
# Namecoin for Tor Onion Service Naming (And Other Darknets)

Jeremy Rand
Lead Application Engineer, The Namecoin Project
https://www.namecoin.org/

OpenPGP: 5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

Presented at 34C3 Monero Assembly / Chaos West Stage

# A brief introduction to Namecoin

- Like the DNS, but secured by a blockchain.
- Uses the “.bit” top-level domain.
- Names are represented by special coins.
- First project forked from Bitcoin (in 2011; Bitcoin was created in 2009).
- Original focus of developers was on censorship-resistance.
  - We later became interested in privacy use cases as well.

# Tor Onion Services' Big UX Problem

- Tor onion services are awesome for hosting TCP services anonymously.
- However, their names aren't human-meaningful.
- ~~http://[illegible].onion~~
- http://odmmeotgcfx65l5hn6ejkaruvai222vs7o7tmtllszqk5xbysola.onion

# Human-meaningful naming layers for Tor

- Namecoin
- OnioNS (Onion Name System)
- GNS (GNU Name System)
- Blockstack

# Namecoin

- Decentralized
- Supports lightweight (SPV) clients
- Global namespace
- Relies on game-theoretic security

# OnioNS

- Semi-decentralized (relies on Tor DirAuths)
- Lightweight
- Global namespace
- Doesn't rely on game-theoretic security

# GNS

- Decentralized
- Lightweight
- No global namespace
- Doesn't rely on game-theoretic security

# Blockstack

- Only decentralized in theory (not practice)
- No lightweight clients (you need the entire Bitcoin blockchain)
- Global namespace
- Relies on game-theoretic security

- Don't seem like ethical players (obfuscated security documentation, false security claims, etc.)
- Funded by investors who have endorsed mandatory crypto backdoors

# Methods of naming layer integration

- Intermediate proxy
- Tor control port
- Pluggable naming

# Intermediate proxy

- Tor Browser → Naming SOCKS5 proxy → Tor SOCKS5 proxy
- Tricky to do safely due to stream isolation
  - Need to pass through SOCKS authentication
  - Tor sometimes uses source IP for stream isolation as well
- Early examples of this approach were NmcSocks by ItsNotLupus, and Convergence for Namecoin by me.
- Yawning Angel from Tor has an intermediate SOCKS proxy that could be modified to do naming as well.

# Tor control port

- Catch events for new TCP streams
- Redirect them to a different host/IP
- Stream isolation works fine for application traffic
- No stream isolation for naming system traffic
- Tor-specific
- OnioNS has an implementation of this.
  - I modified it to use Namecoin – it worked fine as a proof of concept.

# Pluggable Naming

- Tor Prop279
- Based on Pluggable Transports spec
- Not yet implemented in Tor
  - But meejah has a shim that makes it usable
- Stream isolation works fine for application traffic
- No stream isolation for naming system traffic
- Might not support input hostnames outside of .onion (due to political reasons).

# DNS-Prop279

- Shim layer between Pluggable Naming and DNS
  - (I'm the author)
- Configure it to use a local Namecoin-DNS bridge, and Tor will magically resolve Namecoin domains.
- .onion service goes in a TXT DNS record (in Namecoin).

- Source code is posted, it's confirmed to work.  See Beta Downloads page at https://www.namecoin.org/
- Try http://federalistpapers.bit/

# DNS-Prop279 (2)

- .bit → Try resolving via .onion TXT, then fall back to IP/CNAME.
  - Don't assume encryption unless it's HTTPS.
- .bit.onion → Only try .onion TXT, if not present return an error.
  - You can assume encryption even if not HTTPS.

- Is that sane behavior?  Curious what you think – please give me feedback!

# Problems with DNS-Prop279's Design

- The DNS wire protocol doesn't have a good way of conveying stream isolation data.
- EDNS could possibly be abused to do this, but it's incredibly ugly.
- After talking with Nick Mathewson from Tor, I now think that using the DNS wire protocol isn't a great approach.
  - I'm currently planning to rewrite, without using DNS.
  - It'll be the 3rd iteration – iteration is how we gain experience and make a better system.

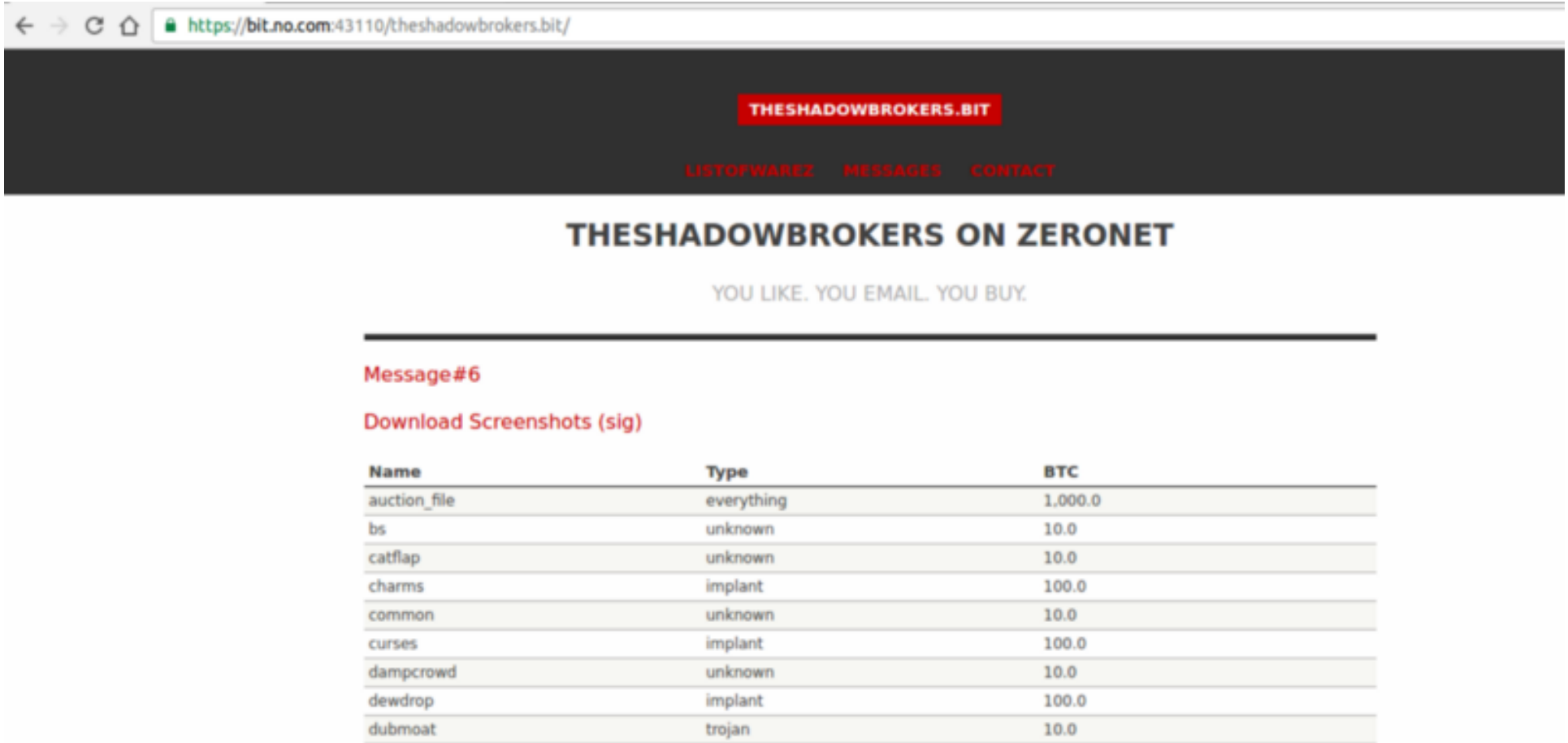
# Non-Tor darknets

- There are lots of darknets out there.
- Tor isn't the only one that's experimenting with Namecoin.

# ZeroNet

- A darknet that uses Bitcoin-compatible ECDSA keypairs for addressing.
- Basically like BitTorrent for websites.
- The ZeroNet devs are using Namecoin (kind of) for human-readable names.
  - Currently relies on a centralized name lookup service... we want to help them fix that.

# ZeroNet+Namecoin in the news: TheShadowBrokers



# Other darknets

- Namecoin should be usable for just about any cryptographically addressed darknet.
  - I2P (including Kovri!), Freenet, etc.
  - We'd love to see integrations happen – if you work on darknet software, please talk to me!
- Also please give feedback to Tor on the Prop279 Pluggable Naming API.

# Other naming systems

- If you work on OnioNS, GNS, or any other naming system, please give feedback to Tor on the Tor Prop279 Pluggable Naming API.
- These naming systems all make different tradeoffs – we want to collaborate with you, not compete with you.  Teamwork!

# Contact Me At...

- https://www.namecoin.org/
- OpenPGP:
  5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85
- jeremy@namecoin.org
- Or just find me here at the Congress!  (The Namecoin logo on my shirt should help you find me.)