

a. A common e-mail worm, which carried an attachment that was infected with the W32.Mimail.A@mm. IP Addresses are not forged. The address admin@psu.edu does not exist.

Received: from f05n09.cac.psu.edu (r02a08.cac.psu.edu [146.186.15.18])
by seawolf.aset.psu.edu (8.9.32.1/8.9.3) with ESMTTP id RAA1400926
for abc123@e-mail.psu.edu>; Tue, 2 Dec 2003 17:28:58 -0500
Received:(from daemon@localhost);by f05n09.cac.psu.edu (8.9.3p2.1/8.9.3)
id RAA36718 for abc123@e-mail.psu.edu; Tue, 2 Dec 2003 17:28:58 -0500
From:admin@psu.edu
Received: from localhost (69-162-40-193.stcgpa.adelphia.net [**69.162.40.193**]);by
f05n09.cac.psu.edu (8.9.3p2.1/8.9.3) with SMTP id RAA134936;
for Tue, 2 Dec 2003 17:28:11 -0500
Date: Tue, 2 Dec 2003 17:28:11 -0500
Message-Id: <200312022228.RAA134936@f05n09.cac.psu.edu>
X-PH:V4.1@f05n09
To: xxx <abc123@psu.edu>;
Reply-To:admin@psu.edu
X-Mailer:The Bat! (v1.61)
X-Priority: 2 (High)Subject: your account anolyypc
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----CEDF5D290026C8C"-----CEDF5D290026C8C
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit Hello there, I would like to inform you about important information
regarding your e-mail address. This e-mail address will be expiring.
Please read attachment for details.
Best regards,
Administrator
ureukouk

The Received: “paragraphs” give information about the three hops of this e-mail’s travel, a simple three step trip, and all of it actually happened. There are no forged Received: lines in this example. e-mail headers are always read from last to first, as the server at each hop adds its own information to the *beginning* of the headers.

This e-mail traveled from a customer of Adelphia Cable, to Penn State, to the person it was addressed to.

TECHNICAL CONCEPT

A word about the timestamps found throughout the headers, which indicate the date, current time, and time zone of each hop. Here is a sample:

Mon, 1 Dec 2003 03:10:09 -0500

The very last part of the timestamp, -0500, is the time difference in hours, from Greenwich Mean Time (GMT), which is indicative of the time zone at the location of the hop. In the Eastern Time Zone, we are -0500 during Eastern Standard Time, and -0400 during Eastern Daylight Time. In the Pacific Time Zone, they are at -0800 during Pacific

Standard Time, and -0700 during Pacific Daylight Time. (three hours behind Eastern Time) In e-mail from the United Kingdom, you will see -0000 or GMT/[UTC](#), from Japan you will see +0900.

Under most Internet traffic conditions, it only takes a couple of seconds to move from one hop to the next, even if an e-mail travels a great physical distance. The time an e-mail takes to travel one hop *within* a 100 MBS network, can be measured in milliseconds.

Time zone information may help you to pick out the bogus Received: lines in e-mail headers, when determining the portions of the headers that have been forged. For example if the Received from: entries are several hours apart, have the wrong time zone, or non-sequential date/time.