

The Growing Problem of Outbound Spam

An Osterman Research Survey Report

Published June 2010

SPONSORED BY



Executive Summary

OVERVIEW

Two-thirds of email service providers consider dealing with outbound spam to be an important or extremely important issue for them in 2010. Outbound spam is also a high priority issue for end users: when asked about their preference for email providers that actively ensure that spam is not sent out from their networks, 80% believe that this is important or extremely important. Further, 87% believe it is important or extremely important for email providers to actively eliminate zombies – a primary source of outbound spam – from their networks.

BACKGROUND AND METHODOLOGY

Osterman Research conducted two surveys specifically for this research report. The first was with 100 knowledgeable individuals at Web hosting companies, Internet access service providers, free email service providers and other email providers that deal with the issue of spam on a regular basis. The second survey was conducted with 266 end users who were queried about their use of email and the Internet at home. The goal of both surveys was to quantify the issues surrounding outbound spam and what service providers and end users can do to remediate the problems they experience.

KEY TAKEAWAYS

- Outbound spam is a serious issue and it is getting worse.
- There are a number of sources that can generate outbound spam, including compromised accounts, zombies and malicious users.
- Conventional anti-spam techniques and technologies are not effective in the fight against outbound spam and can result in a very high level of false positives, disgruntled customers, higher costs and lost business.
- Resolving the outbound spam issue can help service providers to retain customers: our research found that 56% of end users whose outbound email was blocked because of their providers' outbound spam problem would probably or definitely switch to a provider that would not block innocent users.

ABOUT THIS RESEARCH REPORT

This report discusses the growing problems associated with outbound spam and the even bigger problems for those service providers that address the problem with inadequate solutions. This document also provides a brief overview of Commtouch's recently introduced outbound spam solution.

Outbound Spam is a Serious Problem

WHAT EXACTLY IS "OUTBOUND SPAM"?

Although first sent as far back as 1978, inbound spam has been a top-of-mind problem for about the past nine years. For example, in 2001, spam represented roughly one in

six email messages sent across the Internet; today, spam represents upwards of 80% of all email. However, this masks the rapidly increasing *absolute* volume of spam, which doubles roughly every 12-18 months.

Although inbound spam is a serious and perennial problem, outbound spam is a more rapidly growing problem, primarily for service providers who act as the unwilling hosts of this content. Outbound spam – that content sent from Web hosting companies, SaaS email providers, Internet access service providers, free email service providers, and onsite email managed service providers – creates enormous problems on a number of levels, as discussed later in this report. For example, more than two in five service providers surveyed for this white paper report that outbound spam is a problem – 15% report that it is a “serious” or “critical” problem. Further, nearly 40% of the service providers we surveyed reported that their IPs have been blocked or blacklisted at some point during just the past 12 months.

THE SOURCE OF THE PROBLEM

There are three primary sources of outbound spam in service provider networks:

- **Zombies**
One of the more common sources of outbound spam is “zombies” that reside on a service provider’s network. A zombie is an individual home- or business-based computer, such as one on an Internet Service Provider’s (ISP’s) network that has been infected by malware specifically designed for control by a remote party. That party can control many thousands of computers for the purpose of sending spam, phishing attempts, malware and other unwanted content. Service providers report that 11.2% of their users’ accounts are currently part of a botnet that is being used for sending out spam—86% of service providers report that they are actively battling zombies in their networks.
- **Compromised accounts**
These are accounts that have in some way been compromised other than by malware, such as through the theft of access credentials, that has enabled spammers to use them to send outbound spam. Service providers reported that 12.6% of their users have had their credentials stolen for the purpose of sending outbound spam.
- **Malicious use of email accounts**
Another source of outbound spam is the creation and use of email accounts by spammers specifically for the purpose of sending unwanted content. The service providers we queried reported that one in eight users’ accounts are openly sending out spam and/or malware.

Spammers of all three types may make efforts to stay “under the radar” by sending hundreds of emails per day or “testing” before sending large volumes.

Clearly, the problem of outbound spam has not been lost on service providers – among those we surveyed, 69% consider dealing with outbound spam to be a priority over the next 12 months.

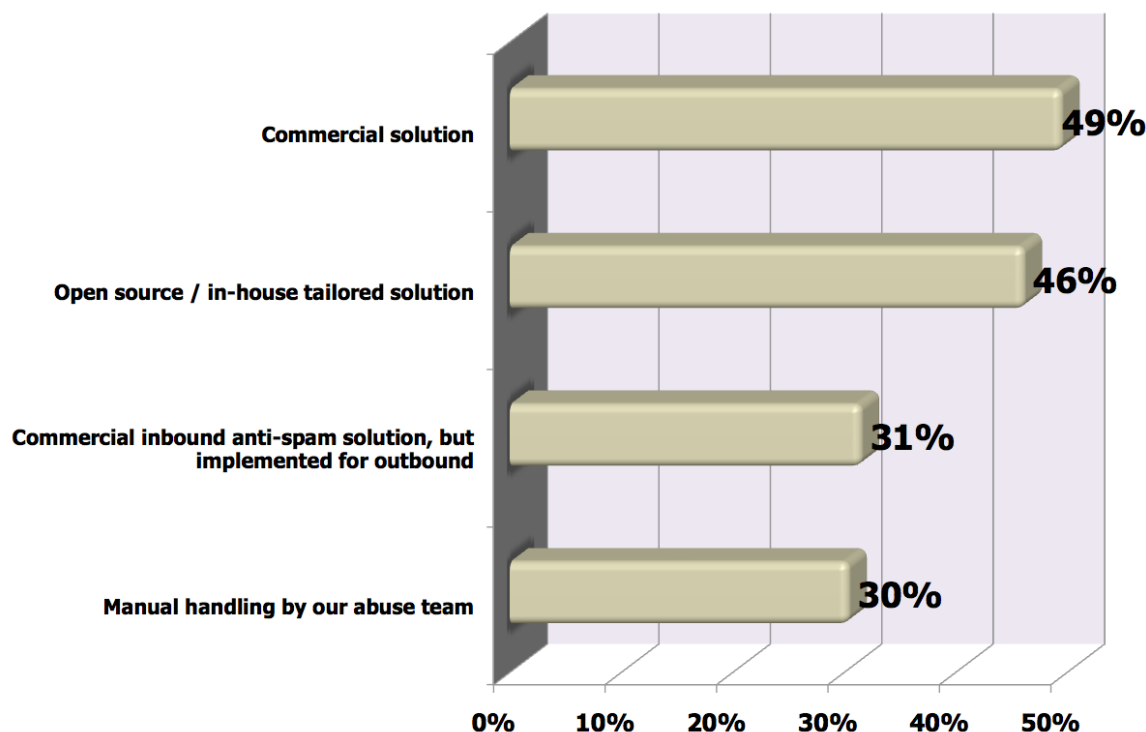
CURRENT SOLUTIONS ARE NOT EFFECTIVE

Many service providers, faced with the growing problem of outbound spam, use a variety of conventional techniques and technologies to address the problem. However, most of these solutions are not satisfactory:

- **Use of standard inbound spam technologies in reverse**
Because many spam detection technologies have a high spam capture rate for content sent *into* a service providers' networks, many assume that simply using these technologies for email sent *out* of the same networks will be effective. Unfortunately, practice has demonstrated that this approach can result in unacceptably high levels of false positives, resulting in a large proportion of valid outbound email being identified as spam and subsequently blocked.
- **Blocking of Port 25 for outbound email**
Blocking Port 25 is unacceptable in many cases because it blocks legitimate email along with outbound spam, again resulting in a very high level of false positives. For example, if a customer of an ISP needs to send legitimate email through a server other than the one provided by their ISP, blocking Port 25 prevents this from happening.
- **Blocking entire ranges of IP addresses**
Some service providers, in an attempt to block outbound spam from a single IP address, will block a range of IP addresses that may be used by the offending sender. This results in email for legitimate senders being blocked.
- **Manual handling by the abuse team**
Our research also found that 30% of service providers use manual methods to address outbound spam, such as deleting accounts that have been compromised. This can be a slow and ineffective method of dealing with the problem given the large number of compromised accounts hosted by many service providers.

Methods Used to Deal With Outbound Spam

(% Responding a Problem or Significant Problem)



The result of these practices is a very high level of false positives, many customer complaints, and unhappy customers and, as a result, a potentially high level of churn. Our research found that 70% of service providers are not completely satisfied with their current solutions and practices designed to thwart outbound spam.

The Consequences of Outbound Spam

THERE ARE MANY CONSEQUENCES OF OUTBOUND SPAM

For service providers who are suffering the effects of outbound spam sent from their networks, there are a variety of negative consequences:

- **Significantly higher costs of providing service**
Outbound spam drives up the cost of providing services to customers in several ways, including an unnecessarily large number of calls to technical support staff to address false positives, switching customers to new IP addresses, and additional IT staff time to identify and resolve outbound spam issues. Nearly one-half of the service provider respondents we queried report that outbound spam driving up the cost of doing business is a problem or a significant problem. Among the service providers we surveyed for this white paper, 68% reported that they spend up to \$100,000 in both direct and indirect costs associated with outbound spam, including things like help desk calls, unblocking IP addresses, etc. – 15% spend in excess of

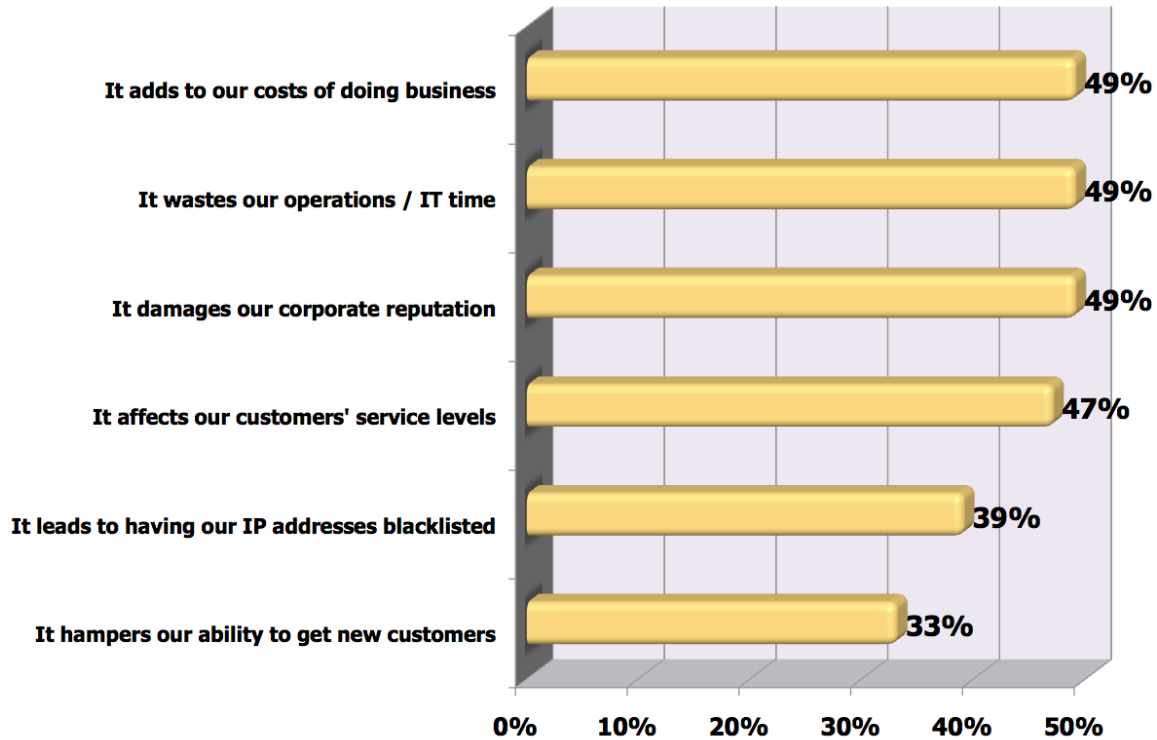
\$100,000 annually on outbound spam-related expenses and 4% report the cost is more than \$250,000 per year.

- **Corporate reputation can be damaged**
A service provider that sends outbound spam can suffer damage to their reputation. For example, being known as a provider that hosts a large number of zombies or one that blocks an unacceptably high proportion of legitimate outbound email is simply not good for business and, ultimately, can put a provider out of business. 49% of the service provider respondents we surveyed report that outbound spam damaging their corporate reputation is a problem or a significant problem.
- **Blacklisted IPs create problems**
When IP addresses get blacklisted, service providers' abuse staff must spend time working with blacklist operators and convince them that they are not spammers, they must deal with dissatisfied customers that may jump to another provider, and spend time resolving problems related to their placement on blacklists.
- **Remediation efforts are poor, resulting in disgruntled customers**
Using remediation efforts like blocking Port 25 or large numbers of IP addresses in an attempt to block outbound spam will irritate many customers and drive them to other providers that use more sophisticated and more granular approaches to solving the problem. In fact, the survey of service providers reported that one-third view outbound spam as a hindrance to their ability to win new customers.

We asked end users what they would do if their current email provider blocked an entire IP address range in an attempt to block outbound spam: 12% of end users responded that, if possible, they would definitely switch to a new provider that blocked only zombies, not innocent users; another 43% indicated they would probably switch to a new provider.

- **Increases the amount of network traffic**
Outbound spam also increases the overall amount of network traffic that a service provider must support. This can force providers unnecessarily to add more capacity over time, driving up their cost of doing business.

Problems Associated with Outbound Spam
(% Responding a Problem or Significant Problem)

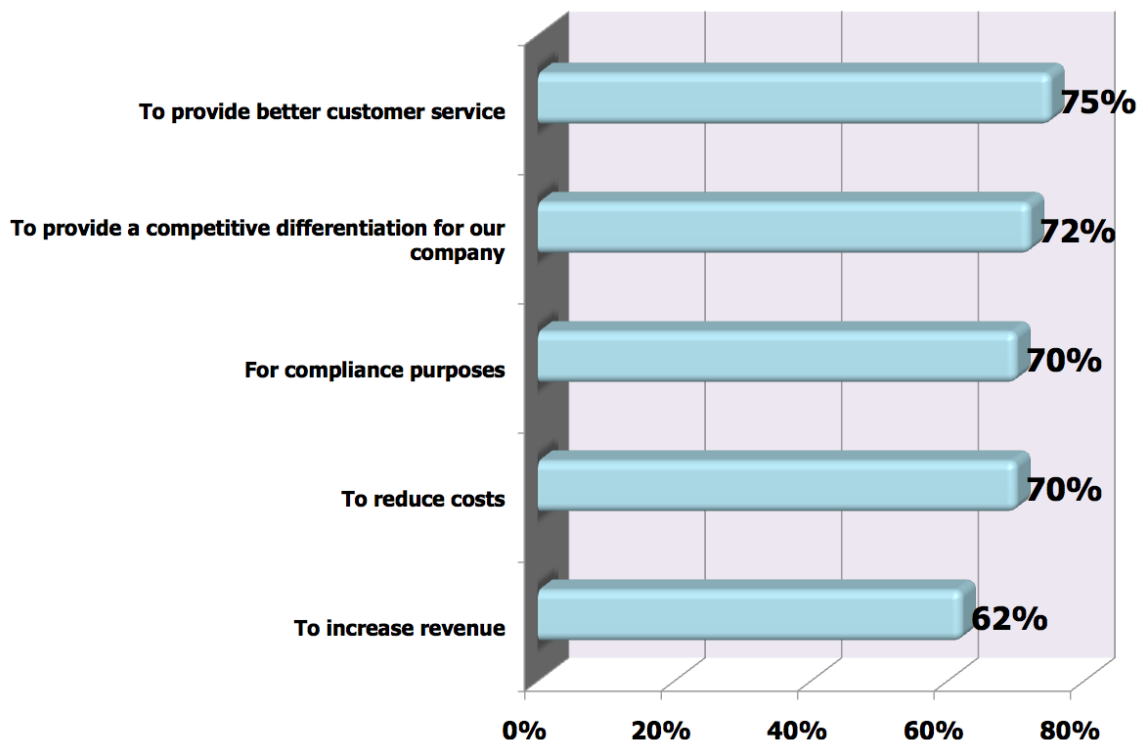


THE BENEFITS OF DEALING EFFECTIVELY WITH OUTBOUND SPAM

Simply put, the benefits of dealing effectively with the problem of outbound spam are just the opposite of the problems discussed above: the costs associated with supporting customers are reduced, less effort is required to manage a given number of users, corporate reputation is maintained because spammers are blocked in a granular fashion with low false positives, customers are happier and network traffic is minimized.

However, our research found that among the service providers that have not yet implemented an outbound spam solution, more than one-half either do not have the resources to implement a solution or they have not found a solution to deal with the problem effectively. That said, 75% of service providers believe an important or extremely important reason to deploy an outbound spam solution is to provide better customer service – 72% believe it would provide a competitive differentiation for their company.

Reasons to Deploy an Outbound Spam Solution
(% Responding an Important or Extremely Important Reason)



WHAT FEATURES ARE IMPORTANT IN A SOLUTION?

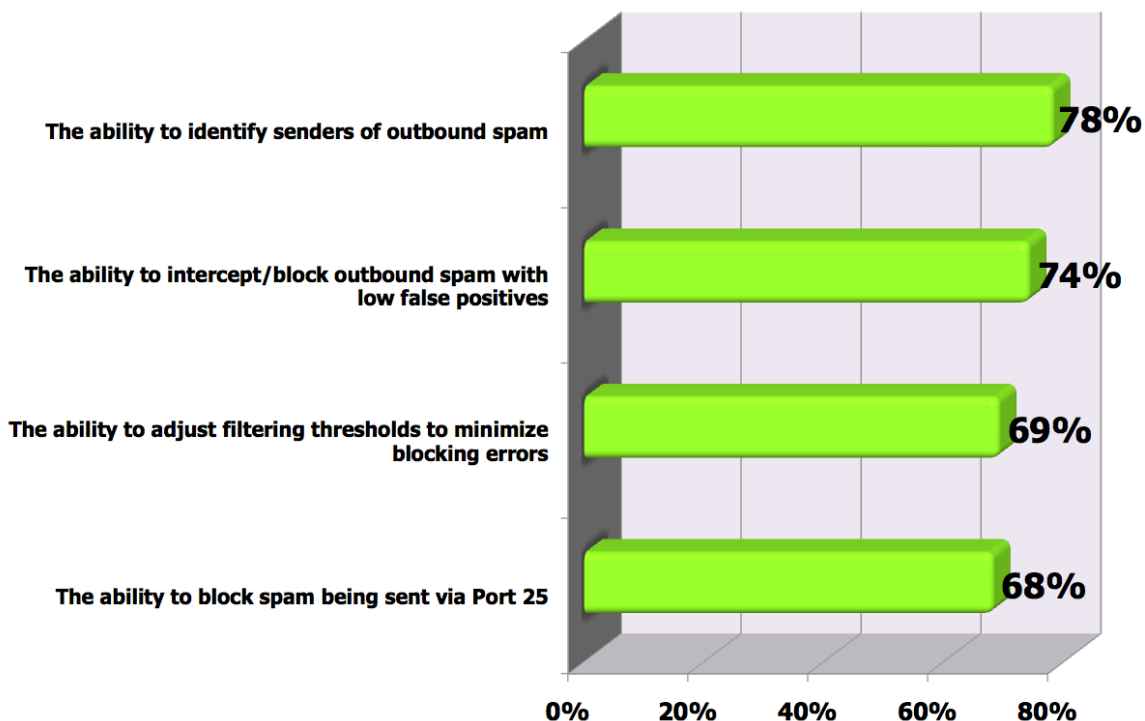
There are a variety of features that any service provider should seek in an outbound spam solution, but three features are critical:

- **Low false positives**
Any outbound spam solution should produce as low a level of false positives as possible. This certainly means false positives well below 1% and as close to zero as practical. Our survey of service providers found that 74% consider low false positives to be an important or extremely important attribute of any outbound spam solution.
- **Identifying senders of spam**
A good outbound spam solution will identify individual senders, not simply block the spam itself or a range of IP addresses from which outbound spam originates. This allows individual offenders to be blocked and/or remediation efforts to be directed in a highly granular fashion. For example, a service provider that can identify individual senders of outbound spam can contact each sender and offer them assistance with malware scanning or some other method of resolving the issue. 78% of the service providers we queried for this research study feel that identifying senders is an important or extremely important attribute of an outbound spam solution.

- **Adjusting filtering thresholds**

A good outbound spam solution will also allow a service provider to adjust filtering thresholds on the fly in response to changing conditions, new zombie outbreaks, recently discovered intelligence on new malware threats, and the like.

Desired Attributes of an Outbound Spam Solution
(% Responding an Important or Extremely Important Attribute)



Summary

Our research supports four basic conclusions:

- Outbound spam is a serious issue today and the problem is getting worse.
- Conventional remediation efforts and technologies focused on outbound spam are not adequate to fully solve the problem.
- New technologies and approaches are necessary to ensure that outbound spam is minimized in service provider networks.
- Many customers will switch to service providers that address the outbound spam problem in a granular way.

Commtouch's Outbound Spam Protection Solution

Commtouch's Outbound Spam Protection solution has been specifically developed to prevent the potential hazards of outbound spam and protect service providers against this rapidly growing threat. Commtouch's solution includes a number of unique properties essential for protecting against outbound spam:

- Real-time classification allowing fast detection and blocking of outbound spam.
- Detection of locally generated outbound spam as well as outbound spam that is part of a global outbreak.
- Identification of spammers, not only the spam, whether they are compromised accounts, zombies, or legitimate accounts used by spammers to send unsolicited mail.

For more information about Commtouch's Outbound Spam Protection solution, visit <http://www.commtouch.com/outbound-spam-protection>.

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.