

Forum:[Hack Forums](#)

Thread: [Account Security Notification](#)

Omniscient - May 3, 2016, 1:33 pm

I can't say when or how but apparently somewhere at some point we had a compromise of account security. It has to be based on my findings today.

While conducting my normal day of checking for stolen accounts I came across a dozen or so Ub3r accounts stolen in the last few days. Upon further inspection and looking for more accounts stolen or sold related to these accounts I found something rather alarming. In my logs I found that nearly 40 accounts had attempts to login and it became obvious these were not sold accounts. Indeed these appear stolen. I conclude that because out of the 40 accounts only the ones without 2FA were actually logged into and stolen. And more than a few members of these stolen accounts closed have contacting me to claim they were not sold and their computers are not infected.

That leads me to believe this person has the password of the account. They can only get that either by the member using the same password on another site, being infected by a RAT/keylogger, or if their hashed password was cracked from a dump. So it's rather alarming to find this out.

I have to conclude this was on our old hardware or some fluke compromise at some point when I was working on something. Could even have been MyBB vulnerability which is likely now patched. If there was some way for the person to still have DB access I would assume they'd alter the member login or other site details and have their way. Even do a complete dump (I have measures in place to make that very very difficult) which does not appear to have happened. They'd also disable 2FA if they had SQL access and steal any account they wished.

All accounts compromised are older than 1 year ago. Which might be when the compromise occurred, maybe.

I am going to add a plugin which will now require 2FA to post in the Marketplace or to send a PM if you have an upgraded account with 2FA/Gauth access. I have also altered the setting for the minimum character length of a password from 10 to 12 characters. In the future that should slow down any decrypting of hashed passwords in case of a dump.

If there is a silver lining in this it's that we now know that 2FA works to secure accounts.

I have contacted all the accounts compromised with 2FA enable and still open instructing them to immediately change their passwords and leave 2FA enabled.

Still, questions remain. When did it happen? How did it happen? Are we still insecure? And unfortunately at the time of this writing I can't say. I am still investigating this and messages have been sent to the members involved. With their help I should be able to get some answers to the previous questions.

I will need all members to change their passwords immediately and enable 2FA if you have an account with access.

Oh....btw some good news also...HF database does not store any private order data like name, address, or phone. We only have the most basic info which is IPs and emails.

It's very important for all members to check Trust Scan before making any deals. The information provided on the page is plenty and should be enough to give you an indication of how secure the account has been and if it has behavior that would deem them a high risk.

An email is being sent to all Ub3r instructing them to create a new password and to enable Gauth/2FA.

This will give everyone something to talk about at the very least.

Thehackerguy1 - May 3, 2016, 1:37 pm

Well, this is scary. I will change my password right now. I hope to god that nothing goes wrong ?

Rikk?a - May 3, 2016, 1:37 pm

Changing my password right now, thanks for informing us.

chase. - May 3, 2016, 1:38 pm

Thank you for this Omni will change password ASAP

Omniscient - May 3, 2016, 1:38 pm

It's very important everyone enables 2FA.

?Kill? - May 3, 2016, 1:39 pm

(May 3, 2016 01:38 PM)Omniscient Wrote: [\[CITE\]](#) It's very important everyone enables 2FA.

I honestly enabled it as soon as I got l33t because I didn't want anything happening to my account, I don't know why some people don't have it enabled.

Bluffer - May 3, 2016, 1:39 pm

I will change my password right now and honestly I've been thinking about using something like last pass which should make things even more secure and I might do just that.

glitchgxd - May 3, 2016, 1:39 pm

I definitely thought it was gonna be a phishing attempt first when I saw the email and thought "really? they think that'll work?".

But looks like it's legit. I heard were able to trust the pink name guys.

Trust - May 3, 2016, 1:39 pm

This is why I verify my gauth every day.

Ooze - May 3, 2016, 1:39 pm

Does the DB save old info like past emails and passwords?

It must save past IP's or the trustscan wouldn't work correct?

Mint - May 3, 2016, 1:40 pm

Thank you for bringing this to my attention.

Ooze - May 3, 2016, 1:40 pm

(May 3, 2016 01:39 PM)?rust Wrote: [\[CITE\]](#) This is why I verify my gauth every day.

Wait how do you verify it?

?Kill? - May 3, 2016, 1:41 pm

(May 3, 2016 01:39 PM)?rust Wrote: [\[CITE\]](#) This is why I verify my gauth every day.

How do you verify it?

Regulus - May 3, 2016, 1:41 pm

Holy shit this is some scary stuff.

I haven't got a Email yet so I guess nothing has happened to my account.

I'll change the password though to be on the safe side. If my account got hacked just like that, randomly I don't know what I would do to be honest.

Thanks a lot for this Omni!

bank\$ - May 3, 2016, 1:41 pm

(May 3, 2016 01:38 PM)Omniscient Wrote: [\[CITE\]](#) It's very important everyone enables 2FA. So I have to buy l33t in order to use the marketplace and stuff?

Bluffer - May 3, 2016, 1:42 pm

(May 3, 2016 01:40 PM)The JOker Wrote: [\[CITE\]](#) Wait how do you verify it?

You just go [here](#) and put in the code!

I don't think you are the only one who hasn't even heard about being able to verify your gauth but it's a great step to keep your account secure.

I personally verify mine at least once a week.

Trust - May 3, 2016, 1:42 pm

(May 3, 2016 01:40 PM)The JOker Wrote: [\[CITE\]](#) Wait how do you verify it?

You can validate your gauth code here: <https://hackforums.net/gauth.php>

Rubentastic - May 3, 2016, 1:43 pm

Damn I thought the mail was fake at first. I'm sure I never got infected and use an unique pass for HF so how could they get it then? Must be from a cracked hash from db..

chase. - May 3, 2016, 1:43 pm

my new pass is sp00ki complex

Ooze - May 3, 2016, 1:43 pm

(May 3, 2016 01:41 PM)luckytakashi Wrote: [\[CITE\]](#) So I have to buy l33t in order to use the marketplace and stuff?

Hmm I guess so, you couldn't even PM the owner to get a deal.

I mean it protects people but also will get a lot more people upgrading

bank\$ - May 3, 2016, 1:44 pm

(May 3, 2016 01:43 PM)The JOker Wrote: [\[CITE\]](#) Hmm I guess so, you couldn't even PM the owner to get a deal.

I mean it protects people but also will get a lot more people upgrading

Gauth to PM?

ez money

Stashyy - May 3, 2016, 1:44 pm

I have 2FA, but I have to change my PW?

It's one of those u know random generated hf ones.

If so I'll do it now. ;)

Ooze - May 3, 2016, 1:45 pm

I changed my PW like 2 days ago, so I think I should be good. But I can always change it again if its

required

Roytoy - May 3, 2016, 1:46 pm

Just changed my password. Hope this doesn't get bigger than it is.

Tutelary - May 3, 2016, 1:48 pm

I have changed my password and am glad 2FA was enabled to prevent trusted Ub3rs from getting hacked.

SixInchesDeep - May 3, 2016, 1:48 pm

Rip stolen accs I enabled 2fa right when I upgraded

Omniscient - May 3, 2016, 1:49 pm

(May 3, 2016 01:40 PM)Panik Wrote: [\[CITE\]](#) Didn't you close Tokyo when he tried to tell you about this db compromise?

I've known about it for a year.

I get told every few weeks that there is a dump and the site is compromised. Been that way for nine years. I can only take it seriously if I'm shown actual evidence that indeed we're compromised. But I often do security checks to make sure things are as they should.

I don't freak out about being compromised either. I just fix it. I know for a fact it's going to happen probably every 2-3 year. Just a matter of how much work it requires for me to secure it again.

What I question now is....are we secured since we moved to the new hardware and have a completely different setup?

?Kill? - May 3, 2016, 1:49 pm

On my trustscan it hasn't said I changed my pass yet is that normal or does it take a bit to go in to the db?

Random - May 3, 2016, 1:49 pm

Just changed my password.

Thanks for the update, Omni.

I'm not a Robot - May 3, 2016, 1:50 pm

Thanks for letting us know Omni,
Going to change my PW now

minimalist - May 3, 2016, 1:51 pm

Thanks for making this announcement, I'll get to changing my things right away.

Support™ - May 3, 2016, 1:52 pm

Made my new password 30+ character long. Crack that motherfuckers!

Rikk?a - May 3, 2016, 1:52 pm

(May 3, 2016 01:49 PM)Omniscient Wrote: [\[CITE\]](#) What I question now is....are we secured since we moved to the new hardware and have a completely different setup?

I really hope we will be.

A NEW ERA... - May 3, 2016, 1:53 pm

Was this from the Micasa incident? Heard about it on another thread, his community alert.

Trust - May 3, 2016, 1:53 pm

Now getting a bunch of errors.

Quote:Parse error: syntax error, unexpected end of file in
/home/hfaccount/domains/hackforums.net/public_html/inc/plugins/loginattempts.php on line 212
Quote:[403 Forbidden Error] - Access Denied

FiftyTwo - May 3, 2016, 1:53 pm

Damn, thank you very much for informing us Omni.

Kinda scary to think that somebody might have access to our accounts sooner or later.

I'll also be keeping an eye on the IP's that login to my account and I'll report anything suspicious immediately.

Best of luck on figuring more out regarding this situation.

Rubentastic - May 3, 2016, 1:53 pm

@Omni, a friend of mine Koolhunk got closed today. Was this also because of possible compromision?

Cryptic™ - May 3, 2016, 1:53 pm

(May 3, 2016 01:53 PM)?rust Wrote: [\[CITE\]](#) Now getting a bunch of errors.

Omni was probably making changes to the file.

FiftyTwo - May 3, 2016, 1:56 pm

Whoa, whoa, whoa.

I just did a trust scan on my account:

"Matching region of registration and latest IP: No"

I haven't travelled out of this region at all since last year.

?Kill? - May 3, 2016, 1:57 pm

(May 3, 2016 01:56 PM)52?? Wrote: [\[CITE\]](#) Whoa, whoa, whoa.

I just did a trust scan on my account:

"Matching region of registration and latest IP: No"

I haven't travelled out of this region at all since last year.

<https://hackforums.net/usercp.php>

check ur latest ips

Omniscient - May 3, 2016, 1:58 pm

Quote:On my trustscan it hasn't said I changed my pass yet is that normal or does it take a bit to go in to the db?

We log the PW email resets. I don't yet, but soon will, log all PW changes. I will add that to TS when I do.

Quote:Now getting a bunch of errors.

Was making an adjustment. Should be fine now.

Quote:@Omni, a friend of mine Koolhunk got closed today. Was this also because of possible compromision?

Yes, and since I now know these accounts were compromised and not stolen I will work to help recover them. I have logs and a list of the effected accounts.

FiftyTwo - May 3, 2016, 1:58 pm

(May 3, 2016 01:57 PM)v7KillStreaker Wrote: [\[CITE\]](#) <https://hackforums.net/usercp.php>

check ur latest ips

That's what's confusing - I already checked it but there's no different IP's to mine.

Rubentastic - May 3, 2016, 2:00 pm

(May 3, 2016 01:58 PM)Omniscient Wrote: [\[CITE\]](#) We log the PW email resets. I don't yet, but soon will, log all PW changes. I will add that to TS when I do.

Was making an adjustment. Should be fine now.

Yes, and since I now know these accounts were compromised and not stolen I will work to help recover them. I have logs and a list of the effected accounts.

Awesome, just changed my pass. Thanks for notifying and prompt replies.

Chocky - May 3, 2016, 2:01 pm

Just received the email of this. Thanks for the heads up. Will be sure to change my password shortly.

Cryptic™ - May 3, 2016, 2:03 pm

My friend was closed a few days ago for "stolen" account even though he never sold his account and was surprised when it happened.

Gonna send him a text to use the contact form. Hopefully he can get it back.

His profile link <https://hackforums.net/member.php?action=profile&uid=1858235>

Quad - May 3, 2016, 2:05 pm

(May 3, 2016 01:38 PM)Omniscient Wrote: [\[CITE\]](#) It's very important everyone enables 2FA. I already have 2FA enabled. Should I disable and reenable it to get a new secret?

Rikk?a - May 3, 2016, 2:05 pm

(May 3, 2016 02:05 PM)Quad Wrote: [\[CITE\]](#) I already have 2FA enabled. Should I disable and reenable it to get a new secret?

That's what I'm wondering are the secrets saved on the DB?

SawCyanic - May 3, 2016, 2:06 pm

I got the mass e-mail you sent out 4 times but, thanks for letting us know about it.

Regulus - May 3, 2016, 2:11 pm

For some reason I got this:

Number of Unique Country Logins (last 30 days): 1

Although I haven't been outside Sweden anytime, I'm not even logging into HF anywhere except from home.

Could I get this if I've used like a VPN or something and accidentally been trying to access HF?

—

But overall I should be good:

1. Gauth / 2FA Validation - Done
2. Changed Email - Check (For even further safety reasons)

3. Changed Password - Check

EthanX - May 3, 2016, 2:11 pm

(May 3, 2016 02:06 PM)Republique Wrote: [\[CITE\]](#) I got the mass e-mail you sent out 4 times but, thanks for letting us know about it.

Was that only for people effected? I never got that.

SawCyanic - May 3, 2016, 2:11 pm

(May 3, 2016 02:11 PM)EthanX Wrote: [\[CITE\]](#) Was that only for people effected? I never got that. It says in the OP it was sent to all Ub3r members. Check your spam maybe?

EthanX - May 3, 2016, 2:12 pm

(May 3, 2016 02:11 PM)Republique Wrote: [\[CITE\]](#) It says in the OP it was sent to all Ub3r members. Check your spam maybe?

Nope. Checked my email in usercp, It's correct but I only get private message emails. Have not got the emails omni sent out.

Regulus - May 3, 2016, 2:13 pm

(May 3, 2016 02:11 PM)Republique Wrote: [\[CITE\]](#) It says in the OP it was sent to all Ub3r members. Check your spam maybe?

For some reason I didn't get that Email, hmm.

Chaos Theory - May 3, 2016, 2:13 pm

I would be surprised if there was a security compromise on your end.. Guess time will tell.

EthanX - May 3, 2016, 2:13 pm

(May 3, 2016 02:13 PM)Regulus Wrote: [\[CITE\]](#) For some reason I didn't get that Email, hmm. Good to hear that I am not alone.

J?son - May 3, 2016, 2:14 pm

I haven't got the email yet either.

Kinda scared of enabling 2fa and not being able to login, then losing all the rep I earned.

I'll changed my password to a 60 char hash.

Juicy - May 3, 2016, 2:14 pm

Good news is I don't ever remember my own password, so how could a hacker?

I have it written down somewhere im sure

Omniscient - May 3, 2016, 2:16 pm

Quote:I already have 2FA enabled. Should I disable and reenable it to get a new secret?

If you have 2FA enabled you should be fine. Which brings up another good point. If indeed we still had a leak they'd be able to disable Gauth or steal the secret key. I'm going to make an assumption (gulp) that we're currently secure. No current accounts from the past year were compromised yet and 2FA prevents theft.

If we're lucky then that's true and we just need to enforce 2FA and rotate passwords. We've had to rotate passwords before. Not that big of a deal really. I may need to be more diligent in the next few days to prevent stolen accounts and help with recoveries but that's just part of my day anyways.

Quote:For some reason I got this:

Number of Unique Country Logins (last 30 days): 1

Although I haven't been outside Sweden anytime
Yes, 1 country....Sweden. That's how it should be.

Also for the emails they do not send all at once. I have them to send them in a steady stream. So far 35% have gone out. Just be patient. Once all the Ub3r emails are sent I will be sending to the l33t members. I'll likely not bother with 3P1C since almost all 3P1C are Ub3r or L33t.

Rikk?a - May 3, 2016, 2:16 pm

(May 3, 2016 02:13 PM)Chaos Theory Wrote: [\[CITE\]](#) I would be surprised if there was a security compromise on your end.. Guess time will tell.

Doubt Omniscient would of been compromised if the DB leak were to happen because of the fact he has 2FA Enabled.

Unless someone manage to get his Secret key.

EthanX - May 3, 2016, 2:17 pm

(May 3, 2016 02:14 PM)N??b Wrote: [\[CITE\]](#) I haven't got the email yet either.

Kinda scared of enabling 2fa and not being able to login, then losing all the rep I earned.

I'll changed my password to a 60 char hash.

There is NO reason you won't be able to enable Gauth. USE AUTHY!

If you do not have a phone, use <https://www.authy.com/app/desktop/>.

(May 3, 2016 02:16 PM)Rikk????????????????a Wrote: [\[CITE\]](#) Doubt Omniscient would of been compromised if the DB leak were to happen because of the fact he has 2FA Enabled.

Unless someone manage to get his Secret key.

Haha, I don't think that's what he means. He means there was probably a compromise on Omni's forum.

Regulus - May 3, 2016, 2:19 pm

(May 3, 2016 02:16 PM)Omniscient Wrote: [\[CITE\]](#) Yes, 1 country....Sweden. That's how it should be.

Also for the emails they do not send all at once. I have them to send them in a steady stream. So far 35% have gone out. Just be patient. Once all the Ub3r emails are sent I will be sending to the l33t members. I'll likely not bother with 3P1C since almost all 3P1C are Ub3r or L33t.

Okay thanks a lot for letting me know.

I appreciate it a lot!

Changed everything now so I should be fine.

Thanks for the updates Omni, You're the man! ?

EthanX - May 3, 2016, 2:21 pm

Just thought about what if people that use authy are using the same password on authy and hackforums? They sort of deserve what comes, but i'm sure that's been the case for hackers getting past 2fa a few times.

J?son - May 3, 2016, 2:21 pm

(May 3, 2016 02:17 PM)EthanX Wrote: [\[CITE\]](#) There is NO reason you won't be able to enable Gauth. USE AUTHY!

If you do not have a phone, use <https://www.authy.com/app/desktop/>.

I've tried authy and it still asks for a cellphone number.

EthanX - May 3, 2016, 2:22 pm

(May 3, 2016 02:21 PM)N??b Wrote: [\[CITE\]](#) I've tried authy and it still asks for a cellphone number. You could try a google voice number, but i'm not sure how secure that would be and if it would work or not.

Un-Named - May 3, 2016, 2:24 pm

Got the E-Mail and just now reset it again.

I never reset my password after it's been automatically generated & all of my accounts have unique passwords.

Thank you for the email notification.

Ritract - May 3, 2016, 2:24 pm

I'm upgrading soon so I can enable 2FA.

Armada - May 3, 2016, 2:26 pm

So reading OP, is it safe to assume being I got that email my PW needs to be changed and keep 2FA enabled @ all times?

Seaking - May 3, 2016, 2:26 pm

I've always used a random password, but I went ahead and made another and re-verified my auth. Appreciate the email.

-edit- Also reminded me to run a scan through my desktop just to make sure. I probably should of scanned first then changed everything, but I don't have enough time. I'm sure I'm not infected with anything but I'd rather be safe than sorry.

Bluffer - May 3, 2016, 2:27 pm

(May 3, 2016 02:14 PM)N??b Wrote: [\[CITE\]](#) I haven't got the email yet either.

Kinda scared of enabling 2fa and not being able to login, then losing all the rep I earned.

I'll changed my password to a 60 char hash.

Well you could use Authy on your computer which would make it much less likely to have an issue, you can also connect Authy to your phone and once you have it setup it's extremely easy to use and verify your account. Unfortunately for you, with those new restrictions it will really prevent you from using a lot of important areas on HF and you may even have people refuse to deal with you because you don't have 2fa enabled.

mrnapolean1 - May 3, 2016, 2:27 pm

Changed my Password and re-validated my 2FA.

Doctor Blue - May 3, 2016, 2:27 pm

I always admire administrators who are open about breaches. Password changed, thanks for letting us know :)

Also might make sense to ask people to log out after changing the password to kill all other sessions.

EDIT: Just realized that it signs out all sessions except the current one. I guess that makes just as much sense.

J?son - May 3, 2016, 2:30 pm

Guys, I used another app called Authenticator and it was almost too easy.

<https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai>

Rikk?a - May 3, 2016, 2:30 pm

(May 3, 2016 02:27 PM)Doctor Blue Wrote: [\[CITE\]](#) I always admire administrators who are open about breaches. Password changed, thanks for letting us know :)

Also might make sense to ask people to log out after changing the password to kill all other sessions.

I assume he has already done this, lately I've been automatically signed out, I check my IP History everything seems normal.

?Kill? - May 3, 2016, 2:31 pm

(May 3, 2016 02:30 PM)Rikk????????????????a Wrote: [\[CITE\]](#) I assume he has already done this, lately I've been automatically signed out, I check my IP History everything seems normal.

I've been randomly signed out recently also odd

Narrate - May 3, 2016, 2:32 pm

Well that fucking sucks now doesn't it.

netFaux_temp - May 3, 2016, 2:32 pm

I emailed omni 2 days ago and explained the situation. Hopefully he realizes it is me and my account can be reopened.

I've been a member for 6 years and love this site, I would hate for me to be absent from here. Hopefully everything works out for everybody.

Omni is just doing his job and I understand that.

I have about any information he could possibly want that would ensure him it is my account.

Good luck everybody to securing accounts!

deafness - May 3, 2016, 2:34 pm

Updated the account info and enabled authy once again. Better safe than be sorry; thanks for notified us in ahead of time.

Trapology - May 3, 2016, 2:35 pm

(May 3, 2016 02:31 PM)v7KillStreaker Wrote: [\[CITE\]](#) I've been randomly signed out recently also odd Me too, today actually. I have 2FA though.

funtela - May 3, 2016, 2:38 pm

Do we need to re-enable 2fa after we change the password?

Rikk?a - May 3, 2016, 2:40 pm

(May 3, 2016 02:30 PM)Rikk????????????????a Wrote: [\[CITE\]](#) I assume he has already done this, lately I've been automatically signed out, I check my IP History everything seems normal.

(May 3, 2016 02:31 PM)v7KillStreaker Wrote: [\[CITE\]](#) I've been randomly signed out recently also odd

(May 3, 2016 02:35 PM)Vos. Wrote: [\[CITE\]](#) Me too, today actually. I have 2FA though.

So I'm guessing this was normal.

FiftyTwo - May 3, 2016, 2:40 pm

I've updated my password, I enabled 2FA on my email and have added lots of recovery options.

I'd recommend anybody who hasn't already to do the same.

Binary Ghoul - May 3, 2016, 2:46 pm

(May 3, 2016 01:39 PM)Bluffer™ Wrote: [\[CITE\]](#) I will change my password right now and honestly

I've been thinking about using something like last pass which should make things even more secure and I might do just that. Dont use lastpass its basically useless if someone gets access to you computer, instead use keepass

Xerif - May 3, 2016, 2:46 pm

Why do we have to install an app on our phone to enable 2FA? Why can't an SMS just be sent with a code?

Xepher The Cat - May 3, 2016, 2:47 pm

I was about to panic, my account seems alright though. 2FA activated and everything.

Rikk?a - May 3, 2016, 2:47 pm

(May 3, 2016 02:46 PM)Xerif Wrote: [\[CITE\]](#) Why do we have to install an app on our phone to enable 2FA? Why can't an SMS just be sent with a code?

Because that can easily be rerouted.

YayHar - May 3, 2016, 2:47 pm

Enabled 2FA. Making an email dedicated to HF and a unique password.

Thanks for the heads up.

? [\$(1000)\$] ? - May 3, 2016, 2:48 pm

Oh damnnnnn.

Thanks for the heads up brother!

J?son - May 3, 2016, 2:48 pm

(May 3, 2016 02:46 PM)Xerif Wrote: [\[CITE\]](#) Why do we have to install an app on our phone to enable 2FA? Why can't an SMS just be sent with a code?

I didn't have to use phone to enable 2fa. I just installed a fancy chrome app ?

Irish™ - May 3, 2016, 2:48 pm

(May 3, 2016 02:46 PM)Xerif Wrote: [\[CITE\]](#) Why do we have to install an app on our phone to enable 2FA? Why can't an SMS just be sent with a code?

SMS can come with a hefty price tag compared to using an app on your phone.

Rebustly - May 3, 2016, 2:50 pm

Is there any way we can talk, Jesse? It's salty.

I warned you all about this .. hackforums.net/showthread.php?tid=5256139

I just finally want to talk things out with you, Omni - all I ever did was for the good, PM me with a contact method. I just want to talk with you, and hopefully sort things out.

EvanLB7 - May 3, 2016, 2:50 pm

Had 2FA enabled since release, got the email while I was trying to fall asleep for a nap, jumped up and redid 2FA and changed pass lol. Thanks Omni for the announcement.

Queen Cin - May 3, 2016, 2:51 pm

I enabled 2FA a long time ago

Glad I made that decision

Mohatu - May 3, 2016, 2:52 pm

Glad to hear 2FA is becoming more mandatory for use of certain areas of the site.

Grim - May 3, 2016, 2:53 pm

Thanks for the info, for some reason I got like 5 emails about it though might just be how I have notifications set up. Anyhow changing my password now and renewing my 2FA.

reBELLYus - May 3, 2016, 2:57 pm

Thanks for the heads up, per usual. Hopefully you find the source. Good luck.

Zack Fair - May 3, 2016, 2:58 pm

Thank you for the heads up, I think I should get on top of doing 2FA at this point.

JoshAllen - May 3, 2016, 3:01 pm

Changing my password now. Thank you for the heads up.

CyberGuard - May 3, 2016, 3:01 pm

It was probably the 2015 HF DB dump that was abused.

This is a good measurement you took, good job.

Egregious - May 3, 2016, 3:02 pm

Just got the email and changed my password. Thanks for the warning.

7even - May 3, 2016, 3:02 pm

Welp just activated my 2FA. Thanks for this update Omni.

Raymond Reddington - May 3, 2016, 3:02 pm

(May 3, 2016 03:01 PM)CyberGuard Wrote: [\[CITE\]](#) It was probably the 2015 HF DB dump that was abused.

This is a good measurement you took, good job.

Are you saying HF's 2015 DB was dumped?

Zexo - May 3, 2016, 3:03 pm

Just changed my password wasn't too worried.

LordCoder - May 3, 2016, 3:03 pm

(May 3, 2016 03:02 PM)Raymond Reddington Wrote: [\[CITE\]](#) Are you saying HF's 2015 DB was dumped?

I also heard a while back ago, but I didn't think it was real. Damn.

SparkMasterTape - May 3, 2016, 3:05 pm

I'll enable 2FA right now, just need to find an app. Thanks omni.

Just enabled it.

webdev77 - May 3, 2016, 3:05 pm

The heads up is appreciated. Thanks for the reminder to not reuse passwords. I am not guilty of doing so, but I've realized that some are far too close to one another. I just spent the past half hour changing everything around.

CyberGuard - May 3, 2016, 3:07 pm

(May 3, 2016 03:03 PM)LordCoder Wrote: [\[CITE\]](#) I also heard a while back ago, but I didn't think it was real. Damn.

Yup it was real, I know someone that bought it on a private forum.

Raymond Reddington - May 3, 2016, 3:07 pm

(May 3, 2016 03:03 PM)LordCoder Wrote: [\[CITE\]](#) I also heard a while back ago, but I didn't think it was real. Damn.

Possibly a rumor? IDK, I don't believe this.

Weebex - May 3, 2016, 3:08 pm

Got the email, changed the pass, thanks for the fast heads up Omni!

Raymond Reddington - May 3, 2016, 3:08 pm

(May 3, 2016 03:07 PM)CyberGuard Wrote: [\[CITE\]](#) Yup it was real, I know someone that bought it on a private forum.

Does the forum begin with D and end with e? ?

CyberGuard - May 3, 2016, 3:09 pm

(May 3, 2016 03:07 PM)Raymond Reddington Wrote: [\[CITE\]](#) Possibly a rumor? IDK, I don't believe this.

In 2011, 2014 and 2015 the HF db was dumped.

2011 is public

2014 is pretty private

2015 is private

Yin Yang - May 3, 2016, 3:10 pm

Even though a PM hasn't been sent to me, I activated Gauth.

Knucklez. - May 3, 2016, 3:10 pm

Thanks for the update, changed password like requested.

I freaked out a little bit when I received the email notification, thought I was the only one.

SIM-1729678 - May 3, 2016, 3:10 pm

This is the reason that I change my password every month. When I saw the email I had a feeling that it was fake, though after reading this I changed my password twice just to be sure. Thanks for the update.

Coton Pker - May 3, 2016, 3:12 pm

I was finally forced to enable my 2FA today :(

I did it once before when it was new, but it just disappeared randomly afterward and I never re-did it until now.

though my password has been the same since the day I joined this forum :(I had to change it today

Duk3 - May 3, 2016, 3:13 pm

If you recently change your password, would you still need to change your password?

Brendan - May 3, 2016, 3:14 pm

(May 3, 2016 03:13 PM)Duk3 Wrote: [\[CITE\]](#) If you recently change your password, would you still need to change your password?

I would still change it just to be safe.

exploit.c - May 3, 2016, 3:14 pm

Omni, I shot you a PM. You should read it.

Silicon - May 3, 2016, 3:14 pm

Yeah, I've just enabled 2FA now as a precaution, even though I don't frequent HF any more. Don't want my account being compromised.

Raymond Reddington - May 3, 2016, 3:14 pm

(May 3, 2016 03:13 PM)Duk3 Wrote: [\[CITE\]](#) If you recently change your password, would you still need to change your password?
How long does it take anyways lol?
Just do it, wouldn't do harm.

Rebustly - May 3, 2016, 3:15 pm

(May 3, 2016 03:13 PM)Duk3 Wrote: [\[CITE\]](#) If you recently change your password, would you still need to change your password? Change it to be safe, but a straight answer would be no. The database is from late 2015 -- early 2016.

SIM-1729678 - May 3, 2016, 3:15 pm

(May 3, 2016 03:13 PM)Duk3 Wrote: [\[CITE\]](#) If you recently change your password, would you still need to change your password?
You can never be too secure. Just do it, it will make you feel better also.

Raymond Reddington - May 3, 2016, 3:15 pm

(May 3, 2016 03:14 PM)exploit.c Wrote: [\[CITE\]](#) Omni, I shot you a PM. You should read it.
Time to get closed. Good time mate. ?

Cyber - May 3, 2016, 3:15 pm

Alright, all taken care of. Thanks for letting us know omni

exploit.c - May 3, 2016, 3:17 pm

(May 3, 2016 03:15 PM)Raymond Reddington Wrote: [\[CITE\]](#) Time to get closed. Good time mate. ?
Get closed? Why would I get closed? I asked him to read PM because I have information on where a bug is sitting.

Backopy - May 3, 2016, 3:17 pm

Sounds like a sophisticated persistent threat, I'm sure HF has many. The database that was leaked some years ago is pretty old and hashed, why would the APT initiate an attack so long after and more importantly, how? That doesn't appear to be the vector of attack for this APT.

The smart APTs initiate an attack against an infrastructure to provoke a quick/rushed or targeted response such as the actions you took;

- Forced PW resets
- Increase minimum password character length
- Applied a new plugin

Is it possible to post the list of members who were compromised? I can't see any harm in doing so and I think it would only benefit you because as a community we have the ability to cross-reference data considerably faster as we have more numbers - we as a community might be able to find similarities between the accounts to potentially narrow down the attack vector.

Retribute - May 3, 2016, 3:17 pm

I appreciate the heads up. Password changed.
Still have not received the email, but I will wait.

liam1uk - May 3, 2016, 3:18 pm

Hello,

I am one of these 40 or so users that have apparently been breached. I would recommend anyone of these 40 users to use Authy the application. It is what I have been using.

Arizonalce - May 3, 2016, 3:20 pm

(May 3, 2016 01:39 PM)The JOker Wrote: [\[CITE\]](#) Does the DB save old info like past emails and passwords?

It must save past IP's or the trustscan wouldn't work correct?

I'd like to know this awell

Rikk?a - May 3, 2016, 3:23 pm

(May 3, 2016 03:18 PM)liam1uk Wrote: [\[CITE\]](#) Hello,

I am one of these 40 or so users that have apparently been breached. I would recommend anyone of these 40 users to use Authy the application. It is what I have been using.

Disregard my last post anyways glad to see you got your account back.

I assumed you were trolling but you aren't my apologies.

BooGod - May 3, 2016, 3:24 pm

Well, I wouldn't be surprised if someone tried to log on my account before since I've got ratted twice and got doxed once by not taking much care in the past. I am using a new email, the password is not to old but I'll change again when on laptop.

Thanks for letting us know Omni :nohat:

Riggs - May 3, 2016, 3:25 pm

Was there a forced password reset following the last known dump? I can't remember...

YayHar - May 3, 2016, 3:26 pm

Does changing your password log you out of all devices?

e?erg1zer - May 3, 2016, 3:27 pm

So does this mean that I should then disable and re-enable 2FA, or that it will automatically disable 2FA after changing my password, or finally that I have nothing else to worry about having made a new password, that I can leave my current 2FA situation as it is?

liam1uk - May 3, 2016, 3:28 pm

(May 3, 2016 03:25 PM)Riggs Wrote: [\[CITE\]](#) Was there a forced password reset following the last known dump? I can't remember...

Yes, I believe there was. At least from what I can remember but that was a while ago if I remember correctly. I never received issues with my account back then.

Egregious - May 3, 2016, 3:28 pm

(May 3, 2016 03:26 PM)YayHar Wrote: [\[CITE\]](#) Does changing your password log you out of all devices?

No, it doesn't, unfortunately.

Retribute - May 3, 2016, 3:28 pm

(May 3, 2016 03:28 PM)Egregious Wrote: [\[CITE\]](#) No, it doesn't, unfortunately.It logged me out.

SOS. - May 3, 2016, 3:28 pm

Just changed my password again, thanks for the heads up.

Rikk?a - May 3, 2016, 3:28 pm

(May 3, 2016 03:28 PM)Egregious Wrote: [\[CITE\]](#) No, it doesn't, unfortunately.
It does for me apparently.

Rubixa - May 3, 2016, 3:29 pm

(May 3, 2016 03:26 PM)YayHar Wrote: [\[CITE\]](#) Does changing your password log you out of all devices?

Yes it does, changed my password yesterday and had to log back in on my phone. It would be silly for it not to log out when changed.

??? ??? - May 3, 2016, 3:32 pm

Thanks for this Omni. I just received the email :)

tweety - May 3, 2016, 3:32 pm

I got an email about it, does that mean I'm one of the 40? My account doesn't seem compromised.

Rikk?a - May 3, 2016, 3:33 pm

(May 3, 2016 03:32 PM)Tweety. Wrote: [\[CITE\]](#) I got an email about it, does that mean I'm one of the 40? My account doesn't seem compromised.

He sent this to all Ub3r's.

Rubixa - May 3, 2016, 3:33 pm

I activated Gauth as soon as I was able to with Google Authenticator, Works well I would recommend it and I also recently changed my email and password, Thanks for the heads up, Omni.

J?son - May 3, 2016, 3:33 pm

I just received the email and have changed my password and enabled 2fa.

Thanks for looking out for the community. ?

tweety - May 3, 2016, 3:34 pm

(May 3, 2016 03:33 PM)Rikk????????????????a Wrote: [\[CITE\]](#) He sent this to all Ub3r's.
Ah, I'm potato, never mind.

Ahri????? - May 3, 2016, 3:34 pm

Considering my HF password is 30 characters+ don't know if I need to even change my password. Never really had a security breach considering everything has 2FA. Plus the only device with ease of access to everything requires my fingerprint to access. Personally I believe most of HF takes security as a joke. Questions me how people get infected and reuse the same password.

ClassifiedHex - May 3, 2016, 3:34 pm

This must be frightening for upgraded members they put time and their own money into their accounts

minimalist - May 3, 2016, 3:34 pm

(May 3, 2016 03:32 PM)Tweety. Wrote: [\[CITE\]](#) I got an email about it, does that mean I'm one of the 40? My account doesn't seem compromised.

At first, Omniscient said this:

Quote:I have contacted all the accounts compromised with 2FA enable and still open instructing them to immediately change their passwords and leave 2FA enabled.

...but I guess that he changed his mind and sent it to everybody:

Quote:An email is being sent to all Ub3r instructing them to create a new password and to enable Gauth/2FA.

?Fazzer - May 3, 2016, 3:35 pm

Well thanks for the heads-up omni. Changed my pass and hoping that this does not long last.

Also guys enable 2fa it's very secured.

\$lick - May 3, 2016, 3:37 pm

So I got an email about this, my HF password is unique to HF, and has only ever been shown in my email account (because HF generated it for me) could it be that my email was hacked? Or even HackForums outgoing emails?

Edit: Just checked, my email account was not hacked and I have 2FA here, so I'm safe.

WoahWhat - May 3, 2016, 3:38 pm

All accounts compromised are older than 1 year ago. Which might be when the compromise occurred, maybe.

Breached again?

Oh....btw some good news also...HF database does not store any private order data like name, address, or phone. We only have the most basic info which is IPs and emails.

Yeah, but your Witz-a-thingie does store it.

This once again proves no one should ever sign up with real info on a website.

Coton Pker - May 3, 2016, 3:39 pm

I never got an email, and instead I got a -10 (DO NOT DEAL) and a PM about it :p
does that mean I'm one of the super elite at risk members yo?

Ov3rFl0w_ - May 3, 2016, 3:39 pm

There is many many many (New accounts) posting infected threads (Crypters) specially in Cryptography board. Just saying if u could stop these new registered spammers from posting such threads it will be really helpful to protect some members

Epicur - May 3, 2016, 3:40 pm

Thanks for being honest about this Omni, another person would have just kept it for himself and try to solve it from behind, which could have lead to serious problems, now we only have to change our PWds, not a big deal.

Good luck to everyone.

\$lick - May 3, 2016, 3:40 pm

(May 3, 2016 03:39 PM)Coton Pker Wrote: [\[CITE\]](#) I never got an email, and instead I got a -10 (DO NOT DEAL) and a PM about it :p
does that mean I'm one of the super elite at risk members yo?
I never got a PM about it :C

Khamul - May 3, 2016, 3:40 pm

(May 3, 2016 03:38 PM)WoahWhat Wrote: [\[CITE\]](#) All accounts compromised are older than 1 year

ago. Which might be when the compromise occurred, maybe.

Breached again?

Oh....btw some good news also...HF database does not store any private order data like name, address, or phone. We only have the most basic info which is IPs and emails.

Yeah, but your Witz-a-thingie does store it.

This once again proves no one should ever sign up with real info on a website.
You should know, you have 5 separate accounts...

YayHar - May 3, 2016, 3:41 pm

(May 3, 2016 03:39 PM)Coton Pker Wrote: [\[CITE\]](#) I never got an email, and instead I got a -10 (DO NOT DEAL) and a PM about it :p
does that mean I'm one of the super elite at risk members yo?
Rest in peace

Rikk?a - May 3, 2016, 3:41 pm

(May 3, 2016 03:39 PM)Coton Pker Wrote: [\[CITE\]](#) I never got an email, and instead I got a -10 (DO NOT DEAL) and a PM about it :p
does that mean I'm one of the super elite at risk members yo?Well what do you think? Of course.

(May 3, 2016 03:39 PM)Ov3rFI0w_ Wrote: [\[CITE\]](#) There is many many many (New accounts) posting infected threads (Crypters) specially in Cryptography board. Just saying if u could stop these new registered spammers from posting such threads it will be really helpful to protect some membersHe stops spammers and there needs to be new people on this forum not all members in this community are here to infect members.

Coton Pker - May 3, 2016, 3:43 pm

woohoo then I guess I'm special :)

WoahWhat - May 3, 2016, 3:43 pm

(May 3, 2016 03:40 PM)Microsoft Word ® Wrote: [\[CITE\]](#) You should know, you have 4 separate accounts... Hurr durr, let me protect Omni, our great lord and saviour

Just shut up. HF isn't the place for anonymity, or security for that part.
Also, since you're asking:
uid=792136

Waziti - May 3, 2016, 3:45 pm

Well damn, just changed my password. That's scary.

Khamul - May 3, 2016, 3:46 pm

(May 3, 2016 03:43 PM)WoahWhat Wrote: [\[CITE\]](#) *Hurr durr, let me protect Omni, our great lord and saviour*

Just shut up. HF isn't the place for anonymity, or security for that part.
Also, since you're asking:
uid=792136

Lol, butthurt much? Why even bother making a new account, it's just gonna get banned?

Omoi - May 3, 2016, 3:47 pm

Just seen the email and already have it enabled.

Ov3rFl0w_ - May 3, 2016, 3:49 pm

(May 3, 2016 03:41 PM)Rikk????????????a Wrote: [\[CITE\]](#) He stops spammers and there needs to be new people on this forum not all members in this community are here to infect members.

More (Sub Moderators) to watch and analyze files are very helpful in such threads. its not even like a mod,, its like a trusted member who can give a feedback on forums but in more official way.

WoahWhat - May 3, 2016, 3:52 pm

(May 3, 2016 03:46 PM)Microsoft Word ® Wrote: [\[CITE\]](#) Lol, butthurt much? Why even bother making a new account, it's just gonna get banned?

Do you see me care, broski?

?

Speed Test - May 3, 2016, 3:52 pm

Thanks a lot about this thread! I was so scared!

I'm changing my password right now!

Pharcyde - May 3, 2016, 3:53 pm

I'm glad I enabled 2fa within days of its release. Changing my password now.
Cheers!

i a m g o n e - May 3, 2016, 3:56 pm

So do i change my password or what? im confused

Khamul - May 3, 2016, 3:56 pm

(May 3, 2016 03:53 PM)Nexus™ ?? Wrote: [\[CITE\]](#) Linking that dump was stupid.

Also I've never used a stressed so it couldn't have been.

Wait but I thought you weren't compromised or did you get a PM?

Retribute - May 3, 2016, 3:56 pm

(May 3, 2016 03:56 PM)I like candy Wrote: [\[CITE\]](#) So do i change my password or what? im confusedYes, that is the recommended action.

Rikk?a - May 3, 2016, 3:57 pm

(May 3, 2016 03:56 PM)I like candy Wrote: [\[CITE\]](#) So do i change my password or what? im confused

Read the thread for once.

Mooncake - May 3, 2016, 3:57 pm

This is super strange, couple months ago, my Coinbase was hacked, and I lost a few BTC, I couldn't understand why since the same password I use for there, is used here. It's super complex, as well as, only used here, and on Coinbase. Now it all makes sense. Super sad though.

brian188246 - May 3, 2016, 3:57 pm

(May 3, 2016 03:56 PM)Kogon Wrote: [\[CITE\]](#) You sure?

Your username on HF is Coton Pker, you have lots of active threads in the Runescape section of HF.

The usernames used on the leaked database were different but match a similar string in the second part of your username (Pker) and the email nolifepker@web.de was used on the DB.

None of your posts are accurate it's actually annoying

Vaxxor - May 3, 2016, 3:59 pm

Thanks for updating us, i changed my pw

Rikk?a - May 3, 2016, 3:59 pm

(May 3, 2016 03:56 PM)Kogon Wrote: [\[CITE\]](#) -snip-
Stop posting personal data you idiot.

\$lick - May 3, 2016, 4:00 pm

(May 3, 2016 03:56 PM)Microsoft Word ® Wrote: [\[CITE\]](#) Wait but I thought you weren't compromised or did you get a PM?

I got an email, so I'm guessing that somebody tried to log into my account but failed due to 2FA.

Either that or everybody got the email.

Khamul - May 3, 2016, 4:01 pm

(May 3, 2016 04:00 PM)Nexus™ ?? Wrote: [\[CITE\]](#) I got an email, so I'm guessing that somebody tried to log into my account but failed due to 2FA.

Either that or everybody got the email.

Every Ub3r got the email.

i a m g o n e - May 3, 2016, 4:03 pm

(May 3, 2016 03:56 PM)Retribute Wrote: [\[CITE\]](#) Yes, that is the recommended action.
Ok cool thanks for the help

Stoke - May 3, 2016, 4:04 pm

Updated my password and re-checked my gauth.

I'm good.

SIM-1676753 - May 3, 2016, 4:04 pm

Haven't changed my password to something new since I registered. Gonna make a new one now.

Coton Pker - May 3, 2016, 4:05 pm

(May 3, 2016 04:03 PM)\$tash Wrote: [\[CITE\]](#) It seems you have an extreme case of retardation.
it's a conspiracy maaaann @.@
they staff is out to get our info yo!
panic!

HCIM - May 3, 2016, 4:05 pm

Wow.... How unfortunate... Good thing I'm not Ub3r.

Rikk?a - May 3, 2016, 4:05 pm

(May 3, 2016 04:01 PM)ByteNull Wrote: [\[CITE\]](#) And to enjoy your botnet. Not trusting this, 2FA sounds like something the HF staff can use to track me here.

Thank fuck I don't go on HF anymore.

Totally considering almost every forum has it.

<http://community.mybb.com/thread-162369.html> | 2FA (2 Factor Authentication)

Mooncake - May 3, 2016, 4:08 pm

(May 3, 2016 04:05 PM)Frostic Wrote: [\[CITE\]](#) Wow.... How unfortunate... Good thing I'm not Ub3r. I think, it's worse that you aren't.

Dredd - May 3, 2016, 4:08 pm

So I got your email like 4 times does that mean that someone knows my password? Should I be alarmed?

Ambien - May 3, 2016, 4:09 pm

I just changed my password right now.

Retribute - May 3, 2016, 4:09 pm

(May 3, 2016 04:08 PM)? Wrote: [\[CITE\]](#) So I got your email like 4 times does that mean that someone knows my password? Should I be alarmed?The email has been sent to all Ub3rs.

Dredd - May 3, 2016, 4:10 pm

(May 3, 2016 04:09 PM)Retribute Wrote: [\[CITE\]](#) The email has been sent to all Ub3rs. Ah okay in the OP I thought omni said he only sent it to compromised accounts might of read it wrong I'm on my phone.

Rikk?a - May 3, 2016, 4:10 pm

(May 3, 2016 04:08 PM)Profitvolt Wrote: [\[CITE\]](#) I think, it's worse that you aren't. People who want to hijack accounts here would possibly aim for ub3r or anything higher.

Ov3rFI0w_ - May 3, 2016, 4:11 pm

(May 3, 2016 04:01 PM)ByteNull Wrote: [\[CITE\]](#) And to enjoy your botnet. Not trusting this, 2FA sounds like something the HF staff can use to track me here.

Thank fuck I don't go on HF anymore.

1st of all, Stupid whom running a botnet and saying that to public forum LOL,,,
2nd of all, This forum is not illegal nor any service on it ... if u did anything stupid it authorities can just hunt u down from ur info in DB Mr black hat hacker !

Rubixa - May 3, 2016, 4:12 pm

(May 3, 2016 04:10 PM)blessthefall Wrote: [\[CITE\]](#) Wtf? I don't think that's even possible unless Omni owns the 2FA apps and websites.
You are correct.

Retribute - May 3, 2016, 4:12 pm

(May 3, 2016 04:10 PM)? Wrote: [\[CITE\]](#) Ah okay in the OP I thought omni said he only sent it to compromised accounts might of read it wrong I'm on my phone."An email is being sent to all Ub3r instructing them to create a new password and to enable Gauth/2FA."

Coton Pker - May 3, 2016, 4:13 pm

(May 3, 2016 04:12 PM)Retribute Wrote: [\[CITE\]](#) "An email is being sent to all Ub3r instructing them to create a new password and to enable Gauth/2FA."
but but but... I didn't get an email and I'm ub3r :(

Retribute - May 3, 2016, 4:14 pm

(May 3, 2016 04:13 PM)Coton Pker Wrote: [\[CITE\]](#) but but but... I didn't get an email and I'm ub3r :(

Neither have I. It takes time, however. Last I checked a couple hours ago, only 35% of the emails have been sent. So patience.

Coton Pker - May 3, 2016, 4:15 pm

(May 3, 2016 04:14 PM)Retribute Wrote: [\[CITE\]](#) Neither have I. It takes time, however. Last I checked a couple hours ago, only 35% of the emails have been sent. So patience.
nah I won't get one.. I got a personal PM.
this nigga legit thinks my shit is stolen.

Rubixa - May 3, 2016, 4:15 pm

(May 3, 2016 04:13 PM)Coton Pker Wrote: [\[CITE\]](#) but but but... I didn't get an email and I'm ub3r :(It didn't get sent at all at once in an instant, I believe I read it's being rolled out in a percentage.

Dredd - May 3, 2016, 4:15 pm

(May 3, 2016 04:14 PM)Retribute Wrote: [\[CITE\]](#) Neither have I. It takes time, however. Last I checked a couple hours ago, only 35% of the emails have been sent. So patience.
I got 5 emails saying the exact same thing.

Ludicolo - May 3, 2016, 4:16 pm

Thanks Omni for the heads up.

Horizon - May 3, 2016, 4:16 pm

Thanks for the heads up Omni. Enabling mine now. Thanks.

Mooncake - May 3, 2016, 4:22 pm

(May 3, 2016 04:10 PM)Rikk????????????????a Wrote: [\[CITE\]](#) People who want to hijack accounts here would possibly aim for ub3r or anything higher.

Really ? Logically, I think they would go for accounts that are less likely to have 2FA enabled, but you have a point, maybe I assumed every UB3R enabled 2FA.

Goodies - May 3, 2016, 4:22 pm

(May 3, 2016 04:01 PM)ByteNull Wrote: [\[CITE\]](#) And to enjoy your botnet. Not trusting this, 2FA sounds like something the HF staff can use to track me here.

Thank fuck I don't go on HF anymore.

I have personally reverse engineered the 2FA and can confirm that it is not a botnet.

Rikk?a - May 3, 2016, 4:23 pm

(May 3, 2016 04:22 PM)Profitvolt Wrote: [\[CITE\]](#) Really ? Logically, I think they would go for accounts that are less likely to have 2FA enabled, but you have a point, maybe I assumed every UB3R enabled 2FA.

Some ub3r's are lazy, No offense to the ones who have 2FA Disabled.

YayHar - May 3, 2016, 4:23 pm

(May 3, 2016 04:22 PM)Profitvolt Wrote: [\[CITE\]](#) Really ? Logically, I think they would go for accounts that are less likely to have 2FA enabled, but you have a point, maybe I assumed every UB3R enabled 2FA.

Lots of ub3rs don't have it enabled

Shoe - May 3, 2016, 4:23 pm

(May 3, 2016 04:22 PM)Goodies Wrote: [\[CITE\]](#) I have personally reverse engineered the 2FA and can confirm that it is not a botnet.

Don't trust Goodies.

OT: Thanks for the warning. I'll be taking the precautions necessary.

HFTetramorph - May 3, 2016, 4:24 pm

Massive props for reporting it as soon as you figured out. Some companies and other organizations can barely stand the idea of doing this. It is great to see you following the best practices when it comes down to these kinds of things.

Omni, a question however. If a database breach did occur, doesn't that mean the secrets for the Two Factor Auth could also be compromised? Meaning that the tokens could be generated client side for the attackers?

Regards

(May 3, 2016 04:01 PM)ByteNull Wrote: [\[CITE\]](#) And to enjoy your botnet. Not trusting this, 2FA sounds like something the HF staff can use to track me here.

Thank fuck I don't go on HF anymore.
Im sorry.. Just how uneducated in what Two Factor Authentication actually is can you be? Are you going for a new world record?

2FA in no way can be used to track you. You must be a complete idiot to even think that something that doesn't even require an active network connection (Only prerequisite is a correctly set time) can actually be used to track you..

2FA is a shared secret used with the current time to generate a 6 digit number. That is all it is. The shared secret is on both the server, and your phone or wherever you store it. You can do napkin math if you must to figure out the 6 digit number..

Miniature - May 3, 2016, 4:25 pm

Just changed pass, changed email and changed the pass on the email :)
Hopefully I'm secure now.

Supreme???????? - May 3, 2016, 4:25 pm

Thanks for the heads up, Omni. Will change password in a few minutes.

Coton Pker - May 3, 2016, 4:26 pm

(May 3, 2016 04:23 PM)YayHar Wrote: [\[CITE\]](#) Lots of ub3rs don't have it enabled

(May 3, 2016 04:23 PM)Rikk????????????????a Wrote: [\[CITE\]](#) Some ub3r's are lazy, No offense to the ones who have 2FA Disabled.

I was lazy lol.
I had it when it first was put on here, but then somehow or another it got removed and I just never bothered to put it back on.

but when they say high risk accounts without 2FA, they're not talking about just Ub3r, they're talking about Ub3r with mad awards/posts/rep that someone could steal and use to scam a quick few thousand on their established trust.

which is why my shit's folded currently.
but I'mma laugh when I get banned and RF'd for making jokes about it :p

Omniscient - May 3, 2016, 4:26 pm

Quote:So reading OP, is it safe to assume being I got that email my PW needs to be changed and keep 2FA enabled @ all times?

That's like asking if you should keep your car door locked with the alarm on. I've been pushing for months for more 2FA usage. Over 40 accounts would have been stolen but instead at least 25 of those accounts were saved by 2FA. And that's just this past few days. Who knows how many other accounts were saved because of it.

And I still assume the compromise was on our end because this is a lot of accounts and the logins are not attempts...they are logins. So they 100% know the password. I'm extremely doubtful this was shared site passwords. A few members who were compromised have more or less confirmed that. What is still possible is that HF has a rogue software infecting members with RAT's or keyloggers. That's actually a possibility but I'm leaning toward a site compromise from a year ago. Unless only older members have been infected a long time ago and didn't know. And not one person has confirmed being infected on their local computer. So again, most likely scenario is we had a compromise a year ago and passwords are being decrypted.

Quote:Also might make sense to ask people to log out after changing the password to kill all other sessions.

I may force logout of all members. Still considering options and I have to write some code to add extra logging. In the meantime it's ultra important 2FA is enabled.

Quote:Why can't an SMS just be sent with a code?
So you'd like HF to store your cell phone number?

Quote:It was probably the 2015 HF DB dump that was abused.

Still have yet to see any real evidence, other than these stolen accounts, that it happened. I have to assume it must have. We moved to new servers 7 months ago. Unsure if that's stopped the compromise or not. It's possible there is a 0-day MyBB exploit.

Quote:Are you saying HF's 2015 DB was dumped?

It's starting to seem possible and even likely that it was at some point. Almost surely not a full DB dump but probably a grab of the user table. Still investigating and trying to get actual confirmation.

Quote:Yup it was real, I know someone that bought it on a private forum.

Unfortunately I continue to get the "I have a friend of a friend who saw it" type of remarks and I have yet to see any evidence myself. Likely if the dump does exist the person who grabbed it has been extremely careful with it. But now that I'm making this thread and alerting members that may change.

Very likely within one week all users will have new passwords and all upgraded accounts will have 2FA enabled.

Quote:Is it possible to post the list of members who were compromised? I can't see any harm in doing so and I think it would only benefit you because as a community we have the ability to cross-reference data considerably faster as we have more numbers - we as a community might be able to find similarities between the accounts to potentially narrow down the attack vector.

I contemplated that. I don't think it's going to help members. It's almost all Ub3r accounts with the newest account from June 2015. That's why so far I don't think it's that new the dump.

And I have some working theories on the compromise. Until I know more I can't really say much else about it.

Quote:Was there a forced password reset following the last known dump?

Yes.

Quote:Does changing your password log you out of all devices?

Yes, it should.

Quote:So does this mean that I should then disable and re-enable 2FA

At this time I am not recommending that. I actually prefer you leave it enabled.

Now all L33t are getting the email too.

Sadly, if indeed we're still compromised with a MyBB exploit we may need to do a full PW reset again for all members.

Quote:Yeah, but your Witza-thingie does store it.

No, it doesn't. I ceased storing that data at Witza a long time ago. And when I stopped taking PP I stopped requiring address information. And then I deleted from HF's databases any of that private data.

Closing this for now so everyone can read my lengthy post.

Walt Disney™ - May 3, 2016, 5:39 pm

Password updated. Thanks for letting us know.

Omniscient - May 8, 2016, 2:31 pm

<https://hackforums.net/showthread.php?tid=5263387>