

Forum:[Hack Forums](#)

Thread: [OMCWallet.com ??](#)

Invincible. - July 29, 2014, 1:49 pm

Why when I try to send OMC to my other wallet I get this:

Spoiler ([Click to View](#))

I just get a blank screen and nothing happens, sometimes I can send little amounts of 5 or 10 OMC, but I still got 2k OMC on there what I want to send to my Offline wallet...

Anyone?

Sacred Symmetry - July 29, 2014, 1:51 pm

Someone had this problem when they were trying to send me OMC last night. Give it a hour or so

Invincible. - July 29, 2014, 1:52 pm

(Jul 29, 2014 01:51 PM)Google Chrome™ Wrote: [\[CITE\]](#) Someone had this problem when they were trying to send me OMC last night. Give it a hour or so

It's been doing this for over 3 days man, I can't wait another hour, Luckily my good friend Ortek has helped me out and send some OMC to my offline wallet....

Abraham Lincoln - July 29, 2014, 2:08 pm

Not to raise false alarm, but when the other 2 online wallets got hacked they did the same thing.

It could be that the wallet daemon has just crashed though, I'll take a look.

EDIT: Nope, the daemon appears to be fine, it's showing balances / transactions. Still looking around for any possible cause other than hacking.

Invincible. - July 29, 2014, 2:15 pm

(Jul 29, 2014 02:08 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Not to raise false alarm, but when the other 2 online wallets got hacked they did the same thing.

It could be that the wallet daemon has just crashed though, I'll take a look.

EDIT: Nope, the daemon appears to be fine, it's showing balances / transactions. Still looking around for any possible cause other than hacking.

Alright, It's still sending small amounts of 5-10 OMC now and then....

Ortek - July 29, 2014, 2:20 pm

(Jul 29, 2014 02:08 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Not to raise false alarm, but when the other 2 online wallets got hacked they did the same thing.

It could be that the wallet daemon has just crashed though, I'll take a look.

EDIT: Nope, the daemon appears to be fine, it's showing balances / transactions. Still looking around for any possible cause other than hacking.

Thanks a lot for looking into this Abe.

Abraham Lincoln - July 29, 2014, 2:22 pm

Can anyone link me to some transactions that they sent into the wallet?

Invincible. - July 29, 2014, 2:24 pm

(Jul 29, 2014 02:22 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Can anyone link me to some transactions that they sent into the wallet?

This is a 5 OMC transaction that I sent from OMCWallet.com to my Offline Omniqoin-qt Wallet.

<https://omnicha.in/?transaction=19e50d206196a065b54487708b5d96cce230408375e4e61e28430922860b5221>

And when you look here: <https://omnicha.in/?search=oMYtvYNA7cNBNoYsiqqeU96qQC65eb5WrH>

That is my OMCWallet.com address it says I've send 2300 OMC, but I've actually only send small amounts of 5-10

Abraham Lincoln - July 29, 2014, 2:24 pm

Just sent some funds in and tried to pull them out and got the blank screen. From what I've seen I'd say it's been hacked using the same method as the other 2 wallets. Still looking into this.

(Jul 29, 2014 02:24 PM)Vanish. Wrote: [\[CITE\]](#) This is a 5 OMC transaction that I sent from OMCWallet.com to my Offline Omniqoin-qt Wallet.

<https://omnicha.in/?transaction=19e50d206196a065b54487708b5d96cce230408375e4e61e28430922860b5221>

Thanks, do you have any where you sent OMC into the online wallet from the offline wallet?

(Jul 29, 2014 02:24 PM)Vanish. Wrote: [\[CITE\]](#) This is a 5 OMC transaction that I sent from OMCWallet.com to my Offline Omniqoin-qt Wallet.

<https://omnicha.in/?transaction=19e50d206196a065b54487708b5d96cce230408375e4e61e28430922860b5221>

And when you look here: <https://omnicha.in/?search=oMYtvYNA7cNBNoYsiqqeU96qQC65eb5WrH>

That is my OMCWallet.com address it says I've send 2300 OMC, but I've actually only send small amounts of 5-10

That's normal for this type of online wallet.

Invincible. - July 29, 2014, 2:30 pm

(Jul 29, 2014 02:24 PM)Abraham Lincoln Wrote: [\[CITE\]](#)

Thanks, do you have any where you sent OMC into the online wallet from the offline wallet?
I've sent 5 OMC from my Offline wallet to the Online wallet, it's not yet showing up on the transactions.

Abraham Lincoln - July 29, 2014, 6:35 pm

It is definitely exploitable using the same method as the other wallets. I haven't tested it or exploited it, but from experience I'd say it is definitely possible.

I can't even withdraw 1 OMC from my account, I'd say it has all been stolen.

Doctor Blue - July 30, 2014, 5:59 am

(Jul 29, 2014 06:35 PM)Abraham Lincoln Wrote: [\[CITE\]](#) It is definitely exploitable using the same method as the other wallets. I haven't tested it or exploited it, but from experience I'd say it is definitely possible.

I can't even withdraw 1 OMC from my account, I'd say it has all been stolen.

I don't understand. Wasn't the bug in the other wallets that you could deposit 1 OMC and then withdraw more than you actually had? How can that possibly be hard to fix?

I'm confused.

Invincible. - July 30, 2014, 6:08 am

(Jul 30, 2014 05:59 AM)Doctor Blue Wrote: [\[CITE\]](#) I don't understand. Wasn't the bug in the other wallets that you could deposit 1 OMC and then withdraw more than you actually had? How can that possibly be hard to fix?

I'm confused.

I cant withdraw any OMC from the Online wallet....

Abraham Lincoln - July 30, 2014, 6:26 am

(Jul 30, 2014 05:59 AM)Doctor Blue Wrote: [\[CITE\]](#) I don't understand. Wasn't the bug in the other wallets that you could deposit 1 OMC and then withdraw more than you actually had? How can that possibly be hard to fix?

I'm confused.

The exploit is caused by the way the omnicoin wallet handles different accounts. Basically you link addresses with an account. When OMC is received from that address, it adds that to your account balance in the wallet. When sending OMC though the inputs used aren't from that address, they are from any input in the wallet. It's not the greatest way to do it, but it keeps the TX fees low.

It all works fine and dandy until a private key is leaked. Then that messes up the wallet. It assumes that only it has access to the private keys. Basically you deposit money into the online wallet, then withdraw it using the private key. The wallet doesn't count the withdrawal from the private key as a withdrawal from the account though and so your balance stays the same. Then you simply withdraw from the online wallet, rinse, and repeat. Basically doubling your OMC each time.

The other 2 wallets allowed exporting / importing of private keys, opening up a door to the exploit. OMCwallet didn't allow importing / exporting, but if you are clever there is a way to still get a private key.

Doctor Blue - July 30, 2014, 6:36 am

(Jul 30, 2014 06:26 AM)Abraham Lincoln Wrote: [\[CITE\]](#) The exploit is caused by the way the omnicoin wallet handles different accounts. Basically you link addresses with an account. When OMC is received from that address, it adds that to your account balance in the wallet. When sending OMC though the inputs used aren't from that address, they are from any input in the wallet. It's not the greatest way to do it, but it keeps the TX fees low.

It all works fine and dandy until a private key is leaked. Then that messes up the wallet. It assumes that only it has access to the private keys. Basically you deposit money into the online wallet, then withdraw it using the private key. The wallet doesn't count the withdrawal from the private key as a withdrawal from the account though and so your balance stays the same. Then you simply withdraw from the online wallet, rinse, and repeat. Basically doubling your OMC each time.

The other 2 wallets allowed exporting / importing of private keys, opening up a door to the exploit. OMCwallet didn't allow importing / exporting, but if you are clever there is a way to still get a private key.

Ah okay. Because with an online wallet planned, I'd need to be aware of this kind of things so I don't make the same mistake. I guess it can be quite tricky then, because you could tie the amount to an address, but the amounts sent to change addresses wouldn't appear in the online wallet (Major issue).

Abraham Lincoln - July 30, 2014, 6:56 am

Correct. Really the wallet should send the change back to the original address. Bitcoin does this, I have no idea why OMC doesn't.

If I where to make another online wallet I'd just write a custom wallet daemon to suit my needs.

Really all you have to be careful of is this:

Never ever ever ever let private keys be imported or exported.

Fees aren't taken into account when sending from an account. It will let you send the entire amount but then take a fee which will put the account negative. They must be manually handled.

Fees aren't always the same. I've seen them ranging from 0 to 0.01 OMC. And then can probably be bigger depending on the inputs.

CSFR protection needs to be on everything.

Doctor Blue - July 30, 2014, 7:36 am

(Jul 30, 2014 06:56 AM)Abraham Lincoln Wrote: [\[CITE\]](#) Correct. Really the wallet should send the change back to the original address. Bitcoin does this, I have no idea why OMC doesn't.

If I where to make another online wallet I'd just write a custom wallet daemon to suit my needs.

Really all you have to be careful of is this:

Never ever ever ever let private keys be imported or exported.

Fees aren't taken into account when sending from an account. It will let you send the entire amount but then take a fee which will put the account negative. They must be manually handled.

Fees aren't always the same. I've seen them ranging from 0 to 0.01 OMC. And then can probably be bigger depending on the inputs.

CSFR protection needs to be on everything.

CSRF protection is probably one of the more obvious things, wouldn't want anyone to be able to forge requests sending money from other users' wallets.

I'll keep the fees and private keys in mind, thank you for the advice :)

Aceman - July 30, 2014, 7:38 am

If I remember correctly this was created by a l33t member who hasn't been maintaining it. I believe I know how to recreate the exploit on this wallet but it's clearly already all been stolen which was only a matter of time. The creator wasn't maintaining it or even active in this section anymore to my knowledge.

Abraham Lincoln - July 30, 2014, 7:49 am

(Jul 30, 2014 07:38 AM)Aceman Wrote: [\[CITE\]](#) If I remember correctly this was created by a l33t member who hasn't been maintaining it. I believe I know how to recreate the exploit on this wallet but it's clearly already all been stolen which was only a matter of time. The creator wasn't maintaining it or even active in this section anymore to my knowledge.

Yea, [Boldheart](#).

He hasn't been on HF at all in 2 weeks. I just PMED him anyways.

And thread is here: <https://hackforums.net/showthread.php?tid=4234217>.

Only 10 posts.

.Matt - July 30, 2014, 10:50 am

Can someone give me a reason why this wallet was even being used in the first place?

Abe made me aware yesterday it's using the same script as a LTC scam wallet;

Owner doesn't have any credibility at all;

No updates or anything from the owner.

Pretty sure i warned about this when it was released. Oh well. Either it was exploited like the other

wallets or the owner just ran off.

Crypto™ - July 30, 2014, 11:05 am

(Jul 30, 2014 06:56 AM)Abraham Lincoln Wrote: [\[CITE\]](#) Correct. Really the wallet should send the change back to the original address. Bitcoin does this, I have no idea why OMC doesn't.

If I where to make another online wallet I'd just write a custom wallet daemon to suit my needs.

Really all you have to be careful of is this:

Never ever ever ever let private keys be imported or exported.

Fees aren't taken into account when sending from an account. It will let you send the entire amount but then take a fee which will put the account negative. They must be manually handled.

Fees aren't always the same. I've seen them ranging from 0 to 0.01 OMC. And then can probably be bigger depending on the inputs.

CSFR protection needs to be on everything.

I'll look into the change situation. Also, Doctor Blue, we should chat on this some in a bit. I'll let you know when I have my XMPP client redownloaded.

Doctor Blue - July 31, 2014, 1:18 pm

(Jul 30, 2014 11:05 AM)Crypto™ Wrote: [\[CITE\]](#) I'll look into the change situation. Also, Doctor Blue, we should chat on this some in a bit. I'll let you know when I have my XMPP client redownloaded.

I am waiting with anticipation and bated breath.

Who Soup - July 31, 2014, 6:18 pm

Thanks for looking into this Doctor Blue and Abe, I've been running into this trouble as well. Luckily I only have 26 OMC on it :Blackhat:

Syracusia - July 31, 2014, 6:20 pm

Blank page is often result of a php syntax error

Abraham Lincoln - July 31, 2014, 6:44 pm

(Jul 31, 2014 06:20 PM)Novaly Wrote: [\[CITE\]](#) Blank page is often result of a php syntax error
Yes, when sending and there isn't enough OMC in the wallet an error is thrown.

Knar. - August 2, 2014, 12:44 pm

(Jul 30, 2014 06:26 AM)Abraham Lincoln Wrote: [\[CITE\]](#) The exploit is caused by the way the omnicoins wallet handles different accounts. Basically you link addresses with an account. When OMC is received from that address, it adds that to your account balance in the wallet. When sending OMC though the inputs used aren't from that address, they are from any input in the wallet. It's not the greatest way to do it, but it keeps the TX fees low.

It all works fine and dandy until a private key is leaked. Then that messes up the wallet. It assumes that only it has access to the private keys. Basically you deposit money into the online wallet, then withdraw it using the private key. The wallet doesn't count the withdrawal from the private key as a withdrawal from the account though and so your balance stays the same. Then you simply withdraw from the online wallet, rinse, and repeat. Basically doubling your OMC each time.

The other 2 wallets allowed exporting / importing of private keys, opening up a door to the exploit. OMCwallet didn't allow importing / exporting, but if you are clever there is a way to still get a private key.

Thanks for explaining that. It's nice to know the mistake I made. This is the reason I initially didn't think it was hacked, because all of the balances were still there.

Shouldn't have released a wallet with such little knowledge on crypto's.

xploD - August 7, 2014, 5:42 am

The site was working for me, for the last 3-4 days. Sending OMC amounts in the thousands. Now today its stopped working. Saw a post that its been hacked.

.Matt - August 7, 2014, 6:11 am

(Aug 7, 2014 05:42 AM)xploD Wrote: [\[CITE\]](#) The site was working for me, for the last 3-4 days. Sending OMC amounts in the thousands. Now today its stopped working. Saw a post that its been hacked.

It only worked for you due to you adding the omc and then taking it out. The reason it didn't work for others was due to it not having any balance.

(Aug 7, 2014 05:42 AM)xploD Wrote: [\[CITE\]](#) The site was working for me, for the last 3-4 days. Sending OMC amounts in the thousands. Now today its stopped working. Saw a post that its been hacked.

It only worked for you due to you adding the omc and then taking it out. The reason it didn't work for others was due to it not having any balance.

Abraham Lincoln - August 18, 2014, 10:33 pm

Looks like the hosting finally ran out on this. Finally something to stop people from using it.

Aceman - August 19, 2014, 9:20 am

(Aug 18, 2014 10:33 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Looks like the hosting finally ran out on this. Finally something to stop people from using it.

I'm really glad to hear that. Too many people who don't regularly check this section were using that as a wallet and subsequently losing their coins because of it.

Abraham Lincoln - August 19, 2014, 11:17 am

The only problem is people will keep sending OMC there until they try to access it and realize they can't. Even on the omnichain.ini wallet there weren't a whole ton of users but I still get received transactions here and there.

Aceman - August 19, 2014, 1:29 pm

(Aug 19, 2014 11:17 AM)Abraham Lincoln Wrote: [\[CITE\]](#) The only problem is people will keep sending OMC there until they try to access it and realize they can't. Even on the omnichain.ini wallet there weren't a whole ton of users but I still get received transactions here and there.

That's their own fault. It's the price they pay for being careless with a currency.

frutk - August 20, 2014, 11:03 pm

And now what? All are omnicoins are gone? I had 50\$ worth OMC on that wallet?:(Is someone gonna pay us back?

Obli - August 20, 2014, 11:05 pm

(Aug 20, 2014 11:03 PM)frutk Wrote: [\[CITE\]](#) And now what? All are omnicoins are gone? I had 50\$ worth OMC on that wallet?:(Is someone gonna pay us back?

All OMCs are gone, the owner of the wallet must have taken them.

I'm afraid not.

frutk - August 20, 2014, 11:07 pm

(Aug 20, 2014 11:05 PM)+Oblivious Wrote: [\[CITE\]](#) All OMCs are gone, the owner of the wallet must have taken them.

I'm afraid not.

Holy freaking shit.

That is the only money I had for the moment :O
This is not happening

Aceman - August 21, 2014, 7:24 am

(Aug 20, 2014 11:05 PM)+Oblivious Wrote: [\[CITE\]](#) All OMCs are gone, the owner of the wallet must have taken them.

I'm afraid not.

The owner of the wallet hasn't been on for quite some time if I remember correctly. He took open source code and implemented it for OMC and then never really checked back. To my knowledge the wallet was working correctly until it was exploited and even then, it worked when there was a balance. I imagine the owner may not even be aware of how much OMC he could be holding and could have 10k OMC on a rented VPS for all we know.