and a chance that a nonspam is filed in the likely spam folder (a false positive). If you increase the filtering threshold, the chance of false negatives increases, so more spam gets through to your inbox. At the same time, the

chance of false positives decreases, so less nonspam mail is filed along with the spam.

Where the threshold should be set depends on the sort of email that each user receives. If you receive mail that tends to score highly, such as HTML-formatted newsletters, commercial announcements, and so on, you may prefer a higher threshold to allow this mail through to your inbox while accepting that a higher amount of spam will get through with it. If you receive only relatively "clean" mail, you may prefer a lower threshold. You may also prefer a lower threshold if you are prepared to check your likely spam folder often, while a higher threshold would allow you to check it less often.

Employees responsible:

Strategic: Executive Board

Operational: IT Manager

10th December 2019