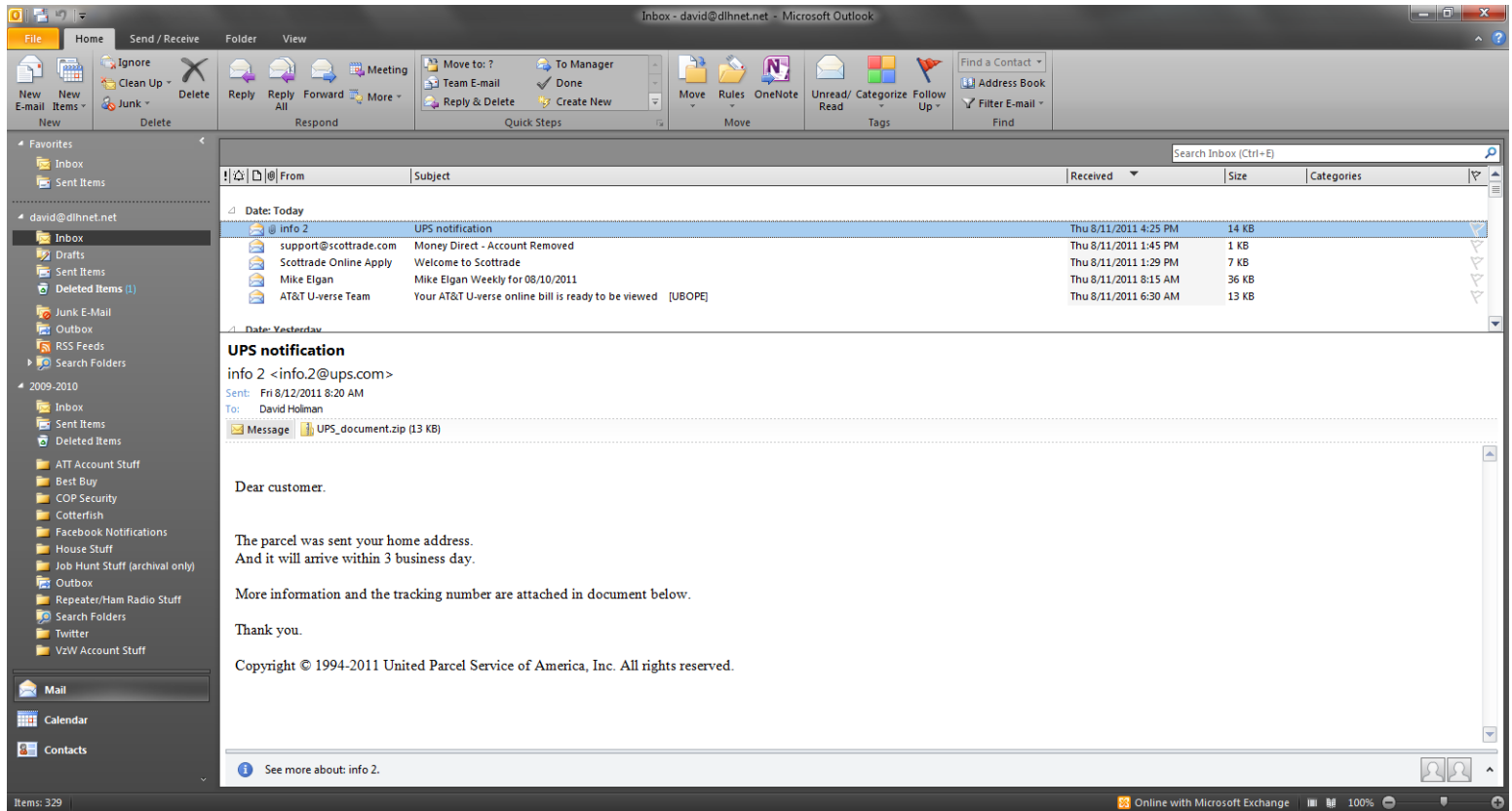
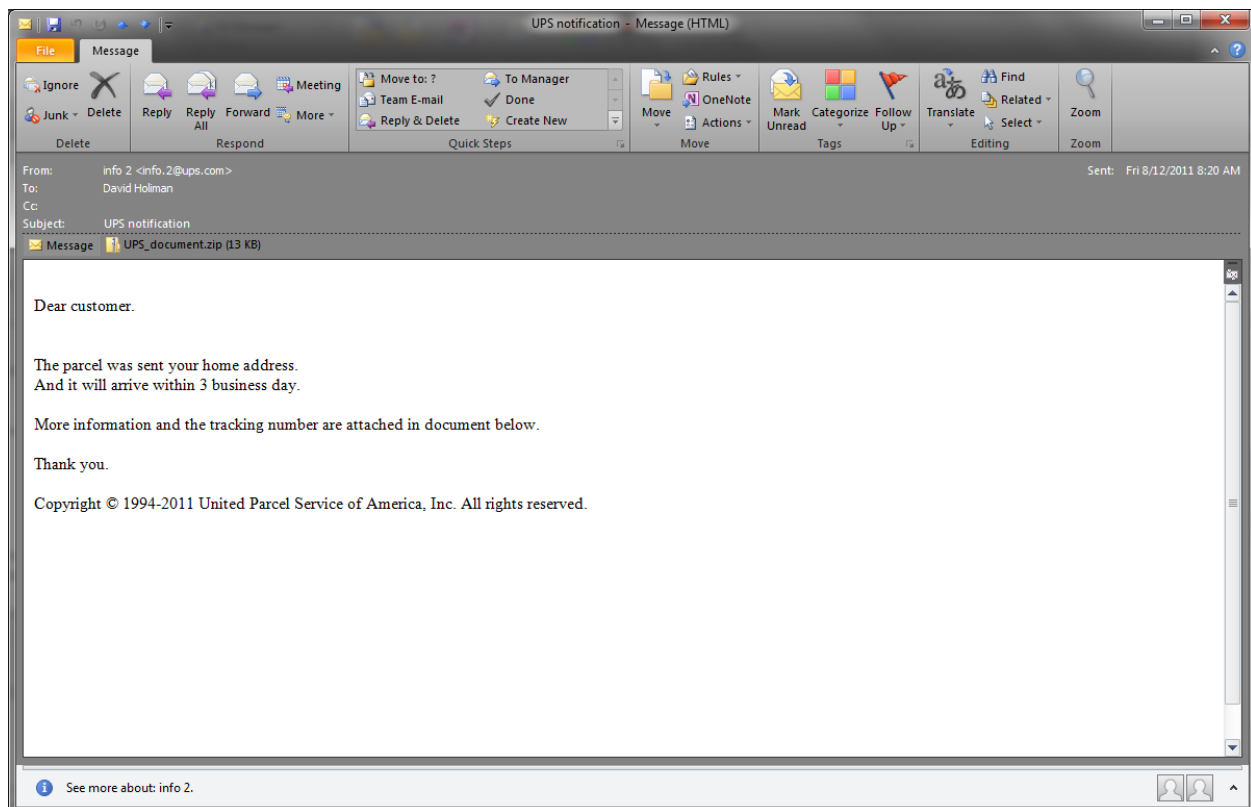


Anatomy of an E-mail Threat

I got this little gem (below) in my inbox today at home and, rather than just deleting it, I thought I'd do a little write up for the benefit of my friends and colleagues in the IT world.

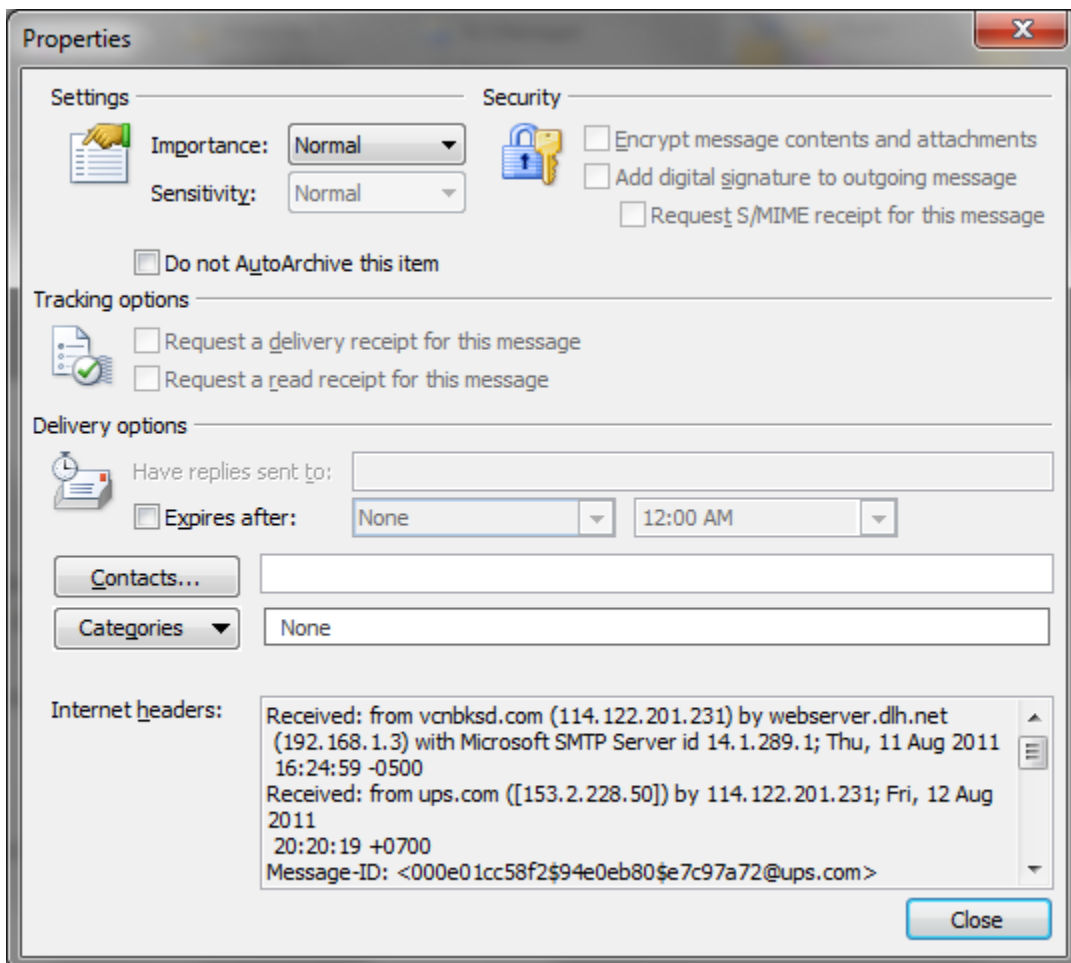


Seems fishy anyway, even at first glance, doesn't it? Let's look deeper. If you're using Outlook for your corporate or personal e-mail, double click on the message to open it in its own window...



Still looks fishy. How can you tell? First – let’s make some assumptions. UPS is a pretty big company and they’ve been around a long time. Large companies usually spellcheck and grammar check their correspondence. Note some obvious errors in the image above: “The parcel was sent your home address.” “And it will arrive within 3 business day.” (*sic*) Shouldn’t those read: “The parcel was sent TO your home address.” “It will arrive within three business dayS.” Or, heck, I personally would combine it into one sentence: “The parcel was sent to your home address and will arrive within three business days.”

Now, another assumption. UPS tracks their packages by tracking number. True, this e-mail says you can get the tracking number in the attachment (and we’ll look at that a bit later). But, in the past, I’ve seen real UPS correspondence with either the tracking number in the body of the message and/or a link to the tracking information on their website. Looks even more fishy now...so let’s go in a bit more. If you have Outlook 2007/2010 and you have the message up in its own window, click on File and then click the button for Properties at the bottom of the window. The following will appear...



We’re only interested in the Internet headers section at the bottom. This helps us determine the path the message took through the Internet to get to our inbox. According to the headers, the last stop this message took before hitting my Exchange server was at a server (114.122.201.231) in the “vcnbksd.com” domain. Network admins, now’s the time to use some of those tools in your toolkit! Whois is my first choice here to find out information about the domain names in question...

```
C:\Windows\system32\cmd.exe

C:\Users\dholiman\Downloads>whois vcnbksd.com

Whois v1.01 - Domain information lookup utility
Sysinternals - www.sysinternals.com
Copyright (C) 2005 Mark Russinovich

Connecting to COM.whois-servers.net...
No whois information found.

C:\Users\dholiman\Downloads>_
```

Whois has no information on that domain. Obviously, ups.com would turn up something since it IS a valid domain:

```
C:\Windows\system32\cmd.exe

Connecting to COM.whois-servers.net...
No whois information found.

C:\Users\dholiman\Downloads>whois ups.com

Whois v1.01 - Domain information lookup utility
Sysinternals - www.sysinternals.com
Copyright (C) 2005 Mark Russinovich

Connecting to COM.whois-servers.net...
Connecting to whois.ascio.com...

The data in Ascio Technologies' WHOIS database is provided
by Ascio Technologies for information purposes only. By submitting
a WHOIS query, you agree that you will use this data
only for lawful purpose. In addition, you agree not to use the data to:
(a) allow, enable, or otherwise support the transmission by e-mail,
telephone, or facsimile of mass, unsolicited, commercial advertising
or solicitations to entities other than the data recipient's
own existing customers; or
(b) enable high volume, automated, electronic processes that
send queries or data to the systems of any Registry Operator
or ICANN-Accredited registrar, except as reasonably necessary
to register domain names or modify existing registrations.
Ascio Technologies reserves the right to
modify these terms at any time. By accessing and using
Ascio Technologies WHOIS information, you agree to these terms.

NOTE: FAILURE TO LOCATE A RECORD IN THE WHOIS DATABASE IS NOT
INDICATIVE OF THE AVAILABILITY OF A DOMAIN NAME.
Registrant:
United Parcel Service <UNITE56638>
340 MacArthur Blvd
Mahwah, NJ, 07430
US
Domain name: ups.com

Technical contact:
Administrator, Domain (D0515504)
NetNames Hostmaster
3rd Floor Prospero House
241 Borough High Street
Borough, London, SE1 1GA
GB
corporate-services@netnames.com
+44.2070159370 Fax: +44.2070159375

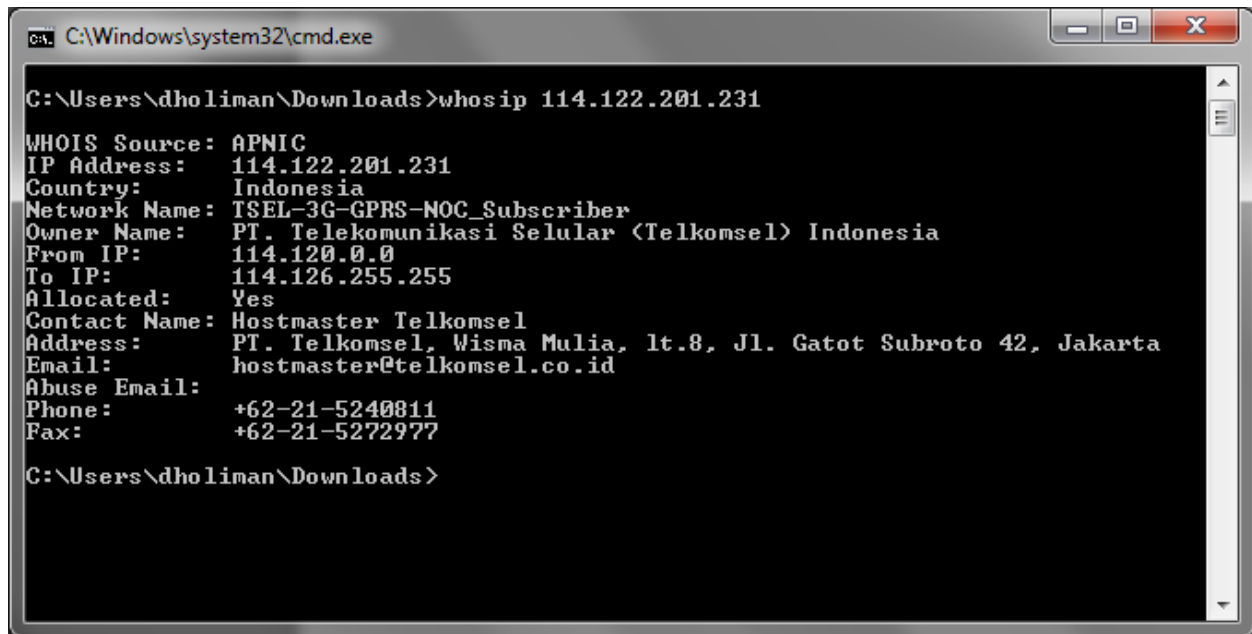
Administrative contact:
Hostmaster, UPS (UH72110)
United Parcel Service
340 MacArthur Blvd
Mahwah, NJ, 07430
US
internet@ups.com
+1.2018282480 Fax: +1.2018284895

Record created: 2011-02-14 00:05:58
Record last updated: 2011-05-05 04:26:56
Record expires: 2011-10-31 00:00:00

Domain servers in listed order:
CBRU.BR.NS.ELS-GMS.ATT.NET <CBRUB93658>
CHTU.NI.NS.ELS-GMS.ATT.NET <CHTUN93658>
NS1-AUTH.SPRINTLINK.NET <NS1A066415>
```

OK, great. So domain names alone aren't going to do anything for us. Now we need to look at IP addresses. Look back at the message properties window...now we're going to concern ourselves with the IP addresses listed in the headers.

Another useful tool is the American Registry for Internet Numbers (ARIN) website. They have a whois tool similar to the domain whois tool. The ARIN whois tool shows you information regarding to whom a block of IP addresses belongs. Let's start at the last hop (114.122.201.231). My "whosip" command line tool shows the following:



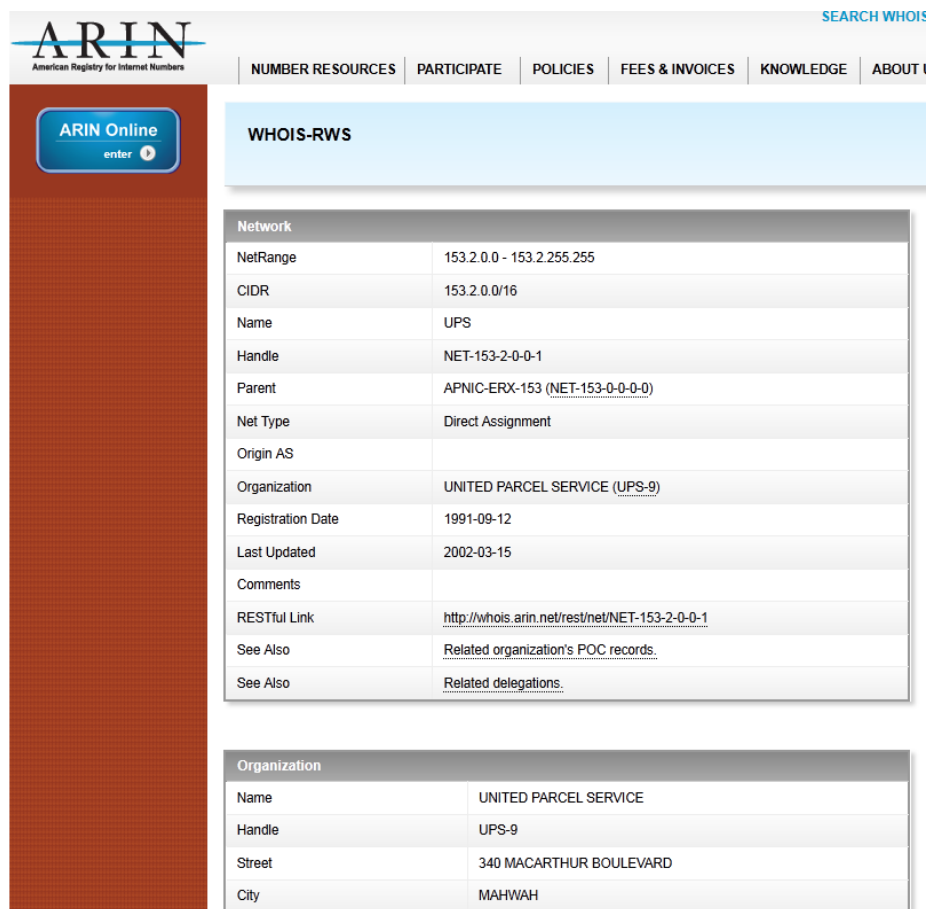
```
C:\Windows\system32\cmd.exe

C:\Users\dholiman\Downloads>whosip 114.122.201.231

WHOIS Source: APNIC
IP Address: 114.122.201.231
Country: Indonesia
Network Name: TSEL-3G-GPRS-NOC_Subscriber
Owner Name: PT. Telekomunikasi Selular (Telkomsel) Indonesia
From IP: 114.120.0.0
To IP: 114.126.255.255
Allocated: Yes
Contact Name: Hostmaster Telkomsel
Address: PT. Telkomsel, Wisma Mulia, lt.8, Jl. Gatot Subroto 42, Jakarta
Email: hostmaster@telkomsel.co.id
Abuse Email:
Phone: +62-21-5240811
Fax: +62-21-5272977

C:\Users\dholiman\Downloads>
```

This is useful in that it lets us know which part of the world that e-mail came from. In this case, it came from a mobile device in Indonesia; possibly either a smartphone or a computer connected to the Internet via tethering or a USB "modem." The 'Network Name' and 'Owner Name' fields help in determining that. Next, let's look at the other IP (153.2.228.50) using the whois.arin.net website:



ARIN Online enter

SEARCH WHOIS

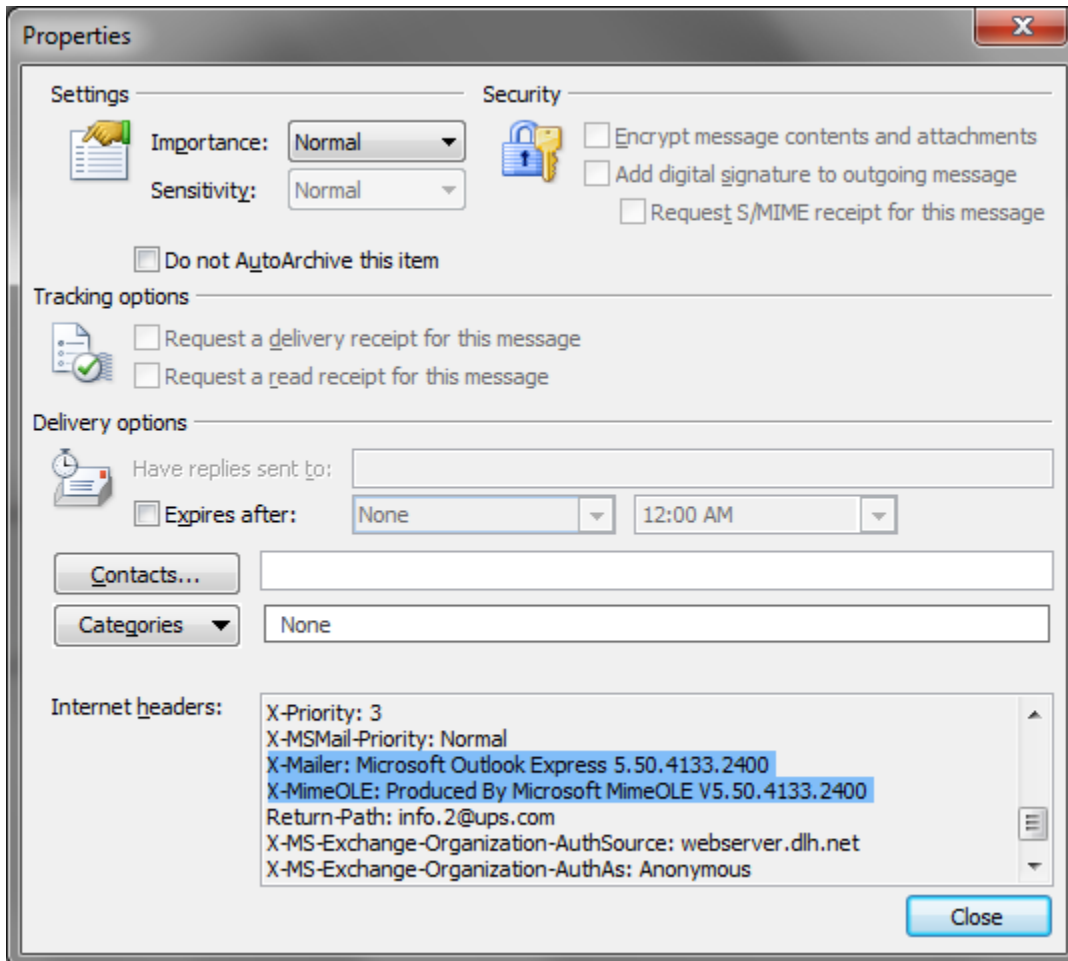
NUMBER RESOURCES PARTICIPATE POLICIES FEES & INVOICES KNOWLEDGE ABOUT I

WHOIS-RWS

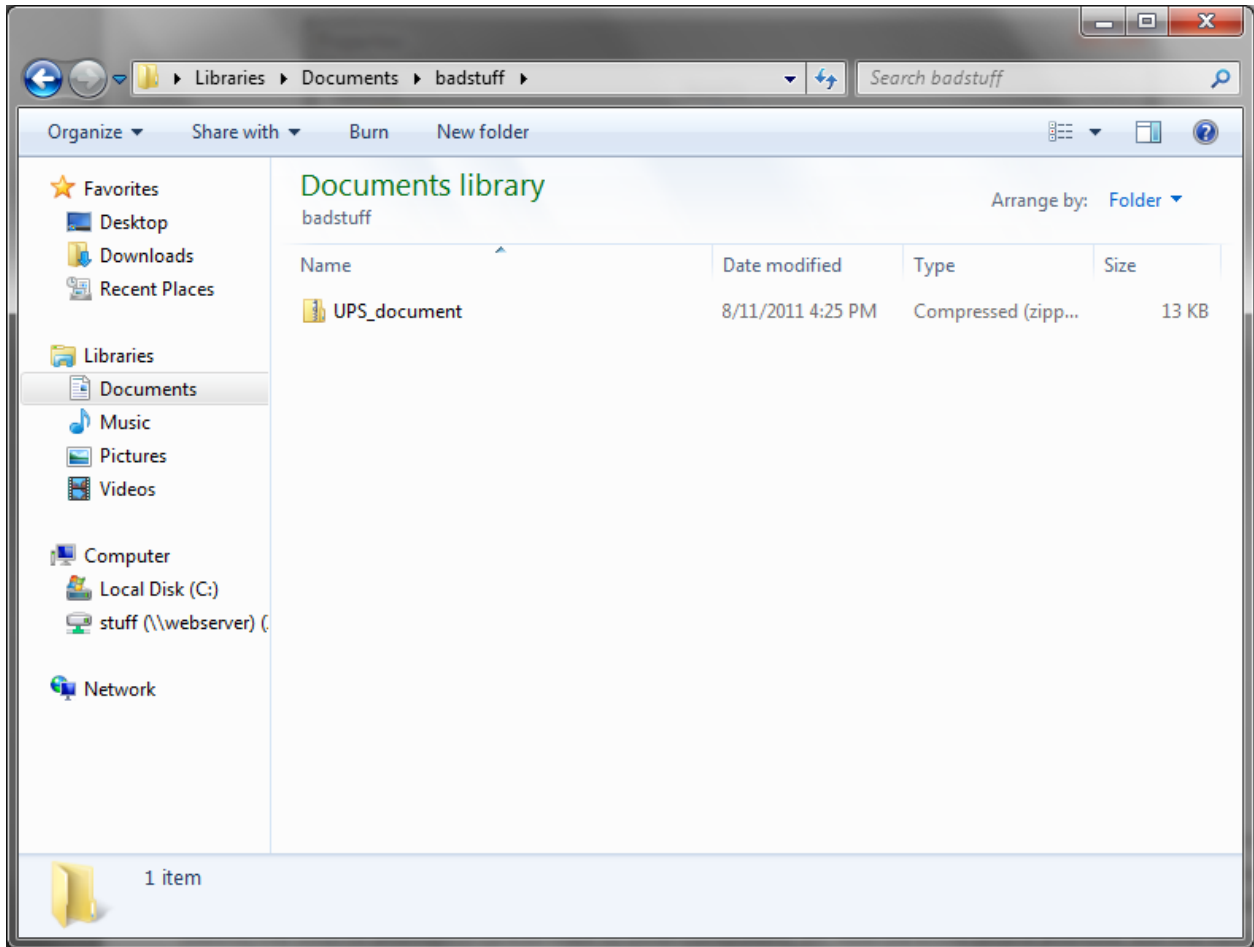
Network	
NetRange	153.2.0.0 - 153.2.255.255
CIDR	153.2.0.0/16
Name	UPS
Handle	NET-153-2-0-0-1
Parent	APNIC-ERX-153 (NET-153-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	UNITED PARCEL SERVICE (UPS-9)
Registration Date	1991-09-12
Last Updated	2002-03-15
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-153-2-0-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

Organization	
Name	UNITED PARCEL SERVICE
Handle	UPS-9
Street	340 MACARTHUR BOULEVARD
City	MAHWAH

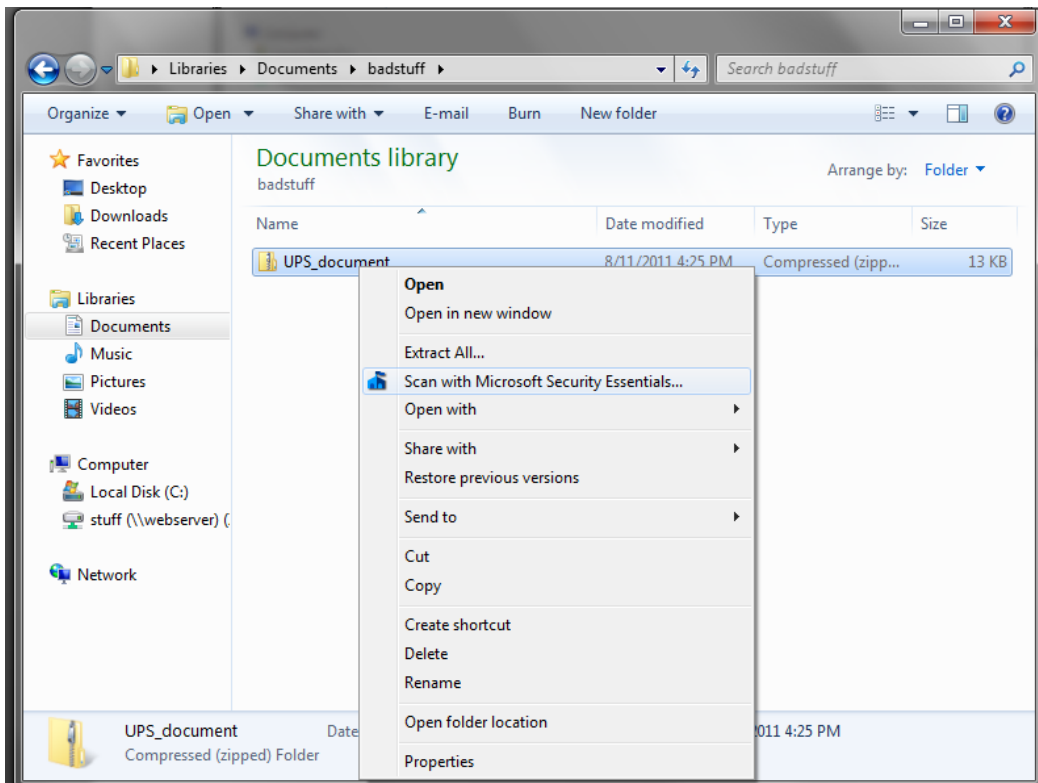
It looks like 153.2.228.50 is, indeed, owned by UPS. One of two things has happened to make that e-mail come to me. Either a workstation somewhere in UPS' network has been compromised with a virus/malware and made that infected computer into a mini e-mail server OR the message came (still) from a virus-infected, compromised computer somewhere in the Internet and the IP address has been spoofed somewhere along the line, making it appear to have come from UPS' network. I'm almost willing to bet on the latter but it is entirely possible that the first event could have happened. Let's scroll down a bit in those headers:

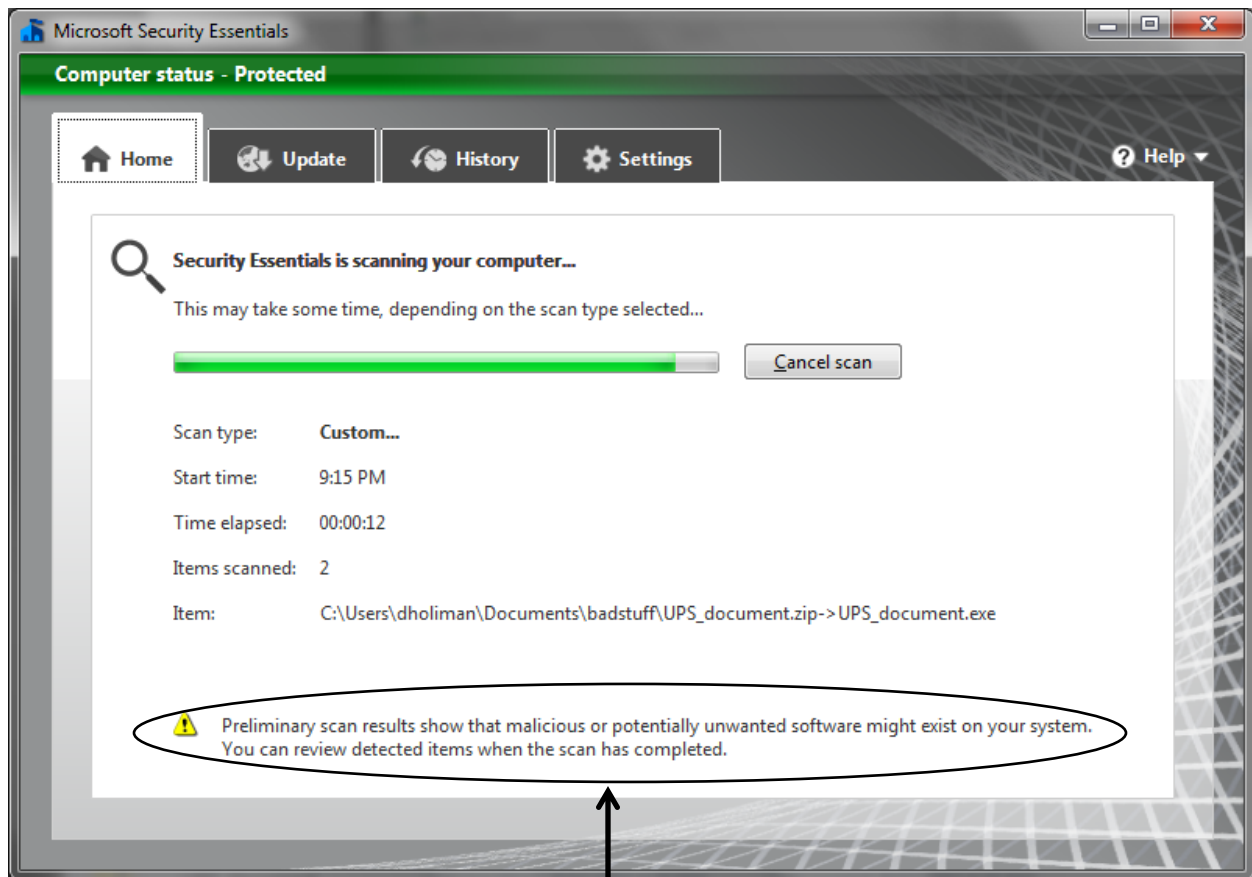


The highlighted text shows us which e-mail program sent the message. In this case, it is a VERY old version of Microsoft Outlook Express, included with Windows Millenium Edition (circa 2000 – yikes!) and Windows 2000. It is a safe bet, now, that a computer somewhere in the Internet (most likely in Indonesia) has been infected by a virus and is being used by the virus to attempt to spread itself to other computers. So, now we know where and how, but the next question is what. Let's look at the payload/attachment that was sent along with the message...

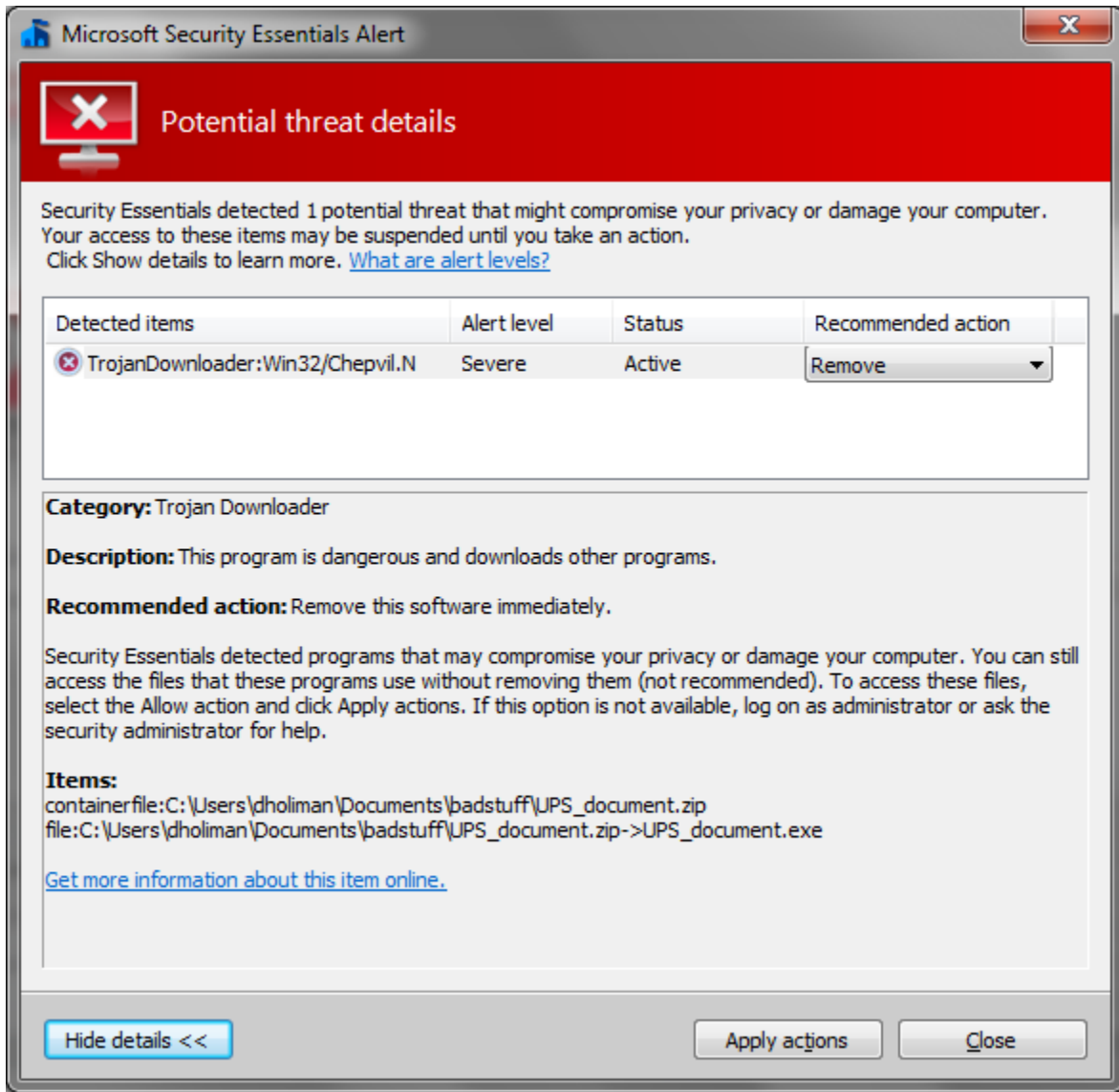


I've saved the file and placed it in a folder in my Documents library called "badstuff" and now I can open it OR, even better (read: safer) yet, run a quick virus scan on it.

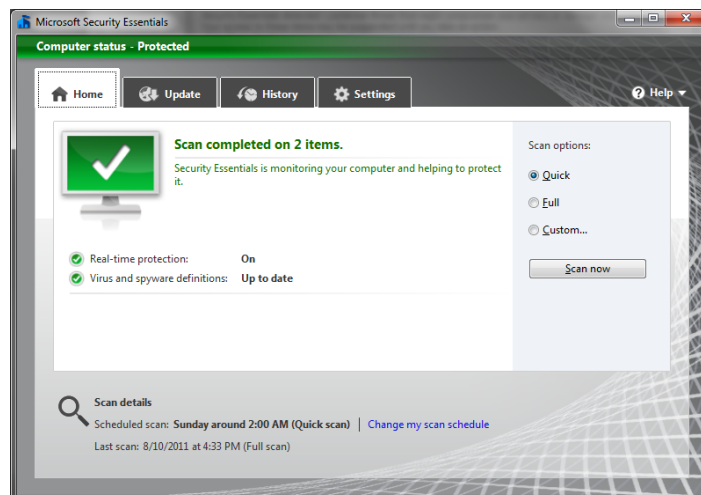




Yes, definitely "badstuff" for sure. I let the scan finish...



We'll definitely remove this baddie right now. I never unzipped the files and/or ran them, so I was never at risk. Most modern anti-virus software programs will scan inside compressed (.zip) files and the files contained therein.



All is well again.

That pretty much takes us through a “bad” e-mail from header to attachment, demonstrating the fact that if you either don’t know the sender, weren’t expecting the message, or have a gut feeling that it’s bad, just DELETE THE MESSAGE!

Speaking of that, I think I’ll do that to this particular message right now...