

USA.NET

Quadrupling the Catch Rate of Image-Based Spam with Symantec Brightmail Helps Keep Inboxes Spam-Free at Leading Email Service Provider



USA.NET, a message service hosting provider, saw the quality of its message services threatened by a jump in image-based spam in late 2006. Symantec analysts developed new tools and techniques for an antispam solution that more than quadrupled the catch rate for image-based spam. This virtually eliminated it from USA.NET customer mailboxes, ending complaint calls from customers about spam, and helping to reduce the processing and storage burden from image based spam by as much as 95 percent.

Just Press “Send”

Available, secure, cost-effective email is a price of entry for doing business today. USA.NET, a global electronic messaging service provider, fills this need so well it is the leading exclusively-focused hosted email provider in the United States. The company serves over 1,300 corporate customers including such industry leaders as United Airlines and Farmers Insurance.

One reason for its broad customer base is quality of service. USA.NET has been named the 2006 “Top Player” in the hosted email provider space by The Radicati Group, Inc. It is also SAS 70 Type II audited, a Microsoft Gold Partner, a member of the Microsoft Technology Adoption Program for Exchange 2007, and winner of the 2006 Microsoft Excellence Award for Hosting Solutions.

Dan Wills, USA.NET’s vice president operations, explains the company’s value proposition: “Our Hosted Microsoft Exchange and CMS email solutions provide reliability, security, and scalability backed by a commitment to operational excellence. Since our solutions are modular and scalable, our customers can grow their business without having to invest additional resources, time or capital into their mission-critical messaging infrastructure.”

Customers can choose from three tiers of hosted Microsoft Exchange service, and all include spam and virus protection, multiple secure access methods, and a 99.9% SLA for guaranteed uptime.

“Stopping spam is like stopping graffiti. It’s a distraction you need to take care of. Brightmail stopped it so we could get back to our mission: providing reliable email service.”

Dan Wills

Vice President Operations
USA.NET

ORGANIZATION PROFILE

USA.NET (www.usa.net) is the recognized leader in outsourced electronic messaging (“eMessaging”) services provided on a Software as a Service (SaaS) subscription model to small and medium businesses and large, multi-national organizations alike. USA.NET offers a complete end to end solution including assessment, integration, migration, hosting, customer care, research and development and a comprehensive suite of high value-added enhanced services.

Headquartered in Colorado, the Company is the trusted provider of complex, mission critical eMessaging solutions to corporate enterprises. From its proprietary Commercial Messaging Solution (CMS) messaging platform, offered to franchisees, affinity groups and smaller organization seeking industrial strength email, to its Hosted Exchange platform being used from SOHOs to major enterprises who seek additional features and functionality around email, USA.NET is the one-stop shop for outsourced, hosted email to more than 1,300 business customers in over 120 countries.

INDUSTRY

Business Services

SOLUTION

Information Security

The Brightmail catch rate for image-based spam jumped from 20 percent to over 95 percent.

A Picture can be Worth a Thousand Problems

In the second half of 2006, however, the quality of email service for USA.NET customers and email users everywhere became degraded by a surge in image-based spam. This is spam consisting of an image with embedded text employed as a trick to bypass text-based spam filters.

The tactic became dramatically more effective in 2006 when new high-performance software became available that can rapidly generate messages with randomized images. The images are just different enough to fool filters that attempt to detect and block large groups of uniform messages.

Spammers have exchanged this new authoring software in underground marketplaces and are using it to push out millions of unique spam messages every hour.

The actual work of generating image-based spam is typically done by botnets, or networks of compromised computers driven from remote locations. By one estimate, more than 150 million computers (or one out of every four PCs connected to the Internet) could be infected by Trojans allowing them to be remotely driven for illicit purposes.¹

By December of 2006, image-based spam generated by botnets had jumped from representing 10 percent of all spam just six months before to becoming 35 percent of all spam, as estimated by analysts on the Symantec Brightmail AntiSpam team.

Everyone is Hurt

This increase in image-based spam penalizes email users and companies in two ways: More spam evades filters and reaches inboxes, forcing users to lose precious time sorting messages and deleting spam. And because image-based messages are often five to seven times larger than text-based spam, they put an unexpected and costly burden on email server processing time and storage space. Some businesses are forced by regulations to retain every email they receive for a given period of years. For them, the burden is even heavier.

Spam had ceased to be a problem at USA.NET when it implemented Brightmail AntiSpam software in 2002, before the emergence of image-based spam and before Brightmail was acquired by Symantec. “At that point, spam virtually disappeared and everybody forgot about it,” says Jennifer Angle, senior marketing director at USA.NET.

The company has been successful using a three-layered approach to fight spam. On the outside are appliances that deny connections to known spammers. “On a given day, we’ll block over 40 million attempts to connect from known spammer IPs,” Wills says. A second layer is proprietary software that performs behavioral analysis on incoming messages and blocks them if it detects spam-like behavior. “These first two layers stop 85 percent of spam,” Wills says. “Symantec Brightmail is at the third layer, filtering out what gets through.”

In late 2006, however, image spam started appearing in the inboxes of USA.NET customers. High level executives at some of the company’s most prominent accounts were particularly disturbed at having to delete spam once again. A number of them called USA.NET to complain, and the company relayed their concerns to the team at Symantec Brightmail.

Setting Out to Turn Back the Tide

With customers such as USA.NET and millions of other companies in mind, analysts at Symantec Brightmail developed new techniques for detecting image-based spam, and new kinds of rules that block it. They increased the frequency of updates to Brightmail regarding image spam heuristics from weekly to daily. This countered the fact that spammers were speeding up the frequency with which they test, enhance, and modify their image-based spam tactics.

The new enhancements for Symantec Brightmail AntiSpam became available in release 6.0.4, reaching customers in the fall of 2006.

The Brightmail catch rate for image-based spam, as measured by the Brightmail team, jumped from 20 percent to 95+ percent—a more than a fourfold gain in effectiveness.

“Our customers are grateful that image spam is blocked. That’s a key service differentiator for USA.NET and it’s due to our multi-layer antispam solution that includes Symantec Brightmail.”

Victor Silva

Director of Client Services
USA.NET

At USA.NET, image spam disappeared from executives' inboxes. "From what we're seeing," says Wills at USA.NET, "the catch rate is even higher than that." Complaint calls about spam from executives at the company's customers stopped.

One USA.NET customer that appreciated the change was Hellmuth, Obata + Kassabaum, Inc. (HOK), a global architectural leader with 2,000 architects in North America, Latin America, Europe, and Asia. "Last fall, it seemed we went from one spam message a week in inboxes to one a day," says Ken Young, senior vice president and chief information officer at HOK. "Spam went from nothing to being an annoyance—but then it stopped."

Even one spam message a day has an impact. It takes an employee about three seconds to identify and delete it. That may not seem like much, but multiply three seconds a day by 2,000 architects and HOK gains \$17,000 a year in productivity by preventing this interruption.²

"I was just part of a C-level roundtable put on by an industry magazine," Young says, "and the panelists started to talk about how much time it took to fight image-based spam and how much was getting through. I sympathized, but didn't participate in the topic because we don't even have spam—much less a spam problem—thanks to USA.NET."

Reeling in Phishing Attempts

In addition to blocking spam, Brightmail protects USA.NET customers by detecting phishing emails received at over two million decoy email accounts in Symantec's Global Intelligence Networks. Then Brightmail updates its filters worldwide via Symantec LiveUpdate to block these messages.

Stopping phishing attempts provides added value. At one USA.NET customer, a senior executive had mistakenly responded to a phishing email before subscribing to USA.NET and Brightmail. As a result, the executive had to divert his IT security team to perform the many hours of work it takes to clear up a case of identity theft. According to executives at USA.NET, this customer is especially appreciative that virtually no phishing attempts are reaching users today.

SOLUTION AT A GLANCE

Business Drivers

- Minimize customers' productivity loss from spam
- Reduce the burden on message infrastructure by blocking spam
- Minimize and eliminate customer complaint calls

Technology Challenges

- Enhance the detection and blocking of image-based spam
- Increase the ability to keep up with a faster enhancement cycle in spammer techniques
- Enhance protection from spam-borne threats such as viruses, spyware, and phishing attempts

Solution

Symantec antispam solution incorporating LiveUpdates from the Symantec Global Intelligence Network

Symantec Products

Symantec Platinum Technical Support

Technology Environment

- Applications: Microsoft Exchange 2003, proprietary gateway and messaging services
- Databases: Microsoft SQL 2000, Oracle 10g
- Server Platform: 350 servers including Sun running Solaris, and HP ProLiant running Microsoft Windows 2000 and 2003 and Red Hat Enterprise Linux
- Storage: EMC CLARiiON, Hitachi Thunder 9570 V series

Symantec Services

- Symantec Technical Support

“The Symantec Brightmail team has also been very responsive and willing to work with us in a timely manner. The result is a good business relationship and good service for our customers.”

Jennifer Angle

Senior Marketing Director
USA.NET

BUSINESS VALUE AND TECHNICAL BENEFITS

Enhanced Information Protection

- Approximately 95% of all email traffic is blocked or filtered as spam, totaling millions of messages a day
- Fourfold or greater increase in catch rate for blocking image spam
- 99.8% accuracy rate with virtually no false positives—almost all customers switch from flagging to blocking spam³
- Elimination of customer complaint calls regarding image spam
- Virtual elimination of phishing emails

Operational Efficiency/Revenue Enhancement

- Less burden on email infrastructure/costs due to effectively blocked spam
- Increased ability to retain and acquire email service customers

Brightmail has a 99.8 percent accuracy rate, according to one study.³ Most customers new to USA.NET start with Brightmail cautiously by having it flag rather than block spam. “Within days, they see that Brightmail is stopping only spam, and they switch from ‘flag’ status to ‘delete’ status,” says Wills.

Spam You’ll Never See

“Our customers are grateful that image spam is blocked. That’s a key service differentiator for USA.NET and it’s due to our multi-layer antispam solution that includes Symantec Brightmail,” says Victor Silva, director of client services. “Our customers read in the media that image spam is afflicting most companies, yet they know it’s not reaching them. This is a valuable benefit for us in maintaining customer satisfaction and retention.” USA.NET has one of the highest renewal rates in the hosted email industry, Silva points out.

Another benefit is that with image spam blocked, customers require less email storage space. Spam makes up as much as 95 percent of the incoming email stream for USA.NET customers, the company reports, and because Brightmail and USA.NET’s multilayer approach successfully blocks it, the demands on email infrastructure are substantially reduced. “Our customers may be paying as little as 10 percent of the message infrastructure costs they’d face if spam wasn’t blocked,” says Wills.

¹ “Botnets could eat the Internet” at Silicon.com, from a speech by Vincent Cerf, one of the founders of the Internet, at the World Economic Forum in Davos, Switzerland, published Friday, January 26th, 2007.

² 3 seconds/day * 2,000 employees * 250 work days/year = 1.5 million seconds/year = 25,000 minutes = 417 hours lost to spam * \$40 per hour burdened labor rate = \$17,000 in annual productivity lost to just one spam message per day. \$40 burdened labor rate determined as follows: \$60,000 annual median salary for U.S. architects per the U.S. Department of Labor Bureau of Labor Statistics Occupational Handbook. Add 1/3rd for benefits to arrive at \$80,000 annual burdened labor cost / 2,000 hours per year = \$40 per hour burdened labor rate.

³ GCN report, 2006