

¿Piensas en si un día te roban el portátil?

Fuente: Blog de Vicente Navarro Jover

URL: <http://www.vicente-navarro.com/blog/2007/12/26/piensas-en-si-un-dia-te-roban-el-portatil/>

Fecha de Publicación: 26-12-2007

Los ordenadores portátiles, cada día más ligeros y móviles ellos, son un caramelo muy apetitoso para los “amigos de lo ajeno”. Y a menudo los solemos llevar con nosotros en lugares en los que éstos abundan: estaciones, aeropuertos, oficinas, hoteles, cafeterías... Conozco de primera mano casos de oficinas en los que el propio guardia de seguridad de la empresa se dedicaba a “tomar prestados” durante la noche los portátiles de los empleados que se los dejaban allí de un día a otro incluso con el [Kesington lock](#) puesto. Por la mañana los usuarios llegaban y sólo encontraban un trozo de cable de acero colgando de la mesa. Por supuesto, lo descubrieron, pero los portátiles ya no aparecieron. También conozco otro caso de alguien que se dejó el portátil con un importante trabajo de varios meses a punto de finalizar dentro de la caja fuerte de un hotel que fue fácilmente forzada en un rato que él se encontraba fuera de la habitación. Los casos de maletines de portátiles robados en aeropuertos o en coches aparcados ya ni siquiera son anécdota.

La motivación de un ladrón será mayormente económica y en la inmensa mayoría de los casos no buscará específicamente *nuestro* portátil, ya que muchas veces será un efecto colateral de un robo más amplio (robo en una vivienda, en un coche, del equipaje durante un viaje...). Sin embargo, también puede darse el caso de que nuestro portátil haya desaparecido por motivos relacionados con la información que contiene.

Posibles móviles del robo de un portátil:

- Económico, por el valor del portátil
- Porque alguien quiere tener la información que hay en él
- Porque alguien no quiere que tengamos la información que hay en él

Asimismo, a nosotros, como propietarios del portátil nos puede perjudicar el robo de un portátil por motivos más o menos asociados:

- Por su valor económico
- Por su valor en tiempo invertido en elegirlo, comprarlo, configurarlo a medida, conocerlo
- Por el valor de la información que contiene de la que no tenemos copia de seguridad en ningún otro sitio
- Por la importancia de la información que contiene que, aunque la tenemos copiada en otro sitio no queremos que caiga en otras manos
- Por nuestro derecho a la privacidad, ya que aunque no contiene nada importante no queremos que nadie curioseé entre nuestras cosas

De todo lo anterior, lo más fácil de prevenir es evitar perder la información haciendo copias de seguridad tan frecuentemente como importante sea lo almacenado. Nunca se puede insistir suficientemente en la importancia de hacer copias de seguridad cuando es tan sencillo como copiar los ficheros a otro sistema o dispositivo externo al portátil. Resulta evidente que si hacemos un backup en una memoria USB que solemos llevar con el portátil, no habremos ganado nada en caso de robo. Por tanto, las copias de seguridad han de ser en un medio de almacenamiento físicamente independiente del portátil. El [rsync](#) es una herramienta excelente para hacer copias de seguridad en remoto consumiendo la cantidad mínima de ancho de banda posible. Está disponible para todos los sistemas UNIX, así como para Windows como parte de Cygwin.

Si tenemos copia de seguridad, lo siguiente que nos ha de preocupar es en qué manos van a caer los datos de nuestro portátil. Es posible que en él almacenemos información sumamente privada y confidencial de nuestra empresa o de nuestros asuntos particulares, pero también es posible que tengamos simplemente correos, fotos, la declaración de la renta, hojas de cálculo con nuestras cuentas domésticas o, en definitiva, multitud de documentos que, en mayor o menor medida, no quisiéramos que fueran visibles a ojos diferentes a los nuestros.

Hay muchas soluciones enfocadas a prevenir el acceso al sistema operativo instalado en el sistema y que ya vienen a menudo en los portátiles con orientación empresarial, como lectores de huellas digitales o lectores de tarjetas [Smart Card](#). Sin embargo, si el atacante tiene acceso físico al sistema, nada le impide sacar el disco duro y leerlo en otro sistema o, simplemente arrancar con otro sistema operativo (p.e. con un Knoppix desde el lector de CD/DVD) y acceder fácilmente a los datos del disco local.

Para impedir que alguien arranque nuestro portátil con otro sistema operativo es importante al menos poner una contraseña de arranque y de BIOS. En los ordenadores de sobremesa la contraseña se suele poder eliminar fácilmente reseteando la BIOS, pero en los portátiles modernos, aunque también tienen una pila de botón para mantener la hora y la configuración de la BIOS, la contraseña no se puede eliminar reseteando la BIOS. Los fabricantes se dejan una puerta de atrás para desbloquear el portátil en caso de pérdida de la contraseña, pero requieren la factura de compra antes de realizar tal operación. También, muchos de los portátiles empresariales actuales llevan un chip [TPM](#) que, entre otras funciones, se puede usar para solicitar una contraseña de arranque del sistema.

Si hemos conseguido evitar que el ladrón del portátil entre al sistema operativo y que ni tan siquiera logre pasar de la BIOS al encender la máquina, no podemos evitar que saque el disco duro y trate de usarlo en otro sistema. Para evitar que obtenga información de él, la solución pasa por cifrar la información sensible que almacenemos o usar una contraseña de disco duro, algo que ya llevan muchos portátiles actualmente (HP, por ejemplo, lo llama [DriveLock](#)). Una contraseña de disco duro es la medida más sencilla que

podemos adoptar para prevenir que el atacante no pueda usar el disco duro, ya que la contraseña (realmente hay dos, una de usuario y otra de administrador o *master*) se almacenará en el *firmware* del disco y si no es introducida, el disco duro sencillamente no arrancará. Esto no previene ataques más agresivos como cambiarle la controladora integrada del disco por otra compatible y sin contraseña o como dispositivos hardware precisamente para saltar esta protección, como el [VOGON Password Cracking POD](#), pero al menos ya detiene a los atacantes meramente curiosos que no estén buscando algo específico y muy importante en nuestro sistema.

Si la importancia de los datos es muy alta, es absolutamente obligatorio cifrar los datos del disco (algo muy recomendable a hacer también en memorias y discos USB), ya que nada de lo anterior llegará a prevenir que un atacante realmente empeñado acceda a la información. Windows lleva por defecto [EFS](#) para NTFS, y [BitLocker](#) (que hace uso de chips TPM) en ciertas versiones de Windows Vista. [Para Linux tenemos muchos sistemas de cifrado del sistema de ficheros](#), como el [EncFS](#), el [CFS](#) o el [CryptoFS](#). Sin embargo, como en muchos casos el sistema de ficheros a cifrar debería ser accesible desde cualquier sistema operativo y a ser posible con un algoritmo bien conocido que no ponga nuestros datos en manos de un fabricante, yo opino que hay que huir tanto como nos sea posible de cualquier solución propietaria, cerrada o ceñida a un único sistema operativo. Por ello me gusta la solución de cifrar de forma transparente para el SO el disco desde la BIOS (en los últimos portátiles haciendo uso del chip TPM, si está disponible), y me gusta aún más el [TrueCrypt](#), que funciona de forma extraordinaria tanto en Windows (con versión portable) como en Linux permitiendo crear discos duros virtuales cifrados con la información privada de nuestro entorno. Desafortunadamente, TrueCrypt, aunque es de código abierto, tiene una licencia con ciertas restricciones que no permite ser empaquetado en Debian.

Por otra parte, si en el caso de robo de un portátil queremos tener alguna posibilidad de recuperarlo, inspirándonos en [la noticia aparecida hace unos meses del ladrón que se hizo una foto con la webcam integrada y que se subió automáticamente a Internet](#), podemos implementar una solución similar usando DynDNS.

[DynDNS](#) es una empresa que permite asociar hostnames/dominios en el DNS de Internet a nodos con una IP dinámica que cambia frecuentemente. Para ello, la máquina monitoriza su propia IP y cuando cambia le pide al servidor de DynDNS que modifique los registros del servidor DNS asociado. Esto permite, entre otras cosas, ofrecer servicios de Internet desde máquinas conectadas a Internet con ISPs que sólo ofrecen IPs dinámicas. DynDNS vive de vender dominios y asociarlos a IPs dinámicas, pero también ofrece [una serie de dominios](#) (p.e. homelinux.org, dyndns.org o homeip.net) en los que es gratis tener hasta 5 hostnames registrados. Hay otras empresas que dan este servicio, como [no-ip.com](#), pero sin duda alguna, DynDNS es la más conocida y, en mi opinión, el servicio que dan es de gran calidad.

Pues bien, la idea es que el ladrón encienda el portátil robado y cometa la imprudencia de conectarlo a Internet. El cliente de DynDNS se conectará a los servidores de DynDNS y actualizará la IP para el hostname que hayamos asociado a la máquina. Nosotros, simplemente mirando a qué resuelve dicha IP y viendo si cambia, podremos estar al tanto de si alguien se ha conectado a Internet con nuestro portátil y desde qué IP. Con dicha información, el paso siguiente es ir con una factura de compra en la que aparezca el número de serie del portátil y la IP obtenida a la comisaría más cercana a poner una denuncia. Si la policía hace bien su trabajo, contactará con el ISP asociado a la IP para pedirle información sobre quién ha tenido dicha IP en el día tal a la hora cual. El ISP debería ser capaz de asociar una IP en un instante de tiempo con una localización física. El problema que podemos tener es que la conexión se haya hecho, no desde un hogar, sino desde un lugar público como un hotel, un Ciber Café o una red WiFi pública. Esa es la teoría pero, ¿funcionará en la práctica? ¿se tomará la policía la molestia de contactar con el ISP por recuperar un portátil valorado en algo más o algo menos de 1000€?

Como mínimo, aunque no podamos recuperar el portátil, siempre podríamos haber tenido la precaución de dejar un servidor SSH abierto (en Windows lo podemos hacer con Cygwin: [Servicios en Cygwin \(syslogd, sshd, telnetd, ftpd, nfsd, etc.\)](#)) que nos permita investigar sobre quién es el ladrón o incluso para recuperar o borrar la información que podamos tener en el portátil. Si la nueva IP se registra correctamente al hostname que le hayamos asignado podríamos simplemente hacer un “ssh miportatil.dyndns.org” para entrar en el portátil... siempre que el portátil no esté tras un router que esté haciendo NAT. Al menos deberíamos haber configurado previamente el firewall integrado de Windows para que permita tráfico entrante al puerto 22.

Hay varios factores que facilitan que esto funcione:

- Que el sistema operativo por defecto sea Windows. Si sólo tenemos Linux o tenemos ambos sistemas pero el sistema por defecto es Linux, es posible que el intruso, ante el desconocimiento del sistema que se le presenta no vuelva a intentar arrancar el portátil y/o lo reinstale.
- Que se pueda entrar al sistema operativo sin contraseña (lo que implica no poner contraseña de arranque en la BIOS también). En caso contrario, el intruso tal vez sólo lo pruebe una vez y ya no lo intente más veces. Si vamos a permitir eso, **no hay que olvidar que la información sensible ha de almacenarse cifrada.**
- Tener bien configurado el sistema para que se conecte a Internet sin restricciones (por ejemplo, los firewalls personales instalados en el sistema podrían impedir la conexión del cliente de DynDNS).

En realidad, esta idea no es muy novedosa y hay multitud de aplicaciones pensadas precisamente con este fin: [Laptop tracking software](#). Sin embargo, la solución con DynDNS nos permite hacer prácticamente lo mismo sin tener que pagar una suscripción. Al fin y al cabo, tampoco podemos hacer nada sin contar con la policía.

El cliente de DynDNS oficial para Windows es el [DynDNS Updater](#). [Para sistemas Linux hay varios clientes](#), siendo el [ddclient](#) uno de los clientes más populares y de hecho, ya viene en muchas distribuciones como Debian.

El primer paso es [crear una cuenta en DynDNS](#). A continuación, vamos a [añadir nuevo hostname](#) donde elegiremos un dominio y un hostname que no estén usados (en mi caso miportatil.dyndns.org) y crearemos el dominio:

Add New Hostname

[Host Services](#)

Note: You currently don't have Account Upgrades in your account. You cannot use some of our Host Service features. Please consider buying Account upgrade that make this form full-functional and will add several other features. [Learn More...](#)

Hostname: .

Wildcard: ☒ Yes, alias "*.hostname.domain" to same settings.

Service Type: ☒ Host with IP address
☐ WebHop Redirect
☐ Offline Hostname

IP Address:
[Use auto detected IP address 83.34.128.243.](#)
TTL value is 60 seconds. [Edit TTL.](#)

Mail Routing: ☐ Yes, let me configure Email routing.

Create Host

A los pocos segundos de crear el hostname, ya podremos comprobar que su resolución funciona:

```
$ nslookup miportatil.dyndns.org
Server:      80.58.61.250
Address:     80.58.61.250#53
```

```
Non-authoritative answer:
Name:   miportatil.dyndns.org
Address: 83.34.128.243
```

y además, podemos ver en [la lista de hosts que hemos creado](#) la hora de la última actualización, dato importantísimo para nuestro propósito:

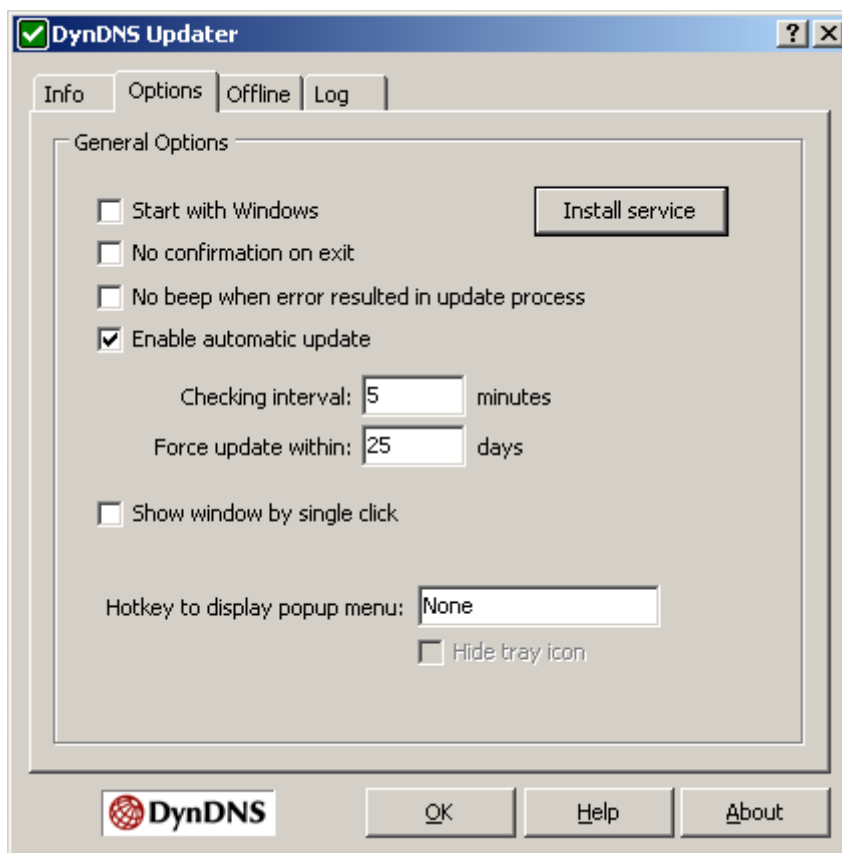
Host Services

[Add New Hostname](#) - [Host Update Logs](#)

Hostname miportatil.dyndns.org created.

Hostname	Service	Details	Last Updated
miportatil.dyndns.org	Host	83.34.128.243	24/Dec/2007 17:47

Ahora es cuestión de configurar los clientes de actualización de DynDNS. El DynDNS Updater es bastante sencillo de usar, y tenemos una buena guía de su uso en [DynDNS Updater Installation Guide](#). Para nuestro propósito, lo más importante es instalarlo como servicio de Windows, de forma que si tenemos pantalla de login, la actualización la haga incluso sin registrarnos en el sistema siempre que el portátil esté conectado a Internet.



Para usar el ddclient en Debian sólo tenemos que hacer un “apt-get install ddclient” y responder a las preguntas que nos van saliendo:

Package configuration

Configuring ddclient

Please select the dynamic DNS service you are using. If the service you use is not listed, choose "other" and you will be asked for the protocol and the server name.

Dynamic DNS service provider:

- www.dyndns.org**
- www.easydns.com
- www.dslreports.com
- www.zoneedit.com
- other

<Ok>

Package configuration

Configuring ddclient

Enter the list of fully qualified domain names for your host (like "myname.dyndns.org" if you have only one host or "myname1.dyndns.org,myname2.dyndns.org" for two hosts).

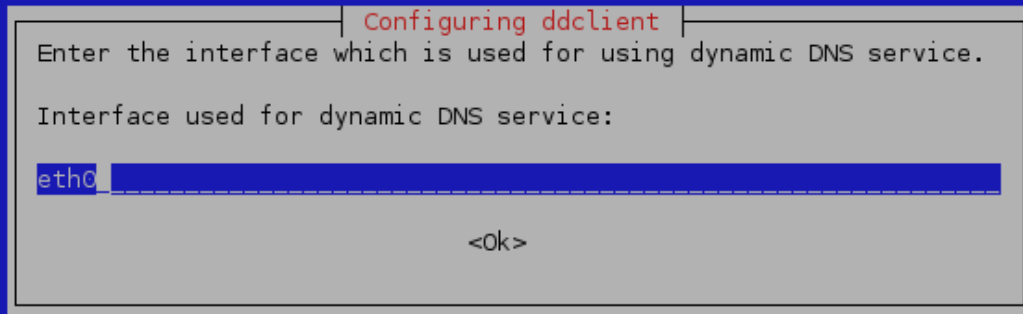
DynDNS fully qualified domain names:

miportatil.dyndns.org

<Ok>

Tras esto, introducimos el usuario y el password de DynDNS y finalmente, especificamos el interfaz conectado a Internet con una IP dinámica:

Package configuration



Configuring ddclient

Enter the interface which is used for using dynamic DNS service.

Interface used for dynamic DNS service:

eth0

<Ok>

Esto nos dejará una configuración en el /etc/ddclient.conf como esta:

```
pid=/var/run/ddclient.pid
protocol=dyndns2
use=if, if=eth0
server=members.dyndns.org
login=XXXXXX
password='XXXXXX'
miportatil.dyndns.org
```

Si el interfaz especificado no está realmente conectado a Internet sino a un router que hace NAT, tendremos que especificarle que la IP usada actualmente es la que devuelve la página web <http://checkip.dyndns.org/> cambiando la línea del use=if por esta:

```
use=web, web=checkip.dyndns.org/, web-skip='IP Address'
```

Tras esto, la máquina chequeará, cada 5 minutos (configuración del demonio en /etc/default/ddclient) la IP pública y actualizará con ella el hostname de DynDNS si ha cambiado.

Para comprobar el buen funcionamiento del cliente, nuestro mejor amigo es el comando “ddclient -v”.

Conclusiones

Con esta entrada sólo pretendo hacer reflexionar sobre qué podemos hacer de antemano pensando en si un día nos roban el portátil. En forma de resumen, aquí tenemos los pasos más importantes:

- Tener siempre backup de la información importante (por ejemplo con rsync).
- Cifrar la información sensible que almacenemos en el disco (por ejemplo con TrueCrypt).
- Leer bien la documentación del portátil para entender qué características de seguridad nos proporciona de fábrica y poder hacer un uso correcto de ellas sin correr riesgos de pérdida de datos.

Tras estos pasos fundamentales, podemos querer seguir dos caminos:

- Bloquear el acceso físico al portátil con contraseña en la BIOS para el arranque y para el disco duro.

ó

- Permitir que la máquina arranque en la esperanza de que sea conectada a Internet y por medio del cliente de DynDNS que se actualice la IP de forma que podamos, o conectarnos a la máquina, o al menos, poner una denuncia que facilite la localización efectiva de la misma.

Páginas de geolocalización de una IP

- [ARIN WHOIS Database Search](#)
- [IP2Location](#)
- [GeoBytes IP Address Locator Tool](#)
- [IP Location Finder](#)
- [IP Address Location](#)

Documentación de fabricantes sobre seguridad física de sus portátiles

- [HP ProtectTools security suite](#)
- [HP Security solutions - data security](#)
- [Dell Client Security Solutions](#)
- [Lenovo Security Solutions](#)

Enlaces a las páginas que me han sugerido la entrada

- [DynDNS Newsletter: Issue 4: Laptop LoJack](#)
- [El Catalejo: El ordenador que se la jugó a su ladrón](#)