

Forum:[Hack Forums](#)

Thread: [How a Rogue Tor Node Hijacked Blockchain.info Accounts](#)

w34k - November 29, 2014, 6:51 am

Blockchain.info security concerns

You may have noticed [recent reports](#) about people having their bitcoins stolen from Blockchain.info. Many report that their accounts have been hacked into and their coins withdrawn. What caused the recent spike in account breaches at blockchain.info?

According to the blockchain PR account [blockchainwallet](#) on reddit, the top 3 issues concerning their security are:

- Malicious Tor exit nodes

- Weak password management

- Sophisticated phishing attacks

- Securing your coins

Having a strong password with many different characters is a no brainer and I hope most of you are using different passwords for different accounts. Phishing attacks can be avoided by accessing blockchain.info by typing it's address in the url bar in your browser. We reported [previously about a phishing site for blockchain.info](#) which appeared at the top of the front page on google because of a google adword campaign. That attack wasn't very successfull because redditors brought it to google's attention promptly and the phishing site got taken down.

Tor nodes perform MITM attack

Lastly, the most recent security issue which caused massive btc losses for customer funds was due to malicious Tor nodes. The attack was a simple and archaic MITM (man in the middle) attack. In simple terms the exit node does not know where the traffic originates from (the TOR user) but it can intercept the traffic if it is not encrypted. So, when someone accessed blockchain.info the rogue exit node would record the data being send and extract a victims wallet ID and the password. The catch here is that blockchain and many other sites that have the user send sensitive account information encrypt their traffic using SSL. So even if somebody was looking at the packets exchanged the information would be encrypted and the attacker would not be able to get the password.

[img]http://www.btcfeed.net/wp-content/uploads/2014/11/https-blockchain.png[/img]

Well, the rogue exit node was able to strip the SSL from blockchain.info. Those who noticed in the upper left corner would see that they are connecting to a http:// version of the site. When not using https:// protocol the information is not encrypted and thus you can fall victim to a MITM attack.

[img]http://www.btcfeed.net/wp-content/uploads/2014/11/blockchainhack.png[/img]

Now, if you try to connect to blockchain.info using tor you will get the above message. Blockchain has made a .onion mirror which ensure the integrity and encryption of traffic. Furthermore, it looks like they fixed a bug where you could connect to a SSL stripped version of the site, which is yet another preventative measure to a MITM vulnerability.

Blockchain.info uses something that is called [HSTS](#). What it does is force all your request to go through https if you ever accessed the site with https before. Now, when somebody accesses

blockchain by typing http:// then the HSTS header is not sent to force those https connections, and the tor browser bundle by default will not save the HSTS header either. That leaves rogue exit nodes free to start doing redirects. What blockchain could do is set a static page for any incoming http connection and tell the user to reconnect using https that way the HSTS header would be set and the user would end up accessing the site over a secure, encrypted connection.

Source : <http://btcfeed.net/news/rogue-tor-node-hijacked-blockchain-info-accounts>

Feel free to post your thoughts on this.

NiktoKan - November 29, 2014, 7:10 am

Is advisable to use offline wallet for big amount of BTC.

w34k - November 29, 2014, 7:52 am

(Nov 29, 2014 08:10 AM)NiktoKan Wrote: [\[CITE\]](#) Is advisable to use offline wallet for big amount of BTC.

Yeah, I don't trust online wallets.

Aceman - November 29, 2014, 10:11 am

Hm so basically as long as you were not on TOR, have a strong password, and aren't silly enough to fall for phishing attacks you should be fine. Is that correct? If so I'm going to continue to stick with blockchain.info since it offers the IP restriction and 2FA which I so love.

w34k - November 30, 2014, 1:49 am

(Nov 29, 2014 11:11 AM)Aceman Wrote: [\[CITE\]](#) Hm so basically as long as you were not on TOR, have a strong password, and aren't silly enough to fall for phishing attacks you should be fine. Is that correct? If so I'm going to continue to stick with blockchain.info since it offers the IP restriction and 2FA which I so love.

I believe this attack was only pertained to Tor users. There also has been a number of reports of blockchain users getting their accounts hacked. (Tor users and non-Tor users) even with strong password and 2FA. It could be by linking an email with their blockchain wallet, which isn't that smart and secure. Blockchain allowed users to login through a non-SSL webpage, what's that say about their security ?

All in all, I will never trust online wallets. It's really no big deal to keep them offline and more secure. Better safe than sorry, the choice is yours. Although there is a chance of getting infected with a RAT, which is a different story.

~Jay~ - November 30, 2014, 4:13 am

Tor was never the most secure proxy to use. People have known that for years.

~Jay~ - November 30, 2014, 4:14 am

Tor was never entirely secure, people have known that for years.

z0tpyrk - November 30, 2014, 4:50 am

(Nov 29, 2014 08:10 AM)NiktoKan Wrote: [\[CITE\]](#) Is advisable to use offline wallet for big amount of BTC.

Ofcourse offline wallets are better then online wallets who trust them is just dumb if you are using BTC with large transactions.

w34k - December 1, 2014, 5:39 am

(Nov 30, 2014 05:14 AM)Schizotypal Wrote: [\[CITE\]](#) Tor was never entirely secure, people have known that for years.Well, some people seem to choose "anonymity" over security and don't know

the risk. They just use it. Some also like to think things are impossible. One of the reasons for the share was to show the possibilities. If you're routing your traffic through Tor, a proxy/VPN, you set yourself up as a subject to some type of MiTM attack.

(Nov 30, 2014 05:50 AM)KryptozServices Wrote: [\[CITE\]](#) Ofcourse offline wallets are better then online wallets who trust them is just dumb if you are using BTC with large transactions.Right. They don't seem to listen. They want to start using offline wallets after their funds have been stolen. ?