

## WHITE PAPER

---

### Choosing the Best Technology to Fight Spam

---

Sponsored by: Commtouch and Sybari

---

Mark Levitt

Brian E. Burke

April 2004

#### IDC OPINION

Spam is the latest scourge of the Internet, second only to viruses and other malicious code in the anger and frustration that it evokes. Filling networks, servers, and inboxes with unwanted and often offensive content, spammers continue to wreak havoc by frequently changing spam's appearance and masking its source to prevent companies from identifying and blocking spam before it reaches its target: email inboxes. Due to the remarkable surge in volumes and sophistication of spam that IDC has tracked during the past two years, it is critical to choose the most effective spam detection technology. Antispam solutions that focus on spam's content or format have been fighting a never-ending battle to keep up with the latest spam created specifically to evade content filters. To keep pace with today's spam, solutions need to be able to detect spam regardless of format or content, automatically adapting to changes in and providing protection to enterprises and service providers in real time.

#### METHODOLOGY

As part of IDC's coverage of email usage and trends, we have tracked spam volumes as part of all email volumes for several years. To meet the need for spam-related market analysis, IDC recently completed a sponsored study of the costs of spam and the value of antispam solutions involving surveys of more than 1,000 mid- to upper-level managers. For the specific Recurrent Pattern Detection (RPD™) technology developed by Commtouch and customer information in this study, IDC interviewed vendors employing RPD technology, including Commtouch, BlueCat Networks, and Sybari Software, and several of their customers.

#### IN THIS WHITE PAPER

This IDC white paper examines the problem of spam and the challenges in detecting spam that is constantly changing. It reviews antispam technologies, including honey pot signatures, content analysis, blacklisting/whitelisting, reverse DNS lookup, sender authentication, and RPD, and suggests criteria for selecting the right antispam solution.

## EXECUTIVE SUMMARY

During the past two years, IDC has tracked huge increases in the volume and complexity of spam. Despite the availability of many approaches to detecting spam, it continues to plague email users. Antispam solutions that were considered effective a year ago based on their ability to block as many as 90 out of every 100 spam messages may no longer be considered effective when the actual number of spam messages reaching email user inboxes rises rather than falls due to the higher volumes of spam being sent by spammers. To reduce spam in real terms, antispam solutions need to detect more spam by identifying and blocking new forms of spam in real time, during the first few minutes of an outbreak. Recurrent Pattern Detection, a technology used by several server software, server appliance, and client software vendors and their customers, provides real-time proactive detection of spam regardless of content, language, or format.

## SITUATION OVERVIEW

---

### What Is Spam?

*Spam* is "unsolicited bulk email" sent by both legitimate direct marketers offering commercial products and services and less reputable firms and individuals offering illicit, offensive, and even nonexistent products and services or using email to deliver viruses. "Bulk email" refers to the automated broadcast of high volumes of spam.

---

### Spam Trends

#### *Spam*

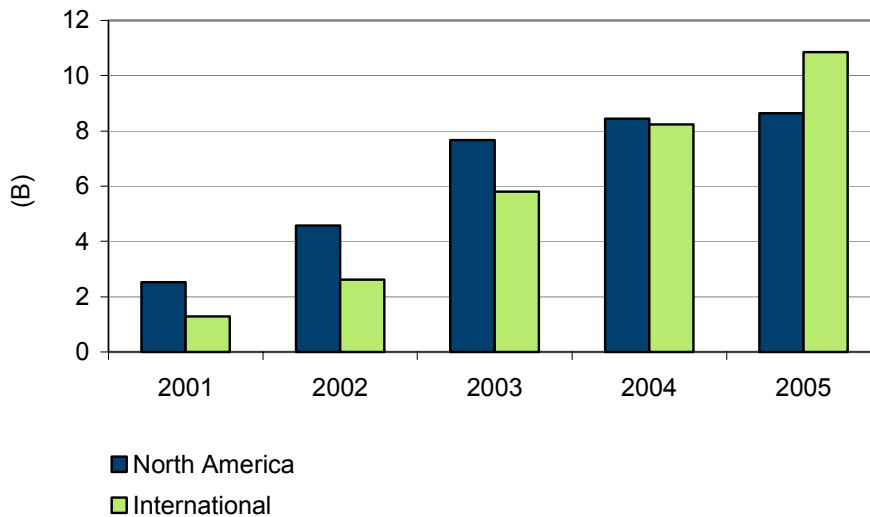
Spam has been a major problem for service providers for several years. However, for most organizations, it has only recently emerged as a high-priority problem requiring high-priority attention and resources.

Prior to 2002, companies and other organizations considered spam more of a nuisance than anything else. They considered the volumes of spam received to be manageable through the use of the Delete key, simple keyword email filters to delete or folder suspected spam, and real-time blackhole lists (RBLs) to block known sources of spam. Corporate IT departments were too busy with other projects, including battling viruses and other malicious code capable of bringing down entire networks and damaging servers and personal computers, to invest time and money in fighting spam.

What a difference two years make. The volume of spam sent worldwide every day will jump from 7 billion in 2002 to 17 billion in 2004, according to IDC estimates. Spam has grown into too difficult and costly a problem for most IT departments to ignore or leave to email users. Fighting spam can be very time consuming and is best handled by experts who spend all of their time and resources focused on developing even more effective ways to block it. Moreover, spam will contain more non-English language content as the majority of spam will be sent to email users outside North America by 2005 (see Figure 1).

**FIGURE 1**

North America and International Spam Messages Sent Daily, 2001–2005



Source: IDC, 2004

### ***Spammers***

Spammers are motivated by the money to be made in selling legitimate or illegitimate products and services through spam and in delivering spam on behalf of their customers. Before most organizations deployed antispam solutions over the past two years, spammers had little difficulty in sending spam. Life has become more difficult for spammers, but the financial incentive has pushed spammers to be very aggressive and creative in developing new forms of spam that can evade detection. These include spoofing email addresses, constantly changing spam content, incorporating random and innocent text, and replacing text with images to fool content analysis and other spam detection technologies. Spammers take advantage of their ability to deliver a sizable portion of their spam broadcasts to email user inboxes before most antispam solutions are able to recognize and begin detecting new forms of spam.

### ***Service Providers***

The first line of defense against spam consists of service providers that are asked to relay huge volumes of email, including an abundance of spam, to other service providers, organizations, and email users. Because service providers are close to the source of spam, they are in a unique position of being able to either stop or at least slow down the rate at which spam reaches the Internet by detecting spam as it attempts to enter their networks. Due to the limited amount of revenue that is directly generated by most hosted email services, the challenge for service providers is to block spam effectively with minimal cost and subscriber involvement.

### ***Corporate IT Departments***

The second line of defense against spam consists of corporate IT departments that are tasked with delivering email without viruses or spam. Spam, including spam carrying viruses, is best stopped at Internet gateways as it attempts to enter corporate networks. The challenge is to stop spam, and only spam, with minimal cost. To achieve this goal, corporate IT departments, with input from business management, need to determine what constitutes spam in the context of their organizations. While corporate IT evaluates, deploys, and configures antispam solutions, direct email user involvement in choosing between rejecting and accepting suspected spam can ensure that spam and only spam is blocked.

---

## **Criteria for Antispam Solutions**

### ***Effectiveness and Accuracy***

The most important element of blocking spam for an antispam solution is to detect all or nearly all spam. While blocking 100% of spam is the ideal, removing 94–95% of spam goes far in alleviating the costs imposed by spam on email users and IT staff. In addition, organizations generally prefer letting some suspected spam through in the interests of accuracy. With the huge rise in spam volumes, antispam solutions needed to block a rising percentage of spam to reduce the actual number of spam reaching email users. As a result, solutions that blocked 90 out of 100 (90% of) spam and that were considered effective in the past must now block 94–95% of spam to be considered effective. Accuracy refers to the degree to which an antispam solution can block spam and not block legitimate email messages (i.e., avoid false positives).

### ***Frequency of Updates***

The key to effective and accurate detection of spam is for antispam solutions to evolve along with spam. With hundreds of thousands of spam outbreaks disseminated every day, filters can quickly become ineffective against the latest spam. Antispam solutions must be able to catch today's spam, not yesterday's spam. The same way that out-of-date antivirus products are ineffective at identifying the latest viruses, out-of-date antispam solutions that know nothing about the latest spam become increasingly ineffective over time at stopping spam.

To minimize administration time and effort, product and spam pattern updates provided by commercial antispam solution providers that spend all of their time keeping up with spammers and supporting customers are needed. Ideally, these updates should be automatic and frequent. IT departments know better than to rely on homegrown solutions to fight viruses. The same appreciation for outside expertise applies to fighting spam that is constantly changing its content and format to avoid detection.

### ***Global Coverage of Multilingual Spam***

Due to the global nature of email and the preference of many spammers to operate in countries where their spamming activities will not be easily detected or prosecuted, spam is often sent from countries where a language other than English dominates. Antispam solutions must be able to block spam regardless of the language or dialects used. Otherwise, spam sent from foreign countries will have a good chance of evading detection.

## Antispam Approaches

The key approaches used by enterprises to detect spam are as follows:

### ***Honey Pot Signatures***

"Honey pots" or decoy email mailboxes, created on service provider and enterprise networks to act as spam catchers or traps, are used to provide the basis for generating signatures or patterns of spam received for testing emails sent to real mailboxes. This approach focuses on the "unsolicited" aspect of spam by relying on the fact that any email sent to a mailbox that does not belong to a real person could not have been solicited and is spam by definition. An advantage of this approach is that only actual spam is blocked, helping to avoid false positives. A disadvantage is that only spam exactly matching known spam already caught can be blocked. Because spammers are constantly changing spam, signature-based solutions are always playing catchup. Inherent in the design is a delay from when patterns for new forms of spam can be created and distributed before spam can be blocked. In addition, not all spam reach honey pots due to spammers using validated email addresses.

### ***Content Analysis***

One or more content analysis techniques are used to analyze everything about the content of inbound email by service providers, gateway or email servers, or even client antispam solutions. This approach focuses on the "commercial" aspect of spam by relying on the suspicious characteristics of legitimate and illegitimate offerings or information requests that spammers try to hide from spam filters and email users at least until they open the emails. Many content analysis techniques are in use, including:

- ☒ **Keyword analysis:** This approach involves analyzing the text section of an email for specific keywords and phrases (e.g., sex, profanities, Viagra) that are unlikely to appear in legitimate business correspondence. Keyword analysis, when used as a standalone spam solution, is a very primitive technique and often produces a high risk of false positives.
- ☒ **Lexical analysis:** Unlike keyword analysis, lexical analysis works by analyzing the context of all of the words and phrases in a particular message. The presence of a particular suspicious word or phrase by itself does not necessarily mean that the message is spam. Instead, each word or phrase is assigned a weight depending primarily on the context in which it is found.
- ☒ **Bayesian analysis:** The basis of Bayesian logic uses the knowledge of prior events to predict future events. When used to detect spam, a Bayesian filter examines emails that are known to be spam and emails that are known to be legitimate and compares the content in both emails in order to build a database of words that will, according to probability, identify or predict future emails as spam or legitimate email. Although Bayesian analysis is a new technique used to fight spam, the Bayesian logic theory was actually first published in 1763.

- ☒ **Heuristics:** Heuristics is a technique that looks for spam-like characteristics in an email message. Each characteristic is assigned a spam probability, and the message is given a cumulative probability score based on the overall test results. If a certain probability threshold is reached, the email is determined to be spam and is blocked.
- ☒ **Header analysis:** Header analysis examines headers, looking for such items as the validity of the sender's address, whether the same information is found in the "sender" and "from" fields of an email, and whether a specific message contains information not common to normal email.
- ☒ **URL analysis:** Spammers are increasingly embedding URL links inside emails to direct users to specific Web sites. URL analysis looks at the embedded links in email messages and compares them to a list of URL rules or known spam URLs to determine if the messages are spam.

Multiple techniques can be combined to generate aggregated scoring for each inbound email representing the probability of it being spam. An advantage common to any content analysis technique is that it can block the very first spam sent by a spammer. Two disadvantages are that spammers can change the content of spam sufficiently to evade content filters and false positives occur when legitimate emails contain sufficient content that is also common to spam.

### ***Blacklisting/Whitelisting***

Blacklisting and whitelisting rely on the identification of email senders to determine whether messages are spam. Most blacklisting relies on RBLs containing domain names or email addresses maintained by antispam Web sites, service providers, IT departments, and even individual email users that block all email from known spammers. Whitelisting relies on similarly maintained lists that allow all email from known legitimate or "good" senders. An advantage of this approach is that all content from known spammers is blocked and all content from known "good" senders is passed through. A disadvantage is that managing RBLs requires much time and effort. RBLs are often ineffective on their own in blocking spam because they often include legitimate sources misclassified as spammers and miss spammer IP addresses and domains, which change rapidly. In addition, spammers hijack legitimate domain names and individual email addresses to make spam appear to come from good senders.

### ***Reverse DNS Lookup***

Reverse DNS lookup runs DNS queries on the IP addresses of incoming email to determine if the identified host name matches an actual host name for the sender's IP addresses. Because many spammers use spoofed hosts to disguise the source of the spam, a query that doesn't recover a matching host and IP address is a good indication that the message is spam. An advantage of this approach is that it quickly and easily blocks spam with spoofed addresses. A disadvantage is that it does nothing about spam without a disguised source.

### ***Sender Authentication***

Sender authentication is a new approach that promises to identify spam by checking the identification of named email senders based on either sender email or IP addresses. Emails with sender information that cannot be authenticated with the sending domains can be blocked or identified as suspicious for further scanning. An advantage of this approach is the prevention of email fraud, the most harmful form of spam. A disadvantage is the time and will needed to incorporate compatible sender authentication tools into all of the message transfer agents (MTAs) routing email at Internet gateways.

---

### **Challenges for Current Antispam Technologies**

Effectiveness and accuracy of antispam solutions vary depending on the specific approach, product, and customer settings as well as their ability to respond to spammers' evasion efforts. For example, faster distribution of spam with different subject lines poses challenges for honey pot signature-based solutions, which take time to identify spam and create and distribute exact signatures of the spam received before they can begin blocking spam. Spoofing of email addresses to make spam appear to be sent from someone else poses challenges for blacklisting/whitelisting techniques. The use of randomized text and images instead of straight text in spam poses challenges for content analysis-based solutions.

Another challenge for antispam solutions is the time required for administration and usage. According to IDC's study of the cost of spam and the value of antispam solutions, companies spend a considerable amount of time dealing with spam, even after antispam solutions are in place. Survey respondents indicated that email users spend 5 minutes and IT staffs spend 19 minutes on average every day dealing with spam. They perform a variety of tasks such as maintaining and updating the solution, reviewing suspected spam, tracking down false positives, and asking or answering questions about spam. To further reduce spam's impact on worker productivity and other resources, organizations will be looking for antispam solutions that provide appropriate levels of automated operation, end-user involvement, effectiveness, accuracy, and up-to-date detection of new forms of spam that have yet to be created.

---

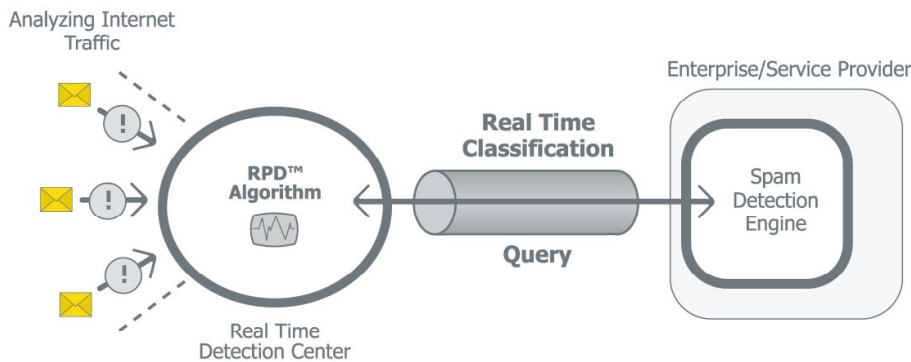
### **Recurrent Pattern Detection**

Given the nature of spam, it is important to consider an innovative antispam technology — Recurrent Pattern Detection. This approach to detecting spam relies on the fact that spammers send spam in bulk over a relatively short period of time to satisfy their own or their customers' business needs. Using a set of sophisticated algorithms applied to analyzing Internet traffic in key points around the world for repetitive components in multiple emails, RPD is able to trace a spam outbreak as soon as it begins. The ability to trace spam in the first few minutes of an outbreak is critical to preventing spam from reaching email user inboxes during the early portion of an outbreak of tens or hundreds of millions of spam messages before detection begins.

Once an outbreak is detected, RPD then creates and stores a spam "DNA" or hash pattern in its Spam Pattern Repository. Spam detection engines at customer sites submit the DNA of inbound emails as queries to this repository, which can start classifying email as spam in the first few minutes of an outbreak (see Figure 2). Local copies of the Spam Pattern Repository or caches of completed queries located at customer sites minimize response times.

**FIGURE 2**

RPD Technology



Source: Commtouch, 2004

Several advantages of the RPD approach enable it to detect and block spam in the first few minutes of an outbreak, unlike other antispam approaches. First, its proactive, real-time analysis of Internet email traffic and responses to queries from spam detection engines minimizes delays. Second, its reliance on detecting spam outbreaks, rather than individual spam characteristics, means that spam and nothing but spam associated with bulk mailings are blocked.

The RPD technology has been embraced by providers of security and management software (such as Sybari Software and Waterford Technologies), security appliance (such as BlueCat Networks and BarbedWire Technologies), and desktop software (such as Spamfree.com). RPD has been deployed as both a standalone antispam solution and an additional layer of antispam protection.

**Customer Profile: BlueCat Networks**

BlueCat Networks ([www.bluecatnetworks.com](http://www.bluecatnetworks.com)) is a leading provider of network security appliances. Founded in 2000, BlueCat Networks is a privately held firm headquartered near Toronto, Ontario. In 2002, in addition to its award-winning Adonis DNS Management Server™, BlueCat Networks released its Meridius Security Gateway™ appliance for relaying and filtering email. Both appliances are available in a slender 1-U, rackmountable chassis running a customized hardened Linux® OS kernel.

BlueCat Networks' Meridius appliance features several layers of protection against spam, including blacklisting, whitelisting, real-time DNS lookups, open relay checking, and open source SpamAssassin for header and body text analysis. An incoming email that is determined to be spam can be rejected, marked as spam and delivered to the email user's inbox, or quarantined to the Meridius Quarantine Mailbox for further review. Users receive on a scheduled basis, typically daily, an email alert advising that new messages have been quarantined. The alert includes a link to an HTML page that offers a simple choice to either delete or release each message for delivery. Administrators set the "time to live" for deleting quarantined messages. Each Meridius Security Gateway appliance includes a ZMailer server as its SMTP MTA, a DNS server, and a Java technology-based client management console with SSL and HTTPS encryption. Antivirus protection from a third party is optional. The appliance is designed to sit in the demilitarized zone (DMZ) in front of the email servers to provide optimal security at the Internet gateway.

During the past year, BlueCat Networks recognized that spam was changing quickly and becoming more sophisticated to detect. Thus, it looked for a way to boost its product's effectiveness by blocking the latest spam in real time.

BlueCat Networks was introduced to Commtouch's RPD technology. After several months of testing, the engineers at BlueCat Networks reported that Commtouch RPD delivered an unprecedented detection rate for spam as it continues to evolve. The engineers also reported minimal false positives, which tended to be bulk newsletters that could be whitelisted using the Meridius Management Console. BlueCat Networks proceeded to license the Commtouch SDK and now offers its customers the option to add a real-time, content-, format-, and language-agnostic spam detection engine as the first layer of protection against spam in its Meridius Security Gateway appliances. Customers continue to use the other layers of antispam protection, and the Meridius Management Console manages all of the features of the appliance, including the Commtouch engine.

"The market has become saturated with antispam products that use 'tired' techniques such as Bayesian filtering and heuristics text analyses. These methods are no longer as effective at detecting spam as they once were," noted Michael Hyatt, president of BlueCat Networks Inc. "Professional spammers have become more sophisticated at avoiding detection and are earning a lot of money doing so. RPD technology differentiates BlueCat Networks and the Meridius Security Gateway appliance from all other players and products on the market today. It's what is helping stop spam before spam stops customers."

BlueCat Networks' customers are equally impressed. "Since our deployment of Meridius, we have quarantined literally a few thousand messages per day and we have less than 400 mailboxes. The most impressive piece, in my opinion, has been the Commtouch Real Time RPD add-on," said one customer. Another customer said, "I had people who had as many as 400 spam messages a day cluttering their box. After installing the Meridius — especially with a new upgrade to the spam engine — people's spam consumption has gone way down. We are seeing [detection] rates much higher than 95%. When spam does get caught, users are notified directly without any intervention from me and they retrieve any false positive, of which there are few, all by themselves. I set this thing up and watch it go! Perfect!"

For a snapshot look at Commtouch's effectiveness at BlueCat Networks, see Figure 3 for a timeline of received and quarantined emails read from right to left that shows the significant increase in spam detection (i.e., quarantined emails) when the RPD layer on a Meridius appliance is turned on.

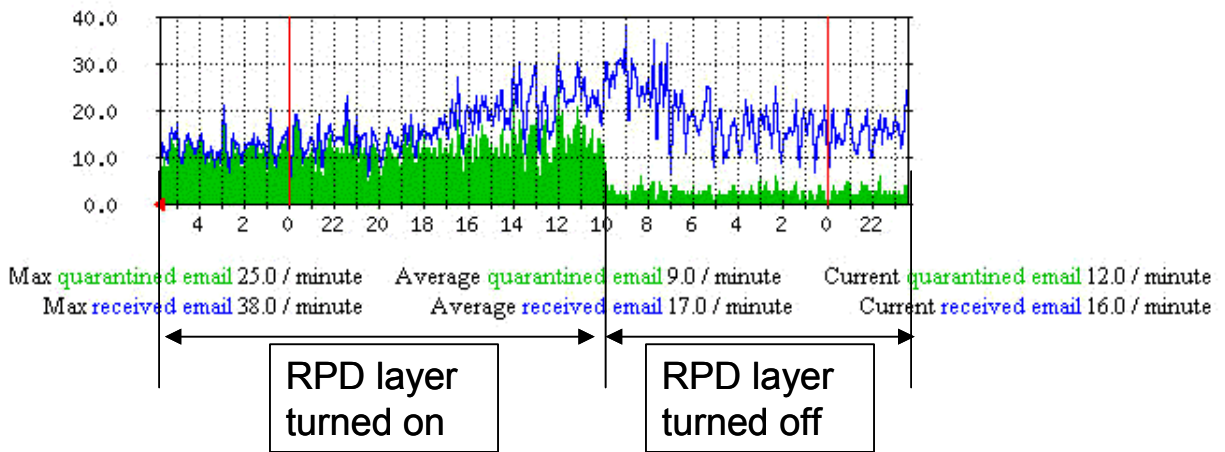
**FIGURE 3**

Effectiveness of RPD at BlueCat Networks

## Quarantined Emails

The statistics were last updated Wednesday, 3 March 2004 at 5:47

### Daily Graph (5 Minute Average)



Source: BlueCat Networks, 2004

### **Customer Profile: Houlihan Lokey Howard & Zukin**

Houlihan Lokey Howard & Zukin ([www.hlhz.com](http://www.hlhz.com)) is an international investment bank that provides a wide range of services, including mergers and acquisitions (M&A), financing, financial opinions, board advisory services, financial restructuring, and merchant banking. The firm has ranked among the top 20 M&A advisors in the United States for the past 11 years, and it has the largest financial restructuring practice of any investment bank in the world. The firm has over 600 employees and 1,000 clients. Established in 1970, HLHZ is a privately held firm headquartered in Los Angeles, with nine offices in the United States and the United Kingdom.

Constant dissatisfaction with the time spent by email users on spam, including complaints from company executives, convinced HLHZ's IT department that the spam problem had to be resolved. Initially, HLHZ tried blocking known spammer addresses and domains with the help of a commercial software product. However, even with continuous updates requiring significant management effort, as spammers became

more inventive and spam volumes tripled, the solution did not block enough spam and false positives reached an unreasonable level due to domain blocking. In spring 2003, HLHZ deployed a second commercial antispam software product that was self-managed, automatically updated, and touted zero false positives. This product was effective in blocking about 15,000–18,000 messages daily, but email users complained that too much spam — approximately 10–15 messages daily — still reached their inboxes.

When HLHZ heard about Commtouch's RPD technology, it decided to conduct a side-by-side comparison with its existing system. After 3–4 weeks of running spam messages received in test mailboxes through both systems, The Commtouch solution missed only 2 spam messages, while the other system missed 129 spam messages.

HLHZ began deploying the Commtouch solution in fall 2003 as an addition to the existing spam solution, acting as a complimentary filter. HLHZ has experienced very positive results. Email users report that only 0–2 spam messages reach inboxes on average each day with the Commtouch solution. Senior executives have stopped the CIO in the hallway to say, "The spam thing that IT did is working really well." The IT staff appreciates the minimal administration time needed to keep the Commtouch solution running smoothly. One example is that spam quarantine folders are created quickly and easily in Microsoft Outlook by adding email users to an antispam group in Microsoft Exchange. The software is easily installed when users click on their quarantine folder without any administrator privileges. Another example is a recent software upgrade that was accomplished in the middle of the workday without any disruption.

A unique feature identified by HLHZ is the way the Commtouch solution can hold suspected spam for a specified amount of time and then recheck it with the latest information about new spam attack waves. HLHZ's other system tended to allow new spam messages get through before the system's spam database was updated, and therefore it was unable to recognize the messages as spam.

When the Commtouch system occasionally suspects legitimate newsletters or other bulk mailings as spam, these emails are quarantined in the junk mail folder. Email users can subsequently review their junk mail folders and approve the legitimate mailings and exempt them from future quarantine by clicking a single button.

Overall, HLHZ is very pleased with the Commtouch solution's effectiveness in detecting spam, very low false positives, and minimal administration.

## **CHALLENGES AND OPPORTUNITIES**

Finding the key to unlock the spam problem will continue to challenge antispam solution vendors and customers alike. Spammers remain highly motivated by the money to be made from spam and will work hard to find new ways to send spam that will reach at least a portion of the intended recipients. Spammers are known to buy antispam solutions to figure out how they work and how they can be beaten.

The creativity of spammers must be matched by the innovation of solution providers. To maximize effective and accurate spam control, antispam solutions will need to combine various layers of protection against both known and unknown spam while

minimizing the number of false positives. In addition, while many firms currently choose standalone antispam products or services in the interest of getting a best-of-breed solution, a growing number of firms will prefer integrated comprehensive secure content management (SCM) solutions with antivirus, firewall, encryption management, Web filtering, instant messaging, and other capabilities. Vendors with spam detection technologies will benefit from partnerships that can offer customers these comprehensive solutions.

## **CONCLUSION**

When considering an antispam solution, companies should pay close attention to the detection technology it utilizes. Key success factors for antispam solutions include spam detection effectiveness of at least 94–95% with minimal false positives, frequent and automatic spam pattern updates, and multilingual coverage and durability over time to keep up with the latest spam.

Organizations should consider innovative approaches that can quickly detect spam based on characteristics that spammers cannot easily change, such as the innovative RPD technology that proactively scrutinizes the Internet to detect new spam outbreaks in real time based on bulk mailing characteristics.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.