WHY DID SHADOW BROKERS SWITCH CRYPTO CURRENCIES TO NOT MAKE MONEY WITH?

The other day, Shadow Brokers announced its new Warez of the month club: Send 100 Zcash, over the next 30 days, and they'll send back … goodies that have yet to be described.

Zcash is, like Bitcoin, a cryptocurrency, but with a whole lot of smart thinking about how to make it secret.

Now, if the idea were to make money, the switch to Zcash would make sense. Days before Shadow Brokers announced this new gig, someone started cashing out the measly $20K in BTC it had made thus far, and people around the world watched as the money was dispersed through a bunch of other accounts. If the theory is to make money and cash it out, Zcash is a better option. As Matthew Green, who had a hand in setting up Zcash described it, to me.

> [U]nlike Bitcoin, it supports untraceable transactions. In these transactions I can send you money such that only you and I (and nobody else) can see the amount or nature of a payment. These are called "shielded transactions", and they use zero knowledge proofs. Presumably it is this feature that ShadowBrokers are interested in — assuming they are actually interested in any part of making money, and the whole thing isn't a sham.

It's the last bit, though, that raises questions for me.

Shadow Brokers set up an auction that was virtually designed to fail. That provided SB the opportunity to keep bitching about it publicly, then ultimately to release more files. It then set up a crowdfunding scheme, which again failed. Which led it to release files that ultimately led to a global ransomware being let loose.

So why switch currencies? SB can fail to make money just as easily with BTC as it can with ZEC.

One possibility is that SB wants to taint the currency. In its post, SB claims ZEC has ties to the federal government.

> Zcash is having connections to USG (DARPA, DOD, John Hopkins) and Israel. Why USG is "sponsoring" privacy version of bitcoin? Who the fuck is knowing? In defense, TOR is originally being by similar parties. TheShadowBrokers not fully trusting TOR either. Maybe USG is needing to be sending money outside from banking systems? If USG is hacking and watching banking systems (SWIFT) then adversaries is also hacking and watching banking systems. Maybe is for sending money to deep cover foreign assets? Maybe is being trojan horse with cryptographic flaw or weakness only NSA can exploit? Maybe is not being for money? Maybe is being for Zk-SNARKs research? Maybe fuck it, lets be finding out.

I asked Green about the DARPA, DOD, John Hopkins [sic] slam, and he pointed to the research paper that forms the basis for the currency. In the acknowledgments, the authors thank their underlying sources of funding.

> This work was supported by: Amazon.com through an AWS in Education research grant; the Broadcom Foundation and Tel Aviv University Authentication

> Initiative; the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-0939370; the Check Point Institute for Information Security; the U.S. Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL) under contract FA8750-11-2-0211; the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 240258; the Israeli Centers of Research Excellence I-CORE program (center 4/11); the Israeli Ministry of Science and Technology; the Office of Naval Research under contract N00014-11-1-0470; the Simons Foundation, with a Simons Award for Graduate Students in Theoretical Computer Science; and the Skolkovo Foundation with agreement dated 10/26/2011. The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Green describes (rightly, says a girl who probably took Soros funding in several ways while an academic) this as just good academic form.

> These aren't organizations that specifically funded *this project*, they're just organizations that had provided funding to support the various scientists involved. It's good form to list them all. And obviously Johns Hopkins is my institution, although I don't do spook stuff.

He also suggested that the dig at ZEC's funding is just part of the entertainment value that SB uses to get attention.

> SB seems to be very astute in the way they cultivate interest among

> Information Security folks on Twitter. This could be because they're legitimately also hackers (probably true at least in part). But it also serves their larger information needs because they have a complex message to get out there — and reporters are good at ignoring the message if there are no good interpreters to process it. Entertaining and relating to the infosec community on Twitter means they have a ready-made pool of infosec experts willing to talk to reporters about whatever new thing they've done. More tech companies should learn from this strategy, which is sort of clever (in an evil way)!
>
> Along the above lines, adopting a new (and technically very advanced) private cryptocurrency keeps infosec people entertained. It gets RTs and makes people ask questions. Throwing in all the nonsense about backdoors and the DoD is probably entertainment value. Just like their "Russlish" grammar is, and the whole drama about auctions and subscription services.

I'm not so sure.

I can think of at least two other possibilities.

First, currencies have been bouncing around in response to some of this stuff. So it's possible this is an attempt to flood the market.

Certainly, too, the invocation of DARPA seems about increasing distrust, just as SB did in its efforts to increase the distrust between Microsoft and the government.

More interestingly, though, perhaps this is SB's way of adding to the risk to NSA of any releases. While some people believe NSA has already disclosed all the vulnerabilities it believes SB to have (indeed, SB's last post suggested as much as well), if there's any doubt

about that, by using a more secretive currency, it will add the risk to NSA of not knowing who has anything SB sells.