SpamLion™

Product Review

Meet Bob, the Network Administrator at My Company, Inc. Today is Friday. It is way past quitting time and Bob is still engaged in some frantic research. That day, Betty, the President's Executive Administrator, received a piece of unsolicited e-mail with content that was downright rude! Bob's boss, Tom, became upset because, the President became upset because Betty was upset, and now our friend Bob has once more been drafted to "Fix the problem – permanently!"

You're thinking, "Not another Anti-Spam story!" Alas, it is – with a happy ending. When Bob visits the SpamLion web site, http://www.SpamLion.com, he will quickly discover like many others have recently, a truly world-class solution to the proliferation of Unsolicited Commercial E-mail into our professional lives.

Why filter 60% when you can block 100% of all unsolicited e-mail entering your corporate mail server? All this, without interrupting correspondence with your existing contacts or any new people you send mail to? Why work at trying to fine-tune a filtering policy that is prone to error and misdirected e-mail? An ever-increasing amount of spam now comes with HTML-embedded images. Current filter technology is ineffective on embedded gif images. These messages force recipients to wait until often-offensive graphics fully load before the messages can be deleted. Perhaps, this was Betty's experience. The illustration in Figure 1 clearly illustrates Bob's e-mail world with "spam factories" cranking out hundreds of messages targeted at his mail domain.

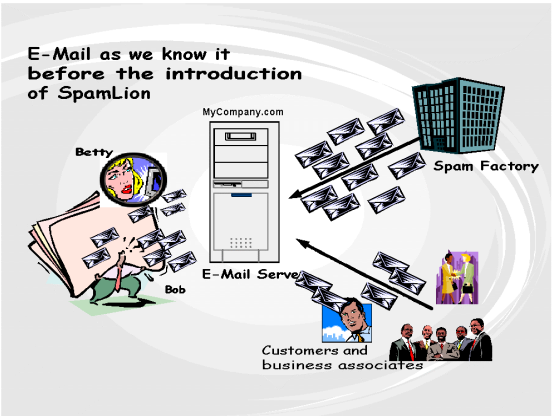

Figure 1, E-Mail before SpamLion

Perhaps the question to ask is, "Why place the entire burden of spam prevention on yourself when it belongs with the sender?"

The credit for soon cleaning up Betty's mailbox and making Bob a "Hero" goes to SpamLion™, an innovative and revolutionary product from a seasoned technology company, located just North of San Francisco in Sonoma County.

I have SpamLion protecting my company's mail server and I have installed it to protect three of my customer's mail servers over the last two months. The idea behind SpamLion's method is flat-out brilliant - it just blows away the competition!

Here's how it works. SpamLion stands apart from the crowd in that it works at the mail server level not at the recipient mailbox. This means that there is a central point of administration and there is absolutely no client software to install or configure. This is great news for Administrators!

SpamLion automatically places the e-mail address of folks you communicate with on a "White List," which means that e-mails from those parties come through without interference. The program "learns" by adding the addresses of any outgoing e-mails to the White List automatically. It operates on the assumption that people want to hear back from anyone they write to.

But here is where the big difference comes in. SpamLion was developed based on the premise that real people exist behind the e-mail address. E-mail from anyone who is not already "registered" on the white list is automatically held in a Quarantine located on the SpamLion server. The program sends a message on the recipient's behalf to all those would-be correspondents that tells them that their e-mail has arrived at the intended destination, but is being held in a Quarantine. The e-mail asks them to "register" with the company's SpamLion server in order for their message to be delivered to the intended recipient. The message contains a specific, easy to follow instruction that directs the person to perform a simple action, like clicking on a URL that will quickly complete the verification process. Each registration is uniquely coded to insure that it can't be spoofed or duplicated by some automatic process.

Since SpamLion focuses on "First Contact", it relies upon real people to respond to this registration process. According to Jennifer Sealy one of the SpamLion developers, "Spammers will be wasting their time. The product works because it's simple for real people to comply, but impossible for mass-mailing machines." The entire SpamLion "First Contact" concept is illustrated in Figure 2.

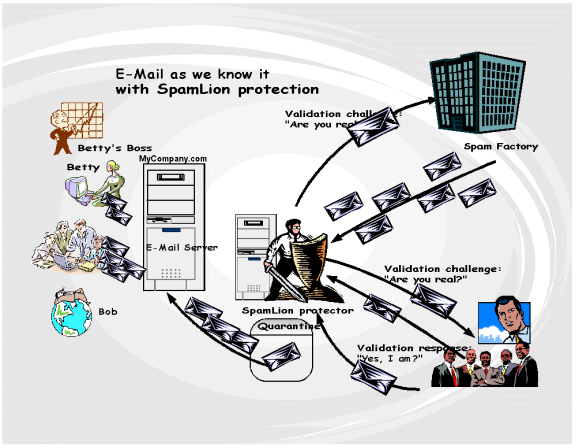

Figure 2, SpamLion protected mail domain

In essence, SpamLion software turns your Mail server into the digital equivalent of your front door. If strangers want to enter your house, they have to knock and identify themselves first. Anyone who won't do that is automatically turned away without bothering you. Current e-mail protocol openly welcomes all visitors regardless of their intent or message content. SpamLion takes this analogy and applies this process of identification to what they call the "First Contact" approach to e-mail management.

Most all Spammers use invalid e-mail addresses, so they simply won't receive the notice to be validated. Those few who do would have to deal with people one at a time, a task beyond their ability. Simply put, the problem goes away.

In the past, the burden of dealing with unwanted e-mail was placed on our poor friend, Bob or on us. SpamLion's automation easily eliminates that burden.

So now that you know how it works, what does it take to make it work? Warning, technical details ahead!!

Quite simply, SpamLion runs on a Windows 2000 server and relies on Internet Information Services (IIS 5.0) components SMTP and WWW services to do the heavy lifting. But not everyone has Windows, you might be thinking. What about Unix, Linux, Netware and Macintosh? Well, mail servers running on those platforms will communicate with other mail servers using the SMTP mail protocol across the Internet, so SpamLion will work with any mail server, regardless of the operating system they use.

It's also rumored that SpamLion is developing a "SpamLion Appliance" – a self-contained hardware and software solution that will ship pre-configured to the customer's e-mail environment. You simply connect it to your network and turn it on. No monitor, keyboard, mouse required.

Let's get back to Bob's world. The SpamLion installation program needs to know the IP address of your SpamLion Server, the name of your protected e-mail domain(s), the Fully Qualified Domain Name (FQDN) and the IP address of your mail server. The installer program will configure the web site and the SMTP virtual server as well as a Collaborative Data Object (CDO) Event Sink to be able to examine the headers of the mail traveling through your mail server. SpamLion doesn't replace your mail server - it supplements its functionally by providing you with a level of e-mail management.

You enable SpamLion on your network by adding a Domain Name System (DNS) host record (A record) for the User and Administrative web-based interface. You also, create a DNS Mail Exchange (MX) record so that all inbound mail destined to your Post Office first passes through SpamLion before reaching your mail server. In order for SpamLion to see your outbound e-mail, configure your mail server to deliver mail directly to SpamLion. This is not a Relay in the "bad" sense of the word. This is considered a "Gateway" or "Smart Host" that delivers mail directly to the designated server for final distribution. Spammers simply can't use the SpamLion server as a "Spam Relay".

Periodically, some users will like to log in to SpamLion to check their individual Quarantine. SpamLion is set to notify users if they have new, un-validated mail in their Quarantine. Are you notified each time an e-mail message arrives in Quarantine? No, the user sets the notification interval to match their preference. Remember, e-mail in quarantine is from "non-real people"!

Users, request a secure login from SpamLion that arrives as a URL in an e-mail message. Launching the URL admits them to their Quarantine. A sample screen shot is shown in Figure 3.

This illustration of the SpamLion User Interface shows the number of messages currently in quarantine as well as new messages that have arrived since the last login. The interface allows the user to SpamLion protection. Bypass Protection? Well, it is a matter of choice. Isn't it?

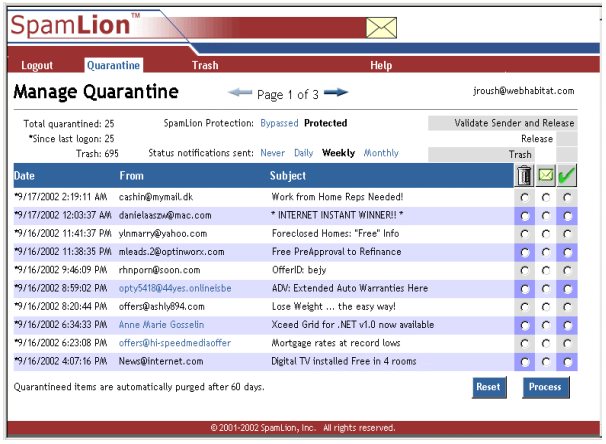

Figure 3, Manage Quarantine

change the notification interval and allows the individual user to bypass SpamLion protection. Bypass Protection? Well, it is a matter of choice. Isn't it?

Once inside the Quarantine, you can choose to send the message to Trash, Release the message to your inbox, or Release the message and Validate the sender. With a single click, the interface allows you to perform an action on all that are displayed (select all for "trash" is very popular), or mix and match by selection specific actions for each message (validate and release the automated newsletter I belong to). Press the Process button and you're done!

So far, we have SpamLion consuming mass quantities of "spam" and the individual user, like our Betty, periodically checking in Quarantine to find that things are all under control. What's left for Bob, our SpamLion Administrator and "Hero of the First Order", to do?

Well, Periodically, Bob can log in to SpamLion using the Administrator login and check on the system's overall activity. The home page is shown in Figure 4.

(please turn to page 35)

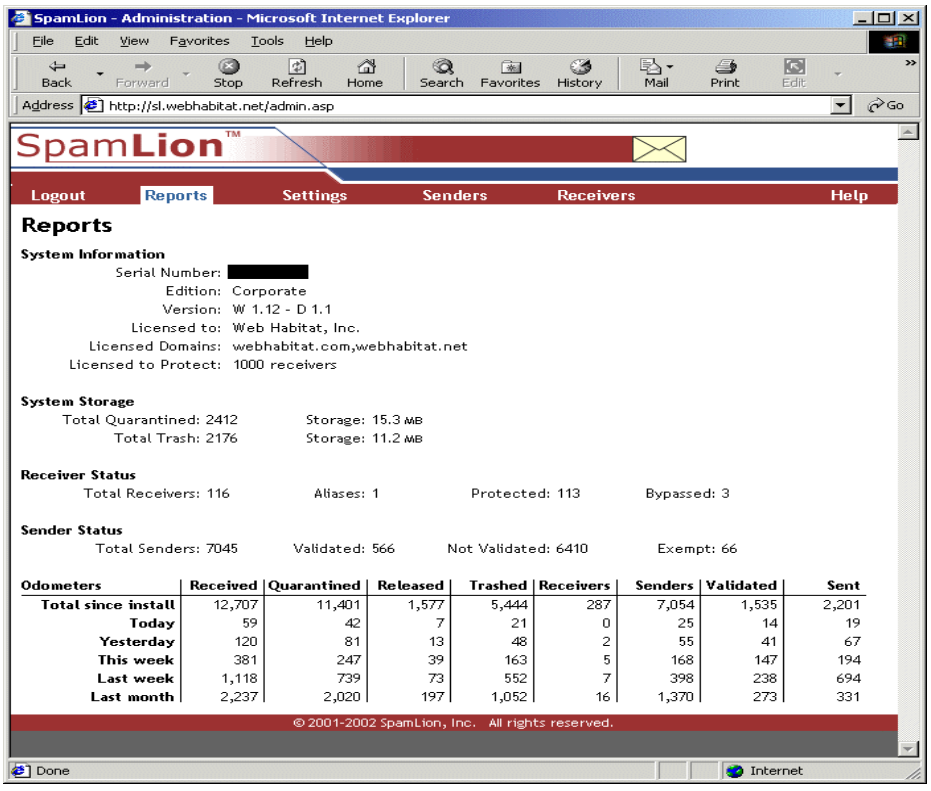

Figure 4, Reporting and Management

SpamLion Product Review

The SpamLion developers have been quite busy lately and they promise that the next version, release 1.2, will have increased reporting capability. For now, the "Home Page" lists various statistics that Bob could use to keep his manager informed of how well SpamLion is performing. Let's take a quick tour of the next illustration.

We see SpamLion's statistics for Web Habitat, Inc., one of the early SpamLion deployment sites. The top of the display shows the size of the database and the message count. Quarantine and Trash containers are automatically cleaned at a time interval specified by the administrator. The internal database is also compacted at a set schedule in order to reclaim disk space.

The odometers register the message counts. We see the number of inbound messages in the "Received" column, the number temporarily held or "Quarantined", the number "Released" from the quarantine and forwarded to the recipient, and last, the number of messages that have been deleted or "Trashed".

We can use this formula, (Quarantined – Released) / Received, to derive the percent of spam received by this company. In the illustration, last month, approximately 81% of the messages were considered "spam". All were stopped – dead in their tracks!

The remaining columns on the right indicate a count of new "Receivers" or mailboxes discovered by SpamLion, the number of "Senders" or mail addresses that were sent outbound mail, the number of people who have "Validated" their e-mail address and registered with SpamLion and the number of outbound e-mail messages that were "Sent".

That about wraps up the SpamLion story. Once, installed it just keeps running and doing its job – protecting your e-mail domain.

The happy ending? Oh yeah, Bob convinced his boss to convince the president to buy the product. Bob installed it in a matter of a few hours and Bob has some free time on his hands – don't tell his boss. As for Betty, not only is she no longer receiving offending spam; but she is also discovering that she is more productive in her work place. That pleases, the President and when the President is pleased, everyone is happy.

John Swanson is an independent consultant currently on assignment with Web Habitat where he uses his spare time to write reviews for products that he believes in. He can be reached at jswanson@webhabitat.com

Reprinted Article