barricademx

Executive Summary

Industry estimates state that there are 70 million subverted computers worldwide and that 8 to 9 million are used to send spam in a given month. Using our live spam trap, Fort Systems Ltd and SnertSoft developed techniques to analyze, in detail, the Mail Transfer Agent (MTA) connection between the bots and other spammer systems and the receiving MTA. The result of this analysis enabled us to develop techniques that are extremely effective in determining that an incoming email is spam well before the bulk of the message is accepted for delivery.

A new lightweight, small footprint computer-based anti-spam application, BarricadeMX is designed to sit in front of one or more Mail Transfer Agents on SMTP port 25 where it acts as a proxy, filtering and forwarding mail to one or more MTAs.

Introduction

BarricadeMX supports a variety of well blended anti-spam filtering tests that can be individually enabled or disabled according to the rigors of the postmaster's local filtering policy. Some of the tests available are:

- ClamAV anti-virus support
- "Client-Is-MX" heuristics for PTR and IP in name checks
- Concurrent connection limits
- Connection rate throttling
- DNS real-time blacklists
- Drop on N bad SMTP commands
- Enhanced grey-listing
- HELO claims to be us
- Local black/white list by IP, host name, domain, MAIL, RCPT
- Message limit controls
- Message size controls
- Recipient verification using call-ahead
- Sender verification using call-back
- SIQ protocol support for reputation services
- SMTP command & greet pause
- SpamAssassin anti-spam support
- SPF Classic support
- Tar pitting negative SMTP responses
- URI blacklist test of PTR & HELO
- URI blacklist testing of message content
- White wash & backscatter prevention using EMEW (Enhanced Message-ID as Email Watermark)

Most of these tests are optional and many are configurable by Domain.

If the existing receiving MTA is running on the same system as BarricadeMX, the existing MTA is simply reconfigured to listen for messages on another port. If BarricadeMX is running as a standalone email gateway, it can be configured to connect to the receiving MTA on another system or configured to route mail for individual domains to different ports and other systems. BarricadeMX also supports both IPv4 and IPv6 routing and addressing.

BarricadeMX may be configured to run on multiple gateways which share multicast or unicast caches. These caches provide a fast, simple, and efficient means to share cache updates across multiple gateways on the same network segment or back and forth to a set of remote hosts. Both the multicast and unicast caches use a broadcast-and-correct model and support IPv4 and IPv6.

By using an independent SMTP pre-filter in the form of a proxy, BarricadeMX avoids portability differences and limitations present in MTA extension methods (milters, plug-ins, rule sets) which allows it to tightly couple and integrate certain tests to improve performance and message throughput. It may be configured to run as a proxy for any MTA, Sendmail, Postfix, Exim, or Qmail. This allows BarricadeMX to be used in front of any existing anti-spam application to enhance spam detection and reduce loads on existing mail servers, gateways and mail hubs.

The BarricadeMX Architecture

BarricadeMX is a small (4 MB resident memory), lightweight, multi-threaded C program. Much more efficient than the typical MTA, it can gracefully handle more simultaneous incoming connections. A single CPU system has been seen to handle over 1018 concurrent MTA connections without failing. Many servers that are in production routinely handle only 100 to 200 incoming simultaneous connections without the load on the system exceeding 3.0.

BarricadeMX is equipped with a comprehensive web interface that enables the administrator to fully configure all of the options necessary to protect each domain from spam and to white or black list specific sender, domains, IP and IP ranges.

The BarricadeMX User Experience

In a real life implementation of Barricade MX, the program reduced fifteen (15) gateways that were handling between 1.2 and 1.4 million messages per day to three lightly loaded gateways. Before the installation of BarricadeMX, the fifteen existing servers were overloaded and regularly fell behind with a message delivery delay in excess of thirty minutes during peak times of the day.

The system configuration on the three servers was as follows:

- Intel(R) Pentium(R) D CPU 3.00GHz
- 2 GB memory
- BarricadeMX and MailScanner software installed

After installing BarricadeMX the load average on the servers rarely exceeded two and usually ran below 1.0.

The application of Barricade MX therefore resulted in the following:

- Average Connections / day: 323,446
- Average Connections / second: 3.74
- Load Average: hovers around 1
- Messages accepted through DATA Phase: 9.93%
- Messages rejected before DATA Phase: 90.07%

These results are typical of all BarricadeMX sites; over 90% of the messages are rejected at the MTA level. These messages are comprised of mostly spam and viruses, with almost no instances of “good” email being rejected. In these few cases, the “good” mail was rejected because of easily detected, very poorly configured servers that were not RFC compliant. The rejected mail was white listed where appropriate.

- Non-existent DNS records for the sending MTA

- Unqualified hostnames for the sending MTA. i.e., localhost not “mail.abc.com”, a FQDN

The rules we enforce for delivery are no more stringent than those enforced by AOL.

While almost all non-spam email will be accepted by BarricadeMX, it may be necessary to accept email for some senders whose email gateways are not configured in conformance with published and accepted Internet Standards. This may occur when sending MTAs:

- Which answer the HELO with a hostname which is not a fully qualified DNS hostname, i.e. local host instead of mail.abc.com

- Which do not follow the mandatory retry of the email transmission after receiving a temporary failure (4xx error)

- Which attempt to send email before receiving the MTA banner message, i.e. they assumed pipelining was okay

Because BarricadeMX’s efficiently detects spam emails, it is not necessary for the user to create white lists or black lists, however, black and white listing any senders that are currently listed on existing anti-spam software is recommended.

Conclusion

New light weight, small footprint Barricade MX is a computer-based anti-spam application designed to filter and forward mail to one of more MTAs. Equipped with a variety of spam filtering tests, Barricade

MX may be configured to run on multiple gateways. It is much more efficient than any typical MTA, gracefully handling more simultaneous incoming connections. BarricadeMX greatly reduces the load on existing email systems by correctly rejecting most spam and dangerous email before these messages are accepted for delivery.

WWW.FSL.COM

3807 Fulton St., NW
Washington, DC 20007

SALES INFORMATION:
Local: +1 604-507-1699
Toll Free: +1 866-484-5669
Fax: +1 604-677-6675

info@fsl.com

FOR TECHNICAL SUPPORT:
Phone: +1 202-338-1670
Fax: +1 202-448-2969