

## What happened

On March 16, 2014 at 18:53:20 bitcoins belonging to Fr33 Aid, a charitable organization, were stolen via the following transaction:

<https://blockchain.info/tx/c121bd17f2045610a6f7e8583e126a0c61f8b0272c270462f233bfe145f9d8bf>

According to Teresa Warmke, Treasurer of Fr33 Aid, their email account may have been hacked at some point, or she may have been phished by someone mimicking Blockchain.info's authentication link email for switching between wallets. A two factor authentication reset request was submitted on March 15 2014 at 09:00:26 UTC. All of the information provided in the request matched up to the information Blockchain.info had on file, resulting in the form being approved on March 16, 07:36:47 UTC.

2014-03-16 08:40:07	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:40:05	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:40:05	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:40:04	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:40:04	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:40:03	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:37:07	update wallet	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:37:00	get account settings	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 08:33:09	viewed login page	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-16 07:36:47	admin (mandrik) approved two factor authentication reset	Unknown	Unknown
2014-03-15 09:06:55	viewed login page	185.21.188.146	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-15 09:06:54	viewed login page	185.21.188.146	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-15 09:06:54	viewed login page	185.21.188.146	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-15 09:06:53	viewed login page	185.21.188.146	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-15 09:00:26	create two factor reset request	77.247.181.162	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-15 08:26:15	viewed login page	72.52.91.30	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
2014-03-14 13:10:32	viewed login page	178.217.187.39	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0

At no point did Blockchain.info ever approve any type of a password reset, as we never have the password information. This was stolen from Fr33 Aid, and was used to log into the wallet after the 2FA reset request was approved.

## What we learned

The attackers who stole Fr33 Aid's money were successful in exploiting the information they gathered from Fr33 Aid's compromised accounts to further compromise Fr33 Aid's Blockchain wallet through a social-engineering attack on our customer support staff. Our 2FA reset service is used daily by dozens of customers who lose their phones, lose access to computers or suffer catastrophic hardware failure on their devices. These customers depend on Blockchain's support staff to help them regain access to their accounts.

In providing this service to our customers we faced a compromise between speed of service and scrutiny of the requests. The Fr33 Aid theft demonstrated that our desire to provide speedy service could be used against our customers with a sufficiently informed adversary who could effectively masquerade as a legitimate customer. In the case of Fr33 Aid, the adversary had all the necessary identifiers to masquerade as Fr33 Aid and request the 2FA reset. Furthermore, they had access to the primary wallet password which they used to compromise the account once 2FA was disabled.

## What we do differently

Since the Fr33 Aid incident, we conducted a thorough review of our customer service process and security process. Based on this, we decided to change the balance between speed of response and security and have introduced a new process for two-factor authentication resets.

Each 2FA-reset request we receive is now scored based on risk. Using that information, we now perform 2FA requests with a *cool off* period during which we attempt to contact the account owner and to notify them of the impending reset. Depending on the risk score of the request, the waiting time can be as short as 24 hrs, or as long as several weeks. The more information that is provided in the request, the less likely it has all been sourced from compromised accounts and the faster we can process the 2FA reset. If during the cool off period we receive contact from the account owner, or there is a successful login from the account owner, the 2FA-reset request is invalidated.