



## **Spam Protection Powered by Brightmail Technologies and Response**



# Spam Protection Powered by Brightmail Technologies and Response

## Contents

<b>Executive summary</b> .....	<b>2</b>
<b>The state of spam</b> .....	<b>3</b>
Definition of spam .....	3
The lifecycle and evolution of spam .....	4
Spammers' tactics: spam creation and dissemination .....	5
<b>Advanced spam protection</b> .....	<b>10</b>
The BLOC™: spam analysis and operations .....	10
Multilayered filtering technology .....	12
Filter delivery and engine updates .....	18
<b>Conclusion</b> .....	<b>18</b>

## **Executive summary**

Aside from making money, a spammer's chief obsession is evading antispam filters. The cat-and-mouse game between spammers and antispam vendors has continued for over a decade. The first generations of spam were ASCII-based and somewhat random—easily handled by homegrown approaches and static keyword filters. But that game has evolved. The latest generation of spam incorporates sophisticated tactics such as extreme randomization, origin concealment, and filter evasion using HTML. Spammers continue to raise the stakes by devising ways to escape filtering and new ways to profit from their actions. This technology brief describes how Symantec's research and development groups continually adapt filtering techniques to challenge spammers and screen out their spam attacks.

This paper covers the following:

- **The state of spam.** A quick look at the preferred weapons of spammers, including filter evasion and dissemination tactics.
- **Advanced spam protection.** A summary of the antispam filtering technologies, infrastructure, and resources available in products powered by Brightmail technologies and response. These products include Symantec Brightmail Antispam, as well as certain Symantec Mail Security products. The topics include Symantec's comprehensive proactive and responsive filter technologies, its unique spam analysis features, and its 24x7 operations centers.

## The state of spam

This section covers the following:

- Definition of spam
- The lifecycle and evolution of spam
- Spammers' tactics

## Definition of spam

The average person, when asked to define spam, might respond by citing specific types of offensive or fraudulent email solicitations—the relentless stream of Viagra ads or the creatively punctuated Nigerian scam emails. Others might include chain letters or newsletters in which they have long since lost interest. Still others consider any sort of advertisement from any source, legitimate or not, to be spam. Indeed, for such a subjective mode of communication, an authoritative per-recipient definition can be elusive. However, it remains imperative to distinguish spam sent by malicious spammers from legitimate mail.

Symantec uses the guidelines outlined in Figure 1 to distinguish spam from legitimate email communication.

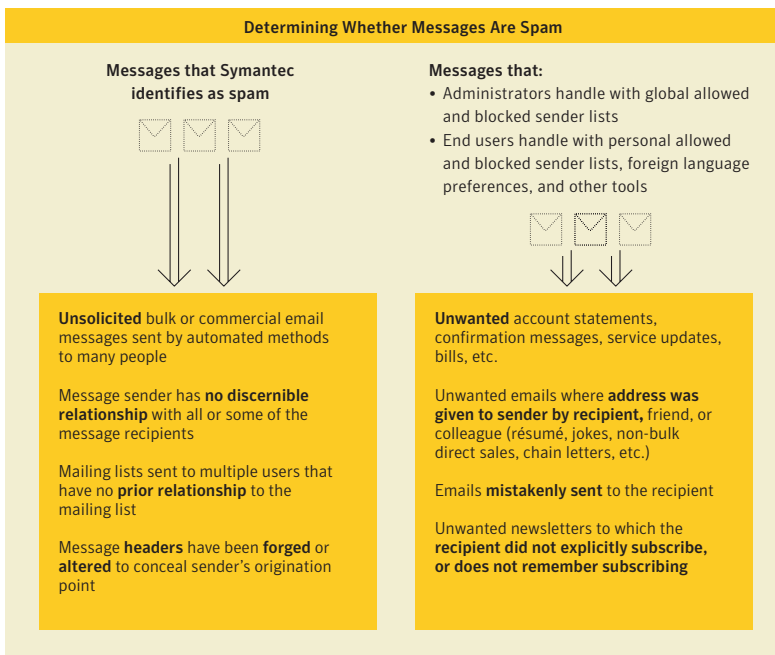


Figure 1. Determining whether messages are spam

## Spam Protection Powered by Brightmail Technologies and Response

Spam messages waste corporate resources. Random, untargeted email sent by automated methods has a measurable impact on enterprises. Such spam directly consumes IT administrators' time, along with company mail server and storage resources. And, because large companies estimate that their employees spend as much as 15 minutes of their day reading, deleting, and responding to these messages, spam is robbing employees of precious time and costly productivity.<sup>2</sup>

### The lifecycle and evolution of spam

Spam has been a side effect of the Internet for over a decade. In that time, it has matured to follow a predictable lifecycle with three key constituencies (see Figure 2).

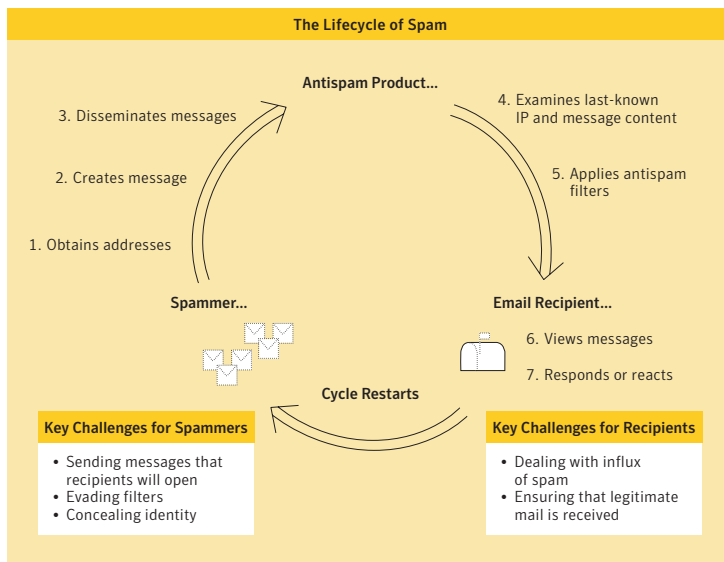


Figure 2. The lifecycle of spam

The ongoing lifecycle is driving the evolution of spam, both in its form and its implications. As a result of increased antispam filtering, along with the advent of new technologies and opportunities at the spammers' disposal, spam is rapidly morphing into an even more dangerous phenomenon.

The constant increase of spam is only one part of the equation; just as troubling is the form that many spam attacks are taking (see Figure 3). Gone are the days when spammers would simply send their unsophisticated sales pitches from their own ISP accounts. Filter-resistant spam from concealed senders is quickly becoming the dissemination mechanism of choice for costly virus attacks or email fraud attempts.

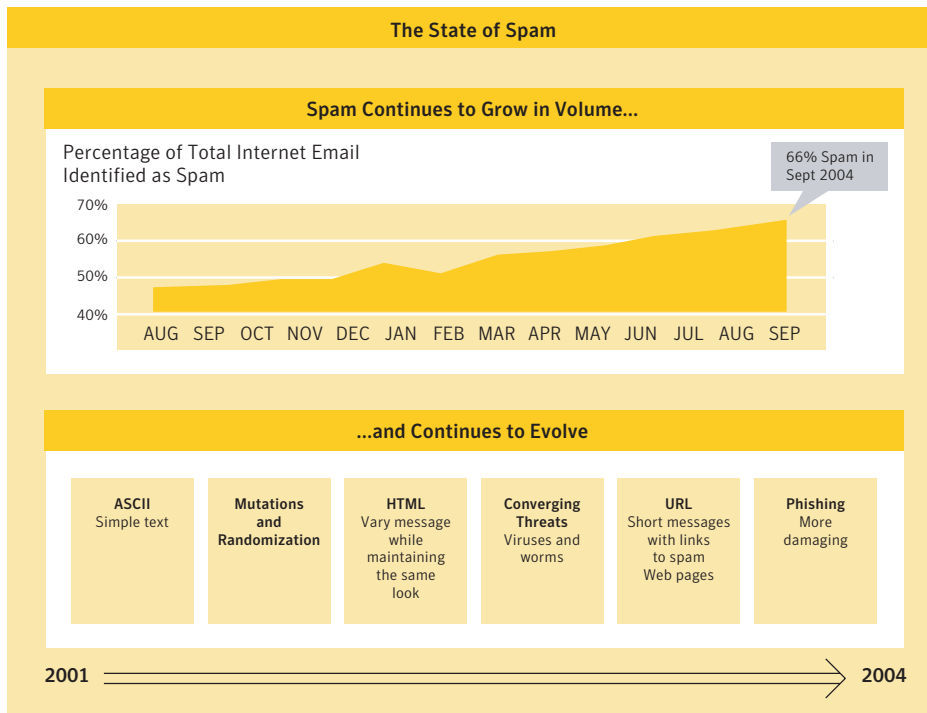


Figure 3. The state of spam

The next section covers the key aspects of the lifecycle from the perspective of the spammer.

## Spammers' tactics: spam creation and dissemination

According to the magazine Business 2.0, for some spammers to bring in \$1 million a month, all that is required is a \$20 purchase from one out of every 2,000 spammees—a 0.05% response rate. The economics of spam are hard to beat: for next to nothing, spammers can obtain lists of millions of harvested email addresses. The barrier to these riches is antispam filters. This section summarizes a few of the tactics used by spammers to evade filtering.

### *Evading filters with HTML-based content modifications*

Large-scale spammers are increasingly adaptable and sophisticated. These people or organizations can cycle through fake domain names and alter subject lines so precisely and efficiently that by the time old-line antispam tactics can discern a pattern, the damage is done and a new attack with different characteristics has already been launched. Mass mail software even allows spammers to run mail through preprogrammed checklists, evaluating whether mail will likely be blocked by spam filters.

Content modification using HTML is the effective spammer's latest and most powerful antifiltering technique.

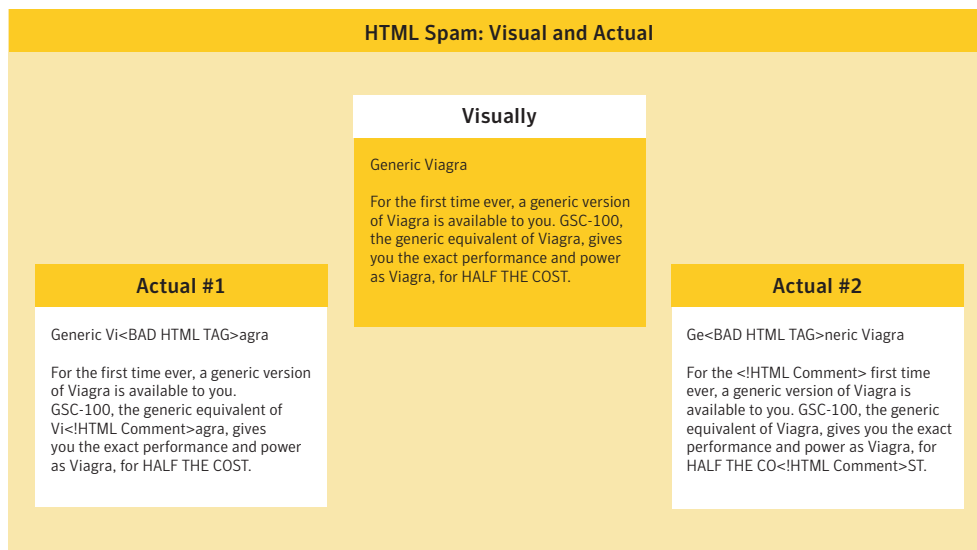


Figure 4. HTML spam: visual and actual

There are many reasons why spammers choose HTML:

- Attracts attention. Using rich media, spammers can add flashy and provocative messages without significantly adding to their costs or file sizes.
- Enables tracking. With embedded beacons and tracking devices that activate as soon as images are downloaded, spammers can verify whether the targeted email address is a live, or valid, address.
- Enables randomized or polymorphic spam. Because the underlying text of the messages is unique, this type of spam is very difficult to filter. Inserting white text on a white background, bogus HTML tags, or HTML tables are just a few of the HTML-based antifiltering tricks.

Due to infinite variations and randomizations, formatting spam in HTML provides spammers with a powerful way to circumvent filtering.

### ***Evading filters with URL obfuscation***

Spammers frequently use URL-based antifiltering techniques, soliciting recipients to perform a further action beyond just reading the message. In most cases, the spammer wants the recipient to purchase a product or register for a service. To further the transaction, spammers often include a URL that points to a Web site. Spam that encourages recipients to click on a URL is often problematic for antispam filters. First, spammers can introduce an excessive amount of personalization, sprinkling innocuous and seemingly legitimate text around the intended link. Not only can such text make the email look legitimate, but it also allows spammers to create many substantially different messages where only the underlying URL is the same. There is also a plethora of obfuscation and URL-relaying tactics that spammers can employ to conceal the target URL.

Spammers have also proven adept at disguising the external appearance of URLs so that recipients are fooled into believing that the URLs belong to a legitimate organization. The recent success of email “brand spoofing” attacks are testimony to the power of this tactic. In such attacks, spammers create fraudulent emails and disguise URLs, purporting to originate from legitimate organizations, enticing recipients to provide private and financial information.

### ***Dissemination using identity-masking relays***

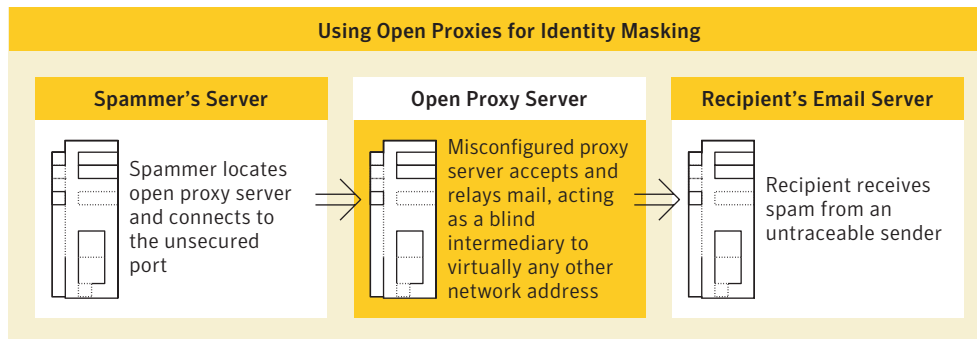
Physically sending out bulk email is a trivial matter. Special-purpose email server appliances can send out as many as 1 million email messages per hour. However, to avoid legal repercussions or source blocking via IP address, spammers need a mechanism to conceal their identities.

A common way spammers deal with the concealment issue is by using identity-masking relays. One application of such a technique is the misuse of open proxy servers. Open proxy servers are misconfigured or virus-infected computers that allow traffic for virtually any network service to be channeled through a host computer. The following table shows how open proxy servers used in this way differ from open SMTP relays, which are not actually used to mask identities.

## Spam Protection Powered by Brightmail Technologies and Response

	Open SMTP Relay	Open Proxy
<b>Description</b>	Mail server that processes mail where neither the sender nor the recipient is a local user.	Insecure host computer that accepts requests from any random computer to share the Internet connection. Also refers to misconfigured legitimate software or malicious Trojan horse viruses that allow the computer to be used in such a manner.
<b>How spammers use them</b>	Connects to the mail server with the open relay, and pushes spam mail through. The origin of the spam appears to be the intermediate server.	Connects to port 25 of the mail server as an HTTP service through the open proxy, sends a POST request, and hides the SMTP content in the body of the posted data. The mail server ignores the HTTP headers and accepts the SMTP commands in the body of the email.
<b>Identity concealment</b>	Low. Doesn't hide the source of spam, because most mail transfer agents (MTAs) add a Received: header before relaying the mail.	High. Proxies forward raw TCP/IP connections, leaving no headers. Because proxy servers allow one computer to masquerade as another, it is impossible to identify the actual originating IP address.
<b>Used for sending legitimate mail?</b>	Occasionally. Sometimes administrators use open relays to route around a problem server. Other times, they may forget to turn off open mail relays.	No. There are no valid reasons for sending mail through a proxy server.
<b>Popularity as source of spam</b>	Dwindling. Most administrators lock down their relays to stay off blacklists.	Method of choice. Most spam is not sent through the conventional mail port; it is almost always relayed using proxies. Thanks to misconfigured software and Trojan horses, vulnerable proxy servers abound.

Spammers routinely identify and hijack insecure proxy servers. Unbeknownst to the owners of the misappropriated computers, spammers then use the computers as vehicles to send huge volumes of unsolicited mail. By some accounts, two-thirds of all spam emanates from these insecure servers.



**Figure 5. How open proxy servers are an ideal way to hide the sender's identity**

## Spam Protection Powered by Brightmail Technologies and Response

Once spammers discover an open proxy, they will continue to send spam through it until the open proxy is closed. Spammers are also coming up with new ways to hijack computers to send spam, as evidenced by the recent mass-mailing computer worms, such as Sasser, Netsky, and SoBig. Initial analysis suggests that, while they didn't have especially malicious payloads, the viruses did install a mail program on victims' computers, setting the stage for an immense network of identity-masking conduits through which spam could be relayed.

### **Advanced spam protection**

#### **The BLOC: spam analysis and operations**

The high effectiveness and accuracy of Symantec's premium antispam filters are made possible by the BLOC (Brightmail Logistics and Operations Center). The BLOC consists of several centers working cooperatively on three continents, comprising a round-the-clock protection network that spans the globe. These antispam operations centers are responsible for all of the real-time tuning and adjustments that underlie Symantec's filters.

Sophisticated automatic tools, assisted and monitored by BLOC technicians, evaluate Internet mail for new variations of spam, then issue filters to identify and capture similar messages. The BLOC continuously provides updated filters to filtering software running at customer sites. BLOC technicians play an important role in confirming the identification of possible spam. This combination of automation and human intervention is essential to maintain an effective defense against ever-changing spamming techniques yet still prevent overblocking and false positives.

## Spam Protection Powered by Brightmail Technologies and Response

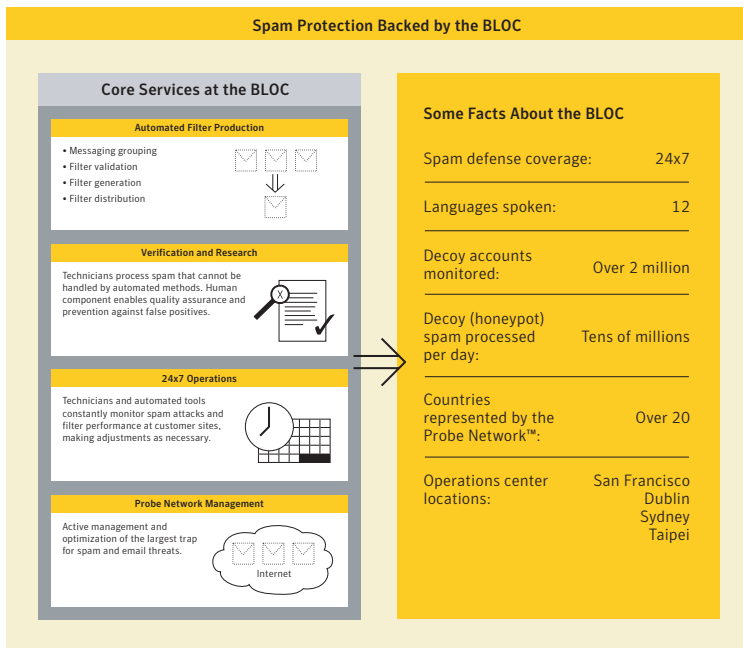


Figure 7. Spam protection backed by the BLOC

The BLOC also manages the patented Probe Network, an extensive array of over 2 million decoy email addresses and domains, also known as spamtraps or honeypots. When extended with junk mail submissions from customers, the Probe Network is statistically representative of over 300 million email inboxes. This global network of email accounts attracts and collects large quantities of spam—tens of millions of spam messages pass through the Probe Network every month. As messages come into the BLOC, automated processes and expert technicians go into action, analyzing incoming spam and developing effective countermeasures.

This spam-catching infrastructure gives Symantec knowledge about spam attacks as soon as they happen, making it possible for Symantec to automatically protect its customers against real attacks while tracking the distribution and content of spam attacks worldwide. Unlike other approaches where the filters need to be trained for three to six months before they are effective, Symantec's Probe Network is real time. Any necessary maintenance of more proactive filters, such as heuristic filters, is managed entirely by the BLOC. The BLOC also leverages over six years of history tracking spam and writing antispam filters.

## Spam Protection Powered by Brightmail Technologies and Response

The real-time spam traffic that flows through the Probe Network drives Symantec's responsive and accurate filters, such as BrightSig2™. Probe Network also provides valuable source and spam URL information for the Sender Reputation Service and URL filters, respectively.

The other essential component of Symantec's spam analysis process is the Business Intelligence team. The mission of the Business Intelligence group is to keep Symantec at the forefront in the war against spam. Among their activities are:

- Constantly analyzing spam traffic for new threats and new defenses
- Analyzing spammers' frequently used Web sites and mass-mailing software
- Monitoring forums and chat rooms frequented by spammers
- Staying abreast of evolving spammer techniques so that defenses can be incorporated in future releases

### Multilayered filtering technology

There is no silver bullet against spam. Symantec takes a comprehensive and multilayered approach to spam filtering, employing a variety of filtering techniques to keep spammers at bay. Some of the filters examine the source of the email, while others sift through the message content, leveraging both real-time spam data as well as proactive techniques such as heuristic filtering.

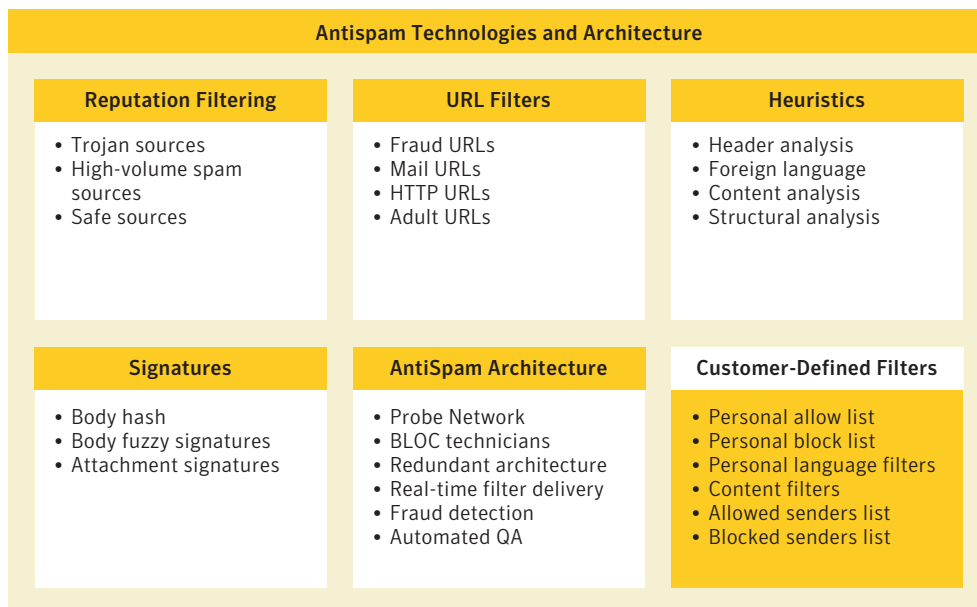


Figure 8. Antispam technologies and architecture

## Spam Protection Powered by Brightmail Technologies and Response

Symantec continuously evaluates new filtering techniques and adds new technologies to its arsenal. Each new approach is evaluated to ensure that it does not compromise Symantec's rigorous accuracy rate—which currently stands at 1 false positive in 1 million messages, an accuracy rate of 99.9999%.

### ***Sender Reputation Service***

Reputation-based blocking is a powerful filtering technique that examines the quality or reputation of the sending source or mail server. To this end, Symantec monitors hundreds of thousands of email sources to determine how much email sent from these addresses is legitimate and how much is spam. This data is incorporated into the Sender Reputation Service. By tracking data such as mailing patterns, the presence of open proxy or unsecured mail servers, volume of messages sent, and complaints, the Sender Reputation Service can determine a reputation value for a given email sender or IP address. In some cases, this value is used to allow or block senders; in other cases it is used in conjunction with other filters.

#### **Reputation Filters**

**Tactic:** Leverages reach of the Probe Network and analytical capabilities of the BLOC to create a reputation profile of email sources

**Effective against:** Large-scale spammers who use large networks with many domains and IP addresses

**Available filters:** Dynamically updated IP address lists of open proxy servers, safe servers, and suspect servers

**Unique to Symantec**

## Spam Protection Powered by Brightmail Technologies and Response

The Sender Reputation Service currently includes the following lists of IP addresses, which are continuously compiled and updated:

- **Open Proxy List.** IP addresses that are open proxies used by spammers.
- **Safe List.** IP addresses from which virtually no outgoing email is spam.
- **Suspect List.** IP addresses from which virtually all of the outgoing email is spam.

Where many competing source or reputation-based filtering techniques miss the mark is in their limited or poor quality of sender information. Unlike other collections of source lists, the Sender Reputation Service is:

- **Large in scope.** Given that Symantec filters over 15% of the world's Internet email (more than 100 billion messages per month) and protects over 300 million end users' inboxes, Symantec is in a unique position to assess the reputation of email sources. With access to this data, the Sender Reputation Service represents a substantial swath of mail server activity.
- **Automated and data-driven.** Inclusion and removal from the lists is based entirely on traffic patterns of the mail servers. Organizations or individuals cannot request or pay to be added or removed from any lists in the Sender Reputation Service.
- **Proactive and accurate.** Other lists are poorly staffed and simply aggregate information, resulting in sites being inappropriately blacklisted. The Sender Reputation Service, on the other hand, regularly generates its database by proactively seeking out insecure servers and high-volume senders, enabling rapid, automatic updates to the list. For example, in the case of the open proxy list, once an open proxy server identified by the Sender Reputation Service is secured by the owner, the server's IP address will be automatically removed when the lists are next regenerated (every hour).
- **Automatically incorporated.** Like other filters powered by Brightmail technologies and response, no ongoing administration is required.

### **Heuristics filters**

Heuristic technology provides a very proactive framework for fighting spam. Heuristic filters analyze the header, body, and envelope information for incoming messages, checking for the presence of distinct spam characteristics. For example, excessive exclamation marks or capital letters would increase the spam score for a message. Each message is assigned an overall score, which is then compared to a threshold that determines whether the message is spam or not. Heuristic filters, once they are trained to determine what spam and legitimate mail looks like, can be very effective at identifying new spam.

The downfall of many competing heuristic filters is that they can create a substantial administrative burden. Worse, if not properly trained and weighted for accuracy, they can produce significant numbers of false positives.

In Symantec's premium antispam products, heuristic analysis tests are used to determine the likelihood that a message is spam. Each test is weighted to reduce false positives. The total probability that a message is spam is examined to determine an overall score.

Symantec's heuristics are tuned and updated to deliver the standard 99.9999% accuracy<sup>4</sup> characteristic of filters powered by Brightmail technology. Unlike other solutions, heuristic filtering is not the only tool used by Symantec against all spam attacks. Also, before the filters are deployed at the customer site, Symantec optimizes the filters, weighting each heuristic based on how strongly it represents a spam characteristic. Lower-weight heuristic filters—for example, incorrect punctuation—safeguard against false positives. Higher-weight filters, such as those matching a known IP address range of a spammer, are very effective at differentiating spam from legitimate messages.

Symantec's heuristic filters do not impact administrator resources. No customer tuning or training is required, as Symantec is constantly pruning ineffective or overaggressive filters before automatically deploying filters to the customer site. The filters also do not rely on an interpreted language, such as Perl, which can be resource-intensive, choking server performance as the messages are parsed.

#### Heuristic Filters

**Tactic:** Proactively looks for common spam characteristics in all parts of the message and computes score; if score exceeds threshold, message is spam

**Effective against:** New spam

**Symantec heuristics are tuned for accuracy and performance**

## Header filters

Symantec's header filters are a combination of proactive and responsive approaches. To proactively identify first-time spam, header filters consist of regular expression-based filtering rules that exploit commonalities or trends that are present in spam messages. Examples of telltale spam characteristics that a header filter would address include:

- Watermarks of spammer tools. Traces of information left in messages by some spammer tools; for example, the name of the program used to send the message.
- Modified time zones. For example, if the time zone is off by more than 12 hours.
- Spoofed received lines. For example, if the message purports to be coming from an MTA at an organization that the BLOC knows.

Header filters also target specific spam messages that have passed through Symantec's vast spam analysis system. These attack-specific filters are very effective, leveraging the Symantec Probe Network and filter delivery system.

## Brightsig2 filters

Symantec's signature technology is the catalyst for Symantec's industry-leading accuracy rate. In general, spam signatures work by distilling a specific spam attack down to a unique string of bits, or a signature. This essential fingerprint of a spam attack can be used to identify variants of the attack. Accuracy is preserved because signatures are based on actual spam.

Spammers responded to first-generation signature technology by introducing large amounts of personalization and HTML obfuscation. Symantec, in turn, responded with its patented BrightSig2 technology. BrightSig2 technology is the cornerstone of Symantec's signature technology. The technology characterizes spam attacks using proprietary algorithms, which are added to a database of known spam. BrightSig2 matches seemingly random messages that originate from a single attack, which expedites and streamlines filter creation and deployment. This process enables Symantec to create tight targeted filters without having to write numerous such filters against a single attack. By distilling a complex and evolving attack to its DNA, more spam can be deflected with a single filter.

BrightSig2 now has specific defenses against HTML spam, specifically combating randomization and HTML noise (comments, constants, bad tags) that spammers insert to evade filters.

### Header Filters

**Tactic:** Traps spam with targeted header-based filters

**Effective against:** Messages with telltale spam characteristics in the headers

### BrightSig2 Filters

**Tactic:** Strips random HTML from spam and uses fuzzy logic to group messages

**Effective against:** Highly randomized, HTML-based spam attacks

**Unique to Symantec**

## **Attachment signatures**

Message attachments have long been a favorite tool of spammers. By attaching a deceptively named file or image to an email, spammers tempt recipients to click through and open the file. Often, the result is annoyance: The recipient must contend with an explicitly offensive image. Other times, the attachment might be malicious content, such as a Trojan horse, worm, or an executable that wreaks havoc on the recipient's computer. In response, many organizations are now simply deleting all attachment types of a certain kind (e.g., exe or zip) that have caused problems, even if a particular incoming attachment is legitimate business communication.

Attachment signatures, which target specific MIME attachments, are the latest example of Symantec's signature technology. With fuzzy algorithms similar to BrightSig2, attachment signatures enable Symantec to create filters based on a particular MIME attachment (for example, a specific pornographic image used in a real-time spam attack) and stop that attachment from reaching customers. Attachment signatures make it unnecessary to block entire categories of certain attachments.

## **URL filters**

Symantec continues innovation in URL-based filtering technologies. URL filters now address mailto URL links, preventing end users from replying to spammers via email. This next generation of URL filters also improves Symantec's ability to reverse new methods of URL masking and obfuscation techniques developed by spammers in recent months.

This patent-pending URL filter technology leverages infrastructure elements that are unique to Symantec. Using real-time spam data, Symantec builds a list of spammers' Web sites. At the customer site, URL filters compare embedded links in messages to the list of spam URLs maintained at Symantec.

### **Attachment Signatures**

**Tactic:** Extracts a precise signature of objectionable or malicious attachments in spam messages (e.g., pornographic image or worm)

**Effective against:** Embedded images, executables, zip files, etc.

**Unique to Symantec**

### **URL Filters**

**Tactic:** Identifies spam URLs in messages. Removes characters that conceal a Web site address in a message

**Effective against:** Call-to-action spam attacks; spam attacks with common URLs and radically different bodies

**Unique to Symantec**

## Spam Protection Powered by Brightmail Technologies and Response

This list is created by using a combination of offline and real-time processes, incorporating URLs from the following sources:

- **Probe Network data.** The majority of the spam URLs are extracted from incoming spam and historical data from the Probe Network.
- **Trusted third-party lists.** URL lists maintained by third-party vendors and partners are also carefully verified, cross-checked, and incorporated into Symantec's spam URL list.

URL filters are especially effective against:

- **Disguised URLs.** URL filters reverse spammers' attempts to encode URLs with extraneous characters. This newest version of URL filters features expanded defenses against URL obfuscation and filter evasion tactics.
- **Extreme randomization.** URL filters can identify a message as spam even if spammers place so much randomization into a message that other filters are ineffective.
- **Very short messages.** If a message consists of innocuous HTML text or simply a URL link to a spam Web page, URL filters would identify and block the message.

### ***Non-English language antispam technology***

Symantec estimates that between 10 and 20% of all global spam is written in languages other than English, making non-English spam a critical issue for any company doing business outside the United States.

As multilingual spam becomes a larger problem for organizations, antispam solutions must take into account the language in which messages are written. With new antispam operations centers in Taipei and Sydney, Symantec increased its global presence and multilingual base to help prevent spam sent from foreign countries from evading detection.

Symantec strengthens its antispam filtering defenses with advanced language identification abilities and heuristics that apply only to that language. By identifying the language of a message, the antispam filtering engine can run only the filters that apply to the message's language. This process results in better performance. In addition, using the available software for email clients such as Outlook, end users can define the languages in which they want to receive messages.

Although the Language Identification features are always deployed in Symantec's Heuristics filters, the per-language actions are currently supported only when the plug-in is deployed on desktops. The plug-in is a toolbar that lets users customize aspects of Symantec filtering.

#### **Defenses Against Non-English Spam**

**Tactic:** Address pervasive non-English language spam with a combination of technology and infrastructure

- ✓ Language-agnostic filtering technology
- ✓ Language identification
- ✓ Language-specific heuristics
- ✓ Fluent/multilingual BLOC technicians
- ✓ Per-user language preferences

### Filter delivery and engine updates

Every minute, Symantec software deployed at customer sites initiates a secure HTTPS connection with the BLOC. Using this pull-based connection, filter updates flow from the BLOC to the customer site. Using a similar mechanism, spam-filtering statistics from customer sites are transmitted to the BLOC, allowing the BLOC to gauge the performance and effectiveness of deployed filters.

This global spam filter update process has many advantages:

- **Easy administration.** Rules and filters are automatically and securely downloaded and installed. Heuristic filters are auto-updated every few weeks. New spam signatures and filters are pulled down from Symantec automatically, in real time, whenever there is a new spam outbreak. Administrators need never manually write, train, or update existing rules or filters.
- **Antispam protection.** The Symantec software at the customer site always has the most current antispam filters, and the BLOC has constant visibility into how effectively those filters are performing.
- **Security and privacy.** Two-way validation guarantees that filtering rules are coming from Symantec and cannot be spoofed by any other entity. Also, no confidential customer information is transmitted to Symantec during the collection of the package of aggregate rule statistics.
- **Availability.** The filtering software is never stopped during the update process. This capability prevents messages from getting through during the update process, which would leave the mail server unprotected.

### Conclusion

The lifecycle of spam continues to evolve. Spammers are escalating the battle with new filter evasion and dissemination techniques.

In response, Symantec has fortified its filtering engine and its approach to the spam problem. The multilayered antispam protection includes patented, proprietary technologies such as BrightSig2 and the Sender Reputation Service, which address the most complex and egregious spam: randomized spam and spam relayed through unsuspecting open proxy servers. Other filters, such as heuristic filters, proactively assess the probability of a message being spam. URL filters—now in their fourth generation—tackle the growing category of spam with URLs.

These and other antispam filters used by many of Symantec's antispam products are backed by the largest and most comprehensive spam-fighting resources. The patented Probe Network and Symantec's globally distributed BLOC infrastructure are further layers of defense, rounding out an accurate, effective, and unique answer to the spam problem.



## About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at [www.symantec.com](http://www.symantec.com).

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
1 408 517 8000  
1 800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. Copyright © 2004 Symantec Corporation. All rights reserved. 12/04 10337689