Dark web anonymity

Description

I downloaded a bitcoin wallet to my smartphone on 3 July 2017, and filled it with Â£100 of bitcoin procured via my debit card. The transaction cost Â£3. A bank transfer would have been free, but I was in a hurry. (With currency fluctuations, and 3 weeks later, my wallet today contains Â£110.19. So I am up on the deal!)

This â??digital cashâ?• was for backup while travelling. Nervous travellers used to carry a few travellers checks or US dollars. I had heard that bitcoin is popular in some former Soviet countries, as not everyone trusts the banks. I didnâ??t see any â??bitcoin accepted hereâ?• logos in Ukraine, though I believe thereâ??s a coffee shop near the train station in Lviv.

I inquired once about bitcoin while travelling, and that was to our local tour guide at a cafe in the Chernobyl Exclusion Zone. â??Do you think they take bitcoin?â?• I asked. My question came over as a joke, as it would here. Who even knows what it is? Who has the knowledge and apparatus to process a bitcoin transaction?

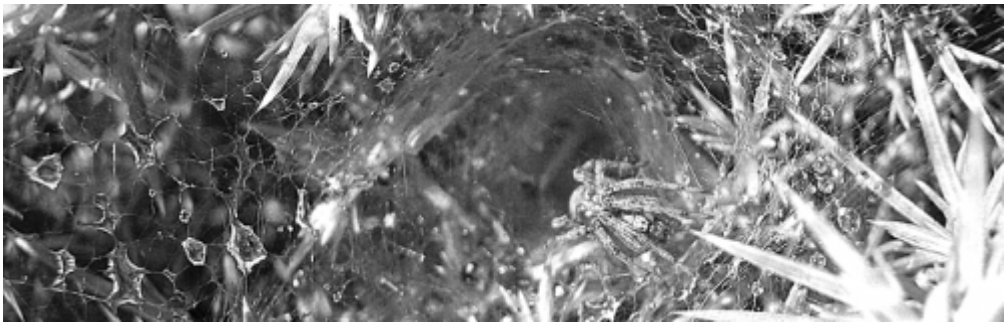
Hidden economies

Bitcoin has most currency in the hidden world of anonymous transactions for goods and information. Bitcoin and similar cryptocurrencies are used in those parts of the web hidden from public view, i.e. invisible to regular browsers and search engines.

Secretive markets like cash. An envelope containing Â£50 notes can be exchanged for goods without leaving a trace. Digital cash is similarly useful in secretive digital markets. The other component of secret transactions is the ability to enter the marketplace anonymously. The Tor browser software provides such access. Hereâ??s my summary of the aims of Torâ??s developers from the Tor website.

- Improve peopleâ??s privacy and security online
- Tor servers are operated by volunteers
- It works by providing a â??series of virtual tunnelsâ?• that effectively makes the source and destination of information flows untraceable
- Allows users to break through barriers to sites with censorship restrictions
- Allows people to publish websites without disclosing where they are located geographically, or in terms of jurisdiction or domain.
- So people can use Tor for â??socially sensitive communication.â?• The website refers to â??chat rooms and web forums for rape and abuse survivors, or people with illnesses.â?•
- Apparently, journalists can â??communicate with whistleblowers and dissidentsâ?•
- NGO workers can â??connect to their home website while theyâ??re in a foreign country, without notifying everybody nearby that theyâ??re working with that organization.â?• Itâ??s more secure than VPN.
- Users include Indymedia, the Electronic Frontier Foundation (EFF), the U.S. Navy, and law enforcement.

Tor was created originally in the 1990s by the US Navy and defense departments and was made public around 2003, and is supported by volunteers.



Dark web intelligence

Iâ??ve described online anonymity here in benign terms, driven by security and privacy rights, supporting dissidents, whistleblowers, and legitimate, undercover intelligence gathering.

But anonymous transactions and secret identities are also the stuff of blackmarket transactions, as in the case of Hansa and Alphabay. These digital blackmarkets are/were notorious in bringing together traders and buyers of illegal drugs, munitions and pornography. Such sites are in turn prone to hacks and raids by law enforcers.

The Guardian reported yesterday that EUROPOL and the FBI managed to raid and capture the physical servers of Hansa and AlphaBay. In an international effort, EUROPOL took control of these sites a month ago. In a clever cyber sting operation they closed down one of these sites (Alphabay) but still left Hansa open for users.

EUROPOL then monitored users who migrated their activities from AlphaBay to Hansa, providing EUROPOL with usernames and passwords for â??thousandsâ?• of illegal traders: buyers and sellers of drugs and guns â?? a clever ruse to not only shut down the market places, but also monitor users, and potentially trap illegal activity.

Cyberwars

With some irony, the Guardian article included a photograph of the US Attorney General (AG) topping the chain of command for the US side of the operation. The controversial AG (Jefferson Beauregard Sessions III) delivered the news of the intelligence victory at a US press conference, with a speech decrying the way the illicit drug trade was destroying lives in the US (see transcript).

At the same time the AG and several other US White House staff and former campaign operatives are under investigation for complicity in the attempts by Russia to influence the US presidential election. Thatâ??s also dark web stuff.

Whatever the culpability of the individuals under investigation, the current wave of cyber-espionage and counter-espionage, points not just to drug cartels, but money laundering, targeted political influence, blackmail and trade in stolen information. It seems many people already and unwittingly have their feet stuck in the dark web.

Reference

- Gibbs, S. and L. Beckett. (2017), â??Dark Web Marketplaces Alphabay and Hansa Shut Downâ??. *Guardian*, 20 July. Available online: https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down (accessed 22 July 2017).

Category

1. Economics

Tags

1. bitcoin
2. blockchain
3. ciphercity
4. dark web

Date Created
July 23, 2017
Author
rcoyne99