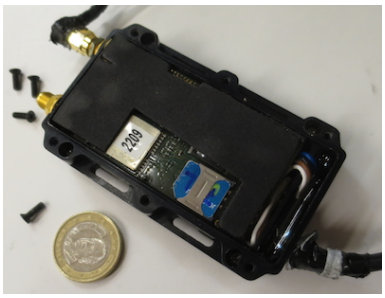
https://info.nodo50.org/Desempaquetando-el-vergonzoso.html

Desempaquetando el vergonzoso rastreador del CTF

- Noticias - Noticias Destacadas -



Publication date: Lunes 23 de marzo de 2015

El 4 de marzo de 2015, un dispositivo de seguimiento fue encontrado en el interior del paso de rueda de un coche de una asistente al Circumvention Tech Festival en Valencia. Solo unas pocas fotografías del dispositivo están disponibles públicamente (en 1 y 2). Las marcas de los componentes del dispositivo de rastreo estaban tapadas con pegotes de resina epoxi negra sobre los chips.

<dl class='spip_document_21338 spip_documents spip_documents_left' style='float:left;'> <a href='https://info.nodo50.org/IMG/jpg/gps-01.jpg' title='El dispositivo desmontado' type="image/jpeg"> [https://info.nodo50.org/local/cache-vignettes/L275xH207/gps-01-428bc-2e1e4.jpg] **El dispositivo desmontado** <dl class='spip_document_21339 spip_documents spip_documents_right' style='float:right;'> <a href='https://info.nodo50.org/IMG/jpg/gps-02.jpg' title='El dispositivo desmontado' type="image/jpeg"> [https://info.nodo50.org/local/cache-vignettes/L275xH207/gps-02-f1b92-77ec4.jpg] **El dispositivo desmontado** <a href='https://info.nodo50.org/IMG/jpg/gps-03.jpg' title='El dispositivo colocado en el vehículo' type="image/jpeg"> [https://info.nodo50.org/local/cache-vignettes/L207xH275/gps-03-27ec8-57665.jpg] **El dispositivo colocado en el vehículo**

Después de revisar las imágenes y estudiar los circuitos se pueden extraer las siguientes conclusiones:

¿Qué contiene el circuito?
El circuito se compone de cuatro bloques funcionales: (a) un regulador de voltaje, (b) un módem GSM/GPRS de Wavecom/Sierra Wireless, (c) un receptor GPS de U-blox y (d) un microcontrolador (MCU) posíblemente de Renesas. El circuito tiene dos antenas separadas para interactuar con el operador de telefonía móvil (Movistar) y con los satélites GPS.

¿Es un sistema de última generación?
No, a juzgar por el tipo de componentes que se incluyen en el rastreador, creo es bastante antiguo (5-7 años) ya que el nivel de integración de circuitos de GPS/GSM disponible en los últimos años en el mercado es mucho mayor. Por ejemplo, no incluye una antena combo GSM/GPRS o chips que integran GPS con GPRS como el GE864-GPS.

¿Se necesitan un grupo de baterias tan grande?
Aunque el microcontrolador incluido en el dispositivo tiene un bajo consumo de energía y funcionalidades de "modo en espera", hoy hay un montón de mejores alternativas de bajo consumo. Esto me hace creer que el dispositivo no fue originalmente diseñado para ser conectado a una batería pequeña. Otras alternativas como las basadas en procesadors ARM Cortex de 32-bits son mucho m[a comunes.

¿Qué hacen esas baterías de litio?
Las dos baterías de litio presentes en la placa proporcionan energía para los Relojes en Tiempo Real (RTC) del módulo GPS (U-blox Neo) y para el microcontrolador. El gran tamaño de una de las baterías (CR2032) puede indicar la presencia de algún sistema de detección de desconexión del pack de baterías que arrancaría alguna rutina para borrar todos los datos de la unidad.

¿Cómo se configura el dispositivo?
El dispositivo carece de una interfaz para programar la unidad. Dicha programación podría tener lugar a través de SMS o enviando comandos a la unidad a través de GPRS. El tipo de diseño indica que el dispositivo está diseñado para ser reutilizado y probablemente recogido por personal diferente al que lo instaló.

¿Es un sistema convencional?

No, se ha puesto cierto esfuerzo en ocultar los elementos tecnológicos utilizados para prevenir la ingenieria inversa y aunque los componentes se pueden encontrar en el mercado de componentes tradicional, el tipo de integración y el uso de un controlador más avanzado me hacen pensar que el rastreador es un diseño especificamente adaptado y vendido para el rastreo "no oficial" de vehículos.
<dl class='spip_document_21341 spip_documents spip_documents_left' style='float:left;'> <a href='https://info.nodo50.org/IMG/jpg/gps-04.jpg' title='Vista trasera del ratreador' type="image/jpeg">
[https://info.nodo50.org/local/cache-vignettes/L275xH207/gps-04-e362d-7d033.jpg] **Vista trasera del ratreador** <dl class='spip_document_21342 spip_documents spip_documents_right' style='float:right;'> <a href='https://info.nodo50.org/IMG/png/gps-05.png' title='Vista frontal del rastreador' type="image/png">
[https://info.nodo50.org/local/cache-vignettes/L275xH207/gps-05-49945-5525d.png] **Vista frontal del rastreador**

Bloques funcionales

La placa se compone de cuatro partes principales.

(a) Alimentación eléctrica
La unidad se alimenta con cuatro pilas tamaño D (o baterías IEC R20). Las cuatro baterías se conectan en serie para proporcionar 6 voltios a la placa. El componente amarillo marcado como "447 6V" es un condensador de tantalio TAJD447K006.

Hay dos baterías incluidas en la placa. Las dos baterías de litio (CR2016/2032) proporcionan 3-3.6 voltios al reloj de tiempo real (RTC) del GPS y del microcontrolador (MCU). La pequeña batería redonda permite, en caso de pérdida de potencia, mantener almacenada en la memoria interna del módulo GPS la última posición registrada. El uso de una batería externa conectada al microcontrolador ofrece la posibilidad de detectar una desconexión de las baterías.

(b) Módem GSM/GPRS
La conexión a la red de telefonía móvil se realiza mediante un módulo de control GSM/GPRS Wavecom/Sierra Wireless AirPrime (modelo número Q2687RD). El módem que proporciona acceso a la red móvil es cuatribanda y puede operar en 850, 900, 1800 y 1900 Mhz. La tarjeta SIM es de Movistar, el principal operador español de telefonía móvil, propiedad de Telefónica S.A. El módem isa la red 2G (GPRS).

La placa de este módem no tiene las etiquetas que habitualmente se incluyen y que informan del IMEI.
<a href='https://info.nodo50.org/IMG/png/gps-06.png' title='Módem GPRS Wavecom' type="image/png">
[https://info.nodo50.org/local/cache-vignettes/L275xH196/gps-06-40ef0-669e6.png] **Módem GPRS Wavecom**

La antena GSM/GPRS es un simple monopolo (cable) conectado al conector SMA externo.

(c) Módem GPS
El tercer bloque funcional es un receptor GPS. El receptor obtiene la localización via GPS y envía dicha información a otro punto mediante la red de telefonía móvil. Es circutito es receptor GPS U-blox, probablemente de la serie NEO 6.
<a href='https://info.nodo50.org/IMG/jpg/gps-08.jpg' title='Receptor GPS U-blox' type="image/jpeg">
[https://info.nodo50.org/local/cache-vignettes/L275xH243/gps-08-0c653-3359f.jpg] **Receptor GPS U-blox**

La placa incluye el receptor GPS U-blox sin la etiqueta.

El receptor no incluye una antena integrada. Los GPS portátiles normalmente incluyen una antena cerámica (como la de la imagen) o una antena externa de alta ganancia. En vez de eso el GPS está conectado a una antena externa con base magnética.

<a href='https://info.nodo50.org/IMG/png/gps-07.png' title='Tradicional antena cerámica GPS' type="image/png">[https://info.nodo50.org/local/cache-vignettes/L259xH194/gps-07-427cd-5df5e.png] **Tradicional antena cerámica GPS**

(d) Microcontrolador (MCU)
El cuarto bloque funcional es el microcontrolador (MCU), la CPU del rastreador. La MCU es responsable de interconectar el receptor GPS y el módem GPRS. Es difícil determinar el fabricante de la MCU sin tener acceso físico al dispositivo, pero sabemos que la MCU tiene 120 pines y que tiene un encapsulado Thin Quad Flat Pack (TQFP). Esta forma y encapsulado coincide con las MCU fabricadas por Renesas.

En este mismo bloque también podemos encontrar una memoria flash NAND de 32 pines.

Rtr, 16 de marzo de 2015
rtr@nodo50.org

Mas información

[-] La Directa, 05/03/2015: Una activista de Barcelona localitza un dispositiu de rastreig GPS amagat al parafang del seu cotxe
[-] Jacob Appelbaum, 06/03/2015: Fotos del dispositivo
[-] Eldiario.es, 08/03/2015: Cómo es el dispositivo rastreador que pusieron a la activista que fue a un congreso de privacidad
[-] Ara.cat, 12/03/2015: La història de l'espia britànic i de l'activista barcelonina que va trobar un GPS al cotxe
[-] La Directa, 15/03/2015: Entrevistem 'Lily', de 37 anys, ciutadana britànica que, l'any 2010, va descobrir que un infiltrat havia estat la seva parella sentimental. Des d'aleshores, s'ha implicat a fons en la lluita pel dret a la privacitat
[-] La Directa, 15/03/2015: Un infiltrat de la policia britànica va passar per centres socials de Barcelona i Reus

English version: Un-boxing the infamous CTF location tracker

<a href='https://info.nodo50.org/IMG/pdf/gps_infamous_tracker_by_rtr_v2.pdf' title='PDF - 390.9 KB' type="application/pdf">[https://info.nodo50.org/local/cache-vignettes/L52xH52/pdf-39070.png] **Un-boxing the infamous CTF location tracker (PDF, 400 Kb)**