UNDERSTANDING THE HTML5COIN ATTACK

REPORT 1

Html5coin blockchain experienced a double spend attack between April 25 and 26, 2017. This attack caused two large transactions with dozens of confirmations to be unduly erased from the current blockchain, causing an insolvency in the exchange.

The double-spend attack is only successful if the attacker has more than 51% of the network's mining power to be able to replace the current blockchain with another of his choice. Similar attacks have already occurred with Virtacoin, Ambercoin, Vertcoin, CannabisCoin and e-Gulden, this type of attack is becoming common with outdated coins and few miners and several exchanges are suffering because of this.

We should follow what is registered in blockchain.

In 2017-04-25 Bleutrade received two large deposits from the same user:

Value: 2,852,036,157.86637402
Address: HTENYcoKi3NYM13AhwrjzsEN9AGnVYYYui
TXID: 9699446ff34e6224a177df2566c6503f791330256601c7126ad10ed225c61b3b

Value: 2,947,478,457.86636400
Address: HRYCxScEBr8R4eLRc9zwsmU8jX8gvcoM6a
TXID: c8d657812abc1779d924235e6938a5c35e7428f5916eec38c64ea34ec18217f2

After 20 confirmations the system approved this balance and the user was able to use it legitimately for trades and withdraws, after all, that was what the blockchain showed. The user's attitudes were to sell a little to doge and **withdraw the rest of the html5 balance to his wallet out of the exchange.**

How does Html5coin software work with deposits and withdraw?

When a Html5coin wallet receives a deposit, this balance is stored at the end of the queue. When you are required to send balance to another wallet, the Html5coin system uses the oldest coins to be selected within the transaction. So when the user requested withdrawals from his html5 balance deposited in our hotwallet, the Html5coin system did not send the same money as it had deposited, but the old ones stored, and this should not be a problem.

All transactions have a digital signature that proves the origin and destination of the coins being transacted.

Problem with transactions

- After a few minutes Bleutrade decides to send the balance to coldwallet, and this is only a periodic action.
- After hours the transactions sent to coldwallet are with 0 (zero) confirmations.
- We decided to resubmit the same transaction and the transaction was denied by the network.

This would be technically impossible, after all, there is no conflict in the deposits.

- We decided to rescan and we noticed that the blockchain was changed, the two large deposits were erased even with more than 20 confirmations.

Hacking Html5coin Blockchain

- To hack the original blockchain of Html5coin the hacker had to replicate the withdrawals of our hotwallet system (read about Replay Attack: goo.gl/GK424m) in unofficial blockchain.
- Spend, in **unofficial blockchain**, in **another address** the **same coins that had previously been deposited in Bleutrade** in the original blockchain.
- Make a 51% attack on the poor html5coin network, making your blockchain dominant in the network.
- The failed html5coin system does not understand the network conflict and cancels already confirmed blocks, replacing them with the unofficial hacker. This is a bug and should never occur.
- The result of this is an insolvency of 5.8 Billions html5coins without that there was failure in our system, because we acted according to the official blockchain.

Conversation with creators

- After finding the problem, Bleutrade placed an alert message on the html5 trade page.
- April 28:
  - Devs open a ticket and with information that the fix is already being performed.
  - Bleutrade informs the size of the problem and asks how this will be resolved.
  - Devs report that they can resolve the insolvency issue or create a swap for a new coin.
  - Bleutrade accepts the proposal, informs users that the developers are working on a fix and wait for the update.
- April 29 to 02 may: We provide all data for the correction to be healthy.
- June 08 and 09:
  - Bleutrade asks for progress information.
  - It is informed that progress is good.
  - Bleutrade provides more details of the blockchain attack.
- June 12:
  - Devs request to inform users that attacker has been deleted from the network.
  - Bleutrade informs that the source code still does not present the solution.
- June 14 to 17:
  - Devs request further information about the attack.
  - Bleutrade provides full access to the hacker's account.
  - Bleutrade again provides an explanation of what has happened.
  - Developers understand the problem but do not care more about Bleutrade.
  - Bleutrade informs that without the original proposal there is no solution.

Proof of existence of the deposit that was deleted from the blockchain

- 2,852,036,157.86637402 Deposit signature: https://pastebin.com/xDp3faqX
- 2,947,478,457.86636400 Deposit signature: https://pastebin.com/Ki845EEU