



Informe sobre el estado de la seguridad en los juegos online

El 79% de los cracks para videojuegos son sospechosos de contener virus

- Las copias ilegales y la modificación de las restricciones impuestas por los fabricantes de videojuegos y dispositivos tecnológicos son la principal puerta de entrada de hackers y malware.
- Más del 50% de los juegos de Android tienen acceso al número de teléfono, 1 de cada 4 tiene permiso para obtener la ubicación del jugador y el 1% puede enviar SMS Premium de coste elevado.
- S2 Grupo ha realizado su primer estudio sobre la seguridad en los juegos en red para detectar y advertir sobre las principales amenazas que pueden afectar a los usuarios en las diferentes plataformas tecnológicas y sistemas.
- La compañía ha presentado un Decálogo con consejos básicos para acceder a juegos online de una forma segura.

Valencia 20 de diciembre de 2011.- La empresa de seguridad digital S2 Grupo ha presentado su **"I Informe sobre el estado de la seguridad en los juegos online"** cuyo objetivo es mostrar la situación del mercado y detectar los principales riesgos a los que se enfrentan los usuarios. En este estudio se han analizado las amenazas y fortalezas de las diferentes plataformas y sistemas operativos desde los que se puede acceder al juego en red, se advierte sobre los principales objetivos de los hackers en la actualidad y se ha incluido un "Decálogo de seguridad en juegos online".

En Navidad es frecuente regalar videoconsolas y todo tipo de dispositivos tecnológicos desde los que se puede jugar en red con personas de cualquier parte del mundo. Esto puede convertirse en un grave problema si no se toman las medidas necesarias de protección frente a los hackers y el malware (software malicioso como por ejemplo virus, troyanos, gusanos, etc.) que ya ha conseguido llegar a todo tipo de terminales (smartphones, PC, consolas, etc.).

Entre las principales **conclusiones** del estudio se advierte de que las copias ilegales y la modificación de las restricciones impuestas por los fabricantes de videojuegos y dispositivos son las principales puertas de acceso para la acción de hackers y malware.

Los ordenadores continúan siendo una de las plataformas más utilizadas por los jugadores, donde uno de los principales riesgos que se cometen es la piratería. De un análisis de casi 2.000 cracks utilizados para realizar copias ilegales, un 3% contenían virus y troyanos y el 79% eran sospechosos de estar infectados, con el consiguiente riesgo que conllevan.

Lo mismo ocurre con las videoconsolas. Convertidas en el terminal favorito de los usuarios, la posibilidad de jugar on-line unidas a la modificación de los aparatos y juegos para utilizar copias no originales, las ha situado en una vía para la difusión de acciones maliciosas como malware, control de las máquinas o robo de datos.

En el caso de los juegos para smartphones, el método más usado por hackers es realizar cambios en las aplicaciones para añadirles funcionalidades que les reporten beneficios como obtener sus datos privados o la posibilidad de enviar mensajes SMS Premium que generan un coste alto a los usuarios. Esto es lo que ocurre con Android. Después del análisis de 3.387 juegos, se ha concluido que más del 50% tienen acceso al número de teléfono y al IMEI, casi 1 de cada 4 programas tiene permisos para obtener nuestra ubicación y el 1% de los videojuegos requieren de un permiso para enviar SMS, algo que no debería solicitar. Además, la facilidad para los desarrolladores de modificar las aplicaciones de Android ha propiciado la aparición de "Markets" alternativos. Según el estudio, los juegos descargados de internet son más peligrosos que los oficiales de Android, porque solicitan un porcentaje mayor de permisos considerados peligrosos.

En el caso de iOS, aunque puede presentar alguna vulnerabilidad, es más seguro porque Apple cuenta con un sistema de control del origen de las aplicaciones que prácticamente garantiza la inexistencia de programas maliciosos.

Las redes sociales se han convertido en la plataforma que más malware genera. El caso más representativo es el de Facebook, que gracias a permitir a los desarrolladores publicar juegos, ha conseguido obtener la práctica hegemonía en los juegos sociales. Este carácter social, ha sido aprovechado por el malware para distribuirse de forma viral mediante publicaciones sugerentes hacia los demás usuarios que contienen virus, troyanos y estafas en general.

"El mismo desarrollo que han vivido los creadores de videojuegos para aprovechar su presencia en los nuevos dispositivos tecnológicos, lo han realizado los hackers y creadores de malware. Por este motivo, consideramos fundamental realizar anualmente un análisis que muestre las debilidades y fortalezas de cada plataforma de modo que el jugador pueda tomar las precauciones necesarias", asegura José Rosell, socio-director de S2 Grupo.

Objetivos de los hackers

Actualmente, la acción de los hackers en este sector busca diferentes objetivos que van desde los más inocuos para la seguridad del jugador hasta los más perjudiciales:

- recolección y venta de dinero virtual a cambio de dinero real,
- robo de cuentas de juego exitosas o de datos personales a través del phishing,
- distribución de programas falsos para controlar las máquinas de las víctimas a través de virus o troyanos,
- envío de spam a las direcciones de correo obtenidas,
- robo del número de las tarjetas de crédito,
- control de la máquina del usuario para utilizarla con fines ilícitos,
- establecimiento de trampas online para modificar programas y aventajar a sus adversarios, algo que es especialmente grave en el caso de los casinos donde la cantidad de dinero en juego es elevada.

DECÁLOGO DE SEGURIDAD EN JUEGOS ONLINE

Para promover la seguridad tecnológica en todos los ámbitos, concienciar sobre los peligros que existen en este sector y evitar la acción de los atacantes, S2 Grupo ha presentado un Decálogo con 10 consejos básicos para promover un uso seguro del juego en red:

1. Tener un ordenador protegido, no garantiza que los datos del jugador estén seguros.
2. Modificar el sistema operativo de las consolas las convierte en más vulnerables frente al malware.
3. Desactivar las restricciones impuestas por el fabricante de un videojuego, consola u otro dispositivo, elimina sus medidas de protección.
4. Es necesario proteger cada terminal desde el que se tiene acceso a juegos online.
5. Hay que desconfiar de todas las notificaciones recibidas donde se nos inste a introducir nuestro usuario y contraseña.
6. Los juegos descargados de sitios no oficiales son un peligro para la seguridad del jugador, es aconsejable descargarlos de fuentes oficiales.
7. En las redes sociales hay que desconfiar de los mensajes sospechosos que nos envíen los usuarios porque podrían ser un virus.
8. Es muy recomendable tener instalado, tanto en los ordenadores como en los dispositivos móviles, un antivirus.
9. Sólo debe introducirse el número de tarjeta de crédito cuando sea estrictamente necesario.
10. La concienciación en materia de seguridad es muy importante, todos los usuarios son posibles víctimas de ataques.

Sobre S2 Grupo

Fundada en 1999, es la primera empresa de la Comunidad Valenciana especializada en servicios globales de seguridad digital. En este ámbito, destaca su trabajo de consultoría para el diseño e implantación de Sistemas de Gestión de la Seguridad en todo tipo de organizaciones y procesos. La compañía prevé cerrar 2011 con una facturación de 3,85 millones de euros, lo que refleja un crecimiento del 21% respecto al ejercicio anterior, motivado por un aumento de la cartera de clientes y de la actividad de innovación. La inversión en I+D+i es uno de los ejes vertebradores de la compañía que en 2011 ha destinado 1,2 millones de euros a diferentes proyectos nacionales y europeos, lo que supone un 30% de su facturación.

Para más información:

Tinkle : Patricia Berzosa/ Miguel Cegarra
600 591 801 / 609 688 809
pberzosa@tinkle.es / mcegarra@tinkle.es