The Silk Road OPSEC Fail

“Whoops!”

Disclaimer

Any opinions presented in this talk by the presenter do not in any way represent an official endorsement of these opinions by Freeside Technology Spaces, Inc., nor is intended to reflect the views of Freeside and its membership.

Freeside does not encourage or promote any illegal activity, including but not limited to accessing a virtual marketplace to buy and sell illegal drugs using cryptocurrency on an anonymous darknet. Illegal drugs are known to have harmful side-effects, such as destabilizing the price of Bitcoin. They can lead to NSA attacks on the Tor network, and may even draw the attention of law enforcement to your online activities.

"We had two bags of grass, seventy-five pellets of mescaline, five sheets of high powered blotter acid, a salt shaker half full of cocaine, and a whole galaxy of multi-colored uppers, downers, screamers, laughers... and also a quart of tequila, a quart of rum, a case of Budweiser, a pint of raw ether and two dozen amyls.

Not that we needed all that for the trip, but once you get locked into a serious drug collection, the tendency is to push it as far as you can."

Hunter S. Thompson, *Fear and Loathing in Las Vegas*

What is OPSEC?

Operational Security.

“...a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.”

What is OPSEC? (cont.)

OPSEC includes the use of encryption and other technical countermeasures, but also includes physical security and how to behave to protect yourself and your assets.

Example: If you always run a laptop with the battery removed, in an emergency, you can unplug the power supply to defend against some forms of cold boot attack.

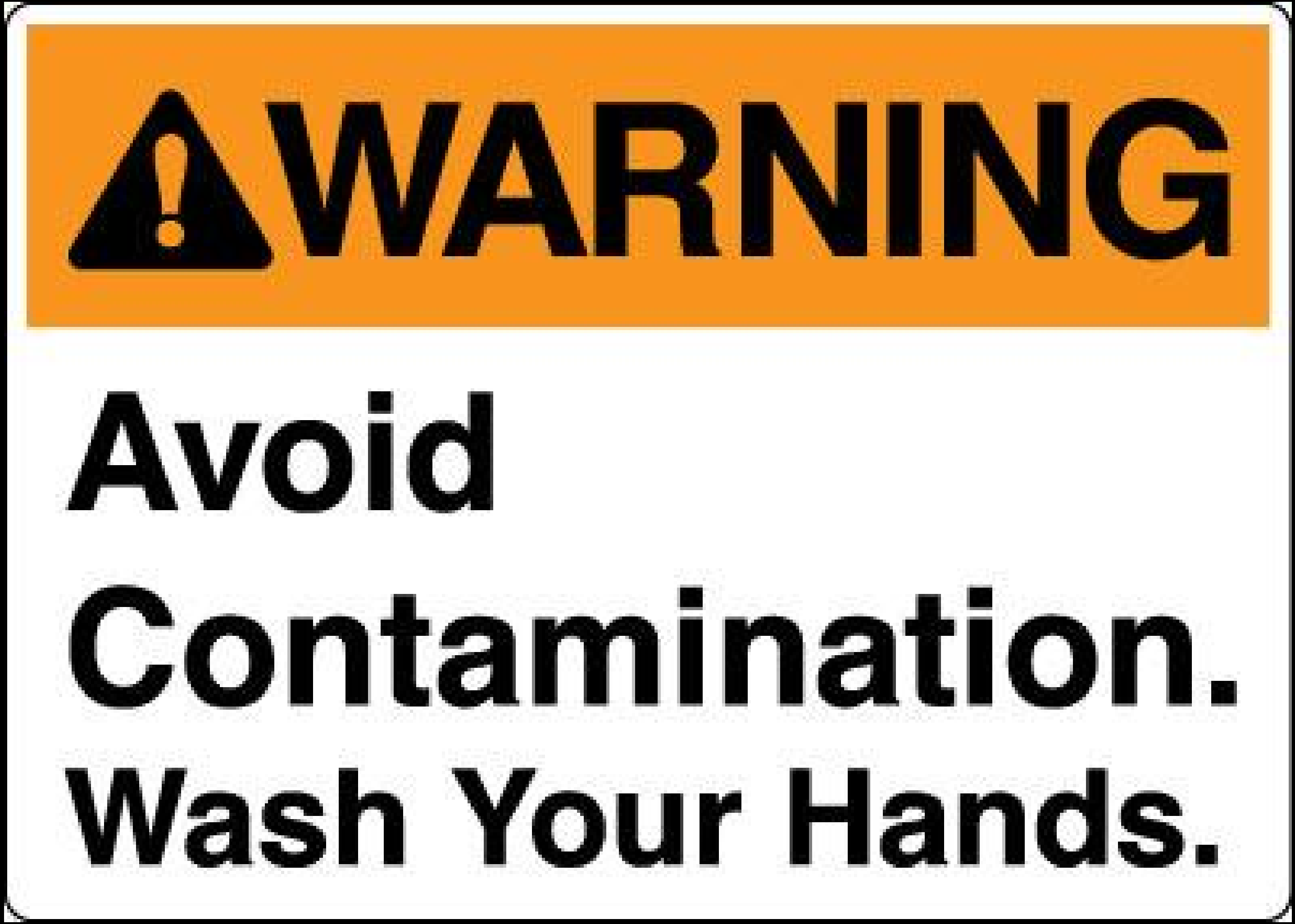
In other words, OPSEC == STFU

OPSEC Fail #1

In October of [2011], a user also going by the name of "altoid" made a posting on Bitcoin Talk titled "a venture backed Bitcoin startup company", which directed interested users to "rossulbricht@gmail.com".

PROTIP: When starting your drug-based virtual empire, don’t hop on a public forum and solicit investors to contact you at an email address that contains your full name.

OPSEC: Contamination



⚠WARNING

Avoid Contamination.
Wash Your Hands.

OPSEC: Contamination

When creating an alias, any connection or contact between your alias and your real identity is known as **contamination**.

It sounds bad, because it is.

Avoid linking your real identity to your alias, both online and offline.

OPSEC Fail #2

Ulbricht's Google+ page and YouTube profile both make multiple references to the a website dubbed the "Mises Institute". DPR's signature on the SR forums contained a link to the Mises Institute.

DPR cited the "Austrian Economic theory" along with the works of Ludwig von Mises and Murray Rothbard, all of which are closely associated with the Mises Institute.

Ulbricht left yet another cookie crumb by telling a Silk Road user that he was in the Pacific time zone.

PROTIP: To remain anonymous on the internet, try to not volunteer personal or identifying information like your specific personal politics or the time zone you live in to strangers you meet in chat rooms, and post the same information on your social network profiles.

OPSEC: Don’t Leak Information

OPSEC: Information Theory

Anonymity is an inverse function of the number of bits (data) you release into the world.

The more bits you generate, the less anonymous you are.

The moral of the story is: don’t volunteer unnecessary information.

OPSEC Fail #3

DPR connected to the Silk Road server(s) like this:

1. Home
2. Neighboring Wifi
3. Tor
4. VPN
5. Silk Road Server(s)

Not too shabby...except...

OPSEC Fail #3 (cont.)

Except for that one time that he logged into the VPN directly from the Neighboring Wifi.

Agents coordinated that IP address with the subpoenaed gmail address records (remember Fail #1?)

DPR also kept the IP address to the VPN IP block in a comment on the server-side code.

OPSEC Fail #4

Another piece of evidence used to snag Ulbricht was his purchase of a counterfeit California ID with his face and another name on it. The package was addressed to Ulbricht's San Francisco apartment.

PROTIP: When ordering illegal items that may or may not cross national borders, don't send the items directly to your home.

Bonus PROTIP: Don't order any illegal items with a photo of your face on them.

OPSEC Fail #5

A user called "redandwhite" then proceeded to contact DPR, stating that he was FriendlyChemist's supplier and also the owner of his debt. DPR then solicited redandwhite to "execute" FriendlyChemist, supplying redandwhite his full name and address. After having agreed on terms, DPR sent redandwhite approximately $150,000USD (1,670BTC) to have FriendlyChemist killed. redandwhite later provided photographic proof of the alleged murder.

PROTIP: When running a drug empire, you should brush up on common confidence tricks and scams.

OPSEC Fail #6

“Pursuant to a Mutual Legal Assistance Treaty request, an image of the Silk Road Server was made … and produced thereafter to the FBI.”

PROTIP: Don’t host your servers in a country that is a party to the Mutual Legal Assistance Treaty.

Mutual Legal Assistance Treaty Parties