From: Vincenzo Iozzo <[redacted]>
Sent: Saturday, August 23, 2014 11:07 AM
To: jeffrey E.
Cc: Joi Ito
Subject: Re: de-anonymize tor/bitcoin

hmm yeah, I like it - it's crazy :-) so, why not?
The problem we have is that we need to create an actual physical network =here people on food stamps have some kind of 'debit card' and merchants =ave a special POS to process those transactions (probably something =ike a Square reader will be sufficient). Not sure how big of a deal =hat is in terms of capital, but it's probably the only option unless we =ant to assume people on food stamps have smartphones..

But the good news is that if we do that and we succeed we obtain the =ollowing:
1) A good enough code base to then to the SWIFT thing + a lot more
2) A govt stamp of approval in crypto-currency stuff
3) Once merchants have our POS we can extend the currency to literally =everyone*

Jeffrey, does the govt on our side comes with money attached?

Joi, what do you think?

On 23/ago/2014, at 11:34, jeffrey E. <jeevacation@gmail.com> wrote:

> =ttp://www.foxnews.com/politics/2014/08/22/food-stamp-fraud-rampant-gao-re=ort/ make food stamps a test bed for transparant cyryto? govt on =ur side
>
>
> On Sat, Aug 23, 2014 at 5:54 AM, Vincenzo Iozzo <[redacted]> =rote:
> Jeffrey,
>
> this stuff is a bit heavy but if you care for it here are a couple of =inks:
>
> 1) One obvious technique to de-anonymize tor is to control the 'exit =odes', meaning the nodes that connect Tor to the Internet. If you =ontrol enough of them you can de-anonymize a lot of it.
>
> 2) A friend of mine (among other people), found ways to de-anonymize a
> =ot of the 'hidden services' (roughly the 'secret' websites inside
> tor) =uch more efficiently. I believe Tor fixed those flaws by now,
> but it's = pretty ingenious attack:
> =ttp://www.ieee-security.org/TC/SP2013/papers/4977a080.pdf The bottom
> =ine there is that with roughly $11k you can realistically
> de-anonymize =ny hidden service on tor. You do that by 'pretending' to
> be one of the =ervers handing out the addresses of the hidden services
>
> 3) The third option is to just attack the machine(s) of the 'bad
> =uys', this is for instance what the FBI did a while ago against a
> =etwork oh pedophiles:
> =ttp://www.reddit.com/r/onions/comments/1jmrta/founder_of_the_freedom_

> host=ng_arrested_held/ This option is targeted but it always works.
> The trick there was to =ttack the computer and then have the computer
> connect to a non-tor =ebsite, by doing that they could get the IP
> address and de-anonymize =he user. Of course once you have control
> over the machine you can do =uch more that that, but they sticked to
> that
>
> As for bitcoin itself, I believe I sent you the BitIodine paper.
> =nother very good one is this:
> =ttp://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf
>
> Now some of these approaches are probabilistic, (3) is not. But I
> =uess my point is: if you *really* want to figure out what somebody is
> =oing on tor/bitcoin you can do it given enough resources. Not that it
> =atters too much, but well
>
>
>
> --
> please note
> The information contained in this communication is confidential, may
> be attorney-client privileged, may constitute inside information, and
> is intended only for the use of the addressee. It is the property of
> JEE Unauthorized use, disclosure or copying of this communication or
> any part thereof is strictly prohibited and may be unlawful. If you
> have received this communication in error, please notify us
> immediately by return e-mail or by e-mail to jeevacation@gmail.com,
> and destroy this communication and all copies thereof, including all
> attachments. copyright -all rights reserved


```
<?xml version=.0" encoding=TF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version=.0">
<dict>
        <key>conversation-id</key>
        <integer>299373</integer>
        <key>date-last-viewed</key>
        <integer>0</integer>
        <key>date-received</key>
        <integer>1408792037</integer>
        <key>flags</key>
        <integer>8590195713</integer>
        <key>gmail-label-ids</key>
        <array>
                <integer>6</integer>
                <integer>2</integer>
        </array>
        <key>remote-id</key>
        <string>433850</string>
</dict>
</plist>
```