The Role of Country-based eMail Filtering In Spam Reduction

Using Country-of-Origin Technique to Counter Spam eMail

By Computer Mail Services, Inc.

Updated November 1, 2007

Executive Summary

The relocation of spamming mail servers, originally hosted in the United States, to foreign sites is a direct outgrowth of the CAN-SPAM law of 2004. Globally, several other countries, including Australia and New Zealand, have also used legislation to attempt to control spamming operations within their borders.

To circumvent the rule-of-law, spammers have turned to countries with fewer controls and rules to host their operations. Today, the United States is declining as the leading source of spam and countries such as China, Korea, Russia, Vietnam, and Brazil are fast becoming prolific sources. This knowledge of international spam email trafficking can be used to great advantage and assist businesses and organizations in their efforts to reduce unwanted and often harmful email.

Email traffic received from places where an organization has no legitimate interest will likely be spam. Blocking email from those countries or geographic regions (city, state, country, or continent), instantly eliminates a very large percentage of total spam received. This is the key concept behind Computer Mail Services' (CMS) XE-Filter software.

With over 200 countries in the world, the basic question when it comes to email is:

Why allow email traffic originating from countries where your company has no legitimate business?

Spam eMail "Country of Origin" Statistics

Experts on electronic messaging since 1982, Computer Mail Services, Inc. tracks messaging trends and statistics. With the 2006 release of XE-Filter, CMS has been monitoring all inbound message traffic on their mail servers to determine the "Country of Origin".

#	Country	% Of Total Spam
1	United States	24.13%
2	China	21.54%
3	South Korea	7.39%
4	France	5.29%
5	Spain	4.62%
6	Poland	3.86%
7	Brazil	2.93%
8	Italy	2.34%
9	Germany	1.90%
10	Russia	1.63%

See up-to-date figures on XE-Filter at CMS

This table shows the top 10 countries originating spam received by CMS during the month of March 2006. While the United States is still a leading source of spam, other countries are contributing significantly to the global problem. Excluding the United States, the next 9 of the top 10 spamming countries account for almost 47% of all spam email.

Asian sources among the top 10 now account for almost as much spam as North America (32.1% vs. 35.4%).

CMS expects the growing volume of spam email from Asian sources to continue until Asia becomes the greatest source of global spam.

Using a Well Defined "Business Region" to Reduce Spam by 50% - 80%

Using "Country-Of-Origin" spam filtering benefits any company, school, or government entity wherever it is based in the world. Simple elimination of regions where an organization has no interest instantly reduces the spam volume by 50% to 80%.

#	Business Region	Instant Spam Reduction
1	USA only	75%
2	North America only	72%
3	Europe only	73%
4	Asia only	53%
5	South America only	80%

See several XE-Filter customer statistics

This chart shows how an organization doing business in a well-defined region can reduce spam by banning email traffic from the rest of the world.

For example, a US company receives an instant reduction of 75% in spam email by only allowing email from US sources.

With country of origin filtering, spammers can no longer use countries with lax regulations, monitoring, and enforcement to conceal their operations.

How “Country of Origin” Filtering Works

In concept, “Country of Origin” filtering is simple and straightforward.

Every computer or device connected to the Internet has a unique Internet Protocol (IP) address assigned to it. This unique IP address is difficult to forge when used for email transmission. Every email message will contain the IP address of its originating email server so this can be used to identify the server’s country-of-origin.

With CMS’ XE-Filter, if the country is in the administrator-defined banned list, it automatically refuses the attempted email transmission thereby preventing the message from ever reaching the local mail server. Messages that are sent by mail servers from allowed countries are accepted by XE-Filter and any general spam filter can further evaluate them for delivery to the local mail recipients.

● An XE-Filter Customer’s Experience

Recently a US-based manufacturing firm found within the first 24 hours of operation their inbound email traffic consisted of 97% that were blocked by XE-Filter, amounting to over 1.3 million messages! Of that quantity nearly 895,000 (68%) originated from the top 10 banned sources.

Just imagine what load this number would represent if the messages had made it to the local mail server.

The Limitations with Blacklists

Using the originating IP address is not something new; it has been used for years to combat spam. Typical IP filtering tactics include local blacklists and DNS-based blacklists (DNSBL).

XE-Filter’s use of IP addresses to perform country-centric filtering is a new tactic that overcomes many limitations of DNS-based blacklists. Even its use of DNS-base blacklists work to mitigate several areas of concern when relying solely on local blacklists or remote DNS Blacklist servers.

● Local Blacklists: Overwhelmed by Spam Volumes

Many companies and organization rely on the use of a local table containing banned IP addresses or ranges of IP addresses. If the number of IP address entries is small, maintenance is not an issue but then the email filtering is limited and ineffective due to the large numbers of spam sources. The reality is maintaining a local IP blacklist to provide the maximum filtering coverage is a reactive and very time-consuming task requiring constant updating.

DNS Blacklists: A Popular Antispam Technique

To deal with the constant need to update IP address lists, a new type of server/service came into existence in the late 1990s. The DNS Blacklist (DNSBL) server is a shared resource that stored a database of known spammer IP addresses. These public servers receive queries from antispam filters concerning IP addresses. The DNSBL server then determines if the IP addresses are blacklisted.

Today the use of DNSBL servers is often the first line of defense against spam. An affirmative response to a query indicates that the IP address was found in the DNSBL database, so the message can be refused.

DNSBL use is very effective but there are a few limitations and issues.

Slow Response Time under Heavy Load

With every inbound message, spam filters must determine the IP address, make a query to a DNSBL server located somewhere on the Internet and wait for a response. Typically, this waiting period lasts several hundred milliseconds. It can be even longer if the selected DNSBL server is popular and fields thousands of queries per second, or if it under spammers' denial-of-service attack.

A response time of several hundred milliseconds may seem trivial but when a mail server handles thousands of messages daily this becomes important. Delays add up and can impact email server performance and slow message delivery times.

Artificially Slowed Response Time

To prevent abuse and induce paid subscriptions, some free DNSBL servers will artificially slow the response time when queries from a single mail server exceed some threshold per unit time. When this happens, the already slow response time from a busy DNSBL server will worsen.

Open to Inappropriate Blacklisting

DNSBL servers are not infallible and sometimes can blacklist innocent mail servers. This happens whenever an infected machine on a network sends out spam, one of which lands in the 'honey pot' mailbox for the DNSBL server. The end-result is that messages from this mail server will be rejected whether from business associates, suppliers and other important contacts.

DNSBL Servers Go Dark

A remote possibility occurred a few times in the last five years, which was the worst-case scenario for DNSBLs – the blacklisting of the entire Internet. Whether by malfunction or intent, these few DNSBL servers responded by labeling every IP address queried as a source of spam. Email filters relying on these servers rejected every inbound email message as spam.

No Local Control

Other than selecting which servers to use, email administrators have no control over the operation of DNSBL servers. Thus a corporate email system becomes dependent on the companies maintaining and managing the selected DNSBL servers for the accuracy of their blacklist IP databases.

XE-Filter: A New Approach To Stopping Spam

XE-Filter is the first antispam product to approach IP-based filtering on a regional or country-based level to augment traditional connection-based techniques. Depending on XE-Filter's configuration and a company's defined geographic region of operation, 50% to 90% of all unwanted email can be stopped before ever reaching a local email server.

In concept, XE-Filter operations are similar to DNSBL techniques. Indeed DNSBL testing is still performed, but only as a last of four tests to minimize frequency to query to a DNSBL server which mitigate many of the inherent DNSBL weaknesses.

USER QUOTE:

"[XE-Filter] is a very elegant and unique solution to a very real problem that is neglected by all of the other products on the market today".

Farid Saddik
CIO - R&L Brosamer

Up To 10,000 Times Faster Than DNSBL

With the local whitelist, blacklist, and IP-to-Country database held in memory, studies have shown that queries are up to 10,000 times faster that DNSBL operations.

Instead of relying on a remote DNSBL server that responds slowly to determine if a message is acceptable, XE-Filter accesses the locally cached databases. If the source is whitelisted, the message is received; if the source is blacklisted or originates from country found in the banned country list, the email is refused.

This pre-filtering of messages reduces the volume of email any installed antispam filter must process. Thus fewer queries are made to remote DNSBL servers on messages from allowed countries so that the entire messaging infrastructure becomes more efficient with improved mail delivery.

Use DNSBL Only As the Last Test

The DNSBL query to a distant and remote server is usually the slowest IP connection-based test, so do this only when needed. Only after three other quicker tests are performed by XE-Filter (local whitelist and blacklist, country-of-origin) do not result in some action will the DNSBL server query be performed.

Cache DNSBL Blacklisted Responses

To prevent unnecessary queries with duplicate IP addresses XE-Filter caches the affirmative responses from DNSBL servers of blacklisted IPs. This greatly speeds up the process and results in speed of determination on par with the other quicker tests. This feature is especially important during periods of spam surges, e.g. holiday season.

IP Number Changes for Countries

DNSBL servers need active maintenance of the IP database to stay current and accurate, but country IP address assignments change slowly due to geopolitical and technical reasons. This is because regional and country authorities control the IP assignments. Thus monthly XE-Filter "IP-to-Country" database update easily keeps up with any assignment changes, making country-based filtering operations efficient without the need for more frequent updates.

Impossible for Catastrophic Loss

Since the IP-to-country database is local, there is no possibility that its use can ever cause a catastrophic loss of email. This was the case with sites that depended on a few DNSBL servers that went dark and blacklisted the entire Internet.

Retain Complete Control

With the geographic region of business operations determined, the email administrator is in complete control. Management tools provided lets administrators easily change countries in the banned list, which are put into effect by XE-Filter the moment the list is saved.

Conclusion

IP-based filtering at the SMTP connection level is an effective strategy against the global spam problem. Now XE-Filter's country-centric approach adds one more simple and effective tactic to prevent spam from entering the email stream.

Since most companies are unaware of the extent of the foreign email traffic they receive, a free 21-day XE-Filter evaluation is available as a free download from the Computer Mail Services' website. Installing this evaluation will safely monitor to show and enumerate the country-of-origin for inbound email traffic without any filtering.

XE-Filter

Business eMail Only From Countries Where You Do Business