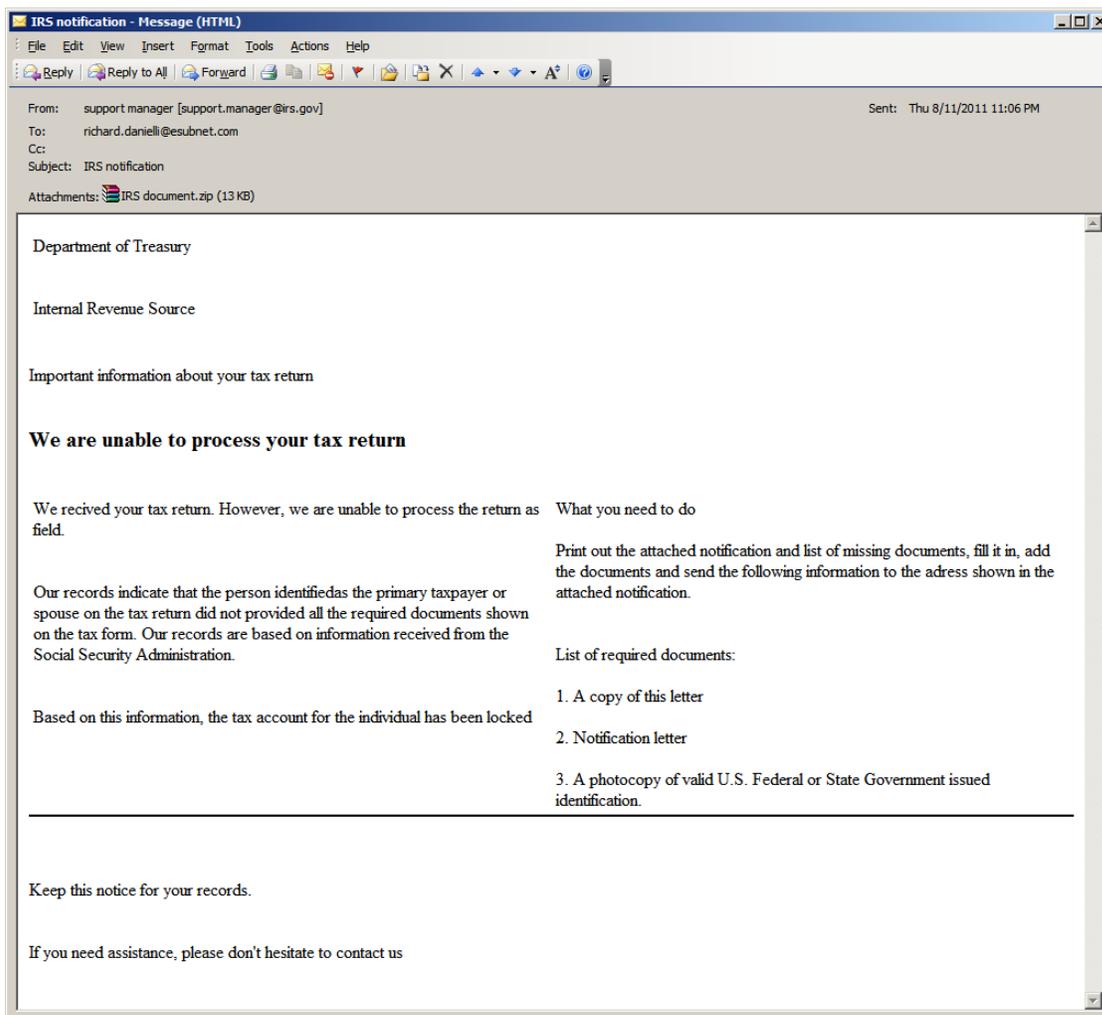eSubnet

Dissecting Malware Email
Understanding how to identify bad email
By: Richard Danielli, President - eSubnet

The email example I'm using for this paper recently arrived in my inbox. While I knew it was likely to include malware, I wanted to review the current practices of those who send malware out. This paper provides information on identifying email which may be bad and signs to watch out for.

Below is an image of the example email I opened:

IRS notification - Message (HTML)

File   Edit   View   Insert   Format   Tools   Actions   Help

Reply | Reply to All | Forward

From: support manager [support.manager@irs.gov]   Sent: Thu 8/11/2011 11:06 PM
To: richard.danielli@esubnet.com
Cc:
Subject: IRS notification
Attachments: IRS document.zip (13 KB)

Department of Treasury

Internal Revenue Source

Important information about your tax return

We are unable to process your tax return

We recived your tax return. However, we are unable to process the return as field.

Our records indicate that the person identifiedas the primary taxpayer or spouse on the tax return did not provided all the required documents shown on the tax form. Our records are based on information received from the Social Security Administration.

Based on this information, the tax account for the individual has been locked

What you need to do

Print out the attached notification and list of missing documents, fill it in, add the documents and send the following information to the adress shown in the attached notification.

List of required documents:

1. A copy of this letter

2. Notification letter

3. A photocopy of valid U.S. Federal or State Government issued identification.

Keep this notice for your records.

If you need assistance, please don't hesitate to contact us

1. What's Interesting Here

On first glance there are a number of key items wrong with this email. The table below mentions just the most obvious ones. I'm going to move from top to bottom:

Item	Problem
From: Address	• support.manager@irs.gov: This is called a ROLE address, an address which does identify a person but rather a business function. While role addresses are commonly used, they are usually used for receiving emails rather then sending. When they are used for sending, "no-reply" is typically included in the address as well.
To: Address	• richard.danielli@esubnet.com: I occasionally change my email address to avoid spam, and this one is out of date. The pattern firstname.lastname@ hasn't been in use for years at eSubnet. So I can quickly suspect spam for this reason alone.
Subject: line	• IRS Notification: I noticed this giveaway first. There should be a case or file number mentioned, but there isn't. Check with the IRS to see: http://www.irs.gov/ • When you have initiated contact, their response will include a case or file number in the Subject: line. • Many systems attach the case number to the subject line for easier reference. This allows the pseudo-automated response system to direct the email to the right recipient and allows the recipient to more easily manage their messages.
Email Body	• While my name is in the To: field, my name is absent from the message body. Showing that this is not personalized for me alone. • IRS stands for "Internal Revenue Service" **NOT** "Internal Revenue Source". • The spelling while correct still doesn't hold up to scrutiny. The sentence "*we are unable to process the return as field.*" Should probably have read, "we are unable to process the return as filled". • The email speaks of an attached letter which is attached in .ZIP format. If it is simple a letter it should have been a .PDF or at worst a .DOC • The email suggests that if there is a need for assistance to contact the IRS, but no contact information is given. • I'm a Canadian citizen and have no dealings with the American Internal Revenue Service
Attachment	It is a .ZIP file from someone I don't know or trust.

To sum up, an official document should be addressed to me in the body of the letter. It should have contact information and one would expect some sort of case number. And, in this case, the IRS clearly states that they will not initiate contact in the first place. Their website http://www.irs.gov/ says that it is the policy of the IRS to never initiate contact via email.

This "no initial contact" policy has become standard practice for many institutions that hold Personal Identifiable Information and Financial Information on the general public.

2. Something More Interesting

The public is starting to learn to dig a little deeper before opening an email attachment. One way of checking things out is to look at the path the email has traveled. This is done by looking at what IT professionals call email *headers*. Below I've displayed the email header for our example email.

```
Return-Path: <support.manager@irs.gov>
Received: from oxmail.esubnet.com ([unix socket])
        by oxmail.esubnet.com (Cyrus v2.2.12-Invoca-RPM-2.2.12-8.1.RHEL4) with
LMTPA;
        Thu, 11 Aug 2011 07:11:31 -0400
X-Sieve: CMU Sieve 2.2
Received: by oxmail.esubnet.com (Postfix, from userid 99)
        id DB5CE34E6A5; Thu, 11 Aug 2011 07:11:31 -0400 (EDT)
X-Spam-Checker-Version: SpamAssassin 3.1.9 (2007-02-13) on oxmail.esubnet.com
X-Spam-Level: ***
X-Spam-Status: No, score=3.4 required=3.9 tests=DATE_IN_FUTURE_12_24,
        EXTRA_MPART_TYPE,HTML_FONT_BIG,HTML_MESSAGE,UPPERCASE_25_50 autolearn=no
        version=3.1.9
Received: from mailgate.esubnet.com (mailgate.esubnet.com [xxx.xxx.x.xx])
        by oxmail.esubnet.com (Postfix) with ESMTP id 41BDE34E69A
        for <rdanielli@oxmail.esubnet.com>; Thu, 11 Aug 2011 07:11:29 -0400 (EDT)
Received: from vela.com (localhost [113.168.240.46] (may be forged))
        by mailgate.esubnet.com (8.13.8/8.13.8) with ESMTP id p7BBBL1i009075
        for <richard.danielli@esubnet.com>; Thu, 11 Aug 2011 07:11:22 -0400
Received: from irs.gov ([199.196.144.6]) by 113.168.240.46; Fri, 12 Aug 2011
10:05:49 +0700
Message-ID: <000e01cc589c$bca56480$2ef0a871@irs.gov>
From: "support manager" <support.manager@irs.gov>
To: <richard.danielli@esubnet.com>
Subject: IRS notification
Date: Fri, 12 Aug 2011 10:05:49 +0700
MIME-Version: 1.0
Content-Type: multipart/related;
        type="multipart/alternative";
        boundary="----=_NextPart_000_0006_01CC589C.BCA56480"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2314.1300
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2314.1300
X-Greylist: Delayed for 00:01:46 by milter-greylist-3.0 (mailgate.esubnet.com
[xxx.xxx.x.xx]); Thu, 11 Aug 2011 07:11:24 -0400 (EDT)
```

2.1. Analyzed

The email header contains the path that the email took from start to finish showing every server it touched along the way. Each server identifies itself and announces where the mail arrived from. The path is identified in the email header by the "Received: from" lines and is read from bottom to top.

What makes this email very interesting is the last "Received: from" line shown below.

```
Received: from irs.gov ([199.196.144.6]) by 113.168.240.46; Fri, 12 Aug
2011 10:05:49 +0700
```

The IP address 199.196.144.6 actually does belong to the US Department of the Treasury. Though there is no local host name associated to the IP address. This is not probable in a network as complicated as the one belonging to the US Department of the Treasury.

The earlier "Received: from" line is the dead giveaway for malware.

```
Received: from vela.com (localhost [113.168.240.46] (may be forged))
      by mailgate.esubnet.com (8.13.8/8.13.8) with ESMTP id p7BBBL1i009075
```

The IP address 113.168.240.46 belongs to the Vietnam Post and Telecom Corporation and I suspect that the US Treasury is never going to be sending emails from the Socialist Republic of Vietnam.

Besides the common-sense review of the content of the email the path the email itself tells us it followed is suspicious.

2.2. How is this possible

IP addresses are configurable by the owner of the computer system. In fact, we can also set the domain name server (DNS). Fiddling with these two things allows the sender to report anything. Fortunately, since so much of how the Internet works is open to inspection, the malware sender can hide everything.

This network diagram shows what's involved in forging the route of an email.

Drawing 1

The table below shows the components in the network diagram above.

Label	Description
B1	Computer used to send out spam has an IP address of 199.196.144.6 network. Email program is configured to send mail to the IP address of B2
B2	Mail Transport Agent (MTA) and Internet connection manager for source of SPAM network. Has forward and reverse DNS entries for 199.196.144.0 network. Outside address of 113.168.240.46
G1	eSubnet Firewall - outside to DMZ
G2	eSubnet MTA – mailgate.esubnet.com has spam filtering technologies. This is the primary MX record.
G3	eSubnet MTA – relay.esubnet.com has spam filtering technologies. This is the secondary MX for backup
G4	eSubnet firewall – DMZ to inside
G5	eSubnet email server located securely inside the network

We can trace the email from source to destination. We can see that it started out on one of the internal computers at the bad guy's network, say B1, and we can trace the path through to the good guy's network, in this case, eSubnet.

3. How You Can Help

The first step in helping your organization remain malware free is to pay attention to the emails you open, especially those with attachments.

1. Look at the sender address: does it make sense that you would be receiving the email from this sender?
2. Look at the message body: do the words make sense, and while they may be spelled correctly, are they the correct words within the context?
3. Look at the headers: In Microsoft Outlook 2003 the headers are available for an email under View and then select Options. In Outlook 2010 you must first open the email and the find View and select Options.
4. Your IT department needs these headers to diagnose problems, just as I did above with the example email. Include them in any email you forward to the helpdesk.
5. **Do not open the attachment.**

By remaining vigilant, curbing your curiosity and being just a little paranoid you can help to protect the safety and integrity of your firm.

Richard Danielli
President, eSubnet