

GFI White Paper

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 (DDoS) 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.

Contents

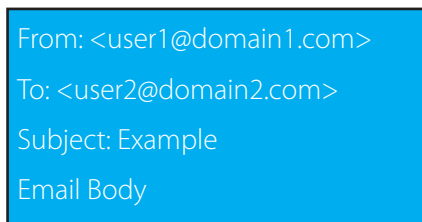
What is a non-delivery report?.....	3
How does NDR spam work?.....	4
Why does NDR spam work?.....	6
How to reduce exposure to NDR spam.....	7
A better solution.....	7
About GFI®.....	8

What is a non-delivery report?

Email systems support a service called Delivery Status Notification or DSN¹ 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.com². 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.

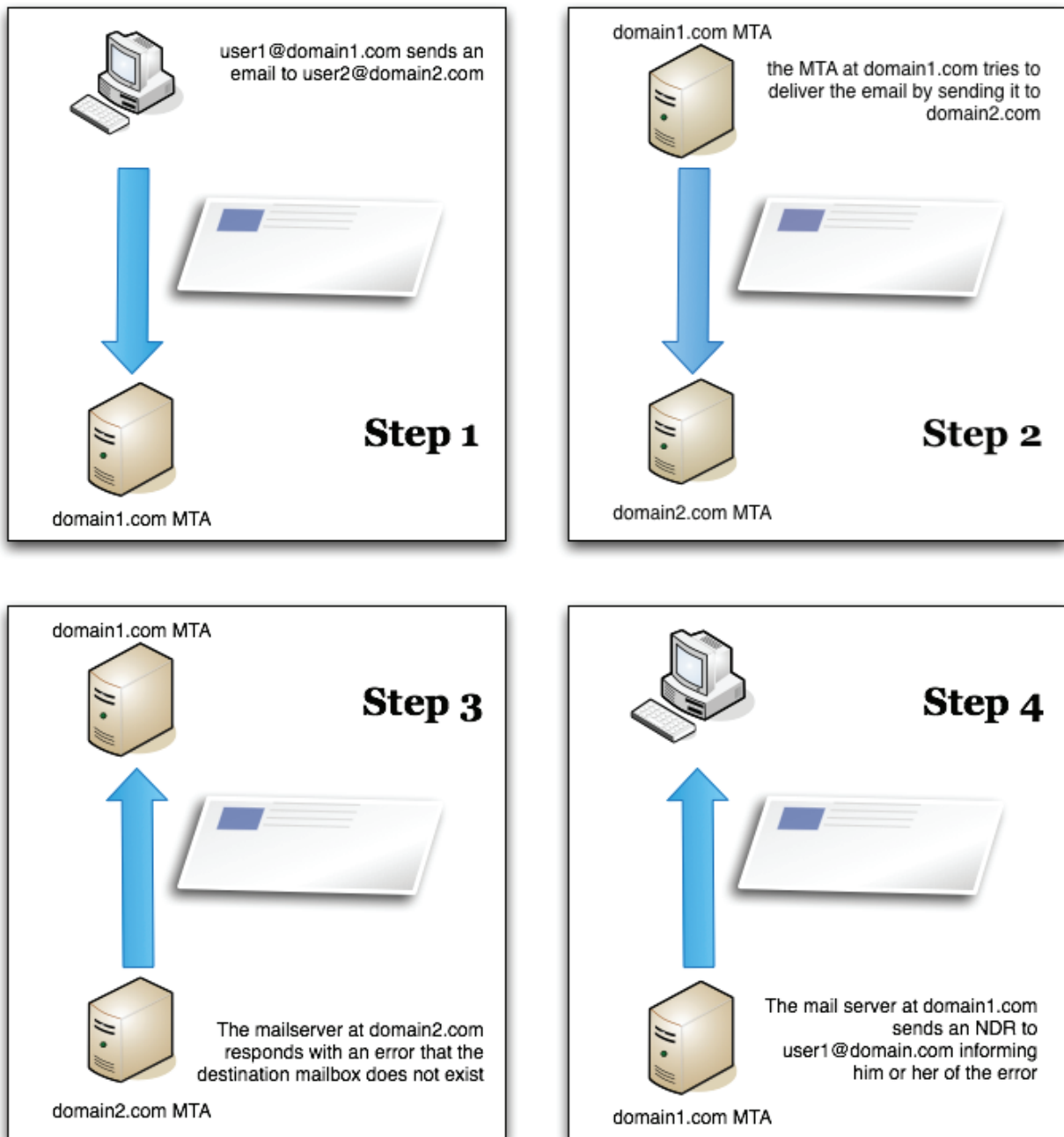
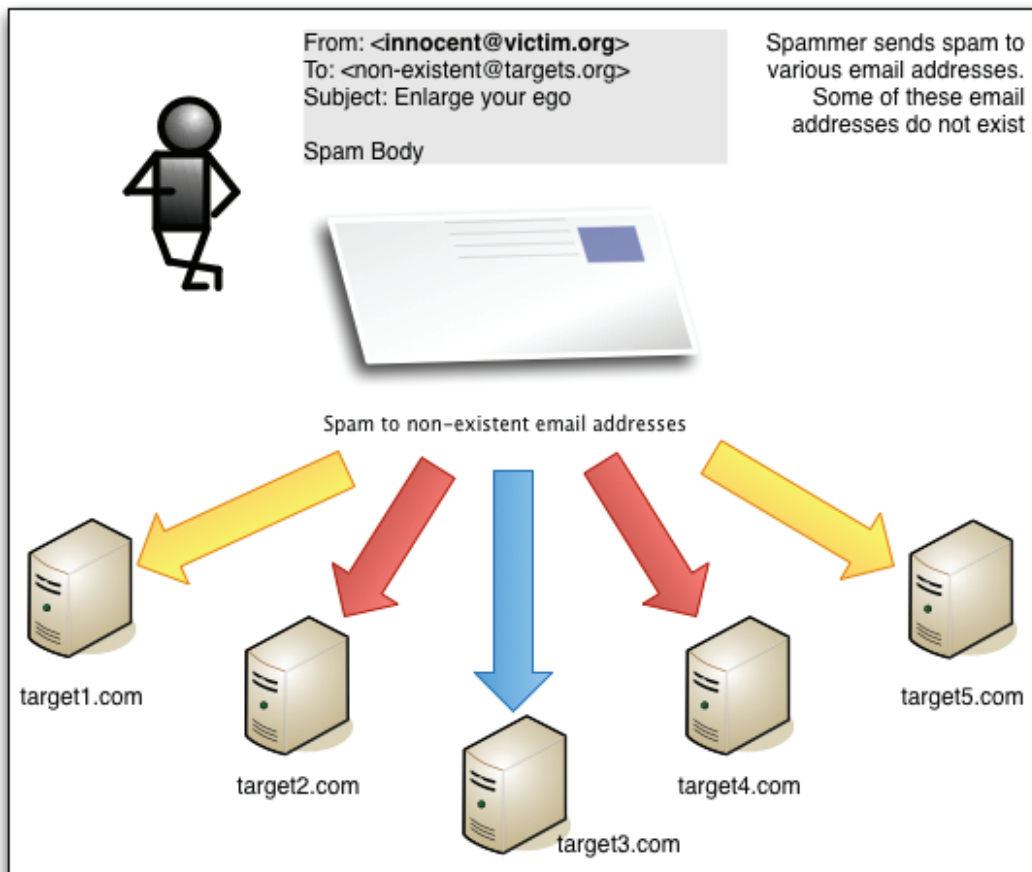


Figure 2

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.



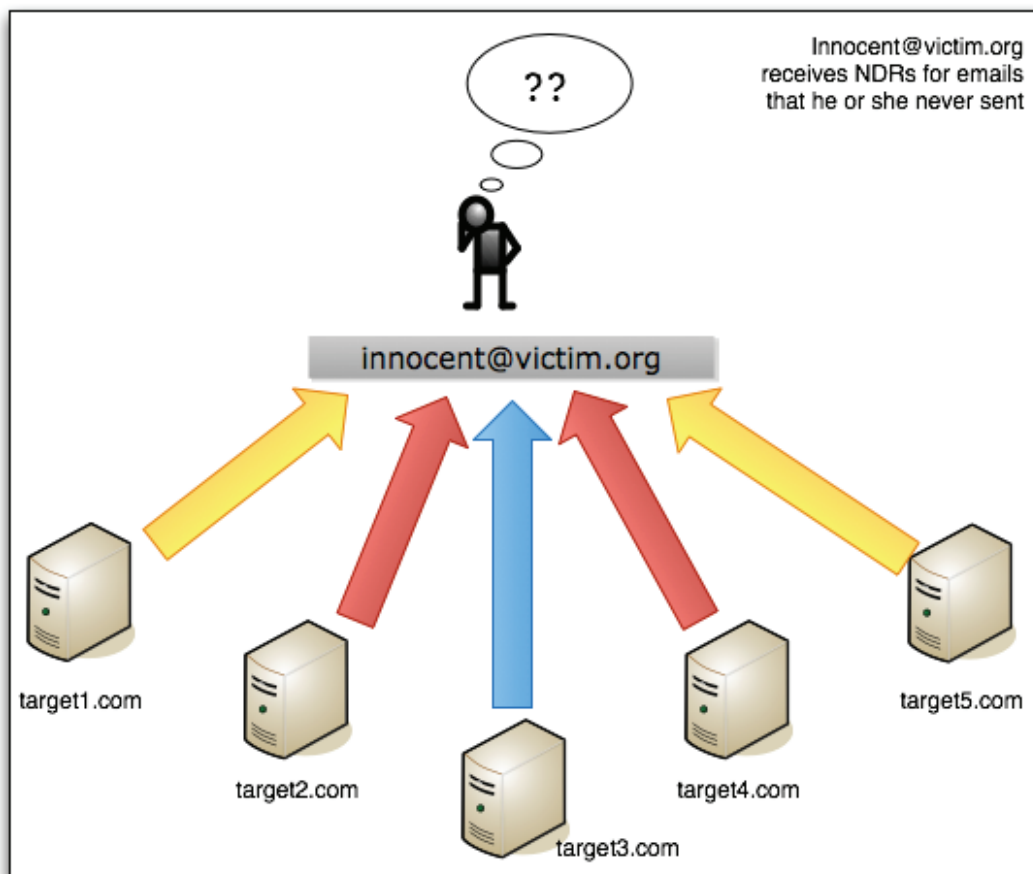


Figure 3

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.

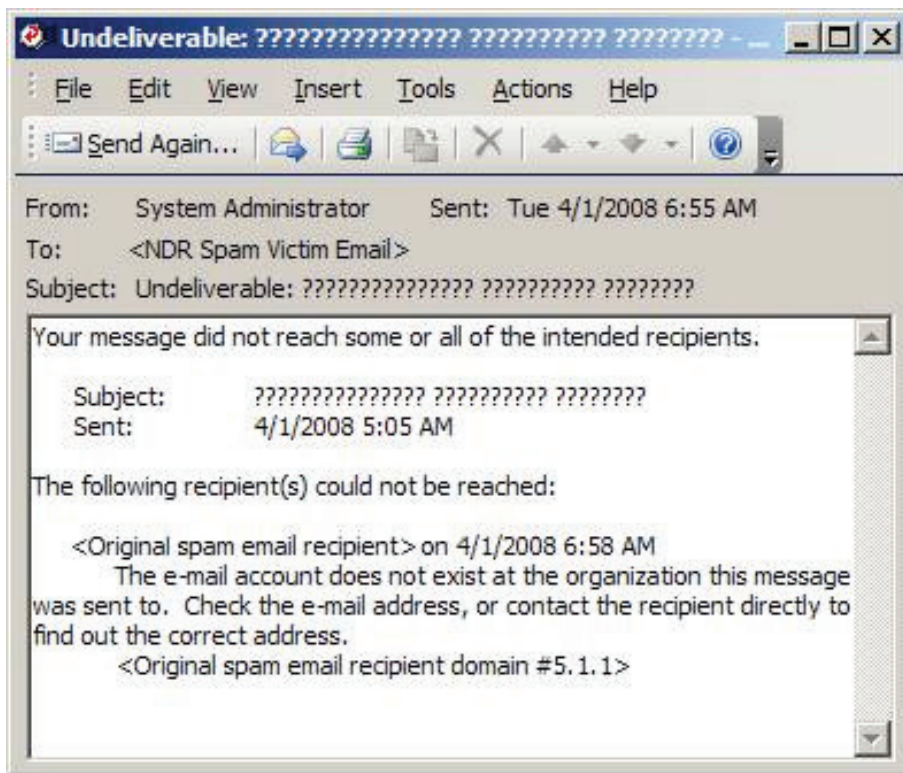


Figure 4

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 mailboxes³. 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 create less backscatter. One can find online resources which detail⁴ how to configure these servers to prevent the NDR spam problem getting worse.

A better solution

The latest version of GFI MailEssentials™ for Exchange and SMTP⁵ allows automated blocking of NDR spam. This solution does not require any changes to be made on the mail server's side. GFI MailEssentials scans NDR emails by making use of the existing anti-spam features employed by GFI MailEssentials, such as the Bayesian filter, DNS blacklists, sender URI real-time blocklists and keyword checking. GFI MailEssentials will also make use of the directory harvesting feature⁶ 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 Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

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

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

⁴ Preventing Backscatter

⁵ How to check for NDR spam

⁶ Directory harvesting

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.