MANUAL DE ABUSE

Octubre 2005

INDICE

1. E-MAIL DE CONTACTO

Dirección de correo que se utilizará para el contacto con el denunciante. Se recomienda utilizar una cuenta de correo de Euskaltel si el denunciante es cliente de Euskaltel. Obligatorio.

2. DESCRIPCION

Resumen del incidente que ha originado la reclamación. El tamaño máximo de la descripción no puede ser superior a 40 caracteres. Obligatorio.

3. TIPO DE ATAQUE

Permite indicar el tipo de ataque que ha originado la reclamación. Obligatorio.
A continuación se detallan los distintos tipos de ataque de los que puede ser objeto:

SPAM

El SPAM se podría definir como la recepción de correo no solicitado que normalmente incluye publicidad sobre algún producto o servicio. El envío de SPAM constituye una violación de los términos de uso del servicio de Internet de Euskaltel, S.A. (Política de Uso Aceptable de Euskaltel).

PHISING

Se trata de un tipo de SPAM que simula proceder de supuestas entidades bancarias, tanto en inglés como en castellano, solicitando información confidencial (códigos de tarjetas de crédito, datos de acceso etc...). Es importante recordar que este tipo de mensajes persiguen obtener información sensible de los usuarios para posteriormente cometer fraude y que las entidades bancarias jamás solicitarán este tipo de información por correo.

Importante: Es necesario que nos envíe una copia del SPAM recibido con la información completa de cabeceras de Internet, de lo contrario no podrá ser tramitada la denuncia. Las cabeceras muestran el camino que ha seguido el mensaje desde su origen hasta su destino, así como la dirección IP de origen, necesario para enviar una reclamación al responsable. Para obtener las cabeceras de Internet, consulte la sección: **¿Cómo obtener las cabeceras completas de un mensaje de correo electrónico?.** Por favor envíenos únicamente reclamaciones cuyo origen sea un cliente de EUSKALTEL, S.A., consulte ¿Cómo saber si la IP origen corresponde a un cliente de Euskaltel, S.A.?

VIRUS

Los virus son programas maliciosos que se distribuyen por Internet de maneras diversas *(*correo, redes P2P, Messenger, Chats, etc…*)*, aunque la más frecuentemente utilizada es el correo electrónico. Si recibe un mensaje con virus por correo electrónico, por favor envíenos también las cabeceras completas del mensaje. Para obtener las cabeceras de Internet, consulte la sección*:* **¿Cómo obtener las cabeceras completas de un mensaje de correo electrónico?.**

ESCANEO DE PUERTOS

El escaneo de puertos puede indicar un intento preliminar de un Hacker por intentar acceder a un equipo o la acción automática de un virus o gusano que intenta propagarse, asimismo, tenga en cuenta que es muy probable que su cortafuegos *(*firewall*)* detecte a su vez falsos positivos, esto es, intentos de ataque que son provocados por el tráfico normal de Internet, es por ello que le pedimos que nos envíe únicamente aquellos incidentes que estime que pudieran representar una amenaza, sepa que si está protegido por un cortafuegos, se encuentra a salvo de estos intentos de acceso. En caso de que su cortafuegos detecte un intento de escaneos de puertos, le rogamos que nos envíe como evidencia un extracto del log de su Firewall como prueba del incidente con al menos la siguiente información*:* Fecha, Hora, Zona horaria, Dirección IP origen, Puerto origen, Dirección IP destino, Puerto destino. Tenga en cuenta que únicamente podemos atender aquellas reclamaciones relativas a direcciones IP de origen de Euskaltel, S.A. consulte **¿Cómo saber si la IP origen corresponde a un cliente de Euskaltel, S.A.?**

INTRUSION PROPIEDAD INTELECTUAL

Por intrusión se entiende cualquier tipo de acceso no autorizado a un sistemas de un usuario y/o la utilización ilícita del mismo por un tercero *(*hacker*)* para cometer actos maliciosos. Normalmente este tipo de intrusiones se llevan a cabo mediante la introducción en el sistema de la víctima de un caballo de troya *(*troyano*)*, esto es, un programa destinado a proporcionar una interfaz al hacker para conectarse al sistema de la víctima, así como recopilar información sensible como las contraseñas de acceso a banca on-line. Si sospecha que ha sido víctima de una intrusión, reúna toda la información de la que pudiera disponer y envíenosla como evidencia. Cualquier incidente derivado de la infracción por parte de alguno de nuestros clientes de los derechos de propiedad intelectual. Le rogamos que en estos casos nos facilite información acerca del material que infringe la ley de propiedad intelectual y el poseedor de los derechos.

DoS

Denegación de Servicio. Incluye cualquier ataque registrado que tratara inutilizar el sistema de la víctima mediante el consumo excesivo de recursos del mismo.

OTROS

Cualquier otro tipo de incidencia de seguridad que por tipología no encaje en ninguna de las anteriormente descritas. Recomendamos que a ser posible se intente encajar la incidencia en alguna de las anteriores y dejar este tipo de incidencia como último recurso. Esto nos ayudará a atender mejor su reclamación.

4. ZONA HORARIA (TIME ZONE)

Las **zonas horarias** o **husos horarios** corresponden a cada una de las veinticuatro áreas en que se divide la Tierra. Todos los husos horarios se definen en relación al Tiempo Universal Coordinado (UTC), el huso horario centrado sobre el meridiano de Greenwich, por lo que también se pueden definir en relación a GMT (Greenwich Mean Time) u Hora Media de Greenwich. Asimismo, hay que tener en cuenta que la hora se adelanta o retrasa en algunas partes del mundo, dependiendo de la estación. Obligatorio.

Puede consultar la zona horaria en la que se encuentra en:

http://es.wikipedia.org/wiki/Zona_Horaria

5. BREVE EXPLICACION DE CÓMO OBTENER LA DIRECCIÓN IP DE ORIGEN

Todos los sistemas necesitan una dirección IP para poder comunicarse en Internet. Dicha dirección IP proporciona información sobre el proveedor de servicios de Internet cuyo cliente es responsable de la incidencia registrada. Así como las direcciones de correo electrónico son fáciles de falsificar y por lo tanto no son fiables a la hora de investigar el origen de una incidencia, las direcciones IP, por el contrario son mucho más fiables y es por ello que es preciso disponer de ellas para poder identificar el origen de un incidente. Obligatorio.

Las direcciones IP son una cadena compuesta por 4 números separados por puntos. Cada uno de estos números va desde el 0 hasta el 255. (p.e: 212.55.8.132).

Para incidentes de intrusión o de escaneo de puertos, la dirección IP del atacante podrá obtenerse del extracto de log de su cortafuegos. Para más información sobre como obtener la información del log, consulte por favor con el fabricante de su cortafuegos.

Para incidentes relacionados con el correo electrónico, como spam o virus, la dirección IP del origen del correo aparece en la última línea "Received: from" de las cabeceras de Internet del correo. Es por ello que para este tipo de incidentes se solicite siempre la información completa de cabecera. A continuación le indicamos las instrucciones precisas para interpretar las cabeceras de Internet de un correo y como obtener esta información.

Para más información acerca de cómo obtener la información de cabecera en un determinado programa de correo electrónico, por favor consulte Evidencias.

a. ¿Cómo saber si la IP origen corresponde a un cliente de Euskaltel?

El departamento de abuse del servicio de Euskaltel , S.A. solamente atenderá aquellas reclamaciones que hayan sido causadas por clientes de Euskaltel, S.A., dado que solamente podemos tomar medidas correctoras contra nuestros clientes.

Contra clientes de otros operadores, lo único que podemos hacer es reenviar la denuncia al operador correspondiente por ello, entendemos que la forma más rápida y apropiada es que sea el propio denunciante el que envíe la reclamación directamente al operador responsable del envío con objeto de que sea atendida lo antes posible. En el apartado **¿Cómo enviar una reclamación de abuse a otro operador?** le explicamos como puede hacerlo de manera rápida y sencilla, no obstante, si es usted cliente de Euskaltel y tiene alguna duda al respecto de cómo enviar estas reclamaciones, no dude en contactar con nosotros, a través de info@euskaltel.com y le aclararemos cualquier duda que pudiera tener.

Una vez que hemos obtenido la IP origen del incidente, siguiendo las directrices indicadas en **Breve explicación de cómo obtener la dirección IP Origen**, para saber si dicha dirección IP esta registrada a nombre de Euskaltel, S.A. y por tanto identifica a un cliente de Euskaltel, S.A. debe consultar la IP en la siguiente página web:

http://www.ripe.net/fcgi-bin/whois

Introduzca la dirección IP en el cuadro de texto y pinche en "Search" obtendrá la información sobre el proveedor responsable, así como la cuenta de correo de contacto

o en caso de que disponga de ello, la URL del formulario web de abuse. Si aparece Euskaltel como responsable, entonces significa que la IP es propiedad de Euskaltel y por tanto podremos atender la reclamación.

Nota: Las direcciones o personas de contacto que aparecen en dichos registros, no son los responsables directos de la incidencia o del ataque, sino que son contactos administrativos en la operadora responsable de dichas direcciones IPs con los que contactar en caso de incidencias.

Si la dirección IP no es de Euskaltel, S.A. entonces debe enviar la reclamación al operador responsable, siguiendo el procedimiento indicado en **¿Cómo enviar una reclamación a un operador ajeno a Euskaltel, S.A.?**

b. ¿Cómo enviar una reclamación a un operador ajeno a Euskaltel?

Si la dirección IP de origen no pertenece a Euskaltel, S.A. debe enviar una reclamación al operador responsable ya que es el único que puede tomar medidas efectivas contra el usuario que ha causado la incidencia.

Para encontrar el contacto del operador responsable, deberá buscar en las páginas web de las entidades de registro de IPs territoriales.

En el mundo existen tres grandes entidades de registro que se encargan de asignar las direcciones IP a los operadores según en la zona del mundo en la que se encuentren:

- RIPE *(*http://www.ripe.net*)*: Esta es la autoridad de registro de IPs para EMEA: Europa, Medio Este y África y contiene una base de datos con todas las direcciones IP asignadas a operadores de estas regiones.
- ARIN*: (*http://www.arin.net*):* Esta es la autoridad de registro de IPs para América. Contiene una base de datos con las direcciones IP de todas aquellas direcciones IP asignadas a operadores tanto de América del Norte como de América del Sur.
- APNIC*: (*http://www.apnic.net*):* Esta es la autoridad de registro de IPs para Asia – Pacífico. Contiene una base de datos con todas aquellas direcciones IP asignadas a operadores de los países asiáticos, incluyendo a Japón y a Australia.

La operativa a seguir sería la de buscar una dirección IP primero en RIPE y si no obtenemos la información de contacto, buscaríamos en ARIN o en APNIC hasta que encontremos la información de contacto. La cuenta de contacto para temas de abuse suele ser: abuse@dominio.xxx, dado que es un estándar adoptado mundialmente. No obstante todavía existen organizaciones que no se han adaptado dicho estándar, en cuyo caso sería conveniente enviar la reclamación a todas las direcciones de correo que aparezcan en le consulta. Asimismo, al igual que Euskaltel, S.A. muchos operadores ofrecen formularios web para enviar los incidentes de Abuse, en cuyo caso se recomienda hacer uso de éstos en lugar de enviarla a través de correo electrónico, dado que con toda probabilidad su reclamación será atendida más rápidamente.

Existe una organización dedicada completamente a las denuncias de Abuse, que se dedica a recopilar las cuentas de Abuse de contacto para todos los operadores *(*mediante consultas a RIPE, ARIN y APNIC*)* y que proporcionan una base de datos centralizada con los contactos de todas ellas y que por tanto nos darían la dirección de contacto directamente con introducir la IP *(*sin tener que buscar en los diferentes registros*)*.

No obstante, recomendamos utilizar esta opción en el caso de que con las consultas en ARIN, APNIC o RIPE no encontremos la información buscada, dado que las entidades de registro disponen de información mucho más actualizada. La URL es la siguiente:

http://www.fr1.cyberabuse.org/whois/?page=whois_server

A la hora de enviar la reclamación, le recomendamos que siga los consejos ofrecidos en esta página sobre qué evidencias deberá facilitar para que puedan atender su incidencia: logs del cortafuegos, encabezados de un correo electrónico...

Si es usted cliente de Euskaltel y tras leer el procedimiento le queda todavía alguna duda al respecto, no dude en consultarnos (info@euskaltel.es), estaremos encantados de responderle a sus cuestiones y ayudarle a enviar su reclamación al proveedor responsable.

En el caso específico de reclamaciones por recepción de SPAM desde direcciones IP que no sean propiedad de Euskaltel, S.A., le recomendamos que tome en consideración denunciar las mismas a través de SPAMCOP (www.spamcop.net). Se trata de una asociación que proporciona una interfaz sencilla y gratuita para la denuncia automática de mensajes de SPAM. Simplemente deberá darse de alta con una cuenta de correo y pegar las cabeceras y el contenido del mensaje en el formulario que proporcionan al respecto. La herramienta se encargará de buscar los contactos responsables y enviar la denuncia por usted de manera anónima.

Información necesaria sobre el incidente que permite investigar el incidente y determinar una solución para el mismo, como por ejemplo los encabezados de un mensaje de correo o el extracto de un log de un Firewall. Obligatorio.

6. EVIDENCIAS

a. ¿Cómo Interpretar las cabeceras completas de un correo?

A continuación se muestra una cabecera de ejemplo seguida de una explicación sobre el significado de la misma:

Return-Path: <xxx@euskaltel.es>
Received: from correo1.euskaltel.es ([172.18.1.1]) by correo2.euskaltel.es (Netscape Messaging Server 4.15) with ESMTP id I9C80J00.IEY for <abuse@euskaltel.es>;
Sun, 26 Dec 2004 17:19:26 +0100

Received: from eui3smtp.euskaltel.es ([172.18.1.2]) bycorreo1.euskaltel.es (Netscape Messaging Server 4.15) with ESMTP id I9C80J00.M2O for <abuse@euskaltel.es>;
Sun, 26 Dec 2004 17:19:26 +0100

Received: from ID ([10.10.0.1]) by eui3smtp.euskaltel.es (Netscape Messaging Server 4.15) with SMTP id I9C80D02.A1K for <abuse@euskaltel.es>; Sun, 26 Dec 2004 17:19:25 +0100

Message-ID: <001c01d4gb6d$a3a2cj20$4b30d55436@ID>
From: <xxx@euskaltel.es>
To: <abuse@euskaltel.es>
Subject:ABUSE TEST
Date: Sun, 26 Dec 2004 17:19:15 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0007_01C4EB6F.06AAA380"

X-Priority: 3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2900.2180 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

Dentro de todos los campos que contiene la cabecera del correo los más interesantes son las líneas **Received**. En un correo electrónico pueden existir muchas de ellas y cada una de ellas, ordenadas desde abajo hacia arriba, señalan el camino que ha seguido un correo desde el origen hasta que ha llegado al servidor destino y ha sido entregado en el buzón del destinatario, todas ella, salvo que hayan sido falsificadas, han sido añadidas por un servidor de correo. Tomando como ejemplo las cabeceras indicadas arriba, empezaríamos a analizarlas desde la línea **Received** de más abajo, en este caso sería:

"Received: from ID *([10.10.0.1])* by eui3smtp.euskaltel.es *(*Netscape Messaging Server 4.15*)* with SMTP id I9C80D02.A1K for <abuse@euskaltel.es>; Sun, 26 Dec 2004 17:19:25 +0100 "

Todas las líneas **Received** tienen un formato similar y tomando el ejemplo de esta primera línea sería el siguiente:

- **ID:** Sería el nombre de dominio o del sistema que envía el mensaje.
- *([10.10.0.1]):* Esta es la IP correspondiente al sistema del que se ha recibido el mensaje. Dado que ésta es la primera línea "Received" en este caso sería equi valente a la dirección IP origen del mensaje que es la información que estaríamos buscando.
- **By:** El nombre que viene después de la claúsula "by" indica el siguiente salto o servidor de correo al que se va a entregar el mensaje para el envío. Ej:- eui3smtp.euskaltel.es
- Entre paréntesis aparecerá el software y la versión del servidor de correo que lo atiende. **Ej:-***(*Netscape Messaging Server 4.15*)*.
- **SMTP**: identificador único que todos los servidores de correo añaden a cada mensaje que procesan y que poste riormente sirve para identificarlos en el log del servidor. **Ej:-** I9C80D02.A1K
- **For:** indica la dirección del destinatario del mensaje recibida por el servidor Ej:- abuse@euskaltel.es.
- Por último, el servidor añade la fecha, hora y la zona horaria, por ejemplo "0100" significaría GMT + 1.

Asimismo, hay que señalar que en condiciones en las que no existan líneas "Received" falsificadas, como en el ejemplo anterior. Hay que observar que cada línea "Received" está enlazada con la inmediatamente superior, formando en conjunto *(*desde la inferior hasta la superior*)* un camino por el cuál el mensaje pasa hasta llegar a su destino. Como ejemplo, la interpretación del camino que ha seguido el mensaje anterior es la siguiente:

El mensaje ha sido enviado desde la IP 10.10.0.1 dirigido hacia la dirección de correo electrónico "abuse@euskaltel.es" y ha sido recogido por el servidor de correo "eui3smtp.euskaltel.es". Dicho servidor, dado que no posee el buzón del destinatario, reenvía el mensaje al servidor de correo que cree que lo puede atender *(*previa consulta al registro MX para el dominio destino en un DNS –Servidor de nombres de dominio*)*, en este caso sería el servidor "correo1.euskaltel.es". Este servidor recoge el mensaje que procede de "eui3smtp.euskaltel.es" y le añade la información habitual, un SMTP ID nuevo, el destinatario y la fecha y hora. A su vez y dado que correo1.euskaltel.es tampoco tiene el buzón del destinatario, lo envía a otro servidor que cree que tiene el buzón del destinatario: "correo2.euskaltel.es".

Por último, "correo2.euskaltel.es" recibe el mensaje y vuelve a crear la línea "Received" con la información habitual y en este caso entrega el mensaje al destinatario ya que posee el buzón del mismo.

Tal y como se ha señalado anteriormente, en un correo, pueden existir líneas "Received" falsas. Esto es sobre todo muy habitual en incidentes de SPAM, dado que los spammer lo suelen utilizar para dificultar, en la medida de lo posible, la obtención del camino seguido por el mensaje. No obstante, a pesar de que se pueden añadir líneas "Received" falsas al final del camino *(*por la parte inferior*)*, la línea "Received" superior siempre es correcta, dado que es la que añade el servidor de correo que finalmente entrega el mensaje al destinatario. Aunque algunas cabeceras falsificadas pueden ser difíciles de distinguir un simple análisis del enlace que debe haber entre el servidor que aparece después de la cláusula "by" de la línea "Received" inmediatamente inferior, del servidor que aparece después de la cláusula "from" de la línea "Received" inmediatamente superior, puede ser indicativo *(*en caso de que no haya tal enlace, o que las fechas y horas no tengan relación*)* que dicha línea "Received" no es correcta y ha sido un añadida a priori. En caso de detectar esto, la línea "Received" y por tanto la dirección IP que en ella aparece que deberemos tomar como referencia ha de ser siempre la superior en las cabeceras.

El resto de campos que aparecen en la cabecera, como el "To", el "From", el "Returnpath", no deben ser considerados como fiables dado que son siempre añadidos por el cliente que lo envía y por tanto son fáciles de falsificar, de hecho, la gran mayoría de los mensajes de SPAM y los virus que se envían por correo electrónico, lo hacen falsificando estos campos de tal forma que se cause confusión en el receptor o para potenciar que el receptor abra el mensaje, al hacer aparecer como cuenta origen una que es familiar para el receptor.

b. ¿Cómo puedo obtener las cabeceras de un correo desde mi cliente de correo?

Si utiliza el cliente de correo **Microsoft Outlook Express 4, 5 o 6** por favor siga los siguientes pasos para facilitarnos dichas cabeceras:

1. Seleccione el mensaje en cuestión y haga "clic" con el botón derecho del ratón sobre él, seleccione la opción "propiedades" del menú desplegado.
2. En la ventana que se le muestra a continuación haga "clic" sobre la pestaña "detalles", haga "clic" sobre el botón "Origen del mensaje" y seleccione todo el texto *(*CTRL + A*)* y cópielo *(*CTRL + C*)*.
3. Copie la información mostrada en el campo Evidencias del formulario.

Si utiliza el cliente de correo de **Netscape *(4.x, 6.x, 7.x)*** por favor siga los siguientes pasos:

1. Active la opción del menú "Ver-->Encabezados-->Todos los mensajes".
2. Seleccione el mensaje en concreto y las cabeceras deberían mostrarse en la parte baja de la ventana.
3. Copie la información mostrada en el campo Evidencias del formulario

Si utiliza **Outlook Express para Macintosh** siga los siguientes pasos:

1. Seleccione el correo y escoja la opción del menú "Ver-->Origen". Aparecerá una nueva ventana conteniendo el correo con las cabeceras completas.
2. Copie el contenido de dicha ventana *(*Ctrl +a*)* y péguelo en el campo Evidencias del formulario.

Si utiliza **Microsoft Outlook 98, 2000 o 2002** siga los siguientes pasos:

1. Abra el mensaje y seleccione "Ver", después seleccione "Opciones" del menú desplegable.
2. Cerca del final de la pantalla verá una sección denominada "Encabezados de Internet".
3. Pinche con el botón derecho sobre los encabezados y seleccione "Copiar".
4. Pegue el contenido en el campo Evidencias del formulario.

Si dispone de cualquier otro cliente de correo, puede consultar la página siguiente *(*en Inglés*)*: http://spamcop.net/fom-serve/cache/19.html o bien consultar la ayuda de su cliente de correo.