kaos.theory security research presents:

Anonym.OS

Because no one needs to know

Who We Are

- kaos.theory: loose-knit group of security professionals, hackers, artists and general lunatics

Show and Tell

- Anonym.OS is:
  - An OpenBSD 3.8 live CD
  - A secure environment, usable by anyone, that provides a full suite of applications configured to run anonymously and over encrypted channels
  - Easy enough for your mum...
    assuming she has something to hide

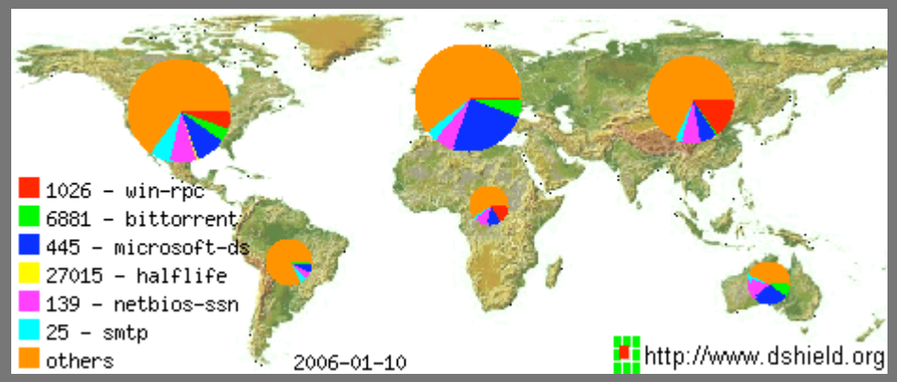
What It Isn't

- An auditor / pen-testing / haxx0ring toolkit
- Anonym.OS does not have:
  - Port scanners
  - Vulnerability scanners
  - Exploit collections
  - Password crackers
  - Forensic tools
  - Office suite

Why?

The Environment Today

- Hostile: adware, malware, spyware
- Insecure: apps, OSs, networks, protocols
- Heightened monitoring by governments and corporate interests

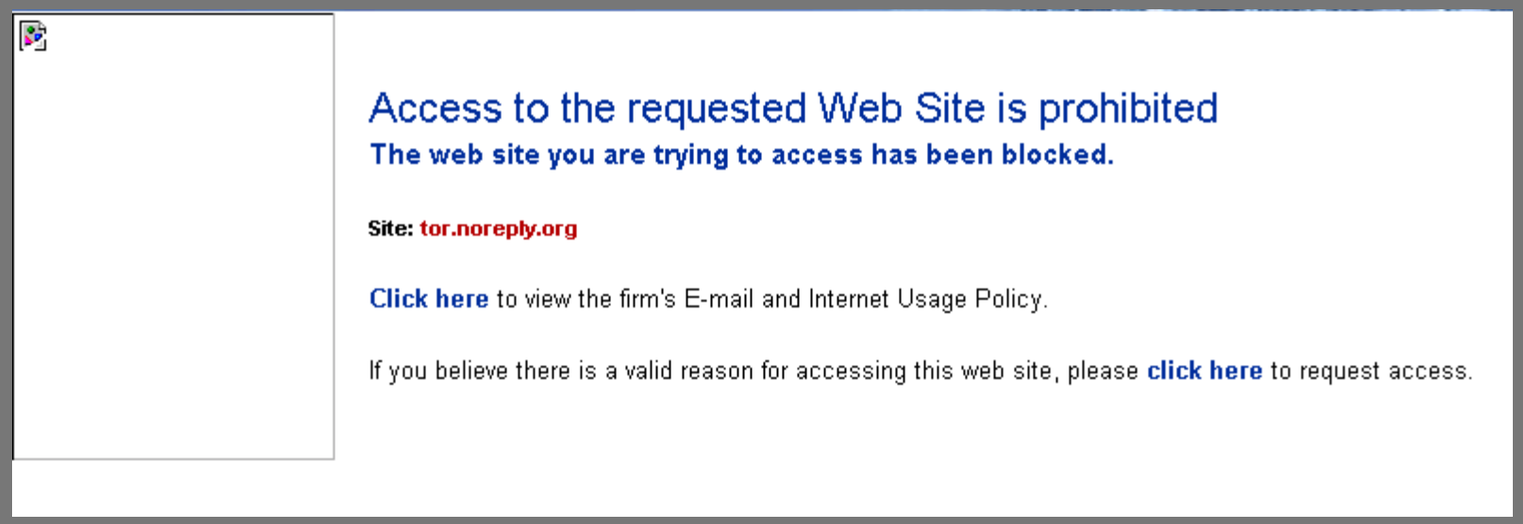


but...

- also the place where alot of people:
  - communicate
  - create
  - buy and sell
  - share
  - work and play
- speaking of work.....

Annoying Proxies

- While trying to research for this presentation...



Access to the requested Web Site is prohibited

The web site you are trying to access has been blocked.

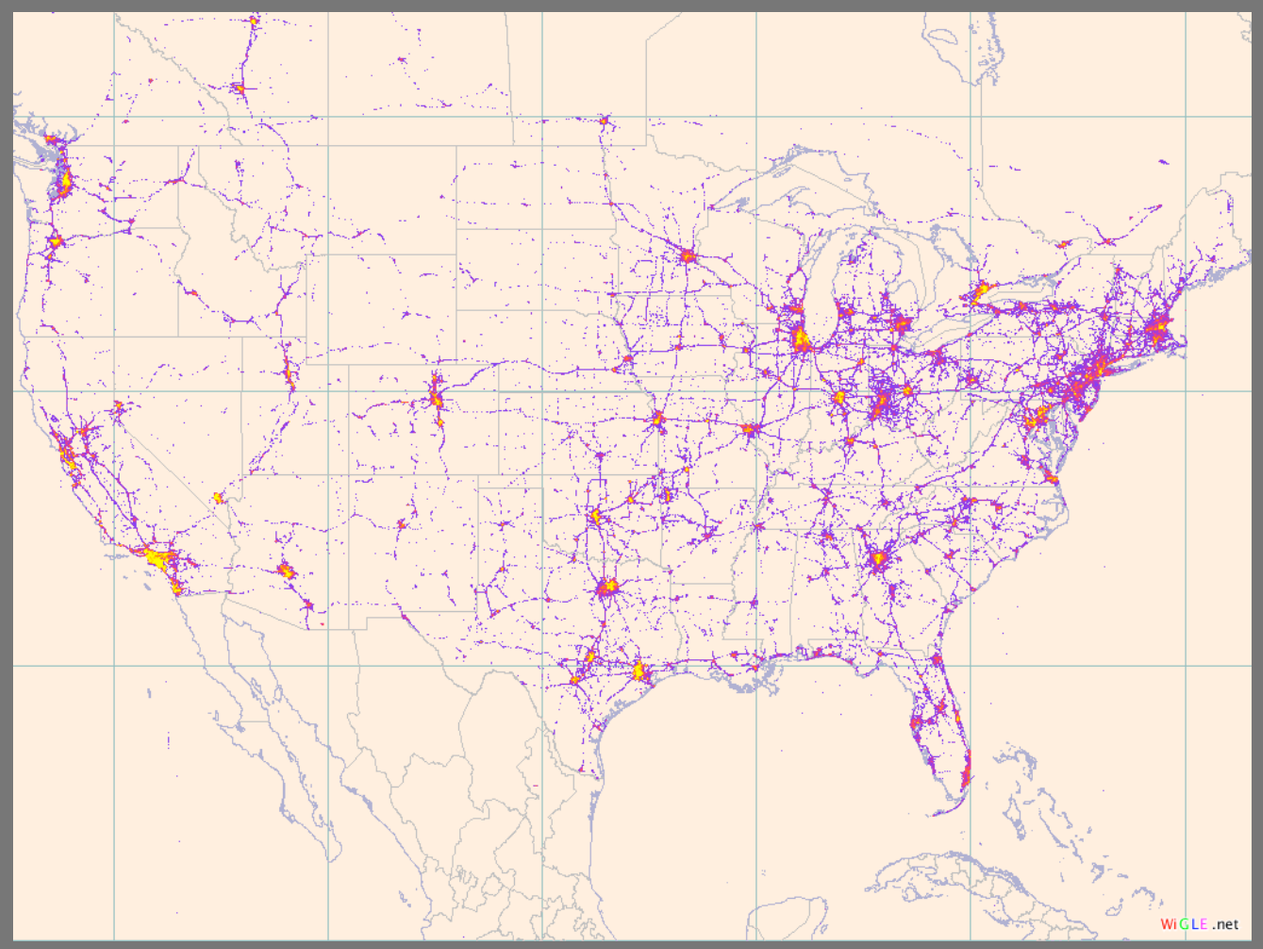
Site: tor.noreply.org

Click here to view the firm's E-mail and Internet Usage Policy.

If you believe there is a valid reason for accessing this web site, please **click here** to request access.

More Networks

- The proliferation of very convenient but dubiously secured networks



You don't have to wear a tinfoil hat any more to be worried about privacy

- activists, organizers and dissenters
- "Persons of Interest" under scrutiny from fascist regimes
- Wage slaves (and executives) on corporate networks
- people who buy stuff
- your mom
- her mom

Investigation Tool

- Privacy is as useful to a federal agent as it is to an average citizen who wants to protect their own privacy
- Provides the ability to investigate child porn, identity theft, terrorism without raising alarms or scattering originating IPs in the bad guys logs

Good! ....except...

- Maintaining anonymity is becoming a difficult thing to do
- Many tools exist to assist the savvy user in remaining anonymous...

Configuration Overload!

- But what about a normal user faced with multiple manual configurations?

```
ctionsfile
==========

ies:

e actions file(s) to use

f value:

le name, relative to confdir, without the .action suffix

t values:
```

```
hostname, turn on network
starting network'
/netstart

x /usr/local/bin/tor ]; then
  echo -n ' tor';
  /usr/local/bin/tor --runasdaemon 1


x /usr/local/sbin/privoxy ]; then
  echo -n ' privoxy';
  /usr/local/sbin/privoxy --user _privoxy._privoxy \
          /etc/privoxy/config


x /usr/local/sbin/tor-dns-proxy.py ]; then
  echo -n ' tor-dns-proxy';
  /usr/local/sbin/tor-dns-proxy.py
```

```
#
## See the man page, or http://tor.eff.org/tor-manual.html, for more
## options you can use in this file.
#
# On Unix, Tor will look for this file in someplace like "~/.tor/torrc" or
# "/etc/torrc"
#
# On Windows, Tor will look for the configuration file in someplace like
# "Application Data\tor\torrc" or "Application Data\<username>\tor\torrc"
#
# With the default Mac OS X installer, Tor will look in ~/.tor/torrc or
# /Library/Tor/torrc


## Replace this with "SocksPort 0" if you plan to run Tor only as a
## server, and not make any local application connections yourself.
SocksPort 9050 # what port to open for local application connections
SocksBindAddress 127.0.0.1 # accept connections only from localhost
#SocksBindAddress 192.168.0.1:9100 # listen on a chosen IP/port too
```

```
    REDIRECT_TO = os.devnull
else:
    REDIRECT_TO = "/dev/null"

class DNSHandler:
    def handle_dns(self, buf):
        dns = dpkt.dns.DNS(buf)
        name = dns.qd[0].name
```

How?

Design Goals

- Must be an inherently-secure system
- Must be able to bypass restrictive filters without user interaction
- Must be as “quiet” as possible on a network; no “chatty” protocols like SMB or NTP
- Must help ensure confidentiality and integrity without additional configuration
- *Must be easy to use!*

Tools Available:

- Anonymizing networks:
  - Tor
  - JAP
  - I2P
  - Morphmix / Tarzan
  - Freenet
  - Entropy
- Local web proxies
  - Privoxy
  - Junkbuster
  - RabbIT
  - WebCleaner

Building the Anonym.OS

- Start with a minimal base OS
- Harden the host
- Institute strong ingress and egress filtering
- Perform onion routing
- Utilize anonymizing proxies
- Use encrypted protocols wherever possible
- Provide GUI and CLI applications to accomplish typical tasks

Securing the Host

- Which operating system? OpenBSD!
  - Secure by default
  - Hasn't been done before (at least not well)
  - Using OpenBSD makes you k-rad 1337
- Modified TCP behaviors to fool passive OS fingerprinting

Ingress / Egress Filtering

- All incoming and outgoing packets are managed by pf (packet filter)
- Anonym.OS blocks *all* inbound and outbound traffic by default, with the exception of the following outbound:
  - ‘Anonymized’ and encrypted
  - TCP: 80, 443, 9001, 9030, 9090, 9091

Included Major Apps

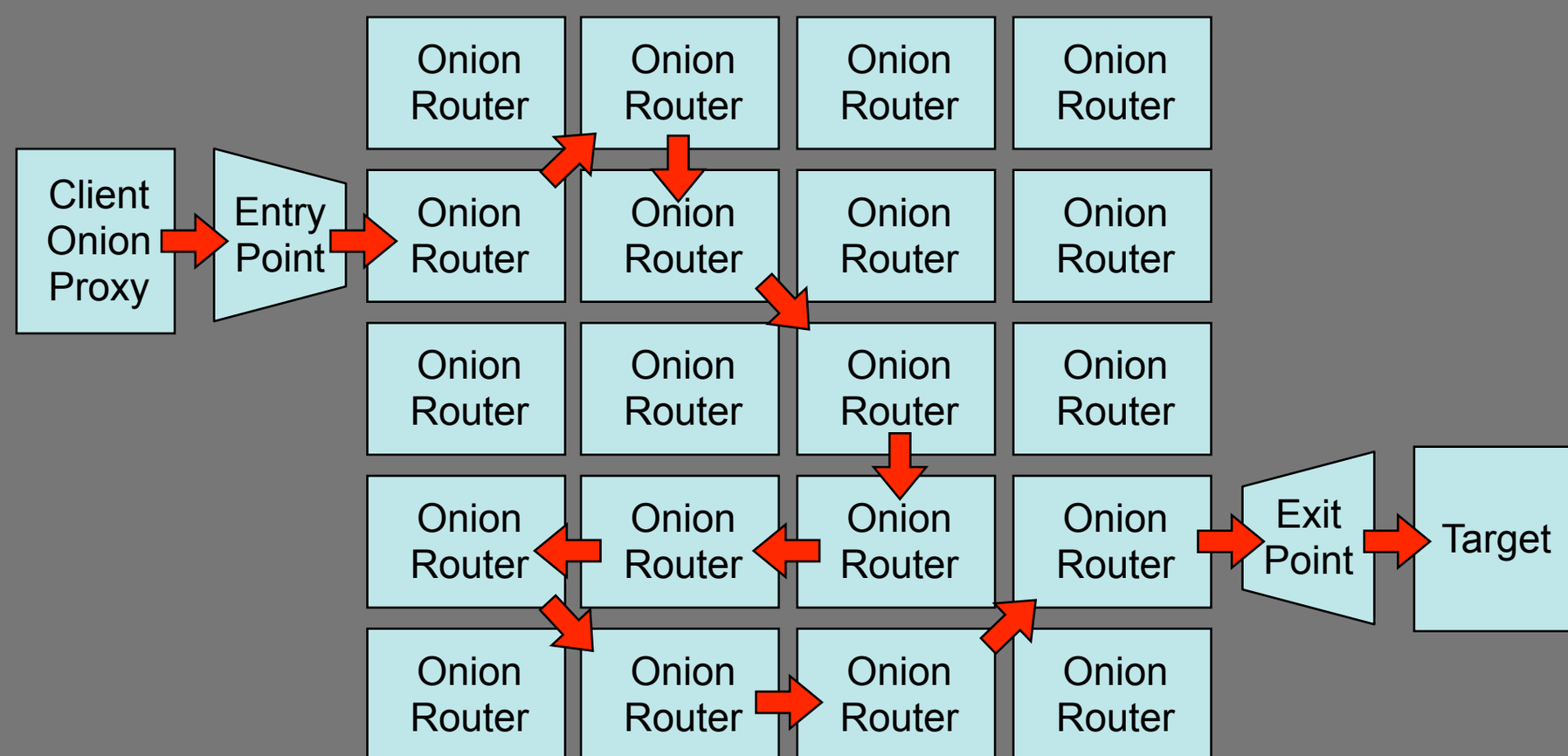
- Graphical:
  - Xorg 6.8.2
  - Fluxbox 0.9.13
  - Firefox 1.0.6
  - Thunderbird 1.0.7
  - Gaim 1.5.0

Command Line:

- Links .99
- Mutt 1.4.2i
- GPG 1.4.1
- SSH 4.2
- Vim 6.3.85

Onion Routing

- Accomplished using Tor 0.1.0.14



Local Proxy

- Privoxy 3.03 - local web browsing proxy
- Works to connect between SOCKS (Tor) and non-SOCKS (http clients)
- Configured to block:
  - User agent*
  - Referrers
  - Client operating system and host variables

Encrypted Protocols

- Most clients natively support encrypted protocls and SOCKS proxies, thus HTTPS, IMAPS, POPS, SSMTP
- dsocks pushes non-SOCKS aware applications over SOCKS proxies (example: FTP over Tor)
- Anonym.OS thus automagically “socksifies” all non-SOCKS aware clients and protocols, including DNS

What’s Next?

Issues

- Tor can be, umm, slow
- OpenBSD is not optimized for live CD usage
- Distribution is not small

Roadmap

- Optimizing performance:
  - Speed
  - Compressed file system
- Run Tor (alpha) inside a chroot
- Boot from / save settings to a USB stick
- Install to local HD
- Mounting local file systems automatically (NTFS, EXT2 hard drives)

Roadmap (cont.)

- Packaged emulator version (QEMU)
- More boot-time automation (i.e. brain-dead mode)
- Automatic evasion of egress filtering (Tunneling over DNS, ICMP)
- Anti-phishing mechanisms

What you can do!

- Run a Tor server!
- Contribute to Tor and the EFF!
  (we wouldn't refuse donations either)
- Use encrypted protocols!
  (Our tor servers have exit policies that only allow:
  22, 443, 993, 995, 465)
- Internationalization / translation help
- Tell us what you want to see!

Worst. Idea. Ever.

(Live Demo)

Blame:

- fade
- ~elmore~
- arcon
- dr. kaos
- digunix
- beth
- atlas

Questions?

If you liked this... you'll love what's comin' next