WeCloud
PEACE OF MIND IN EVERY CONNECTION

Whitepaper: Decoding Headers

The header of an email contains information needed when processing that email and responses to it, it also contains information from every system that has processed this email and last but not least it contains the information that is shown to your user when reading the email (such as sender and subject). All different server types and server configurations have their own custom headers that they add to an email, so to list all possibilities in this document would be impossible, but we will try to walk you through the standard header entries and how to interpret them.

Note: The headers of an email are part of the data and can be manipulated by malicious senders, so there are no guarantees that the information contained in the headers is correct.

The anatomy of the headers is that it starts with the name of the header and then follows the content of that header, like this: *Header-Name: Content*

The first part of the header that we will look at is the *Received headers*. The Received headers allows us to trace an email's route from start to finish as every server that handles the email puts its stamp on the email. As soon as a server receives an email it adds a stamp (Received header) to the email giving details on the transaction that took place. When looking at the Received headers of an email the last server in the chain is always listed first, meaning that if you want to follow the email from start to finish you need to start at the bottom Received header and work your way upwards.

A Received header looks like this:

Received: from smtp1-ext.ord1.corp.rackspace.com (smtp1-ext.ord1.corp.rackspace.com [173.203.4.141])
(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by se-in1.mx-wecloud.net (Postfix) with ESMTPS id 912F7420394
for <jla@wecloud.se>; Thu, 13 Apr 2017 04:04:49 +0000 (UTC)

The received header starts with telling which server was the sending server in the server-to-server transaction (in this case the server was smtp1-ext.ord1.corp.rackspace.com). In the example above it moves on to give information reading the transaction (that TLS was used), however this is not mandatory for servers and if and how it is done differs from server to server. Next the receiving server is listed, including optional extra information that can help an administrator track the email locally on the server (in the example above the receiving server was se-in1.mx-wecloud.net), in some cases the stated recipient is also listed (as it is above). And last the server adds a timestamp showing when this transaction took place (please note that different Received headers might be in

different time zones.

MX Toolbox have a good online tool for reading headers that can be used to interpret the Received headers and show any occurred latency in the transactions:
https://mxtoolbox.com/EmailHeaders.aspx

Sender Recipient and subject
The information read by the email client to show the sender, the recipient and subject of an email is also header based and controlled by the following headers (note that this also controls replies to emails and where error notifications should be sent.
From: Name of Sender <senders address>
To: <recipient's address>
Subject: Subject to be shown
Date: Day and time to be shown
Reply-To: <address that replies should be sent to>
Return-Path: address that should receive errors if this message can't be delivered

From
This is what will be shown as the sender to the user opening this email in their email client. There is no guarantee that this in any way matches the real sender (envelope sender) of the email.

To
This is what will be shown as the recipient to the user opening this email in their email client. There is no guarantee that this in any way matches who the e-mail was really sent to.

Subject
This is the subject line that the email client should show.

Date
This is what will be shown in the email client as the time and date the email was sent. There is no guarantee that this is the correct time and date that the email was sent.

Reply-To
If the recipient of this email hits the reply button this is the address that should be in the To field for that reply. There is no guarantee that this will be the same address as either the real sender (envelope sender) or the shown sender.

Return-Path
This is the address that should receive and Mailer Daemons or similar if this email can't be delivered. This is generally the same address as the real sender of the email (envelope sender).

Other standard headers
MIME-Version: - This tells the MIME version of the content of this email
Content-Type: - This tells the type of content within the email and the character set used
Content-Transfer-Encoding: - This tells the method used to encode the email for transfer
Message-ID: - This is a unique ID for the email generated by the originating server

X-Headers
Since there a vast number of different servers and services adding their own custom headers to an email during process it is common that custom headers begin with an X to make it easy to sift them out when analyzing the header of an email. These are rarely used by any other system than the one generating them.

Some headers added by WeCloud
X-Scanned-By: WeCloud MailSecurity – This is added by WeCloud on all emails processed
X-MailSecurity-Status: - This shows the overall classification made by WeCloud
X-Virus-Status: - This will show the result of WeCloud's Malware scanning
X-Mailsecurity-Score: - this will show the spam score for the email