VIRCOM
email security matters

Image Spam

AN INCREASING THREAT

Table of Contents

An Increasing Threat

Never before has it been so easy to communicate with the majority of the world's population almost instantaneously. For businesses and enterprises of all sizes, email has become the number one form of communication.

However, with the good usually comes the bad and with email comes spam.

As Vircom's SpamBuster team has observed, spam accounts for over 80% of all email traffic and this number continues to grow. One of the key factors for this dramatic increase is image-based spam, an increasingly common and sophisticated nuisance accounting for more than 25% of all spam.

Image spam is difficult to block because email filters cannot read messages embedded within an image. As a result, spammers can easily bypass filters by sending a variation of the same image for each spam campaign. Spammers combine this technique, known as image serializing, with the use of spam zombies or bots (infected desktop PCs that they secretly hijack) to relay their spam. By combining these two methods, image spammers confound most spam technologies on the market today.

For businesses, spam is no longer simply a productivity issue. Spam exposes employees to potential fraud and it is a company's responsibility to protect their employees. For system administrators, the battle against image spam occurs on several fronts:

- Image spam is more difficult to detect
    > IT will spend more time fine-tuning conventional email filters

- An Image spam message is usually significantly larger than a text-based spam message
    > A text-based spam message is approximately 5 to 10KB in size while the an image spam message is approximately ranges from 10 to 70 KB
    > Therefore, IT will be required to allocate significantly more bandwidth and storage for their email infrastructure

- Image spam messages takes longer to analyze
    > IT may be required to upgrade or replace existing platforms to cope with the needed processing power

If not properly handled and managed, image spam can flood networks, drastically reducing response time and impacting of other critical business applications.

An Evolving Threat

Image spam is a relatively new occurrence. When first introduced, these messages did not contain any images. Instead, images were loaded from the Internet via hidden URLs. Since most email filters were looking for keywords, these spam messages went through.

As email filtering solutions began to incorporate the use of Spam URL Real-time Block-lists (SURBLs) or proper URL databases, image spammers were forced to improve their methods. They began to embed the image in the message, avoiding URL links to circumvent filters.

This last point raises a question: Why would anyone who receives this type of image spam type or copy the advertised URL into his/her web browser? To answer this question, we must look at the nature of image spam messages. While some promote low-priced Viagra for example, the majority of these messages are pump & dump stock scams where spammers first invest in a stock and then send out spam hyping the stock (pump). The goal is to raise the stock price before selling their shares at inflated prices (dump). No link is required - just a lure, urging you to call the broker. Many victims fall into this "easy money" trap. To make matters worse, speculators ride the stock momentum surrounding the spam campaign to make a profit.

Not all pump & dump stock scams use image spam but they are moving in that direction, as put forth in Vircom's Pump and Dump white paper. Pump & dump scams are becoming so prevalent that, on March 8 2007, the SEC suspended trading of 35 companies that had been the subject of recent and repeated spam email campaigns[1].

This highlights the potential profit from such fraud and explains why spammers are so cunning when considering ways to circumvent filtering techniques. For example, to bypass fingerprinting spammers began sending a unique, slightly different image each time by changing the image format, adding pixels, tiling images, etc.

Several email filters have tried using optical character recognition (OCR) technology to identify messages within graphics. While this effort requires significantly more processing power, spammers have learned to bypass OCR technology by varying font and backgrounds or using speckle patterns to make the message fully legible by the human eye but indiscernible to a machine.

In this never-ending cat-and-mouse game, image spam now disguises key words or phrases within an image or appends text that is not considered spam at the end of the message. This portion of text, often referred to as word salad, contains words that are strung together yet have no meaning. Frequently, spammers use passages from works of literature or copies of press releases. This technique fools most spam filters as it decreases the likelihood that the message is spam because of the high number of meaningful words. Another method that is becoming popular is the use of animated and layered GIF files that divide messages into several images and layering them on top of each other.

Spammers combine these techniques with the use of spam bots or, worse, use botnets (a network of bots) to perform spam image serialization.

An Unbeatable Threat?

In an effort to alleviate image spam, companies could block every message that contains images or attachments from being delivered to users' inboxes. However, for most companies, this would be too drastic a measure as employees may send and/or receive mail containing images (e.g. signatures using a company logo).

With the variety of techniques spammers employ to circumvent spam filters, a successful solution should combine various methods, including tried and true ones and new and adaptive ones targeted to specific threats. To fight image spam, three filtering strategies are essential:

- Edge Defense: Providing a single entry point to limit the ways in which spam enters the network and granting a suite of sender scrutiny features, including sender authentication, validation and accreditation layers.

- Message Scrutiny: Looking for recognized spam patterns (including embedded URLs), analyzing the way messages have been constructed and which network characteristics were involved with their delivery.

- Image Scrutiny: Examining the image format and content, comparing it to known spam images or with follow-up images to prevent new image spam waves.

While essential, these filtering techniques should not stand alone in the fight against image spam. Two important aspects must not be minimized:

- Human Analysis: Depending solely on OCR technology to combat image spam is not recommended as machine-only solutions are rarely foolproof. Human analysis is required to improve catch-rates or to correct inevitable errors as a result of machine-made decisions.

- Forward-looking Technology: Image spam is simply the latest round in the fight between spammers and email users. As spammers constantly change their tactics and techniques, email filtering solutions must rely on flexible designs to provide the capabilities necessary to meet today's threats as well as the essential flexibility and scalability to meet tomorrow's.

Vircom's modus™

modusGate™ Processes
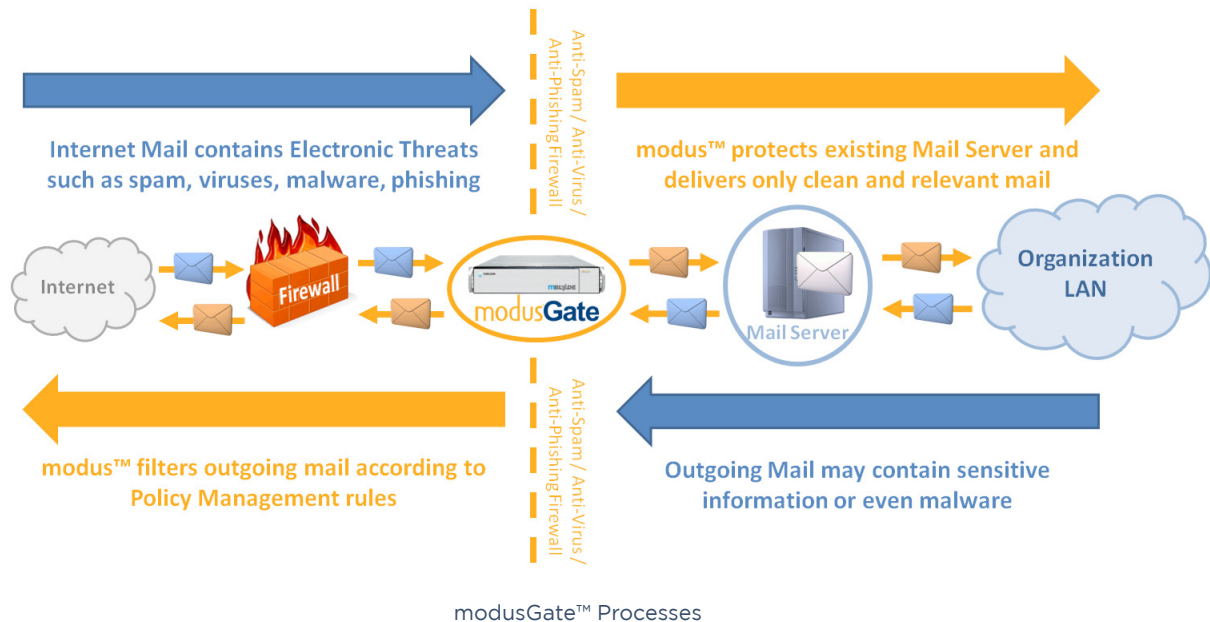
Vircom's modus™ technology was introduced more that 10 years ago and is continuously being enhanced with innovations and industry firsts. It was conceived from the realization that there is no single tool that can adequately solve the complex problems of spam. As a result, modus'™ Sequential Content Analyzer (SCA™) technology combines multiple predictive and deterministic technologies to detect spam patterns within messages instead of spam instances:

- Early interception of email DoS and harvesting threats
- Sender authentication & accreditation
- Content analysis performed by two separate engines
- Language filtering
- Multi-layered predictive/deterministic technology
- Image content analysis o of modusGate™ appliances from entry-level to an enterprise solution.
-

Vircom's dedicated SpamBuster team combines human analysis with an unparalleled self-learning mechanism to constantly update customers' spam engines. They gather information about spam and spammers by, for example, monitoring the Internet and by users reporting their spam and false-positives. This centralized approach ensures that every spam lesson learned serves every modus™ system. Most important, it relieves IT staff from repeated training and fine-tuning of their email filtering solution.

Peace of mind and freeing IT staff from continually fine-tuning and configuring their email filtering solution are the foundation for Vircom's suite of products: modusGate™ email gateway software, modusGate™ Appliance and modusMail™ mail server:

- ndustry-leading catch rates, which represent
  > Less spam in user inboxes and fewer false-positives for them to retrieve
  > Fewer requests and complaints to help desks
  > Reduced bandwidth and storage requirements

- Effortless administration
  > Automation, delegation and monitoring greatly reduce the time administrators spend operating their system, often making modus™ an install it and forget it solution

- Efficient user interfaces:
  > By regularly enhancing their user interfaces, Vircom has considerably reduced the time employees spend reviewing their quarantined mail
  > Users can easily release false-positives or add email addresses to their trusted senders list, thus removing these tasks from the IT staff

It is this combination of performance, automation and delegation makes modus™ one of the most manageable and most accurate technologies used to fight image-spam in the industry.

About Vircom

Vircom is a global leader in email security, specializing in software, appliance solutions and professional services. With over 15 years of experience, Vircom has been the first to market with several solutions, including technology to block image spam and predictive email content management.

Vircom's products include modusMail™, modusGate™ software, modusGate™ Appliance and are made available to several major security providers and deployed through third-party vendors to more than 6.6 million inboxes worldwide. For more information, visit www.vircom.com.