Evadiendo la censura por diez pavos

USANDO TOR EN MODO GUERRILLA

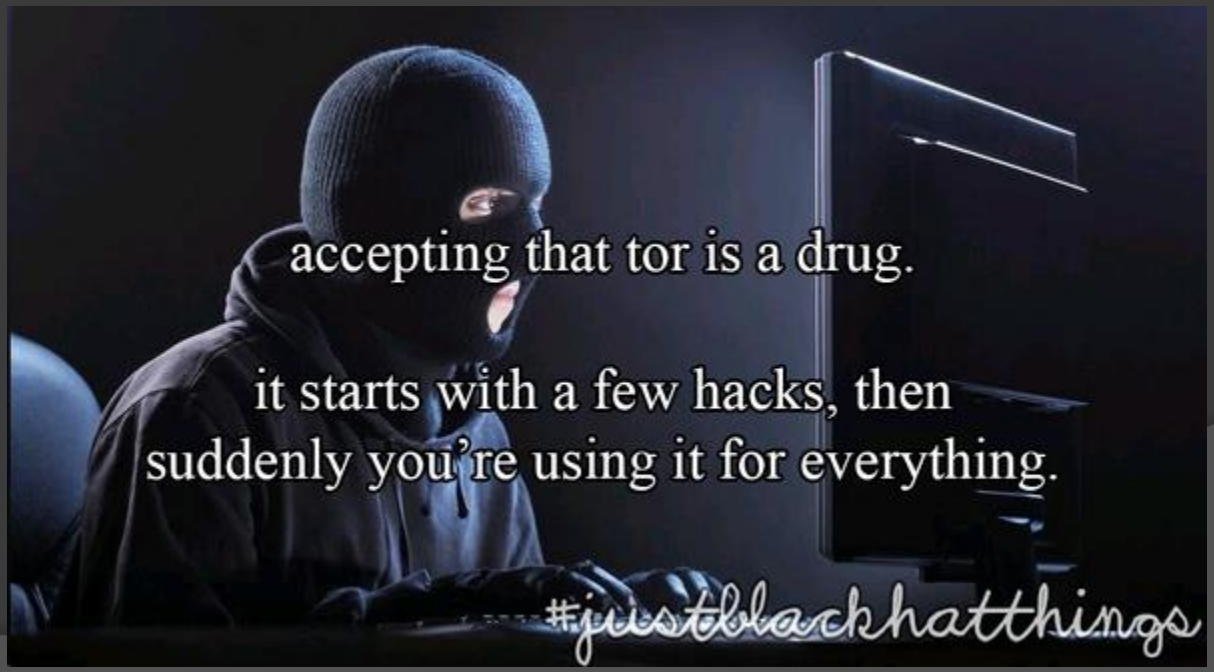
Venimos a hablar de nuestro libro

Para los que han visto esta charla antes…

- Release 1.0 de la herramienta
  - Ahora funciona!
  - En serio!
  - Lo prometemos!
  - Esta vez es de verdad!
  - Y no sólo en nuestra máquina!

Vamos a ocultar nuestra IP...

- VPN/proxy implica confiar en un tercero
  - Y la mayoría están mal configuradas…
- Tor implica confiar en los nodos de salida
  - Esto se arregla con nuestros propios nodos



Seattle police raid home of privacy activists who maintain Tor anonymity network node

By Mary-Ann Russson

March 31, 2016 19:02 BST

techdirt

Techdirt | Wireless News | Innovation | Case Studies | Startups | Net Neutrality | Techdirt Deals!

Main | Submit a Story | RSS

PODCAST Techdirt - The Link Between Credit And Surveillance SOUNDCLOUD

<< Citizens On Terrorist Watchlist - Including A... | Sony Finally Releases PS4 Remote Play For PC... >>

Law Enforcement Raids Another Tor Exit Node Because It Still Believes An IP Address Is A Person

from the *TASE-THAT-ROUTER* dept

(Mis)Uses of

An IP address is **not a person**, even less so if said IP address traces back to a Tor exit relay. But that's not going to stop the "authorities" from subjecting people with no knowledge at all of alleged

nd searches.

unch of **computer equipment** from a residence

rward with nothing more than an IP address -- seized

running a Tor exit relay.

upon information and belief" affidavit statements

ation" and recommended law enforcement check

conducting raids based on IP addresses. ICE,

take, no matter what information was brought to its

on nothing more than an IP address -- at least not

Seattle PD conducting a child porn investigation.

Sure enough, investigators had traced the activity back to an IP address, which was all the probable cause it needed to **show up at privacy activist David Robinson's home at 6 a.m. and demand access to his computers**

the grugq

@thegrugq

Following

Ran Tor exit node out of residence. Police showed up with a warrant. Sad this still happens, but that's police logic

Nuestra idea

- Armar nodos de Tor **descartables**:
  - Es nuestra máquina, no la de un tercero
  - Sólo se usarían un breve período (OPSEC)
  - Sin comprar hosting
    - Se podría rastrear a tu tarjeta de crédito
  - ¡Debe ser barato!
    - Sobre todo si queremos ***muchos***
  - Debe usar infraestructura de red pública
    - Porque sino es delito…

Ok, todo muy lindo, pero...

Qué ~~maldades~~ podemos hacer con esto?

- Poner nodos de salida propios (VPN/SSH)
- Almacenamiento anónimo
  - Jirafeau: como Megaupload, pero de pobres ☺
- Comunicaciones seguras
  - IRC, para los old sch00l
    - Si hay huevos… BBS!
  - Esas mierdas nuevas para los jóvenes, como XMPP

¿Podemos confiar en Tor?

- Ehhmmm… no. Pero no hace falta:
  - Controlamos los nodos de salida ☺
  - Usando OpenVPN se evitan ciertos fallos criptográficos y de análisis de tráfico
  - Aquí el tiempo es nuestro aliado…
  - ¡Pero nada reemplaza una buena OPSEC!

Conectándose a Internet

- Muchas ciudades tienen Wi-Fi público
  - Parques, buses, trenes…
- Dependiendo de la legislación local, puedes llegar a conectarte a Wi-Fi no público si no está protegido con clave, o en espacios semipúblicos (como bares)
- El problema no es técnico, sino humano
  - ¡Consulta con tu abogado favorito!

Conectándose a Internet

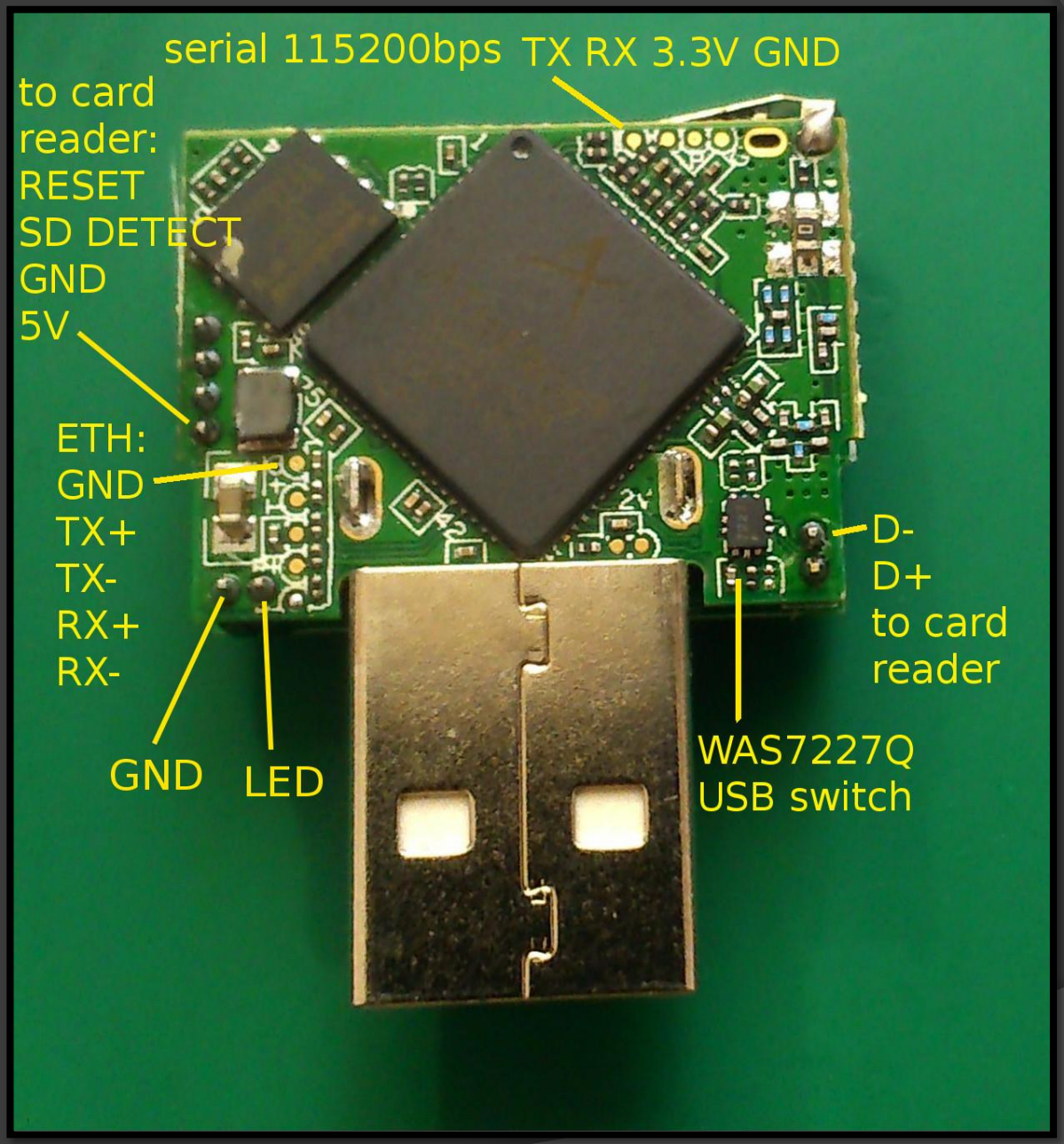
Conectándose a Internet

COMTREND
Multi-DSL CPE

- Device Info
  - Summary
  - WAN
  - Statistics
  - Route
  - ARP
  - DHCP
- Advanced Setup
- Wireless
- Diagnostics
- Management

Lucass-MacBook	18:ff:0f:30:34:aa	100.100.100.104	2 days, 17 hours, 10 minutes, 13 seconds
android-047h6319764j0yaw	00:25:9e:da:b8:74	100.100.100.105	2 days, 17 hours, 43 minutes, 39 seconds
Annas-MacBook	18:ff:0f:2b:21:61	100.100.100.106	2 days, 17 hours, 55 minutes, 17 seconds
hostname	0c:82:68:ee:7f:3e	100.100.100.107	2 days, 21 hours, 46 minutes, 5 seconds
android-02feqr1uw2j7jq9j	58:3f:54:b5:30:55	100.100.100.109	2 days, 19 hours, 18 minutes, 45 seconds
android-qn23oj1i48f9m567	f8:3d:ff:89:5b:e3	100.100.100.110	2 days, 19 hours, 27 minutes, 12 seconds
android-p091n709kqi90om6	ac:e2:15:7a:8a:7e	100.100.100.111	2 days, 19 hours, 43 minutes, 51 seconds
Islas-iPhone	00:f4:b9:44:4a:c7	100.100.100.112	2 days, 19 hours, 55 minutes, 17 seconds
Jazmin-Notebook	00:10:18:b4:cb:09	100.100.100.113	2 days, 20 hours, 45 minutes, 55 seconds
Kaspars-MacBook	18:ff:0f:8a:c1:53	100.100.100.114	2 days, 20 hours, 53 minutes, 26 seconds
android-e1tlq04mo8411ae4	00:25:9e:81:61:50	100.100.100.115	2 days, 21 hours, 23 minutes, 33 seconds
android-5d2pfrgim3dj8u0b	58:3f:54:ac:ad:a1	100.100.100.116	2 days, 21 hours, 41 minutes, 57 seconds
William-Laptop	5c:51:4f:75:54:55	100.100.100.117	2 days, 21 hours, 47 minutes, 28 seconds
android-0474pg35t6th3hj7	f8:95:c7:d9:41:07	100.100.100.118	2 days, 21 hours, 54 minutes, 28 seconds
Harry-Computer	00:10:18:8b:85:6c	100.100.100.119	2 days, 21 hours, 56 minutes, 22 seconds
Maksims-MacBook	18:ff:0f:88:c9:4e	100.100.100.120	2 days, 23 hours, 51 minutes, 33 seconds
Emilys-iPhone	00:f4:b9:3c:c2:5e	100.100.100.121	2 days, 23 hours, 58 minutes, 7 seconds

El hardware: ZSUN



Fuente: https://wiki.hackerspace.pl/projects:zsun-wifi-card-reader


zsun
4GB
Kingston

El hardware: ZSUN

- Compacto, barato, soporta MicroSD
- MIPS, 16 MB ROM, 64 MB RAM

- Precios (aproximados):
  - ~8 € – ZSUN WiFi SD Card Reader
  - ~10 € – Waterproof Solar Power Bank
  - ~3 € – USB Charger
  - ~1 € – MicroSD

OpenWrt Happy Hacker Edition

- Fork de OpenWrt con parches de Hackerspace.pl porque el “oficial” fallaba mucho en nuestras pruebas
- Sistema propio de builds, nos permite:
  - Tener un entorno aislado de compilación
  - Aplicar parches al código fuente
  - Cambiar configuraciones por default al vuelo
  - Sistema propio de paquetes (“componentes”)

OpenWrt Happy Hacker Edition

- Certificados para SSL/SSH/VPN/Tor autogenerados con cada compilación
- Permite configurar las WiFi a las que se conecta y los hidden service que provee

- Haces git clone y funciona ☺

OpenWrt Happy Hacker Edition

- Se puede conectar a varias redes Wi-Fi al mismo tiempo, por si una se cae
  - …aunque a Tor no le gusta mucho eso ☹
- Cada conexión tiene una “identidad” nueva, con hostnames y MAC al azar ***realistas***
- Todos estos features son configurables y se pueden deshabilitar en cada build

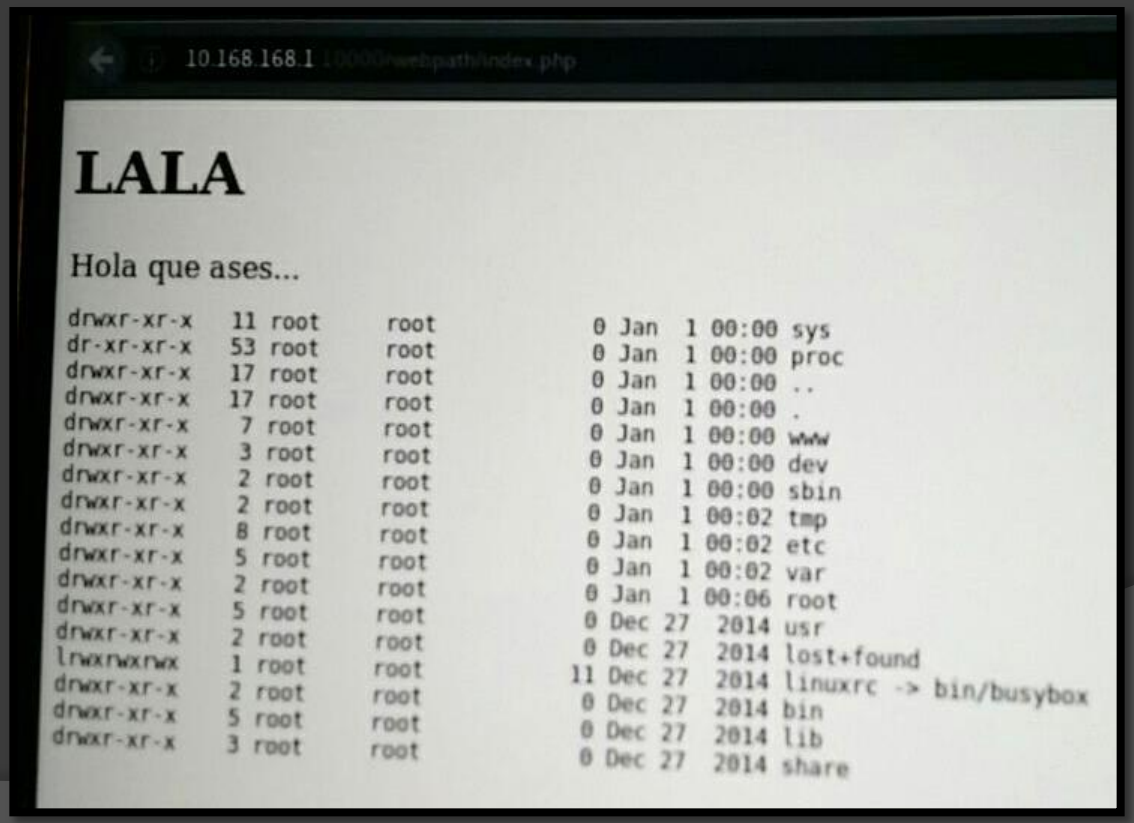
Método 1 de flasheo:

- El firmware original viene con “premio”

```
$ socat - TCP4:10.168.168.1:11880
??????!????
(none) login: root
root
Password: zsun1188

Welcome to
          -------      |            /    /--/         ___       |
           /           |           /|     \/         _____    --|--|
          /_____\      |---       --|--   //--/      /         /  |
           __|__       |           /|\    / \/      /___\     /   |
          ___|___   ___|____      / | \     /                /   \|
                                深圳至上移动科技有限公司
                                Shenzhen Zsun Cloud Technology Co., LTD.
                                www.zsuncloud.com

BusyBox v1.01 (2014.12.27-02:50+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ #
```

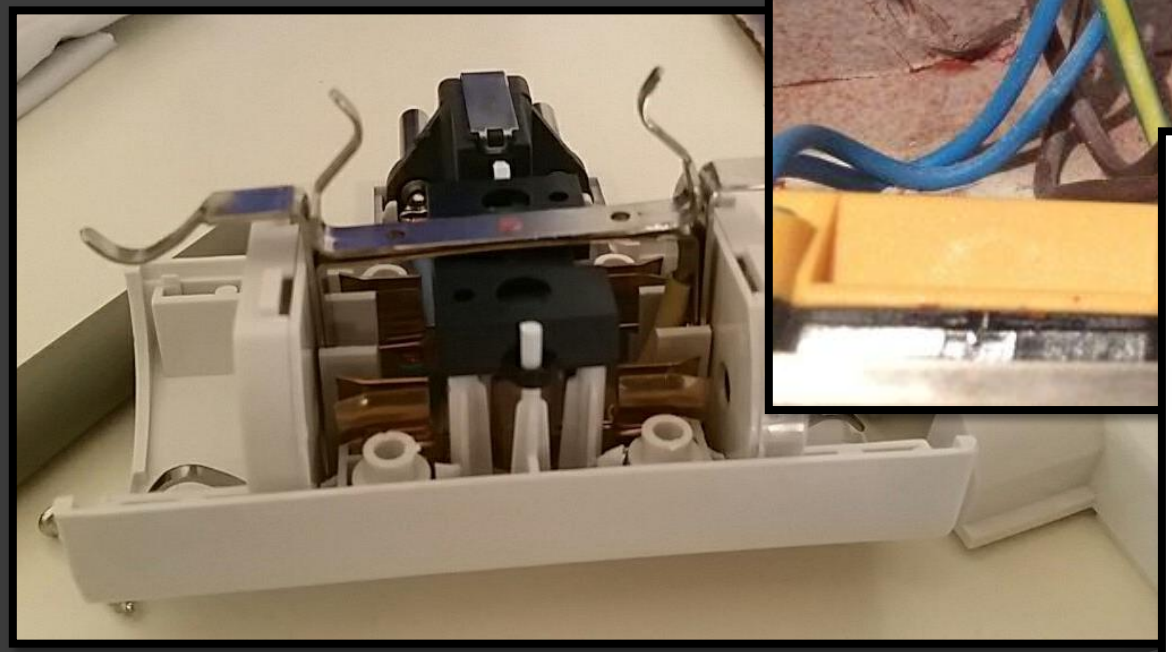
Método 2 de flasheo:

La aplicación web tiene un bug que permite subir un .php a la MicroSD y ejecutarlo (!)



Deployment

¡Sé creativo! ☺



Demo time!

¡Y ahora sóis todos TARGET!