

## La caza de los espías del P2P

### La caza de los espías del P2P.

Este artículo de investigación es la finalización del estudio realizado por la [Asociación de Internautas](#) donde se demuestra que las [redes P2P pueden ser espiadas](#) y de hecho lo son, por empresas que quieren obtener datos de forma ILEGAL. Esto ha causado bastante revuelo en la comunidad P2P pero sólo se pretendía con el artículo ayudar a los usuarios para "tener un poco más de seguridad" y perder el miedo a utilizar programas de intercambio de ficheros, pero siempre pendientes de no ser espiados por empresas sin escrúpulos que roban datos de los usuarios P2P. Algo interesante también sería que los programadores de aplicaciones de intercambio evolucionen y mejoren estos programas para que se pueda obtener una privacidad cercana al 100% para la comunidad P2P.

En este segundo artículo realizado por José María Luque miembro de la comisión de [seguridad de la Asociación de Internautas](#) se trata de dar *caza al cazador* de redes P2P quedando de paso demostrado que realmente **NOS ESPIAN de forma ILEGAL**. ¿Para qué quieren estos datos esas empresas? ¿Quieren bases de datos de los usuarios P2P? ¿Qué interés tan grande tienen para saltarse la ley de privacidad de los internautas? Muchas son las preguntas que nos surgen al comprobar que somos espiados y para las que no tenemos respuestas seguras, son estas empresas las que tienen que dar una razón de este espionaje.

En el artículo hemos contado además con la inestimable colaboración de [www.megaciudad.com](http://www.megaciudad.com), encargados de mantener actualmente los principales servidores de edonkey:  
-[SEDG](#), [Elitemusic.org](http://Elitemusic.org) & [Naiadadonkey.com](http://Naiadadonkey.com) & [descargadeprogramas.com](http://descargadeprogramas.com) y [eMuleitor](#).

Mediante una entrevista hecha a su administrador Paco quien nos contestó a todas las preguntas que le realizamos y nos ayudó bastante en este artículo, queremos agradecer su colaboración.

También tuvimos la fortuna de contar con [Manuel Alonso](#) creador y programador del programa [P2P Hazard](#) que sirve para protegerte mientras usas programas P2P.

### **-Cazar al cazador.**

Manos a la obra, nos pusimos a trabajar en el estudio de investigación, creando un fichero FALSO (Fake) con archivos de manuales de matemáticas (gratuitos), al cual pusimos un nombre que llamara la atención de algún posible "espía" que quisiera obtener datos del fichero (para generar listados de checksum) las famosas listas negras y además obtener datos de nuestra máquina;

Como se puede comprobar también creamos una web ([www.miburrito.da.ru](http://www.miburrito.da.ru)) para que fuese más real nuestro fake.

Lo compartimos en una máquina durante cinco días las 24 horas y con una aplicación llevamos un seguimiento de los paquetes que circulaban por nuestro ordenador. Transcurrido este tiempo nos dimos cuenta del fracaso en nuestro estudio puesto que los datos obtenidos resultaron ser mínimos y no valían para sacar información útil en nuestra demostración de que somos espíados.

Como Roma no se hizo en un día, no nos desanimamos y proseguimos con nuestro empeño de dar caza a los espías de redes P2P tras analizar en qué fallamos. El problema resultó estar bastante claro, tan solo teníamos una fuente para compartir y esto no atrae a nadie. Solicitamos ayuda a unos amigos que tienen algunas máquinas sin usar. Procedimos a cambiar el fichero a compartir sustituyéndolo por uno más llamativo y apetecible para cualquier usuario de P2P. Para trabajar nos prestaron 6 máquinas con conexión y dedicación exclusiva a este estudio, en las cuales instalamos la aplicación para monitorizar los paquetes de información que pasan por estos ordenadores, el nuevo fichero que compartimos que también era un FAKE con un tamaño muy pequeño de tan sólo 1,29 MB (el anterior era muy grande) al que llamamos:

La web que teníamos de señuelo ([www.miburrito.da.ru](http://www.miburrito.da.ru)) también se modificó para llevar un registro de las IPs de las máquinas que la visitaban y ver su procedencia de origen.

Ya estaba todo en marcha de nuevo y a la espera de comprobar si esta vez tendríamos algún éxito en este trabajo de investigación. Las máquinas se pusieron a compartir el fichero "trampa" (con prioridad alta) durante más de dos semanas y no se hizo mención del mismo en ningún foro ni web para comprobar si los posibles espías comprueban "nuevos" ficheros. Después de tres días empezamos a obtener datos de tres máquinas, pero las horas de los registros eran por la noche y de madrugada, tuvimos la fortuna de poder realizar capturas de los posibles espías, algunos eran usuarios del P2P. Capturas del fichero trampa,

Estadísticas de peticiones y subidas de las diferentes máquinas;

Capturas de nombre de usuarios (nicks);

Capturas de IPs de algunos usuarios;

Fuentes;

Después reunimos todas las IPs que se obtuvo de todas nuestras maquinas donde estaban el archivo fuente y quisieron acceder a la descarga de nuestro fichero trampa. Llego el momento de hacer una selección de las mismas y solo vamos a publicar algunos ejemplos;

IP; 217.128.1XX.XXX Origen Francia (Miramos algunas bases de datos pertenece a una empresa francesa que se dedica a monotorizar usuarios P2P).

IP; 81.53.2XX.XXX Origen Francia, desconocemos si pertenece alguna empresa o es un usuario P2P.

IP; 66.150.161.XXX Origen USA, Retspan.info localizada en la base de datos de PGIPDB (PeerGuardian IP DataBase).

IP; 200.68.119.XXX Origen Argentina, ¿; nos parece raro pero comprobamos que también se encuentra en la base de datos de PGIPDB (PeerGuardian IP DataBase).

IP; 217.116.XXX.XXX Origen España y haciendo un "whois" nos da; Acens Technologies, S.A no comprendemos esta IP y dudamos que se dedique a espiar pero comprobamos que en la base de datos PGIPDB viene esta información "Javier Ribas PGIPDB" no sabemos si es correcto este dato de la base PeerGuardian IP DataBase simplemente lo ponemos como anecdotia.

También encontramos en nuestro listado de IPs varias de origen algo extraños como Australia (4 intentos, incluso algunos escaneos de nuestras máquinas) y de Uruguay. Mas dos IPs que por motivos de "seguridad" no nos atrevemos a publicarlas.

Después de ver nuestros datos estamos completamente convencidos que hay mucho interés en "espiar" a los usuarios de P2P y que nuestra privacidad es violada varias veces.

#### **-Entrevistas con los expertos en P2P.**

##### **Servidores Edonkey/Emule;**

Paco de [www.megaciudad.com](http://www.megaciudad.com) y su equipo son los encargados de mantener actualmente los principales servidores de edonkey:

-[SEDG](#) Grupoelitedivx, [Elitemusic.org](http://Elitemusic.org) & [Naiadadonkey.com](http://Naiadadonkey.com) & [descargadeprogramas.com](http://descargadeprogramas.com) y [eMuleitor](#).

*AI- "Qué tipo de seguridad tenéis en vuestra máquina donde trabaja el servidor del Emule?"*

**Megaciudad-** "Están absolutamente todos los servicios desactivados. Solo tienen funcionando ssh para el control del servidor y el software de servidor."

*AI- "Tenéis sensación de que nos espían?"*

**Megaciudad-** "No solo sensación: tenemos logs. Especialmente una empresa llamada [overpeer.com](http://overpeer.com), abre decenas de clientes ficticios buscando determinados programas, obteniendo la IP de los usuarios que lo tienen."

*AI- "¿Alguna empresa os ha querido comprar el logs de IP que se conectan a vuestro servidor Emule?"*

**Megaciudad-** Nunca:

- 1.- Saben que jamás le daríamos esa información.
- 2.- No existen dichos logs (serían inmensos).

*AI- "¿Que cambiarías del Emule para tener más privacidad?"*

**Megaciudad-** Es muy complejo: sería interesante un "organismo" encargado de mantener actualizado una lista de ip's no deseadas, pero por otro lado, si esto no es una red enfocada a la ilegalidad entonces no debería existir, al no haber nada que ocultar.

**AI-** "¿Filtráis algunas IPs (listados de Ips)?"

**Megaciudad-** Sí. Pero basado en nuestras propias experiencias, no en listados estilo ipfilter.txt, que más de la mitad de las ip's que contienen son fakes y/o putadas hacia otros usuarios.

**AI-** "¿Sugieres alguna pregunta?"

**Megaciudad-** ¿Cuál piensas que es la lacra del emule actualmente?

Los clientes leechers sin duda alguna. No dan ni un kb y solo chupan de los demás. Es una pena que esa gente no haya entendido lo que es una red de igual a igual: yo te doy, tu me das. Más doy, mas recibo.

Desde los servidores, se detectan muchos de ellos conocidos y se expulsan del servidor, pero eso no vale de mucho, ya que los clientes no los detectan (culpa de los usuarios de no mantener actualizado su emule) y les envían tanto datos como intercambio fuentes, con lo que lo único que hemos hecho es "retrasar" un poco su descarga.

- ¿Qué cambiarías para mejorar?

El concepto "horde" que tiene overnet/edonkey es bastante bueno, y es también la base del funcionamiento de Bittorrent. Se trata de formar un grupo casi cerrado de usuarios que se están descargando un determinado fichero: no paran de transmitirse entre ellos partes de dicho fichero, con lo cual la descarga es rápida, en perjuicio de los ficheros más raros o menos pedidos, que no los atienden.

Cuando la gente dice que bittorrent es mas rápido, yo siempre contesto lo mismo: imagínate a los 1.800.000 usuarios de emule con solamente 100 o 200 ficheros diferentes. ¿Como iría eso? Como un tiro!!!. La gran ventaja de edonkey de su variedad de ficheros es también su lacra de cara a velocidad.

Paco, <http://www.megaciudad.com> empresa de hosting y servidores dedicados.

mail: [admin@megaciudad.com](mailto:admin@megaciudad.com)

### **P2P Hazard:**

[P2P Hazard](#) es un programa gratuito y en castellano que te protege de los "espías" bloqueando las IPs de los que quieren usurpar la privacidad de los usuarios P2P. El creador de esta maravilla de programa es [Manuel Alonso](#) que también quiso acceder a ser entrevistado.

**AI-** ¿Como se te ocurrió crear el programa P2P Hazard?

**P2P Hazard-** Hay que decir que la idea original no es mía sino de los chicos de PeerGuardian. Lamentablemente tras probar el programa, comprobar su funcionamiento, los recursos que necesitaba de la máquina y que no estaba en español decidí ponerme manos a la obra y crear algo más al alcance de todos, tanto por recursos como por idioma. Así es como nace P2P Hazard. Durante estos meses he recibido la colaboración de muchísima gente (en especial de la comunidad del conocido WinSMS) que han hecho que deje de ser más que un proyecto personal e incluso la gente de PeerGuardian colabora junto a nosotros hoy día.

**AI-** ¿Recibiste alguna presión de alguna empresa por la creación de P2P Hazard?

**P2P Hazard-** Afortunadamente aún no, de todas formas no creo que ninguna empresa se vea afectada por el uso de P2P Hazard. La funcionalidad del programa no es otra que bloquear IPs que el usuario piensa que podrían comprometer su intimidad, el hecho de compartir no conlleva a que el material compartido sea ilegal y por lo tanto no veo ninguna razón por la que empresa alguna tuviese que presionarme por ello. De todas formas no existe presión válida porque no violamos

ninguna ley, únicamente promovemos el derecho a la intimidad en las comunicaciones.

*AI- ¿Tienes sensación de ser espiados cuando estás utilizando programas P2P?*

**P2P Hazard-** Más que la sensación lo compruebo día a día y no sólo mediante el uso de P2P sino en muchísimas páginas que se nos controla mediante cookies o exploits, otro ejemplo claro son los programas que incluyen spyware. En internet existe una tendencia desmesurada a sacar la máxima información del usuario a costa del desconocimiento o extremada confianza de éste. Tenemos que concienciarnos que en Internet sólo por el hecho de estar detrás de un ordenador no somos ni anónimos ni estamos seguros y especialmente aplicarlo a las redes P2P.

*AI- ¿Que cambiarías de los P2P para tener más privacidad?*

**P2P Hazard-** Yo creo que el problema más que residir en los programas P2P reside en los protocolos que estamos utilizando actualmente así que para mi la solución está en un protocolo más seguro. Por otra parte si usáramos programas P2P basados en redes de confianza (es decir, compartir sólo con amigos y a su vez amigos de los amigos etc etc) no deberíamos preocuparnos de si estamos siendo espiados o no.

*AI- ¿Filtras algunas IPs (además de los listados PeerGuardian )?*

**P2P Hazard-** Personalmente confío en la gente de PGIPDB (PeerGuardian IP DataBase) y no bloqueo más que lo que está en la lista. De todas formas P2P Hazard incluye una opción para que los usuarios añadan cómodamente cualquier rango o IP que ellos crean oportunos. Además tanto los foros de Hazard como los de PeerGuardian están en colaboración por lo que si un usuario reporta un nuevo rango y comprobamos que es real pasa a añadirse a la lista. Hay que recordar que en esta batalla para la privacidad debemos unirnos todos y que una pequeña aportación, como mandar un simple rango por parte de un usuario, no es más que otro paso hacia nuestro objetivo.

P2P Hazard programado por Manuel Alonso.

Web, <http://www.p2phazard.com>

mail: [webmaster@p2phazard.com](mailto:webmaster@p2phazard.com)

Antes de finalizar este artículo queremos destacar a las personas que con su ayuda facilitaron llevar a cabo este estudio de investigación;

Agradecimientos muy especiales a los amigos que nos cedieron el material de forma desinteresada para llevar a cabo este estudio: Nos cedieron sus máquinas y sus conexiones- Daniel Inarejos (Webmaster de [DondePuedo.com](http://DondePuedo.com)) , J.J.Peñalver , J.I.Ariza , Pablo Martín (Administrador de redes de [GrupoSat.com](http://GrupoSat.com)). Los entrevistados- Paco de [MegaCiudad.com](http://MegaCiudad.com) (Administrador de los servidores Edonkey) y Manuel Alonso de [P2P Hazard](http://P2P Hazard). Gracias a todos ellos por su colaboración.

La Asociación de Internautas con la publicación de los dos artículos de investigación solo trató de dar veracidad a las noticias de un posible espionaje a los usuarios de P2P cuyo resultado es muy

claro, son espiados.

También recomendamos que la comunidad P2P y más en lo posible los nuevos usuarios de P2P, tengan en cuenta no descuidar su seguridad para que su privacidad esté siempre a salvo de miradas indiscretas y recomendamos el uso de programas como [P2P Hazard](#) (muy recomendado y en castellano) y [PeerGuardian](#) ambos gratuitos.

Nuestro próximo artículo es un manual de como sacarle el máximo partido al programa [P2P Hazard](#) para poder estar a salvo de los espías del P2P.

Enlaces relacionados con la privacidad y seguridad de redes P2P:

[Como se espía una red P2P](#)

[Ámbito legal P2P](#) (Por Pedro Tur, abogado y editor de <http://www.iurislex.net>)

[Salvaguardar la intimidad en peer to peer \(P2P\)](#)

[P2P Hazard](#) (Programa de seguridad para P2P, recomendado)

[PeerGuardian](#)

Realizado por;

José María Luque Guerrero

Comisión de seguridad en la red. [www.seguridadenlared.org](http://www.seguridadenlared.org)

Asociación de Internautas. [www.internautas.org](http://www.internautas.org)

**Fecha artículo: 2004-03-15 15:14:12 - url artículo: <http://www.internautas.org/html/288.html>**

**Logos y marcas propiedad de sus respectivos autores.**

**Los comentarios son propiedad y responsabilidad de cada autor.**

**© 1998-2009 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)