

Forum:[Hack Forums](#)

Thread: [Allcrypt disabled Omnicoin \(temporarily?\)](#)

Raoul Duke - February 10, 2015, 10:30 am

30 min before I post this thread I saw a lot of omnicoin transactions on Allcrypt (more than usual). Quickly after, Allcrypt went down for maintenance.

The site is now back up online and every crypto-currency market are alive except omnicoin...

Spoiler ([Click to View](#))

I hope our coins are safe and the market to be back online soon ...

FRANKIE - February 10, 2015, 10:32 am

Hopefully everything goes back to normal soon.

So many people were in panic earlier because they thought Allcrypt pulled an MT Gox

SwiftBot - February 10, 2015, 10:33 am

Seems alive now. ? Is it still down.

Raoul Duke - February 10, 2015, 10:34 am

They fact is every market are alive except OMC... So I'm just wondering myself why?

EDIT:

extra_sauce - February 10, 2015, 10:49 am

Someone fucked the profits for everyone with that 600k listing...

Ombra - February 10, 2015, 10:51 am

I wonder how much concrete is the scenario in which they were hacked in order to steal our OMC.

Raoul Duke - February 10, 2015, 10:51 am

(Feb 10, 2015 11:49 AM)Raidingbuffalo Wrote: [\[CITE\]](#) Someone fucked the profits for everyone with that 600k listing...

The problem come from what happend before that order but I haven't think of making a screenshot...

extra_sauce - February 10, 2015, 10:54 am

(Feb 10, 2015 11:51 AM)Raoul Duke Wrote: [\[CITE\]](#) The problem come from what happend before that order but I haven't think of making a screenshot...

What happened before this? It just really sucks having these people holding a MAJOR percentage of the entire blockchain.

Raoul Duke - February 10, 2015, 10:55 am

(Feb 10, 2015 11:51 AM)Ombra Wrote: [\[CITE\]](#) I wonder how much concrete is the scenario in which they were hacked in order to steal our OMC.

An user from here have found some vulnerabilities in Allcrypt multiple times but never used them... If one person can find a vuln a lot of other people can too...

But for now we don't know what happend it's just a thread to inform you, so wait and see...

Adium - February 10, 2015, 10:56 am

(Feb 10, 2015 11:54 AM)Raidingbuffalo Wrote: [\[CITE\]](#) What happened before this? It just really sucks having these people holding a MAJOR percentage of the entire blockchain.

So people with more money invested than you shouldn't be able to sell? You wouldn't be so annoyed if someone bought up 600k OMC raising the price.....

Raoul Duke - February 10, 2015, 11:01 am

600k OMC may be a bad thing for the coin or maybe not... But it should'nt take Allcrypt down !

Aceman - February 10, 2015, 11:04 am

They're updating their wallet in anticipation for the change to DGW. Crypto let them know ahead of time that it would be necessary for them to do so and that's the reason why the wallet is currently down.

Abraham Lincoln - February 10, 2015, 11:04 am

(Feb 10, 2015 12:04 PM)Aceman Wrote: [\[CITE\]](#) They're updating their wallet in anticipation for the change to DGW. Crypto let them know ahead of time that it would be necessary for them to do so and that's the reason why the wallet is currently down.

I'm pretty sure they upgraded their wallet a few days ago. And a simple upgrade shouldn't take down the entire site.

Raoul Duke - February 10, 2015, 11:10 am

(Feb 6, 2015 01:01 PM)Crypto™ Wrote: [\[CITE\]](#) I've already contacted both AllCrypt and CoinPayments, and they've both updated their wallets, so you're good.

If I understand right it was done a few days ago

extra_sauce - February 10, 2015, 11:14 am

(Feb 10, 2015 11:56 AM)BrokenGlass Wrote: [\[CITE\]](#) So people with more money invested than you shouldn't be able to sell? You wouldn't be so annoyed if someone bought up 600k OMC raising the price.....

Not when this can, and will cause OMC to crash...

Aceman - February 10, 2015, 11:15 am

(Feb 10, 2015 12:04 PM)Abraham Lincoln Wrote: [\[CITE\]](#) I'm pretty sure they upgraded their wallet a few days ago. And a simple upgrade shouldn't take down the entire site.It's AllCrypt, anytime they have a wallet issue it's down for several hours. From what I understand they don't have a lot of staff so they'll pretty much just let the wallet sync and come back several hours later to see if it's done.

Abraham Lincoln - February 10, 2015, 11:15 am

That's strange, even though the market is disabled someone is still apparently putting in orders:

Spoiler [\(Click to View\)](#)

That wasn't there earlier

Aceman - February 10, 2015, 11:18 am

(Feb 10, 2015 12:15 PM)Abraham Lincoln Wrote: [\[CITE\]](#) That's strange, even though the market is disabled someone is still apparently putting in orders:

Spoiler [\(Click to View\)](#)

That wasn't there earlier You're right, I did notice that but I didn't think anything of it.

allcrypt - February 10, 2015, 11:59 am

I was going to ask a dev to contact us, but since a thread is here I'll be open about what happened, but start with a question:

Is OMC secure? Whats the hashrate? And has someone gotten to 51%?

A quasi-anonymous user with a bullshit username accessing the site through a rental server from a host known for spamming and hacking somehow made about 3 million OMC worth of deposits to AllCrypt, and then, by a method I've no clue how, invalidated all the blocks. It wasn't a double spend - the entire block that the transactions appeared in are invalid.

Best part - this happened after the required 6 confirmations. AllCrypt validates the blocks of deposits with every new block, until 6 are made. We actually constantly re-validate the blocks. After the 6 confirmations, somehow, the block got trashed. Over the course of 8 deposits totaling almost 3 million OMC.

A ton of it was sold off, and the user withdrew at least 2 BTC from the sales. We were alerted to the issue when the wallet started throwing Insufficient Funds errors on a 200k OMC withdrawal.

So. One you, and I'm sure since OMC is the currency of hackforums, and not many other people care about it's existence, that the culprit will be reading this, stole 3 million OMC from the rest of you.

Any dev here on the site who has access to IP address logs I'd be happy to share my info with you. Jackass who stole the coins: You had an anonymous account. Our anonymous accounts don't store logs so that in the case we are subpoenaed, we have no logs to provide. Nowhere does it say I cannot find your IP address. Happy to share. Like I said, I'm sure they logged in here at some point.

So for now, the OMC wallet is on lockdown. Because I've no idea if they can do it again. After someone in charge of the wallet software contacts me and we discuss options and we figure it out, I'll get the wallet back up.

As it stands now though, our audit software reports we are short about 2.5 million OMC, and there is about 13k left in the wallet.

One of your compadres stole all your OMC.

For anyone who wants to do detective work, the withdrawals of OMC went to:
ofquhkd2UbzqL7QgbzzYghcQwm9KYAc5WT
oQNwHSamQTJi7bVfaz8hUoBLYadu93bRyF

BTC withdrawals went to:
1AYktdZUZSHrGqZZtfHDtvjfh4Vij1VbY

A member of the dev team or hackforums administration can contact me either through a support ticket at support.allcrypt.com, or directly at contact@allcrypt.com

Signing this message with our public BTC address for authenticity. Everything from the top of the message to the end of this line, not including the dashed break below.

Signing address: 1GsWDfEfLv3JkUUDXugmkZhB3jWWT2ytYU (verifiable on blockchain.info and in the footer of AllCrypt.com)

Signing key:

H0zzuFs4nZjA3K4UeRIKWQN5iSLI75WpRlZQinXZ2jb63nfAFSHmhNNIHUkiCgagnTq3UftQ6BkjPhCw16mwHI4=

Made this account to post this, likely won't follow the thread.

(Feb 10, 2015 12:18 PM)Aceman Wrote: [\[CITE\]](#) You're right, I did notice that but I didn't think anything of it.

That MIGHT be possible if the user had the screen open and never refreshed before clicking the button to submit the order. I'll have to doublecheck our error checking on that.

(Feb 10, 2015 12:15 PM)Aceman Wrote: [\[CITE\]](#) It's AllCrypt, anytime they have a wallet issue it's down for several hours. From what I understand they don't have a lot of staff so they'll pretty much just let the wallet sync and come back several hours later to see if it's done.

We haven't touched the wallet in months. To be sure we didn't miss an upgrade and fork, I even checked the sources today. It's the same version as it's been for months now.

(Feb 10, 2015 12:04 PM)Aceman Wrote: [\[CITE\]](#) They're updating their wallet in anticipation for the change to DGW. Crypto let them know ahead of time that it would be necessary for them to do so and that's the reason why the wallet is currently down.

We have no record of anyone contacting us to upgrade OMC. And even if we had, the git sources haven't been updated. Or if they HAVE, no one changed version numbers, so our system assumes nothing is different. We don't bother going through an upgrade if it's the same version as the last one.

.Matt - February 10, 2015, 12:40 pm

I really hope allcrypt has insurance as i personally lost 40k ~ 1.5 BTC.

bandors - February 10, 2015, 12:51 pm

(Feb 10, 2015 12:59 PM)allcrypt Wrote: [\[CITE\]](#) I was going to ask a dev to contact us, but since a thread is here I'll be open about what happened, but start with a question:

Is OMC secure? Whats the hashrate? And has someone gotten to 51%?

A quasi-anonymous user with a bullshit username accessing the site through a rental server from a host known for spamming and hacking somehow made about 3 million OMC worth of deposits to AllCrypt, and then, by a method I've no clue how, invalidated all the blocks. It wasn't a double spend - the entire block that the transactions appeared in are invalid.

Best part - this happened after the required 6 confirmations. AllCrypt validates the blocks of deposits with every new block, until 6 are made. We actually constantly re-validate the blocks. After the 6 confirmations, somehow, the block got trashed. Over the course of 8 deposits totaling almost 3 million OMC.

A ton of it was sold off, and the user withdrew at least 2 BTC from the sales. We were alerted to the issue when the wallet started throwing Insufficient Funds errors on a 200k OMC withdrawal.

So. One you, and I'm sure since OMC is the currency of hackforums, and not many other people care about it's existence, that the culprit will be reading this, stole 3 million OMC from the rest of you.

Any dev here on the site who has access to IP address logs I'd be happy to share my info with you. Jackass who stole the coins: You had an anonymous account. Our anonymous accounts don't store

logs so that in the case we are subpoenaed, we have no logs to provide. Nowhere does it say I cannot find your IP address. Happy to share. Like I said, I'm sure they logged in here at some point.

So for now, the OMC wallet is on lockdown. Because I've no idea if they can do it again. After someone in charge of the wallet software contacts me and we discuss options and we figure it out, I'll get the wallet back up.

As it stands now though, our audit software reports we are short about 2.5 million OMC, and there is about 13k left in the wallet.

One of your compadres stole all your OMC.

For anyone who wants to do detective work, the withdrawals of OMC went to:
ofquhkd2UbzqL7QgbzzYghcQwm9KYAc5WT
oQNwHSamQTJi7bVfaz8hUoBLYadu93bRyF

BTC withdrawals went to:
1AYktdZUZSHrGqZZtfHDTvjyfh4Vij1VbY

A member of the dev team or hackforums administration can contact me either through a support ticket at support.allcrypt.com, or directly at contact@allcrypt.com

Signing this message with our public BTC address for authenticity. Everything from the top of the message to the end of this line, not including the dashed break below.

Signing address: 1GsWDFeFLv3JkUUDXugmkZhB3jWWT2ytYU (verifiable on blockchain.info and in the footer of AllCrypt.com)

Signing key:
H0zzuFs4nZjA3K4UeRIKWQN5iSLI75WpRlZQinXZ2jb63nfAFSHmhNNIHUkiCgagnTq3UftQ6BkjPh
Cw16mwhI4=

Made this account to post this, likely won't follow the thread.

That MIGHT be possible if the user had the screen open and never refreshed before clicking the button to submit the order. I'll have to doublecheck our error checking on that.

We haven't touched the wallet in months. To be sure we didn't miss an upgrade and fork, I even checked the sources today. It's the same version as it's been for months now.

We have no record of anyone contacting us to upgrade OMC. And even if we had, the git sources haven't been updated. Or if they HAVE, no one changed version numbers, so our system assumes nothing is different. We don't bother going through an upgrade if it's the same version as the last one.

So all of our OMC funds are gone? Fuck me with a rake :|

Krew - February 10, 2015, 12:53 pm

WHAT THE FUCK. First time in my life I put a crypto on an online wallet and this shit happens. ffs

Indecisive enough - February 10, 2015, 12:59 pm

Damn things just for real, sad to see something like this happen.

Hydra - February 10, 2015, 1:10 pm

What actions can AllCrypt take, does anyone know if they have some type of insurance to

compensate for the damages?

Dean Winchester? - February 10, 2015, 1:10 pm

(Feb 10, 2015 01:59 PM)indecisveenough Wrote: [\[CITE\]](#) Damn things just for real, sad to see something like this happen.

"Sad to see something like this happen"?

This didn't just happen, a member of Hackforums actually did this (on purpose), quite possibly just to destroy OMC.

It is sad to see that we actually have psychopaths roaming around the forums that literally don't give a shit about anyone but themselves.

Indecisive enough - February 10, 2015, 1:13 pm

(Feb 10, 2015 02:10 PM)Dean Winchester? Wrote: [\[CITE\]](#) "Sad to see something like this happen"?

This didn't just happen, a member of Hackforums actually did this (on purpose), quite possibly just to destroy OMC.

It is sad to see that we actually have psychopaths roaming around the forums that literally don't give a shit about anyone but themselves.

Welcome to Hackforums, A shit load of people are here. Its no surprise we have psychopaths here.

Zettabit - February 10, 2015, 1:18 pm

Oh fuck me in the ass... Looks like I just lost all of my OMC...

Nickelodeon - February 10, 2015, 1:19 pm

There will be no insurance as far as I can see, since it clearly says: "AllCrypt.com is not responsible for losses or trade delays caused by network volatility, outages, or market conditions."

Rolls Royce Cars - February 10, 2015, 1:21 pm

Still have my coins but it says it's disabled, does this mean I lost my coins?

Abraham Lincoln - February 10, 2015, 1:21 pm

(Feb 10, 2015 02:21 PM)Bigbos Wrote: [\[CITE\]](#) Still have my coins but it says it's disabled, does this mean I lost my coins?

Yes, your account balance is still there, but they don't have any OMC to fulfill your account balance.

Canada - February 10, 2015, 1:31 pm

This is why I cash out my coins as soon as I get them. Condolences to those who lost their OMC. ;/

Rolls Royce Cars - February 10, 2015, 1:34 pm

(Feb 10, 2015 02:21 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Yes, your account balance is still there, but they don't have any OMC to fulfill your account balance.

Shit that sucks... So if allcrypt can't pay it back there are 2 million less OMC in circulation and a lot of people lost their money?

James Brown - February 10, 2015, 1:34 pm

More than likely there will be a rollback as with Vericoins Mintpal incident, the 2 stolen BTC isn't that big a deal but can't have a thief walking around with millions of OMC waiting to dump them

BLURRYF?CE - February 10, 2015, 1:41 pm

(Feb 10, 2015 02:34 PM)James Brown Wrote: [\[CITE\]](#) More than likely there will be a rollback as with

Vericoin Mintpal incident, the 2 stolen BTC isn't that big a deal but can't have a thief walking around with millions of OMC waiting to dump them True, but keep in mind pretty much the only person who can fund such a rollback, is the main investor in OMC, Omniscient. I wonder what long-term issues that missing 2.5 million OMC might cause, that's what I'm ultimately more worried about.

afk0 - February 10, 2015, 1:42 pm

Selling 2.5 million Omnicoin, hmu thanks.

Spoiler ([Click to View](#)) Just kidding.

typhoid - February 10, 2015, 1:51 pm

what if the guy tries to use the stolen omnicoin to buy the group?

Moon Rock - February 10, 2015, 1:51 pm

Wow, sucks for you guys that kept your OMC in trust of Allcrypt. So who the hell are we going to use now for an exchange site?

bandors - February 10, 2015, 1:55 pm

(Feb 10, 2015 02:51 PM)typhoid Wrote: [\[CITE\]](#) what if the guy tries to use the stolen omnicoin to buy the group?

That's obviously what it's going to be used for. It'll probably just be laundered and then used.

Abraham Lincoln - February 10, 2015, 1:56 pm

(Feb 10, 2015 02:55 PM)Bandors Wrote: [\[CITE\]](#) That's obviously what it's going to be used for. It'll probably just be laundered and then used.

It's pretty much impossible to launder. There isn't much other OMC out there to launder it with.

James Brown - February 10, 2015, 1:59 pm

(Feb 10, 2015 02:41 PM)vurezo Wrote: [\[CITE\]](#) True, but keep in mind pretty much the only person who can fund such a rollback, is the main investor in OMC, Omniscient. I wonder what long-term issues that missing 2.5 million OMC might cause, that's what I'm ultimately more worried about. Its nothing to do with Omni, a roll back means the theft and all subsequent transactions are wiped out as those blocks don't exist any longer. Means a few people who purchased or mined coins after the theft getting fucked over and having to go after allcrypt or whoever's fault this turns out to be but I don't see another way the currency can survive. 2.5m coins is half the coins in circulation not counting omni's wallet.

Zettabit - February 10, 2015, 2:03 pm

(Feb 10, 2015 02:51 PM)typhoid Wrote: [\[CITE\]](#) what if the guy tries to use the stolen omnicoin to buy the group?

It would be pretty obvious if he starts throwing out random and high ass numbers. BUT, the real question is, how do we know he's not giving somebody else the coins to buy it?

Nature - February 10, 2015, 2:03 pm

(Feb 10, 2015 02:51 PM)typhoid Wrote: [\[CITE\]](#) what if the guy tries to use the stolen omnicoin to buy the group?

Since allcrypt posted the addresses they sent the OMC to. You should be able to trace them.

BLURRYF?CE - February 10, 2015, 2:04 pm

(Feb 10, 2015 02:59 PM)James Brown Wrote: [\[CITE\]](#) Its nothing to do with Omni, a roll back means the theft and all subsequent transactions are wiped out as those blocks don't exist any longer. Means a few people who purchased or mined coins after the theft getting fucked over and having to

go after allcrypt or whoever's fault this turns out to be but I don't see another way the currency can survive. 2.5m coins is half the coins in circulation not counting omni's wallet. If they roll back there's still ~2.5m coins missing, and people still wouldn't be able to withdrawal, well, not anymore than the measle 13K OMC that was left behind.

.Matt - February 10, 2015, 2:06 pm

(Feb 10, 2015 03:04 PM)vurezo Wrote: [\[CITE\]](#) If they roll back there's still ~2.5m coins missing, and people still wouldn't be able to withdrawal, well, not anymore than the measle 12K OMC that was left behind.

If they roll back to 12PM yesterday then there will be no problems.

Jeff Jordan - February 10, 2015, 2:07 pm

Aaaaaand, the OMC price just got fucked. Smh.

BLURRYF?CE - February 10, 2015, 2:11 pm

(Feb 10, 2015 03:06 PM).Matt Wrote: [\[CITE\]](#) If they roll back to 12PM yesterday then there will be no problems. How would there be no problems? If they roll back all the coins are still missing, unless you suppose we should all share the measle 13K OMC that's left behind?

Aceman - February 10, 2015, 2:12 pm

We're a community coin and we're the only ones really impacted by it. That means doing a rollback which is in the best interest of the community is in the best interest of the coin. It's something I definitely support and hope we'll do unless the culprit were to come forward (Imfao).

crossera - February 10, 2015, 2:12 pm

(Feb 10, 2015 02:51 PM)typhoid Wrote: [\[CITE\]](#) what if the guy tries to use the stolen omnicoin to buy the group?

inb4 Omni taking the coins and banning him ?

BLURRYF?CE - February 10, 2015, 2:15 pm

(Feb 10, 2015 03:12 PM)Aceman Wrote: [\[CITE\]](#) We're a community coin and we're the only ones really impacted by it. That means doing a rollback which is in the best interest of the community is in the best interest of the coin. It's something I definitely support and hope we'll do unless the culprit were to come forward (Imfao). Wait, is there actually some way to forcefully rollback OMC altogether?

extra_sauce - February 10, 2015, 2:17 pm

(Feb 10, 2015 02:19 PM)Nickelodeon Wrote: [\[CITE\]](#) There will be no insurance as far as I can see, since it clearly says: "AllCrypt.com is not responsible for losses or trade delays caused by network volatility, outages, or market conditions."

Would security flaws, on their part, constitute as any of those though?

Abraham Lincoln - February 10, 2015, 2:20 pm

(Feb 10, 2015 03:11 PM)vurezo Wrote: [\[CITE\]](#) How would there be no problems? If they roll back all the coins are still missing, unless you suppose we should all share the measle 13K OMC that's left behind?

If we roll back everything goes back to how it was. So the coins go back to where they were.

(Feb 10, 2015 03:15 PM)vurezo Wrote: [\[CITE\]](#) Wait, is there actually some way to forcefully rollback OMC altogether?

Yes, there is.

BLURRYF?CE - February 10, 2015, 2:22 pm

(Feb 10, 2015 03:20 PM)Abraham Lincoln Wrote: [\[CITE\]](#) If we roll back everything goes back to how it was. So the coins go back to where they where.

Yes, there is.Okay, that would be lovely. The question in my mind is if this perhaps was a 51% attack or something of such sorts. Considering how "low" the hashrate can be at times, it shouldn't be all that to perform such an attack.

mti1993 - February 10, 2015, 2:23 pm

(Feb 10, 2015 03:20 PM)Abraham Lincoln Wrote: [\[CITE\]](#) If we roll back everything goes back to how it was. So the coins go back to where they where.

Yes, there is.

but we MUST move to another exchange site which is more secure

I remember that you too have found a bug before and you reported it

If I get my coins back I won't risk keeping it on Allcrypt

James Brown - February 10, 2015, 2:24 pm

(Feb 10, 2015 03:04 PM)vurezo Wrote: [\[CITE\]](#) If they roll back there's still ~2.5m coins missing, and people still wouldn't be able to withdrawal, well, not anymore than the measle 13K OMC that was left behind.No you aren't understanding, a rollback basically means forking the blockchain back to the state it was in before the theft, those 2.5m coins go back to wherever they were before the theft. The thief ends up with nothing but the 2 BTC he managed to withdraw.

Raoul Duke - February 10, 2015, 2:24 pm

If there is a rollback some people will loose money but without a rollback a theft like this one will mean the end of that currency and everybody will loose a lot more...

I hope the OMC team and Omniscient will make the good decision about this.

Abraham Lincoln - February 10, 2015, 2:27 pm

(Feb 10, 2015 03:22 PM)vurezo Wrote: [\[CITE\]](#) Okay, that would be lovely. The question in my mind is if this perhaps was a 51% attack or something of such sorts. Considering how "low" the hashrate can be at times, it shouldn't be all that to perform such an attack.

No, it's not terrible difficult. This isn't a whole lot that can be done about this on such a small network. The only thing that can help prevent it is the payment processors increasing the amount of required confirmations.

But in the end nothing can stop a 51% attack.

(Feb 10, 2015 03:23 PM)mti1993 Wrote: [\[CITE\]](#) but we MUST move to another exchange site which is more secure

I remember that you too have found a bug before and you reported it

If I get my coins back I won't risk keeping it on Allcrypt

This will be addressed in due time. We'll make sure that there is still a safe place to trade.

BLURRYF?CE - February 10, 2015, 2:28 pm

(Feb 10, 2015 03:27 PM)Abraham Lincoln Wrote: [\[CITE\]](#) No, it's not terrible difficult. This isn't a whole lot that can be done about this on such a small network. The only thing that can help prevent it is the payment processors increasing the amount of required confirmations.

But in the end nothing can stop a 51% attack.

This will be addressed in due time. We'll make sure that there is still a safe place to trade.That's

what I thought... :/

Anyhow, can't wait for the rollback! ?

Abraham Lincoln - February 10, 2015, 2:29 pm

(Feb 10, 2015 03:25 PM)vurezo Wrote: [\[CITE\]](#) I see, sorry misunderstood!

Anyhow, is this "attack" repeatable? Is it an Allcrypt weakness or is it i.e. 51% attack or such? Yes, it is repeatable. No, it's not a weakness in AllCrypt necessarily, except that they had no system to monitor for these types of attacks and mitigate them.

Nothing can stop a 51% attack. You can make it very difficulty, but it's always possible.

Adium - February 10, 2015, 2:34 pm

(Feb 10, 2015 03:24 PM)James Brown Wrote: [\[CITE\]](#) No you aren't understanding, a rollback basically means forking the blockchain back to the state it was in before the theft, those 2.5m coins go back to wherever they were before the theft. The thief ends up with nothing but the 2 BTC he managed to withdraw.

No I think you are misunderstanding, a cryptocurrency rollback is where you delete all the blocks mined in a certain date range so those coins no longer exist.

At least that's what I understood it to be.

James Brown - February 10, 2015, 2:36 pm

(Feb 10, 2015 03:34 PM)BrokenGlass Wrote: [\[CITE\]](#) No I think you are misunderstanding, a cryptocurrency rollback is where you delete all the blocks mined in a certain date range so those coins no longer exist.

At least that's what I understood it to be. The coins that were in existence (including the 2.5m) up until the roll back still exist, the ones mined since yesterday or wherever they decide to roll back to don't exist.

Adium - February 10, 2015, 2:40 pm

(Feb 10, 2015 03:36 PM)James Brown Wrote: [\[CITE\]](#) The coins that were in existence (including the 2.5m) up until the roll back still exist, the ones mined since yesterday or wherever they decide to roll back to don't exist.

Ohhh, that's pretty cool. In that case there's not too much harm done then, obviously there's a bit of financial lost but nothing catastrophic.

I thought whatever happened the 2.5m omc would be gone forever.

?lixir - February 10, 2015, 2:42 pm

Damn, this is a crazy way to get the blackhat award and a group.

BLURRYF?CE - February 10, 2015, 2:46 pm

(Feb 10, 2015 03:42 PM)?lixir Wrote: [\[CITE\]](#) Damn, this is a crazy way to get the blackhat award and a group. No, it's a crazy way to get repfucked and closed...

Adium - February 10, 2015, 2:47 pm

(Feb 10, 2015 03:42 PM)?lixir Wrote: [\[CITE\]](#) Damn, this is a crazy way to get the blackhat award and a group.

I'm pretty certain Omni wouldn't award the hacker, he had quite a vested interest in the cryptocurrency named after him, this hack has brought his personal stock value down a lot.

Mix - February 10, 2015, 2:47 pm

<https://hackforums.net/showthread.php?tid=4679983>

Omni's posted why this has happen

Eagerkid - February 10, 2015, 6:44 pm

I am confused as to what actually happened.

allcrypt - February 10, 2015, 7:47 pm

Ok, so after hearing from the dev and hearing what happened, I figured I'd come back and read the thread.

Time to clear up a few things:

Like Omni posted in the other thread, we believe it was a 51% attack. When I say "we" I mean that thats what I've been told they think it is, and it's what I know it is, as there is NO other way to make what happened, happen.

The only security that AllCrypt could have, since we were blamed for a gamut of things in this thread, would be to increase the required number of confirmations to a few hundred, so that the hacker gets bored and walks away. That also means that any time you deposit OMC, you need to wait a few days to use it, or not be able to make any withdrawals for a few days. Which shitty option do you prefer?

RDD was attacked like this, and Cryptsy upped the required confirmations to 999. I personally had some RDD and since I feel it's in bad form to trade on my own site, I sent it to Cryptsy. Who does NOT allow you to use unconfirmed deposits. And it was about 2-3 days later I had my coins available.

As for losing faith in AllCrypt, that is akin to you never buying a Chevrolet vehicle again because someone fired a rocket at your car, and now it doesn't run anymore. Obviously shitty Chevy engineering.

And yes, I'm a bit bristly. Site got attacked today, then I come here and see all sorts of blame with no one knowing the story. Hell, I said what happened in my post on page 2. The deposits fully confirmed, then LATER, the blocks were invalidated. We have no control over your blockchain.

Ok, so now that I'm done my childish rant, some details.

The total amount WITHDRAWN from AllCrypt was just over 2 million OMC. 2.075 I believe.

1.98 BTC worth was sold and withdrawn.

Another 500k was up for sale. That order was removed and the phantom coins nuked. Leaving us at -2mil and change. 13k is still in the wallet.

Good news - I believe there is talk about a rollback. That means the thief loses everything he withdrew, and we get OMC back.

Possible bad news: Anyone who bought OMC from him, until we do the math I'm not sure what happens. The BTC is gone. Withdrawn. If the rollback restores our balance, and I believe it should (we've never had to do one before, so, this is new to us), you should still have the OMC you bought. Maybe. Not sure, since you bought OMC that didn't exist. Though if we can time the rollback

correctly, we may be able to "steal" back some of the original coins the thief deposited. Gotta talk to the dev team.

I have other details, but don't want to share too much as I'm sure the asshole is reading this too.
waves

Zettabit - February 10, 2015, 7:52 pm

(Feb 10, 2015 08:47 PM)allcrypt Wrote: [\[CITE\]](#) -snip-

Well hopefully the rollback will clear shit up, cause this was a pretty serious hit. Thanks for clearing shit up, and now hopefully people will understand.

Omniscient - February 10, 2015, 10:53 pm

End result is that this is going to get resolved. It's not important to place blame or get emotional. Figure out the problem, resolve it, and we all get to go about our normal routine again. Everything else is just drama we don't need.

Thanks.