SHADOW BROKERS' PERSISTENCE: WHERE TSB HAS SIGNED, MESSAGE, HOSTED, AND COLLECTED

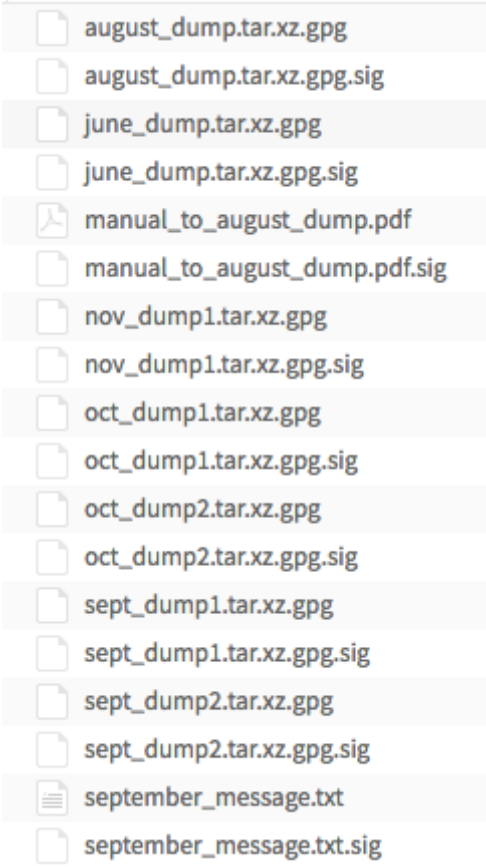
Back in April, Shadow Brokers boasted about his operational security.

> TheShadowBrokers is practicing obfuscation as part of operational security (OPSEC). Is being a spy thing. Is being the difference between a contractor tech support guy posing as a infosec expert but living in exile in Russia (yes @snowden) and subject matter experts in Cyber Intelligence like theshadowbrokers. TheShadowBrokers has being operating in country for many months now and USG is still not having fucking clue. Guessing so called global surveillance is not being as good as @snowden is claiming?

I started thinking about this boast again after TSB deleted all his Twitter feed in June (which served to hide the truly moronic failed doxing of @DRWolfff, which he then followed with an even more moronic post claiming he hadn't failed). Good to know being an asshole on Twitter will keep you alive for more than a year after dumping NSA tools all over the InterWebs.

Still, since then TSB hasn't tweeted at all. And his September dump — which given the normal pattern, would have been released in the last days of August — didn't come out until September 6 (just a few days after a bunch of us were wondering if he had finally snuck off to join Snowden in Sheremetyevo). On that day, TSB dumped the files he claims to have dumped in his Warez of the Month club since June, as well links for twice-monthly dumps going through

November.



While we were chatting about TSB running off to Sheremetyevo, Matt Suiche raised a point I had been thinking about too: TSB's key. By now, that key must be set to loud alarms in Fort Meade, such that any time it appears transiting across the InterTubes, lights flash in an attempt to ID TSB's location.

Of course, all that's done for the next three months, because everything is safely loaded on Mega's servers in one fell swoop.

Suiche noted that TSB hadn't signed a post since June; he actually had in July (but over at ZeroNet rather than on Steemit), but not the for the late June post tied to the July dump.

In other words, since June, TSB has been either not signing posts, or signing them somewhere else, away from the Steemit account that (in the wake of his Twitter demise) has now become his persistent identity, where people can follow him.

Anyway, because I'm a loser, I decided to track

what he had done for the entire year plus to be able to sustain a persistent identity while still avoiding drone strikes. A draft table of what TSB has done to sustain persistence with 1) key-signing, 2) stable messaging identity, 3) file-hosting, and 4) payment since August 2016 is here. In addition to increasingly signing remotely, and shifting from Twitter to Steemit to alert followers, TSB has also moved away from stable, public cryptocurrency addresses, and encrypted emails with individual buyers, instead relying on the security of Zcash and its memo line.

- Zcash only, no Monero, delivery email in encrypted memo field
- Delivery email address clearnet only, recommend tutanota or protonmail, no need exchange secret, no i2p, no bitmessage, no zeronet

In any case, this is just a draft. I'm sure I fat-fingered some stuff, and I'm sure I didn't understand some of what I was looking at. But please take a look and see what I'm missing/gotten wrong.

There are some interesting bits even from what's here. I hadn't realized, for example, that TSB cashed out his BTC wallets the same day, May 29, he posted the new ZEC and XMR sales. Also, TSB posted "Don't Forget Your Base" at his old-school haunts — Medium and Reddit — as well as Zero and Steemit (he was transitioning from one to another that day), I guess to reinvigorate his fan base after claiming he was done in January.