

Incident Report External Email - February 2017

Incident #2017-182

External Email Delay for Campus Feb 3 - 8th

Summary

On Friday February 3 after 17:00, some external email coming into Queen's was not delivered. As the weekend progressed, delivery of external email continued to degrade. Late Sunday night, all external email stopped being delivered to Queen's users. This incident was the result of a technical issue with the three spam filters that check incoming email for viruses. The filters stopped working correctly and started queueing email. When ITS staff arrived on Monday morning, they began troubleshooting and called in vendor support. The vendor experienced telephone service issues and was not able to be reached by phone. ITS then emailed the vendor and at 11:30 contact was made. While waiting on the initial vendor contact, the units were rebooted and performance returned. Queued email delivery began.

The spam filters crashed again Monday night before all queued mail could be delivered. Tuesday morning, ITS staff again contacted the vendor and worked on the problem throughout the day. The vendor worked throughout the night. By Wednesday morning, the root cause of the issue was determined, all queued mail was delivered, and a patch was applied to the filters to ensure the problem will not happen again.

Because the spam filters were still running, our monitoring did not alert us to a problem and therefore the on-call person was not paged.

Impact

Mail delivery to Queen's from non-Queen's O365 accounts was delayed by varying amounts of time from Friday February 3 until the morning of Wednesday February 8, 2017. No mail was lost.

Root Cause

A bug in the code for the spam filter accepted an email with a large attachment, causing the virus scanner to fail and mail to be queued. The email passed to the next two spam filters and the same problem occurred causing all external email to be queued.

INCIDENT REPORT

INFORMATION TECHNOLOGY SERVICES



Resolution

Working with the vendor, a new patch was created for the spam filters. The vendor applied this patch. The spam filters will now drop emails with attachments larger than Queen's maximum attachment size without doing any scanning or processing.

Communications (Internal)

ITS internal teams communicated via skype, phone, face-to-face and email in an effort to solve the issue. These communications channels were used during business hours as well as outside of business hours to ensure proper coordination of tasks.

ITSP Communication (External)

Notices were posted on the ITS notifications page starting on Friday Feb 3, 2017 which also send a tweet and an email to ITAdmin Reps. The notices were updated when new advances were made or new issues were identified.

Lessons Learned

- Monitoring of the incoming and outgoing mail queues need to be included in the on call paging scripts.

Action Items

- Increase monitoring of mail queues - upper limit queue size alerts to page the on call person. Status of work: Completed.

