



How to Defuse an Email Bomb

Spam Soap Whitepaper

*It's 4:30 a.m., Monday morning,
and your cell phone's ringing
— loudly. "Hello?"*

*A frantic employee is shouting
into the phone. Something about
nobody being able to send or
receive email and critical deadlines
they're going to miss because of
the breakdown. You log on and
find your Exchange Server queue
jammed with over 100,000 mes-
sages from unknown users and
domains. "What is going on?"
you wonder.*

*Sound familiar? If not,
it's only a matter of time.*

Welcome to the world of email bombs.

Spammers are using increasingly sophisticated techniques to undermine legitimate businesses, making it more difficult to prevent their attacks. This whitepaper will describe the most common threats, how to defuse them and most importantly, how to prevent them.

Inbound Mail Bombs

Once an infrequent disturbance, Inbound Mail attacks are now the fastest growing email problem. They include File Size bombs, Volume bombs, Dictionary Harvest Attack bombs, and Joe Job bombs. Any one of these attacks can quickly overrun a mail server, completely disabling it. What are they, and how can they be defused?

A File Size bomb takes the form of an email message with huge binary file attachments. Its mission: crash the recipient's mail server or mail reader.

Defusing a File Size bomb:

Set your mail server or firewall to allow only moderate-sized messages; a level you know your server can handle.

Volume bombs send a huge quantity of mail messages to one domain or server. By filling up the recipient's disk space or overloading the server, the volume bomb maxes out the mail queues and disables the server.

Defusing a Volume bomb:

Because volume bombs generate excessive Non-Delivery Reports (NDR). It's important to disable or limit NDR messages during the bomb. If your server is compromised by a growing mail queue, lower the delivery retry interval to conserve server resources. You may also rename the queue folder or move the messages out of the queue folder, hold them until the server is able to process

the volume, and then reintroduce them to the queue.

Dictionary Harvest Attack bomb

(DHA): Spammers flood mail servers by sending hundreds of messages to random addresses, hoping that some of them are valid. In a dictionary attack – also known as a “brute force” or “direct harvesting” attack – spammers will send blank messages to a list of randomly generated addresses with the same domain name. Every email not returned, and every valid (250 OK) SMTP reply, indicates a likely valid address.

DHAs, which have recently doubled, can slow corporate email systems to the point that companies have to increase spending on extra server space and bandwidth.

Defusing a DHA: Standard approaches to spam filtering or IP address blocking are useless against DHAs. In order to prevent the wave of email queries and corresponding non-delivery reports, the attack must be detected at the SMTP layer. The only effective way to prevent a DHA before any of the traffic effects your server or network is to use an offsite email security company like Spam Soap.

Joe Job bombs are master spoofs. The spammer sends out huge volumes of spam under the guise of someone else's – legitimate – domain. Consequently, all undeliverable messages bounce back to the hijacked domain, not the spammer.

Defusing a Joe Job: As with a volume bomb, joe jobs generate excessive Non-Delivery Reports (NDR). It's important to disable or limit NDR messages during the bomb. If your server is compromised by a growing mail queue, lower the delivery retry interval to conserve server resources.

In November, 2004, spammers attacked one of SpamSoap's clients with a Joe Job mail bomb. Here's what that client had to say:

"I'm a Land Surveyor with a limited understanding of the workings behind email and networking in general. I somehow manage to keep things running, but rely on our network consultant to bail me out when I'm in over my head.

"I do know that before SpamSoap took action to counteract our mail bomb attack, our internet connection was so bogged down we were unable to conduct normal business. Our clients rely on us to correspond with them; occasionally transferring large drawing files by email under tight schedules. That wasn't happening.

"Whatever SpamSoap did took care of our problem and things have run smoothly ever since. SpamSoap has solved all our email and spam problems and has been a pleasure to work with. Their response to our problems has been surprisingly quick, personal and effective – unusual these days. I recommend SpamSoap every chance I get."

*– Dan Fischer,
Sunde Land Surveying, LLC*

You may also rename the queue folder or move the messages out of the queue folder, hold them until the server is able to process the volume, and then reintroduce them to the queue.

(For a more detailed look at a Joe Job bomb in action, see page 4.)

Outbound Mail Bombs

Thankfully outbound attacks – where hackers co-opt servers to send out spam and malicious email – are on the decrease. But they do still occur, plaguing system administrators and disabling mail servers. Today the most common are open relays, hijacked accounts and viral attack bombs. If left undetected, these bombs pose real threats. The first is landing the mail server IP address range on real-time black hole lists, blocking all your legitimate email to clients, prospects, and vendors. Second, and even more troubling, is the possibility of losing your internet connection if the flood of junk mail continues.

Hijacked Account: Spammers can run hacking software on email servers in search of valid user accounts when SMTP authentication is enabled. Once they find a valid email, they can crack the password. Then they are fully authorized to send email from an authenticated account on the server.

Defusing a Hijacked Account: First identify when the problem began, then scan the log entry for the culprit account. Resolving the problem is usually as simple as changing the password for that account.

Open Relays allow servers to accept and deliver external email from an unauthenticated user. For your business, this means ease of use. For hackers, it means a weakness they love to exploit. A server with an open relay configuration is a sit-

ting duck. It's only a matter of time before the outbound queue will be full of spam, interrupting the flow of legitimate mail.

Defusing an Open Relay attack:

First, determine the type of relay your server is open to. Many websites – like the resources section of www.spamsoap.com – offer automated tests and detailed descriptions for testing your mail server. In many cases, running the patches provided by such sites will close a relay down. An up-to-date mail server will have the ability to control the relay settings, typically found in the SMTP security area.

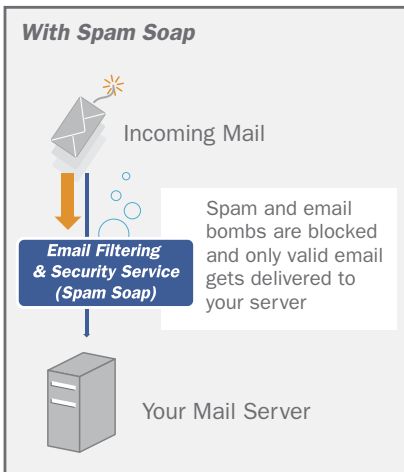
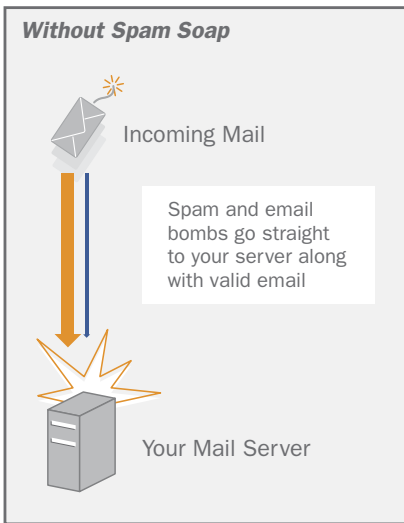
Viral Attack bombs start by scanning contact lists in search of addresses to blast virus-infected emails. They deliver outbound messages using the corporate mail server, clogging the mail queue. Though many have their own SMTP engine, they still flood the gateway. Such attacks can quickly land a network IP range on blacklists.

Defusing a Viral Attack: The good news is that the viral attack originates from a device on your local network. If you remove that device, or isolate the traffic on that device, you can remove the virus before reconnecting it to the network. To prevent viruses from propagating during the attack, set the network firewall to deny outbound SMTP traffic, except that which originates from approved servers or computers.

Defusing Bombs

Once an email bomb has hit you, it's easy to think, "Turn off the mail server!" But it's not that simple. Eventually you have to defuse the bomb. Since SMTP is designed to weather outages, turning off the server will simply delay the inevitable.

Before you can defuse a bomb, you have to know what type of bomb has hit and where: inbound or outbound email



- Valid Email (2%)*
- Spam, Viruses and Email Bombs (98%)*

*Typical among Spam Soap clients as of January 2005.

queues. Since most inbound attacks come from scattered sources on the Internet, trying to stop the attack at the firewall is often pointless. (A quick review of the firewall log should reveal the effectiveness of adding individual IP blocks.) Having identified the type and target, then the real work of defusing and restoring your servers begins. It's an ongoing drain on your time, talent and resources.

You could just wait out the attack, typically a weeklong ordeal, or you could hire a filtering company like www.spamsoap.com. They can recognize attacks and capture the offending email onslaught before it overtakes your servers.

Preventing Bombs

Preventing a bomb is always better than recovering from one. Prevention is the best investment and in the long run, will save your company time and money. By reading this whitepaper, you've already taken an important first step: awareness of the many different ways an attacker can strike. Additionally you should test your server regularly after installing a new patch or upgrade for an open relay. Also set a policy that requires passwords (they should be strong and changed regularly); limit the number of recipients allowed per message; regulate and limit the size of attachments permitted and eliminate catch-all email accounts.

Unfortunately, there's only so much protection you can provide at the server level. You may need security in front of your server. By installing a hardware appliance or server at your gateway, you can manage basic spam, virus and email attacks. But this seemingly affordable option can be prohibitive when you figure in filter maintenance, hardware upkeep and redundancy. And any appliance or server installed on your network still runs the risk of being overwhelmed by an email bomb, compromising available network bandwidth.

The biggest problem with installing an email security solution on your network is that your network is still the battlefield where the bombs will be sent. Spam Soap preemptively removes the problem from your network protecting your information, maintaining quality of service, and safeguarding your email system from Internet-based threats. The Mail Bombs will be systematically defused and absorbed by our redundant, load-balanced network in addition to restoring your bandwidth and server resources to their intended roles.

Your firewall can be configured to completely isolate your mail server from the Internet, only allowing packets from the IP address of the filtering service to reach it. Doing so prevents many unwanted intrusions including hijacked accounts, open relays, and other hacking techniques to which most mail servers are vulnerable. Without a filtering service, your email server must be open to accept messages from all IP addresses on the Internet.

Most companies dread the high cost and inherent vulnerabilities of installing and maintaining hardware solutions. They are opting for a filtering service both for cost and effectiveness. Such a service handles all of their email before their server receives it. Spam Soap Inc., filters all email for viruses, spam and most importantly, the attacks your server can't withstand. Dictionary Harvest, Joe Job and Viral attacks are just a few of the email bombs that a filtering service can disarm before they take your email server offline.

Joe Job Mail Bomb

Scenario

Joe Job Mail Bomb hitting companydomain.com

Environment

200 mailbox organization with average daily inbound Internet email of 60,000 messages

Server

Microsoft Exchange 2003 Enterprise on a single server with dual 2.4Ghz processors, 2GB RAM and RAID 5. Internet connectivity with a full T-1 line.

Joe Job Situation

Approximately 1,000,000 spam messages are sent by a spammer with a forged email address from companydomain.com. These addresses are generated with a random name in front of the @companydomain.com, for example joe123@companydomain.com. Fifty percent of the spam messages—500,000 messages—do not go to valid recipients and non-delivery reports are sent to the forged sender email address. Server becomes unresponsive to receiving additional email when the inbound or outbound queue contains 80,000 messages. Inbound Internet email is delayed and at times not deliverable because the Joe Job Mail Bomb is monopolizing the server resources and bandwidth.

Contributing factors

Microsoft Exchange has a global setting for all outbound SMTP email which, by default, retries delivery for 48 hours before returning the email or sending the Non-Delivery Report, NDR, to the BadMail folder. Because the non-delivery reports coming into the Exchange server did not match valid addresses, new NDR messages were generated. This began to fill the outbound mail queue with NDR messages as well.

Defuse Options

1) No filtering enabled. The email is delivered directly to the Exchange Server

- Turning off the SMTP on the Exchange server will not help, it will only delay the addresses which are queued to be sent to that domain.
- What's required is manually disabling SMTP for enough time to search the queued messages for text contained in non-delivery reports then moving them outside the queue folder. This would need to be monitored at least hourly. The Joe Job Mail Bomb may continue for a number of days causing incremental downtime, diminished bandwidth and server performance and would also require full-time IT staff to manage the mail flow.

2) Premise Filtering Equipment. There is an appliance or server installed on the network in front of the Exchange Server.

- Once the Mail Bomb has been identified as a Joe Job, disabling outbound NDR messages if the option is available would prevent the outbound queue from filling with NDR messages.
- If the inbound NDR messages are being passed to the Exchange Server, implementing a content filter would catch NDR messages and delete or treat them as spam.
- While fully capable of filtering standard email and spam volume, the appliance or server may become overwhelmed with the volume of messages. Key to this approach is regular monitoring of mail flow and periodically removing messages from quarantine or mail queues.

3) Gateway Service. The email is first sent to a filtering service before being delivered to the Exchange using an MX record change.

- NDR messages would normally be let through by spam filtering services, so the initial Joe Job messages would go to the Exchange Server.
- Once the Joe Joe Mail Bomb has been identified, a gateway filtering service like Spam Soap could enable a Joe Job filter, which would delete all inbound NDR messages, effectively disabling the mail bomb. After the Joe Job has subsided, typically one week, the filter would be moved and NDR messages would be sent to the Exchange Server.
- This defuse option would have minimal impact on server resources, bandwidth and IT staff.

In December 2004, spammers attacked inhouseIT's Exchange server with a Dictionary Harvest Attack bomb (DHA).

"We had just brought on a new customer with an existing Exchange 5.5 server," remembers Jeff Linge an IT Manager at inhouseIT. "Their Exchange Internet Mail Service was crashing every few hours and the unreliability of their mail service was causing them to lose business by the hour.

"After some initial research I suspected the problem was due to some type of spam related attack. I recommended that they give Spam Soap a try. After two weeks of filtering, we found out that 99.3% of their email was spam; SpamSoap also caught an average of 30 messages a day with viruses. When I showed them the first report, their jaws hit the ground.

"Now that we've locked down inhouseIT's firewall – only allowing inbound SMTP connections from Spam Soap – the spam-related mail bombs which were causing the server to crash are now a thing of the past.

"I rest easy at night because I know I have Spam Soap on my team," said Jeff. "Spam Soap should be in every IT Professional's toolkit."

Summary

Email is now more critical to business than ever before. But email servers have never been more vulnerable. The mail bomb attacks discussed above are only a few of the growing ways your server may come under attack. Additionally, the tools and knowledge necessary to perform such attacks are available for any user at any skill level who decides he wants to blast your company. You can't protect yourself from everything, but with a little time and due diligence, you can decrease your organization's chances of falling victim.

About Spam Soap

Spam Soap is an enterprise level email security solution that provides Virus Protection, Spam Filtering and Email Security in one complete package. Because Spam Soap filters your email *before* it enters your network, your network is secure from Internet-based email threats and your bandwidth is spared high volumes of spam.

With no hardware or software to install or maintain, Spam Soap delivers a straightforward business email security solution.

Founded in 2002, Spam Soap is a privately held company serving more than 1,500 companies.



www.spamsoap.com

866.SPAM.OUT

**3193 Red Hill Avenue
Costa Mesa, CA 92626**