

Re: impersonating users on usenet

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-04/msg00294.html>

- *From:* "Chip Eastham" <hardmath@xxxxxxxxxx>
 - *Date:* 2 Apr 2006 15:57:10 -0700
-

quasi wrote:

On 2 Apr 2006 11:22:00 -0700, "Chip Eastham" <hardmath@xxxxxxxxxx>
wrote:

Chip Eastham wrote:

quasi wrote:

On Sun, 2 Apr 2006 04:42:57 +0000 (UTC),
magidin@xxxxxxxxxxxxxxxxxxxx
(Arturo Magidin) wrote:

In article
<9fju22tmevpgi6grmeehvg17ibv8aj8q12@xxxxxxxx>,
quasi <quasi@xxxxxxxx>
wrote:

On 02 Apr
2006
04:01:37
GMT,
Peter-Lawrence.Montgomery@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(Peter L.
Montgomery)
wrote:

If you look
at the
headers of
the post to
which I'm
replying,

Re: impersonating users on usenet

you'll
see they
don't
match that
of the real
Peter L.
Montgomery.

However,
except for
the spoofed
username
and email,
the headers
of the
above post
do match
the post
from this
morning in
which my
username
and email
were
spoofed.

In other
words, it's
the same
user,
playing
games by
posting
replies
using names
and emails
of other
users.

So far, the
two such
bogus posts
which I've
noted were
verbatim
copies
used of a
prior real
reply from
the real
user, so no

Re: impersonating users on usenet

apparent
harm was
done.

It's happened to me three
times as well; twice last
November, once
recently.

I don't know if it is
->someone<-, or if
somehow there is a hiccup
in
some server that is causing
this.

But since
the
perpetrator
has done it
twice now
(twice that
I'm aware
of anyway),
impersonating
2 different
real users, it
makes it
absolutely
clear that
it's no
accident. I
guess we
could
complain to
the user's
news
provider
(readfreenews.net)
and get the
user's
usenet
account
canceled,
but I don't
really have
the time
right now to
figure

Re: impersonating users on usenet

out who to
contact and
what proof
to send
them.

I contacted them when the
two spoofs of posts of mine
(also verbatim,
also with the address
modified exactly as this one
and as the ones you
report). I never got any
reponse.

I don't think it's a "hiccup in some server"
since it's being posted
by a specific user from readfreenews.net.

Also note that the bogus posts all have the
header field:

User-Agent: newsSync (Sci4um) 254937

which implies that the spoofed post was
posted using newsSync as the
news posting program as opposed to
whatever application was used by
the original poster. If it was just a hiccup, it
seems likely that the
user application field would have been left
unchanged.

It's very possible that the impersonator
randomly hits many usenet
groups, not just sci.math, and if so, it could
be a prelude to a wider
attack.

Because of the uniformity with which the
header fields were modified,
and the fact that the content of the spoofed
post, so far, has always
been an exact copy of a prior real one, I
believe it's probably being
done by a script, rather than manually. Still,
even if it's a script,
I'm fairly certain that the script is being run
by an actual user.

Re: impersonating users on usenet

Drifting off into conspiracy theory ...

It's very possible that the power elites are aware of usenet and feel somewhat threatened by it. After all, usenet is one of the few remaining outlets for true free speech. Usenet has often been the source of key information, exposing the lies and omissions of the official propaganda. Given that the elites don't have the power (not yet) to censor usenet or suppress it, the next best thing is to destroy it from within.

Perhaps, as a training run, they have started writing low profile, essentially innocent scripts, just to test the waters.

Anyone remember the episode from The Twilight Zone (I forget the title), where aliens arrive and by clever manipulation, lure the residents of a small town into false suspicions of each other, leading to escalating paranoia and finally chaos.

Without some way of being able to verify who is the real user, a wide scale spoofing attack could provoke similar paranoia, driving many users off usenet, effectively sabotaging it.

Fantasy? Maybe.

Ok, end of conspiracy theory speculation -- back to "reality".

Well, let's keep an eye on these posts.

If anyone has the knowledge of how to search google groups for usenet headers, I'd be curious how often that particular readfreenews.net account has been used in sci.math and it would be interesting to know if it's been used in other newsgroups besides sci.math.

Re: impersonating users on usenet

Hi, quasi:

I think it possible that the bulletin board in question, which tries to give a Web-based reader for various newsgroups, occasionally mistakes a post from an external feed for one posted through the site, and duplicates it innocently in sending this "new" post out to Usenet.

I wrote:

I've sent a note to the bulletin board hosting company & will share their reply when one is received.

I got a prompt response, acknowledging the (likely) bug in a script and stating that the script has been stopped while investigating and fixing it. Not bad for a Sunday morning, eh?

regards, chip

Thanks, chip.

I appreciate your taking the trouble to resolve it.

quasi wrote:

You may have saved usenet, all in a Sunday morning.
With such a good start, why stop at that?

Frankly, I don't normally engage in conspiracy theories, but while I've been sitting here at my keyboard, someone drank my latte and finished it all gone! No more help on homework problems until I get an apology and refill !!!

regards, chip

quasi

Re: impersonating users on usenet