From: "jeffrey E." <jeevacation@gmail.com>
To: Vincenzo Iozzo <[redacted]>, Joi Ito <[redacted]>
Subject: Re: de-anonymize tor/bitcoin
Date: Sat, 23 Aug 2014 10:34:26 +0000

---

http://www.foxnews.com/politics/2014/08/22/food-stamp-fraud-rampant-gao-report/ make food stamps a test bed for transparant cyryto? govt on our side

On Sat, Aug 23, 2014 at 5:54 AM, Vincenzo Iozzo <[redacted]> wrote:

> Jeffrey,
>
> this stuff is a bit heavy but if you care for it here are a couple of links:
>
> 1) One obvious technique to de-anonymize tor is to control the 'exit nodes', meaning the nodes that connect Tor to the Internet. If you control 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 lot of the 'hidden services' (roughly the 'secret' websites inside tor) much more efficiently. I believe Tor fixed those flaws by now, but it's a pretty ingenious attack: http://www.ieee-security.org/TC/SP2013/papers/4977a080.pdf The bottom line there is that with roughly $11k you can realistically de-anonymize any hidden service on tor. You do that by 'pretending' to be one of the servers handing out the addresses of the hidden services
>
> 3) The third option is to just attack the machine(s) of the 'bad guys', this is for instance what the FBI did a while ago against a network oh pedophiles:
> http://www.reddit.com/r/onions/comments/1jmrta/founder_of_the_freedom_hosting_arrested_held/
> This option is targeted but it always works. The trick there was to attack the computer and then have the computer connect to a non-tor website, by doing that they could get the IP address and de-anonymize the user. Of course once you have control over the machine you can do much more that that, but they sticked to that
>
> As for bitcoin itself, I believe I sent you the BitIodine paper. Another very good one is this:
> http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf
>
> Now some of these approaches are probabilistic, (3) is not. But I guess my point is: if you *really* want to figure out what somebody is doing on tor/bitcoin you can do it given enough resources. Not that it matters 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