hackerspace.gr

A Russian Bride for Tor

kargig [at] void.gr
@kargig

GPG: 79B1 9198 B8F6 803B EC37 5638 897C 0317 7011 E02C

Intro

- “Anonymity loves company”
- Tor daemon sets up socks5 proxy
- ...but programs lack socks5 support (or have poor implementations)
- So Tor is lonely...

Torification

How could more programs use Tor ?

- implement socks5 everywhere
- torsocks (preload Library)
  - Pros: easy to use
  - Cons: segfaults
- automagically send tcp connections to socks5 port

A Russian Bride

redsocks by Leonid Evdokimov

“redirect any TCP connection to SOCKS or HTTPS proxy using your firewall, so redirection is system-wide”

- redsocks daemon listens on a port
- iptables redirects tcp connections to redsocks daemon port
- redsocks daemon forwards connections to Tor's socks5 port
- WIN!

Prenuptial agreement

(part of) torrc

```
SocksPort 9050
(or SocksPort 9050 IsolateDestAddr IsolateDestPort)
```

(part of) redsocks.conf

```
Redsocks {
        local_ip = 127.0.0.1;
        local_port = 12345;
        ip = 127.0.0.1;
        port = 9050;
        type = socks5;
}
```

(part of) iptables rules:

```
iptables -t nat -N REDSOCKS
iptables -t nat -A REDSOCKS -p tcp -j REDIRECT --to-ports 12345
iptables -t nat -A OUTPUT -p tcp -m owner --uid-owner foobar -j REDSOCKS
```

hackerspace.gr

Happily Married

Marriage problems

- TCP connections are fine...but what about DNS?
- DNS is (mainly) UDP but works over TCP as well
- ...Tor does not like UDP and neither does socks5

Convert DNS queries to TCP → pass them through Tor

dnstc (by redsocks)

- Answers with “truncated query” to every DNS request
- Forces (RFC compliant resolvers) to retry over TCP
- Many issues:
  - eglibc resolver won't retry over TCP (ping won't resolve)
  - sloooow! (every query goes over Tor, significant delay)
  - some DNS authoritative servers won't reply over TCP (in.gr)

A dutch mistress to the rescue

- Add a local resolver to the mix that
  - will listen on UDP + TCP on localhost
  - can send upstream queries only over TCP
  - can use a forwarder (for auth NS w/o TCP)

- **unbound** by NLnet Labs
  - Caching resolver
  - Fast

She likes red socks! ;)

(part of) unbound.conf

```
server:
    do-udp: yes
    do-tcp: yes
    tcp-upstream: yes
    interface: 127.0.0.1

forward-zone:
    name: "."
    forward-addr: 149.20.64.20
```

/etc/resolv.conf
nameserver 127.0.0.1

```
iptables -t nat -A OUTPUT -p tcp -m owner --uid-owner unbound -j REDSOCKS
```

The story of a DNS query

- UDP DNS query to 127.0.0.1 goes to unbound
- unbound creates a TCP upstream query
- redirect with iptables to redsocks
- redsocks forwards to Tor SocksPort
- request goes over Tor to Forwarder (149.20.64.20)
- forwarder asks authoritative NS over UDP or TCP
- forwarder replies back (over Tor) with answer to unbound

(DNS queries are waaay slower...but you wanted anonymity, right?)

Better than Tor's DNSPort

- Caching
- DNSSEC

Gotchas

- **NO IPv6!**
  - socks5 does not support IPv6
  - redsocks does not support IPv6
  - If you have IPv6 address(es) you will use them for DNS queries...**no more Tor/anonymity**...
  - No current workaround (apart from completely disabling IPv6)
- DROP all UDP on your OUTPUT filter

  Yes, everything, DO IT!
- Airport HotSpots?

  use a separate user with another browser (uzbl?) to enter

```
$ echo “xhost +si:localuser:otherusr” >> ~/.xprofile
$ sudo -u otherusr uzbl “http://koko.lala”
```

Misc

- Secure your /etc/resolv.conf from stupid DHCP servers/clients

  # chattr +i /etc/resolv.conf

- Make sure your iptables rules run before everything else
- Use a Tor bridge with **obfs3/scramblesuit/obfs4**

  # tcpdump -ni ethX not host bridge.ip

  if you see any non-local output, you've fucked up!

- So browsers can be torified ? W00h00!
  - **Don't** use your standard browser over Tor
  - Only use TBB or TAILS

hackerspace.gr

Bieber approves redsocks

Outro

Keep calm

and use

redsocks

and

Tor

P.S.

No, I am not giving you my configs/iptables. Experiment carefully on your own. If you can't, then use TBB, Tails, Whonix, Qubes OS, etc

Resources

- Resources:
  - http://darkk.net.ru/redsocks/
  - https://www.nlnetlabs.nl/projects/unbound/
  - http://techcrunch.com/2014/06/22/love-hacking-social-isolation/
  - http://www.gettyimages.com/detail/photo/netherlands-alkmaar-young-woman-in-high-res-stock-photography/200312279-001
  - https://www.dns-oarc.net/oarc/services/odvr
  - Other stolen images from the intewebs