Seguridad en juegos online 2011

S2 GRUPO

Sobre S2 Grupo

S2 Grupo, fundada en 1999, es la primera empresa de la Comunidad Valenciana especializada en servicios globales de seguridad digital. 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.

Datos de contacto

S2 Grupo
Ramiro de Maeztu 7, 46022 Valencia
T 963110300 # F 963106086

Orense 85, Ed. Lexington. 28020 Madrid.
T 915678488 # F 915714244

Autor

David Lladró

Diseño y maquetación

Karina Coste
Manuel Benet

Fecha de publicación

Diciembre 2011

Este informe puede descargarse de la página web de S2 Grupo, **http://www.s2grupo.es**, del blog de seguridad Security Art Work, **http://www.securityartwork.es**, o solicitándolo por correo electrónico a **admin@securityartwork.es**.

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR ER Gestión I+D+i UNE 166002 ID-0066/2010
CERTIFIED IQNet MANAGEMENT SYSTEM
S2 GRUPO

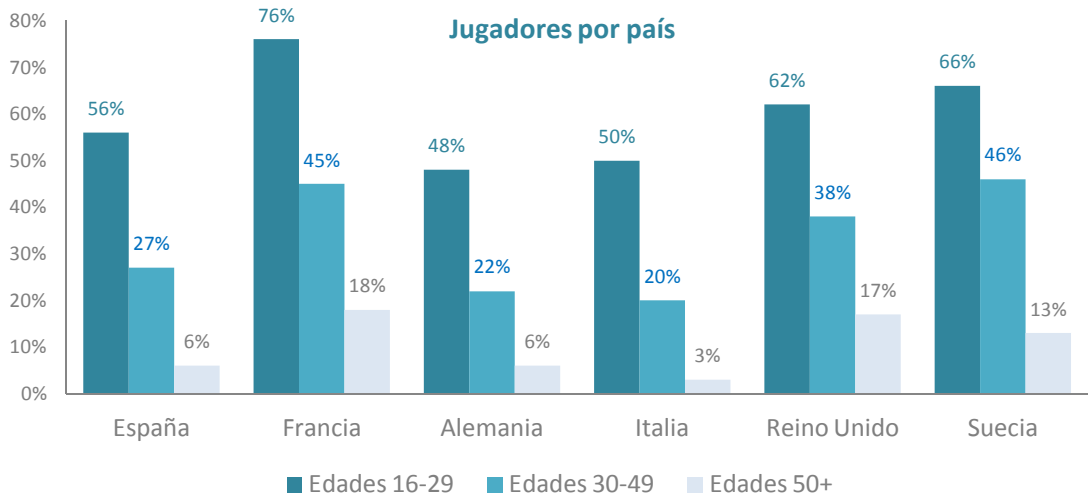
Introducción

Con el tiempo, los videojuegos se han convertido en una opción de entretenimiento más y más importante para la sociedad actual.

La cantidad de horas semanales que los jugadores dedican a los videojuegos ha aumentado considerablemente hasta llegar a las **5,2 horas de media**.

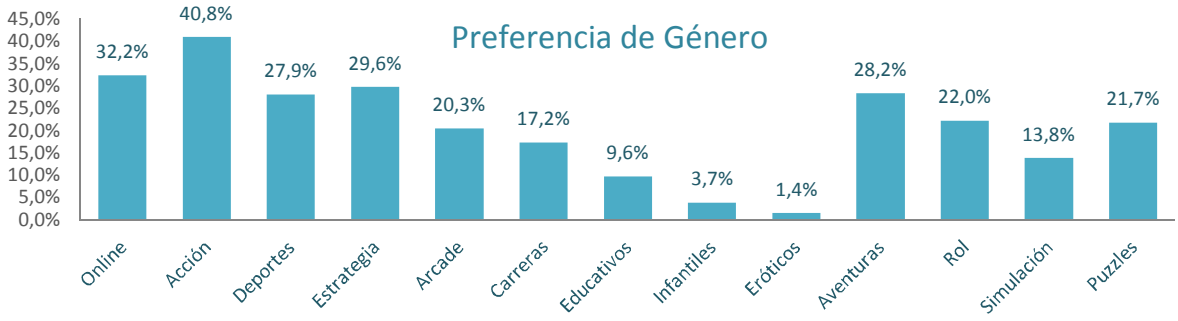
Cada vez, el rango de edad de los jugadores se amplía, y actualmente podemos tener desde niños hasta personas de la tercera edad jugando a videojuegos.

Este fenómeno no ocurre solamente en España, sino que ha ocurrido de la misma forma en toda Europa, donde en mayor o menor medida, ha aumentado el número de personas que disfrutan del entretenimiento ofrecido por los videojuegos.



Fuente [1]

Del gráfico anterior, se puede destacar que el perfil típico del jugador de videojuegos es el de las personas entre los 16 y 29 años, seguidos por el rango de edad de 30 a 49 años. También merece especial mención el caso de Francia y Reino Unido, donde el porcentaje de jugadores por encima de los 50 años supera el 15%.



Fuente [2]

El rango de edades también afecta a la temática de los videojuegos, algo que sin duda resulta obvio, ya que hay videojuegos desarrollados específicamente para niños, adultos o adolescentes. Como se puede ver en la gráfica, el género predominante es el de acción, por encima de otros como estrategia, aventuras o deporte.

Este amplio abanico no solo afecta a las edades, sino también a las plataformas donde se ejecutan estos juegos. Los tiempos en los que para jugar se necesitaba un PC o una consola han terminado.

Otro dato que merece ser destacado es que el 32,2% de los jugadores afirma que juega a videojuegos online, por lo que están expuestos a más peligros que los usuarios que solo juegan de forma local, obviamente debido a la propia naturaleza de Internet.

La diversidad de dispositivos que poseen la capacidad de ejecutar juegos es muy amplia. Aunque la plataforma predominante es el PC, los jugadores también disponen de consolas, teléfonos móviles, tablet PC, consolas portátiles…

En la siguiente gráfica se muestran los resultados de una encuesta realizada recientemente donde se muestra que del 100% de los encuestados, un 70,8% afirma que utiliza el PC para jugar. El segundo dispositivo en cuota de utilización es DS, la consola portátil de Nintendo, con un porcentaje del 37,6%. En la tercera posición se encuentra la consola Wii de Nintendo, que consigue un 36,3%.

Esta explosión de diversidad tecnológica no ha sido aprovechada solamente por los desarrolladores de juegos online: los creadores de *malware* también han visto un nuevo "nicho de mercado" para sus acciones delictivas.
Actualmente, la práctica totalidad de las plataformas de juegos están afectadas por algún tipo de *malware* que puede afectar al usuario.

Por estos motivos en el presente informe se va a mostrar el estado actual de la seguridad en los videojuegos online y los diferentes peligros a los que se enfrenta un jugador en la red.

Fuente [2]

Objetivo de los hackers

Es importante saber los motivos por los cuales un atacante centraría su objetivo en los videojuegos online y cuáles podrían ser sus beneficios.

Hasta hace unos años, los hackers (entendido en el sentido amplio de la palabra), centraban sus esfuerzos en romper las protecciones anticopia de los videojuegos o en modificar los juegos para obtener ventaja (trucos) o para mejorar el juego. Esta motivación parece lógica teniendo en cuenta que los dispositivos estaban aislados entre sí y no era viable el robo de información de los jugadores.

Pero esto ha cambiado con la llegada de Internet y los videojuegos online. Ahora, un atacante que consiga hacerse con el control de la máquina del jugador puede tener acceso a los datos personales, números de tarjeta de crédito o contraseñas del jugador. Estos datos son mucho más "apetecibles" para un potencial atacante, y por ello, los creadores de *malware* han puesto en el punto de mira a los videojuegos y sobre todo a los videojuegos online.

Analicemos cuáles pueden ser los objetivos de un atacante, desde los más inocuos para la seguridad del jugador hasta los más perjudiciales:

Dinero virtual

En la actualidad, muchos de los juegos implementan sistemas de dinero virtual para recompensar los logros conseguidos en el juego. Este dinero se utiliza para aumentar las capacidades del personaje y se ha convertido en un preciado tesoro y una necesidad para los jugadores noveles. Un usuario que empieza a jugar a un determinado juego necesita una gran cantidad de tiempo para conseguir que su personaje obtenga características avanzadas, por lo que resulta mucho más sencillo obtener dinero virtual de otras formas a las establecidas por el juego. De esta forma, el jugador puede obtener de una forma rápida lo que de otra forma necesitaría semanas o meses. Debido a la demanda de dinero virtual, ha aparecido el fenómeno del ***gold pharming*** que consiste en recolectar dinero virtual para luego intercambiarlo con otros jugadores a cambio de dinero real. El máximo exponente de este fenómeno aparece en el juego online World of Warcraft, donde se

sabe que existen jugadores pagados a tiempo completo para recolectar oro virtual [3].

Se han dado casos, como por ejemplo en China, donde se explotaba a presos para que recolectaran oro virtual durante horas. En concreto, los carceleros obligaban a realizar a los presos turnos de hasta doce horas sin parar de realizar tareas repetitivas para conseguir oro. Luego, ese oro recolectado era vendido en Internet a otros jugadores que pagaban dinero real para realizar el intercambio.

Por ejemplo, un jugador que estuviera dispuesto a comprar oro virtual solo debería entrar a webs especializas o a webs de subastas online, donde se vende abiertamente este intercambio de oro virtual. Eso sí, en ningún momento se indica en las webs la procedencia de ese oro. En la siguiente imagen se puede ver la cotización actual para el juego World of Warcraft en Europa.

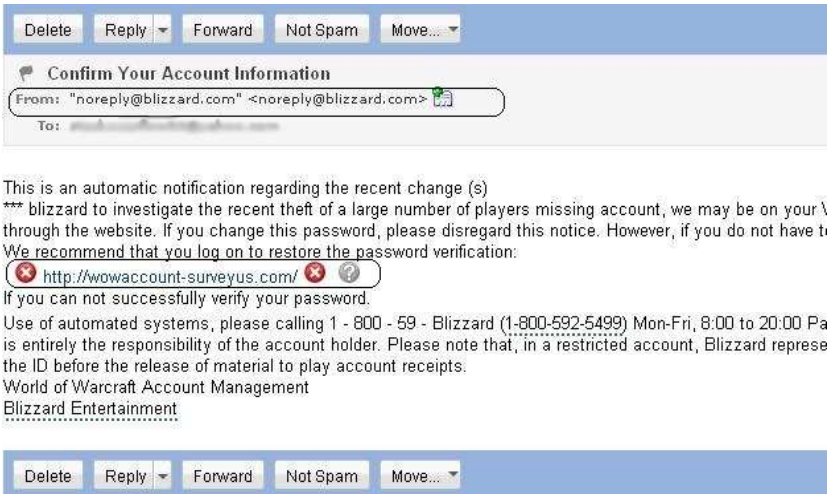
Formulario de compra de oro

Una vez realizado el pago, el vendedor realiza una "donación" de oro al comprador mediante los canales oficiales del juego, exactamente igual que si fueran conocidos y uno de ellos quisiera regalar oro al otro jugador.

Robo de cuentas

Para un atacante, resulta más sencillo robar una cuenta de un jugador online exitoso que generar una cuenta propia y mejorarla hasta el nivel deseado. Una de las técnicas más utilizadas para el robo de cuentas es el *phishing*, donde se induce al usuario a introducir las credenciales de acceso en entornos controlados por el atacante [4]. Por ejemplo, aquí se muestra un ejemplo de un correo electrónico donde se insta al jugador a que cambie su contraseña por motivos de seguridad:

Correo fraudulento



Otra de las técnicas utilizadas por los hackers es la de distribuir programas falsos para controlar las máquinas de sus víctimas. A continuación, se muestra un ejemplo de aplicación que simula realizar acciones beneficiosas para el jugador, pero en realidad contiene virus o troyanos [5].

Programa para crear oro

Trampas online

Uno de los objetivos que persiguen los potenciales atacantes es la modificación de los videojuegos para poder realizar trampas y obtener ventaja sobre sus adversarios. Por ejemplo, hace dos años, con la salida al mercado de Mario Kart para Wii, Nintendo vio como la plataforma de juego online se llenaba de jugadores que cometían trampas (chetos en el argot anglosajón) debido a que se podía modificar el juego para obtener ventaja frente a los adversarios. Por ello, Nintendo se vio obligada a restringir el acceso a los usuarios que utilizaban copias de juegos modificadas, mostrándoles la siguiente pantalla cuando trataban de acceder al juego:

Este problema toma una nueva dimensión cuando hablamos de videojuegos online en casinos, donde la alteración de una partida normal puede acarrear pérdidas monetarias reales tanto al casino como a los demás jugadores. Existen ejemplos de fraudes en casinos online como el de la web de poker *Absolute Poker*, donde un jugador podía averiguar las cartas de los demás jugadores:

Partida de póker realizando trampas.

Robo de datos

En la mayoría de los juegos online actuales, es necesaria la creación de una cuenta asociada al jugador para que el juego pueda guardar los progresos que realiza éste y así ofrecer una continuidad en el tiempo. Normalmente, en esta cuenta se suelen insertar datos personales del jugador, como son su nombre, edad, sexo, dirección de correo electrónico... Todos estos datos pueden ser aprovechados por un atacante para realizar múltiples ataques, desde suplantaciones de identidad hasta campañas de envío de spam con las direcciones de correo obtenidas.

Robo de número de tarjetas de crédito personales

En algunas plataformas online, aparte de los datos citados en el punto anterior, es necesaria la introducción de un número de tarjeta de crédito para crear una cuenta. Este dato es uno de los más valiosos para el crimen organizado, ya que su venta en el mercado negro reporta numerosos beneficios. Aquí se puede ver el importe aproximado que ganan los delincuentes con la venta de las tarjetas de crédito y otros datos en el mercado negro:

Relación de precios por la venta de tarjetas de crédito

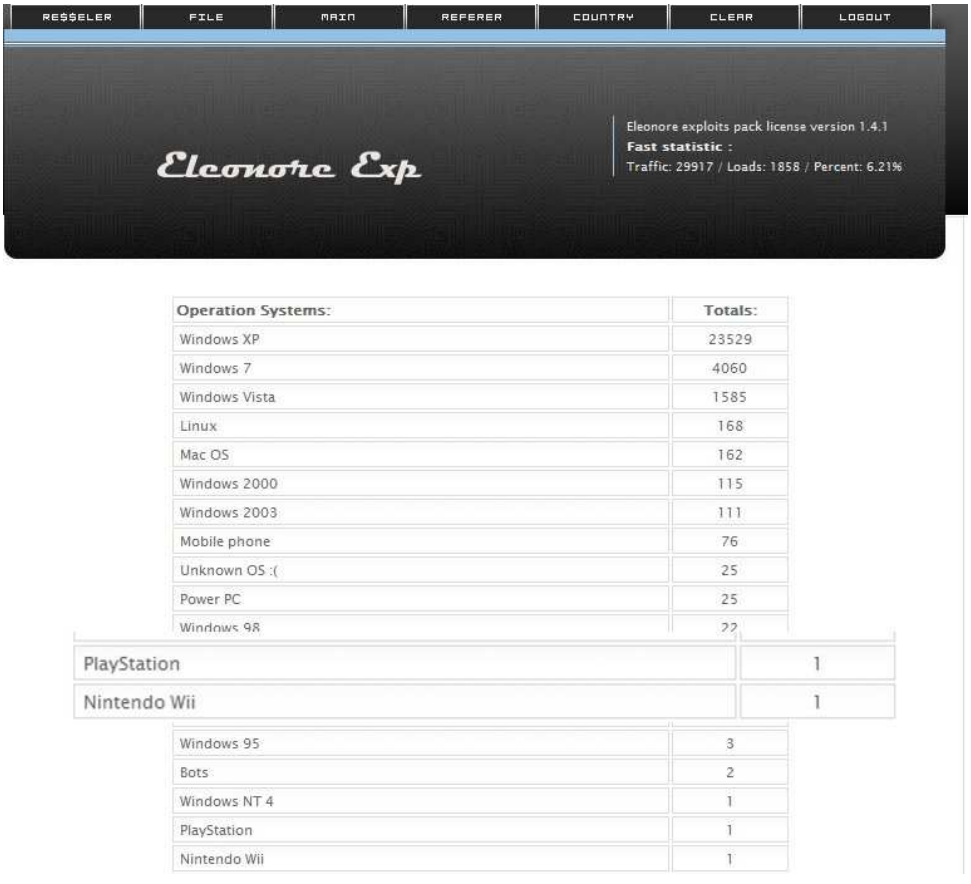
Fuente [6]

Producto	Precio
Tarjeta de crédito	Desde 2$ hasta 90$
Tarjetas de crédito físicas	Desde 180$ + coste de los datos
Máquinas duplicadoras de tarjetas	Desde 200 hasta 1.000 $
Cajeros automáticos falsos	Hasta 3.500$
Credenciales bancarias	Desde 80 y hasta 700$ (con garantía de saldo)
Transferencias bancarias y cobro de cheques	Entre el 10 y 40% del total a transferir o cobrar 10$ para cuenta simple sin saldo verificado
Cuentas de tiendas online y pasarelas de pago	Entre 80 y 1.500$ con saldo verificado
Diseño e implementación de falsas tiendas online	Según proyecto (sin especificar)
Compra y envío de productos	Entre 30 y 300$ (dependiendo del producto)
Alquiler envío de spam	A partir de 15$
Alquiler SMTP	A partir de 20$ 40$ para uso durante 3 meses
Alquiler VPN	20$ para utilización para 3 meses

Control de la máquina del usuario

Por último, no hay que olvidar que muchas veces el objetivo de una infección con *malware* es tomar el control de la máquina en sí para usarla con fines ilícitos, como por ejemplo unir la máquina a una botnet, que es una red de dispositivos zombies que actúan según las indicaciones de su controlador. También se encuentran entre las acciones más comunes el envío de spam y la generación de ataques distribuidos de denegación de servicio.

Por lo que se ha podido comprobar, este tipo de ataques no está limitado a los ordenadores, ya que existen casos de consolas Wii y Play Station 3 que formaban parte de una botnet [7] y estaban al servicio de los propietarios de la red. Por ejemplo, en la captura siguiente, se ve el panel de control de uno de los exploits pack más usados, donde se puede observar que hay dos consolas, una PlayStation y una Nintendo Wii, entre las máquinas infectadas.



Ordenadores

Como se ha apuntado en la Introducción de este Informe, los ordenadores siguen siendo la plataforma preferida por los jugadores en sus horas de entretenimiento…

… pero no solo es la plataforma preferida por los *gamers*, sino que también lo es para los creadores de *malware* y hackers en general.

Debido a que el *malware* en los ordenadores lleva desarrollándose durante años, es técnicamente más avanzado y difícil de detectar que el de las otras plataformas, y por lo tanto mucho más peligroso para los jugadores.

Cracks

Uno de los grandes problemas con los que se ha encontrado la industria del videojuego desde sus inicios ha sido la piratería. Actualmente, la práctica totalidad de los títulos para PC disponen en la red de una copia distribuida ilegalmente que permite a los usuarios jugar al juego en cuestión sin tener que pagar una licencia de uso. Estas copias no solo perjudican a las empresas creadoras de videojuegos, sino que pueden poner en peligro la seguridad de los usuarios que las utilicen.

Los jugadores que descargan estas copias deben instalar unos programas para eludir los sistemas anticopia que implementan las compañías desarrolladoras. Estos programas son más conocidos como *cracks*, *keygens*… en función de la tarea que realicen.

El problema reside en que no se sabe la procedencia ni la integridad de estos cracks. Además, muchos de ellos piden al usuario que deshabilite su programa antivirus dejando al usuario totalmente desprotegido y a merced de un atacante. Para conseguir que los usuarios desactiven el antivirus, los creadores del software que rompen las protecciones anticopia aseguran que el programa que se disponen a instalar está libre de virus y que deben desactivar el antivirus para una correcta instalación.

Esto lleva a muchos usuarios a realizarse las siguientes preguntas:

¿Son seguros los cracks?
¿Contienen virus la mayoría de los cracks?

Para tratar de traer un poco de luz a estas preguntas, hemos realizado un estudio para comprobar qué cantidad de cracks están infectados por programas maliciosos o perjudiciales para el ordenador.

Para realizar este estudio, primero se ha tratado de establecer las pautas de los usuarios cuando descargan cracks.

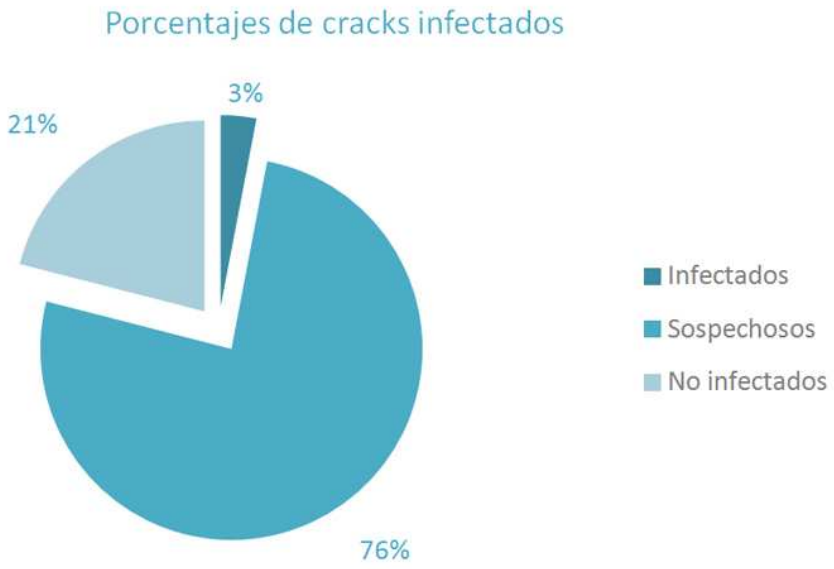
Según una consulta realizada, la mayoría de los usuarios descargan los cracks de la misma página Web donde se han descargado el juego, y en caso de no funcionar o no existir, recurren a páginas especializadas.

Debido a la dificultad de descargar una cantidad considerable de juegos para el estudio, se ha decidido optar por la opción de páginas especializadas en cracks para juegos. De esta forma, se ha podido descargar una muestra considerable de cracks para obtener resultados que se aproximen de la mejor forma a la realidad. Otra de las decisiones tomadas fue la de elegir qué página web sería la escogida para la realización del estudio. Los parámetros que se tuvieron en cuenta fueron la posibilidad de realizar descargas automatizadas y masivas de programas, la inclusión de juegos actuales y que la página en concreto tuviera cierto "prestigio" entre las webs de cracks.

Esta última consideración, fue tomada para evitar caer en el sensacionalismo mostrando resultados de webs controladas por creadores de *malware* donde todos los programas descargados contienen añadidos maliciosos. De esta forma, se ha pretendido mostrar datos reales que puedan interesar a los usuarios.

Finalmente, la página elegida fue *www.gameburnworld.com* de la cual se descargaron un total de 1.943 cracks (es decir, la totalidad de los que se encontraban en la web). Una vez finalizada la descarga, se ha procedido al análisis por parte de diferente software antivirus para obtener una imagen empírica del nivel de infección que presentan estas aplicaciones.

Para determinar si un crack está infectado o no, se ha realizado un análisis de los resultados obtenidos y se han descartado las detecciones genéricas y las que no aportaban la suficiente certidumbre. Por ejemplo, en la mayoría de los casos, los antivirus detectaban que el software había utilizado técnicas para dificultar el análisis por parte de los antivirus, pero no podían asegurar con certeza que estuviera infectado.



Con todos estos datos, el resultado ha sido que **un 3% de los cracks analizados contenían virus o troyanos**.

Como se ha comentado anteriormente, este porcentaje es solo el número de cracks que son detectados con un grado de confianza alto como *malware*. Aunque el número pueda parecer bajo, hay que tener en cuenta que muchos de los cracks analizados podrían estar infectados, pero se ha preferido mantener una estrategia conservadora y solo marcar como infectados los cracks de los que se tenían datos fehacientes.

Steam

Steam es una plataforma de videojuegos desarrollada por Valve Corporation mediante la cual la compañía pone a disposición de los usuarios servicios tales como compra digital, actualizaciones instantáneas, listado de servidores disponibles, logros, servicio de mensajería instantánea entre jugadores, ofertas exclusivas, información de última hora, etc., todo de forma gratuita.

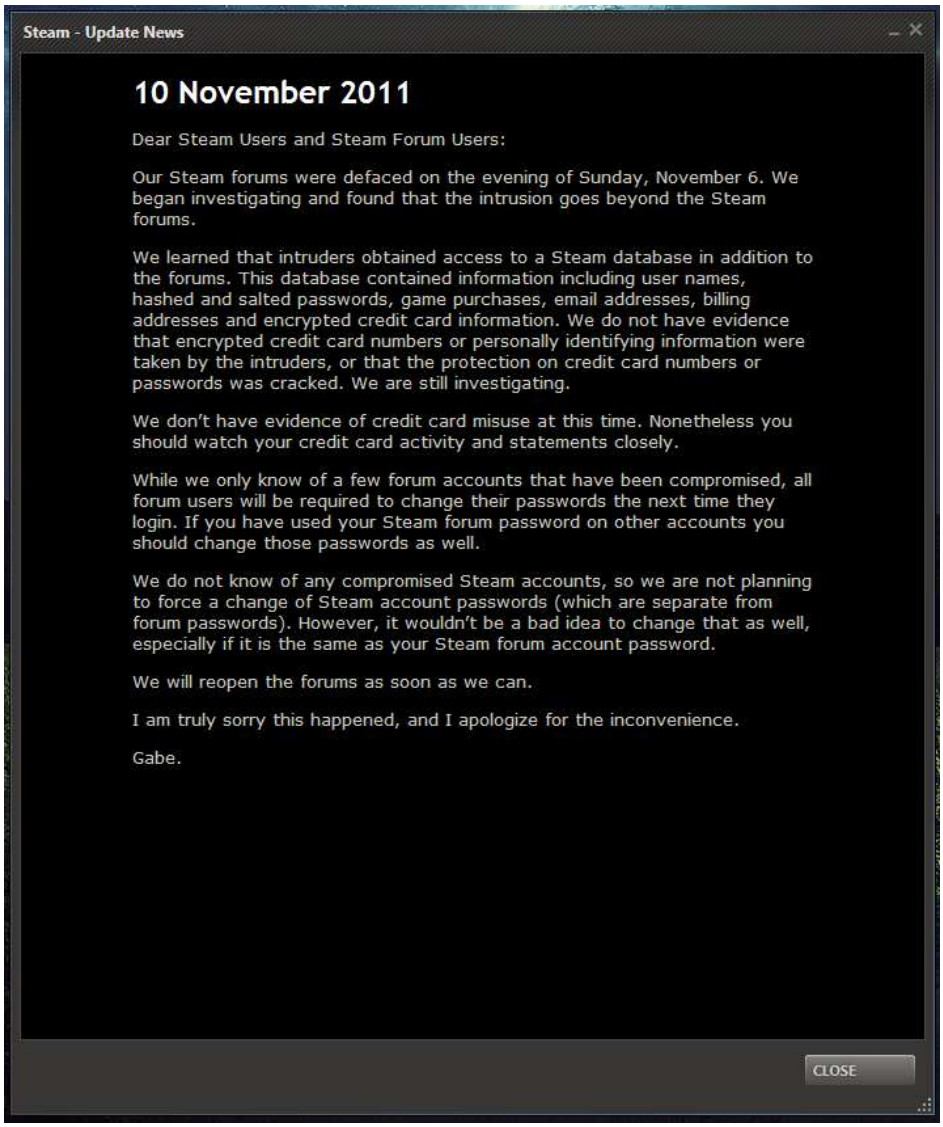
Para poder disfrutar de todos estos servicios, es necesario estar registrado en el servicio mediante la creación de una cuenta gratuita, a la que se vinculan los videojuegos comprados por el jugador. Estos juegos pueden ser tanto los juegos que se ofrecen para la compra en el propio programa, como

ciertos juegos comprados en tiendas físicas.

El pasado 10 de Noviembre de 2011, Valve advirtió a sus usuarios que había sufrido una intrusión por parte de unos atacantes y que información como nombre, dirección, contraseña y tarjeta de crédito podían haber sido robados.

El caso de Steam, es un ejemplo del peligro al que están sometidos los jugadores de juegos online, donde aunque sean cuidadosos con respecto a la seguridad de su PC, hay ocasiones que escapan de su control y en las que sus datos se pueden ver comprometidos.

Aviso de seguridad de Steam



Videoconsolas

Las videoconsolas han sido y siguen siendo el segundo medio preferido por los jugadores para disfrutar de los juegos, ya sean online u offline. Actualmente, son tres las consolas que dominan el mercado en número de ventas: Wii de Nintendo, Xbox 360 de Microsoft y Play Station 3 de Sony.

Todas estas consolas disponen de la capacidad de jugar online aunque en cada una de ellas, es diferente el método de acceso. Por ejemplo, en la plataforma de Microsoft, llamada Xbox Live, para poder acceder se necesita estar suscrito y pagar una cuota. En cambio, para acceder a la plataforma online de Sony Play Station 3, la PlayStation Network, es necesario abrir una cuenta, aunque en este caso gratuita. Por último, Wii también dispone de su propia plataforma de juego online; en este caso, el jugador no tiene que abrir ninguna cuenta especial para poder jugar contra otros jugadores vía Internet.

Típicamente se ha pensado que debido a que las plataformas sobre las que corren las consolas son propietarias, los juegos son seguros y no existen virus adaptados a las videoconsolas.
Para ser más exactos, y según un estudio reciente realizado por la Universidad Europea de Madrid, el 79,1% de los encuestados entre 18 y 45 años considera que los virus y el Spyware no afectan a las videoconsolas [8]. Esto se ha demostrado que no es totalmente cierto, y aunque no llega al nivel de los ordenadores, han aparecido muestras de programas maliciosos para consolas.

Xbox 360

Xbox 360 es la consola de sobremesa de Microsoft. Fue desarrollada en colaboración con IBM y ATI y lanzada al mercado en 2006. Su servicio Xbox Live permite a los jugadores competir en línea y descargar contenidos como juegos arcade, demos, trailers, programas de televisión y películas. Hasta el momento, no se han detectado virus para el sistema operativo de Xbox 360, pero eso no quiere decir que en un futuro próximo no puedan aparecer.

Intento de phishing en Xbox Live

Fuente [9]

Un síntoma de esto último, se puede ver en la fotografía de arriba, donde se expone un intento de ataque de tipo phishing a los jugadores del juego "*Call of Duty Black Ops*". En él, se indica al jugador que su cuenta de Xbox Live va a ser cerrada a menos que envíe su dirección de correo y contraseña. Obviamente, se trata de un engaño que pretende hacerse con las credenciales del jugador.

Aparte de los ordenadores, las consolas también sufren del problema de la piratería. En el caso de la Xbox 360, para que un usuario pueda jugar a copias no originales de un juego, es necesario que modifique el lector de la consola. La modificación del lector acarrea, además de la pérdida de la garantía, algunos problemas para el usuario.

Por ejemplo, Microsoft ha establecido una política para detectar y prohibir la presencia de consolas modificadas jugando en Xbox Live. Para hacer cumplir esta política, Microsoft realiza búsquedas entre todas las consolas conectadas a Xbox Live para determinar las consolas que han sido modificadas y las que no; en caso de encontrar una consola modificada, prohibiría el acceso de forma indeterminada a Xbox Live a esa consola, lo que se conoce comúnmente como baneo.

Recientemente, Microsoft ha lanzado al mercado un nuevo dispositivo que permite interactuar mediante sensores de movimiento y cámaras con el jugador analizando sus movimientos.

Este dispositivo, conocido como Kinect, se está utilizando en multitud de juegos donde el jugador, mediante movimientos reales, controla al

personaje. Pero no solo está siendo utilizado por los juegos, sino que también el *malware* ha visto la posibilidad de utilizar este nuevo dispositivo.

Ha aparecido *malware* que se aprovecha de Xbox Kinect para realizar acciones ilícitas. Para ser más exactos, más que *malware*, es una prueba de concepto realizada por un joven investigador, y que ha demostrado la capacidad de usar Kinect como cámara espía.

El *malware* utiliza las capacidades de detección de movimiento y las cámaras para realizar fotos cuando detecta movimiento. Una vez realizadas las fotos, es capaz de enviarlas por Internet a una cuenta de Picassa controlada por el creador del código [10].

Play Station 3

La consola Play Station 3, también conocida como PS3, es la alternativa de Sony a la Xbox 360 de Microsoft. Fue lanzada a finales de 2006 y fue la primera en utilizar una nueva tecnología para los soportes de los juegos conocida como Blue-Ray.

Al igual que en la consola de Microsoft, no se conoce ninguna muestra de *malware* que esté afectando masivamente a la PS3 para provocarle malfuncionamientos, aunque como se ha visto en la introducción, existen casos aislados donde la consola ha sido utilizada como parte de una botnet.

Al igual que la Xbox 360, en la Play Station 3 ha sido posible la modificación de componentes internos para permitir la ejecución de software no autorizado por Sony. Esta modificación ha permitido a los usuarios ejecutar programas como reproductores de video y de música, pero también ha permitido la piratería de juegos. Para realizar esta modificación, los jugadores debían realizar una arriesgada operación para sustituir el sistema operativo de la consola por otro en el que las protecciones de Sony estaban parcialmente desactivadas.

Esta modificación provocó que algunos jugadores estuvieran a punto de dañar irreparablemente sus consolas cuando intentaron modificar el sistema operativo.

Aparte de los problemas que sufrieron algunos usuarios al modificar la consola, los jugadores también han

tenido problemas con la plataforma de juego online de Sony, conocida como PlayStation Network. El 2 de mayo de 2011, ésta sufrió una intrusión por parte de atacantes desconocidos, los cuales tuvieron acceso a 77 millones de cuentas [11]. Entre otros datos, tuvieron acceso al nombre, a la dirección de correo electrónico y, el más importante, al número de tarjeta de crédito.

Esta intrusión provocó que Sony tuviera que cerrar PlayStation Network hasta que las causas de la intrusión fuesen esclarecidas. El 17 de mayo, Sony reabrió el acceso a todos sus usuarios, pero obligándoles a reestablecer su contraseña para minimizar el daño. Sin embargo, el mismo día, desde el blog de la compañía F-Secure, se advirtió que este mecanismo no era seguro, y que un atacante podría reestablecer la contraseña de otro usuario, tomando el control de su cuenta.

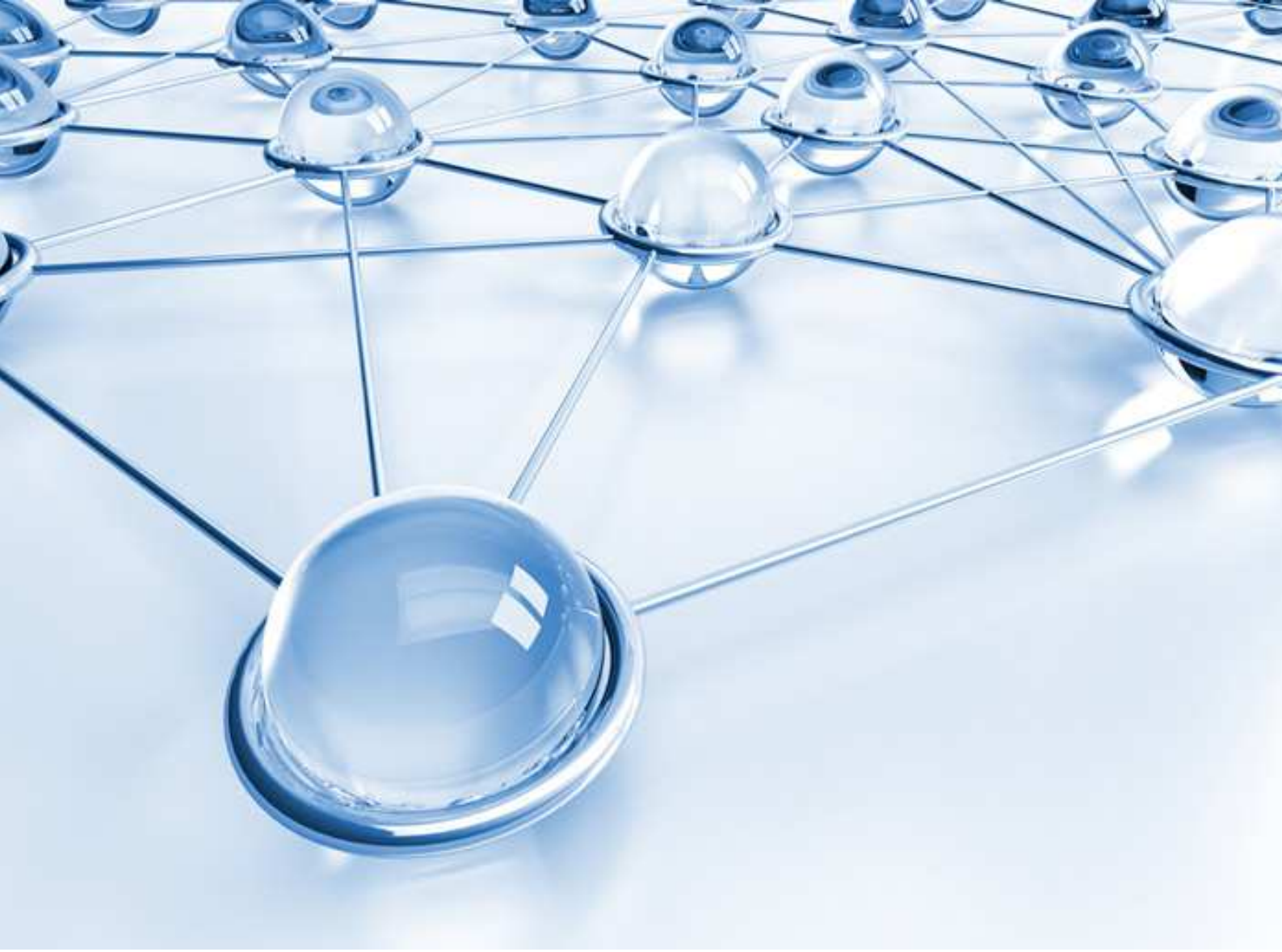
Wii

La Nintendo Wii revolucionó el mundo del videojuego en 2006, cuando salió al mercado y mostró al público su novedoso interfaz. Wii fue la primera consola en la cual el jugador debía de moverse realmente para realizar acciones en el juego.

La seguridad de la consola ha sido vulnerada en varias ocasiones, permitiendo a los desarrolladores ejecutar código no autorizado por Nintendo. Esto ha provocado, que desarrolladores independientes de todo el mundo puedan crear nuevos juegos y aplicaciones sin la aprobación de Nintendo.

Al igual que en la Play Station 3, para poder realizar estas acciones se tenía que modificar el sistema operativo de la consola, con el consiguiente riesgo de deteriorar de forma irrevocable el dispositivo.

La consecuencia de estas modificaciones para el usuario final de las partidas online, ha sido la aparición de juegos modificados que permiten a los jugadores utilizar sistemas para vencer a sus contrincantes, disminuyendo así el valor de las partidas multijugador. Después de recibir múltiples quejas por parte de los usuarios de Wii, Nintendo estableció controles de seguridad por los cuales se impedía que jugadores que realizaban acciones ilícitas en las partidas online se pudieran conectar de nuevo.



Redes sociales

Las redes sociales han sido un fenómeno de masas en los últimos años. Desde su aparición, el crecimiento en forma de número de usuarios ha sido prácticamente exponencial, llegando hasta el punto actual, donde es extraño que alguna persona no tenga cuenta en alguna red social.

Las redes sociales también han sido para los desarrolladores de videojuegos un nuevo espacio en el cual desarrollar su negocio, más aún cuando las diferentes redes han puesto los medios para poder desarrollar juegos colaborativos mediante la publicación de interfaces públicos de programación (API).

Facebook

Facebook es sin duda la red social por excelencia. Desde su inicio en 2004, Facebook ha crecido hasta llegar a ser, con 800 millones de usuarios, la red social más grande de la actualidad.

Su enfoque ha sido el de conectar a personas de diferentes partes del mundo mediante vínculos virtuales de amistad, permitido a personas de todo el mundo compartir sus fotos, pensamientos, opiniones...

Aparte de esto, también permite a los usuarios jugar a juegos online, poniendo especial atención en el aspecto social de los mismos. Un gran ejemplo de estos juegos es FarmVille, uno de los tres juegos con más usuarios en Facebook, donde los jugadores deben crear una granja y cuidar de los animales y de la cosecha. En el juego, se puede invitar a los “amigos” de Facebook para que sean vecinos en la granja y así colaborar en el desarrollo del juego.

Imagen del conocido juego FarmVille

FarmVille también fue uno de los juegos pioneros en notificar en el muro de los jugadores información relativa al juego en nombre de los usuarios. Por ejemplo, en la siguiente imagen se muestra una publicación en la que un jugador ofrece un ítem del juego para el primer contacto que pulse sobre el enlace:

Usuario ofreciendo un ítem del juego en el muro de Facebook

Este comportamiento por parte de los juegos, ha sentado un precedente en las costumbres de los usuarios de Facebook, que han asociado las publicaciones en el muro por parte de sus contactos como publicaciones lícitas.

El tiempo ha demostrado que detrás de algunas publicaciones de los juegos se encontraban virus, troyanos y estafas en general. Un ejemplo de estas publicaciones lo tenemos en la reciente aparición de un

supuesto juego en Facebook que permitía jugar a Mario Kart [20]:

Publicación en el muro invitando a jugar a Mario Kart

Una vez el usuario pulsaba sobre el link, era dirigido a una Web donde se le instaba a instalar un complemento para el navegador. Como el lector imaginará, no se trataba de ningún complemento, sino de un virus que tomaba el control del PC y publicaba el mismo mensaje en el muro del incauto jugador para expandir la cantidad de usuarios infectados. Pero no solo se publicaba en el muro, sino que utilizaba el sistema de mensajería privada del portal para distribuirse:

Mensaje privado incitando a visitar el enlace malicioso

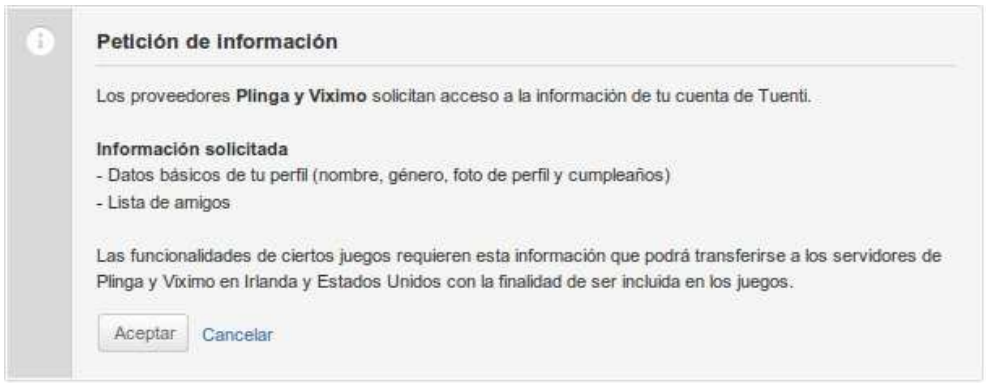
Tuenti

Tuenti es la red social que ha planteado la alternativa, en cuanto a número de usuarios, a la todopoderosa Facebook. Desde noviembre de 2006 y mediante invitación, ha sido posible unirse a la red social para compartir con amigos y conocidos fotos, videos y demás información. En la actualidad, es propiedad de Telefónica y cuenta con más de 12 millones de usuarios.

Tuenti estrenó el día 2 de junio de 2010 una funcionalidad llamada Tuenti Juegos. Esta nueva función permite jugar en tiempo real con la red de amigos de un usuario. Los juegos están servidos por Metrogames, por lo que a diferencia de Facebook no hay terceras personas que puedan añadir nuevos juegos a la plataforma.

Al igual que Facebook, Tuenti indica antes de jugar a cualquier juego los datos a los que se va a acceder.

Petición de Información en Tuenti



También publica en nombre del usuario sus progresos en el juego.

Juego publicando información en nombre del usuario

Otras redes sociales

Aparte de Facebook y Tuenti, existen multitud de redes sociales que también permiten jugar a sus usuarios. Por ejemplo, la reciente Google+ tiene al igual que Tuenti, un apartado en su página donde se puede jugar.
En concreto son 21 los juegos en la fecha de creación de este informe.

Debido al corto tiempo que Google+ se encuentra en marcha, todavía no se conoce ningún juego que intente realizar acciones maliciosas sobre los datos del usuario.

Teléfonos móviles

Con el avance de las nuevas tecnologías, los videojuegos han movido sus plataformas desde las típicas consolas u ordenadores personales a los recientes smartphones (teléfonos inteligentes).

Dentro de la categoría de los smartphones, destacan dos sobre todos los demás: Android y iPhone, por ser las plataformas para las que se desarrollan más juegos.
Al igual que en los ordenadores, el crimen organizado ha visto esta nueva plataforma como una forma más de hacer dinero mediante acciones ilícitas.

El método más usado para conseguir sus propósitos está siendo la modificación de aplicaciones lícitas para añadirles funcionalidades que les reporten beneficios. Típicamente, suelen añadir funciones para enviar mensajes SMS Premium que generan un coste alto a los usuarios o para recabar sus datos privados [12].

Android

Android es el sistema operativo propiedad de Google, lanzado en 2008 y que está basado en el sistema operativo de código libre GNU-Linux. Desde su aparición, Android ha sido un sistema operativo con muy buena acogida por parte de los usuarios que lo han llevado a ser el sistema operativo móvil mas vendido en el último año con un 48% del mercado [13].

Android posee una tienda virtual llamada Market donde los desarrolladores pueden enviar sus aplicaciones para que los usuarios las descarguen. Google es la encargada de mantener el Market y asegurar que las aplicaciones que se suben son seguras.

Este último punto se ha demostrado que no es tan eficaz como debería de ser, ya que se han realizado pruebas de concepto donde se ha podido subir aplicaciones con *malware* al Market sin que Google tuviera conocimiento [14].

Modelos de seguridad Android

Android ha implementado diversos mecanismos para garantizar la seguridad de su sistema operativo. Por ejemplo, Android obliga a que las aplicaciones deban estar firmadas digitalmente y que los desarrolladores compartan el certificado con Google para que puedan publicar la aplicación en el *Market*. También incorpora un mecanismo para aislar las diferentes aplicaciones entre ellas, evitando así que una aplicación pueda obtener datos de otra. Esto ocurre gracias al sistema de permisos por el cual, solo se puede acceder a los recursos que explícitamente se requieran.

Aunque el modelo de seguridad de Android es una gran mejora respecto a los sistemas operativos tradicionales de escritorio, este tiene dos grandes inconvenientes:

El sistema que utiliza Android para obtener el origen de una aplicación podría permitir a un usuario malintencionado crear y distribuir *malware* anónimamente.

El sistema de permisos que utiliza, aunque extremadamente potente, deja en último lugar las decisiones de seguridad al usuario. Desafortunadamente, la mayoría de los usuarios no son técnicamente capaces de tomar esas decisiones, provocando que se instalen aplicaciones que requieren más permisos de los necesarios.

Estudio sobre los permisos requeridos

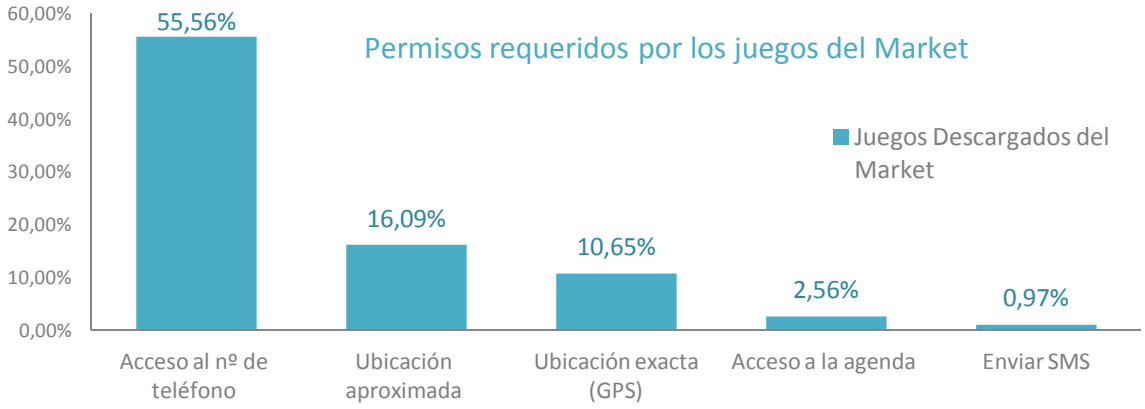
Basándose en estos dos inconvenientes, los creadores de *malware* han aprovechado para modificar aplicaciones lícitas y añadirles funcionalidades como el envío de SMS o el acceso a datos personales.

Como no se disponen de datos sobre *malware* en juegos de Android o sobre los permisos que requieren los diferentes juegos, se ha realizado una investigación para determinar el porcentaje de aplicaciones que solicitan permisos y qué tipo de permisos se solicitan.

Los datos han sido recabados de la Web **https://market.android.com** y se han analizado un total de 3387 juegos, incluyendo los juegos gratuitos y los de pago. A continuación se muestra una relación de los 20 permisos más demandados por los juegos del sistema operativo Android:

Porcentaje	Nº de Aplicaciones	Permiso
93.20%	3157	Acceso íntegro a Internet
74.25%	2515	Ver estado de la red
55.56%	1882	Leer la identidad y el estado del teléfono
39.76%	1347	Modificar o eliminar el contenido de la tarjeta SD
29.79%	1009	Controlar vibración
21.64%	733	Impedir que el dispositivo entre en modo de suspensión
16.09%	545	Ubicación común (basada en red)
14.70%	498	Recuperar aplicaciones en ejecución
10.65%	361	Precisar la ubicación (GPS)
10.56%	358	Establecer fondo de pantalla
9.77%	331	Ver estado de WiFi
9.03%	306	Activar y desactivar sistemas de archivos
6.96%	236	Detectar cuentas reconocidas
4.81%	163	Ejecutar automáticamente al iniciar
2.56%	87	Leer datos de contacto
2.50%	85	Llamar directamente a números de teléfono
2.50%	85	Recibir datos de Internet
1.97%	67	Realizar fotografías y vídeos
1.003%	34	Escribir datos de contacto
0.974%	33	Enviar mensajes SMS

De entre los muchos permisos, hemos querido destacar en la siguiente gráfica los que se han considerado como más críticos respecto a la seguridad del jugador.



De la Figura anterior se extrae que aproximadamente **la mitad de los juegos tienen acceso al número de teléfono** y al IMEI.

También cabe destacar que casi **1 de cada 4 aplicaciones tiene permisos para obtener nuestra ubicación**.

Por último, un permiso que a priori no debería de pedir un juego, como es **enviar SMS, es requerido por el 1% de los juegos**.

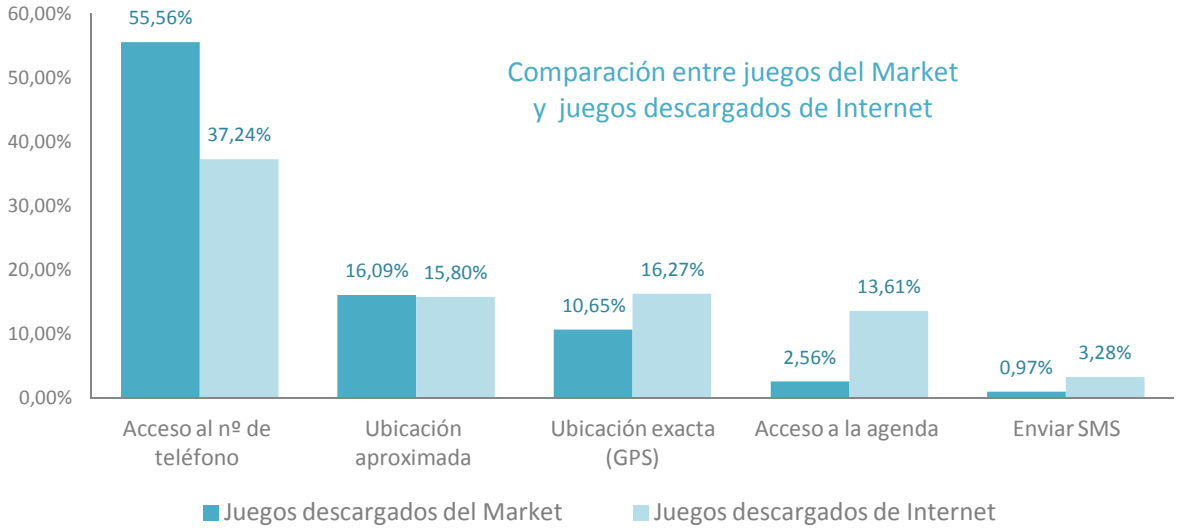
Como hemos indicado, Google realiza un control sobre las aplicaciones que se exponen en el Market, pero debido a lo fácil que resulta para los desarrolladores modificar las aplicaciones de Android han aparecido "Markets" alternativos con aplicaciones modificadas para no tener que pagar por ellas.

Al igual que ocurre con los cracks para los PCs, no tenemos la certeza de que las aplicaciones descargadas no cometan acciones ilícitas aparte de las que son visibles por el usuario.

Ha sido nuestra voluntad establecer si existen diferencias notables entre los permisos que requieren las aplicaciones del Market y los permisos que requieren las aplicaciones descargadas de Internet. Para ello, se ha realizado una descarga masiva de aplicaciones de una web de descargas y se ha realizado un análisis similar al mostrado anteriormente con las aplicaciones del Market.

En total, se han analizado un total de 639 ficheros provenientes de la página web de descargas **www.4shared.com**.

Como se observa en el gráfico siguiente, la distribución porcentual de los permisos requeridos es diferente, siendo los juegos descargados de Internet los que piden, en un porcentaje mayor, permisos de los considerados como "peligrosos".



Este resultado, nos confirma algo que a priori parecía esperado: los juegos descargados del Market son en principio menos peligrosos que los descargados de Internet.

Desgraciadamente, el usuario no solo debe de preocuparse por los juegos que puedan contener *malware*, ya que como se ha demostrado en un reciente estudio [15], juegos muy conocidos por todos los usuarios de Android como Angry Birds, a pesar de ser marcados como seguros, acceden a información como el país, la ciudad, coordenadas y nombre del propietario poniendo en peligro la privacidad del jugador.

Además se sospecha que podría compartir esa información con hasta 17 diferentes dominios para su posterior explotación.

iOS

iOS es el sistema operativo que usan los dispositivos de Apple iPod, iPhone y iPad. Es una versión reducida del sistema operativo de Apple OS X

aunque no compatible con él. Apple presentó el primer iPhone el 29 de junio de 2007, batiendo todos los récords de ventas.

Al igual que Android (y un año antes), una de las grandes novedades fue la App Store, una plataforma donde los desarrolladores podían exponer y vender sus aplicaciones al público.

Apple, desmarcándose de la política de Google, ha establecido un control mucho más estricto para la publicación de aplicaciones en su App Store, denegando el permiso a muchas aplicaciones, ya sea por peligrosas o por que no cumplan con los requisitos de calidad que Apple establece.

En lo que refiere a los juegos online, a partir de la versión 4 de iOS, Apple ha introducido su Game Center, una plataforma para que los poseedores de un dispositivo con iOS puedan jugar entre sí de una forma centralizada manteniendo las puntuaciones de todos los usuarios.

Modelos de seguridad iOS

Apple ha tenido la seguridad de su plataforma muy en cuenta desde el diseño. Ha basado su sistema de seguridad en cuatro pilares: el cifrado, el origen de las aplicaciones, el aislamiento y el modelo de permisos.

El sistema de cifrado provee una fuerte protección sobre los correos electrónicos y sus adjuntos, permitiendo el borrado seguro de información (aunque se ha demostrado que un atacante con acceso físico al terminal podría conseguir acceder a los datos sensibles [4]).

Su sistema de control del origen de las aplicaciones asegura que Apple revisa prácticamente todas las aplicaciones (y por extensión juegos) que se publican en la App Store. Este comportamiento, ha provocado que el número de aplicaciones maliciosas distribuidas en el sitio oficial de Apple sea prácticamente nulo.

El modelo de permisos asegura que las aplicaciones no pueden obtener la localización del dispositivo, enviar SMS o iniciar llamadas sin el permiso explicito del usuario, pudiendo este

último revocar en cualquier momento estos permisos.

Otro de los aciertos del modelo se seguridad de Apple ha sido el correcto aislamiento de las aplicaciones entre ellas y con el núcleo del sistema operativo. Esto provoca que una aplicación no pueda hacerse con el control del dispositivo ni acceder a los datos de las demás aplicaciones.

Este acierto de diseño ha sufrido recientemente un duro revés cuando el investigador Charlie Miller ha mostrado como una aplicación validada por Apple puede ejecutar código sin firmar. Según el ejemplo que expone el propio Miller, un juego como podría ser Angry Birds podría pasar por el filtrado de Apple y realizar acciones maliciosas a voluntad del atacante [15], como por ejemplo leer los SMS, los datos almacenados en el teléfono o enviar la posición GPS del dispositivo.

En la imagen siguiente se observa la prueba de concepto de este ataque, donde un iPhone se conecta a un servidor externo y se descarga código malicioso que hace que el atacante tome el control del teléfono.

iPhone ejecutando código no firmado

Fuente [19]

Desde la aparición de iOS, los usuarios han mostrado su descontento con las limitaciones impuestas por Apple a la hora de aceptar aplicaciones en la App Store. Para saltarse esa limitación, investigadores de seguridad han trabajado en el desbloqueo, o *jailbreak*, del teléfono, que permite tener total control sobre éste. Este control total

es un arma de doble filo, ya que al igual que permite al usuario decidir qué ocurre en su teléfono, también evade todas las restricciones de seguridad de Apple y podría permitir a una aplicación maliciosa tomar el control del teléfono móvil.

Juegos en iOS

A partir de la versión 4 del sistema operativo, Apple ha incorporado una plataforma de juego online para que todos los usuarios puedan jugar entre ellos retándose para conseguir mejores puntuaciones. Esta plataforma se llama Game Center:

Además de la opción de compartir la puntuación con los demás usuarios, Game Center tiene capacidades de Red Social, permitiendo a los usuarios agregar amigos para volver a jugar con ellos de forma rápida. Debido a que no hay datos sobre cómo se comparte la información entre los usuarios y Apple, se ha analizado el tráfico que se produce durante una partida normal.

El resultado ha sido bastante satisfactorio, dado que la mayor parte de tráfico generado, especialmente el

relativo a datos personales, viaja cifrado por Internet garantizando a los usuarios que ningún atacante que pueda ver ese envío lo pueda interpretar.

En cambio, Game Center distribuye por defecto el nombre real del jugador cuando éste invita como amigo a otro usuario. Como se observa en la siguiente imagen, por defecto, cuando se intenta agregar a un amigo, se añade un texto automáticamente en el que aparece el nombre completo del jugador obtenido del propio teléfono móvil.

Seguridad de las personas

A lo largo del documento, se ha analizado la seguridad en el ámbito telemático de los videojuegos online en los distintos dispositivos. Es importante también ofrecer una visión de los problemas o mejoras en el cuerpo humano que este entretenimiento puede provocar.

Un tema preocupante es la cantidad de horas que las personas dedican a diario a formar parte de estos mundos virtuales. Otro el contenido violento, la discriminación y las adicciones que algunos videojuegos promueven.

No obstante, también existen aspectos positivos a tener en cuenta en relación con la salud de los jugadores.

Atendiendo a la parte menos positiva de este punto, la adicción al videojuego online ha provocado numerosos casos de muerte. Una impactante noticia [16], es la de un estudiante coreano que falleció después de pasar 8 horas seguidas en una maratón de juego online, descansando una hora para regresar a su domicilio y continuar 4 horas más.

Los casos de muerte provocados por cansancio, deshidratación y dejadez han ocurrido por la recientemente aparecida adicción a los videojuegos, que ha hecho saltar todas las alarmas.

El gobierno surcoreano tomó una polémica medida que consistía en restringir las horas de juego por usuario. Esto es posible mediante la asignación de un “número de registro residencial”, método parecido al que han adoptado editoras como Square Enix. Por ejemplo, en el juego Final Fantasy XIV se ha usado la estrategia de sumar puntos de experiencia durante un máximo de 15 horas semanales. De esta forma, aunque un jugador pase muchas horas a la semana, solo podrá avanzar en el juego durante 15 horas, evitando así el estrés que supone a los jugadores el tener que mejorar constantemente su personaje.

Según este reciente artículo , el Instituto Nacional de medios y familia de la universidad de Iowa observó algunos síntomas significativos en el jugador con adicción a videojuegos:

Síntomas de adicción

Uso del tiempo libre para jugar

Dormirse en clase

No hacer las tareas

Bajo rendimiento escolar

Mentir sobre el uso de los videojuegos

Preferir jugar en vez de ver a sus amigos o salir

Robar dinero para comprar juegos

Enfados por no jugar

Desordenes del sueño

Ojos secos

Dolores de cabeza

Problemas de higiene

Distorsiones afectivas

Según la investigación, para poder afirmar que una persona es dependiente de los videojuegos, debe reunir al menos 6 de las características citadas.

Entre todos los tipos de videojuegos, encontramos los llamados multijugador masivos en línea o MMORPG (*massively multiplayer online role-playing game*).

Estos hacen posible que miles de usuarios puedan jugar a la vez e interactuar entre ellos desde cualquier parte del mundo a través de Internet.

Ellos crean su propio personaje, del cual deciden una gran variedad de características, y una vez creado pasan a introducirlo en el juego.

Dentro del videojuego, el personaje debe superar retos o misiones para aumentar niveles y generalmente obtener experiencia en retos contra los demás personajes de otros jugadores. Este es el aspecto que mayor adicción genera al usuario, pues en la mayoría de los casos sus personajes están creados con características que a ellos como personas físicas les gustaría tener.

Así, el juego es una forma de hacer "realidad" algunas metas inalcanzables, y los adictos se olvidan de todo para poder conseguirlos. Por este motivo este tipo de videojuegos son los principales responsables de muchos problemas físicos del jugador, hasta causa de muerte en casos extremos.

Por suerte, no todos los efectos de los videojuegos son nocivos para los jugadores.

Según Daphne Bavelier, profesora de ciencias cognitivas y del cerebro en la Universidad de Rochester [17], los videojuegos tienen mucho que ofrecer a nuestra vista.

Según la investigación realizada, los videojuegos de acción mejoran la vista durante meses e incluso años.

Los videojuegos han recibido siempre acusaciones de ser perjudiciales para la vista, y esto es cierto, sobretodo para personas con miopía que sufren estrés adicional y usan sus gafas concentrándose en un punto durante periodos prolongados. Sin embargo, esto se puede evitar haciendo ejercicios de relajación ocular mientras se está delante de la pantalla.

Conclusiones

En este informe se ha tratado de mostrar una instantánea del estado actual de la seguridad en los juegos online y de los problemas a los que se puede enfrentar un jugador.

Como se ha mostrado, la llegada de las nuevas plataformas y tecnologías ha sido aprovechada tanto por los desarrolladores de videojuegos como por los desarrolladores de *malware*, que han conseguido introducirse en prácticamente todas las plataformas.

A pesar del aumento de la diversidad, dos son las categorías preferidas por los jugadores: el PC y las consolas.

Así, hemos visto como un jugador online se enfrenta a peligros como el phishing, en el que intentan robarle las credenciales; la ingeniería social, en la que los atacantes tratan de que el jugador les dé los datos de su cuenta, o la adicción a los videojuegos.

En lo referente a los ordenadores, hay que destacar el análisis realizado sobre una muestra representativa de los programas utilizados para eludir las restricciones anticopia. Este análisis, nos ha brindado el dato de que al menos el 3% de los cracks analizados contenían algún tipo de *malware*. Pero los cracks infectados no son el único problema al que se enfrentan los usuarios de PC. Recientemente, la plataforma de juego online Steam, ha sido atacada y se han conseguido extraer los datos de los usuarios registrados entre los que se encontraban usuario, contraseña, dirección…

Las videoconsolas no se han librado de los peligros que conlleva el juego online. Así, se ha mostrado como consolas como Wii de Nintendo o Play Station 3 de Sony, han formado parte de redes de equipos zombie a merced del atacante, o como un dispositivo de la Xbox 360 de Microsoft llamado Kinect era utilizado en una prueba de concepto para tomar fotografías de los jugadores y enviarlas al atacante. Aparte de los casos de *malware*, el usuario que modifique la videoconsola para poder jugar a copias ilegales se enfrenta a la posibilidad de que no pueda acceder a la plataforma online debido al bloqueo realizado por las compañías como Sony, Microsoft y Nintendo.

Las redes sociales han sabido integrar el entretenimiento online entre sus características. El caso mas representativo es el de Facebook, que gracias a permitir que los desarrolladores publiquen juegos, ha conseguido obtener la práctica hegemonía en los juegos sociales. Este carácter social también ha sido aprovechado por el *malware* para distribuirse de forma viral mediante publicaciones sugerentes hacia los demás usuarios. De esta forma se ha conseguido propagar virus mediante la red social. Sus competidores, Tuenti y Google+, tienen una política de publicación de juegos mucho más restrictiva. En el caso de Tuenti, es una

empresa colaboradora con Tuenti la encargada de realizar los juegos, lo que provoca que el *malware* sea prácticamente inexistente. El caso de Google+ es parecido al de Facebook, pero debido a su corto tiempo de vida, la diversidad de juegos es a día de hoy muy reducida.

En lo referente a dispositivos móviles, Android e iOS son actualmente los sistemas operativos predominantes. Los dos sistemas han planteado estrategias diferentes a la hora de proteger al usuario frente amenazas.

Android ha elegido que caiga sobre el usuario la responsabilidad de elegir qué permisos tiene un juego. El problema es que no todos los usuarios están capacitados técnicamente para tomar estas decisiones. Se ha demostrado además cómo las aplicaciones descargadas de páginas de Internet son mas abusivas respecto al número de permisos que piden al usuario.

Apple, en cambio, ha utilizado la estrategia de poner serias restricciones para la publicación de aplicaciones, tratando de esta forma de reducir el *malware* en los dispositivos con iOS. En lo que respecta a juegos online, iOS dispone de una plataforma centralizada para el juego online. Por lo que se ha podido comprobar, los datos del usuario viajan cifrados entre el teléfono y los servidores que alojan los juegos.

Sin embargo, cuando un usuario intenta agregar a otro como amigo para poder jugar posteriormente, iOS escribe un mensaje por defecto que incluye el nombre completo del propietario de la cuenta. Esto podría poner en peligro la privacidad del jugador.

Por último, hay que hacer notar que todas las medidas de seguridad implantadas por Google o Apple en sus teléfonos, no sirven para nada si los dispositivos son modificados para tener total control de ellos. Esto es lo que en el argot se llamaría *"rootear"* o *"realizar el jailbreak"* al teléfono.

Los videojuegos online no sólo pueden provocar problemas para la salud de las máquinas, sino que en ciertos casos, estos problemas pueden afectar a la salud física del jugador. Existen juegos, donde la dinámica del mismo hace que los jugadores se sientan estresados mientras juegan, creándoles adicción a los mismos. En casos extremos, se ha llegado incluso a la muerte de alguna persona debido a la excesiva cantidad de horas jugadas.

Por todo esto, es necesario concienciar a los usuarios de videojuegos online de que existen peligros en los videojuegos, y que contrariamente a lo que se pensaba hasta hace poco tiempo, el *malware* está atacando a los videojuegos en todas las plataformas. Las previsiones no son mucho mejores para los próximos años, y se espera que en un futuro próximo los ataques a consolas sean mucho más frecuentes y masivos.

Decálogo de seguridad en juegos online

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 dispositivo 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 preferible descargarlos de fuentes oficiales.

7. En las redes sociales hay que desconfiar de los mensajes sospechosos que nos envíen los usuarios, ya que podrían ser un virus.

8. Es muy recomendable tener instalado, tanto en los ordenadores como en los dispositivos móviles un buen antivirus.

9. Es recomendable no introducir el número de tarjeta de crédito si no es estrictamente necesario.

10. La concienciación en materia de seguridad es muy importante: todos los usuarios son posibles víctimas de ataques.

Referencias

[1] "INTECO y aDeSe ponen en marcha una campaña de divulgación para fomentar el consumo responsable de videojuegos". 16, Diciembre 2010. http://www.red.es/notas-prensa/articles/id/5052/inteco-adese-ponen-marcha-una-campana-divulgacion-para-fomentar--consumo-responsable-videojuegos.html

[2] "Adicción a los videojuegos". 26 Octubre, 2011. http://sickmind.com.ar/blog/?p=1205

[3] "Welcome to the new gold mines". 3 Mayo, 2010. http://www.guardian.co.uk/technology/2009/mar/05/virtual-world-china

[4] "WoW account phising" 26 Julio, 2010. http://www.f-secure.com/weblog/archives/00001995.html

[5] "MMORPG Trojans Abound". 1 Septiembre, 2011. http://antivirus.about.com/od/emailscams/a/mmorpg_hacks.htm

[6] "El mercado negro del cibercrimen al descubierto". 20 Enero, 2011. http://prensa.pandasecurity.com/2011/01/el-mercado-negro-del-cibercrimen-al-descubierto

[7] "¿*Malware* en consolas?". 6 Septiembre, 2010. http://blogs.protegerse.com/laboratorio/2010/09/06/%C2%BF*malware*-en-consolas/

[8] "Seguridad y videojugadores". 12 Mayo, 2011. http://www.slideshare.net/joanakin/seguridad-y-videojugadores

[9] "Xbox 360 gamers targeted in phishing attack". 3 Mayo, 2011. http://news.yahoo.com/blogs/technology-blog/xbox-360-gamers-targeted-phishing-attack-225054488.html

[10] "*Malware* for xbox Kinect". 27 Octubre, 2011 http://thehackernews.com/2011/10/*malware*-for-xbox-kinect-created-by-15.html

[11] "Pérdida de datos en la todopoderosa Sony". 4 Mayo, 2011. http://www.securityartwork.es/2011/05/04/perdida-de-datos-en-la-todopoderosa-sony.html

[12] "Everybody is Russian". 15 Noviembre, 2011. http://www.securityartwork.es/2011/11/15/everybody-is-russian/

[13] "Android takes almost 50% share of worldwide smart phone market". 1 Agosto, 2011. http://www.canalys.com/newsroom/android-takes-almost-50-share-worldwide-smart-phone-market

[14] "La cruda realidad del Market de Android". 16 Junio, 2011. http://www.securitybydefault.com/2011/06/la-cruda-realidad-del-market-de-android.html

[15] "Angry Birds know where you live". 9 Noviembre, 2011 http://www.net-security.org/secworld.php?id=11916

[16] "Estudiante coreano muere tras 12 horas jugando online". 29 Diciembre, 2010. http://alt1040.com/2010/12/estudiante-coreano-muere-tras-12-horas-jugando-online

[17] "New research shows action video games can improve vision". http://www.improve-vision-naturally.com/video-games-improve-vision.html

[18] "iPhone Security Bug Lets Innocent-Looking Apps Go Bad". 7 Noviembre, 2011. http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/

[19] "El último hack de Charlie Miller llega a la App Store sin levantar sospechas". 8 Noviembre, 2011 http://es.engadget.com/2011/11/08/el-ultimo-hack-de-charlie-miller-llega-a-la-app-store-sin-levant/

[20] "Mario Kart on Facebook? Fast-spreading scam hits many users' accounts". 26 Octubre, 2011. http://nakedsecurity.sophos.com/2011/10/26/mario-kart-on-facebook-fast-spreading-scam-hits-many-users-accounts/

Usted es libre de

Copiar, distribuir y comunicar públicamente la obra

Remezclar *— transformar la obra*

Hacer un uso comercial de esta obra

Bajo las condiciones siguientes

> ***Reconocimiento*** *— Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).*

Más información en http://creativecommons.org/licenses/by/2.5/es/, o en los datos de contacto indicados.

Contacto

Antonio Villalón Huerta

Director de Seguridad

S2 Grupo

avillalon@s2grupo.es

www.s2grupo.es

www.securityartwork.es