

# IP over DNS tunnels

:-)

Sergey Myasoedov

NetArt Group

old geek's joke

For those who don't want to pay for Internet access in hotels/airports etc.

It's asymmetric by definition!

Low-speed access (Download 5-80 kB/s)

Requires designated zone in the namespace

Uses recursive requests

Client sends data to the server in DNS TXT queries

Server replies in TXT answers

But you can change this practice! :-)

Client



Local DNS  
(paid hotel AP)



\*.zone.myspecialdns.com



Just an example:

*query = TXT R0VUIC8gSFRUUC8xLjEK.zone.myspecialdns.com*  
*answer = TXT "SFRUUC8xLjEgMjAwIE9LCg=="*

After base64 conversion:

*query = "GET / HTTP/1.1"*  
*answer = "HTTP/1.1 200 OK"*

Realization: iodine + tun/tap device

latest release: 2010

How to filter?

Limit your DNS response to A/AAAA/MX/SRV

How to avoid filtering?

Encapsulate answers to A/AAAA