

Tor, Bitcoin, and the Underground Economy

By Paul Benoit



Why should you care?



- Using Tor a couple times \neq knowing enough about the darknet
- If client hit with ransomware asked you to pay attacker 4BTC today, could you do it?

Deep Web vs Darknet



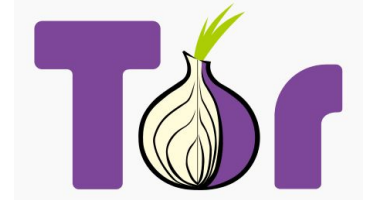
- Deep Web = not indexed by search engines
 - Gmail inbox
 - Cloud storage
- Darknet = parts of Deep Web that can only be accessed with specific software/configurations
 - Alphabay
 - Ransomware websites
 - Hacking forums



Tor



- Anonymity network
- Originally designed by US Navy
- Assigns an anonymous IP address to user
- Allows access to Darknet



You're not an edgy super hacker



YOU'VE BEEN TO THE HIDDEN WIKI?



FBI JUST CALLED, THEY DON'T CARE

Case Study: criminal side



- Eldo Kim, a Harvard sophomore, emailed bomb threats to Harvard
- Tor + Guerrilla Mail from Harvard wifi
- FBI interviews him, he confesses



Case Study: LE side



- Police and FBI notified of Harvard bomb threat
- Search for bomb for five hours, realize it was a hoax
- Inspect email, see that sender used Guerrilla Mail and Tor
- Check who was using Tor on Harvard wifi before the email was sent → Eldo Kim
- Interviewed Kim and got him to confess

Case Study: how he messed up



- Used Harvard wifi
- Confessed
- Talked to FBI without lawyer



Bitcoin



- Cryptocurrency
- Volatile
- No centralized control



How Bitcoin Works



- Bitcoins aren't physical
 - everyone keeps copy of ledger which tracks how much accounts own
 - buying/spending bitcoin is updating ledger
- Prove who sent bitcoin- signature (unique to transaction) comes from private key (unique to wallet)
- Prove when sent- pending transactions sorted into an ordered chain
 - sorted by computers solving math problems (miners), rewarded with bitcoins

Bitcoin buying guide




- Bitcoin ATMs
- PayPal hates Bitcoin
- Bank Account- Coinbase or Circle
- Randos- Localbitcoins



Bitcoin Wallets



- Wallets store bitcoin
- Coinbase, Circle have wallets
 - Monitored for sending to illegal addresses
 - Buy limit
- Blockchain.info
- Multiple wallet addresses can be associated with same wallet

But if we suspect that you purchased a fake ID  , we'll have to close your account and end the good thing we had going.

What can you buy on the Darknet?



- Hitmen
 - NO, they're all scammers or FBI undercover
- Drugs (Popularity: MDMA > Marijuana > cocaine)
- Weapons (high % scams)
- Login Credentials (Banking, CC, email, etc.)
- Bots

What can you buy on the Darknet?



- Hacking tools (RATs, Exploit kits, Keyloggers, etc.)
- DDos attacks
- Ransomware
- Fake Papers
 - US DL's → crazy easy
 - Passports → complicated

Why doesn't LE shut down the sites?



- Hosted in Russia, China, or other uncooperative countries
- Valuable source of intel
-

Evading capture



- Use Tor correctly (updated, not from uni wifi, without connecting to PII, ideally with VPN)
- Launder Bitcoins
 - Debit Card → Circle (PII) → Blockchain wallet (no PII) → vendor
 - Cash → BTC ATM → Blockchain wallet (no PII) → vendor
 - Paypal → LocalBitcoins → Tumbler (Bitcoin blender, Helix) → vendor

Evading capture



- Use PGP if messaging a vendor
- Never talk to LE without Lawyer

test



- test