SEGURIDAD EN JUEGOS ONLINE

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 diaria que los jugadores dedican a los videojuegos en promedio ha aumentado considerablemente hasta llegar a las 5 horas y 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

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. **El género predominante es el de acción, por encima de otros como estrategia, aventuras o deporte.**

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…

La diversidad tecnológica en video juegos no ha sido aprovechada solamente por los desarrolladores de juegos online: los creadores de **malware** también han visto un nuevo "**nicho de mercado**"

OBJETIVO DE LOS HACKERS

Hasta hace unos años, los **hackers**, 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:

- ## 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.

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.

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.

- ## 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, otra de las técnicas utilizadas por los hackers es la de distribuir programas falsos para controlar las máquinas de sus víctimas.

- ## 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 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.

- ## 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.

- **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 computadores, ya que existen casos de consolas Wii y Play Station 3 que formaban parte de una **botnet**

COMPUTADORES

Los computadores 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 computadores 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

Los jugadores que descargan copias piratas de juegos 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.

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.

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 de Microsoft y Play Station 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, 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. Esto se ha demostrado que no es totalmente cierto, y aunque no llega al nivel de los computadores, han aparecido muestras de programas maliciosos para consolas.

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 computadores, las consolas también sufren del problema de la piratería. En el caso de la Xbox, 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. 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, prohibirían el acceso de forma indeterminada a Xbox a esa consola, lo que se conoce comúnmente como **baneo**.

El dispositivo que permite interactuar mediante sensores de movimiento y cámaras con el jugador analizando sus movimientos, 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.

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 SONY Play Station 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, en la Play Station 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 puede provocar 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. Por ejemplo El 2 de mayo de 2011, ésta sufrió una intrusión por parte de atacantes desconocidos, los cuales tuvieron acceso a 77 millones de cuentas. 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 restablecer 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 restablecer la contraseña de otro usuario, tomando el control de su cuenta.

TELÉFONOS MÓVILES

Con el avance de las nuevas tecnologías, los videojuegos han movido sus plataformas desde las típicas consolas u computadores personales a los Smartphone

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 computadores, 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.

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 más vendido.

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.

Desgraciadamente, el usuario no solo debe de preocuparse por los juegos que puedan contener malware, ya que como se ha demostrado en estudios, 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**

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.

SEGURIDAD DE LAS PERSONAS

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

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.

Entre todos los tipos de videojuegos, encontramos los llamados **multijugador** masivos en línea o **MMORPG**

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

¿ERES ADICTO A LOS 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 sus investigaciones, para poder afirmar que una persona es dependiente de jugar a videojuegos, debe reunir **al menos 6** de estas características citadas

DECÁLOGO DE SEGURIDAD EN JUEGOS ONLINE

1. Tener un computador 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 computadores 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/notasprensa/articles/id/5052/inteco-adeseponen-marcha-una-campanadivulgacion-para-fomentar--consumoresponsable-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/technolog y/2009/mar/05/virtual-world-china

[4] “WoW account phising” 26 Julio, 2010. http://www.fsecure.com/weblog/archives/0000199 5.html

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

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

[7] “¿Malware en consolas?”. 6 Septiembre, 2010. http://blogs.protegerse.com/laboratorio/2010/09/06/%C2%BFmalware-enconsolas/

[8] “Seguridad y videojugadores”. 12 Mayo, 2011.

http://www.slideshare.net/joanakin/s eguridad-y-videojugadores

[9] “Xbox 360 gamers targeted in phishing attack”. 3 Mayo, 2011. http://news.yahoo.com/blogs/technol ogy-blog/xbox-360-gamers-targetedphishing-attack-225054488.html

[10] “Malware for xbox Kinect”. 27 Octubre, 2011 http://thehackernews.com/2011/10/ malware-for-xbox-kinect-created-by15.html

[11] “Pérdida de datos en la todopoderosa Sony”. 4 Mayo, 2011. http://www.securityartwork.es/2011/ 05/04/perdida-de-datos-en-latodopoderosa-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/a ndroid-takes-almost-50-shareworldwide-smart-phone-market

[14] “La cruda realidad del Market de Android”. 16 Junio, 2011. http://www.securitybydefault.com/20 11/06/la-cruda-realidad-del-marketde-android.html

[15] “Angry Birds know where you live”. 9 Noviembre, 2011 http://www.netsecurity.org/secworld.php?id=11916