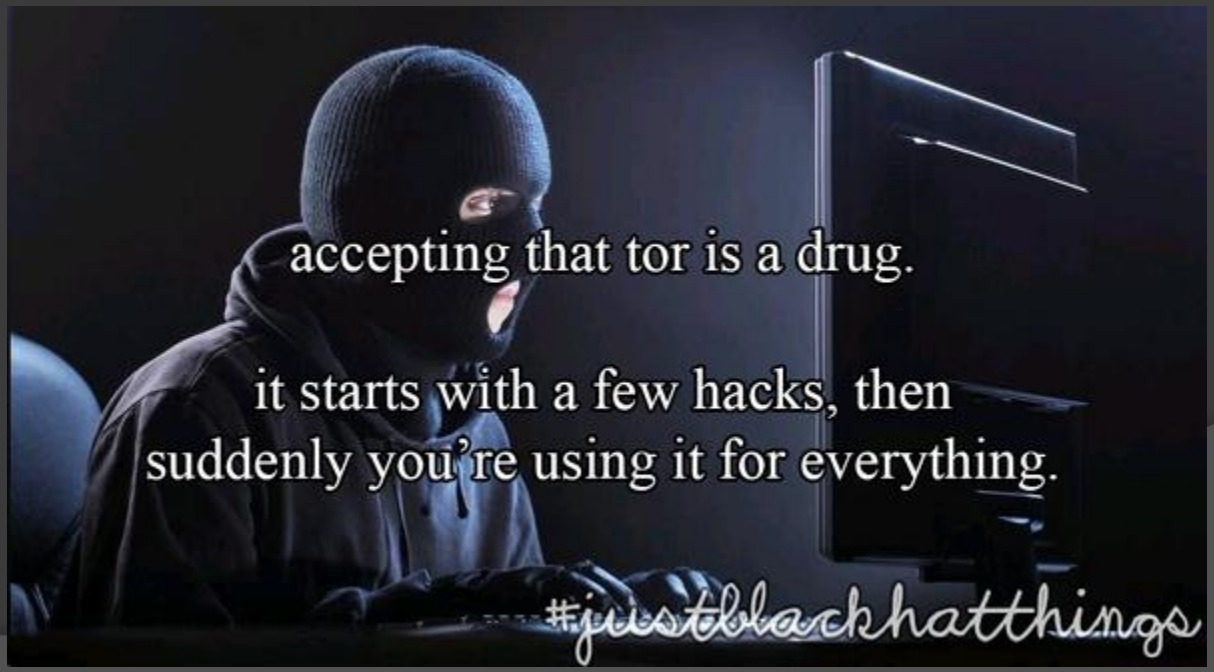
Evadiendo la censura por veinte pavos

USANDO TOR EN MODO GUERRILLA

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!
    - Si fuéramos ricos no estaríamos en Madrid sino en una playa en las Bahamas ☺
  - Debe usar infraestructura de red pública
    - Porque sino es delito…

¿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!

Primer prototipo: TL-WR703N

Problemas

- Un poco grande y llamativo
  - Difícil de ocultar en lugares públicos
- Necesita alimentación externa
- Trae sólo 8 Mb de ROM
  - Cabe una imagen de OpenWRT mínima con Tor, pero nada más
- Necesita un pincho USB si queremos almacenamiento extra

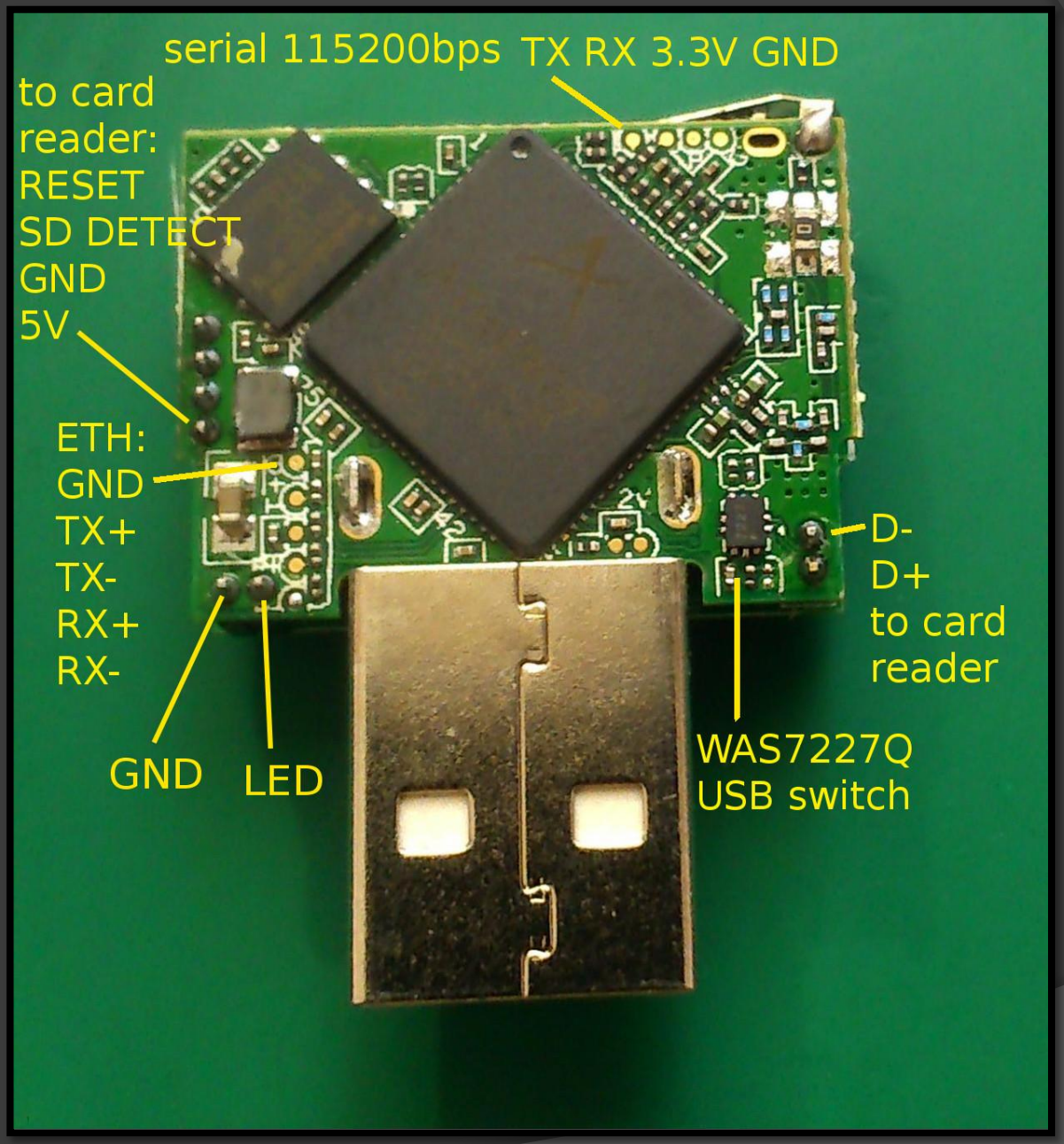
Segundo prototipo: ZSUN

Ventajas

- ¡Más barato que el TP-LINK! ☺
- Mucho, mucho, mucho más compacto
- Trae el ***doble*** de RAM y ROM
- Alimentación desde el puerto USB
- Soporta MicroSD para el almacenamiento externo
- El hardware es fácil de modificar
- Ya lo investigó la gente de ***hackerspace.pl***


zsun
4GB
Kingston


TRAVELADAPTER
Адаптер питания
MODEL NO./МОДЕЛЬ:ART-U90EWE
INPUT/TEG LISTRIK/ВХОД:
100-240V~FREKUENSI 50-60Hz 0.35A
OUTPUT/ВЫХОД : 5.0V⎓2.0A
SIN, Серийный номер: RT1C915CS/B-E
Дата производства: 27.03.2014Z
MADE IN CHINA/ СДЕЛАНО В КИТАЕ
AB10 KZO.02.0072
zsun



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

Consiguiendo el hardware

- Compramos los prototipos por Internet en DealExtreme
  - Pero para ser realmente anónimo no sirve
  - Se puede pedir al fabricante en China

- Precios (aproximados):
  - ~15 € – ZSUN WiFi SD Card Reader
  - ~10 € – Waterproof Solar Power Bank
  - ~4 € – MicroSD & USB Charger

Cambiando el firmware

- Porque el 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.

~ #
```

Compilando OpenWRT

- La gente de Hackerspace.pl ya preparó un parche de kernel para este hardware
  - Era para un kernel viejo, pero lo portamos a versiones más nuevas (3.18.29, 4.1 y 4.4)
- El código fuente de OpenWRT debe ser compilado con Ubuntu
  - Pero tenemos dignidad… :P
  - ¡Vagrant al rescate!

Compilando OpenWRT

- Usando Vagrant, creamos una VM con Ubuntu
  - Todas las dependencias y el código fuente se descargan automáticamente
- Un Makefile automatiza la compilación en paralelo de varias imágenes
  - Soporte para aplicar parches, instalar software adicional y modificar ficheros de configuración
  - Certificados para SSL/SSH/VPN/Tor autogenerados con cada compilación
- Haces git clone y funciona ☺

Compilando OpenWRT

```
~/happyhacker/vagrant-happyhacker$ make help

To build all targets just type:
    make all

To list the available targets:
    make list

To build a specific target:
    make bin/<target>

To clean the build files (but not the VM or output files):
    make clean

To completely clean up everything (including the VM and output files):
    make dirclean

To begin preparing a new firmware image from scratch:
    make menuconfig

To modify the configuration for an existing target firmware image:
    make menuconfig CONFIG=<target>

Vagrant VM control:
    make up
    make suspend
    make destroy

~/happyhacker/vagrant-happyhacker$
```

Compilando OpenWRT


```
~/happyhacker/vagrant-happyhacker$ ls
bin  config  Makefile  patches  README.md  script  src  TODO.md  Vagrantfile
~/happyhacker/vagrant-happyhacker$ make list

The following targets are available:

$ make bin/x86-torrorist
$ make bin/zsun-debug
$ make bin/zsun-extboot
$ make bin/zsun-torrorist

~/happyhacker/vagrant-happyhacker$ make bin/zsun-debug
Bringing machine 'openwrt-happyhacker-build-vm' up with 'virtualbox' provider...
==> openwrt-happyhacker-build-vm: VirtualBox VM is already running.
--------------------------------------------------------------------
BUILDING FIRMWARE IMAGE FOR TARGET: zsun-debug
--------------------------------------------------------------------
‘/vagrant/src/common/files/’ -> ‘./files/’
‘/vagrant/src/common/files/etc’ -> ‘./files/etc’
‘/vagrant/src/common/files/etc/banner’ -> ‘./files/etc/banner’
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:280: space before tab in indent.
        {"w25x10"},     {"w25x20"},     {"w25x40"},     {"w25x80"},
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:281: space before tab in indent.
        {"w25x16"},     {"w25x32"},     {"w25q32"},     {"w25q32dw"},
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:282: space before tab in indent.
```

Compilando OpenWRT


```
bin/{target}/*                  This is where the output files will be written

config/{target}/config          OpenWRT makefile configuration, this is mandatory
config/{target}/sources         List of components to be included in this target
config/{target}/patches         List of patches to be applied on this target

config/{target}/files/*         Files to be included directly in the device filesystem
config/{target}/initialize.sh   Initialization script for this target
config/{target}/finish.sh       Post build customization script for this target

src/{component}/files/*         Files to be included directly in the device filesystem
src/{component}/initialize.sh   Initialization script for this component
src/{component}/finish.sh       Post build customization script for this component

patches/{patch}.diff            Diff-style patch for the OpenWRT source code to be applied
```

Fase 2: “el torrorista” ☺

- Tor con hidden services
  - OpenVPN para transformarlo en un “nodo de salida” privado y más seguro que Tor
- Esto tiene muchos más usos
  - Jiraffeau (clon de Megaupload)
  - Otras ideas:
    - IRC/XMPP para un chat seguro
    - Murmur (Mumble) para voz sobre IP segura

Conectándose a Internet

- Esta es realmente la parte más difícil
- Una primera idea: módems 4G
  - Dan una velocidad suficientemente buena
  - Se puede conectar desde cualquier sitio
  - Algunos países como Irlanda no piden documentos cuando compras una SIM
- Problema: ¡el 4G es muy caro! ☹
  - Pero si tienes el dinero, esta opción vale

Conectándose a Internet

- Otra idea: Internet de acceso público
  - Muchas ciudades tienen Wi-Fi público
  - 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 ya no es técnico… es humano
  - ¡Consulta con tu abogado favorito!

Connecting to the Internet

Usando el Wi-Fi Manager

- Creamos nuestro Wi-Fi Manager
  - Se puede conectar a varias redes Wi-Fi al mismo tiempo, por si una se cae
  - Cada conexión tiene una “identidad” nueva, con hostnames y MAC al azar ***realistas***
  - Se integra con UCI, el sistema de configuración de OpenWRT
  - Modular y muy configurable
    - Pero sin ser complejo de usar

Usando el Wi-Fi Manager

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

Aún queda por hacer...

- Más hardenización:
  - OpenWRT no se presta mucho a la labor de montar un entorno seguro…
    - Todas las medidas contra exploiting están deshabilitadas por defecto
    - Soporta contenedores LXC…
      ¡pero no los usa!
    - Todo corre como root ☹

Aún queda por hacer...

- Estamos desarrollando una forma de arrancar OpenWRT directo de la SD
  - ¡No es tan fácil como parece! No tenemos una BIOS que haga todo el “trabajo sucio” como pasa en un x86 ☹
  - Nuestra idea es hacer un remount del rootfs y cargar un kernel nuevo con kexec, pero aún quedan problemas que resolver
  - La ventaja para el usuario: no hace falta cambiar el firmware, sólo la tarjeta SD ☺

Aún queda por hacer...

- Usos más complejos de LXC
  - Usar contenedores para aislar cada servicio
    - En caso de 0day, el servicio queda aislado
    - También se gana en estabilidad
  - Deployment de contenedores sobre Tor
    - Contenedores volátiles – al apagar el dispositivo se eliminarían los datos
    - Mayor resistencia a un análisis forense
    - Cloud modo: guerrilla ☺

¡Y ahora sóis todos TARGET!