X-Mozilla-News-Host: supernews.sonic.net
Message-ID: <4862AA74.2000804@elvey.com>
From: Matthew Elvey <matthew@elvey.com>
To: Matthew Elvey <matthew@elvey.com>
Subject: All 42 Ameritrade leaking email addresses to Sniffex pump n dumper? posts, from supernews.
Content-Type: multipart/mixed;
 boundary="------------070309010004030400030507"

This is a multi-part message in MIME format.
--------------070309010004030400030507
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

This is simply a compilation for legal filing. It contains the full postings, exactly as they appear in the archive (except for the use of **bold** to highlight portions of it**), including the (largely useless) headers, of an Internet news thread.**
It contains all 42 posts to the "Ameritrade leaking email addresses to Sniffex pump n dumper?" thread on USENET's news.admin.net-abuse.email (AKA n.a.n-a.e or nanae) newsgroup.
For convenience, it is suggested that readers simply go to http://snurl.com/amtd2005 to view this thread instead, in a much more readable format. It is available from any of the many USENET servers that store nanae for long enough.)
I believe it is the first public discussion of the email breach. Since then there have been dozens of other Internet-based discussions, on USENET and elsewhere, which make clear (by including copies of its correspondence) Ameritrade's knowledge of conclusive evidence both that criminals had ongoing access to its customer database and that criminals were actively abusing it on an ongoing basis.
AmeritradeCases.txt (not included) has the censored posts; they're from the 2007 "Another Ameritrade break-in" thread.
-Matthew

--------------070309010004030400030507
Content-Type: text/x-moz-deleted; name="Deleted: AmeritradeCases.txt"
Content-Transfer-Encoding: 8bit
Content-Disposition: inline; filename="Deleted:AmeritradeCases.txt"
X-Mozilla-Altered: AttachmentDeleted; date="Wed Jun 25 13:34:54 2008"

The original MIME headers for this attachment are:
Content-Type: text/plain;
 name="AmeritradeCases.txt"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
 filename="AmeritradeCases.txt"

--------------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

<HR WIDTH="90%" SIZE=4>
Path: number1.nntp.dca.giganews.com!local01.nntp.dca.giganews.com!nntp.comcast.com!
news.comcast.com.POSTED!not-for-mail
NNTP-Posting-Date: Mon, 31 Oct 2005 12:39:16 -0600
From: "User N" <usern@invalid.invalid>
Newsgroups: news.admin.net-abuse.email
Subject: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Mon, 31 Oct 2005 13:39:26 -0500
MIME-Version: 1.0
Content-Type: text/plain;
	format=flowed;
	charset="Windows-1252";
	reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2900.2670
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2670
Message-ID: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
NNTP-Posting-Host: 69.142.47.32
X-Trace: sv3-PlQO88RZxIsAlhpeBUnv0CAtrAg7KC6S0iWbzaQWwEDBVcH0+kj7mzY40KCgJ5T5U0wR5Gxxqj7rx1R!ABXRkCOPKwQ47cZ
+fdf2i3dzEwjVPOuvilmaQAXl/WGjDUljZdzT62ubNh6Zp3cWPFt0JHSlhoGQ!pF0=
X-Complaints-To: abuse@comcast.net
X-DMCA-Complaints-To: dmca@comcast.net
X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your complaint properly
X-Postfilter: 1.3.32
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160765

I create unique, "private" email addresses for every company I submit my email address to. This morning I hooked something. The following UBE was sent to

an email address that was only given to Ameritrade. I checked two of my more public/exposed email addresses and neither of them received the UBE. I know someone else who has an Ameritrade account and asked them if they received the same UBE.... they did. It was sent via a different path and some header fields are rotated, but otherwise it is identical and it was sent within a few minutes of mine.

Did anyone else receive a copy sent to an Ameritrade-unique email address? Did anyone receive a copy sent to an email address NOT given to Ameritrade?

Return-Path: <XXXXXX@XXXXXXX.com>
Received: from thesdsl-00982.otenet.gr (thesdsl-00982.otenet.gr [87.202.131.220])
by XXXXXXXX.com (8.11.6/8.11.6) with SMTP id XXXXXXXXXXX
for <XXXXXXXXX@XXXXXXXXXX.com>; Mon, 31 Oct 2005 01:47:55 -0700
Received: from 198.31.167.53 (EHLO Leanne) (unknown)
by thesdsl-00982.otenet.gr with SMTP; Thu, 13 Oct 2005 09:05:09 -0700
Message-Id: <10351.17737.4361559603@thesdsl-00982.otenet.gr>
To: XXXXXXXXXX@XXXXXXXXX.com
From: Demetrius <XXXXXXX@XXXXXXXX.com>
Date: Sun, 30 Oct 2005 22:45:04 +0200
Subject: Market Headlines

This will be the hottest Issue of NOvember
- Keep reading to see why

Are you tired of Public Companies without
anything substantial backing their story -
how about a revolutionary invention that
will change the Security Industry forever!
Sniffex inc (SNFX) a company so hot that
everybody from Homeland Defense to United
Nations , Unicef and Embassies wants its
breakthrough Anti-Terror product!!

Breaking News: Sniffex, Inc. Announces New
Representation in 11 Countries

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340%
UP

Ground Breaking News (Friday after the
close): Sniffex, Inc. Announces New
Representation in 11 Countries

You see SNFX has plugged perhaps the
biggest hole in the global fight against
terror and their device can perform
accurate and fast Explosive Detection from
distance over 30-100 feet!!

Sniffex makes pocket-sized, hand held
explosive detection device. It operates
through its ability to detect Nitro
Dioxide and Nitro Trioxide ions (the free
radicals around the explosive). This
unique technology allows the device to
penetrate and locate even small amounts of
explosives even behind concrete walls or
metal obstacles, inside cars airplanes or
buses from 10-100 feet away! This device
does not SNIFF (inhale) the air, it uses
the magnetic forces of the ions tens of
feets away!! The magnetic field of the
Earth is present everywhere so this device
works EVERYWHERE and thats why walls or

metal shields cannot stop it from showing where the BAD GUYS are hiding!

This device is so powerful that it can sniff the traces of gunpowder left in gun barrel from 10-20 feet even if you hide it behind wall or put the barrel in your car! ITS SO SENSITIVE

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340% UP

Who is client of Sniffex?? - the company began its activity in June 2005 and started making its first sales in August and September and since then its clients include United Nations and Unicef in Lebanon, Saudi Arabia Embassy even one Mercedes Benz dealership bought the device to protect its premises. Just Read the news from Friday to learn about recent sales of the company.

The Market for device like sniffex is HUUGGGEEEE!!! From Middle East to London , Bali and USA the global threat of terror makes this device a MUST for every building or checkpoint in public transport. Even countries and places that have not been victim of bomb attacs should use Sniffex.

NOW HERE COMES THE BEST PART OF THE STORY - the other companies in the business who produce explosive detection devices, they need to be in almost full contact with the explosive to locate it, a normal sniffer or Xray machine they work from 1-2 feet away, the K9 dogs can sniff from 1-2 feet also, but SNIFFEX can work from up to 100 feet and find any traces of Nitro Dioxide which is the component of 90% of all explosives.

SO SNFX is ahead of the competition!!!

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340% UP

NEWS : -----) Sniffex, Inc. Announces New Representation in 11 Countries

IRVING, Texas, Oct 28, 2005 /PRNewswire-FirstCall via COMTEX/ -- Sniffex, Inc. (OTC Pink Sheets: SNFX) ("Sniffex"),

producers of Sniffex, an explosive detection device, announced today the signing of two new representatives that will sell Sniffex Inc. in Portuguese speaking countries in Africa and South America as well as in the Philippines and Malaysia. 11 new countries will be represented by these two agreements. The two new representatives are WinWealth Ltd. Corp., headquartered in Hong Kong, and Chelworth Investment LTD, headquartered in Lisbon, Portugal. The company stated that an initial order has been received from these relationships and that the Representatives have already invested significant resources to market Sniffex in their areas.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!local01.nntp.dca.giganews.com!nntp.megapath.net!news.megapath.net.POSTED!not-for-mail
NNTP-Posting-Date: Mon, 31 Oct 2005 15:12:33 -0600
X-newsreader: xrn 9.02
X-Sender: murray@glypnod (Hal Murray)
From: hmurray@suespammers.org (Hal Murray)
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Newsgroups: news.admin.net-abuse.email
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
Message-ID: <ys6dnaJ-_o5cFfveRVn-hA@megapath.net>
Date: Mon, 31 Oct 2005 15:12:33 -0600
NNTP-Posting-Host: 64.139.1.69
X-Trace: sv3-Nmwxn6OORKn6DwyWvzz8irEq7VBitXxTeHWRHnqoZ6jqZp+1XTWekyCI3YNxReWF5urCtnovfz4Dx47!0wCt4MdLAxx/
78orwa8VKjpUU0/ZhHh2cbzX6iMhWVNwsFHgw1AIk0u2Fzyx3kb5BtnVboO83YU=
X-Complaints-To: abuse@megapath.net
X-DMCA-Complaints-To: abuse@megapath.net
X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your complaint properly
X-Postfilter: 1.3.32
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160779

> Did anyone receive a copy sent to an email address NOT given to Ameritrade?

I got two back in June/July. Samples in NANAS.

--
The suespammers.org mail server is located in California. So are all my
other mailboxes. Please do not send unsolicited bulk e-mail or unsolicited
commercial e-mail to my suespammers.org address or any of my other addresses.
These are my opinions, not necessarily my employer's. I hate spam.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
o13g2000cwo.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 13:43:40 -0800
Organization: http://groups.google.com
Message-ID: <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130795027 6434 127.0.0.1 (31 Oct 2005 21:43:47 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 31 Oct 2005 21:43:47 +0000 (UTC)
In-Reply-To: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: o13g2000cwo.googlegroups.com; posting-host=24.126.180.194;
   posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160782

I also received the same spam today, also to an address I only use with Ameritrade. This address is one that would take approximately 470 trillion attempts for a brute force attacker to guess, so it is definitely not from a dictionary attack on our mail servers.

I reported this to Ameritrade, as I strongly doubt that they are providing the addresses to spammers on purpose. Rather, I would be more inclined to believe a spammer either found some way to steal the addresses from Ameritrade, or perhaps one of their employees stole the addresses and sold them. Obviously I have no idea, these are only my own educated guesses.

To their credit, I received a response from Ameritrade (below) within an hour of my complaint, stating that they are researching the matter after hearing reports from several customers about this problem. **Although their initial email to me said it could be due to brute force attack of our own mail server, I followed up and explained how this was not plausible in my case, and a manager responded to me that they appreciate my feedback and are still investigating the matter.** Here was their **original** response to me:

"Thank you for contacting us today regarding e-mails that you received.

"We have received reports from some clients that a spam e-mail regarding information on the security SNFX, has been targeted to an address they use with Ameritrade. This is not result from Ameritrade sharing or selling any contact information, nor do we believe any information has been compromised. The cornerstone of our Privacy Statement is the commitment to keep our clients' personal information confidential. Ameritrade does not sell, license, lease or otherwise

disclose your personal information to any third party for any reason, except as noted in the Privacy Statement.

"Several Spam methods do not depend on using purchased or intercepted lists of existing or valid e-mail accounts. Spammers also use known "brute forcing" or dictionary techniques. Brute forcing e-mails basically starts with something like a@doeinvestor.net, aa@doeinvestor, aaa@doeinvestor, aab@doeinvestor, abb@doeinvestor and continues on from there. Brute forcing basically generates and sends out an email to every possible combination of characters/email addresses at a domain like the optiline.net domain. A dictionary email spam basically uses all of the words that would be included in a dictionary or combinations of words which generally produce quite a few valid email accounts. This type of method would not be inhibited by using a separate e-mail address for each business account you may have.

"We have located the ISP that these e-mails originated from and legal has taken the appropriate action to address and prohibit further spam attempts.

"We have no reason to believe that any of our systems have been compromised. Ameritrade deploys state of the art firewalls, intrusion detection, anti - virus software as well as employs a full time staff of employee's dedicated strictly to Information Security and protecting Ameritrade's systems from unauthorized access.

"If you have further concerns or inquiries, please reply to this message.

"Have a good day!"

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!g47g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>

Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 13:47:20 -0800
Organization: http://groups.google.com
Message-ID: <1130795240.496628.15010@g47g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-p
w@comcast.com>
  <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130795245 6740 127.0.0.1 (31 Oct 2005 21:47:25 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 31 Oct 2005 21:47:25 +0000 (UTC)
In-Reply-To: <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g47g2000cwa.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160783

And here is the spam I received (some munged headers to protect my
company's server identity).

Received: from [nnn.nnn.nnn.nnn] by smtp.mycompany.com
[nnn.nnn.nnn.nnn] for myaddress@mycompany.com; Mon, 31 Oct 2005
00:33:18 -0800
Return-Path: <jamal@e-rewards.com>
Received: from dynamic-dsl-114-66.accessatc.net (unverified
[216.81.114.66]) by mycompany.com with SMTP for
<[myaddress@mycompany.com]>;
 Mon, 31 Oct 2005 00:33:18 -0800 (PST)
Received: from 198.31.101.139 (EHLO Nadia) (unknown)
   by dynamic-dsl-114-66.accessatc.net with SMTP; Thu, 13 Oct 2005
09:05:09 -0700
To: my-unique-ameritrade-address
From: Andres <Jamal@e-rewards.com>
Subject: Recent US Market News
Date: Mon, 31 Oct 2005 03:33:04 -0500
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=us-ascii
MIME-Version: 1.0

This will be the hottest Issue of NOvember
- Keep reading to see why

Are you tired of Public Companies without
anything substantial backing their story -
how about a revolutionary invention that
will change the Security Industry forever!
Sniffex inc (SNFX) a company so hot that
everybody from Homeland Defense to United
Nations , Unicef and Embassies wants its
breakthrough Anti-Terror product!!

Breaking News: Sniffex, Inc. Announces New
Representation in 11 Countries

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340%
UP

Ground Breaking News (Friday after the
close): Sniffex, Inc. Announces New
Representation in 11 Countries

You see SNFX has plugged perhaps the biggest hole in the global fight against terror and their device can perform accurate and fast Explosive Detection from distance over 30-100 feet!!

Sniffex makes pocket-sized, hand held explosive detection device. It operates through its ability to detect Nitro Dioxide and Nitro Trioxide ions (the free radicals around the explosive). This unique technology allows the device to penetrate and locate even small amounts of explosives even behind concrete walls or metal obstacles, inside cars airplanes or buses from 10-100 feet away! This device does not SNIFF (inhale) the air, it uses the magnetic forces of the ions tens of feets away!! The magnetic field of the Earth is present everywhere so this device works EVERYWHERE and thats why walls or metal shields cannot stop it from showing where the BAD GUYS are hiding!

This device is so powerful that it can sniff the traces of gunpowder left in gun barrel from 10-20 feet even if you hide it behind wall or put the barrel in your car! ITS SO SENSITIVE

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340% UP

Who is client of Sniffex?? - the company began its activity in June 2005 and started making its first sales in August and September and since then its clients include United Nations and Unicef in Lebanon, Saudi Arabia Embassy even one Mercedes Benz dealership bought the device to protect its premises. Just Read the news from Friday to learn about recent sales of the company.

The Market for device like sniffex is HUUGGGEEEE!!! From Middle East to London , Bali and USA the global threat of terror makes this device a MUST for every building or checkpoint in public transport. Even countries and places that have not been victim of bomb attacs should use Sniffex.

NOW HERE COMES THE BEST PART OF THE STORY - the other companies in the business who produce explosive detection devices, they need to be in almost full contact with the explosive to locate it, a normal sniffer or Xray machine they work from 1-2 feet away, the K9 dogs can sniff from 1-2 feet also, but SNIFFEX can work from up to 100 feet and find any traces of Nitro Dioxide which is the component of 90% of all explosives.

SO SNFX is ahead of the competition!!!

TOP 2005 BUY RATING
Sniffex Inc
Symbol: SNFX
Current Share price: $3.12
52 weeks high: $6.00
Rating: Strong BUY
Industry: Explosive Detection Devices
WallStreet Expectations (1 week): 160% UP
WallStreet Expectations (2 months): 340% UP

NEWS : -----) Sniffex, Inc. Announces New Representation in 11 Countries

IRVING, Texas, Oct 28, 2005 /PRNewswire-FirstCall via COMTEX/ -- Sniffex, Inc. (OTC Pink Sheets: SNFX) ("Sniffex"), producers of Sniffex, an explosive detection device, announced today the signing of two new representatives that will sell Sniffex Inc. in Portuguese speaking countries in Africa and South America as well as in the Philippines and Malaysia. 11 new countries will be represented by these two agreements. The two new representatives are WinWealth Ltd. Corp., headquartered in Hong Kong, and Chelworth Investment LTD, headquartered in Lisbon, Portugal. The company stated that an initial order has been received from these relationships and that the Representatives have already invested significant resources to market Sniffex in their areas.

time, even after positive statements have
been made regarding the above company.
Since we own shares, there is an inherent
conflict of interest in our statements and
opinions. Readers of this publication are
cautioned not to place undue reliance on
for wa rd-loo king s tatements, which are
based on certain assumptions and
expectations involving various risks and
uncertainties, that could cause results to
differ materially from those set forth in
the forward- looking statements. This is
not solicitation to buy or sell stocks,
this text is for informational purpose
only and you should seek professional
advice from registered financial advisor
before you do anything related with buying
or selling stocks, penny stocks are very
high risk and you can lose your entire
investment. This is not solicitation to
buy or sell securities and this newsletter
is not a registered investment advisor.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!bigboote.WPI.EDU!news.tufts.edu!elk.ncren.net!newsflash.concordia.ca!news.sfu.ca!utnut!
qcarhaaa.nortelnetworks.com!zcars129!not-for-mail
From: clewis@nortelnetworks.com (Chris Lewis)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Mon, 31 Oct 2005 21:56:36 +0000 (UTC)
Organization: NortelNetworks
Message-ID: <dk63uk$1uh$1@zcars129.ca.nortel.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com>
NNTP-Posting-Host: wcarh0vt.ca.nortel.com
X-Trace: zcars129.ca.nortel.com 1130795796 2001 47.129.148.231 (31 Oct 2005 21:56:36 GMT)
X-Complaints-To: hawkinsj@nortelnetworks.com
NNTP-Posting-Date: Mon, 31 Oct 2005 21:56:36 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Originator: clewis@nortelnetworks.com (Chris Lewis)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160786

According to Thomas <tomwinzig@gmail.com>:
> And here is the spam I received (some munged headers to protect my
> company's server identity).

These days, the fact of the matter is that if any machine that has
a copy of that email address ever gets infected with a virus or
certain flavours of spamware, you're likely to start getting spam
to it.

Ie: if you got infected with a mass mailer worm, and it found that
email address in your address book or mailboxes, it'll start
sending out viruses with that forged as the from address - and
it'll get collected one way or another (ie: from
 lines hitting
subscription mechanisms). If a computer at Amertrade got infected,
etc.
--
Chris Lewis, Una confibula non set est
It's not just anyone who gets a Starship Cruiser class named after them.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g14g2000cwa.googlegroups.com!not-for-mail
From: slamhead@hotmail.com
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 14:54:39 -0800
Organization: http://groups.google.com
Message-ID: <1130799279.402729.109490@g14g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
NNTP-Posting-Host: 68.4.88.92
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130799284 12389 127.0.0.1 (31 Oct 2005 22:54:44 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 31 Oct 2005 22:54:44 +0000 (UTC)
In-Reply-To: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1),gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g14g2000cwa.googlegroups.com; posting-host=68.4.88.92;
  posting-account=iHh-igwAAAC-TznTds8d8hT6kqMmN6qu
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160788

The same happened to me with Cisco. I a had signed up for a security seminiar and used a unique email address. A few weeks later I received and email from a competitor. Turns out some marketing critter sold my information out the back door. Cisco Legal contacted me and set things straight.

Your case has some very serious implications. I would email your information to enforcement@sec.gov. It could be that Ameritrade has an insider that is running this pump and dump.

At least one of these IP's seem to be unsecured (default password routers) whois remote administration was enabled.

dynamic-dsl-114-66.accessatc.net
thesdsl-00982.otenet.gr

Neither of these looked to be trojaned which is strange.

According to the headers the email was injected from 198.31.167.53 and 198.31.101.139. Would not make sense if they were injected behind the router. Could it be these are open wireless routers that were borrowed from someguy out at the curb? What am I missing.

Strange traceroute:

traceroute to 198.31.101.139 (198.31.101.139), 30 hops max, 40 byte packets
 1 216.115.239.1 (216.115.239.1) 0.465 ms 0.315 ms 0.473 ms
 2 209.203.107.61 (209.203.107.61) 1.812 ms 1.521 ms 1.739 ms
 3 dist-02-ge-3-1-0-508.orng.twtelecom.net (66.192.251.232) 1.614 ms
1.22 ms 1.337 ms
 4 core-02-so-1-0-0-0.lsag.twtelecom.net (66.192.251.18) 2.893 ms
3.134 ms 2.308 ms
 5 tran-01-ge-0-3-0-1.lsag.twtelecom.net (66.192.251.35) 4.032 ms
3.026 ms 3.098 ms
 6 so-6-2.hsa1.LosAngeles1.Level3.net (209.245.88.109) 2.763 ms
2.042 ms 4.077 ms
 7 4.68.102.167 (4.68.102.167) 2.323 ms !H * 2.839 ms !H

198.31.167.53
OrgName: One Stop Wireless-ESG End Cust
OrgID: OSWEC
Address: 1910 S. Archibald
City: Ontario
StateProv: CA
PostalCode: 91761
Country: US

198.31.101.139
OrgName: Level 3 Communications, Inc.
OrgID: LVLT

Address: 1025 Eldorado Blvd.
City: Broomfield
StateProv: CO
PostalCode: 80021
Country: US

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border2.nntp.ams.giganews.com!nntp.giganews.com!npeer.de.kpn-eurorings.net!bloom-beacon.mit.edu!panix!not-for-mail
From: sethb@panix.com (Seth Breidbart)

Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Mon, 31 Oct 2005 23:52:19 +0000 (UTC)
Organization: Society for the Promulgation of Cruelty to the Clueless
Message-ID: <dk6anj$4po$1@reader2.panix.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
NNTP-Posting-Host: panix5.panix.com
X-Trace: reader2.panix.com 1130802739 4920 166.84.1.5 (31 Oct 2005 23:52:19 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Mon, 31 Oct 2005 23:52:19 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160792

In article <l6udnUYgrfNJ-fveRVn-pw@comcast.com>,
User N <usern@invalid.invalid> wrote:
>I create unique, "private" email addresses for every company I submit my email
>address to. This morning I hooked something. The following UBE was sent to
>an email address that was only given to Ameritrade.

>Did anyone else receive a copy sent to an Ameritrade-unique email address?

I got it on my Ameritrade address, and not this (or any other) one.

Seth

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!nx02.iad01.newshosting.com!newshosting.com!216.168.1.162.MISMATCH!sn-xit-02!sn-xit-06!sn-xit-05!sn-post-02!sn-post-01!supernews.com!corp.supernews.com!not-for-mail
From: glgxg <glgxg@mfire.com.invalid>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Mon, 31 Oct 2005 17:00:24 -0800
Organization: Posted via Supernews, http://www.supernews.com
Message-ID: <11mdfgi3lm2g581@corp.supernews.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.12) Gecko/20050915
X-Accept-Language: en-us, en
MIME-Version: 1.0
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130799279.402729.109490@g14g2000cwa.googlegroups.com>
In-Reply-To: <1130799279.402729.109490@g14g2000cwa.googlegroups.com>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Complaints-To: abuse@supernews.com
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160797

slamhead@hotmail.com wrote:

>
> 198.31.167.53
> OrgName: One Stop Wireless-ESG End Cust
> OrgID: OSWEC
> Address: 1910 S. Archibald
> City: Ontario

> StateProv: CA
> PostalCode: 91761
> Country: US
>

Doesn't appear to be a very stable network to begin with...

http://groups.google.com/groups?hl=en&lr=&q=onestopcollect.com

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g14g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 17:02:46 -0800
Organization: http://groups.google.com
Message-ID: <1130806966.803598.113600@g14g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
  <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
  <1130795240.496628.15010@g47g2000cwa.googlegroups.com>
  <dk63uk$1uh$1@zcars129.ca.nortel.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130806971 27075 127.0.0.1 (1 Nov 2005 01:02:51 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Tue, 1 Nov 2005 01:02:51 +0000 (UTC)
In-Reply-To: <dk63uk$1uh$1@zcars129.ca.nortel.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g14g2000cwa.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160798

>These days, the fact of the matter is that if any machine that has
>a copy of that email address ever gets infected with a virus or
>certain flavours of spamware, you're likely to start getting spam
>to it.

**I understand that. I have been using computers for 20 years, and have
never been infected with a virus. (Just trying to provide some evidence
that I'm technically proficient.) The fact is this address has not been**

**revealed by any viruses unless they have infected Ameritrade's servers
directly. In addition, the fact that other Ameritrade users have also
received
the same exact spam, and only to the email address they used on
Ameritrade,
is proof enough that this breach of information occurred at Ameritrade,
and
not from any of our own systems.**

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g44g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 17:06:17 -0800
Organization: http://groups.google.com
Message-ID: <1130807177.891112.287560@g44g2000cwa.googlegroups.com>

References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
<1130799279.402729.109490@g14g2000cwa.googlegroups.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130807182 27285 127.0.0.1 (1 Nov 2005 01:06:22 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Tue, 1 Nov 2005 01:06:22 +0000 (UTC)
In-Reply-To: <1130799279.402729.109490@g14g2000cwa.googlegroups.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g44g2000cwa.googlegroups.com; posting-host=24.126.180.194;
posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160799

>Your case has some very serious implications. I would email your
>information to enforcem...@sec.gov. It could be that Ameritrade has an
>insider that is running this pump and dump.

That is true, I hadn't thought about the content of the message in this
context,
but rather assumed the spammer in question targeted us for that advert
as
we are obviously interested in stocks, having used Ameritrade.

As for alerting the SEC, I will hold off for a few days until I hear
more from
Ameritrade, or until such time as I feel they are not treating the
matter with
respect. So far they seem to be responding to the issue.

Regards,
Thomas

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsmst01b.news.prodigy.com!prodigy.com!postmaster.news.prodigy.com!newssvr29.news.prodigy.net.POSTED!cf2e0109!not-for-mail
From: E-Mail Sent to this address will be added to the BlackLists <Null@BlackList.Anitech-Systems.invalid>
Organization: BlackList@Anitech-Systems.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915
X-Accept-Language: en-us, en
MIME-Version: 1.0
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com>
In-Reply-To: <1130795240.496628.15010@g47g2000cwa.googlegroups.com>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-ID: <8Ez9f.9051$dO2.3619@newssvr29.news.prodigy.net>
NNTP-Posting-Host: 69.231.157.232
X-Complaints-To: abuse@prodigy.net
X-Trace: newssvr29.news.prodigy.net 1130808964 ST000 69.231.157.232 (Mon, 31 Oct 2005 20:36:04 EST)
NNTP-Posting-Date: Mon, 31 Oct 2005 20:36:04 EST
X-UserInfo1: Q[R_PJONTRUAB\\YMBIDM^P@VZ\LPCXLLBWLOOAF@YUDUWYAKVUOPCW[ML
\JXUCKVFDYZKBMSFX^OMSAFNTINTDDMVW[X\THOPXZRVOCJTUTPC_JSBVX\KAOTBAJBVMZTYAKMNLDI_MFDSSOLXINH__FS^
\WQGHGI^C@E[A_CF\AQLDQ\BTMPLDFNVUQ_VM
Date: Tue, 01 Nov 2005 01:36:04 GMT
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160803

Thomas wrote:
> Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?

19 days ago to a SpamTrap. Address harvested from usenet or websites?

Received: from ipnet15-host122.subictel.com (unknown [210.14.46.122])

for <example.invalid>; Wed, 12 Oct 2005 02:21:14 +1000 (EST)
Received: from unknown (HELO Darrien) (192.168.0.25)
by ipnet15-host122.subictel.com with SMTP; Wed, 12 Oct 2005 00:32:01 -0700
Date: Wed, 12 Oct 2005 00:32:00 -0700
From: Elvin <Freddie@ybox.com>
Subject: For Investor's Eyes Only - Presenting the hottest public company of
2005
To: example.invalid
Message-id: <66749123935.11508118682@ipnet15-host122.subictel.com>
MIME-version: 1.0 (Apple Message framework v728)
X-Mailer: Apple Mail (2.728)
Content-type: text/plain; format=flowed; charset=US-ASCII
Content-transfer-encoding: 7bit
Original-recipient: rfc822;example.invalid

Are you tired of Public Companies without anything substantial backing their story -
how about a revolutionary invention that will change the Security Industry forever,
and the company just went public!!!

Company Name: Sniffex Inc
Ticker: SNFX
... <SNIP>

--
E-Mail Sent to this address <BlackList@Anitech-Systems.com>
will be added to the BlackLists.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border2.nntp.ams.giganews.com!nntp.giganews.com!newsfeed101.telia.com!nf02.dk.telia.net!atl-c05.usenetserver.com!news.usenetserver.com!postnews.google.com!g47g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 19:27:40 -0800
Organization: http://groups.google.com
Message-ID: <1130815660.897365.157130@g47g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
<1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com>
<8Ez9f.9051$dO2.3619@newssvr29.news.prodigy.net>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130815666 5385 127.0.0.1 (1 Nov 2005 03:27:46 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Tue, 1 Nov 2005 03:27:46 +0000 (UTC)
In-Reply-To: <8Ez9f.9051$dO2.3619@newssvr29.news.prodigy.net>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g47g2000cwa.googlegroups.com; posting-host=24.126.180.194;
posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160812

> 19 days ago to a SpamTrap. Address harvested from usenet or websites?

I can imagine this spammer has also sent this same email to others
besides Ameritrade users, but the fact that many of us have received it
at addresses created specifically for (and only used on) Ameritrade, I
still think something bad happened at Ameritrade.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border2.nntp.ams.giganews.com!nntp.giganews.com!feeder.xsnews.nl!news.glorb.com!news.isc.org!

calcite.rhyolite.com!not-for-mail
From: vjs@calcite.rhyolite.com (Vernon Schryver)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Mon, 31 Oct 2005 20:56:05 -0700 (MST)
Organization: Rhyolite Software
Message-ID: <dk6p0luks1@calcite.rhyolite.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795240.496628.15010@g47g2000cwa.googlegroups.com> <dk63uk$1uh
$1@zcars129.ca.nortel.com> <1130806966.803598.113600@g14g2000cwa.googlegroups.com>
NNTP-Posting-Host: localhost
X-Trace: calcite.rhyolite.com 1130817365 31389 127.0.0.1 (1 Nov 2005 03:56:05 GMT)
X-Complaints-To: usenet@calcite.rhyolite.com
NNTP-Posting-Date: Tue, 1 Nov 2005 03:56:05 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160814

In article <1130806966.803598.113600@g14g2000cwa.googlegroups.com>,
Thomas <tomwinzig@gmail.com> wrote:

>>These days, the fact of the matter is that if any machine that has
>>a copy of that email address ever gets infected with a virus or
>>certain flavours of spamware, you're likely to start getting spam
>>to it.
>
>I understand that. I have been using computers for 20 years, and have
>never been infected with a virus. (Just trying to provide some evidence
>that I'm technically proficient.) The fact is this address has not been

>revealed by any viruses unless they have infected Ameritrade's servers
>directly.

Why Ameritrade's servers? I thought the other person's point was that
anyone at Ameritrade or elsewhere who had your email address on a
personal machine could be unknowingly responsible for leaking your
address. For example,
- have you ever received any personal mail from Ameritrade?
- do you have anything like personal broker?
- has Ameritrade ever sent you and anyone else any mail in which
both of your addresses were listed?
- could someone inside Ameritrade have sent someone else inside
Ameritrade a message saying something like "Mr. Tomwinzig
said blah de blah" and including your email address?
- could there be a (human or mechanical) leak in your own mail system?
I don't recall that you said you run your own SMTP servers.

Finally, your claim about how hard it would be for a spammer to guess
your email address was not convincing. The number you offered was
either too low or too high. It was vastly too low if you generated the
name with something strong (e.g. `dd if=/dev/random count=1 | md5`).
I suspect your estimate was computed by assuming that the address was
one of 470 trillion said in a population that would be choosen uniformly.
That claim is too strong for me to accept without knowing the address
at issue, and even then I'd probably plead too much ignorance of the
distribution of user name choices to make an honest estimate of
how hard a spammer would work to guess your address.

Vernon Schryver vjs@rhyolite.com

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!nx01.iad01.newshosting.com!newshosting.com!
news.linkpendium.com!news.linkpendium.com!xuxa.iecc.com!not-for-mail
From: johnl@iecc.com (John R. Levine)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 31 Oct 2005 23:48:11 -0500
Organization: I.E.C.C., Trumansburg NY USA
Message-ID: <dk6s2b$t79$1@xuxa.iecc.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>

NNTP-Posting-Host: xuxa.iecc.com
X-Trace: xuxa.iecc.com 1130820491 29930 208.31.42.42 (1 Nov 2005 04:48:11 GMT)
X-Complaints-To: abuse@iecc.com
NNTP-Posting-Date: 1 Nov 2005 0
4:48:11 GMT
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160824

>I create unique, "private" email addresses for every company I submit
>my email address to. This morning I hooked something. The following
>UBE was sent to an email address that was only given to
>Ameritrade. ...

Not Ameritrade, but I've recently gotten spam to a tagged address
known only to the Official Airline Guide. Other people have gotten
spam to tagged addresses given to a variety of other companies like
Orbitz and United Airlines.

The most likely common thread is that they outsource their list mail
to ESPs, and I suspect there is an ESP with a crooked employee who
steals modest number of addresses and sells them to spammers.

R's,
John

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 8bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!border2.nntp.dca.giganews.com!nntp.giganews.com!peer01.cox.net!
cox.net!hwmnpeer01.lga!hwmedia!hw-filter.lga!fe03.lga.POSTED!53ab2750!not-for-mail
From: Ameritrade User <x@y.z>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Message-ID: <p40em1pfs460k6co9i404mdnv4gf9tb9lo@4ax.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
X-Newsreader: Forte Free Agent 2.0/32.652
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Trace:
idmkcnjgmiagocdedefbifpaocembkfcimbejaobhakpmmhleckejbfnfipalldjddjjgfddnbepopomddopejlhjadpckeiiggjdpbeanajdchnamiecbphbhio
dagnofcn&#65533;
NNTP-Posting-Date: Mon, 31 Oct 2005 23:06:35 MST
Date: Mon, 31 Oct 2005 22:06:36 -0800
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160829

On Mon, 31 Oct 2005 13:39:26 -0500, "User N" <usern@invalid.invalid>
wrote:

>I create unique, "private" email addresses for every company I submit my email
>address to. This morning I hooked something. The following UBE was sent to
>an email address that was only given to Ameritrade. I checked two of my more
>public/exposed email addresses and neither of them received the UBE. I know
>someone else who has an Ameritrade account and asked them if they received
>the same UBE.... they did. It was sent via a different path and some header
>fields are rotated, but otherwise it is identical and it was sent within a few minutes
>of mine.
>
>Did anyone else receive a copy sent to an Ameritrade-unique email address?
>Did anyone receive a copy sent to an email address NOT given to Ameritrade?
>
>

I too create unique addresses for every company I give an email
address to and I also received the SNFX email. Ameritrade's initial
(and prompt) denial suggested that it may have been a brute force or
dictionary attack. Neither of these is possible at least not without
me knowing about it. **Their second email suggests they are taking it
seriously, I hope so...**

----------070309010004030400030507
Content-Type: message/rfc822;

name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!local01.nntp.dca.giganews.com!nntp.megapath.net!news.megapath.net.POSTED!not-for-mail
NNTP-Posting-Date: Tue, 01 Nov 2005 02:24:26 -0600
X-newsreader: xrn 9.02
X-Sender: murray@glypnod (Hal Murray)
From: hmurray@suespammers.org (Hal Murray)
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Newsgroups: news.admin.net-abuse.email
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com> <dk63uk$1uh$1@zcars129.ca.nortel.com>
Message-ID: <R5ednXJ-l4enu_reRVn-rA@megapath.net>
Date: Tue, 01 Nov 2005 02:24:26 -0600
NNTP-Posting-Host: 64.139.1.69
X-Trace: sv3-o8GIHBKe8trrt9stzl/zBNzNJviXgsdPl7lFWA0/BQ/quYN3p2B3/qnOJ4xY+ldlWP5q+rbu6kDDdCK!
CuF6IxYXpt5vC1mX1kwIkFuW7QNiUqPXobgKlQisjCL2WpLpM6BtAkteTNYwd2Ecjw736uvxE78=
X-Complaints-To: abuse@megapath.net
X-DMCA-Complaints-To: abuse@megapath.net
X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your complaint properly
X-Postfilter: 1.3.32
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160830

>Ie: if you got infected with a mass mailer worm, and it found that
>email address in your address book or mailboxes, it'll start
>sending out viruses with that forged as the from address - and
>it'll get collected one way or another (ie: from lines hitting
>subscription mechanisms). If a computer at Amertrade got infected,
>etc.

So everybody who uses tagged addresses should setup one more
and send themselves a message using it and save it in their
vital mail collection so if they get infected by a virus, the
virus will find it and send them spam/crap on this magic address
and they will know what's going on.

--
The suespammers.org mail server is located in California. So are all my
other mailboxes. Please do not send unsolicited bulk e-mail or unsolicited
commercial e-mail to my suespammers.org address or any of my other addresses.
These are my opinions, not necessarily my employer's. I hate spam.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsmst01b.news.prodigy.com!prodigy.com!postmaster.news.prodigy.com!newssvr12.news.prodigy.com.POSTED!db498ea5!not-for-mail
From: E-Mail Sent to this address will be added to the BlackLists <Null@BlackList.Griffin-Technologies.invalid>
Organization: BlackList@Griffin-Technologies.net
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915
X-Accept-Language: en-us, en
MIME-Version: 1.0
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com> <dk63uk$1uh$1@zcars129.ca.nortel.com> <R5ednXJ-l4enu_reRVn-
rA@megapath.net>
In-Reply-To: <R5ednXJ-l4enu_reRVn-rA@megapath.net>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-ID: <5CG9f.8162$q%.7909@newssvr12.news.prodigy.com>
NNTP-Posting-Host: 69.231.31.26
X-Complaints-To: abuse@prodigy.net
X-Trace: newssvr12.news.prodigy.com 1130837505 ST000 69.231.31.26 (Tue, 01 Nov 2005 04:31:45 EST)
NNTP-Posting-Date: Tue, 01 Nov 2005 04:31:45 EST
X-UserInfo1: OPXIFT_L[B^UCWDYIBHZOWP@YZOZ@GXOXZ^L\UQHWIWDUWYADNVOPCKZBL
\NX_KHV^GY[KVMG^ZPNHSCZNS[^UXFJVWYXVXKBH[XRWWBBDTN@AX\JSBVH]_@T\EKJHBMZ_WZJFNRY]YWKSPED_U^NC\HSZ
\WS[KEAYI@DO@\K@BP\LD[\GTMPLDFVU]ASJM

Date: Tue, 01 Nov 2005 09:31:45 GMT
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160833

Hal Murray wrote:
>>Ie: if you got infected with a mass mailer worm, and it found that
>>email address in your address book or mailboxes, it'll start
>>sending out viruses with that forged as the from address - and
>>it'll get collected one way or another (ie: from lines hitting
>>subscription mechanisms). If a computer at Amertrade got infected,
>>etc.
>
> So everybody who uses tagged addresses should setup one more
> and send themselves a message using it and save it in their
> vital mail collection so if they get infected by a virus, the
> virus will find it and send them spam/crap on this magic address
> and they will know what's going on.

Done long ago, on every machine I have to deal with at $DayJob,
and on my personal machines as well, in the address book too.
(No hits yet, none expected.) {If we ever see one, we know who
to kill^W err reeducate.}

--
E-Mail Sent to this address <BlackList@Griffin-Technologies.net>
will be added to the BlackLists.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed.hal-mli.net!feeder1.hal-mli.net!
news.alt.net!netheaven.com!usenet
From: Bruce Barnett <spamhater113+U051101070836@grymoire.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 1 Nov 2005 12:08:46 GMT
Sender: <spamhater112+U051101070836@grymoire.com>
Message-ID: <dk7lse$7ko$0$208.20.133.66@netheaven.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795020.879253.48990@o13g2000cwo.googlegroups.com>
<1130795240.496628.15010@g47g2000cwa.googlegroups.com>
<dk63uk$1uh$1@zcars129.ca.nortel.com>
NNTP-Posting-Host: 208.20.133.66@netheaven.com
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
User-Agent: Gnus/5.1002 (Gnus v5.10.2) Emacs/20.7 (gnu/linux)
Cancel-Lock: sha1:2Pf+BJQJSFM5VCbdjQt3qzmvawQ=
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160841

clewis@nortelnetworks.com (Chris Lewis) writes:

> These days, the fact of the matter is that if any machine that has
> a copy of that email address ever gets infected with a virus or
> certain flavours of spamware, you're likely to start getting spam
> to it.

I see a lot of pump and dump spam sent to a mailing list I run, so I
know the spammers are using infected machines to harvest email addies.
Recent ones:

AXCP
AXCP . PK
CWTD.OB
MWIS

--
Sending unsolicited commercial e-mail to this account incurs a fee of
$500 per message, and acknowledges the legality of this contract.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"

Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path
: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!panix!not-for-mail
From: nospam4me@mytrashmail.com
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 1 Nov 2005 16:57:43 +0000 (UTC)
Organization: PANIX Public Access Internet and UNIX, NYC
Message-ID: <dk86q7$6u4$1@reader2.panix.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <p40em1pfs460k6co9i404mdnv4gf9tb9lo@4ax.com>
NNTP-Posting-Host: panix1.panix.com
X-Trace: reader2.panix.com 1130864263 7108 166.84.1.1 (1 Nov 2005 16:57:43 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Tue, 1 Nov 2005 16:57:43 +0000 (UTC)
User-Agent: tin/1.6.2-20030910 ("Pabbay") (UNIX) (NetBSD/2.0 (i386))
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160860

I bet it was a dishonest employee or contractor who downloaded the
Ameritrade customer list (or palmed a backup tape) and sold it.

--
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
 Herb Oxley
 Reply-to: address IS Valid.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!panix!not-for-mail
From: sethb@panix.com (Seth Breidbart)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 1 Nov 2005 19:57:05 +0000 (UTC)
Organization: Society for the Promulgation of Cruelty to the Clueless
Message-ID: <dk8hah$e6p$1@reader2.panix.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <dk63uk$1uh$1@zcars129.ca.nortel.com>
<1130806966.803598.113600@g14g2000cwa.googlegroups.com> <dk6p0luks1@calcite.rhyolite.com>
NNTP-Posting-Host: panix5.panix.com
X-Trace: reader2.panix.com 1130875025 14553 166.84.1.5 (1 Nov 2005 19:57:05 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Tue, 1 Nov 2005 19:57:05 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160884

In article <dk6p0luks1@calcite.rhyolite.com>,
Vernon Schryver <vjs@calcite.rhyolite.com> wrote:

>Why Ameritrade's servers? I thought the other person's point was that
>anyone at Ameritrade or elsewhere who had your email address on a
>personal machine could be unknowingly responsible for leaking your
>address. For example,
>   - have you ever received any personal mail from Ameritrade?

No, just mailinglist.

>   - do you have anything like personal broker?

Not at Ameritrade.

>   - has Ameritrade ever sent you and anyone else any mail in which
>   both of your addresses were listed?

No.

>   - could someone inside Ameritrade have sent someone else inside
>   Ameritrade a message saying something like "Mr. Tomwinzig
>   said blah de blah" and including your email address?

"Could"? Certainly. I don't think it's likely.

>   - could there be a (human or mechanical) leak in your own mail system?

No. (If there were, it would have to have been in panix's systems,
and would have hit a lot more of my addresses.)

>Finally, your claim about how hard it would be for a spammer to guess
>your email address was not convincing.

It went to a domain with a catchall (except for a handfull of
addresses known to spammers). I'd know a dictionary attack on that
domain quite quickly.

Seth

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!local01.nntp.dca.giganews.com!nntp.comcast.com!news.comcast.com.POSTED!not-for-mail
NNTP-Posting-Date: Tue, 01 Nov 2005 17:08:15 -0600
From: "User N" <usern@invalid.invalid>
Newsgroups: news.admin.net-abuse.email
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <dk63uk$1uh$1@zcars129.ca.nortel.com>
<1130806966.803598.113600@g14g2000cwa.googlegroups.com> <dk6p0luks1@calcite.rhyolite.com> <dk8hah$e6p
$1@reader2.panix.com>
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 1 Nov 2005 18:08:28 -0500
MIME-Version: 1.0
Content-Type: text/plain;
	format=flowed;
	charset="Windows-1252";
	reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2900.2670
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2670
Message-ID: <Y9KdndAtGo7CaPreRVn-rQ@comcast.com>
NNTP-Posting-Host: 69.142.47.32
X-Trace: sv3-pKCboqYnboGUgaldUdVzlZincJCt49ERyVP3sdOj+r9fLVSSGV9dNDB9LDrua7fjphUVPWbj2CdmTBa!ye89vUCJte62d51+H/
pXfDUS81kRtT+KJiN6CDzkaMLjDAc4A7XRbjnDr5IEO4wieRYYMeUhAdSN!lgI=
X-Complaints-To: abuse@comcast.net
X-DMCA-Complaints-To: dmca@comcast.net
X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your complaint properly
X-Postfilter: 1.3.32
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160908

"Seth Breidbart" <sethb@panix.com> wrote in message news:dk8hah$e6p$1@reader2.panix.com...
> In article <dk6p0luks1@calcite.rhyolite.com>,
> Vernon Schryver <vjs@calcite.rhyolite.com> wrote:
>
>>Why Ameritrade's servers? I thought the other person's point was that
>>anyone at Ameritrade or elsewhere who had your email address on a
>>personal machine could be unknowingly responsible for leaking your
>>address. For example,
>>   - have you ever received any personal mail from Ameritrade?
>
> No, just mailinglist.

Ditto. IIRC, the only thing I've gotten from Ameritrade was confirmation
of my email address change to the new unique one. That was done some
time ago... can't remember when.

>>   - do you have anything like personal broker?
>
> Not at Ameritrade.

Ditto

>> - has Ameritrade ever sent you and anyone else any mail in which
>> both of your addresses were listed?
>
> No.

Ditto

>> - could someone inside Ameritrade have sent someone else inside
>> Ameritrade a message saying something like "Mr. Tomwinzig
>> said blah de blah" and including your email address?
>
> "Could"? Certainly. I don't think it's likely.

Ditto. I haven't contacted Ameritrade for anything since changing to the unique email address, or even conducted any transactions.

>> - could there be a (human or mechanical) leak in your own mail system?
>
> No. (If there were, it would have to have been in panix's systems,
> and would have hit a lot more of my addresses.)

I'm of the same mind. I've got maybe 120 email accounts associated with the domain name in question, and that list is in an aliases file on my webhost's servers and on my local machine. If the list were compromised one could argue that some of the other email addresses should have been hit. I can't rule out the possibility that the Ameritrade address was compromised at the time I submitted it. However, my box is pretty tight and I've never seen any evidence to suggest that it was ever compromised.

>>Finally, your claim about how hard it would be for a spammer to guess
>>your email address was not convincing.
>
> It went to a domain with a catchall (except for a handfull of
> addresses known to spammers). I'd know a dictionary attack on that
> domain quite quickly.

I don't have a catchall setup and it turns out that SMTP logging wasn't enabled on my account. However, I think the chances of someone guessing my Ameritrade unique email address is exceptionally low, and I think it highly unlikely that a dictionary attack would have magically hit just that one address.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!g44g2000cwa.googlegroups.com!not-for-mail
From: slamhead@hotmail.com
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 1 Nov 2005 19:08:53 -0800
Organization: http://groups.google.com
Message-ID: <1130900933.112642.80070@g44g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
<ys6dnaJ-_o5cFfveRVn-hA@megapath.net>
NNTP-Posting-Host: 68.4.88.92
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1130900938 21669 127.0.0.1 (2 Nov 2005 03:08:58 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Wed, 2 Nov 2005 03:08:58 +0000 (UTC)
In-Reply-To: <ys6dnaJ-_o5cFfveRVn-hA@megapath.net>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1),gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g44g2000cwa.googlegroups.com; posting-host=68.4.88.92;
posting-account=iHh-igwAAAC-TznTds8d8hT6kqMmN6qu
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2160929

Wonder if all the risk of his illegal activities was worth the 6% that

could have been made.
http://finance.yahoo.com/q/bc?s=SNFX.PK&t=3m&l=on&z=m&q=l&c=

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g44g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 21 Nov 2005 15:13:21 -0800
Organization: http://groups.google.com
Message-ID: <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
NNTP-
Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1132614806 4085 127.0.0.1 (21 Nov 2005 23:13:26 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 21 Nov 2005 23:13:26 +0000 (UTC)
In-Reply-To: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g44g2000cwa.googlegroups.com; posting-host=24.126.180.194;
   posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163703

I received another one of these SNFX spam emails today, again to my ameritrade-specific email address only. The content of the message was sent as a GIF file entirely, so I can't even display it here without hand-typing it. Essentially your typical Pump and Dump for SNIFFEX, Inc.

Ameritrade has been giving me the run-around since this first happened 3 weeks ago. I forwarded this one to them, and am going to be contacting the SEC. Ameritrade won't admit it, but in my opinion, the information had to be stolen from them somehow. Nothing else makes sense to me.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g49g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 21 Nov 2005 15:23:00 -0800
Organization: http://groups.google.com
Message-ID: <1132615380.271326.324930@g49g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
   <1130795240.496628.15010@g47g2000cwa.googlegroups.com>
   <dk63uk$1uh$1@zcars129.ca.nortel.com>
   <1130806966.803598.113600@g14g2000cwa.googlegroups.com>
   <dk6p0luks1@calcite.rhyolite.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1132615385 4873 127.0.0.1 (21 Nov 2005 23:23:05 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 21 Nov 2005 23:23:05 +0000 (UTC)
In-Reply-To: <dk6p0luks1@calcite.rhyolite.com>
User-Agent: G2/0.2

X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g49g2000cwa.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163704

> Why Ameritrade's servers? I thought the other person's point was that
> anyone at Ameritrade or elsewhere who had your email address on a
> personal machine could be unknowingly responsible for leaking your
> address. For example,
> - have you ever received any personal mail from Ameritrade?

Yes, but I've never been infected with a virus, on any of my personal computers. And our mail server has never been infected with a virus. And I've never forwarded Ameritrade email to anyone else.

> - do you have anything like personal broker?

No.

> - has Ameritrade ever sent you and anyone else any mail in which
> both of your addresses were listed?

If they have, this is a critical privacy violation on their part.

> - could someone inside Ameritrade have sent someone else inside
> Ameritrade a message saying something like "Mr. Tomwinzig
> said blah de blah" and including your email address?

Therefore my point still stands about the leak being from within Ameritrade.

> - could there be a (human or mechanical) leak in your own mail system?
> I don't recall that you said you run your own SMTP servers.

I do run my own SMTP server, and there is no leak there.

> Finally, your claim about how hard it would be for a spammer to guess
> your email address was not convincing. The number you offered was
> either too low or too high. It was vastly too low if you generated the
> name with something strong (e.g. `dd if=/dev/random count=1 | md5`).
> I suspect your estimate was computed by assuming that the address was
> one of 470 trillion said in a population that would be choosen uniformly.
> That claim is too strong for me to accept without knowing the address
> at issue, and even then I'd probably plead too much ignorance of the
> distribution of user name choices to make an honest estimate of
> how hard a spammer would work to guess your address.

My estimate was accurate. My email addresses created for separate companies
are based on my name, a string loosely based on the company's name as I

refer to them, and a two digit number. Each part is separated by non-alphanumeric
characters. In this case, the email address user part (before the @ sign) is 15
characters long.

Because the address is not found in a dictionary, and only 1/3 of the address
is based on my first name, and because it is comprised of letters, numbers, and
symbols, I calculated the estimate assuming the dictionary attack would have
to use that complete alphabet x 15 characters for a brute force attack.

And this is all ignoring the fact that this is my own SMTP server with dictionary
attack prevention.

Thomas

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"

Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!panix!not-for-mail
From: sethb@panix.com (Seth Breidbart)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 22 Nov 2005 00:34:18 +0000 (UTC)
Organization: Society for the Promulgation of Cruelty to the Clueless
Message-ID: <dltp2alln1@reader2.panix.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130806966.803598.113600@g14g2000cwa.googlegroups.com> <dk6p0l$uks
$1@calcite.rhyolite.com> <1132615380.271326.324930@g49g2000cwa.googlegroups.com>
NNTP-Posting-Host: panix5.panix.com
X-Trace: reader2.panix.com 1132619658 22199 166.84.1.5 (22 Nov 2005 00:34:18 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Tue, 22 Nov 2005 00:34:18 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163714

I got the spam to my Ameritrade-registered address today.

No response from Ameritrade when I asked them about it.

No response from the SEC yet, either.

Seth

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed00.sul.t-online.de!t-online.de!
fr.ip.ndsoftware.net!zen.net.uk!dedekind.zen.co.uk!213.155.197.138.MISMATCH!ilaria.aioe.org!aioe.org!not-for-mail
From: PCBoy <News.20.PCBoy@spamgourmet.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 22 Nov 2005 04:17:49 +0000 (UTC)
Organization: MiloMinderBinderInc
Message-ID: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1130795240.496628.15010@g47g2000cwa.googlegroups.com> <dk63uk$1uh
$1@zcars129.ca.nortel.com> <1130806966.803598.113600@g14g2000cwa.googlegroups.com> <dk6p0luks1@calcite.rhyolite.com>
<1132615380.271326.324930@g49g2000cwa.googlegroups.com>
NNTP-Posting-Host: 5ZEDTKZ0WL5MQcEvBNS0sQ.363.domitilla.aioe.org
X-Complaints-To: abuse@aioe.org
User-Agent: Xnews/5.04.25 Hamster/2.1.0.0
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163750

"Thomas" <tomwinzig@gmail.com> wrote in
news:1132615380.271326.324930@g49g2000cwa.googlegroups.com:

>> Finally, your claim about how hard it would be for a spammer to guess
>> your email address was not convincing. The number you offered was
>> either too low or too high. It was vastly too low if you generated
>> the name with something strong (e.g. `dd if=/dev/random count=1 |
>> md5`). I suspect your estimate was computed by assuming that the
>> address was one of 470 trillion said in a population that would be
>> choosen uniformly. That claim is too strong for me to accept without
>> knowing the address at issue, and even then I'd probably plead too
>> much ignorance of the distribution of user name choices to make an
>> honest estimate of how hard a spammer would work to guess your
>> address.
>
> My estimate was accurate. My email addresses created for separate
> companies
> are based on my name, a string loosely based on the company's name as
> I
>
> refer to them, and a two digit number. Each part is separated by
> non-alphanumeric
> characters. In this case, the email address user part (before the @
> sign) is 15

> characters long.
>
> Because the address is not found in a dictionary, and only 1/3 of the
> address
> is based on my first name, and because it is comprised of letters,
> numbers, and
> symbols, I calculated the estimate assuming the dictionary attack
> would have
> to use that complete alphabet x 15 characters for a brute force
> attack.
>
> And this is all ignoring the fact that this is my own SMTP server with
> dictionary
> attack prevention.
>
> Thomas
>

[... sorry I am not even in the loop re: email your email addr
issues. But computing P values for co-incidences seen in the
wild is something I have studied before ...]

<rant_filters insert = now> <soap_box action = climbs onto >

To calculate this P value many things must be considered, it is not brute
force o
n 15 chars unless you assume the attacker both stupid[1] and had
no access to software written by someone who wasnt stupid.
I can think of a rich variety of powerful yet simple and computationally
tractable algorithms for generating good dictionary attacks that are much
better than blind guessing, those I intend not to describe on usenet
(*I* regard those as export controlled arms.)

Anyways a better guess would be

(Number of First names +1) * Number of Strings Loosley Based on Company
name * Two digt Number * Number of non alpha numerics allowed in email
addr squared

I could also multiply by 5! assuming I didnt know the order of these but
the seperators have a natural place so its 3! and the 3 fields are in
what appear the natural order so its 1!

This number is sitill a large, and given it is your server and your logs
I presume show there is no evidence of other dictionary attemtps. Note
that absenc of evidence is not evidence of absence. A dictionary based
spam run with minimal intelligence wil NOT hammer 1 server with every
possible name, A dictionary based spam run with minimal intelligence will
try every server one with name at a time, to mask the fact that it is a
dictionary attack. All that said I dont believe it was a dictionary
attack by a spammer.
BUT that may not be the only explanation.

Also note: All this assumes that a A random spammer is trying to guess a
password.
If instead someone tried to joe job you or company X and they had in the
past received one or two of these munged names then they know many
things. They know the name you use. They know the name of the company
they want to joe job. If the non alpha chars and the 2 digit number are
chosen using a strong random number generator then the number of
possiblities is still in the 100's or low thousands. However if they are
not chosen at random.

Note the point of this post is not to argue about the odds there are way
better things to do, the point of this post is to exemplify the danger
of attempting to work out the P value of something when operating
in a hostile environment Rule#0 Rule#2. Note that second guessing every
piece of evidence leads/causes to madness, a short examination of this
news group or my posts will prove this point. :)

If you wanted to make this stronger I would use
md5 hash of (company_name + secret key) converted to base64 and clipped
so that appending to companyname did not make it to long. Just 8 chars
are or so of the md5 hash would be strongish for this purpose.
To make this machine parsable I would perhaps add a fixed non alphnum

separator after company name.

> And this is all ignoring the fact that this is my own SMTP server with
> dictionary
> attack prevention.
>
> Thomas

[1] Yes I know Rule #3. WHich is why I see no need to make them smarter
in ways I dont want to[2]

[2] Ways I dont want to? Yes I want spammers to get smarter. I want them
after a few tries on my server and noticing its configuration to work out
oops heres a bad one we wont spam him again, because A/. we *never* get
any sales, occasionally a web hitbut nothing like a sale. B/. we do get
larted. THinks what to do. wash wash wash.

For those still reading... (sound of radiation proof cockcroaches
scuttling),

Apart from being a really strange smiley, What was the +1) for? Well my
computatuioon did not assume there was a first name
ie Every possible first name + ""

</soap_box> </rant_filters>

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed00.sul.t-online.de!t-online.de!
newsfeed.freenet.de!feeder2.ecngs.de!ecngs!feeder.ecngs.de!195.40.4.120.MISMATCH!easynet-quince!easynet.net!
feed1.news.be.easynet.net!reader0.news.be.easynet.net!not-for-mail
From: ash@fakedomainxx.com
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1>
Newsgroups: news.admin.net-abuse.email
X-NNTP-Posting-Host: phenix
Message-ID: <newscache$8smdqi$op2$1@news.rootshell.be>
Date: 22 Nov 2005 22:07:20 GMT
NNTP-Posting-Date: 22 Nov 2005 22:07:20 GMT
NNTP-Posting-Host: 217.22.55.50
X-Trace: 1132697240 reader0.news.be.easynet.net 442 [::ffff:217.22.55.50]:43905
X-Complaints-To: abuse@be.easynet.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163833

>   Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
>
>   From: PCBoy <News.20.PCBoy@spamgourmet.com>
>   Reply to: PCBoy
>   Date: Tue, 22 Nov 2005 04:17:49 +0000 (UTC)
>   Organization: MiloMinderBinderInc
>   Newsgroups:
>   news.admin.net-abuse.email
>   Followup to: newsgroup
>   References:
>   <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
>   <1130795240.496628.15010@g47g2000cwa.googlegroups.com>
>   <dk63uk$1uh$1@zcars129.ca.nortel.com>
>   <1130806966.803598.113600@g14g2000cwa.googlegroups.com>
>   <dk6p0luks1@calcite.rhyolite.com>
>   <1132615380.271326.324930@g49g2000cwa.googlegroups.com>
>"Thomas" <tomwinzig@gmail.com> wrote in
>news:1132615380.271326.324930@g49g2000cwa.googlegroups.com:

>
>>> Finally, your claim about how hard it would be for a spammer to guess
>>> your email address was not convincing. The number you offered was
>>> either too low or too high. It was vastly too low if you generated
>>> the name with something strong (e.g. `dd if=/dev/random count=1 |
>>> md5`). I suspect your estimate was computed by assuming that the
>>> address was one of 470 trillion said in a population that would be
>>> choosen uniformly. That claim is too strong for me to accept without
>>> knowing the address at issue, and even then I'd probably plead too
>>> much ignorance of the distribution of user name choices to make an
>>> honest estimate of how hard a spammer would work to guess your
>>> address.
>>
>> My estimate was accurate. My email addresses created for separate
>> companies
>> are based on my name, a string loosely based on the company's name as
>> I
>>
>> refer to them, and a two digit number. Each part is separated by
>> non-alphanumeric
>> characters. In this case, the email address user part (before the @
>> sign) is 15
>> characters long.
>>
>> Because the address is not found in a dictionary, and only 1/3 of the
>> address
>> is based on my first name, and because it is comprised of letters,
>> numbers, and
>> symbols, I calculated the estimate assuming the dictionary attack
>> would have
>> to use that complete alphabet x 15 characters for a brute force
>> attack.
>>
>> And this is all ignoring the fact that this is my own SMTP server with
>> dictionary
>> attack prevention.
>>
>> Thomas
>>
>
>... sorry I am not even in the loop re: email your email addr
> issues. But computing P values for co-incidences seen in the
> wild is something I have studied before ...]
>
><rant_filters insert = now> <soap_box action = climbs onto >
>
>To calculate this P value many things must be considered, it is not brute
>force on 15 chars unless you assume the attacker both stupid and had
>no access to software written by someone who wasnt stupid.
>I can think of a rich variety of powerful yet simple and computationally
>tractable algorithms for generating good dictionary attacks that are much
>better than blind guessing, those I intend not to describe on usenet
>(*I* regard those as export controlled arms.)
>
>Anyways a better guess would be
>
>(Number of First names +1) * Number of Strings Loosley Based on Company
>name * Two digt Number * Number of non alpha numerics allowed in email
>addr squared
>
>I could also multiply by 5! assuming I didnt know the order of these but
>the seperators have a natural place so its 3! and the 3 fields are in
>what appear the natural order so its 1!
>
>This number is sitill a large, and given it is your server and your logs
>I presume show there is no evidence of other dictionary attemtps. Note
>that absenc of evidence is not evidence of absence. A dictionary based
>spam run with minimal intelligence wil NOT hammer 1 server with every
>possible name, A dictionary based spam run with minimal intelligence will
>try every server one with name at a time, to mask the fact that it is a
>dictionary attack. All that said I dont believe it was a dictionary
>attack by a spammer.
>BUT that may not be the only explanation.
>
>Also note: All this assumes that a A random spammer is trying to guess a
>password.

>If instead someone tried to joe job you or company X and they had in the
>past received one or two of these munged names then they know many
>things. They know the name you use. They know the name of the company
>they want to joe job. If the non alpha chars and the 2 digit number are
>chosen using a strong random number generator then the number of
>possiblities is still in the 100's or low thousands. However if they are
>not chosen at random.
>
>Note the point of this post is not to argue about the odds there are way
>better things to do, the point of this post is to exemplify the danger
>of attempting to work out the P value of something when operating
>in a hostile environment Rule#0 Rule#2. Note that second guessing every
>piece of evidence leads/causes to madness, a short examination of this
>news group or my posts will prove this point. :)
>
>If you wanted to make this stronger I would use
>md5 hash of (company_name + secret key) converted to base64 and clipped
>so that appending to companyname did not make it to long. Just 8 chars
>are or so of the md5 hash would be strongish for this purpose.
>To make this machine parsable I would perhaps add a fixed non alphnum
>separator after company name.
>
>> And this is all ignoring the fact that this is my own SMTP server with
>> dictionary
>> attack prevention.
>>
>> Thomas
>
>
>
>
>
>
>
>
>[1] Yes I know Rule
 #3. WHich is why I see no need to make them smarter
>   in ways I dont want to[2]
>
>[2] Ways I dont want to? Yes I want spammers to get smarter. I want them
>after a few tries on my server and noticing its configuration to work out
>oops heres a bad one we wont spam him again, because A/. we *never* get
>any sales, occasionally a web hitbut nothing like a sale. B/. we do get
>larted. THinks what to do. wash wash wash.
>
>
>For those still reading... (sound of radiation proof cockcroaches
>scuttling),
>
>Apart from being a really strange smiley, What was the +1) for? Well my
>computatuioon did not assume there was a first name
>ie Every possible first name + ""
>
></soap_box> </rant_filters>

Sorry, this thread is so long I don't know where to get in, so I just
chime in at the last thread.

Some background:
1) I contacted Ameritrade this morning about the problem being discussed
this morning without reading this thread.
2) I was about to call them again to provide more information, but I
thought I'd search the news groups first to see if this has been talked
about.
3) I run my own server, so all the talk about brute force attack or
dictionary technique is simply BS, I can review my system logs and see
exactly what happened, the spammers obviously knew the address.

My conclusion is that Ameritrade is 1) absolutely NOT serious about this issue and 2) TOTALLY incompetent and not understand the issue, here is why I say that.

**After reading this thread, I emailed them, asked them since they've been aware of this problem, why didn't they told me so when I called earlier.
I also wanted to know what have they found and done about it. Here is the email response I got:**

==========
From techhelp@ameritrade.com Tue Nov 22 13:59:25 2005
Date: Tue, 22 Nov 2005 13:59:24 -0600 (CST)
From: Ameritrade Technology Support <techhelp@ameritrade.com>
To: XXX@XXXa.com
Subject: Re: regarding my complaint about possible security breach this morning (KMM28991625I20725L0KM)

Dear Bigshot:

Thank you for contacting us today regarding your account security.

I sincerely apologize for any inconvenience. We have received reports from some clients that a spam e-mail regarding information on the security SNFX, has been targeted to an address they use with Ameritrade. This is not a result of Ameritrade sharing or selling any contact information, nor do we believe any information has been compromised. The cornerstone of our Privacy Statement is the commitment to keep our clients? personal information confidential. Ameritrade does not sell, license, lease or othe rwise disclose your personal information to any third party for any reason, except as noted in the Privacy Statement.

Several Spam methods do not depend on using purchased or intercepted lists of existing or valid e-mail accounts. Spammers also use known "brute forcing" or dictionary techniques. Brute forcing e-mails basically starts with something like a@doeinvestor.net, aa@doeinvestor.net, aaa@doeinvestor.net, aab@doeinvestor.net, abb@doeinvestor.net and continues on from there. Brute forcing basically generates and sends out an e-mail to every possible combination of characters/email addresses at any given domain. A dictionary e-mail spam basically uses all of the words that would be included in a dictionary or combinations of words which generally produce quite a few valid e-mail accounts. This type of method would not be inhibited by using a separate e-mail address for each business account you may have.

We have identified the ISP that these e-mails originated from and our Legal Department has taken the appropriate action to address and prohibit further spam attempts.

We have no reason to believe that any of our systems have been compromised. Ameritrade deploys state of the art firewalls, intrusion detection, anti - virus software as well as employs a full time staff of employee?s dedicated strictly to Information Security and protecting Ameritrade's systems from unauthorized access.

If you have further concerns or inquiries, please e-mail us from our secure Web site's "Contact Us" link located in the "Help Center" or at the bottom of each secure page. For security reasons, we do not answer account specific questions that originate from a source other than the secure Web site.

Sincerely,

XX Technology Support, Ameritrade
Division of Ameritrade, Inc.
==========

Well, looks familiar, doesn't it? Apparently, they have created a formed letter for this. That's ok, I suppose they can't personally answer every inquiry, but what happened next is simply ridiculous!

I wrote them back, explaining I run my own server, I can see and analize all the logs, brute forcing or dictionary method is out of the question, and here is what I got:

==========
From techhelp@ameritrade.com Tue Nov 22 15:13:39 2005
Date: Tue, 22 Nov 2005 15:13:35 -0600 (CST)
From: Ameritrade Technology Support <techhelp@ameritrade.com>
To: XXX@XXX.com
Subject: Re: Ameritrade has received your e-mail (KMM28993511I20725L0KM)

Dear Bigshot:

Thank you for contacting us today regarding your account.

We certainly apologize for any inconvenience this matter may have caused.

We would like to assure you that e-mail did not come from Ameritrade. We appreciate the time you have taken to notify us of this issue.

The ?From:? addresses in an e-mail can be altered so the message appears to originate from a false source, not from actual sender. People who send spam and/or attempt a Phishing scheme will alter the ?From:? address to disguise the true origin of the e-mail and avoid being shut down or caught.

We have no reason to believe that any of our systems have been compromised. Ameritrade uses state-of-the-art firewalls, intrusion detection and anti-virus software. We also employ a full time staff of personnel dedicated strictly to Information Security and protecting Ameritrade?s systems from unauthorized access.

Have a nice afternoon.

If you have further concerns or inquiries, please e-mail us from our secure Web site's "E-mail Us" link. For security reasons, we do not

answer account specific questions that originate from a source other than the secure Web site.

Sincerely,

XX Technology Support, Ameritrade
Division of Ameritrade, Inc.

==========

Huh??? Now they're trying to tell me the "from:" filed can be forged, do I really need that kind of insult? Besides, I have never said the spam came from Ameritrade any time, whether when I called or in my emails, I addressed this as a security concern, but that's all the junk responses I got from them.

After all this, I don't think I would waste another minute contacting them about this issue any more, they are obviously insincere about solving this issue, or don't understand the problem, or both.

Very frustrated...

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!panix!not-for-mail
From: sethb@panix.com (Seth Breidbart)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 22 Nov 2005 22:33:44 +0000 (UTC)
Organization: Society for the Promulgation of Cruelty to the Clueless
Message-ID: <dm06c8$5on$1@reader2.panix.com>
References: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1> <newscache$8smdqi$op2$1@news.rootshell.be>
NNTP-Posting-Host: panix5.panix.com

X-Trace: reader2.panix.com 1132698824 5911 166.84.1.5 (22 Nov 2005 22:33:44 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Tue, 22 Nov 2005 22:33:44 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163839

In article <newscache$8smdqi$op2$1@news.rootshell.be>,
 <ash@fakedomainxx.com> wrote:

>After all this, I don't think I would waste another minute contacting them
>about this issue any more, they are obviously insincere about solving this
>issue, or don't understand the problem, or both.

I think the SEC and NASD are the ones who ought to be notified.
Ameritrade can't just send them its bedbug letter.

Seth

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!nx01.iad01.newshosting.com!newshosting.com!
newsfeed.icl.net!newsfeed.fjserv.net!easynet-quince!easynet.net!feed1.news.be.easynet.net!reader0.news.be.easynet.net!not-for-mail
From: ash@fakedomainxx.com
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <dm06c8$5on$1@reader2.panix.com>
Newsgroups: news.admin.net-abuse.email
X-NNTP-Posting-Host: phenix
Message-ID: <newscache$x3pdqi$p6l$1@news.rootshell.be>
Date: 22 Nov 2005 22:57:34 GMT
NNTP-Posting-Date: 22 Nov 2005 22:57:34 GMT
NNTP-Posting-Host: 217.22.55.50

X-Trace: 1132700254 reader0.news.be.easynet.net 440 [::ffff:217.22.55.50]:44599
X-Complaints-To: abuse@be.easynet.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163849

>   Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
>
>   From: sethb@panix.com (Seth Breidbart)
>   Reply to: Seth Breidbart
>   Date: Tue, 22 Nov 2005 22:33:44 +0000 (UTC)
>   Organization: Society for the Promulgation of Cruelty to the Clueless
>   Newsgroups:
>   news.admin.net-abuse.email
>   Followup to: newsgroup
>   References:
>   <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1>
>   <newscache$8smdqi$op2$1@news.rootshell.be>
>In article <newscache$8smdqi$op2$1@news.rootshell.be>,
> <ash@fakedomainxx.com> wrote:
>
>>After all this, I don't think I would waste another minute contacting them
>>about this issue any more, they are obviously insincere about
solving this
>>issue, or don't understand the problem, or both.
>
>I think the SEC and NASD are the ones who ought to be notified.
>Ameritrade can't just send them its bedbug letter.
>
>Seth

Well, I don't see the angle this has something to do with The SEC and The
NASD, thouth, unless you can prove Ameritrade is the spamer, which I
frankly don't think so. What can be learned here is Ameritrade is not
safe, their tech people are incompetent, and they don't take customers'
complaint seriously. Maybe some news organizations should be notified
about this security breach, let them investigate it and tell it to the
public, I think that's the only thing Ameritrade will pay attention to.

I can understand if they screwed up at some point, virtually everyone will
tiven the right circumstance, but I cannot forgive them for ignoring my
complaint, unable to understand the problem and even insulted me with
their reply.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!local01.nntp.dca.giganews.com!nntp.speakeasy.net!news.speakeasy.net.POSTED!not-for-mail
NNTP-Posting-Date: Tue, 22 Nov 2005 18:16:08 -0600
References: <dm06c8$5on$1@reader2.panix.com> <newscache$x3pdqi$p6l$1@news.rootshell.be>
Message-ID: <cone.1132704970.659656.5557.500@commodore.email-scan.com>
X-Mailer: http://www.courier-mta.org/cone/
From: Sam <sam@email-scan.com>
X-PGP-KEY: http://www.courier-mta.org/KEYS.bin
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Mime-Version: 1.0
Content-Type: multipart/signed;
   boundary="=_mimegpg-commodore.email-scan.com-5557-1132704970-0007";
   micalg=pgp-sha1; protocol="application/pgp-signature"
Date: Tue, 22 Nov 2005 18:16:08 -0600
NNTP-Posting-Host: 216.254.115.84
X-Trace: sv3-GHyArh5WJkpDJjsvkpDAMgvrh+Wf0x+NG+NDN5UvdtT40+8U9qIYOzthd/dMmxWnfufYV+9ph7YIFvo!
0DN6vtZ5A2q7Sd78bGusDgkhIFoKVzEGGbrDxzvUq7iXfyFUAY/kISq28cb7JRG4D5MXbs0gfCwd!twyATviWauJ
+UWbMnhJLTnE4bWkRQ2nwSJihdpmW1neV
X-Complaints-To: abuse@speakeasy.net
X-DMCA-Complaints-To: abuse@speakeasy.net
X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your complaint properly
X-Postfilter: 1.3.32
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163853

This is a MIME GnuPG-signed message. If you see this text, it means that
your E-mail or Usenet software does not support MIME signed messages.
The Internet standard for MIME PGP messages, RFC 2015, was published in 1996.
To open this message correctly you will need to install E-mail or Usenet
software that supports modern Internet standards.

--=_mimegpg-commodore.email-scan.com-5557-1132704970-0007
Content-Type: text/plain; format=flowed; charset="US-ASCII"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit

ash@fakedomainxx.com writes:

>
>   [re: spam runs to ameritrade-only E-mail addresses]

>>I think the SEC and NASD are the ones who ought to be notified.
>>Ameritrade can't just send them its bedbug letter.
>>
>>Seth
>
> Well, I don't see the angle this has something to do with The SEC and The
> NASD, thouth, unless you can prove Ameritrade is the spamer, which I
> frankly don't think so.

Well, if you're really crafty with words, you can frame it from the
viewpoint of this being evidence that Ameritrade's internal systems have
possibly been compromised by an outside third party, putting their
customers' financial information at risk, potentially leading to identity
fraud.

That might be something where the SEC or NASD might have standing.

You really need to be familiar with the various securities and trading
regulations. If you can find some bullshit statute saying something like
SEC/NASD members must keep their customers' personal information
confidential, blah blah blah, you might succeed in getting your foot in the
door this way. **This is probably not enough for anyone to get interested in
formally investigating Ameritrade, but might be good enough for a generic
inquiry letter to Ameritrade from SEC/NASD, which should motivate somewhere
@Ameritrade to get their shit together and figure out what happened.**

> complaint seriously. Maybe some news organizations should be notified
> about this security breach, let them investigate it and tell it to the
> public, I think that's the only thing Ameritrade will pay attention to.

That's another angle. If you can get a dozen people to complain to CNet,
for example, some reporter of theirs might end up calling Ameritrade for
comment, which again should get somebody's attention.

--=_mimegpg-commodore.email-scan.com-5557-1132704970-0007
Content-Type: application/pgp-signature
Content-Transfer-Encoding: 7bit

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.7 (GNU/Linux)

iD8DBQBDg7TKx9p3GYHlUOIRAqbdAJ9Fz2cRZ1n0/v+boM4Em3g+uAyF8QCeKmW7
KpIgMgoIT3nPkm1KowwnSV4=
=EZIe
-----END PGP SIGNATURE-----

--=_mimegpg-commodore.email-scan.com-5557-1132704970-0007--

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newscon06.news.prodigy.com!prodigy.net!
newsfeed-00.mathworks.com!panix!not-for-mail

From: sethb@panix.com (Seth Breidbart)
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Wed, 23 Nov 2005 01:12:08 +0000 (UTC)
Organization: Society for the Promulgation of Cruelty to the Clueless
Message-ID: <dm0fl8$n2q$1@reader2.panix.com>
References: <dm06c8$5on$1@reader2.panix.com> <newscache$x3pdqi$p6l$1@news.rootshell.be>
NNTP-Posting-Host: panix5.panix.com
X-Trace: reader2.panix.com 1132708328 23642 166.84.1.5 (23 Nov 2005 01:12:08 GMT)
X-Complaints-To: abuse@panix.com
NNTP-Posting-Date: Wed, 23 Nov 2005 01:12:08 +0000 (UTC)
X-Newsreader: trn 4.0-test76 (Apr 2, 2001)
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163866

In article <newscache$x3pdqi$p6l$1@news.rootshell.be>,
 <ash@fakedomainxx.com> wrote:
>> From: sethb@panix.com (Seth Breidbart)

>>I think the SEC and NASD are the ones who ought to be notified.
>>Ameritrade can't just send them its bedbug letter.

>Well, I don't see the angle this has something to do with The SEC and The
>NASD, thouth, unless you can prove Ameritrade is the spamer, which I
>frankly don't think so. **What can be learned here is Ameritrade is not**
>safe, their tech people are incompetent,

And that's just what the SEC and NASD should investigate.

We _know_ they leaked email addresses.

We _don't_ know what other security holes they might have.

How do you know they _didn't_ also leak account numbers and passwords?

Seth

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed00.sul.t-online.de!t-online.de!tiscali!
newsfeed1.ip.tiscali.net!news.tele.dk!news.tele.dk!small.news.tele.dk!news.astraweb.com!newsrouter-eu.astraweb.com!hwmnpeer01.ams!
nntp.telenet.be!feed1.news.be.easynet.net!reader0.news.be.easynet.net!not-for-mail
From: ash@fakedomainxx.com
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <dm0fl8$n2q$1@reader2.panix.com>
Newsgroups: news.admin.net-abuse.email
X-NNTP-Posting-Host: phenix
Message-ID: <newscache$2pvdqi$4y1$1@news.rootshell.be>
Date: 23 Nov 2005 01:19:50 GMT
NNTP-Posting-Date: 23 Nov 2005 01:19:50 GMT
NNTP-Posting-Host: 217.22.55.50
X-Trace: 1132708790 reader0.news.be.easynet.net 446 [::ffff:217.22.55.50]:48549
X-Complaints-To: abuse@be.easynet.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163869

> Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
>
> From: sethb@panix.com (Seth Breidbart)
> Reply to: Seth Breidbart
> Date: Wed, 23 Nov 2005 01:12:08 +0000 (UTC)
> Organization: Society for the Promulgation of Cruelty to the Clueless
> Newsgroups:
> news.admin.net-abuse.email
> Followup to: newsgroup
> References:
> <dm06c8$5on$1@reader2.panix.com>
> <newscache$x3pdqi$p6l$1@news.rootshell.be>
>In article <newscache$x3pdqi$p6l$1@news.rootshell.be>,
> <ash@fakedomainxx.com> wrote:
>>> From: sethb@panix.com (Seth Breidbart)
>

>>>I think the SEC and NASD are the ones who ought to be notified.
>>>Ameritrade can't just send them its bedbug letter.
>
>>Well, I don't see the angle this has something to do with The SEC and The
>>NASD, thouth, unless you can prove Ameritrade is the spamer, which I
>>frankly don't think so. What can be learned here is Ameritrade is not
>>safe, their tech people are incompetent,
>
>And that's just what the SEC and NASD should investigate.
>
>We _know_ they leaked email addresses.
>
>We _don't_ know what other security holes they might have.
>
>How do you know they _didn't_ also leak account numbers and passwords?
>
>Seth

Okay guys, looks like we shall do something about this, I myself am not
happy about the whole episode at all.

We can all go our separate ways and take whatever actions, or we can setup
a contact point, like an email address, so we can work together. Any
thought?

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed00.sul.t-online.de!t-online.de!
newsfeed.freenet.de!news.newsland.it!ilaria.aioe.org!aioe.org!not-for-mail
From: PCBoy <News.20.PCBoy@sp
amgourmet.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Wed, 23 Nov 2005 04:12:23 +0000 (UTC)
Organization: MiloMinderBinderInc
Message-ID: <Xns97178217C8DD5News.20.PCBoyspamgou@127.0.0.1>
References: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1> <newscache$8smdqi$op2$1@news.rootshell.be>
NNTP-Posting-Host: 5ZEDTKZ0WL5MQcEvBNS0sQ.894.domitilla.aioe.org
X-Complaints-To: abuse@aioe.org
User-Agent: Xnews/5.04.25 Hamster/2.1.0.0
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2163911

ash@fakedomainxx.com wrote in
news:newscache$8smdqi$op2$1@news.rootshell.be:

Ooops sorry for making the thread huge I expect to be bypassed in the
discussion tree or mainly snipped.

>
[.. original content]
> PC Boy said
>>
>>... sorry I am not even in the loop re: email your email addr
>> issues. But computing P values for co-incidences seen in the
>> wild is something I have studied before ...]
>>
>><rant_filters insert = now> <soap_box action = climbs onto >
  [...removed...]
>></soap_box> </rant_filters>

>
> 3) I run my own server, so all the talk about brute force attack or
> dictionary technique is simply BS, I can review my system logs and see
> exactly what happened, the spammers obviously knew the address.

Or the spammers, tried one fake address at every domain they had.
At your domain you see 1 sucessful attack. Nearly every other domain
see's one dumb guess. This is not inconsistent with your logs (the
evidence) it is only highly unlikely because of the default hypothesis is
      Rule #3: Spammers are stupid.

Note on balance I believe you the spammer knew you address and got it
from someone who had it. I can prove it, but I believe it to be true.

[...everything else...]

I agree the rant was because allowing stats to be misused is in my
experience the first tsep to believing in UFO's, esp, Xena(sic)
etc. Note I am not accusing anyone here, of being credulous, but
there may be credulous lurkers...

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
o13g2000cwo.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 9 Dec 2005 12:43:10 -0800
Organization: http://groups.google.com
Message-ID: <1134160990.466487.185310@o13g2000cwo.googlegroups.com>
References: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1>
  <newscache$8smdqi$op2$1@news.rootshell.be>
  <Xns97178217C8DD5News.20.PCBoyspamgou@127.0.0.1>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1134160995 5705 127.0.0.1 (9 Dec 2005 20:43:15 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Fri, 9 Dec 2005 20:43:15 +0000 (UTC)
In-Reply-To: <Xns97178217C8DD5News.20.PCBoyspamgou@127.0.0.1>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8) Gecko/20051111 Firefox/1.5,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: o13g2000cwo.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3lYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2166410

Hello PC Boy,

Please read about Occam's Razor. The evidence from everyone that has
(a) been tagged by this spam and (b) run their own mail servers and (c)
are smart enough to establish random email addresses assigned to
specific companies is overwhelmingly in favor of one conclusion:
Ameritrade has leaked at least our email addresses (and possibly more),
either accidentally (bug in system that is exploited outside
Ameritrade), or on purpose (dishonest employee). Either way it's a very
bad issue that they are trying to sit on.

**I filed a complaint with the SEC as I see this as a serious leak of
private information from a popular online brokerage. This is directly
in the SEC's purview. I urge others in this thread that are similarly
affected should contact the SEC also. I gave Ameritrade plenty of time
to address the issue honestly. I would have accepted an honest "Whoops,
our system had a bug. Whoops we hired a bad employee that has been
fired and is being sued by us.", etc. Instead they are trying to hide
behind a response that I know is about as likely as me winning the
lotto.**

**So I filed a complaint with the SEC. (The response from the SEC to me
is below.) If I do not see anything further on this by the end of
December, I will file another complaint with the SEC, and consider**

whether I need to seek counsel. All I want out of this is for Ameritrade to honestly find/reveal how the information was released, WHAT information was released, what they have done to rectify the problem. That's it. Doesn't seem like too much.

Response from the SEC follows.

Dear XXXXXX:

I am confirming that we received your complaint concerning Ameritrade. We take investor complaints very seriously and try, whenever possible, to provide some form of assistance.

We have sent your complaint to the firm's compliance department and asked them to respond directly to you. We also asked the firm to send us a copy of their letter to you. Please understand that this process may take four to eight weeks.

Our efforts to facilitate informal resolutions of complaints often succeed. But, in some cases, it remains unclear whether any wrongdoing occurred, or the dispute boils down to one person's word against another's. If that happens, we cannot act as your personal representative or attorney, and you will then have to decide whether you want to pursue legal action on your own. The following portion of this email outlines the steps you may wish to take if you choose that option, and includes information on arbitration, mediation, and sources of potential legal assistance. Please read this information carefully. It describes your rights and important deadlines.

Please do not hesitate to contact me if you have any questions.

Sincerely,

APRIL B KEYES
U.S. Securities and Exchange Commission
(202)551-6309

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newshub.sdsu.edu!tethys.csu.net!nntp.csufresno.edu!sn-xit-02!sn-xit-11!sn-xit-05!sn-post-01!supernews.com!news.supernews.com!not-for-mail
From: PCBoy <News.20.PCBoy@spamgourmet.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Sat, 10 Dec 2005 14:25:50 -0000
Organization: MiloMinderBinderInc
Message-ID: <Xns972990963FC0News.20.PCBoyspamgou@127.0.0.1>
References: <Xns971684C96B036News.20.PCBoyspamgou@127.0.0.1> <newscache$8smdqi$op2$1@news.rootshell.be> <Xns97178217C8DD5News.20.PCBoyspamgou@127.0.0.1> <1134160990.466487.185310@o13g2000cwo.googlegroups.com>
User-Agent: Xnews/5.04.25 Hamster/2.1.0.0
X-Complaints-To: abuse@supernews.com
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2166499

"Thomas" <tomwinzig@gmail.com> wrote in news:1134160990.466487.185310
@o13g2000cwo.googlegroups.com:

> Hello PC Boy,
>
> Please read about Occam's Razor.
done already.
> The evidence from everyone that has
> (a) been tagged by this spam and (b) run their own mail servers and (c)
> are smart enough to establish random email addresses assigned to
> specific companies is overwhelmingly in favor of one conclusion:
> Ameritrade has leaked at least our email addresses (and possibly more),
> either accidentally (bug in system that is exploited outside
> Ameritrade), or on purpose (dishonest employee). Either way it's a very
> bad issue that they are trying to sit on.

Just a suggestion

I wonder if they are not really being willfuly stupid it is just that
they expect a certain kind of complaint at abuse@ They may get lots of
people/endLusers complaining back to a spams forged from: and your legit
complaint just got lost in the noise of endLuser LARTS ...
Perhaps searching for some other clueful point of entry eg webmaster@
hostmaster@ etal might get parsed more intelligently as they get less
fluff. You shouldnt have to, but it might work...

Sorry its been little while since I posted the last post in this thread
but I think at the time I was not aware of multiple indpendent
observations of leakage. Fundamentally I think I was responding because I
perceived 1 observation of something thought to be unlikely, and I was
only trying to highlight the dangers of extrapolating from 1 point even
if it is very strange. If multiple people get their frist spam with an
address only given to Ameritrade, an other people dont see matching
failed dictionary attacks that is most certainly strong statiscial
evidence.

I also said.
>Note on balance I believe you the spammer knew you address and got it
>from someone who had it. I can(t) prove it, but I believe it to be true.
mistyped t added, but I dont think it was the cause of confusion

Sorry if I seemed negative about whacking a spammer, or a source of info
for spammers, or ... That was never my intention.

> I filed a complaint with the SEC as I see this as a serious leak of
> private information from a popular online brokerage. This is directly
> in the SEC's purview. I urge others in this thread that are similarly
> affected should contact the SEC also. I gave Ameritrade plenty of time
> to address the issue honestly. I would have accepted an honest "Whoops,
> our system had a bug. Whoops we hired a bad employee that has been
> fired and is being sued by us.", etc. Instead they are trying to hide
> b
ehind a response that I know is about as likely as me winning the
> lotto.

> So I filed a complaint with the SEC. (The response from the SEC to me
> is below.) If I do not see anything further on this by the end of
> December, I will file another complaint with the SEC, and consider
> whether I need to seek counsel. All I want out of this is for
> Ameritrade to honestly find/reveal how the information was released,
> WHAT information was released, what they have done to rectify the
> problem. That's it. Doesn't seem like too much.
>
> Response from the SEC follows.
>
> Dear XXXXXX:
>
> I am confirming that we received your complaint concerning Ameritrade.
> We take investor complaints very seriously and try, whenever possible,
> to provide some form of assistance.
>
> We have sent your complaint to the firm's compliance department and
> asked them to respond directly to you. We also asked the firm to send
> us a copy of their letter to you. Please understand that this process
> may take four to eight weeks.
>
> Our efforts to facilitate informal resolutions of complaints often
> succeed. But, in some cases, it remains unclear whether any wrongdoing
> occurred, or the dispute boils down to one person's word against
> another's. If that happens, we cannot act as your personal
> representative or attorney, and you will then have to decide whether
> you want to pursue legal action on your own. The following portion of
> this email outlines the steps you may wish to take if you choose that
> option, and includes information on arbitration, mediation, and sources
> of potential legal assistance. Please read this information carefully.
> It describes your rights and important deadlines.
>
> Please do not hesitate to contact me if you have any questions.
>
> Sincerely,
>
> APRIL B KEYES
> U.S. Securities and Exchange Commission
> (202)551-6309

It will indeed be intriguing to see how effective filing a complaint with
the SEC turns out to be. Banging my head LARTing spammers to places that
dont do anything, is something I avoid. I dont usually LART to ISPs
listed in spews.

Anyway if I appeared to be being negative sorry.

PC Boy.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
f14g2000cwb.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 12 Dec 2005 08:31:37 -0800
Organization: http://groups.google.com
Message-ID: <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
  <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1134405101 10670 127.0.0.1 (12 Dec 2005 16:31:41 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Mon, 12 Dec 2005 16:31:41 +0000 (UTC)
In-Reply-To: <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8) Gecko/20051111 Firefox/1.5,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: f14g2000cwb.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2166809

Received yet another variation on this spam on my Ameritrade address.
Still pumping SNFX. I guess Ameritrade's excuse that they contacted the
ISPs affected by this and stopped the spammers is a bunch of BS (which
we already knew). So that makes two in December. I believe I have
received 4 or 5 of these ameritrade-related spams now, each one has
been pumping only SNFX.

Headers on this one (munged):

Return-Path: <paradigms@archithema.ch>
Received: from 60.6.23.240 (unverified [60.6.23.240]) by xxxxxxxxxxxx
 with SMTP for <[xxxxxxxxxxxxxxxxxx]>;
 Mon, 12 Dec 2005 01:45:46 -0800 (PST)
Received: from [192.168.62.39] (port=10377 helo=Unitarians)
    by 60.6.23.240 with esmtp
    id 6641311502614499
    for xxxxxxxxxxxxxxxxxxxxxt; Mon, 12 Dec 2005 17:55:39 +0800
MIME-Version: 1.0
Content-Type: multipart/related;
        boundary="=_49631bbb36756b28a8eb4fd9b7e1c8b5"
Date: Mon, 12 Dec 2005 17:55:30 +0800
To: <xxxxxxxxxxxxxxxxxxxxxxxxx>
From: <paradigms@archithema.ch>
Subject: Market news from feature anthropomorphic

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newsfeed00.sul.t-online.de!t-online.de!fr.ip.ndsoftware.net!nerim.net!feed1.news.be.easynet.net!reader0.news.be.easynet.net!not-for-mail
From: ash@fakedomainxx.com
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Organization: ash
References: <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
Newsgroups: news.admin.net-abuse.email
X-NNTP-Posting-Host: phenix
Message-ID: <newscache$ekmeri$8cl$1@news.rootshell.be>
Date: 12 Dec 2005 21:34:10 GMT
NNTP-Posting-Date: 12 Dec 2005 21:34:10 GMT
NNTP-Posting-Host: 217.22.55.50
X-Trace: 1134423250 reader0.news.be.easynet.net 440 [::ffff:217.22.55.50]:32826
X-Complaints-To: abuse@be.easynet.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2166886

> Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
>
> From: "Thomas" <tomwinzig@gmail.com>
> Reply to: "Thomas"
> Date: 12 Dec 2005 08:31:37 -0800
> Organization: http://groups.google.com
> Newsgroups:
> news.admin.net-abuse.email
> Followup to: newsgroup
> References:
> <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
> <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
>Received yet another variation on this spam on my Ameritrade address.
>Still pumping SNFX. I guess Ameritrade's excuse that they contacted the
>ISPs affected by this and stopped the spammers is a bunch of BS (which
>we already knew). So that makes two in December. I believe I have
>received 4 or 5 of these ameritrade-related spams now, each one has
>been pumping only SNFX.
>
>Headers on this one (munged):
>
>Return-Path: <paradigms@archithema.ch>
>Received: from 60.6.23.240 (unverified [60.6.23.240]) by xxxxxxxxxxxx
> with SMTP for <[xxxxxxxxxxxxxxxxx]>;
> Mon, 12 Dec 2005 01:45:46 -0800 (PST)
>Received: from [192.168.62.39] (port=10377 helo=Unitarians)
> by 60.6.23.240 with esmtp
> id 6641311502614499
> for xxxxxxxxxxxxxxxxxxxxt; Mon, 12 Dec 2005 17:55:39 +0800
>MIME-Version: 1.0
>Content-Type: multipart/related;
> boundary="=_49631bbb36756b28a8eb4fd9b7e1c8b5"
>Date: Mon, 12 Dec 2005 17:55:30 +0800
>To: <xxxxxxxxxxxxxxxxxxxxxxxx>
>From: <paradigms@archithema.ch>
>Subject: Market news from feature anthropomorphic

Contacted ISP's? That is soooo lame and so insulting, their reply to me saying the "from:" field can be forged is even more insulting. Who the hell do these incompetent people at Ameritrade think they're dealing with?

The spams I got for example originated from Korea and Span, what a damn thing can Ameritrade do a damn thing about it by contacting the isp's? Nobody wants them to contact any isp's or stop the spam (unless the spam comes from their machines), what we want is for Ameritrade to tell the truth, i.e., what heppened, what has been compromised and what has been done about it. some of you guessed their employees leaked the info, without the straight answer frm Ameritrade, my thinking is that their systems have been compromised, or at least were compromised at some point.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
g44g2000cwa.googlegroups.com!not-for-mail
From: "Thomas" <tomwinzig@gmail.com>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 14 Dec 2005 17:03:40 -0800
Organization: http://groups.google.com
Message-ID: <1134608620.245861.184120@g44g2000cwa.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
  <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
  <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
NNTP-Posting-Host: 24.126.180.194
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1134608625 5478 127.0.0.1 (15 Dec 2005 01:03:45 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Thu, 15 Dec 2005 01:03:45 +0000 (UTC)
In-Reply-To: <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8) Gecko/20051111 Firefox/1.5,gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: g44g2000cwa.googlegroups.com; posting-host=24.126.180.194;
  posting-account=2y_Ebw0AAAAX5uaNo2U94xdN3IYR3OmX
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2167201

Latest spam came today. Headers below (munged). Body is a GIF of the
spam, this time promoting MDEX (all previous promotions were for SNFX).

Return-Path: <apparatus@estupinan.com>
Received: from pc019.abu.org.my (unverified [202.189.26.19]) by
xxxxxxxxxxxxx
 with SMTP for <xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>; Wed, 14 Dec 2005
16:50:11 -0800 (PST)
Received: from [192.168.87.78] (port=20158 helo=secondarily)
        by pc019.abu.org.my with esmtp
        for xxxxxxxxxxxxxxxxxxxxx; Thu, 15 Dec 2005 08:50:08 +0800
MIME-Version: 1.0
Content-Type: mu
ltipart/related;
        boundary="=_9317f818d6cef74ebebeeb9a16b25d6d"
Date: Thu, 15 Dec 2005 08:50:05 +0800
To: <xxxxxxxxxxxxxxxxxxxxx>
From: <apparatus@estupinan.com>
Subject: market recomendation emigrants

I will start a blog for this problem soon to try and put some pressure
on Ameritrade to come clean. (They didn't even respond to my latest
email on this topic a couple days ago.)

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!postnews.google.com!
f14g2000cwb.googlegroups.com!not-for-mail
From: googlegroups@larrysweet.com
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: 20 Dec 2005 15:31:27 -0800
Organization: http://groups.google.com
Message-ID: <1135121487.118807.195060@f14g2000cwb.googlegroups.com>
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
  <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
  <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
  <1134608620.245861.184120@g44g2000cwa.googlegroups.com>
NNTP-Posting-Host: 205.141.247.28
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1135121492 19474 127.0.0.1 (20 Dec 2005 23:31:32 GMT)
X-Complaints-To: groups-abuse@google.com
NNTP-Posting-Date: Tue, 20 Dec 2005 23:31:32 +0000 (UTC)

User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; America Online Browser 1.1; Windows NT 5.0; .NET CLR 1.1.4322),gzip(gfe),gzip(gfe)
Complaints-To: groups-abuse@google.com
Injection-Info: f14g2000cwb.googlegroups.com; posting-host=205.141.247.28;
  posting-account=8sKohA0AAABAZlh3ulQPLG8pZM2MPpTY
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2168126

I too have gotten the various pump and dump spasm to a private email address created only for use with Ameritrade. Pretty much got the same spam as everyone else. Also did not get the spam directed to any email account other than the Ameritrade one. In addition, I have gotten no other spam, except for these pump and dump spams, on my Ameritrade email address.

I too contacted Ameritrade when the first one arrived. I got nothing but a run around, I got multiple copies of the 'dictionary attack' explanation and for the most part my complaints were ignored. They did slip up at one point and acknowledge that I was not the only person making the same complaint. This should have been a clue, but apparently a clue is something that Ameritrade does not possess.

I did file a complaint with the SEC. I got a voice mail and a letter from Ameritrade with the same old crap about they are certain that the problem does not lie on their end and that they have not been hacked or compromised in anyway, blah, blah.... ignoring all the facts that would indicate otherwise.

I had three accounts there and over the past several weeks I have transferred them to other brokerage firms. I just do not feel safe doing business with a company that has obvious security breaches and refuses to acknowledge them. Of course, as I have closed out each account I have been contacted by their retention department with cries of "why would you leave us?" etc. I give them the full detailed explanation of what has happened, and what Ameritrade's response (or lack thereof) has been. They really can't do much but give me a vague "I'll pass along your concerns" type comment. Last account was closed out today.

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newshub.sdsu.edu!newsfeed.news2me.com!sn-xit-15!sn-xit-09!sn-post-01!supernews.com!corp.supernews.com!not-for-mail
From: glgxg <glgxg@mfire.com.invalid>
Newsgroups: news.admin.net-abuse.email
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
Date: Tue, 20 Dec 2005 16:53:26 -0800
Organization: Posted via Supernews, http://www.supernews.com
Message-ID: <11qh9nsq4pd7heb@corp.supernews.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.12) Gecko/20050915
X-Accept-Language: en-us, en
MIME-Version: 1.0
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com> <1132614801.758196.48290@g44g2000cwa.googlegroups.com> <1134405096.997228.242550@f14g2000cwb.googlegroups.com> <1134608620.245861.184120@g44g2000cwa.googlegroups.com> <1135121487.118807.195060@f14g2000cwb.googlegroups.com>
In-Reply-To: <1135121487.118807.195060@f14g2000cwb.googlegroups.com>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Complaints-To: abuse@supernews.com
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2168138

googlegroups@larrysweet.com wrote:

>
> I did file a complaint with the SEC. I got a voice mail and a letter
> from Ameritrade with the same old crap about they are certain that the
> problem does not lie on their end and that they have not been hacked or
> compromised in anyway, blah, blah.... ignoring all the facts that
> would indicate otherwise.
>

http://www.informationweek.com/showArticle.jhtml?articleID=161500879

<quote>
More Customer Data Missing

Retail Ventures and Ameritrade report data mishaps, but a new standard backed by credit-card companies could raise the bar on data protection

By Steven Marlin
InformationWeek

Apr 25, 2005 12:00 AM
.
.
.
Not only are companies compromising security because of credit-card snafus, they're also misplacing data. Last week, Ameritrade Inc. said it misplaced four backup tapes. Three were recovered, but the fourth remains missing. The online-trading company has alerted 200,000 current and former customers whose information was stored on the tape. The incident echoes a case involving Bank of America Corp., which said in February that it lost an undisclosed number of backup tapes.
.
.
.
</quote>

Did they ever recover the fourth missing tape? It is very likely that that tape had email addresses on it & probably was sold on the blackmarket.

http://www.google.com/search?hl=en&q=Ameritrade+%2Bmissing+tape

----------070309010004030400030507
Content-Type: message/rfc822;
 name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newshub.sdsu.edu!peer01.west.cox.net!cox.net!feeder2.ecngs.de!ecngs!feeder.ecngs.de!feed1.news.be.easynet.net!reader0.news.be.easynet.net!not-for-mail
From: ash@fakedomainxx.com
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
References: <1135121487.118807.195060@f14g2000cwb.googlegroups.com>
Newsgroups: news.admin.net-abuse.email
X-NNTP-Posting-Host: phenix
Message-ID: <newscache$7wouri$wae$1@news.rootshell.be>
Date: 21 Dec 2005 13:45:43 GMT
NNTP-Posting-Date: 21 Dec 2005 13:45:43 GMT
NNTP-Posting-Host: 217.22.55.50
X-Trace: 1135172743 reader0.news.be.easynet.net 443 [::ffff:217.22.55.50]:49709
X-Complaints-To: abuse@be.easynet.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2168292

To get Ameritrade serious about this, you need to subpoena its computer records, that's the only way you can show their systems were compromised at some point. YOu also need the computer records of your email provider, that's the only way you can show no discionary attacks ever took place, I can certainly provide this part of evidence, as I stated before, I run my own mail servers, but most of you don't. I am not a pessimist, but what things are going now won't lead you anywhere. For example, if Ameritrade says the problem is at your end, it's a dictionary attack or some bullshit, how do you prove otherwise.

I thought about this before, that's why I suggested we pool our resources together, aut apparently nobody was interested, perhaps you guys just don't trust people you talk to on the net? I could have gone thru all the necessary steps above, but I just didn't think it's worth it, especially when I have to do this all on my own. I have since moved my accounts elsewhere.

> Re: Ameritrade leaking email addresses to Sniffex pump n dumper?

>
> From: googlegroups@larrysweet.com
> Reply to: googlegroups@larrysweet.com
> Date: 20 Dec 2005 15:31:27 -0800
> Organization: http://groups.google.com
> Newsgroups:
> news.admin.net-abuse.email
> Followup to: newsgroup
> References:
> <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
> <1132614801.758196.48290@g44g2000cwa.googlegroups.com>
> <1134405096.997228.242550@f14g2000cwb.googlegroups.com>
> <1134608620.245861.184120@g44g2000cwa.googlegroups.com>
>I too have gotten the various pump and dump spasm to a private email
>address created only for use with Ameritrade. Pretty much got the same
>spam as everyone else. Also did not get the spam directed to any email
>account other than the Ameritrade one. In addition, I have gotten no
>other spam, except for these pump and dump spams, on my Ameritrade
>email address.
>
>I too contacted Ameritrade when the first one arrived. I got nothing
>but a run around, I got multiple copies of the 'dictionary attack'
>explanation and for the most part my complaints were ignored. They did
>slip up at one point and acknowledge that I was not the only person
>making the same complaint. This should have been a clue, but
>apparently a clue is something that Ameritrade does not possess.
>
>I did file a complaint with the SEC. I got a voice mail and a letter
>from Ameritrade with the same old crap about they are certain that the
>problem does not lie on their end and that they have not been hacked or
>compromised in anyway, blah, blah.... ignoring all the facts that
>would indicate other
wise.
>
>I had three accounts there and over the past several weeks I have
>transferred them to other brokerage firms. I just do not feel safe
>doing business with a company that has obvious security breaches and
>refuses to acknowledge them. Of course, as I have closed out each
>account I have been contacted by their retention department with cries
>of "why would you leave us?" etc. I give them the full detailed
>explanation of what has happened, and what Ameritrade's response (or
>lack thereof) has been. They really can't do much but give me a
>vague "I'll pass along your concerns" type comment. Last account
>was closed out today.

----------070309010004030400030507
Content-Type: message/rfc822;
name="Attached Message"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
filename="Attached Message"

Path: number1.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.giganews.com!newshub.sdsu.edu!elnk-nf2-pas!
newsfeed.earthlink.net!stamper.news.pas.earthlink.net!newsread2.news.pas.earthlink.net.POSTED!dd0ca578!not-for-mail
From: d <news@dharty.remove.b4.sending.converttocom>
Subject: Re: Ameritrade leaking email addresses to Sniffex pump n dumper?
User-Agent: Pan/0.14.2 (This is not a psychotic episode. It's a cleansing moment of clarity.)
Message-Id: <pan.2006.01.16.22.02.21.266411@dharty.remove.b4.sending.converttocom>
Newsgroups: news.admin.net-abuse.email
References: <l6udnUYgrfNJ-fveRVn-pw@comcast.com>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit
Date: Mon, 16 Jan 2006 22:02:31 GMT
NNTP-Posting-Host: 69.34.217.81
X-Complaints-To: abuse@earthlink.net
X-Trace: newsread2.news.pas.earthlink.net 1137448951 69.34.217.81 (Mon, 16 Jan 2006 14:02:31 PST)
NNTP-Posting-Date: Mon, 16 Jan 2006 14:02:31 PST
Organization: EarthLink Inc. -- http://www.EarthLink.net
Xref: number1.nntp.dca.giganews.com news.admin.net-abuse.email:2173921

I too create "private" email addresses for every company I submit my email address to.

Lately I have been receiving SNFX spam to the one I designated to

Ameritrade.

I emailed them about it and after a couple of back and fourths I was directed to read the policy statement stating that the are allowed to disclose "non-public personal information" to *any* non-affiliated third parties. (see contents below)

This to me seems to be a tacit confession of them selling/giving customer email addresses to spammers.

Is the fact that they are giving customer emails to investment spammers/pumpers and dumpers an illegality that should concern the SEC???

D

----------begin ameritrade email ----------

Mr. XXXXX,

As discussed in our Privacy Statement
(https://wwws.ameritrade.com/cgi-bin/apps/u/PLoad?pagename=legal/privacy_statement.html),
we may disclose non-public personal information to non-affiliated third
parties. However, you may opt out of sharing your non-public personal
information at any time. To do so, follow these steps:

1. At the bottom of any page on the Web site, click the link labeled Privacy, Security and other Important Information.

2. From the drop-down menu, select Privacy Statement.

3. Click the topic "Can I opt out of sharing my personal information with non-affiliated third parties?"

4. Click Opt Out in the second paragraph.

5. Select the button in front of the phrase "No, please do not share my personal and financial information with outside companies you contract with to provide financial products and services."

6. Click Save Changes.

An opt-out election must be made for each separate account you own at Ameritrade. An opt-out election made by one account owner of a joint account is applicable to all account owners of the joint account.

Have a nice day!

Dawn S.
Technology Support, Ameritrade
Division of Ameritrade, Inc.

----------end ameritrade email ----------

On Mon, 31 Oct 2005 13:39:26 -0500, User N wrote:

> I create unique, "private" email addresses for every company I submit my email
> address to. This morning I hooked something. The following UBE was sent to
> an email address that was only given to Ameritrade. I checked two of my more
> public/exposed email addresses and neither of them received the UBE. I know
> someone else who has an Ameritrade account and asked them if they received
> the same UBE.... they did. It was sent via a different path and some header
> fields are rotated, but otherwise it is identical and it was sent within a few minutes
> of mine.
>
> Did anyone else receive a copy sent to an Ameritrade-unique email address?
> Did anyone receive a copy sent to an email address NOT given to Ameritrade?
>
>

----------070309010004030400030507--