

Bitcoin Client - Transaction Fee Attack

Original: 23 Aug 2012
Last edited: 24 Aug 2012

Summary:

Malicious changes to the Satoshi client transaction fee setting can cause users to lose their entire wallet balance. This change is trivial to achieve and requires no special knowledge or computational resources.

Scope:

This attack has been tested and confirmed on:

- the Windows bitcoin-qt client

This attack may be applicable to:

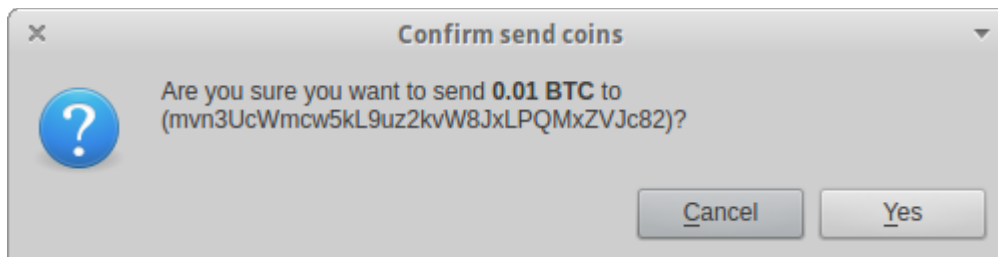
- any of the Satoshi clients, including the daemon clients

This attack does not consider but may also apply to:

- any non-Satoshi client, eg Armory
- thin clients, eg Electrum

Attack Scenario:

- Alice is a regular windows user and somehow manages to obtain a program which contains this particular attack.
- When this program is run, it (unknown to her) alters her bitcoin client settings to have a transaction fee of 50 bitcoin (BTC).
- Alice opens her bitcoin client to send some coins. She has 51 BTC in her wallet.
- Alice sends 0.01 BTC to her friend.
- The alert message asks her to confirm the transaction of 0.01 BTC, which does not show any mention of the malicious transaction fee. (see image below)
- She clicks OK.
- She finds that her balance is now 0.99 BTC and doesn't understand why.
- 50 BTC of her 51 BTC has been sent to to the network as miner fees.



Attack Method:

The value for the amount to pay as a transaction fee is stored in the Windows Registry. This value can be trivially changed in a manner which is not detected by antivirus scanners or apparent to the user. This is demonstrated on line 20 of Form.cs

The attack works because the fee amount is never shown to the user from the time they open the client to the time when they complete a transaction. By the time they are aware the settings has been maliciously changed, the transaction has already happened and their funds are gone.

It also works because the value can be changed by anyone to any value.

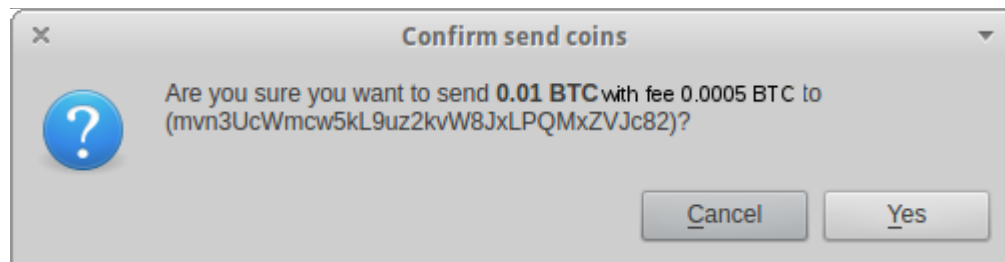
This attack may or may not apply to other operating systems running the Satoshi client, depending on the write permissions at the location the setting is stored.

This attack may or may not apply to other clients, depending on how the client calculates and displays the transaction fee for each transaction the user makes.

Proposed Solutions:

1. Change the client dialog

The client dialog for confirming a transaction should display the fee every time, even if the fee is 0 BTC. This is demonstrated in the image below. By displaying the fee there is less chance the user will be fooled into making the transaction with the high fee. They can cancel the transaction and change the fee setting to their desired value.



Changing the UI does not prevent repeats of the attack. It also requires the user to pay close attention to the dialog, which users may not do. With this change, the user will still be required to check the fee setting every time they start the client if they are to be sure they are not affected by this attack.

Fortunately the value is only read from the registry when the client starts. If the user changes the fee setting in the client, and the attacker is continually altering the registry value, the malicious registry value will not be used until the client is next started.

This is not a robust solution to the problem, but is a simple way of addressing an important user interface (UI) issue in the client.

2. Encrypt / lock the settings

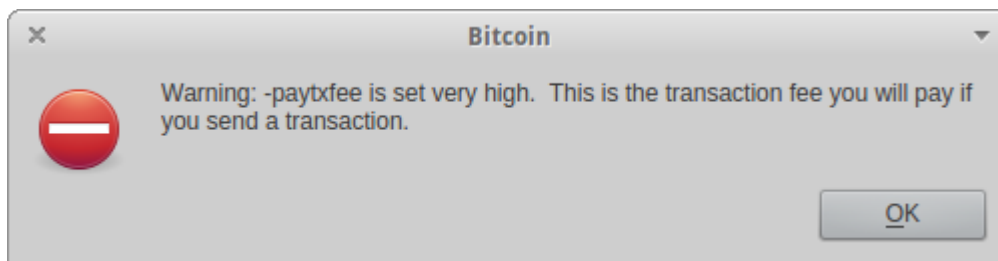
If the settings are stored in a way which cannot be manipulated without some specific knowledge from the user, the setting cannot be maliciously altered. Ideally this would

be implemented in a way which allows the settings to be read by anyone, so that frequently unlocking the settings isn't required, but only the person with knowledge to decrypt / unlock can write to the settings.

The registry also stores other settings which may cause vulnerabilities, however they are beyond the scope of this report. It is worth considering the security of any settings which can cause change to the user's funds.

Point Of Interest:

If the client is started with the `-paytxfee=50` flag or `bitcoin.conf` contains the entry `'paytxfee=50'` (or any high value) the following warning is shown when the client is started. This does not happen if the client value in the registry is set very high. It may be worth making this behaviour consistent.



Conclusion:

An attack exists which can cause loss of all coins in the user's wallet. It requires no special knowledge or computational resources. This attack can be prevented with two methods - a UI change, and by making it computationally infeasible to change the settings.