From: Vincenzo Iozzo <[redacted]
Sent: Saturday, August 23, 2014 9:55 AM
To: jeffrey E.
Subject: de-anonymize tor/bitcoin

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 guys', =his is for instance what the FBI did a while ago against a network oh =edophiles:
=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. Another =ery good one is this:
=ttp://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Now some of these approaches are probabilistic, (3) is not. But I guess =y point is: if you *really* want to figure out what somebody is doing =n tor/bitcoin you can do it given enough resources. Not that it matters =oo much, but well

```
=?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>1408787676</integer>
	<key>flags</key>
	<integer>8590195717</integer>
	<key>gmail-label-ids</key>
	<array>
		<integer>6</integer>
		<integer>2</integer>
	</array>
	<key>remote-id</key>
```

```
		<string>433835</string>
</dict>
</plist>
```