Messaging Firewall

Whitepaper

www.cmsconnect.com

Introduction

"Well, there's egg and bacon; egg sausage and bacon; egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam; …"

-- Monty Python's Flying Circus, 1970

Beginning from the time when the word "spam" was used as a pejorative item in this now-famous Monty Python sketch to what you are experiencing with the deluge of unsolicited junk messages clogging your electronic mail, spam has gone from being humorous to the harbinger of serious consequences. In spite of the US CAN-SPAM Act of 2004, spam continues to increase. Today as much as 85% of messages being received by corporate mail servers are spam with no signs of abating.

Everyone now realizes the consequences of spam are numerous:

1. Loss of human resources on the part of the recipient whose inbox is full of spam, opening some and deleting many others.
2. Loss of human resources on the part of the email administrator who has to deal with why Internet mail delivery is bogged down.
3. Loss of computer resources as spam consumes disk space.
4. Loss of stolen connectivity bandwidth being used to carry spam.
5. Loss of company reputation if the mail hosts are being hijacked to relay spam and the public believes the company is engaged in spamming others.

The price paid by spam victims is too high. Assuming it takes only five seconds to complete the deletion of a single spam email, at a fully-loaded average of $25 per hour per employee[1] the productivity loss for a single spam is about US $0.03. While that may seem small, on an annual basis the loss amounts to $200 per employee who receives 25 spam messages every day![2]

It is truly ironic that the root cause of spam is its extremely low cost for the perpetrators. Using a single ISP account with a monthly charge of $20 or less, a spammer can send out millions of messages each month even using a slow 56Kbps modem. An estimate of a penny for 10,000 messages is probably "in the ballpark" as far as the cost to blanket-mail spam.

The conclusion: spam continues to grow unabated and any organization incurs substantial losses in productivity and other valuable IT resources. It is like a worsening fever that prevents your company from attaining peak performance and the negative results will show in the bottom line.

This whitepaper describes the anti-spam and email content filtering technology behind Praetor®, our product introduced in 1999, during the early stages of the war against spam. It also describes the various facilities provided for administrators and users to access quarantined messages and generate useful traffic reports.

[1] Add salary, benefits, taxes, and the pro-rata share of general overhead expenses.

[2] Try the spam calculator at the CMS website using your own figures and see how much spam costs your company.

PRAETOR ANTI-SPAM COUNTERMEASURES

In accordance with the best security practices recommended by experts, Praetor implements many different anti-spam countermeasures. They are all built on an infrastructure that maximizes flexibility by allowing customization to use Praetor's filtering capabilities in ways that go beyond combating the spam.

The anti-spam countermeasures include:

- Bayesian statistical analysis that scores the message based on its content
- Heuristic analysis that scores the message based on spammer tricks found
- Ability to query multiple actively maintained DNS-based blacklists on the Internet
- Defense against the Reverse NDR vulnerability found in mail servers such as Lotus Domino, Microsoft Exchange, Novell GroupWise, etc.
- Pre-configured weighted word lists that score the message body
- Several whitelists for sender addresses, domains, listservers
- Default rules to check content for individual spammer tricks, profanity, etc.

These are summarized in the sections below.

Bayesian statistical analysis

This advanced antispam technique uses a database of words and numbers called "tokens" to rate the likelihood of a message is spam. Each received message is broken into its many tokens that is given a probability of being spam according to the token database. An overall probability is then computed, combining the individual probabilities of each token.

Praetor is installed with a default pre-configured database that is trained from several thousand actual email samples, approximately 80-85% of it being spam. This default database eliminates the need for any lengthy initial Bayesian filter training or daily updates. Immediately upon installation, Praetor efficiently stops over 90% of all spam email messages.

To obtain even greater accuracy, the Bayesian filter can be easily trained by the administrator using sample messages that are incorrectly classified. With such training, it is possible to stop over 95% of all spam with less than 0.01% error in rating good messages as spam (referred to as "false positives").

Heuristic analysis

Spammers use a multitude of common tricks that normal business-related or personal messages would never contain. These tricks are detectable clues to identifying spam email and Praetor employs heuristic analysis to score these spammer tricks from messages that its Bayesian filter classified as "uncertain". A partial list of common tricks in HTML messages include

● Tiny Text	A very small font is chosen in an attempt to hide text and mislead spam filters.
● Invisible Ink	A font color very similar to the background color is chosen to hide text within a message. This is an attempt to confuse spam filters and let the message be delivered to the users' mailbox.
● Obfuscated URLs	Explicit IP addresses and encoded domains are used deliberately to make it difficult for the user to decipher.
● Embedded Comments	Spammers use comments placed within a message's HTML code to confuse Bayesian filters with new words not seen before, or excerpts from news articles.

DNS-based blacklists

Praetor can query the multiple DNS-based blacklist servers (DNSBLs) on the Internet that are actively maintained with IP addresses of spammers. When compared to other products, CMS enhanced the use of DNSBLs in the following ways:

- Perform the query in parallel, waiting for the first response that indicates the IP address is found in the blacklist.
- Query at the message level instead of the SMTP protocol level, which is vulnerable to a possible denial-of-service attack.
- Correctly perform the query even when Praetor is not the first mail server in the network to receive the message from the outside.
- Record more information than just the IP address of the offending spam server, such as the addresses of the sender, recipient, and the subject.

Defense Against “Reverse NDR” Vulnerability

Reverse NDR (RNDR) is an insidious attack that subverts the compliance of all mail servers to Internet standards and makes them into unwitting indirect mail relays. By sending messages to fictitious addresses at unprotected domains, the receiving mail server tries to return a non-delivery report to the original sender usually accompanied with the original spam message. Of course, the spammer has forged the sender address for the intended spam victim.

Since first announced publicly by CMS in June 2003, Praetor has provided a successful and proper defense against this attack. Other products such as Microsoft Exchange Server 2003 claim to address this vulnerability but their implementation is partial or incorrect. With a partial RNDR defense, spammers can still succeed in this attack. An incorrect implementation creates vulnerability to the dreaded "Directory Harvest" attack from which there is no defense once your user email addresses have been harvested.

Additionally Praetor includes a traffic report that specifically monitors Reverse NDR attempts. Using this report, the IP source can be identified and added to the local blacklist.

Weighted Word Lists

Praetor includes three pre-configured weighted word lists containing key phrases and their associated points for scoring. If the total points for phrases found in the message body exceed a threshold value, that message would be rated as undesirable.

The pre-configured lists are in the areas of:

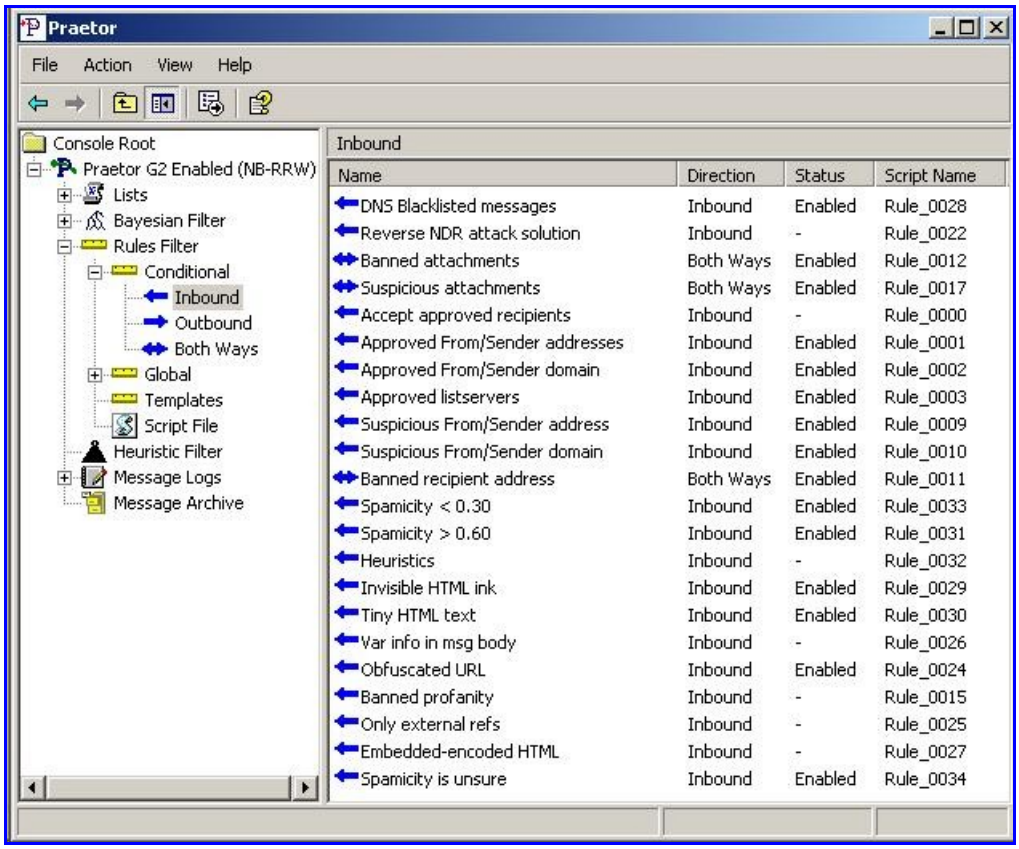
- Drug solicitations
- Advanced fee fraud, e.g. Nigerian 419 solicitations
- Sexual terms used in pornographic offers

Whitelists

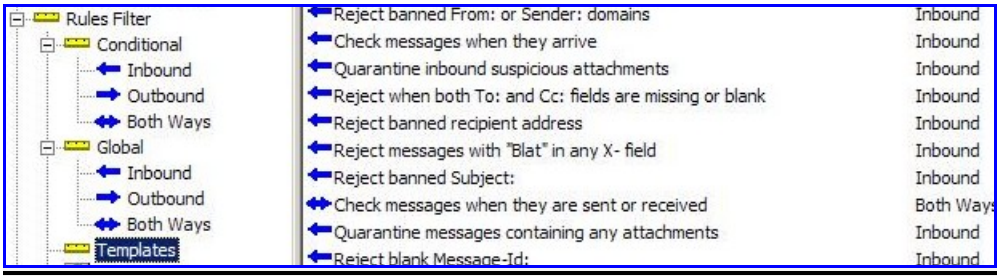
At the administrators’ discretion, whitelists can be used for sender addresses, sender domains, list server addresses, etc. These lists will be used to approve messages after they have been checked for disallowed or suspicious attachments. This check is an omission in many competing products, exposing vulnerability in light of today’s viral infections that forged the sender addresses taken from the local address book as it tries to propagate itself.

Default Rules

As mentioned earlier, Praetor's multiple antispam countermeasures are all implemented through its flexible infrastructure. Over a dozen rules are provided as default antispam and antivirus rules as shown below.



There are even more rules available as templates that you can quickly modify to suit your needs by changing and adding conditions, optional actions, and exceptions.



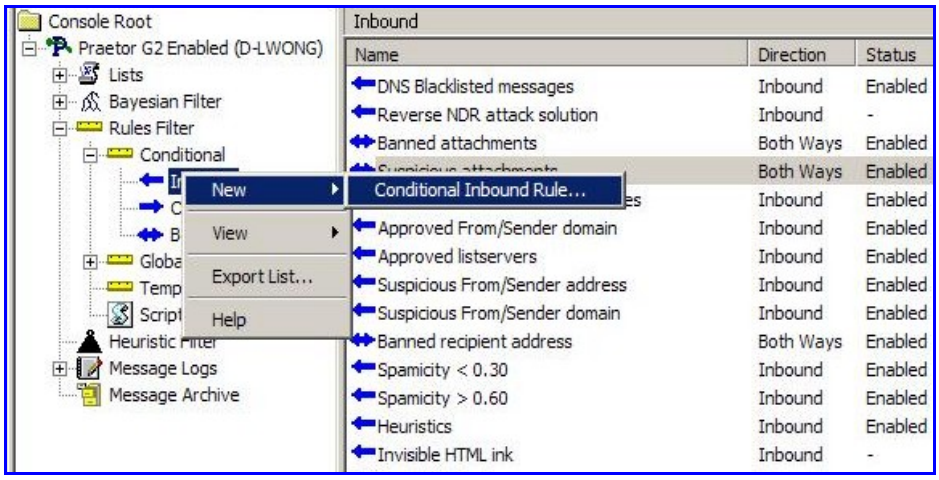
RULE WIZARD

One of the basic truths of messaging is that no two sites are completely identical, despite whatever surface similarities might exist. Business models, corporate policies, user populations, industry, and IT management all contribute endless variations to the overall operation of any messaging system. As a result, objectionable email for one company may not be considered as such for another. Thus, to make any email content filtering product truly useful, it must have the ease and flexibility to accommodate such variances.

Praetor has a built-in Rule Wizard similar to the one found in Microsoft Outlook. This facility allows the administrator to create custom filtering rules that reflect actual experiences to protect the site. Your custom rules augment the anti-spam countermeasures in Praetor and can further extend the product to filter your email for non-spam issues, e.g. add custom disclaimers, scan for leaks of trade secrets, etc.

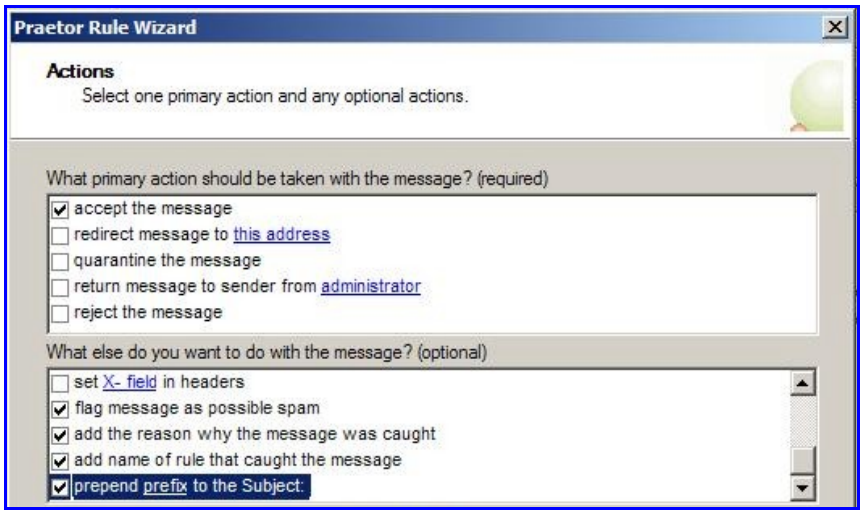
Here are the simple steps to create a rule in Praetor.

1. Select the message direction when creating a new rule.

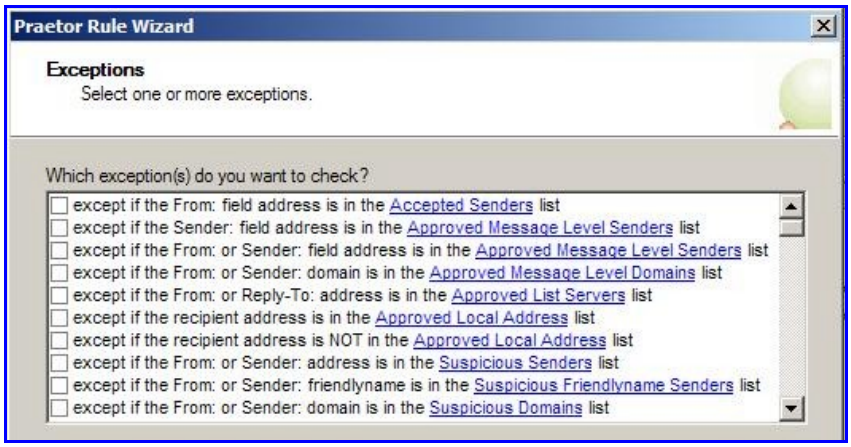


2. Select the conditions.

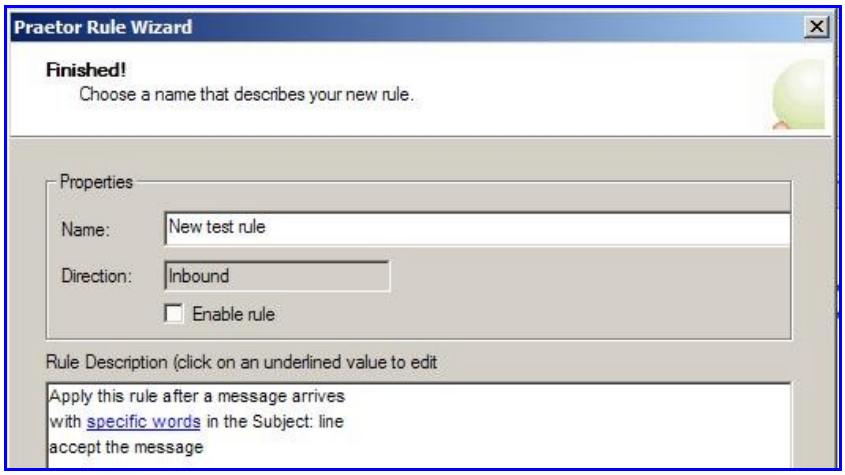
3. Select the actions to take when the conditions are present.



4. Select any exceptions.



5. Name the rule and make it active.

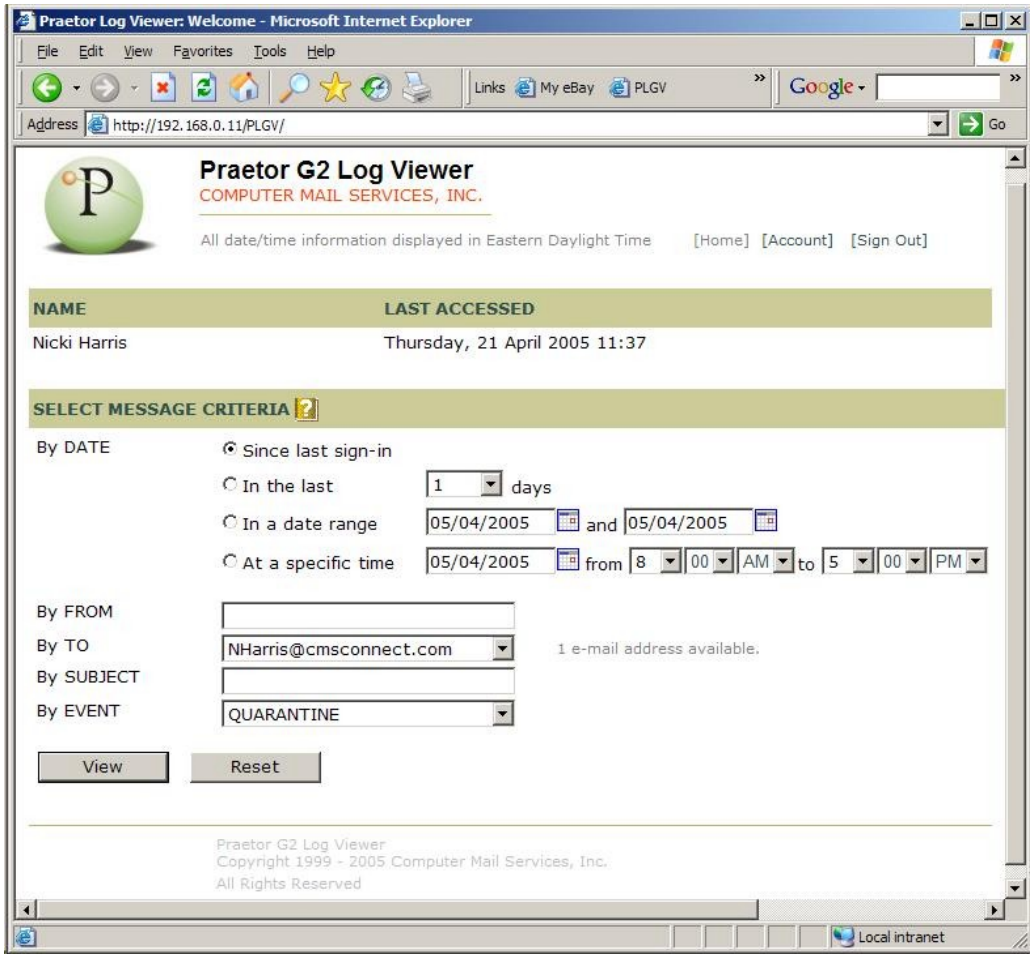


EMPOWER USERS TO RELEASE QUARANTINED MESSAGES

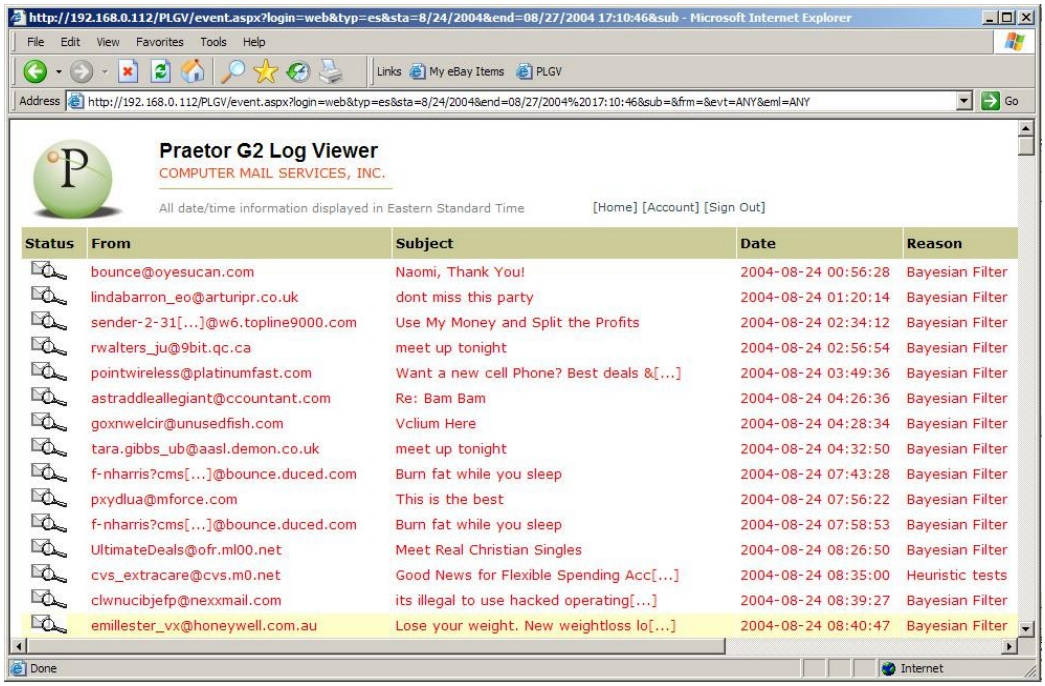
So, now that Praetor's multi-layer antispam technologies and your supplemental rules have quarantined messages without letting them pass onto and clog your mail server, how do the users deal with them?

Praetor's answer is the web-browser access tool called the "**P**ersonal **L**o**G** **V**iewer" (PLGV). This facility may be optionally enabled to give access to the recipients' quarantined all or some users at the site. Authentication of each user is performed automatically via LDAP or a user table that can be configured to let department managers review and control message disposition over their subordinates.

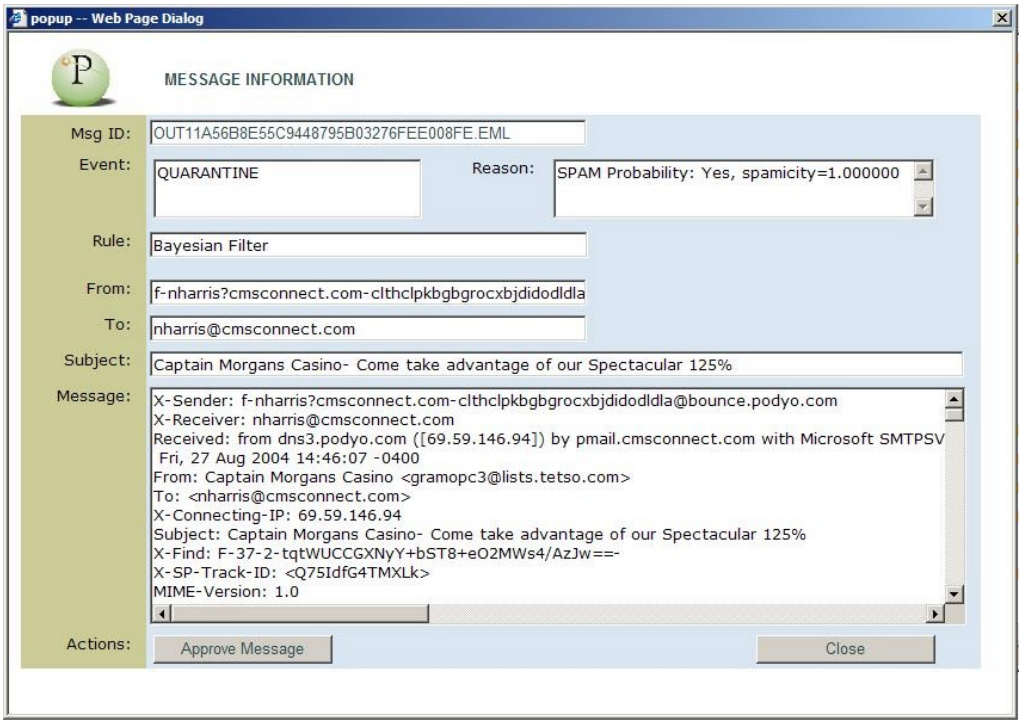
After logging into the local PLGV website various message selection criteria are available in the main webpage that is presented.



Once the criteria are selected pressing the 'View' button will display a list of the messages.

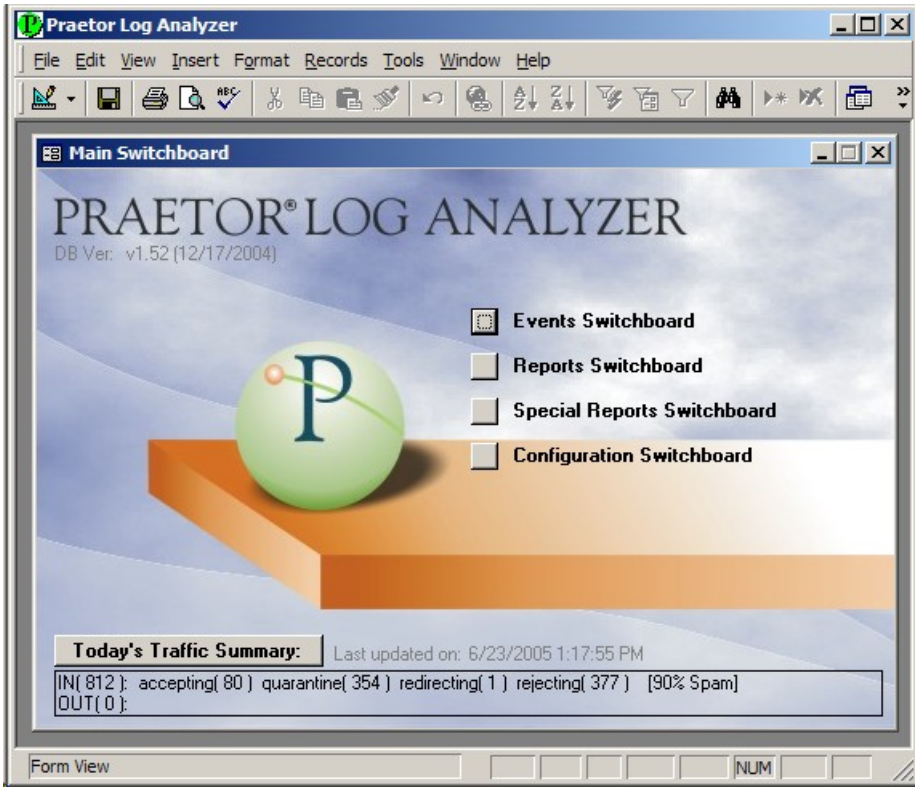


From this list full message details can be safely viewed by double-clicking on the line in red, and the message may be approved to release it for delivery to the email client software.



TRAFFIC REPORTS

Praetor includes several useful administrative traffic reports using the Log Analyzer application. From the main screen it will display a summary of the current day's traffic activity and estimate the percentage of spam received.



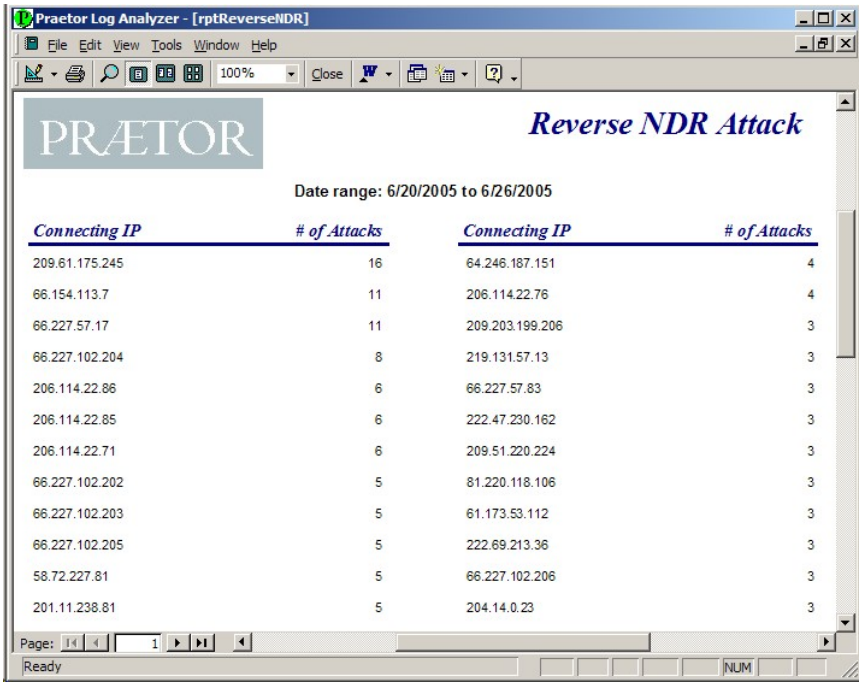
Several reports are available to show:

- Message count summary for those rejected, quarantined, accepted, re-directed, or returned to the sender.
- Sender domain report for email received from the Internet.
- Destination domain report for email sent to the Internet.
- Recipient address report for email delivered locally.
- Destination address report for email delivered to the Internet.
- Rule report showing the number of messages that were filtered or accepted.
- IP addresses of the most frequent sources of Reverse NDR attacks.
- Traffic summary grouped by rules.

The last two reports are extremely useful to show the sources of Reverse NDR attacks and rules that are overly sensitive that cause false positives. Samples are shown below.

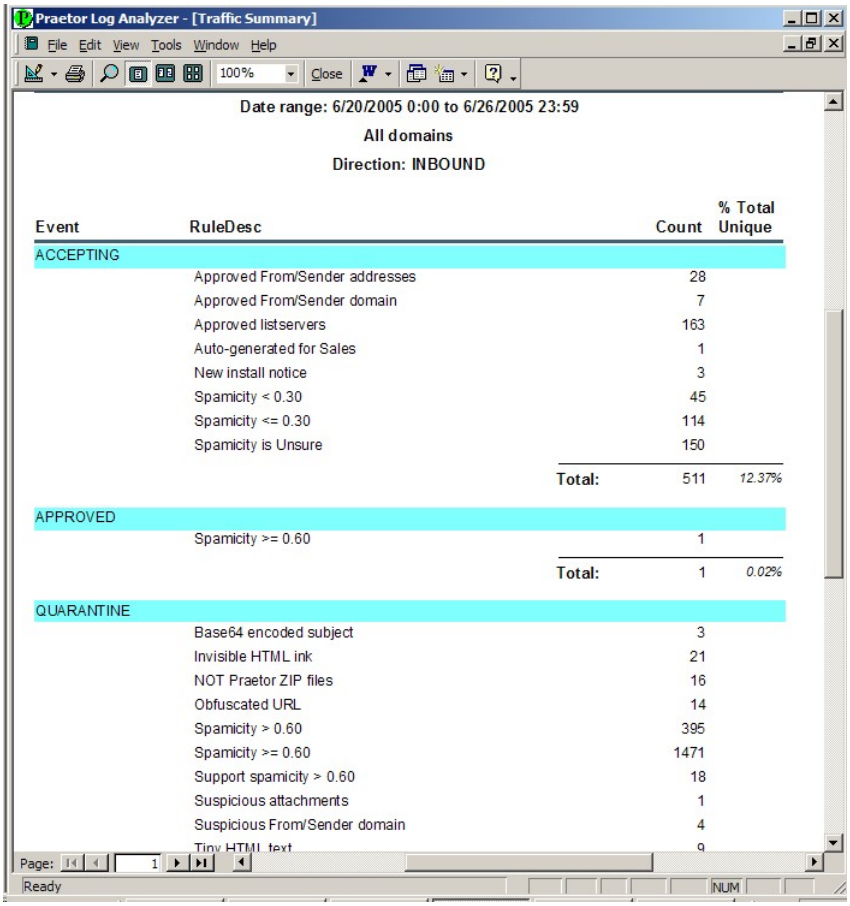
Using these reports, the administrator can add the IP addresses of attacking spammers into the blacklist and adjust the rules or train the Bayesian filter to lower the number of false positive incidents while raising the accuracy.

Source of Reverse NDR Attacks



Connecting IP	# of Attacks	Connecting IP	# of Attacks
209.61.175.245	16	64.246.187.151	4
66.154.113.7	11	206.114.22.76	4
66.227.57.17	11	209.203.199.206	3
66.227.102.204	8	219.131.57.13	3
206.114.22.86	6	66.227.57.83	3
206.114.22.85	6	222.47.230.162	3
206.114.22.71	6	209.51.220.224	3
66.227.102.202	5	81.220.118.106	3
66.227.102.203	5	61.173.53.112	3
66.227.102.205	5	222.69.213.36	3
58.72.227.81	5	66.227.102.206	3
201.11.238.81	5	204.14.0.23	3

Traffic Summary by Rule



Event	RuleDesc	Count	% Total Unique
ACCEPTING			
	Approved From/Sender addresses	28	
	Approved From/Sender domain	7	
	Approved listservers	163	
	Auto-generated for Sales	1	
	New install notice	3	
	Spamicity < 0.30	45	
	Spamicity <= 0.30	114	
	Spamicity is Unsure	150	
	Total:	511	*12.37%*
APPROVED			
	Spamicity >= 0.60	1	
	Total:	1	*0.02%*
QUARANTINE			
	Base64 encoded subject	3	
	Invisible HTML ink	21	
	NOT Praetor ZIP files	16	
	Obfuscated URL	14	
	Spamicity > 0.60	395	
	Spamicity >= 0.60	1471	
	Support spamicity > 0.60	18	
	Suspicious attachments	1	
	Suspicious From/Sender domain	4	
	Tiny HTML text	9	

CONCLUSION

The Internet has been both a blessing and a curse. The benefits of connectivity are numerous but there is a broad palette of security loopholes that can be used by others to serve their own agenda. Unfortunately, these loopholes often give way to precarious viruses, hacker attempts to intrude and gain access to company confidential information, and spam mail. All these can easily bog down your email system infrastructure, negating much of the benefits gained from such an essential business tool as email.

Even more damaging is the way in which modern mail servers can be manipulated by spammers to relay their spam, perhaps even damaging your company's name. Companies who have closed their mail servers to a direct relay assault only to see their effort nullified by an indirect form of relaying we call the "Reverse NDR Attack". The end result is the same – a legitimate mail host is added onto several Internet blacklists. This not only disrupts normal mail flow but also taints the victim's business image and professional reputation. Clearly the burden of hijacked server resources only adds to the myriad of spam-related troubles.

Praetor is the culmination of substantial analysis, technique observation, and dedicated study. Its multi-layered defenses significantly reduce the spam deluge. With the spam problem solved, Praetor's flexibility as an email content filter can also serve to detect unauthorized leaks of confidential information and unprofessional conduct in your communications. More importantly, it has been completely effective at implementing your company policy with regards to email attachments to eliminate the threat of unknown viruses, even without the need for virus pattern file updates.

We feel it's the very best messaging firewall on the planet. Download the free 21-day evaluation from our website and try it for yourself. We think you'll feel the same way.

LINKS TO PRAETOR

- Product information: **http://www.cmsconnect.com/Praetor/prMain.htm**
- 21-day free evaluation: **http://www.cmsconnect.com/Downloads.htm**
- Online price quote: **http://www.cmsconnect.com/Sales/prPrice.htm**