2021-03-13 UH hacked

(All times listed by me are CT. Wordpress screenshot times show a +6 hour time difference.)

03/12/21 Deleted Raul’s domains that were parked on Whitney’s hosting plan.

03/12/21

https://twitter.com/hijodelcuervo/status/1370464551171411969?s=20

03/12/21

https://twitter.com/_whitneywebb/status/1370489861854085123?s=20

This was the first time Whitney publicly said she was leaving Chile.
The Support Us page was live on the website when she posted this. It was a page letting people know the preliminary details about the membership plan that would be launching through the website.

03/13/21 6:20am
*netlify.com*

Issued by: DigiCert SHA2 Secure Server CA
Expires: Tuesday, August 3, 2021 at 7:00:00 AM Central Daylight Time

⚠️ “*netlify.com” certificate name does not match input

**Trust**

When using this certificate: Use System Defaults

<table>
<thead>
<tr>
<th>Secure Sockets Layer (SSL)</th>
<th>no value specified</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.509 Basic Policy</td>
<td>no value specified</td>
</tr>
</tbody>
</table>

**Details**

<table>
<thead>
<tr>
<th>Subject Name</th>
<th>Common Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country or Region</td>
<td>US</td>
</tr>
<tr>
<td>State/Province</td>
<td>ca</td>
</tr>
<tr>
<td>Locality</td>
<td>San Francisco</td>
</tr>
<tr>
<td>Organization</td>
<td>Netlify, Inc</td>
</tr>
<tr>
<td>Common Name</td>
<td>*netlify.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issuer Name</th>
<th>Common Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country or Region</td>
<td>US</td>
</tr>
<tr>
<td>Organization</td>
<td>DigiCert Inc</td>
</tr>
<tr>
<td>Common Name</td>
<td>DigiCert SHA2 Secure Server CA</td>
</tr>
</tbody>
</table>

OK
6:45am Admin is locked out of hostinger-password changed

Website back up by 8am with help from Hostinger

03/13/21 https://twitter.com/hijodelcuervo/status/1370790743015587845?s=20
Is he chatting with customer service about his websites? No real evidence here, but the tweet is interesting.

**Event viewer logs**

03/12/21 7:11pm
Failed login attempt from Whitney Webb Subscriber account
2a00:1370:8113:c46:6df7:e336:555d:f67
Who is the Whitney Webb Subscriber? When you click on it, it takes you to this admin account

When you click into this admin account, these are the details.
Raul has whitney@unlimitedhangout.com listed as his email address

**3/14/21**

11:40pm (saw the notification on 3/15)
Someone tried to reset Star’s Instagram password
**3/15/21**

2:48am

Another failed Whitney Webb admin login attempt location Russia
Star reset password on the admin Whitney Webb account

Admin installed Wordfence. Immediately after installing, received this notification. This was the first one after installing Wordfence. When a user tries to login, they get an alert that they were blocked by Wordfence.

10:18am Mexico City login attempt
10:22am
Another failed attempt immediately after with login through “admin” this time from Colorado Springs. The location and IP address can easily be spoofed with a VPN.

If it was Raul who hacked the site, he would not have expected the Wordfence alert with the 10:18am login attempt. This could be an attempt to cover tracks.

Another reason I think it is possible this second recorded event is the first person trying to cover their tracks is the timing. It was done 4 minutes after the Mexico City login attempt. There were four more attempts throughout the day. The timing is key.
There were subsequent attempts to log in throughout the day from the following locations and times.

11:48am India username unlimitedhangout
This email was sent from your website "unlimitedhangout.com" by the Wordfence plugin at Monday 15th of March 2021 at 04:43:33 PM
The Wordfence administrative URL for this site is: https://unlimitedhangout.com/wp-admin/admin.php?page=Wordfence
A user with IP addr 2500:484:2977:6a00:28c4:76c5:92ca:4522 has been locked out from signing in or using the password recovery form for the following reason: Exceeded the maximum number of login failures which is: 20. The last username they tried to sign in with was: 'unlimitedhangout'.
The duration of the lockout is 4 hours.
User IP: 2500:484:2977:6a00:28c4:76c5:92ca:4522
User hostname: 2500:484:2977:6a00:28c4:76c5:92ca:4522
User location: Bogotá, Colombia

...To change your alert options for Wordfence, visit:
To see current Wordfence alerts, visit:

No longer an administrator for this site? Click here to stop receiving security alerts: https://unlimitedhangout.com/?waf=removeAlertEmail&amp;waf=removeAlertEmail

2:36pm Israel username unlimitedhangout

This email was sent from your website "unlimitedhangout.com" by the Wordfence plugin at Monday 15th of March 2021 at 07:36:27 PM

The Wordfence administrative URL for this site is: https://unlimitedhangout.com/wp-admin/admin.php?page=Wordfence

A user with IP addr 2406:5550:0:6520:0:1812:1:12345 has been locked out from signing in or using the password recovery form for the following reason: Exceeded the maximum number of login failures which is: 20. The last username they tried to sign in with was: 'unlimitedhangout'.

The duration of the lockout is 4 hours.

User IP: 2406:5550:0:6520:0:1812:1:12345
User location: Tel Aviv, Israel

To change your alert options for Wordfence, visit:

To see current Wordfence alerts, visit:

3:54pm San Diego unlimitedhangout

This email was sent from your website "unlimitedhangout.com" by the Wordfence plugin at Monday 15th of March 2021 at 08:54:42 PM

The Wordfence administrative URL for this site is: https://unlimitedhangout.com/wp-admin/admin.php?page=Wordfence

A user with IP addr 2600:1702:850:2fe0:84e0:cc4:b301:7ad9 has been locked out from signing in or using the password recovery form for the following reason: Exceeded the maximum number of login failures which is: 20. The last username they tried to sign in with was: 'unlimitedhangout'.

The duration of the lockout is 4 hours.

User IP: 2600:1702:850:2fe0:84e0:cc4:b301:7ad9
User hostname: 2600:1702:850:2fe0:84e0:cc4:b301:7ad9
User location: San Diego, California, United States

To change your alert options for Wordfence, visit:

To see current Wordfence alerts, visit:

No longer an administrator for this site? Click here to stop receiving security alerts: https://unlimitedhangout.com/?waf=removeAlert&email=Kw+sbrwv+JhbGo+C9JUz1NilslnR6cCfUpyxVCjR+ewJlwWp6bC6RmlJuZm9AdW6eawW1pG4VkaGFuZ291dC5b20LJCfZlxhrioxJNE2NDQ2NDgyYQ_PyryFyype+kinvNdsHyW59JmYQoQ6MNMLUc9MwChYPY