

## Como se espía una red P2P.

La [Asociación de Internautas](#) es consciente de que los usuarios de P2P se encuentran diariamente atemorizados por las noticias sobre presuntas denuncias contra ellos. La comunidad de usuarios P2P está sufriendo ataques a su privacidad de manera ilícita. Como ejemplos más claros tenemos las continuas demandas que se dan en EEUU mediante la obtención de datos.

Es este artículo de investigación vamos a enseñar cómo se obtienen estos datos de forma ilícita. Son las técnicas ILEGALES usadas por la empresas que se dedican a asustar al colectivo P2P, atentando contra la privacidad de estos usuarios.

El artículo está realizado por un miembro de la comisión de seguridad de la Asociación de Internautas, Jose M<sup>a</sup> Luque, y en él también se demuestra que los usuarios de P2P han de poner más cautela en su seguridad para evitar que obtengan de sus máquinas tan fácilmente datos que luego son usados para asustarlos o intimidarlos.

Dentro de los programas P2P hay mucha variedad siendo todos ellos para el intercambio de cualquier tipo de fichero. Para el artículo se pensaba utilizar el famoso KaZaA pero después de comprobar la facilidad con la que se obtenían datos de los usuarios del mismo se descartó. Se probó también el programa Bittorrent pero pasaba lo mismo, se conseguían las IPs de los usuarios con una facilidad excesiva:

Los programas P2P tienen distintos grados de privacidad, unos más y otros menos, y al final se optó por el famoso Emule ya que es uno de los más usados por los internautas y posee mejores opciones de privacidad, no facilita la IP y permite elegir si quieres mostrar los ficheros que compartes o no. Repetimos que las técnicas sometidas a estudio en este artículo de investigación son "ilegales" y las analizamos aquí porque son ejemplos de las usadas por algunas empresas para obtener datos de los usuarios P2P.

Buscamos un archivo que tenga muchas fuentes y cuya descarga sea rápida para intentar conseguir lo antes posible un listado de 30 usuarios con sus correspondientes nick;

Previamente hemos preparado nuestra máquina, con un netstat gráfico junto con un sniffer, para monitorizar los paquetes que pasan por nuestra red (se han empleado herramientas muy simples puesto que nuestra máquina es bastante antigua). Después de esperar unos minutos el fichero empieza a descargarse y vamos obteniendo los Alias (Nick) de los usuarios que tienen el fichero que se está descargando, simultaneamente vamos comprobando sus IP. Ambas cosas se obtienen mediante la comparación de los kb/s que se están descargando del Emule y que el sniffer va monitorizando:

Al final hemos conseguido un listado de 30 IPs con sus Alias correspondientes y no ha resultado difícil. Ahora vamos a INTENTAR obtener más datos privados de estos usuarios.

Conseguimos localizar el área más cercana de conexión de algunas de esas IPs;

Pero estos datos (30 IPs, Alias, y localización en algunos) no son suficientes para poder contactar con estos usuarios. En esta parte del artículo de investigación pasamos a un nivel más ILEGAL (técnicas usadas por algunas compañías). Se escanean las IPs para buscar más datos privados, para ello usamos el programa comercial llamado "LANguard Network Security Scanner" (para buscar fallos o vulnerabilidades y ver el nivel de seguridad). Después de varios minutos tenemos bastante éxito y logramos suficientes datos de 5 de las IPs, como números telefónicos, correo electrónico y algún curriculum vitae (recordamos de nuevo que ha sido de forma ILEGAL). Pensaran ustedes que obtener datos de cinco máquinas es un porcentaje muy bajo, pero realmente se trata de un gran logro, imaginen una empresa que se dedique en exclusividad a realizar esto con una frecuencia diaria y verán que al final del día han conseguido muchos datos de los usuarios de P2P. Además hay que tener en cuenta que nosotros hemos logrado esto contando con muy pocos medios y recursos tanto humanos como materiales.

Vamos a describir los fallos de estos usuarios. Se han obtenido los números de teléfono de tres de las IPs con sólo teclear la IP en el navegador,

Los routers de Telefónica; SpeedStream 5660 y 3Com OfficeConnect Remote 812 configurados con el programa Megavía, muestran el número telefónico del usuario, en el caso del 3com hace falta usar una vulnerabilidad del mismo para poder acceder el número telefónico (las versiones nuevas no tienen este fallo).

También se obtiene el número tecleando las claves por defecto del router, accediendo con ello a la configuración y al número telefónico;

Accedemos a las carpetas compartidas de un usuario y vemos que tiene sus curriculum vitae, pero no procedemos a la descarga de los ficheros por preservar la privacidad y no tener un conflicto legal con este usuario. Pero verán que el tremendo fallo expone todos los datos de esta persona y las empresas dedicadas a realizar espionaje no van a tener escrúpulos a la hora de robarle todo lo necesario para obtener alguna identificación de las IPs y Nicks.

Comprobamos los puertos que tienen abiertos los 30 usuarios localizados y comprobamos que uno de ellos tiene un ftp en su máquina, accedemos y nos encontramos con su cuenta de correo electrónico

Consejo: como siempre nosotros recomendamos no tener ningun dato que pueda identificarnos, tanto en los servidores FTP, como en servidores WEB.

Después de localizar datos de estas IPs se puede "asustar" a estos usuarios, llamándoles a su telefono o enviándoles un correo electronico por ejemplo. Para rizar el rizo nos ponemos a ver como reaccionan estos tres usuarios P2P de los cuales hemos obtenido datos entre los que figura su número telefónico y les llamamos por teléfono.

1ª llamada. Descuelgan el telefono y es una empresa del sector metal, preguntamos por el encargado de administrar la red de la empresa, la chica que nos atiende no sabe qué es un administrador de red y explicamos que preguntamos por el encargado de los ordenadores y de la linea de Internet . Con esto sí nos entendió y nos puso con la persona en cuestión, transcribimos a continuación la conversación mantenida entre el administrador (X) y nosotros (A.I.):

X: "¿Sí? ¿Quién es?"

A.I.: "Hola buenos días, hemos comprobado que están usando la red de internet de forma ilícita, descargando y compartiendo ficheros ilegalmente porque poseen derecho de autor y copyright.

X: "¿Quien es usted?"

A.I.: "Somos de la Sociedad de Cantautores Hispanos Independientes (no se nos ocurrió nada mejor en ese momento) y hemos comprobado que están ustedes descargando y compartiendo canciones nuestras.

X: "¿Quien les dió este teléfono? ¿Como saben si hago estas cosas de las que me acusan?"

Notamos que estaba nervioso y como ya teníamos suficiente para el artículo acto seguido le contamos la verdad indicándole que estábamos realizando un trabajo de investigación para la [Asociación de Internautas](#), para demostrar a la comunidad P2P que se pueden espiar las redes P2P y que hay empresas que se dedican hacer estas cosas de forma ilegal. Después de calmarle nos pregunta de nuevo como obtuvimos el número de la empresa, le explicamos la forma y cómo poder evitarlo, se queda sorprendido y se muestra agradecido por los consejos y la información. Le preguntamos si podemos contar en nuestro artículo la llamada, y accede a ello pero nos pone una condición, el anonimato de la empresa y de sus datos, cosa que nos pareció de lo más correcto y por tanto hemos omitido dicha información en nuestro artículo.

- 2ª llamada. Partido XXXXX le atiende XXXXX .... . Directamente colgamos, no queremos tener ningun conflicto.

- 3ª llamada. Después de seis intentos durante un día entero nadie descuelga el teléfono y salta el contestador.

En este artículo se deja patente que las redes P2P se pueden espiar y con algo de suerte también se pueden obtener bastantes datos privados de los usuarios. Leemos diariamente que la RIAA (Recording Industry Association of America) esta asustando y demandando a la comunidad de P2P. No olvidamos que también generan "listas negras" de ficheros más descargados con su correspondiente checksum para comprobar si son los mismos ficheros o son nuevos, realizando listados de usuarios con los ficheros que comparten. El checksum lo usan como prueba en la demanda para certificar la autenticación del archivo.

También advertimos que los programas de intercambio P2P tienen que evolucionar para intentar en lo máximo posible que los usuarios de estas redes tengan asegurada su privacidad. Hay algunos programas que lo están consiguiendo pero los miembros de la comunidad P2P no suelen migrar a estos nuevos programas más seguros ya que son más lentos.

Desde la [Asociación de Internautas](#) aconsejamos a los usuarios de P2P que revisen las opciones de su router para evitar que sus datos estén a merced de los demás y puedan ser robados, y también todo aquello que pueda exponer su IP como servidores web y ftps.

En el próximo artículo de investigación llamado "**La caza de los espías del P2P**" demostramos que nos están espiando y "cazamos" a estos espías. Un trabajo de dos semanas donde colaboran amigos que nos cedieron sus equipos.

Enlaces relacionados con la privacidad y seguridad de redes P2P:

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

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

[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: 2004-02-28 21:00:58 - url artículo: <http://www.internautas.org/html/283.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)