Boîtier matériel Tor

Pourquoi ? Comment ?

@aeris, 30 juin 2016, PSES/HSF

BY NC SA

Aeris

Groupe cyber-terroriste individuel auto-radicalisé sur Internet

Mail / Jabber :
aeris@imirhil.fr
GNU/Social :
https://status.imirhil.fr/

Blog : https://blog.imirhil.fr/
Conférences :
https://confs.imirhil.fr/

GPG : EFB7 4277 ECE4 E222
OTR : 5769 616D 2D3D AC72

Devops chez Cozy Cloud

Sommaire

1. Pourquoi ?
2. Comment ?
3. Questions

Le besoin existe-t-il ? (1/2)

- Anonabox (585.549$ ><)
- Sever
- Veiltower
- TorFi
- Cloak
- Dark Ingress
- Wemagin
- Kiri
- …

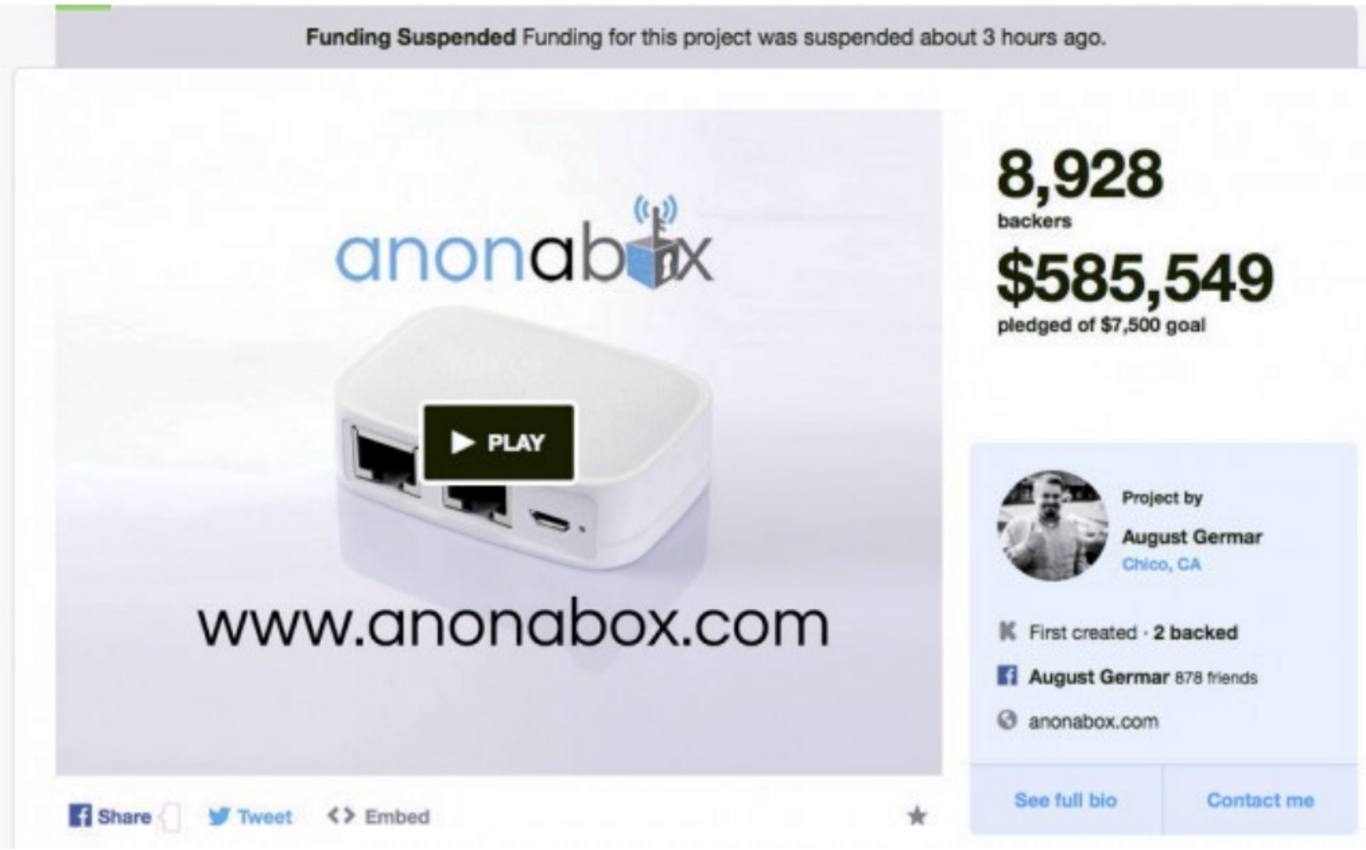
Le besoin existe-t-il ? (1/2)

- Anonabox (585.549$ ><)
- Sever
- Veiltower
- TorFi
- Cloak
- Dark Ingress
- Wemagin
- Kiri
- …

Apparemment, oui… Mais pas de bol, **snake oil**…

Now Everyone Wants to Sell You a Magical Anonymity Router. Choose Wisely.
https://www.wired.com/2014/10/anonymity-routers/

Le besoin existe-t-il ? (2/2)



Le besoin existe-t-il ? (2/2)

Sever is your Anonymity restored! It's a Peer to Peer Network that goes far beyond the capabilities of TOR and provides you with optimized throughput for up to 10X your current internet speed.

Le besoin existe-t-il ? (2/2)

Les manques actuels (1/3)

- Pour le web, Tor Browser
- Pour la messagerie instantanée, Tor Messenger
- En déplacement, Tails
- Qubes OS / Subgraph OS

Les manques actuels (1/3)

- Pour le web, Tor Browser
- Pour la messagerie instantanée, Tor Messenger
- En déplacement, Tails
- Qubes OS / Subgraph OS

Mais pour le reste ?

- SSH ? (I Hunt Sysadmin)
- Mail ?
- Clients réseaux sociaux ?
- Tout ce qui se connecte à Internet en général
- Un invité à la maison ?

Les manques actuels (1/3)

- Pour le web, Tor Browser
- Pour la messagerie instantanée, Tor Messenger
- En déplacement, Tails
- Qubes OS / Subgraph OS

Mais pour le reste ?

- SSH ? (I Hunt Sysadmin)
- Mail ?
- Clients réseaux sociaux ?
- Tout ce qui se connecte à Internet en général
- Un invité à la maison ?

Pas de système « plug & forget »…

Les manques actuels (2/3)

- Tor Browser/Messenger = 1 client Tor par application
  - Bientôt 10/20/30 clients Tor sur une seule machine ?
  - Du travail en cours pour mutualiser, mais compliqué

- Mauvais support proxy SOCKS5 (voire inexistant)
  - ZNC : pas de support
  - SSH : compliqué
  - Généralement, configuration manuelle

```
Host *.onion
        ProxyCommand nc.openbsd -X 5 -x 127.0.0.1:9050 %h %p
```

- **Risque de leaks** (DNS…)

Les manques actuels (3/3)

- Pas vraiment très grand public
  - Tails
    - Persistence pas complète, au cas par cas
  - QubesOS/SubgraphOS
    - Fonctionnalités sécuritaires mais limitantes
      - Copier/coller
      - Partage de fichiers

- Pas forcément envie d'avoir X machines à configurer
  - Celles des autres
  - Celles qu'on ne contrôle pas (invités)

Les manques actuels (3/3)

- Pas vraiment très grand public
  - Tails
    - Persistence pas complète, au cas par cas
  - QubesOS/SubgraphOS
    - Fonctionnalités sécuritaires mais limitantes
      - Copier/coller
      - Partage de fichiers

- Pas forcément envie d'avoir X machines à configurer
  - Celles des autres
  - Celles qu'on ne contrôle pas (invités)

En bref, Tor **partout et pour tous**, « c'est compliqué » ™

Comment ?

Un **routeur** qui envoie **tout** son trafic via **Tor**

Ce qui ne peut pas passer (UDP, IPv6…) est **bloqué**.

Aucune exception.

Les problèmes (1/2)

- **Mises-à-jour** logicielles possibles (Tor, OpenSSL, OS…)
  - Exit les systèmes BSP à flasher (OpenWRT, Yocto…)
  - Idéalement, distribution GNU/Linux standard (Debian…)

- **Tor dans du Tor** à éviter
  - Mais Tor Browser à privilégier pour le web
  - Liste des nœuds Tor disponible

- UDP non disponible
  - Pas de DNS
    - Support minimal via Tor (A/AAAA & MX)
  - Pas de NTP
    - Matériel sans RTC :'(

Les problèmes (2/2)

- Support des fonctionnalités de Tor
  - Proxy SOCKS5
  - Usage de ponts
- Facilité d’utilisation
  - Design / UX

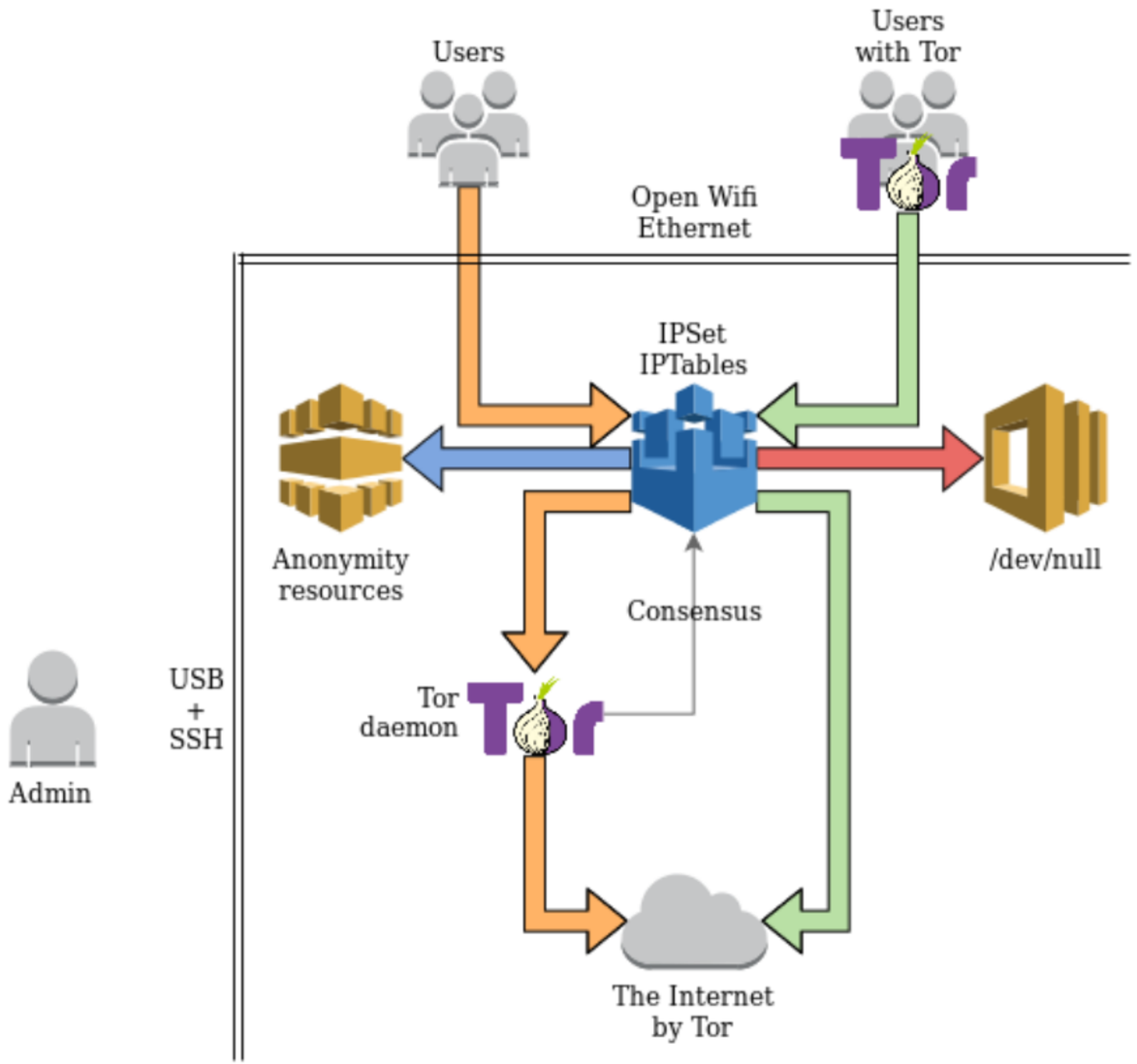
Mise-en-œuvre

Projet OnionBox https://github.com/aeris/onionbox/

- Basé sur une carte Olimex A20 OLinuXino LIME
- Noyau vanilla 4.4
- Distribution Debian Jessie

- Usage de stem pour la gestion de Tor
- Iptables & Ipset pour la gestion du pare-feu
  - Détecte aussi le trafic déjà torréfié

- Réglage de l'horloge
  - Analyse des logs Tor pour réglage grossier
  - Passage via HTPdate dès connexion Tor réussie


Users
Users
with Tor
Open Wifi
Ethernet
IPSet
IPTables
Anonymity
resources
/dev/null
Consensus
USB
+
SSH
Tor
daemon
Admin
The Internet
by Tor

Reste à faire

- Gestion du wifi
- Une UX propre pour la gestion de Tor
  - tor-arm / vidalia, version web
- Embarquer des logiciels/doc Tor/anonymat/protection
  - Tor Browser / Tails
  - Guide d'auto-défense numérique
  - Manuel RSF
  - …
- Et gérer la mise-à-jour des ressources
- Modèle de distribution à définir

Contributors needed !

Questions ?

(Merci à Lunar, jvoisin et les autres pour la relecture !)