

Forum:[Hack Forums](#)

Thread: [BLC IS STILL SECURE - READ IF YOU HAVE A CUSTOM BLC ADDRESS](#)

Chris ?ansen - May 14, 2013, 5:55 am

[READ THIS THREAD FOR ANSWERS](#)

So... I was mining on the night of 5/13/2013, and left the miner on all night so I could earn more. I woke up to 66 hashes that I had solved, but only 38 coins connected to my account. I thought to myself, "Okay, just let the network refresh for a second, and you will have the BLC." I refreshed the network, and I got no more BLC. WTF RIGHT?! I was starting to think that I got fucked over by not reading somewhere that someone takes a cut of what you mine... not the case. I refreshed the transaction history, and found that the notorious Who? has been stealing BLC from people, and I was just his latest victim. It looks really weird because it says that the BLC was sent directly from me, to his many addresses that I assume he just made with a script, but that is not the case at all. My best guess is that he has access somehow to the network that BLC runs off of. How else would he had be able to do this.

I have already checked my PC for malware, scanned the IP addresses coming from my PC, and to my PC, and nothing is out of the ordinary... just that I lost a lot of BLC. I also understand that this is a giant wall of text to read, but I just woke up to this, and I am in a rush to send messages all around to people who are close to BLC to make sure they understand that their stuff might just be taken away if it even so much looks like you can earn a profit. THIS IS NOT AT THE FAULT OF BLOOCOINS CREATORS... ITS AT THE FAULT OF Who? AND OTHER HACKERS.

tl;dr BLC has been hacked probably, and Who? is stealing BLC from miners of it like myself.

PROOF:

<https://imgur.com/h6NA834,ZhkWLCj,Spcde6j>

<https://puu.sh/2TgTH.png>

<https://i.imgur.com/GFwwzA5.png>

Any additional proof that anyone submits will show up here.

UPDATES:

UPDATE 1: Don't know if its because of a related issue, or something else, but the network keeps going down for me...

UPDATE 2: Who? admitted to stealing the BLC from me, and most likely other people too. Now we wait for the hole to be closed by Max... :\

UPDATE 3: Narrowing down the possibility's of this attack...

UPDATE 4: IF YOU HAVE A CUSTOM BLC ADDRESS FROM ZSNAG, THEN YOU NEED TO MAKE YOUR OWN ADDRESS THAT YOU GET FROM RUNNING THE BLOOCOIN.PY FILE FOR THE FIRST TIME, AND SEND THE BLC FROM YOUR CUSTOM ADDRESS TO THE NEW RANDOM ADDRESS!

Any updates will be shown here as I get it so that people know the newest story...

Mohatu - May 14, 2013, 6:06 am

Interesting.

Keep in mind the difficulty also switched to 8 last night, so that may be why some of the coins weren't added to your account (eg. you were still solving for difficulty 7, which were rejected by the

lvl 8 server).

Who? does have the most BLC at the moment, stating that he has a GPU miner he "whipped up" in an evening.

Chris ?ansen - May 14, 2013, 6:10 am

(May 14, 2013 06:06 AM)Mohatu Wrote: [\[CITE\]](#) Interesting.

Keep in mind the difficulty also switched to 8 last night, so that may be why some of the coins weren't added to your account (eg. you were still solving for difficulty 7, which were rejected by the lvl 8 server).

Who? does have the most BLC at the moment, stating that he has a GPU miner he "whipped up" in an evening.

I thought about the difficulty being ramped up, but when the history says that I sent a bunch of BLC to addresses like "RyanC_stealing_your_bloocoins_here93njsz" in 1 BLC per transaction increments... I have my doubts that it was because of the difficulty. But thanks for the input.

ThePainfulPanda - May 14, 2013, 6:17 am

It's not implausible that you could write a GPU miner in an evening. He's claiming that he use the JtR Kernels, which would make it quite achievable in an evening.

TheCuban - May 14, 2013, 6:23 am

You guys are all just totally off the grid out of control

Mohatu - May 14, 2013, 6:27 am

Unfortunate.

Lol7575 - May 14, 2013, 6:29 am

That's just sad. Won't be mining any more BLC from now on :/

Chris ?ansen - May 14, 2013, 6:30 am

(May 14, 2013 06:27 AM)Mohatu Wrote: [\[CITE\]](#)

Unfortunate.Well fuck... this god damn sucks. :\

Approach - May 14, 2013, 6:31 am

Ah wow, although this sucks for a lot of users it was an impressive attack by Who?.

Mohatu - May 14, 2013, 6:42 am

Can't guarantee it's an actual attack. If Who? (or whoever this is) simply had access to the bloostamp file at one point in time, the account would be permanently unsecure. This is why you shouldn't generate bloostamp files on websites (so you can have "custom" names).

He has a custom name, meaning he most likely used that one website to get it. If that website stores the keys, and it is compromised, then it isn't our faults the account gets stolen from.

I recommend just having an anonymous SHA1 username generated by either mine or the official client.

Chris ?ansen - May 14, 2013, 6:55 am

(May 14, 2013 06:42 AM)Mohatu Wrote: [\[CITE\]](#) Can't guarantee it's an actual attack. If Who? (or whoever this is) simply had access to the boostamp file at one point in time, the account would be permanently unsecure. This is why you shouldn't generate boostamp files on websites (so you can have "custom" names).

He has a custom name, meaning he most likely used that one website to get it. If that website stores the keys, and it is compromised, then it isn't our faults the account gets stolen from.

I recommend just having an anonymous SHA1 username generated by either mine or the official client. Already a head of you... working on it right now.

Sir Paul McCartney - May 14, 2013, 7:32 am

Uhm, I don't believe one bit of this thread, I've been talking to him on the IRC I doubt he could. You can edit the transactions by double clicking on them (Probably local only) but it's still easily fake-able.

Danoontje Power - May 14, 2013, 7:33 am

Awww man just getting the feeling of BLC now it's hacked :(

Mohatu - May 14, 2013, 7:34 am

(May 14, 2013 07:33 AM)Danoontje Power Wrote: [\[CITE\]](#) Awww man just getting the feeling of BLC now it's hacked :(

It's not hacked, learn to read before taking sides.

His account is compromised because he decided to go for a custom address.

Danoontje Power - May 14, 2013, 7:35 am

(May 14, 2013 07:34 AM)Mohatu Wrote: [\[CITE\]](#) It's not hacked, learn to read before taking sides.

His account is compromised because he decided to go for a custom address.

Ooow Okay thanks for the heads up, im gonna mine now xD

rather - May 14, 2013, 7:43 am

(May 14, 2013 07:34 AM)Mohatu Wrote: [\[CITE\]](#) It's not hacked, learn to read before taking sides.

His account is compromised because he decided to go for a custom address.

Way to disregard potential vulnerabilities.

"It could be this so it has to be this"

Chris ?ansen - May 14, 2013, 7:52 am

(May 14, 2013 07:34 AM)Mohatu Wrote: [\[CITE\]](#) It's not hacked, learn to read before taking sides.

His account is compromised because he decided to go for a custom address. Yea.. um... I agree this is a possibility... but its not 100% confirmed that this is the reason. If more people with custom address come forward about getting their BLC taken, then sure, its probably the problem, but until then its not 100% that the reason is because of a custom address.

(May 14, 2013 07:32 AM)?Ice ?King™ Wrote: [\[CITE\]](#) Uhm, I don't believe one bit of this thread, I've been talking to him on the IRC I doubt he could.

You can edit the transactions by double clicking on them (Probably local only) but it's still easily fake-able. Don't doubt Who?... he has shown his skills in the past.

As for being faked, if I understand the "transactions" command correctly... it does not store the transactions locally on the HDD, but when the command is entered, it pulls the info from the BLC network. If you think this is incorrect, or wrong, let me know, but here is another picture...

<https://i.imgur.com/GFwwzA5.png>

ComponY - May 14, 2013, 7:54 am

Lmao. This is kind of funny in a way. I guess sites need more security.

Sir Paul McCartney - May 14, 2013, 8:02 am

(May 14, 2013 07:52 AM)Jennifer Lawrence Wrote: [\[CITE\]](#) Yea.. um... I agree this is a possibility... but its not 100% confirmed that this is the reason. If more people with custom address come forward about getting their BLC taken, then sure, its probably the problem, but until then its not 100% that the reason is because of a custom address.

Don't doubt Who?... he has shown his skills in the past.

As for being faked, if I understand the "transactions" command correctly... it does not store the transactions locally on the HDD, but when the command is entered, it pulls the info from the BLC network. If you think this is incorrect, or wrong, let me know, but here is another picture...

<https://i.imgur.com/GFwwzA5.png>well in this case bloocoins didn't get hacked, YOU did. Stop causing a lot of drama to it, bloocoins didn't get hacked

Mohatu - May 14, 2013, 8:09 am

I hope this clears it up for everyone, EVERYONE who made a custom Bloocoin address on that website now has a compromised account.

<https://hackforums.net/showthread.php?tid=3479074>

Chris ?ansen - May 14, 2013, 8:11 am

(May 14, 2013 08:02 AM)?Ice ?King™ Wrote: [\[CITE\]](#) well in this case bloocoins didn't get hacked, YOU did. Stop causing a lot of drama to it, bloocoins didn't get hackedI didn't send any BLC to any of those addresses, and there is no malware on my PC. So how did I get hacked? The fucking addresses say "RyanC_stealing_your_bloocoins_here"

Mohatu - May 14, 2013, 8:13 am

(May 14, 2013 08:11 AM)Jennifer Lawrence Wrote: [\[CITE\]](#) I didn't send any BLC to any of those addresses, and there is no malware on my PC. So how did I get hacked? The fucking addresses say "RyanC_stealing_your_bloocoins_here"

Once again: <https://hackforums.net/showthread.php?tid=3479074>

Chris ?ansen - May 14, 2013, 8:15 am

(May 14, 2013 08:13 AM)Mohatu Wrote: [\[CITE\]](#) Once again:
<https://hackforums.net/showthread.php?tid=3479074>Yea, I didn't see the post until after I posted my post...

Mohatu - May 14, 2013, 8:16 am

Could you change the title to reflect that BlooCoins are still secure?

-Max - May 14, 2013, 8:20 am

The server wasn't compromised. Bloocoin wasn't hacked, your stamp was.

Chris ?ansen - May 14, 2013, 8:22 am

(May 14, 2013 08:20 AM)Max00355 Wrote: [\[CITE\]](#) The server wasn't compromised. Bloocoin wasn't hacked, your stamp was. We figured this out. Just trying to get the word out now...

Atharva - May 14, 2013, 8:25 am

He stole 7 BLC of mine. Glad it wasn't alot of amount.
I was using a custom address.

The transactions were going to RyanC_stealing_your_bloocoins_here and some random numbers.

Rob. - May 14, 2013, 6:52 pm

Why don't you just go ask Max to reverse the transactions? ?
Or to change your passwords?

Volim te - May 14, 2013, 7:15 pm

Not like it was very secure in the 1st place, I mean come on kids it's controlled by a central server..

Mohatu - May 15, 2013, 12:48 am

(May 14, 2013 07:15 PM)Jebi se Wrote: [\[CITE\]](#) Not like it was very secure in the 1st place, I mean come on kids it's controlled by a central server..
Most of the world's money is centralized. That doesn't mean it's not secure. Do some research.

rather - May 15, 2013, 6:10 am

(May 15, 2013 12:48 AM)Mohatu Wrote: [\[CITE\]](#) Most of the world's money is centralized. That doesn't mean it's not secure. Do some research.

Now that right there is a massive informal fallacy. You're abusing the meaning of the word "centralized" to apply it to an entirely different situation, which is almost the exact opposite of the situation referred to earlier.

Basically, centralization refers to a system where there is one or many large central hubs. Like in real life there are banks, which aren't used because you have to use them to have money. They're used because it's convenient. Now, with banks there is alternatives. So if you don't like a certain bank, you can use another.

Now, with bloocoins this isn't possible. You're forced to use and trust the (currently two) central servers, both operated by Max.

(Now, we could peer into how stupid your statement about security is. But let's not go there)

See the difference? Whereas "centralized" can be used to describe both, it means quite the different things depending on context.