How to block NDR spam

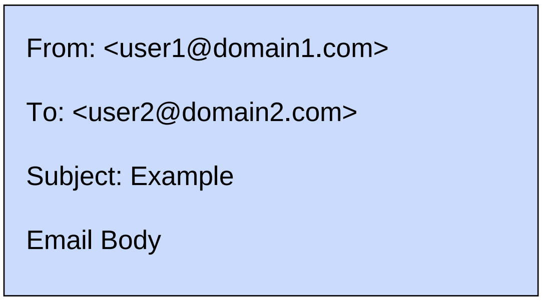
Spam generates an enormous amount of traffic that is both time-consuming to handle and resource intensive. Apart from that, a large number of organizations have been victims of NDR spam that has an effect similar to a Distributed Denial of Service on the email system. In this paper we provide a technical explanation of NDR Spam and recommend solutions that can prevent or limit exposure to this kind of unsolicited email.

What is a Non-Delivery Report?

Email systems support a service called Delivery Status Notification or DSN[1] for short. This feature allows end users to be notified of successful or failed delivery of email messages. Examples include sending a report when email delivery has been delayed or when an email message has been successfully delivered.

A non-delivery report or NDR is a DSN message sent by the email server (mail transfer agent or MTA for short) that informs the sender that the delivery of the email message failed. While there are various events that can trigger an NDR, the most common cases are when the recipient of the message does not exist or when the destination mailbox is full.

A simple email message is typically made up of a set of headers and at least one body. An example of this can be seen in figure 1. In this example, the email is sent from user1@domain1.com to user2@domain2.com. If the domain name domain2.com does not exist or does not have an email server, then the MTA at “domain1.com” will send an NDR to user1@domain1.com[2]. When the domain name exists and the MTA at domain2.com is accepting email, the behavior is different. In this case, the domain2.com email server should check if the destination mailbox exists and is accepting emails. If this is not the case, then the MTA should reject the email message. However, many mail servers will accept any email and then bounce the email later on if the destination address does not exist.



From: <user1@domain1.com>

To: <user2@domain2.com>

Subject: Example

Email Body

Figure 1

Figure 2 describes a scenario where "user2@domain2.com" does not exist, but the mail server at domain2.com still accepts the email as it cannot verify if the mailbox exists or not. The server then sends an NDR message to “user1@domain1.com” which includes the original message attached.

[1] The technical details for DSN can be found in RFC1891

[2] As per RFC 2821, the sender address is taken from the SMTP “MAIL FROM” command

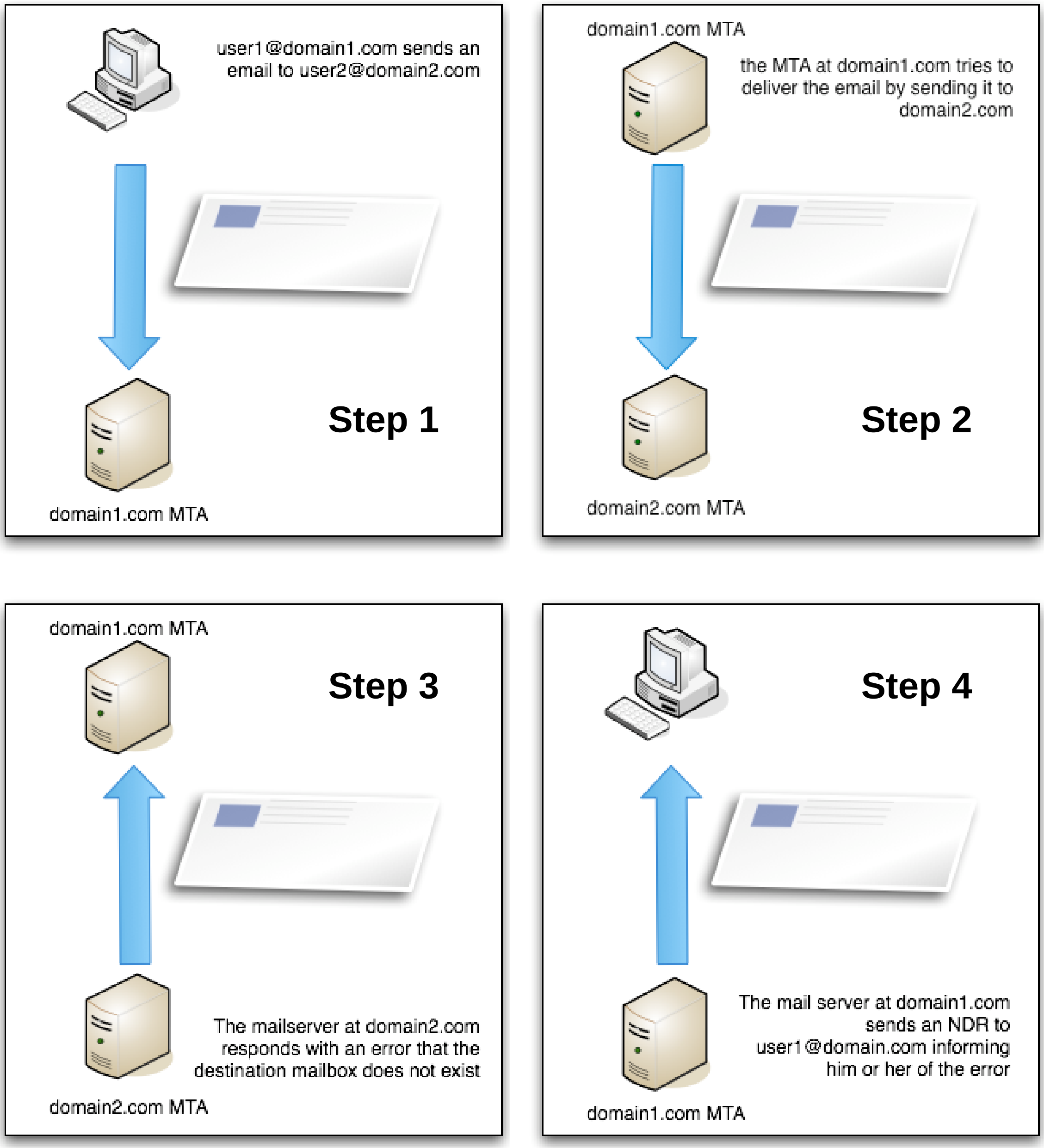
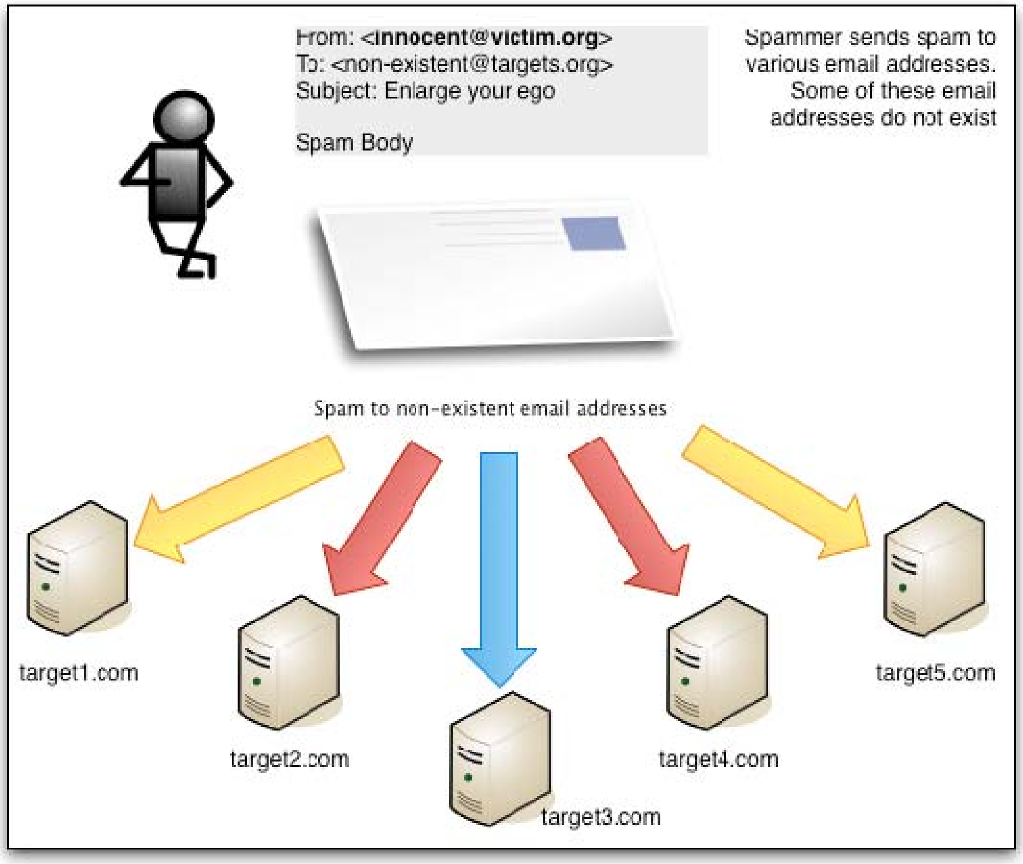

user1@domain1.com sends an email to user2@domain2.com
Step 1
domain1.com MTA
domain1.com MTA
the MTA at domain1.com tries to deliver the email by sending it to domain2.com
Step 2
domain2.com MTA
domain1.com MTA
Step 3
The mailserver at domain2.com responds with an error that the destination mailbox does not exist
domain2.com MTA
Step 4
The mail server at domain1.com sends an NDR to user1@domain.com informing him or her of the error
domain1.com MTA

Figure 2

How does NDR Spam work?

The SMTP protocol does not support authentication of the sender address. As a result, email messages can claim to be coming from any valid email address. Spammers have long known about this and tend to make use of fake addresses when sending their bulk mail. Since successful spam relies on targeting the largest number of clients possible, spammers tend to have large lists of email addresses. Some of the email addresses in their list might not exist or have been disabled. In many of these cases, the mail server handling the nonexistent email address may send an NDR to the faked sender address in the original email. If this address belongs to a valid user then what happens is that this user ends up receiving the non-delivery reports. Since the emails sent out by the spammer tend to be in large numbers, thousands of NDRs may end up in the victim's mailbox. The resulting emails are known as NDR spam or backscatter and an example is illustrated in figure 3.


From: <innocent@victim.org>
To: <non-existent@targets.org>
Subject: Enlarge your ego

Spam Body

Spammer sends spam to various email addresses. Some of these email addresses do not exist
Spam to non-existent email addresses
target1.com
target2.com
target3.com
target4.com
target5.com

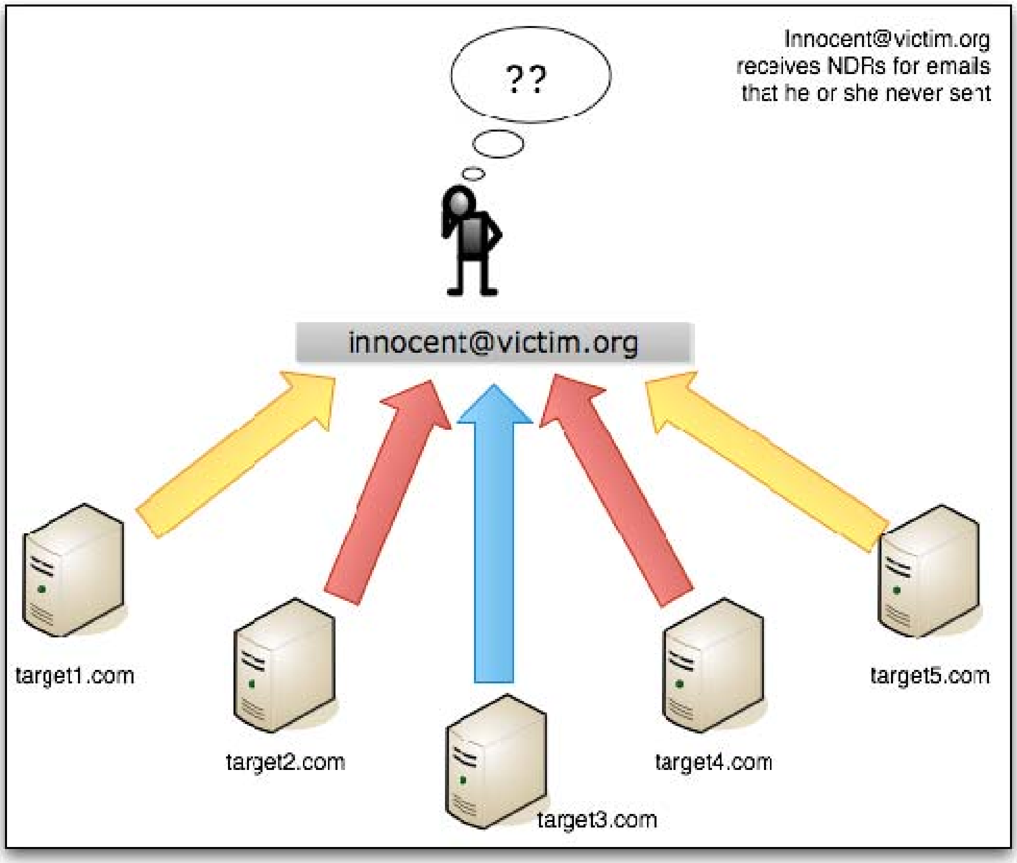
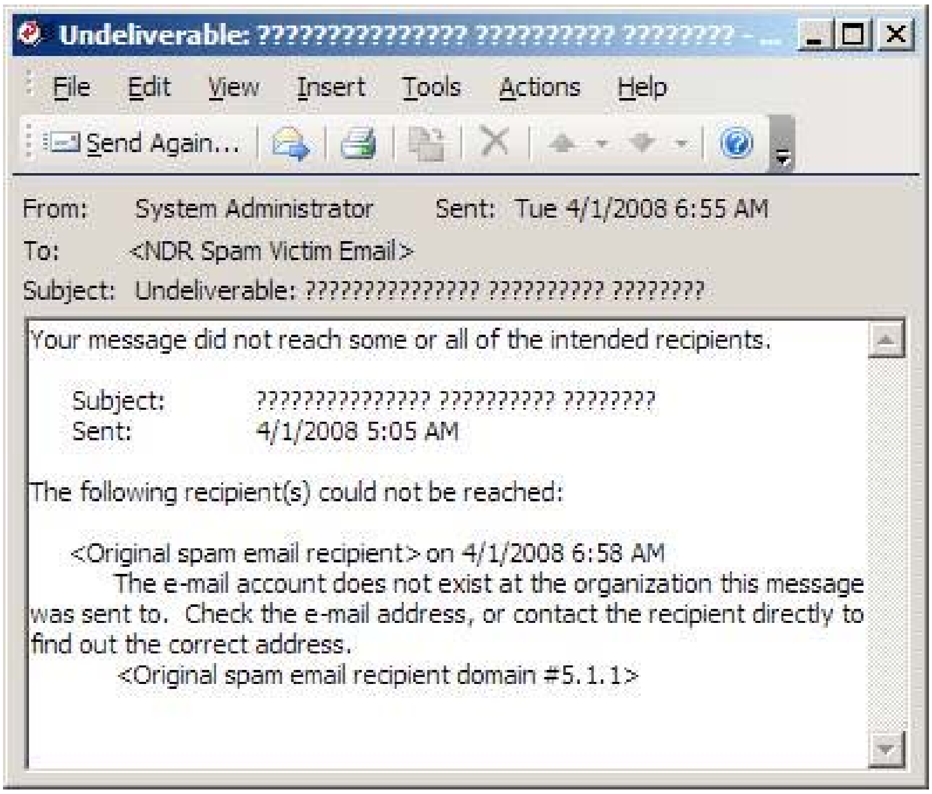


Figure 3

Why does NDR spam work?

Many mail servers are known to block email coming from non-existent domain names. Therefore spammers spoof email addresses which have valid working domain names to bypass this simple check. The result is that the victim MTA handling the email address that was faked by the spammers will receive a large number of NDR messages. These email messages can be difficult to block as it is not straightforward to distinguish between a legitimate NDR and one generated by spam.

It is unlikely that the spammers make use of this method to guarantee the delivery of the spam message. This is especially true when the address being spammed with NDRs is receiving hundreds of emails in a short time. Apart from this, the presentation of the spam message is reduced since the message can be truncated or appear as an attachment. Therefore the message is less likely to be read. An example of an NDR spam email message can be seen in figure 4.



From: System Administrator Sent: Tue 4/1/2008 6:55 AM
To: <NDR Spam Victim Email>
Subject: Undeliverable: ??????????????? ?????????? ????????

Your message did not reach some or all of the intended recipients.

Subject: ??????????????? ?????????? ????????
Sent: 4/1/2008 5:05 AM

The following recipient(s) could not be reached:

<Original spam email recipient> on 4/1/2008 6:58 AM
The e-mail account does not exist at the organization this message was sent to. Check the e-mail address, or contact the recipient directly to find out the correct address.
<Original spam email recipient domain #5.1.1>

Figure 4

How to reduce exposure to NDR spam

If you are responsible for a network that is a victim of NDR spam or backscatter, there are only a few preventive measures that you can take. One of the more straightforward solutions is to turn off your catchall mailboxes[3]. When this feature is disabled, unless the spammer spoofs your email address, your mail server will not be accepting non-delivery reports for email addresses which do not exist on your mail server.

If on the other hand, you are responsible for an email server that is causing NDR spam, then it is recommended that you configure the mail server to reject during SMTP transmission rather than bounce email messages which cannot be delivered. Various email servers such as Microsoft Exchange, Postfix, Sendmail and Qmail have patches to improve the behavior to

[3] Catchall mailboxes are email mailboxes that receive all email messages which do not have a named mailbox

create less backscatter. One can find online resources which detail[4] how to configure these servers to prevent the NDR spam problem getting worse.

A better solution

The latest version of GFI's MailEssentials for Exchange and SMTP[5] allows automated blocking of NDR spam. This solution does not require any changes to be made on the mail server's side. GFI's MailEssentials scans NDR emails by making use of the existing Anti-spam features employed by MailEssentials, such as the Bayesian Filter, DNS Blacklists, Sender URI RealTime Blocklists and Keyword Checking. GFI MailEssentials will also make use of the Directory Harvesting feature[6] on the Gateway to drop email messages and NDRs sent to non-existent users. If the NDR makes it past these protection mechanisms, then the email message is checked against the "NewSender" feature. This feature allows end users to receive only legitimate non-delivery reports, thus allowing them to focus on actual work rather than cleaning up the mailbox.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong and Adelaide which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.

Appendix

Keywords

- ndr spam
- backscatter
- dsn - delivery status notification
- collateral spam

[4] Preventing Backscatter
[5] How to check for NDR spam
[6] Directory Harvesting