

# NETWORK RESOURCE THEFT PREVENTION Destroying the Economics of Spam

A SpamSquelcher™ White Paper

by

ePrivacy Group

December, 2003

How true network perimeter anti-spam protection prevents spammers from stealing your resources, while improving the delivery of legitimate email.

Authors:

David Brussin, CISSP; Stephen Cobb, CISSP;  
Ray Everett-Church, Esq.; Vincent J. Schiavone

## Network Resource Theft Prevention: Destroying the Economics of Spam

The people whose email inboxes overflow with unwanted commercial email (UCE) are only the most visible victims of the Internet scourge that most people refer to as spam.<sup>1</sup> While the adverse impact of spam on consumers and corporate email users is immense, and widely reported, the final recipients of spam messages are by no means the only ones paying the price for this widespread abuse of network resources. The networks that deliver email carry virtually the entire financial burden of spam messages and these include enterprise networks, government and public agency networks, as well as Internet Service Providers. Indeed, now that unwanted and frequently offensive email constitutes, by most accounts, more than half of all email, it is reasonable to refer to the act of spamming as the deliberate theft of network resources. These stolen resources include bandwidth, server capacity, software licenses, administrative time, network infrastructure, and storage.

Ironically, many attempts to address the end-user impact of spam actually contribute to an increase in the theft of network resources. Most anti-spam solutions are based on filtering technologies that accept all messages and then analyze them one-by-one in order to decide what to do with them. These filters divert a certain percentage of spam messages before they reach the inbox of the intended recipient, but the spammers' response to this technology is to

We have yet to see any anti-spam filter attain 99.9 percent accuracy in the field, but if one did, it would actually deliver, as legitimate email, 1,000 spam messages for each 1 million sent to the network. Spammers know and exploit this. Since we have observed 3 million emails sent to a network of only 3,600 mailboxes in a single day, consider what this means:

Even if that network was protected by a filter which achieved 90% accuracy, 80 spam messages would still be delivered to each mailbox that day as legitimate messages (and as many as 700 additional spam messages per user might be quarantined pending user review).

send even more messages, knowing that some will get through (even the best message-by-message filters are not 100 percent accurate). The resulting increases in the volume of spam simply consume, or steal, more and more resources on the networks that are deploying these filters. This effect is a direct and predictable consequence of the spammers' business model, which is fundamentally parasitic. Fortunately, analysis of this model reveals a very effective and efficient anti-spam technology that actually discourages, rather than encourages, an increase in spam.

---

<sup>1</sup> Note that SPAM is a trademark of Hormel Foods.

## The Parasitic Economics of Spam

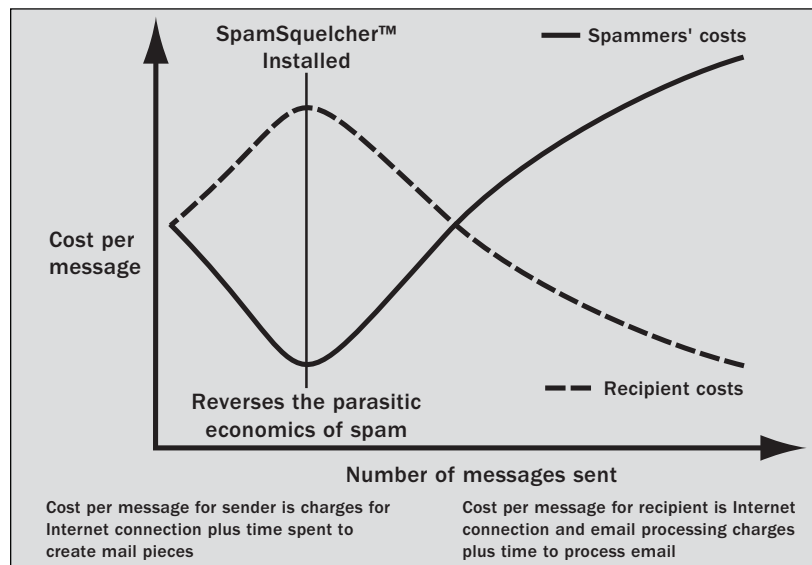
The economics of spam are correctly referred to as parasitic because the cost to spammers of sending email is low to begin with, and decreases asymptotically to an extremely small cost per message as volume increases. The cost to ISPs and enterprises of receiving email, however, is initially much higher and increases nearly linearly as total email volume (both legitimate and spam) increases. Given this situation, the economic motive of the spammer will not be eliminated until the spammer's costs are increased dramatically.

The economic motive of the spammer can be expressed as: Increase spam volume until:

$$\frac{(\text{volume} * \text{response rate} * \text{profit})}{\text{time}} > \frac{(\text{volume} * \text{costs per message})}{\text{time}}$$

Various measures to eliminate the economic motive of spam have been suggested. These include proposals to impose taxes on email or require some form of postage for commercial email. There have even been suggestions that commercial emailers should post bonds and accept fines if they are found guilty of spamming (it is not clear how such schemes could be imposed on spammers, most of whom already break a variety of laws). The reality is that the rate at which spam volume has increased, month-on-month, over the last twelve months, has remained above 10 percent (as high as 33 percent by some accounts), despite new anti-spam laws and numerous high profile prosecutions of spammers that have resulted in fines and indictments.

All proposals to 'make spammers pay' do have one thing right: the idea that spammers, unlike other Internet low-life, such as criminal hackers and virus writers, are profit-driven. Unfortunately, this means that the cost of spam to ISPs and enterprises will continue to rise until some way is found to break the linear relationship between spam volume and the cost of receiving email. Fortunately, that relationship can be broken, by slowing down the rate at which spam is delivered. This is the theory behind SpamSquelcher, a patent-pending technology that manipulates the most sensitive component of the spammers' business model: time.



## From Economics to Technology

The truism that “time costs money” is nowhere truer than in the economic underworld of spamming. Examine a bucket of two-week old spam and you will find that most of the links within the messages are dead. Spammers play a constant shell game, sending as many messages as they can, as quickly as they can, before being forced to move on (the force coming mainly from blacklisting of sending IP addresses, reporting and closing of open relays, and account termination by ISPs on the grounds of abuse). While some spammers are not above stealing bandwidth, serious spammers send so many messages that they now use OC3 and OC12 connections that are not available unless you make prompt payments of considerable sums of money.

Bandwidth costs are priced, and justified, by message flows over time. Because spammers pay these costs with funds generated by response rates measured in revenues over time, they cannot afford to waste time on targets that receive messages at a slow rate.

Many press accounts of the spam phenomenon highlight the low response rates at which spammers claim to make money, such as 10 responses for every 1 million messages sent. Less often noted is the fact that this low rate must be achieved within a short period of time. In other words, millions of messages must be sent per day, or even per hour, so that enough of them get delivered to generate a sufficient number of responses, defined as enough responses to make cover expenses and create a profit, before the links are broken.

By analyzing the economic realities of spam and then manipulating them using the network architecture and security expertise of its founders, ePrivacy Group was able to create a revolutionary new technology, called SpamSquelcher, that accomplishes all of the following design objectives:

1. Break the linear relationship between spam volume and the cost of receiving email.
2. Reverse the parasitic model upon which spammers depend.
3. Prevent the theft of network resources.
4. Improve the ability of email systems to meet their original design objective: delivering the email that users want, and need, to receive.

SpamSquelcher technology returns control of email to enterprises and ISPs. Alone among anti-spam solutions, SpamSquelcher enables costs—for support, servers, and bandwidth—to scale with the volume of legitimate email, rather than with the increasingly spam-heavy total volume of messages.

## The SpamSquelcher Difference

These economic effects, and the benefits they create when protecting your organization's network, are unique to the SpamSquelcher approach to fighting spam. Unlike spam filters, SpamSquelcher keeps most spam from being sent to your network and discourages, rather than encourages, the sending of spam to your network. Furthermore, SpamSquelcher does this without any outsourcing of your organization's email functionality (given the highly sensitive nature of enterprise email today, outsourcing of this critical function to another company is rarely advisable).

### Unique Benefits of SpamSquelcher

#### For the Enterprise:

- Reduces direct costs for servers, infrastructure, support, and bandwidth.
- Reduces indirect cost of lost productivity from receipt and review of spam by employees, without false positive issues.
- Reduces storage costs for mandated archiving of email.
- Reduces liability from inappropriate content in email processed by the company.

#### For Internet Service Providers:

- Reduces direct costs for servers, infrastructure, support, and bandwidth.
- Improves quality of service and speeds the delivery of legitimate email, without false positive issues.
- Provides a positive 'discriminator' when competing with other ISPs.
- Reduces the cost of customer 'churn' due to spam complaints.

Because the economics of spam are reversed by SpamSquelcher, the networks that it protects benefit not just from less spam, but from fewer spam attacks. Such attacks can overwhelm filter-based anti-spam systems and seriously threaten network availability. SpamSquelcher can maintain quality of service for legitimate email, without false positives, even if the protected network is subject to dictionary harvest attacks or email denial of service attacks.

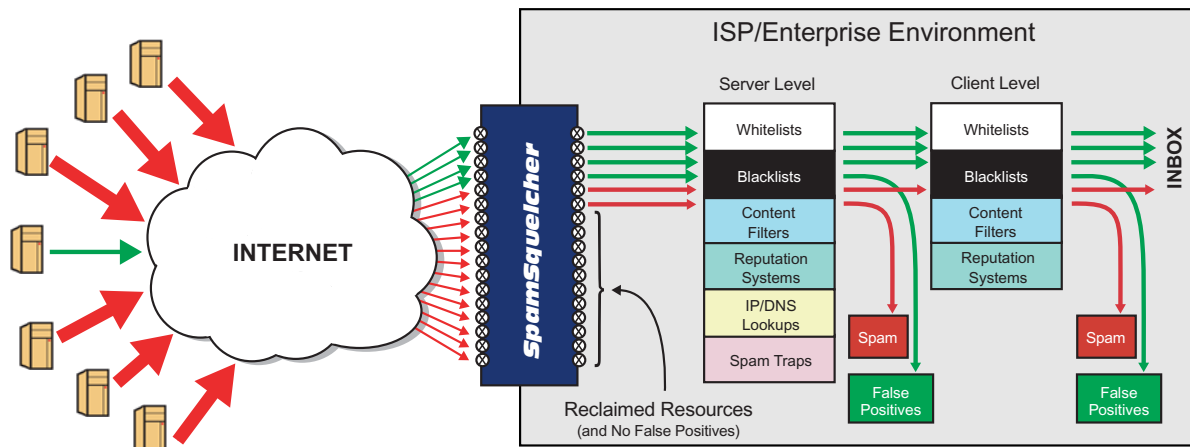
Not only does the SpamSquelcher approach to fighting spam spare your network's resources, SpamSquelcher itself is also an economic user of resources. Even a basic SpamSquelcher implementation can maintain the efficient delivery of legitimate email while at the same time squelching millions of spam messages per day.

As an example, a SpamSquelcher appliance currently protecting a network of 30,000 email users typically operates at 3% to 5% of its CPU capacity. Contrast that with the CPU load on the

multiple spam filtering servers that previously served as this same network's first line of defense against spam: that load frequently exceeded 90 percent. Not only does low CPU load bode well for reliability, but also for scalability. Unlike most other anti-spam solutions, SpamSquelcher, which operates at wire speed, has no upper limit in terms of number of supported users.

## The SpamSquelcher Approach

SpamSquelcher is an intelligent, adaptive network traffic analyzer and TCP/IP traffic-shaper which controls the use of resources by spam through dynamic shaping of incoming traffic. Placed at the edge of an enterprise or ISP network, between the Internet and the existing email

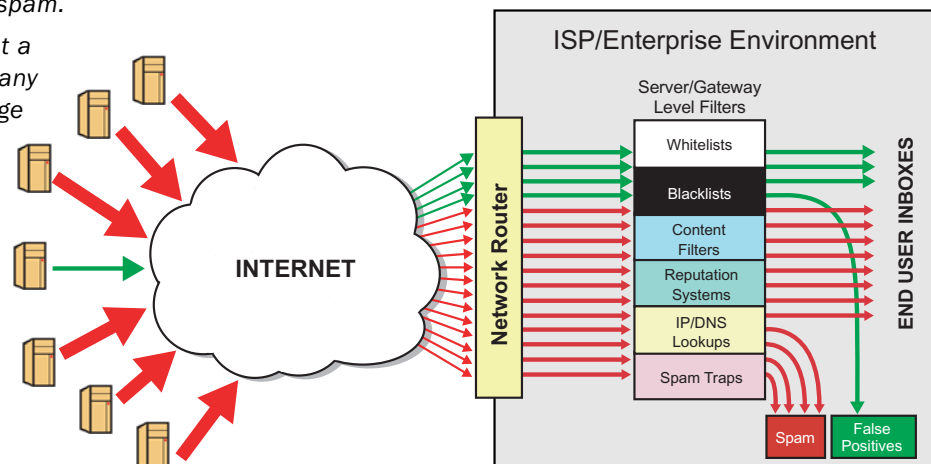


### SpamSquelcher (above) compared with other approaches to fighting spam (below)

Other approaches are resource-intensive, devoting a large percentage of the 'protected' network's total capacity to accepting and processing spam.

Researchers estimate that a typical 10,000-user company running Microsoft Exchange 2000 now deploys 21 messaging servers, 5 of which just process spam. Without the deployment of new technology, such as SpamSquelcher, this could mushroom to 50 servers within 3 years, a full 50% of which are used for processing spam.

ResearchandMarkets.com



processing infrastructure, SpamSquelcher provides quality of service shaping for legitimate email traffic, while preventing spam traffic from stealing network bandwidth, server, and support resources.

The design of SpamSquelcher is such that it does not block or delete any messages, so it has a 'zero false positive' impact on legitimate traffic. At the same time, SpamSquelcher is highly complementary to traditional spam filtering, as well as other filtering-based network defenses, such as malicious mobile code scanning and content filtering. SpamSquelcher customers report that overall mail volumes drop by as much as 80 percent when squelching is activated, so post-squelching filtering of email becomes more effective while using less resources.

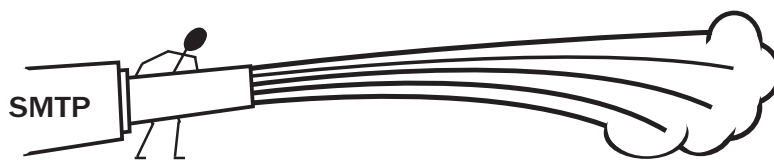
Indeed, one reason that anti-spam filters fail to achieve their published success rates when deployed in the field is that throughput of message-by-message filtering at maximum effectiveness is too slow for production environments when applied to the total inbound traffic stream, resulting in delays to legitimate email. This problem disappears when SpamSquelcher, deployed as the first line of defense, reduces the total inbound email volume to a manageable level.

## True Perimeter Protection

SpamSquelcher acts as a network gateway between the Internet and the existing SMTP infrastructure of the protected organization. Similar, in terms of implementation architecture, to a network load-balancing device, SpamSquelcher is transparent to other gateways, firewalls, intrusion detection systems, and load balancers that might currently be in place.

Instead of trying to control email traffic using SMTP, which is essentially a sender-controlled protocol, SpamSquelcher uses TCP/IP, a receiver-controlled protocol, to restrict traffic on network paths that are trying to deliver spam.

Note that the SpamSquelcher architecture is quite different from that used by some other anti-spam products that also refer to themselves as gateways. SpamSquelcher is a true perimeter gateway—not a potential processing bottleneck—and imposes no delays on legitimate email traffic, maintaining spam protection well upstream from the MTA (for networks that use blacklists and whitelists, SpamSquelcher can handle these, moving them away from the MTA for greater efficiency and ease of maintenance).



The SMTP protocol is controlled by the sender, like a fire hose.



TCP/IP is receiver controlled, like a bucket brigade. The size of the buckets and the rate at which they are transferred can be varied by the receiver.

## How SpamSquelcher Works

As SpamSquelcher analyzes network connection requests and samples SMTP traffic within the connecting paths, it dynamically shapes the network traffic flow, according legitimate traffic priority, while throttling back spam connections. This means very little spam intended for the protected network ever crosses the network threshold, while a good deal of it backs up into the spammer's server, frequently causing the spammer's software to drop the connection and move on to a more promising target network.

SpamSquelcher is capable of immediately detecting spam attacks within the network traffic, using a combination of established and proprietary analyses. Network traffic is dynamically shaped based on these analyses in order to prevent spammers from abusing the receivers' resources. Since the outcome of an individual sample analysis does not result in blocking or deletion of a specific email message, there is no 'false positive' risk. Furthermore, because traffic-shaping decisions are based on the analysis of a sample of the traffic, rather than a single message, the results are extremely reliable.

The spam analysis performed by SpamSquelcher includes established techniques, such as Bayesian header and content analysis, but also incorporates various other characteristics (some of which are proprietary). SpamSquelcher's modular design, which facilitates live updates, also enables incorporation of custom analysis modules should customers wish to include them in the spam analysis.

Nucleus Research estimates spam's annual cost to enterprises at \$875 per employee. A law firm with 500 employees profiled by Network World estimated annual spam costs at:

- Lost productivity \$300,000
- Bandwidth consumption \$17,000
- Storage \$114,000

## The Economic Effects

The direct cost of receiving email, can be expressed in terms of 'messages per second.' This cost includes:

- support (direct support costs, such as help desk personnel payroll, outsourced support resources and vendor support agreements, for all components related to server capacity and bandwidth)
- server capacity (all real-time processing capacity for email receipt and filtering, including hardware, software, network infrastructure, facilities, and utilities) and,
- bandwidth.

Since the 'messages per second' of resources required to keep pace with incoming email volume today is driven by the total volume of incoming email, as well as by the peak rates of all

incoming email, spam is clearly a major component, and in many cases a majority, of these costs. SpamSquelcher provides, for the first time, control of the allocation of recipient ISP and enterprise resources such that the 'messages per second' of resources required must keep pace only with the volume of legitimate email.

At the same time, the cost to send spam to a SpamSquelcher protected network increases as spam delivery is slowed. Indeed, SpamSquelcher customers have observed a decline in overall attempts to spam their network after SpamSquelcher has been installed.

## Summary

The shaping and squelching of incoming email traffic by SpamSquelcher results in several important benefits:

- The cost of receiving email on a SpamSquelcher protected network is immediately reduced. Since the use of resources by spammers is severely limited, the bandwidth, server capacity and support costs for receiving email need scale only with the increase in legitimate email traffic.
- The economics of spamming a SpamSquelcher protected network are reversed. Where an individual spammer might have been able to deliver millions of messages in a few hours, SpamSquelcher ensures that he can deliver at only a minute fraction of that rate. Since spammers' delivery costs now—for the very first time—increase with volume, spammers no longer have a financial model conducive to continued attacks against SpamSquelcher-protected networks. As a result, total cost of ownership for email is reduced and indirect costs, such as archival storage, are brought under control.
- The practicality and efficacy of consumer-focused spam solutions is increased. Many of the most effective existing, and most promising emerging, anti-spam technologies are extremely computationally intensive, meaning they are not practical for deployment as a first line of defense at the ISP or enterprise level. Given SpamSquelcher's perimeter control of resource use, ISPs and enterprises will have more freedom to deploy these tools to improve the consumer and recipient experience.
- Immediate relief from spam is now available, and improves over time. SpamSquelcher is a shipping product that is already deployed successfully at a variety of ISPs and enterprises. SpamSquelcher customers see an immediate reduction in spam volumes and a continuing decline as systems are fine-tuned, either on-site or through remote administration. The SpamSquelcher architecture allows live, remote updating of analysis modules as well as system maintenance, both of which are included in the SpamSquelcher service.

**About ePrivacy Group**

ePrivacy Group develops innovative technology to enhance trust and security in network communications, through patent-pending products such as SpamSquelcher™ and Trusted Sender™, and industry initiatives like the Trusted Email Open Standard. A privately-held company based near Philadelphia, ePrivacy Group was founded by leading experts in privacy, security, and the anti-spam movement.

**Contact Information:**

Paoli Executive II, Suite 300  
43 Leopard Road,  
Paoli, PA 19301  
Phone: +1 (610) 407 0400  
Fax: +1 (610) 407 7085  
[www.eprivacygroup.com](http://www.eprivacygroup.com)  
[info@eprivacygroup.com](mailto:info@eprivacygroup.com)