Report

PUBLISHED BY
THE IRONPORT THREAT OPERATIONS CENTER

IRONPORT

Internet Email Traffic Emergency:

SPAM "BOUNCE" MESSAGES ARE COMPROMISING NETWORKS

OVERVIEW

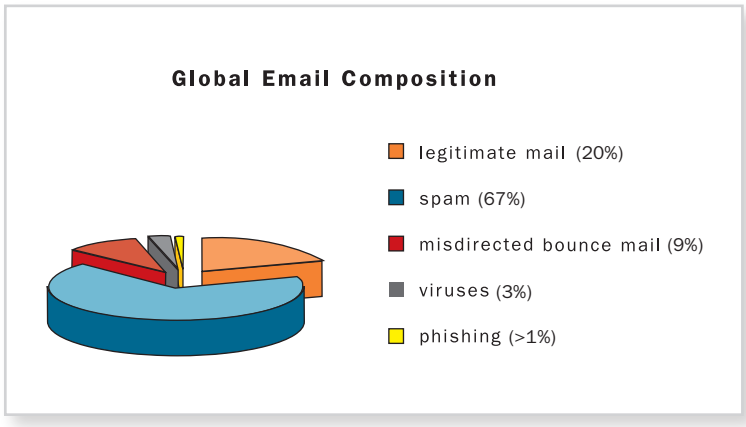
Bounce messages are undeliverable email messages that are returned to their sender. When a receiving mail server gets a message with an undeliverable address, it will generate a new message back to the purported sender—notifying them that "the email you tried to send was undeliverable". This email notification is often referred to as a "bounce" message.

When a spammer is sending out ten million spam messages per day, 20 percent or more will bounce because of invalid addresses. Since the spammers don't want to deal with two million incoming bounce messages, they typically forge the return address and the bounces become "misdirected" or returned to an innocent third party that had nothing to do with the spam in the first place.

The IronPort Threat Operations Center has the ability to measure global email traffic patterns using IronPort's SenderBase® traffic monitoring network. This network samples an astounding 25 percent of the world's email, providing unique insight into trends. SenderBase also has a unique capability to measure the composition of this email. As illustrated in Figure 1, this study shows that in aggregate global email is made up of only 20 percent legitimate messages, spam makes up 67 percent, misdirected bounces make up 9 percent, viruses make up 3 percent and phishing emails make up less than 1 percent.

FIGURE 1.

Spam bounce volume is approaching the same level as legitimate mail volume



The sheer volume of bounce messages generated by spam has grown to the point where it consumes an estimated (US) $5 billion per year in IT resources. This huge expenditure is also growing at the same rate as spam volume, which has historically grown at 100 percent annually— an alarming prospect for the future.

An even more troubling trend has misdirected bounces becoming more than an annoyance. Bounces can actually cause a massive distributed denial of service (DDoS) attack, which can knock even the largest email systems offline for days. IronPort has found that more than 55 percent of Fortune 500 enterprises have experienced a disruption of service or a total denial of service due to misdirected bounces, creating costs that eclipse those quantified in this study.

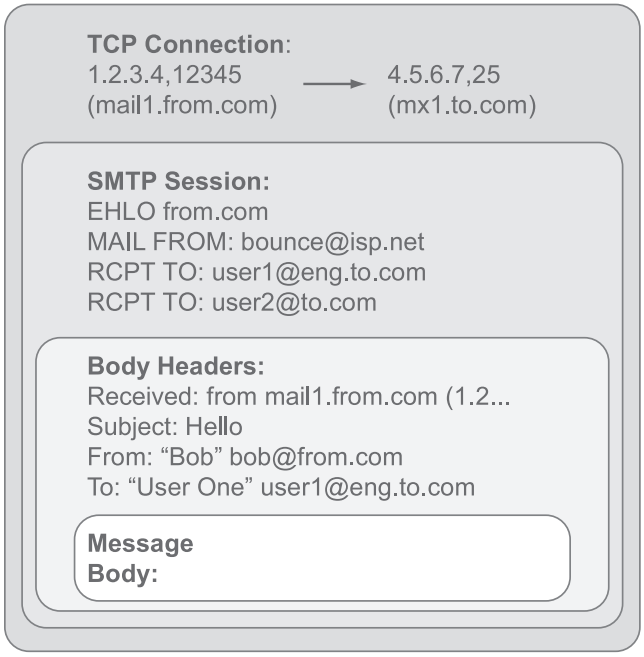
SITUATION

The Bounce Problem

Bounce messages are an inherent part of SMTP. Similar to a postal envelope address, an SMTP email has an "envelope" to and from address that is not exposed to the end-user, but that the email gateways use to properly route mail. It is not uncommon to have an envelope return address be different then the actual from address that is exposed to the end-user in their mail client. For example, if Acme Corporation were to use an email service provider for their monthly newsletter, the emails would appear to the end user to be from "service@acme.com" but would have an envelope return address of "replys@serviceprovider.net". The anatomy of an SMTP email is illustrated in Figure 2.

FIGURE 2.

Anatomy of an SMTP email message



Email was designed at a time when the Internet was a collection of trusted scientists and academics sharing information. At the time the protocols were designed, it was inconceivable that anyone would forge the addressing scheme. As a result, there is virtually no way to verify that a return address is valid or spoofed. Modern spammers have taken advantage of this loophole in the email infrastructure and created a situation where bounce messages are polluting the Internet—in some cases disabling entire email networks.

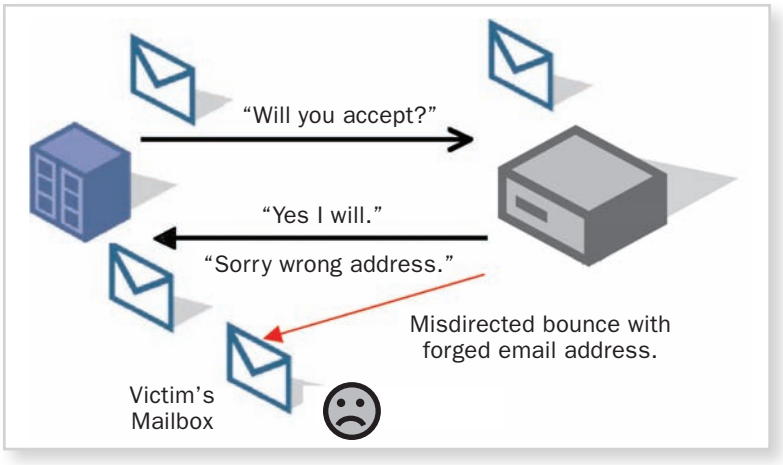
Spam works on volume. Since spam response rates are very low, spammers increase their revenues by blasting out ever-increasing volumes of spam. It is not uncommon for a spam attack to involve ten million messages or more. Since many of the addresses the spammers are mailing to are invalid, a bounce rate of 20 percent or more is also typical. So a ten million message spam attack will create two million bounce messages in return. Spammers don't want that type of volume returning to their network, so they typically forge the return

SITUATION
(CONTINUED)

address with a random address, causing billions of bounce messages to scatter across the Internet. These bounces, aimed at forged return addresses, are know as "misdirected bounces" and have grown to massive proportions. A misdirected bounce is illustrated in Figure 3.

FIGURE 3.

Legitimate mail is sent and accepted. If the address is incorrect, the message is returned to its sender. Spam with a forged email address is also returned—to an unsuspecting victim of misdirected bounces.



Misdirected bounces have a few variants. The most common is the text reply notifying the user that, the message they sent was not delivered, due to invalid address. Another form of misdirected bounce is caused when an end-user sets up an "out of office" autoreply and this out of office notice gets misdirected to an unwitting third party that was unlucky enough to appear in the return address of a spam message. A particularly troublesome variant occurs when a receiving mail server is configured to notify the sender that their message contained a virus. This helpful notice is misdirected to a random third party with a message stating "the message you sent to john@acme.com could not be delivered because it contains the mytob virus". When, in fact, the end-user never sent an email to john@acme.com, it just happened that the mytob virus forged the return address causing a misdirected virus notification.

A Constant Drain on IT Budgets – or Worse

The sheer volume of misdirected bounces have created a nuisance for IT teams around the world, consuming valuable resources. Misdirected bounces consume system capacity and bandwidth used to process and store these messages. They also generate expensive IT trouble tickets from end-users, who are confused by incoming misdirected bounces. Misdirected virus notifications cause a significant amount of end-user confusion. End users may get a message from an address they recognize or one they don't, but in either case the end-user will assume their PC is infected—when in fact they are just the unlucky recipient of a misdirected bounce or virus notification.

The IronPort Threat Operations Center measured global volume of misdirected bounces at an astounding 4.5 billion messages per day. Typically 10 percent of these misdirected bounces have valid addresses, yielding 450 million misdirected bounces that make it through to end-user mailboxes every day. If only 0.2 percent of these messages generate an

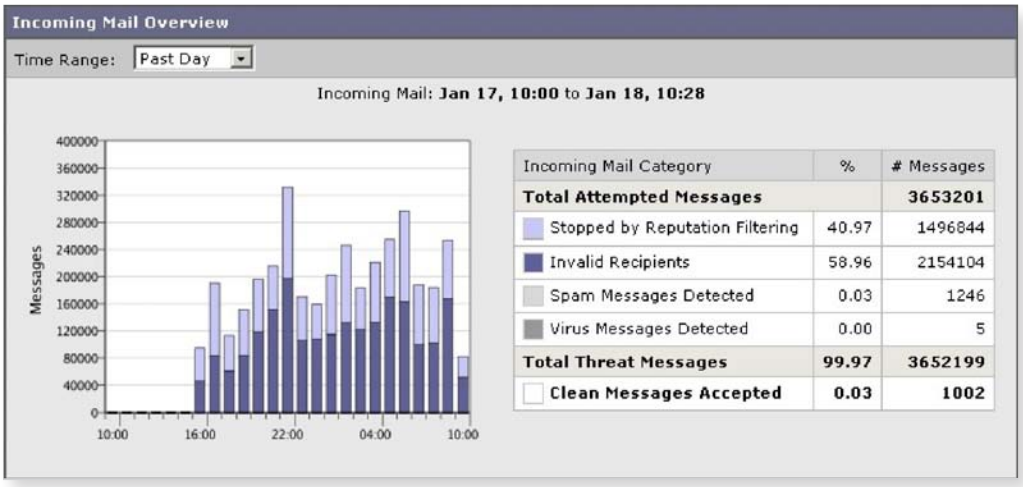
IT trouble ticket (a very conservative assumption) that corresponds with 900,000 tickets per day. At a global ticket cost of (US) $20 per ticket, this equals (US) $4.5 billion annually consumed by misdirected bounces. Adding the cost of system resources, bandwidth and service outages could easily increase this number by 3-5x, but these costs are harder to quantify and where therefore not addressed by this study.

There is another, far more significant, cost associated with misdirected bounces. If a spammer sends out a 100 million message spam campaign, and (instead of rotating through random return addresses) uses a single forged return address of, for example, "postmaster@victim". com, then postmaster@victim.com is going to receive 20 million bounce messages from 20 million different legitimate mail gateways across the Internet. These 20 million legitimate mail gateways are performing what should be an electronic courtesy, but they are actually unwittingly participating in a massive DDoS attack.

These denial of service attacks are not uncommon. In a survey associated with this study, IronPort® found that 55 percent of the Fortune 500 have had a disruption in service or a full scale outage due to misdirected bounce attacks. Consumer brands and financial entities are often targeted as spammers will use their return addresses in an effort to appear more legitimate. Figure 4 illustrates the full impact of one such denial of service attack. This is an actual screen shot taken from the IronPort appliance protecting a Fortune 500 insurance company. During a 24 hour period, this firm saw their typical mail volume of 10,000 messages leap to 3,653,201 messages—a 360x increase in volume driven by a misdirected bounce attack. The good news shown in Figure 4 is that the IronPort appliance was able to withstand this massive volume surge, and dropped 59 percent of the mail prior to accepting it by use of high performance address validation and dropped the remaining 41 percent based on the reputation of the sender.

FIGURE 4.

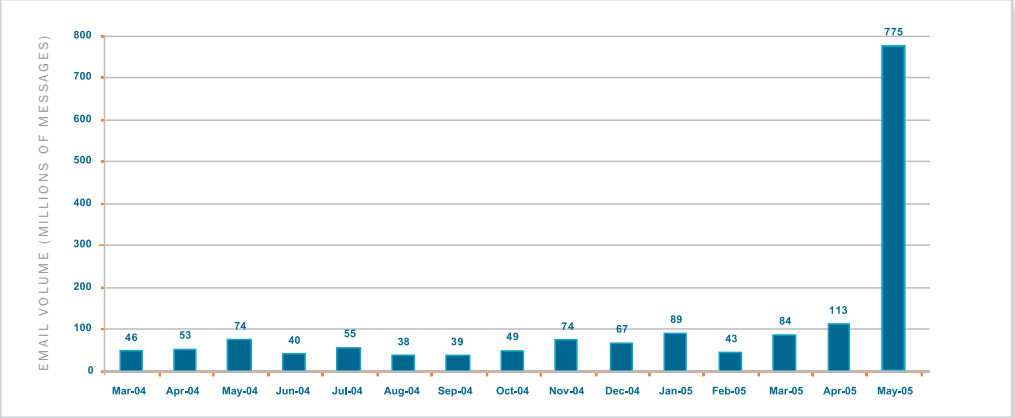
A spam bounce attack resulting in a denial of service attack



Networks of all size and scale are potential victims. Figure 5 shows another real world graph, this time from a large ISP. The graph shows a surge from 175 million messages per day typically to 775 million messages in one day.

FIGURE 5.

Spam bounce attacks



Figures 4 and 5 illustrate a profound point. Misdirected bounces can target any network with a very large increase in volume—on the order of a 50-100x increase. It is very difficult for any messaging system to have sufficient capacity to withstand this type of volume surge. Misdirected bounce attacks can also reach enormous scale. Figure 5 shows one attack generating nearly 800 million messages. The goal of most spammers is not to disrupt, but rather to avoid detection. However, there are groups and organizations whose sole function is to disrupt western economies. Imagine if these organizations launched a misdirected bounce attack on every government organization? With simple spammer tools and a few common servers, anyone can launch a massive DDoS attack that will knock a traditional mail server offline for days with a 10-100x increase in message volume.

SOLUTION

Secure Bounces: The Solution

Misdirected bounces are expensive and extremely dangerous. While there is little that can be done to prevent these attacks using traditional mail infrastructure (such as the very popular open-source "sendmail" program), IronPort has developed unique technology that can withstand a DDoS attack. And, better yet, prevent it from happening in the first place.

PERFORMANCE: CONNECTIONS AND MESSAGE PROCESSING

Withstanding a highly distributed denial of service attack with misdirected bounces is extremely challenging, because the sources of the bounces are legitimate mail servers that cannot simply be blocked. IronPort email security appliances have extremely high concurrency, allowing them to support up to 10,000 simultaneous connections. In addition, a single IronPort appliance can process incoming mail at rates of up to 1 million messages per hour. This breakthrough performance represents a 10x increase in processing versus traditional UNIX based systems, with raw capacity that can shrug off a DDoS attack.

EMAIL ADDRESS VALIDATION

The architecture of the IronPort appliance uses LDAP-based address validation early in the email processing pipeline. Consequently, the appliance can validate the address of incoming mail prior to actually accepting the message. This was a key attribute in allowing the appliance to scale, while under the real world attack shown in Figure 4. 59 percent of the

incoming misdirected bounces were discarded because of invalid addresses, a ratio not at all uncommon in a misdirected bounce. The remaining 41 percent of the incoming volume was originating from illegitimate sources (such as infected zombie PCs) and was thus blocked by IronPort's reputation filters. By intelligently processing mail prior to actually accepting the SMTP message body, the system can increase efficiency by an order of magnitude and shrug off even a large volume spike like the 360x increase shown in this example. However, there is a concern with this approach, because the corporate directory is now exposed to a spammer's directory harvest attack.

THROTTLING TRAFFIC WITH EMAIL SENDER REPUTATION

To protect the corporate directory, the IronPort uses sender reputation and secure bounce logic. The IronPort appliance keeps track of the number of invalid addresses received from a given sender over time. At a certain threshold the IronPort assumes the sender is just guessing at addresses and drops mail from that sender. This threshold varies by the reputation of the sender. A sender with a poor reputation might get one or even zero attempts to deliver a message. A slightly stronger reputation will be allowed five invalid delivery attempts before messages are dropped. A sender with a long history or reliable mail patterns will be allowed 20 or more delivery attempts before their mail is blocked. This type of graduated response allows the IronPort appliance to intelligently determine whether or not to issue a bounce message based on the reputation and behavior of a given sender. Let the punishment fit the crime.

IRONPORT TECHNOLOGY SOLVES THE PROBLEM AT ITS CORE

Attacking the problem at its root, IronPort has developed a secure bounce technology that prevents misdirected bounces from starting in the first place. IronPort appliances can be configured to issue a bounce message during the SMTP conversation. This means that the appliance holds the connection open with the sending mail server and validates the recipient address prior to accepting. Validating the address during the conversation has the advantage of never issuing a misdirected bounce, since the sender gets the bounce notice directly, instead of relying on a separate email notice that is sent to the frequently forged email envelope return address.

Email administrators around the world need to be aware of the problems of misdirected bounces. Administrators using traditional mail gateways need to begin using conversational bounces instead of the delayed bounces that are frequently misdirected and thus are polluting the Internet. Making this change can expose the corporate directory to harvesting, but it is a fair trade off to prevent the DDoS attacks associated with misdirected bounces. IronPort customers can rest assured that they will not be misdirecting bounces and contributing to the Internet email traffic emergency.

IRONPORT®

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, CA 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

IRONPORT 04/06 DOC RELEASE