

Re: Server hacked?

Re: Server hacked?

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2008-01/msg00117.html>

- *From:* NoOp <glg@g@xxxxxxxxxxxxxx>
 - *Date:* Wed, 02 Jan 2008 11:24:07 -0800
-

On 01/01/2008 04:35 PM, Joris Dobbelsteen wrote:

It also has wonk.tar.gz from 2007-03-18.

Anyone familiar with this?

Can you check to see if that is actually a .gz file and if so what's in it? I found one here:

<<http://www.google.com/search?hl=en&q=wonk.tar.gz&btnG=Google+Search>>

Googles 'Cached' shows the file but it is a text file. If you go up to the parent directory: <http://intranet.icbernareggio.it/pmb/>

It shows the the site is hacked:

```
<~quote>  
this site is hacked by ksa hackers ravenous  
</~quote>
```

====

<http://intranet.icbernareggio.it/pmb/>

--- contacting host intranet.icbernareggio.it [81.72.3.35] on port 80

HTTP/1.1 200 OK

Date: Wed, 02 Jan 2008 19:11:14 GMT

Server: Apache/2.0.54 (Debian GNU/Linux) PHP/4.3.10-22 mod_ssl/2.0.54

OpenSSL/0.9.7e mod_perl/1.999.21 Perl/v5.8.4

X-Powered-By: PHP/4.3.10-22

Connection: close

Transfer-Encoding: chunked

Content-Type: text/html

====

Using email addys from the page finds more:

Re: Server hacked?

Re: Server hacked?

<<http://www.google.com/search?hl=en&q=arar3%40HotMaiL.CoM&btnG=Search>>

<<http://www.google.com/search?hl=en&q=brincarar%40HotMaiL.CoM&btnG=Search>>

<http://www.google.com/search?hl=en&q=hetlar_north%40HotMaiL.CoM&btnG=Search>

and

<<http://www.google.com/search?hl=en&q=ksa+hackers&btnG=Google+Search>>

Perhaps that will provide some clues as to what else may have been compromised on your system. Good luck!

--

ubuntu-users mailing list

ubuntu-users@xxxxxxxxxxxxxxxxx

Modify settings or unsubscribe at: <https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>