

Reading mail headers

RIPE 49

Manchester, September 2004

Rodney Tillotson, JANET-CERT
R.Tillotson@ukerna.ac.uk

Reading message headers

- Why?
- Basics
- Trace information
- True and false
- Headers and anti-spam

Why read message headers?

- Forensics for UBE
 - Information from both true and false lines

Message header basics

- Message format RFC2822
 - header
 - blank
 - body

Minimal header (RFC 2822)

From: Rodney Tillotson <cert@cert.ja.net>
Date: Fri, 17 Sep 2004 12:23:22 +0100

Minimal header (RFC 2821)

Return-Path: <cert@cert.ja.net> (**MAIL FROM:**)
Received: from cert.ja.net (**HELO**)
 (mail1.cert.ja.net [212.219.244.20]) (**TCP**)
 by umhost.ukerna.ac.uk;
 17 Sep 2004 12:25:10 +0100
Message-ID: <20040917094@cert.ja.net>
From: Rodney Tillotson <cert@cert.ja.net>
To: JANET alert <spam-alert@ukerna.ac.uk>
Subject: Header demo
Date: Fri, 17 Sep 2004 12:23:22 +0100

Text of message body

Purpose of the header

- Management
 - Message-ID:
- Hints UA -> UA
 - From:
- Trace
 - Received:
 - write-only for MTAs
- Extensible
 - X-header:

Who writes what?

Return-Path: <cert@cert.ja.net>
Received: from cert.ja.net
 (mail1.cert.ja.net [212.219.244.20])
 by umhost.ukerna.ac.uk;
 17 Sep 2004 12:25:10 +0100
Received: from rt ([192.168.19.84])
 by mail1.cert.ja.net;
 17 Sep 2004 12:25.09 +0100
Message-ID: <20040917094@cert.ja.net>
From: Rodney Tillotson <cert@cert.ja.net>
To: JANET alert <spam-alert@ukerna.ac.uk>
Subject: Header demo
Date: Fri, 17 Sep 2004 12:23:22 +0100

Delivery MTA

Delivery MTA

Relay MTA

Originator MTA

Originator UA

Originator UA

Originator UA

Originator UA

Text of message body

Trace information

- Return-Path:
 - <last MAIL FROM:>
- Message-ID:
 - <...@domain>
- Received:

Received:

- from HELO (PTR [IP])
 - match the one before?
- by MTAname
 - match the one after?
- with product
- id queue-reference

- Varied by products

They may chain together

Received: **from** mail1.norse.ukerna.ac.uk
(hermod.cert [10.10.30.220])
by forseti.cert (Postfix) with ESMTTP id 7FA02287
for <cert@forseti.cert>; **Fri, 17 Sep 2004 00:07:01 +0100** (BST)

Received: **from** rimmer.ja.net (rimmer.ja.net [128.86.8.39])
by mail1.norse.ukerna.ac.uk (Postfix) with ESMTTP id 65396D5EF
for <cert@cert.ja.net>; **Fri, 17 Sep 2004 00:07:01 +0100** (BST)

...

- Received by mail1, received from mail1
- Times identical
- OK so far

They may chain ...

...

Received: **from** rimmer.ja.net (rimmer.ja.net [128.86.8.39])
by mail1.norse.ukerna.ac.uk (Postfix) with ESMTP id 65396D5EF
for <cert@cert.ja.net>; **Fri, 17 Sep 2004 00:07:01 +0100** (BST)

Received: **from** [211.175.107.97] (helo=seoul97)
by rimmer.ja.net with smtp (Exim 3.36 #54) id 1C85JG-00018n-00;
Fri, 17 Sep 2004 00:05:03 +0100

Received: from negra.incatel.pe ([200.148.23.77])
by seoul97 with Microsoft SMTPSVC(5.0.2195.6713);
Thu, 16 Sep 2004 17:03:41 -0600

... or they may not chain

Received: from rimmer.ja.net (rimmer.ja.net [128.86.8.39])
by mail1.norse.ukerna.ac.uk (Postfix) with ESMTTP id 65396D5EF
for <cert@cert.ja.net>; Fri, 17 Sep 2004 00:07:01 +0100 (BST)

(Received: from [211.175.107.97] (helo=seoul97) ...)

(Received: from negra.incatel.pe ([200.148.23.77] ...)

Actually had this:

Received: from [211.175.107.97] (helo=128.86.8.39)
by rimmer.ja.net with smtp (Exim 3.36 #54) id 1C85JG-00018n-00;
Fri, 17 Sep 2004 00:05:03 +0100

X-Message-Info: HC921NF1OUEekgq48pnALXdR354L225diPahjJTJ903

Received: from c-28-2-3-825.TYAQT0.toyota@letterbox.org
([80.110.22.82]) by nca495-gohts110.toyota5@letterbox.org
with Microsoft SMTPSVC(5.0.0046.7846);
Thu, 16 Sep 2004 19:56:54 -0400

Truth and lies

- Who might have written each header line?
- What was their motivation?
 - reports from third parties
- What are you trying to find out?
 - true origin?
 - parties involved?
 - how did it get here?

Last hop

- Possibly under your own management
- Logs
 - IP
 - time
 - HELO/EHLO
 - MAIL FROM:
 - RCPT TO:
- How it entered the delivery domain

Guilty until proved innocent

- Generally work back from the last hop
 - good trust for top Received: line
- Look for a flaw in the next one
 - times don't match
 - IP addresses don't match
(domains and DNS may help)
 - more than one block of Received: lines
- If so, you may already be at the boundary between truth and lies

Lots of matches in honest mail

- Message-ID and originating domain
- Originator address and domain
- Date: and timestamps in Received:
- Timezone and originator address

- Some matches are subjective

Honest but tedious

Return-Path: <name.hidden@bbsrc.ac.uk>

Received: from mail1.norse.ukerna.ac.uk (hermod.cert [10.10.30.220])
by forseti.cert (Posstfix) with ESMTTP id ECF46287
for <cert@forseti.cert>; Fri, 17 Sep 2004 11:10:28 +0100 (BST)

Received: from mhub2.bbsrc.ac.uk (mhub2.bbsrc.ac.uk [149.155.202.2])
by mail1.norse.ukerna.ac.uk (Postfix) with ESMTTP id E58BAD5EF
for <cert@cert.ja.net>; Fri, 17 Sep 2004 11:10:28 +0100 (BST)

Received: from rpe2ksv1.arp.bbsrc.ac.uk ([149.155.202.84])
by mhub2.bbsrc.ac.uk with esmtp (Exim 4.30)
id 1C8FhB-0002Uj-FP for cert@cert.ja.net;
Fri, 17 Sep 2004 11:10:25 +0100

Received: from bobse2ksv1.bobs.bbsrc.ac.uk ([149.155.202.61])
by rpe2ksv1.arp.bbsrc.ac.uk
with Microsoft SMTPSVC(5.0.2195.6713);
Fri, 17 Sep 2004 11:10:25 +0100

Message-ID: <3AED..69FB@bobse2knfr1.bobs.bbsrc.local>

Everything false that can be

Return-Path: <CKALCILS@macmail.com>

Received: from maill.norse.ukerna.ac.uk (hermod.cert [10.10.30.220])
by forseti.cert (Postfix) with ESMTP id 00860287
for <cert@forseti.cert>; Fri, 17 Sep 2004 23:48:54 +0100 (BST)

Received: from kryten.ja.net (kryten.ja.net [128.86.8.29])
by maill.norse.ukerna.ac.uk (Postfix) with ESMTP id E0960D5EF
for <cert@cert.ja.net>; Fri, 17 Sep 2004 23:48:54 +0100 (BST)

Received: from adijon-106-1-24-167.w81-51.abo.wanadoo.fr
([81.51.212.167]) by kryten.ja.net with smtp (Exim 3.36 #54)
id 1C8RWS-0005HP-00; Fri, 17 Sep 2004 23:48:34 +0100

Received: from 181.40.136.82 by 81.51.212.167;
Sat, 18 Sep 2004 04:48:32 +0500

Message-ID: <DXCSKPDWHUBKABEZGMWFCN@fadmail.com>

From: "They cheat " <CKALCILS@macmail.com>

Date: Sat, 18 Sep 2004 01:43:32 +0200

IP address as HELO

Return-Path: <don11@7.arsbank.com>

Received: from maill.norse.ukerna.ac.uk (hermod.cert [10.10.30.220])
by forseti.cert (Postfix) with ESMTP id 6AF8A287
for <cert@forseti.cert>; Fri, 17 Sep 2004 23:39:05 +0100 (BST)

Received: from **212.219.244.220** (unknown [222.101.15.148])
by maill.norse.ukerna.ac.uk (Postfix) with SMTP id 303FFD5EF
for <cert@cert.ja.net>; Fri, 17 Sep 2004 23:39:04 +0100 (BST)

Received: from [136.101.37.46] by 212.219.244.220 with ESMTP
id 61780443; Sat, 18 Sep 2004 02:34:12 +0400

Message-ID: <8\$6-5---\$-4-0o\$98w@xrp8v.xc73>

From: "(non-ASCII)" <don11@7.arsbank.com>

Subject: (non-ASCII)

Date: Sat, 18 Sep 04 02:34:12 GMT

Headers and anti-spam

- Identify UBE
- Identify originating ISP
 - report probable compromise
- Reject complaints
- Hard to automate accurately
- Spurious header lines getting better

Reading message headers

- Examples *ad nauseam*

Reading message headers

- Questions?