

Nip spam in the bud

By **JUDHI PRASETYO**

TO combat the surge in spam from local marketers, Singapore recently implemented the Anti-Spam Act. Although this new Bill may prove effective in stopping local spam, organisations need to note that the major part of spam today comes from overseas and the current law does not protect us from that.

Also, it is imperative that once such pieces of legislation are passed, diehard spammers will go back to the drawing board and conceptualise new and innovative ways to squeeze their fraudulent claims through tiny cracks within enterprise systems.

While spam is a traditional nuisance, it can be harmful to the network. Many computer systems are vulnerable to viruses and cyber attacks that arrive via unsolicited email. The volume and sophistication of attacks are growing at exponential rates, threatening entire networks leaving systems battered and bruised. IT ad-

ministrators often have a tough time keeping these nefarious activities at bay and have to constantly stand guard.

Spam is constantly evolving, especially when security solutions are developed to combat it. Take, for instance, image spam. This form of spam does not utilise textual content but rather images embedded within the email.

Traditional key-based spam filters are unable to detect them and so these get through and end up on the user's desktop. In addition, random pixel and colour modification methods make the spam image unique from all others.

Leveraging such sophisticated methods, spammers can create virtually unlimited versions of the same message and trick anti-spam software into identifying each as different from the last.

A more malicious threat comes in the form of zombies that can hijack a PC within a company and spew spam and viruses using your email address. The conse-

quences to enterprises can be devastating. A single disaster, whether it's compromised customer data, downtime due to a virus, or corrupted files and inadequate backups, can destroy a business' reputation, credibility, customer base and sales.

The most devastating of all may prove to be the inadvertent distribution of spam. A creative fraudster can send a Botnet to hijack a computer within the organisation's premises and spew out millions of spam email. The anti-spam initiative will only trace these unlawful acts back to the company, enforcing its legal policies on the company itself.

The anti-spam Bill will lend a measure of comfort to enterprises. However, the legislation is not the be all and end all of spam attacks, and enterprises need to prepare themselves.

Given the security concerns, organisations must take on a holistic view to spam. While the anti-spam legislation acts as a sort of immigration counter, effective policing still needs to be en-

forced to ensure that nothing slips past lawful eyes. Anti-spam solutions need to be implemented and maintained by the organisation like a layer of shields to repel any unwanted and unsolicited spam. Such control perimeter measures can be installed in line with the security policies already established at the gateway or at the client.

A fully integrated solution that enforces perimeter security, providing multiple layers of security, will ensure that enterprises stay a step or two ahead. All data will have to go through a series of checks before it actually reaches the gateway or the client. This will actually prove to be an essential lifeline for organisations everywhere.

Enterprises need to be ever vigilant to survive in a cyber world where fraudsters are continuously developing smarter ways to force through spam.

The writer is country manager, Singapore and emerging markets, Fortinet