
¿Cómo puedes evitar que los ordenadores de un centro acabe en una botnet?

Se recomienda mantener actualizado el sistema operativo y todos los programas instalados en él, proteger el ordenador con alguna herramienta de seguridad como antivirus y tener unos buenos hábitos de uso. ¡Ah! Y aplicando el sentido común: no instalar nada que no se haya elegido, no pulsando enlaces de e-mails cuyo remitente se desconoce, desconfiando de los chollos que te anuncian por Internet, etc.

¿Qué ocurre si algún ordenador se queda encendido en el centro?

Que podría ser infectado con un virus que lo convierta en un terminal zombie, infectando a su vez el resto de los ordenadores del centro y convirtiendo la red escolar en parte de una Botnet. Dando a los hackers herramientas para poder llevar a cabo sus tareas delictivas e ilegales.

Servicio AntiBotnet

Desde la OSI se pone a tu disposición el Servicio Antibotnet, un mecanismo que permite conocer si existen amenazas o incidentes de ciberseguridad relacionados con redes de ordenadores comprometidos o botnets asociados a tu conexión a Internet. Para ello se chequea la dirección IP pública que tengas asignada en cada momento contra nuestra base de datos.

La finalidad del servicio es proporcionar información y herramientas que puedan ayudarte en la desinfección de los dispositivos afectados, contribuyendo así a un Internet más confiable y seguro para todos.



**Junta de
Castilla y León**
Consejería de Educación

BOTNET O RED ZOMBIE EN LA ESCUELA



Botnet o red zombie de ordenadores.



¿Últimamente has notado que tu ordenador va más lento de lo normal, el ventilador hace mucho ruido aún cuando no lo estás utilizando y algunas aplicaciones han dejado de funcionar correctamente?



Mi ordenador es un Zombie

Estos síntomas podrían ser debidos a que tu ordenador se ha convertido en un pc "zombi". ¿Eso qué significa? Que hay alguien, aparte de ti, que está controlando tu ordenador sin que seas consciente de ello.

Pero, ¿cómo tu ordenador se ha convertido en un zombi? Se ha infectado con un tipo de virus capaz de controlar tu ordenador de forma remota. Esto quiere decir que alguien, sin estar físicamente delante de tu ordenador, y con los conocimientos técnicos suficientes, puede manejarlo a su antojo. Pero eso no es todo, si tu ordenador es un zombi, estará formando parte de una red zombi de ordenadores, conocida con el término anglosajón botnet.

Capturar contraseñas y datos personales.

Recopilan las contraseñas de los servicios de banca, redes sociales, correo web (Gmail, Outlook, etc.) que utilizan los usuarios del ordenador infectado para después venderlas en la "deep web", el mercado negro

¿Qué es una botnet?

No es más que un gran número de ordenadores zombi, infectados con el mismo tipo de virus, que están controlados por una misma persona u organización criminal.

¿Por qué quieren que tu ordenador pertenezca a una botnet?

Principalmente para llevar a cabo actividades que les generen unos beneficios económicos de manera ilegal.



¿Qué consiguen los hackers infectando una red?

Capturar contraseñas y datos personales.

Enviar spam y propagar virus.

Hacer que una página web deje de estar disponible.

Manipular encuestas y abusar de los servicios de pago por publicidad.

Llevar a cabo desde los ordenadores otro tipo de fraudes.

Acceder a páginas web cuyo contenido es denunciado o ilegal: pedofilia, prostitución, drogas, etc. Almacenar y compartir ficheros con copyright, suplantar tu identidad para publicar anuncios falsos, etc. ¡Cualquier otra cosa que se te ocurra!