

Fending Off Spam Onslaught with Vircom's modusGate™

Tenaquip, established in 1968, was the first Canadian company to distribute industrial products through a catalog. Today, it remains a leader in the industrial marketplace through phone, fax, online and retail store sales, with more than 450,000 products available.

The Challenge

Tenaquip, a Canadian online vendor and retailer of industrial products, was being inundated with email messages. Unfortunately, the messages were not customer orders but automated return-to-sender notices. Curiously, the return-to-sender messages were not a by-product of mail originating from Tenaquip.

"These email messages started to arrive in the hundreds, then in the thousands," explained Louis Marceau, Network Administrator for Tenaquip. "In a very short period of time, we had received well over a million emails, clogging our mail servers and threatening to shut us down completely. For an organization that is as heavily dependent upon email as we are, this threat could be devastating to all of the company's operations."

The Attack

Tenaquip was inundated with email because of a Joe-job, something that has become more prevalent in the email world. A Joe-job is a spam attack that uses a spoofed or forged sender address, often as an act of revenge. Joe-job attacks result in non-delivery reports, out-of-office notices, challenge-responses, auto-responders, etc. which are generated with the forged sender address. The barrage of spam can often sully the sender's reputation and incur the wrath of the unfortunate recipients.

The mail server receiving these spam messages bounce them back to the unsuspecting sender. When copious amounts of email messages are bounced, the organization's domain name and/or IP address risks being blacklisted (a list of domain names and IP addresses that are reportedly being abused) as a source for spam. The influx of email may also cause the organization's email server to process email too slowly or even shut down.

For Tenaquip, this particular Joe-job resulted in a flood of bounced email messages, most of which were sent to random and non-existent addresses on their domain. This attack was damaging because the company's email gateway was incapable of handling the increased load.

"The load of bounced-back email messages was so great," Marceau recalled, "that our existing email gateway and server just couldn't handle it. Messages were piling up exponentially. And to make it worse, we couldn't get any legitimate emails either in or out."

TENAQUIP

"If we were going to remain operational, then we knew we had to get help quickly."

Louis Marceau
Network Administrator
Tenaquip Limited

“With minimal losses in terms of productivity, we were able to keep external incoming/outgoing email running.”

Louis Marceau

Marceau and his team at Tenaquip had to make an important decision and they had to make it quickly.

The Decision

“We realized there were two ways to go, either we could just wait out this storm, which we knew would not be viable, or we could get additional assistance,” Marceau continued. “If we were going to remain operational, then we knew we had to get help quickly.”

Marceau’s group contacted a number of anti-spam developers before they came upon Microserv®, a Quebec-based computer reseller and integrator. Microserv®, a reseller of Vircom’s modusGate™ secure email gateway solutions, recommended that Tenaquip contact Vircom.

Shortly after their initial contact, Vircom’s SpamBuster Team remotely accessed the Tenaquip’s email servers, which were in the midst of another malicious Joe-job attack. The SpamBuster Team quickly identified the problem and recommended a solution. “What they found was that the majority of the email messages were coming from randomly chosen names combined with the Tenaquip domain name; for example, ‘randomname1@tenaquip.com’,” explained Jean-François Gignac, Sales Director for Vircom.

With little time to spare before the email infrastructure collapsed, two Vircom support technicians arrived at Tenaquip headquarters to install and configure a 500-user modusGate™ Appliance, incorporating Norman Anti-Virus. The modusGate™ Appliance is designed to verify all local email addresses before accepting inbound messages. If the recipients are valid, messages are scanned and processed according to the mail content settings. Messages to non-valid addresses are normally returned to the sending server but, in this case, a temporary custom script was created to quarantine the bounced messages.

“Although it is usually against RFC recommendations to discard bounced-back messages,” said Gignac, “in this case, we really did not have a choice. Either we violate the RFC recommendations for a short period so that they become operational again or we maintain RFC ‘purity’ and they stay down. In this case, we chose the first option.”

The Result

By the end of the day, Tenaquip’s email infrastructure was back online and email traffic was flowing. Marceau also took advantage of modusGate’s™ Web interface to remotely monitor the email traffic while he was on a business trip that evening.

The cost for this fix was just under \$8,000 CAN. Its worth to Tenaquip, however, was priceless.

“With minimal losses in terms of productivity, we were able to keep external incoming/outgoing email running,” Marceau said.

Tenaquip’s return on investment was immediate. Similarly, maintenance costs are minimal thanks to modusGate’s™ Appliance “set-it-and-forget-it” functions.

By thinking long-term and allocating the appropriate funds for the modusGate Appliance at the time of the attack, Tenaquip has not needed to purchase product enhancements to fix gaps that likely would have likely arisen had another solution been chosen. And, as a Vircom client, Tenaquip reaps the benefits of continual enhancements to the modus suite of products.

Today, electronic mail is crucial to any business wanting to be both competitive and successful. In most cases, it forms the backbone of an organization’s day-to-day activities and its uses will certainly continue to evolve. Therefore, organizations will always need protection from the potentially harmful elements of email, such as spam and viruses, and the perpetrators of malicious attacks such as Joe-jobs.

About Vircom

Vircom Inc., based in Montreal, is a privately held software development and professional services company focused exclusively on email messaging security. Founded in 1994, Vircom is the only email security vendor to offer a wide range of deployment options, proprietary anti-spam technology, complete Windows® infrastructure integration, and premium customer service. Its award-winning products include modusMail™, modusGate™ and modusGate™ Appliance. Vircom’s technology is utilized by several major security providers and deployed through third-party vendors to customers in more than 100 countries.

For more information, please visit: www.vircom.com

Contact

Sales:
sales@vircom.com, 1.888.484.7266

Marketing:
ana.plenter@vircom.com, +1.514.845.1666, ex: 291