**TOR 2 DOWNTIME**

## TOR 2.2 PAGE IS DIFFERENT

Tor page changed again. We noticed the change at about: 06:31 AM 14.1.2013 (GMT)

<\*html>

<\*head><title>3301</title><\*/head>

<\*body>

<\*pre>-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

You already have everything you need to continue.

Sometimes one must "knock on the sky and listen to the sound."

Good luck.

3301

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJQ85gbAAoJEBgfAeV6NQkP6joP/iHzBMvK6YZO24wv24RtstGJ

dEMrC9BjtUhrB+F0++sHqWeYuueZ37bDstIoh6EOenRHpECD0QBPTc40aUl2Op1L

4NuUVCUQvfqo/kdWBmSdTP4xGoCtwcXoISfhSM/i+wXqRONSy4z0FrXA3N9yxFaK

eqlNk47aZvyWWHcyYACUEar/V4kfGo8j58r2CisnfeNwat6I6ZfL9P370UVJQyG1

a0WV7rF015TLbwAJkwI1jX7GLPWOkRK3lP8qLJJodNvMPSSyUPyPB01ElgBopm+t

U9bQb/wIGtGG74ezUvwhtDGtXJLWllZtrZx82mQQWzzn8hReqqX0T35idJlTfxIz

aZDNjLCOQJZCngmXEN7iz47w/g67BQ5eoa6iEj7blFwzMwVO7M7pL+L6LZLnuXml

Zv1oDNCuENrIo4j8VGLro9pLptiilsUA6xFRS9bfE7qeeBfmS4J8DScOddzLYNVv

5fKd6iaLJoAqJGkcKnAWPl5VViDhYRL0z1N80zpjm1cWtPBIS2odLMZT80VfMYQI

8XXaEmRqoP8/9EImapqeSk+qcrUkT1+2opKRTOf7754ptjvJq31jQJgeY2gKGtp1

jPXZiu9Pp3QQ5cRKIWIIdOFvcrVtIZ/P3OYhT0p4Z+L13fScUbr/kxI6KcZmY/1D

Szqzyr8SW7zRz1ypGffc

=UPkJ

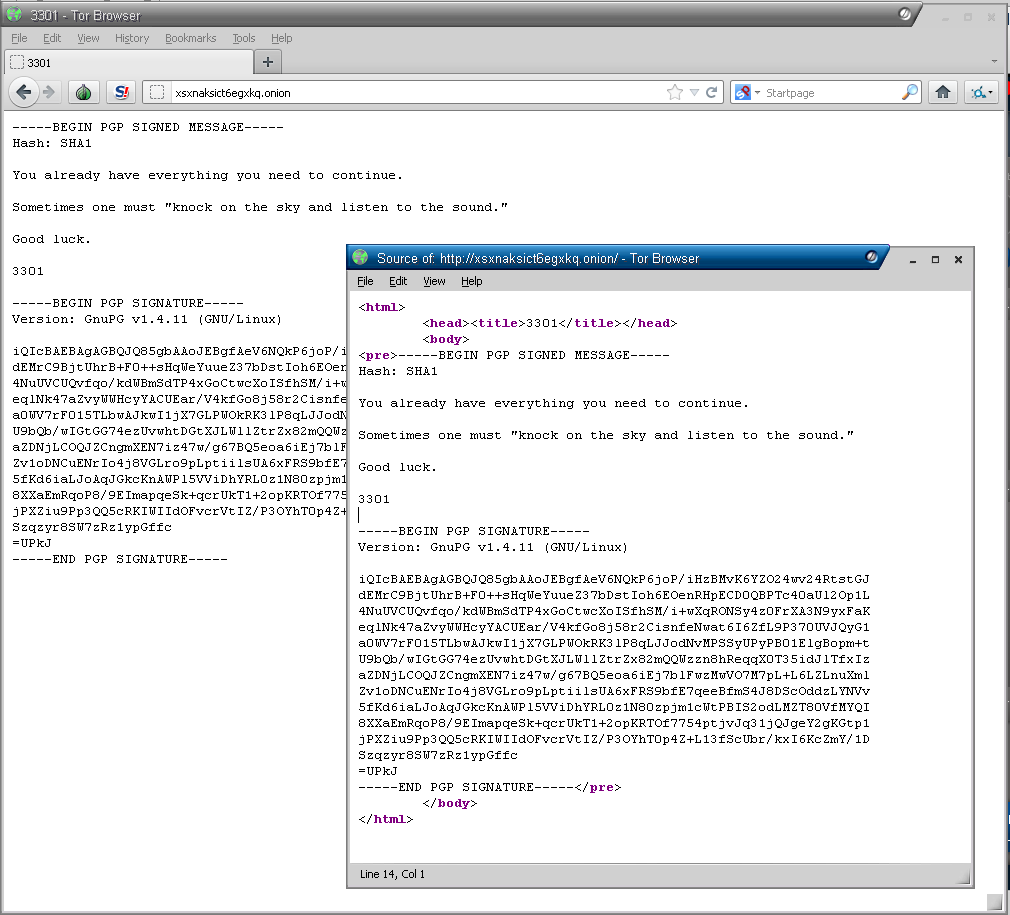
-----END PGP SIGNATURE-----

</body>

</html>

<http://prntscr.com/p4iat> TOR Page

[http://prntscr.com/p4dz2 PGP onion2](http://prntscr.com/p4dz2 PGP%20onion2).2



## TOR 2 PAGE IS BACK UP

As of 1/11 2013, the Tor 2 page, found on <http://xsxnaksict6egxkq.onion/>, is back up. The onion link, hereafter refered to as 'the tor page', had previously featured following piece of source code:

<html>

<head><title>3301</title></head>

<body>

Patience is a virtue.

</body>

</html>

This had changed when the site reopened at approximatly 2:00 AM (GMT +1), and is still (5:14 PM, GMT +1) showing the following:

<html>

<head><title>3301</title></head>

<body>

Welcome back.

</body>

</html>

In short, the text has been changed into 'Welcome back', while the header remains the same. The hidden hint in the source code has been removed, and not replaced by a new one.

Selfdoxing issue (you get this error by telnetting to torrent dress any command: <http://www.anonpaste.me/anonpaste2/index.php?a2b4b6baeb86cc29#cSKB60duEiVV/ZkM0WgfLT7IN9VDBbf0oDn1+igKP4o=>

## Speculations regarding the re-opening of the site.

The fact that the site was closed on the 7th of january 2013 and reopened the 11th of januray has resulted in speculations towards the importance of prime numbers; more specifically, the dates suggest that the site only is up on prime dates.

*•* As a matter of fact, the site did not 're-open'; the new site is hosted on another server with another apache version, and this suggests that it is infact not the same site.

*•* A lot of stuff has been tried to access more information related to the reopened site, and here's a list that includes some of the experiments:

- All ports were scanned 1-65535

- Port knocking is currently being tried (5:25 PM, GMT +1)

## TOR 2 PAGE IS DOWN

I have no idea when that happened or what triggered it.

Note that first tor page also chenged shortly after we discovered it.

There is a theory that the onion2 page leaked its linode hostname via an Apache error page. Shortly afterwards the server became unavailable on port 81 (original clearnet port), and then completely went down on all ports.

It was decided by a handful to call Linode and find out whether the server has been terminated or is just shut down. Absence\_ on IRC was kind enough to make the call through which it was deduced that the server was still active (an active profile existed for the IP).

Also a scan of ports 80 and 81 in the linode subnet was performed by Tech1. It is believed that both onion1 and onion2 are hosted on linode and may have been registered together, thus a high probability of sharing a subnet. At the time of writing only xx.xx.xx.110 had port 81 open, a full portscan is in progress (6379, 12003, 80, 22 for now). This IP is probably unrelated and irrelevant to the quest. Port 6376 had Redis running, fully functional and unauthenticated with a bunch of clients connected, had ad related settings/logs on it. Discontinuing persuit.

**Aprox. time when tor 2 was taken down**

|  |  |
| --- | --- |
| [2013-01-07 18:52:10] <Ymgve> did they just kill it  [2013-01-07 18:52:19] <lull> is it down?  GMT |  |
| **Leaked adress of TOR 2**  $ nc -x localhost:9050 xsxnaksict6egxkq.onion 80  abc  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  <html><head>  <title>501 Method Not Implemented</title>  </head><body>  Method Not Implemented  abc to /index.html not supported.  <address>Apache/2.2.22 (Ubuntu) Server at li528-4.members.linode.com Port 81</address> </body></html> |  |  |
| <http://pastebin.com/n7xtuNqh> <http://pastebin.com/nB98cRuT> |  |  |

|  |  |  |
| --- | --- | --- |
| **Whois and other Links** |  |  |

<http://li528-4.members.linode.com:81/>  
<http://www.netip.de/dns?domain=li528-4.members.linode.com>  
<http://ip-lookup.net/index.php?ip=106.186.17.4>  
<http://sebsauvage.net/paste/?f3711ebf6e2dc1c6#M1GlAKqRsjv3/Rj8IO+ET1d0KhMPlit8yHrMVdo3BxU=>  
<http://cnet.robtex.com/106.186.17.html>  
<http://webcache.googleusercontent.com/search?q=cache:KEMFPtY38R8J:torstatus.info/router_detail.php%3FFP%3D4ac4f47e829ebba21da77ff221bc4f72573632db+li528-4.members.linode.com&cd=6&hl=en&ct=clnk&client=browser-ubuntu>  
<http://106.186.17.4:81/>

odd that port 80 is closed