Greater Accuracy Through Efficient Mail Store Cleanup

The messaging security landscape has long resembled an arms race between attackers and messaging security providers. To penetrate perimeter defenses and successfully deliver spam to user inboxes, attackers constantly alter spam message contents in an effort to get their messages delivered before anti-spam defenses are able to discover and begin blocking them. This practice increases the amount of spam sent, which now constitutes up to 90 percent of all email traffic.

Today, spammers employ sophisticated techniques, including leveraging the size and power of botnets, to ensure that spam is sent as widely as possible. Up to 15 percent of the world’s computers are currently infected with Botnet malware. Spammers use botnets to send out millions of rapidly changing messages in less than a minute through multiple service provider networks. These attacks evade volume-based spam filters since only a small number of messages need to be sent from each computer to launch a very large spam attack. Today’s botnets are highly intelligent and can detect whether individual botnet computers have been blacklisted. This gives them the option to redirect attacks through service providers that have so far failed to block them.

These types of attacks represent a significant challenge to providers. Even with the most effective filtering and anti-spam policies in place, a small amount of spam can get through to the mail store, filling it up with unwanted messages. Cloudmark ActiveFilter is able to delete previously undetected spam from user inboxes, even before users have logged in to check their mail. This post-delivery spam removal can increase blocking accuracy to over 99%.

Key Features

**Industry-Leading Accuracy**
Cloudmark Authority ActiveFilter™ extends the industry-leading accuracy of Cloudmark Authority® by enabling detection of spam messages that have been delivered in the previous seconds or minutes.

**No Rescanning**
Cloudmark ActiveFilter acts upon specific messages within the mail store that have changed classification, without needing to rescan all previously delivered messages.

**Negligible Performance Impact**
Similar to the solution itself, ActiveFilter creates a negligible impact on system resources because it searches only for message ID's of spam messages. There’s no rescanning of terabytes or petabytes of email.

**Minimized Storage Requirements**
Most carriers find that their online storage requirements decrease by as much as 20 percent through the use of Cloudmark ActiveFilter.

**Carrier-Grade Scalability**
ActiveFilter is designed to support even the largest carrier implementations due to its resource efficiency.

**Favorable User Experience**
With Cloudmark ActiveFilter, users are exposed to fewer spam and phishing attacks, leading to greater user satisfaction and lower subscriber churn.
The Cloudmark Advantage

The small percentage of spam messages missed initially are typically identified by Cloudmark within seconds following delivery. Cloudmark ActiveFilter for Mail Stores increases overall spam capture rates and accuracy by continuously reviewing newly-available fingerprints to see if messages already delivered to the mail store, but not reviewed by users, were actually spam. This reduces the impact of high-speed attacks that may attempt to capitalize on any degree of latency in spam filter updates by providing the ability to retroactively act upon spam messages that were able to evade the gauntlet of IP reputation, throttling, and content filtering functions at the network edge.

It is generally accepted that re-scanning the entire mail store for missed spam messages is not feasible for a typical carrier due to the high resource demand required to reprocess terabytes or petabytes of data in the mail store, Cloudmark ActiveFilter is designed so that it is unnecessary to rescan every message in the mail store. Instead, it uses a “push” paradigm that moves or deletes only specific stored messages that have been identified as spam after initial delivery, but prior to users checking their inbox, causing minimal CPU impact.

Fast and Efficient

Cloudmark uses a unique combination of Advanced Message Fingerprinting and real-time threat reporting from the Cloudmark Global Threat Network™, consisting of billions of trusted users in 165 countries, ensuring fast and efficient response times. Cloudmark’s Advanced Message Fingerprinting technology reduces a spam message to a lightweight set of fingerprints. Cloudmark ActiveFilter then caches the fingerprints that have been scanned and delivered to the mail store while also continually monitoring for new fingerprint updates from Cloudmark’s Global Threat Network. If there is a match between a newly-identified spam fingerprint and a message in the mail store, Cloudmark ActiveFilter instructs the mail store to take action on just that specific message.

Cloudmark ActiveFilter virtually neutralizes any advantages of advanced spam distribution techniques designed to evade traditional content filters. The result is dramatically lower levels of spam being stored in the mail store and minimal impact to CPU and disk resources.

Cloudmark ActiveFilter Process Flow

As messages are scanned by the gateway MTA, Cloudmark ActiveFilter keeps track of fingerprints for messages deemed to be legitimate at initial reception time. As new spammy fingerprints are discovered and downloaded by Cloudmark Authority®, they are compared against ActiveFilter’s cache of legitimate messages to check if any of the initially legitimate messages were actually missed spam. Messages are only scanned a single time, as they’re arriving at the edge MTA.

If a missed spam message is found, ActiveFilter is able to undertake the prescribed action within the user’s policy to remediate the missed spam message on the backend mail store host, deleting the message or moving it to the user’s spam folder before the user has checked their inbox.

Cloudmark Industry Affiliations:

More Information:
www.cloudmark.com

Americas Headquarters
Cloudmark, Inc.
San Francisco, USA

Asia Pacific
Cloudmark, Inc.
Singapore

Japan
Cloudmark Japan
Tokyo, Japan

Europe
Cloudmark Europe Ltd.
London, UK

© 2001-2013 Cloudmark, Inc. All rights reserved. Cloudmark, the Cloudmark logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Cloudmark and its subsidiaries in the United States and in foreign countries. Other brands and products are trademarks of their respective holders. All product information is subject to change without notice. DS318.2013Q2