**LOGS ABOUT HOW WE FOUND LINODE SERVER OF ONION 3**

**HERE IS SOME MAGIC HAW THAT WAS DONE**

!!DO NOT DELETE ANY LOGS UNTIL WE HAVE EASY STEP BY STEP EXPLANATION HOW THIS WAS FOUND AND DONE, AND I MEAN AS EASY THAT JOURNALISTS CAN UNDERSTAND AND REPRODUCE IT !!!

DUMP MORE RELEVANT LOGS EXCERPTS OR EVEN TRY TO WRITTE SHORT ABSTRACT OF THIS

BUT DONT DELETE THEM PLS, IF NOT FOR PRIVACY REASONS!!!

<absence\_> Lurker69, last year it was found on a 404. This year it was found on /server-status

[05:40] <Lurker69> how was linode server found?  
[05:40] <L0j1k> onion/server-status  
[05:41] <L0j1k> which is a server status page in apache, found by taiiwo's dirbuster

(Editor's note: It was actually found via Taiiwo's nessus scan)

[05:41] <Lurker69> last year it was in 404  message right?  
[05:42] <L0j1k> yes i think so

<http://82.9.41.159/html/user/>  Some page taiiwoo made, i have no idea what it should do

[04:08] <Surtri> :)  
[04:08] <Lurker69> [04:06] <cracker42jack> There's also an IP there that goes back to a site run by Lurker69 and Taiiwo -- wonder who those guys are....  
[04:08] <Lurker69> [04:06] <Taiiwo> lel  
[04:08] <Lurker69> [04:06] <Taiiwo> That's my boic server  
[04:08] <Lurker69> [04:06] <marcusw> lolololol  
[04:08] <Lurker69> [04:06] <Taiiwo> boinc  
[04:08] <Lurker69> Taiiwo: WAT???

Taiiwo put my name on page, but it has nothing to do with me :-)   Lurker69

[03:24] <Lurker69> also what is with .js comment someone deleted???  
[03:24] <Lurker69> <http://pastebin.com/GvjeKkxP>  
[03:24] <Lurker69> <http://pastebin.com/GvjeKkxP>  
[03:24] <Lurker69> <http://pastebin.com/GvjeKkxP>

[05:40] <Lurker69> how was linode server found?  
[05:40] <L0j1k> onion/server-status  
[05:41] <L0j1k> which is a server status page in apache, found by taiiwo's dirbuster

(Editor's note: It was actually found via Taiiwo's nessus scan)

[05:41] <Lurker69> last year it was in 404  message right?  
[05:42] <L0j1k> yes i think so

[04:00] <Lurker69> can someone fills me in on that linode server and all that IP logs  
[04:00] <Lurker69> [03:50] <Lurker69> !CAN YOU PLESE SHOOT ME ALL IMPORTANT POSTS YOU SEE IN THIS PM?  
[04:00] <Lurker69> [03:50] <Lurker69> LINODE and how to get to that linode thing and that  
[04:00] <Lurker69> [03:50] <Lurker69> for wiki  
[04:00] <Lurker69> [03:50] <Lurker69> i cant follow chat at all since wiki is clusterfuck  
[04:00] <Lurker69> [03:51] <L0j1k> with the li676-224.members.linode.com  
[04:00] <Lurker69> [03:51] <L0j1k> taiiwo found onion3.onion/server-status  
[04:00] <Lurker69> [03:51] <L0j1k> are actually logging external NONTOR connections  
[04:00] <Lurker69> [03:51] <L0j1k> so it's verified  
[04:00] <Lurker69> [03:51] <L0j1k> i verified my own IP on that server-status, so the current onion3.onion machine is actually li676-224.members.linode.com  
[04:00] <Lurker69> [03:52] <Lurker69> how was linode found  
[04:00] <Lurker69> [03:52] <L0j1k> i linked the server-status on onion3 with the fact that it's logging connections to it's own hostname, which is the linode address  
[04:00] <Lurker69> [03:52] <L0j1k> port 80 is open on that linode (li676-224.members.linode.com)  
[04:00] <Lurker69> [03:52] <Lurker69> i dont understand, but i will just post this log in wiki ok?  
[04:01] <absence\_> lawl  
[04:01] <absence\_> <http://pastebin.com/je6Yudvh>  
[04:02] <Lurker69> absence\_: what is this?  
[04:02] <absence\_> onion3.onion/server-status  
[04:04] <Lurker69> how was it found  
[04:05] <absence\_> ur text.  
[04:05] <Lurker69> is that this IP logging fro m linode ppl are talking about?  
[04:05] <absence\_> <L0j1k> taiiwo found onion3.onion/server-status  
[04:05] <absence\_> idk  
[04:06] <Lurker69> i will just dump my logs in wiki  
[04:06] <absence\_> Total accesses: 548166 - Total Traffic: 6.5 GB  
[04:06] <Lurker69> i lost half of my edits

[04:06] <Lurker69> since i have too many editing tabs open, causing colisions with myself

**MORE LOGS**

**MORE:**

[05:17] <Lurker69> who found it and how?  
[05:17] <Lurker69> is that standard path on apache server?  
[05:18] <L0j1k> i found it, that's how  
[05:18] <L0j1k> taiiwo found the server-status/ with dirbuster

(Editor's note: It was actually found via Taiiwo's nessus scan)

<L0j1k> i noticed it on one of the server-status/ pages  
<L0j1k> i scanned linode before and verified and then announced it to be sure  
[05:19] <Lurker69> can you post me linode server http heder or where linode add leaked  
[05:19] <L0j1k> the linode IP points directly to the same exact machine serving content over tor hidden service  
[05:19] <L0j1k> just a sec, yes  
[05:19] <L0j1k> i noticed it on one of the server-status/ pages  
[05:19] <L0j1k> taiiwo got it through dirbuster and i explored the data

(Editor's note: It was actually found via Taiiwo's nessus scan)

[05:19] <L0j1k> found linode  
[05:19] <L0j1k> and then verified they were same  
[05:19] <L0j1k> lemme get you header  
[05:20] <L0j1k> l0j1k@zeitgeist ~ $ telnet li676-224.members.linode.com 80  
[05:20] <L0j1k> Trying 106.186.123.224...  
[05:20] <L0j1k> Connected to li676-224.members.linode.com.  
[05:20] <L0j1k> Escape character is '^]'.  
[05:20] <L0j1k> GET /lol.taiiwo.is.faget HTTP/1.0  
[05:20] <L0j1k> HTTP/1.1 404 Not Found  
[05:20] <L0j1k> Date: Thu, 09 Jan 2014 03:06:11 GMT  
[05:20] <L0j1k> Server: Apache  
[05:20] <L0j1k> Vary: Accept-Encoding  
[05:20] <L0j1k> Content-Length: 295  
[05:20] <L0j1k> Connection: close  
[05:20] <L0j1k> Content-Type: text/html; charset=iso-8859-1  
[05:20] <L0j1k> <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
[05:20] <L0j1k> <html><head>  
[05:20] <L0j1k> <HTML TAG: title>404 Not Found<HTML TAG: /title>  
[05:20] <L0j1k> </head><body>  
[05:20] <L0j1k><HTML TAG:h1>Not Found<HTML TAG:/h1>  
[05:20] <L0j1k><HTML TAGp>The requested URL /lol.taiiwo.is.faget was not found on this server.<HTML TAG/p>  
[05:20] <L0j1k><HTML TAG:hr />  
[05:20] <L0j1k> <address>Apache Server at li676-224.members.linode.com Port 80</address>  
[05:20] <L0j1k> </body></html>  
[05:21] <L0j1k> Connection closed by foreign host.  
[05:21] <L0j1k> that's a lot, sorry, but it's a complete HTTP conversation

[05:13] <crashdemons> no, it has nothing to do with a whitelist  
[05:14] <crashdemons> it just implements DOM element stack  
[05:15] <crashdemons> also, linode is not the onion  
[05:15] <crashdemons> it's proxying the onion  
[05:15] <crashdemons> lag and it's server handles things differently, different kernel version, different response to server-specific URLs  
[05:15] <crashdemons> other responses are forwarded

**MORE 5:00 GMT onion changed**

[05:58] <NiceLurk> <Mothwing> 87de5b7fa26ab85d  
[05:58] <NiceLurk> whats with that string ppl aer posting around?  
[05:58] <soulseekah> NiceLurk: from the onion  
[05:58] <soulseekah> it's back up  
[05:58] <Tech1> from the new onion lruk  
[05:58] <NiceLurk> ah  
[05:58] <L0j1k> dunno if this means anything at all, but in the server-status/ page, "Server Built: Jul 12 2013 13:37:15"  
[05:59] <absence\_> no that could be linode  
[05:59] <NiceLurk> so tere are niews not yet in wiki  
[05:59] <Tech1> when they updated the apache config and rebuilt apache is my guess  
[05:59] <absence\_> Total accesses: 930965 - Total Traffic: 6.6 GB  
[05:59] <soulseekah> NiceLurk: not entirely sure, I think all is intact  
[05:59] <L0j1k> they can put anything in the output they want, so i was interested in the numbers themselves  
[05:59] <soulseekah> absence\_: wow  
[05:59] <absence\_> the total accesses was before at 50000